MATERIAŁY DYDAKTYCZNE 138

Nieuprawnione przejęcie konta w serwisach społecznościowych jako problem kwalifikacji prawnej

KATOWICE 2026

st. asp. Konrad Kędzierski

Zakład Służby Kryminalnej

Nieuprawnione przejęcie konta w serwisach społecznościowych jako problem kwalifikacji prawnej

Katowice 2026

Nadzór merytoryczny:
mł. insp. Tomasz Czylok

Redakcja, korekta, skład:
Paweł Mięsiak

Spis treści

Wstęp

Niniejsza publikacja ma na celu wspomóc policjantów w prawidłowym kwalifikowaniu czynów dotyczących nieuprawnionego przejęcia konta w serwisach społecznościowych. Jest skierowana zarówno do funkcjonariuszy szkolenia zawodowego podstawowego, jak i do policjantów wykonujących codzienne zadania służbowe. W opracowaniu skoncentrowano się na problemie nieuprawnionego przejęcia konta w serwisach społecznościowych, ponieważ kwalifikacja takiego zachowania nie zawsze jest oczywista i może obejmować zarówno samo uzyskanie dostępu, jak i późniejsze działania sprawcy, np. zmianę hasła, usunięcie danych, podszywanie się pod właściciela konta albo wykorzystanie konta do dalszych czynów zabronionych. Na potrzeby niniejszego opracowania pojęcie „przejęcia konta" będzie używane zbiorczo. Obejmuje ono uzyskanie nieuprawnionego dostępu do konta, a także późniejsze działania sprawcy, w szczególności zmianę danych dostępowych, uniemożliwienie albo utrudnienie właścicielowi korzystania z konta, ingerencję w dane informatyczne oraz dalsze wykorzystanie konta. Takie ujęcie wydaje się uzasadnione, ponieważ poszczególne etapy jednego zdarzenia mogą prowadzić do rozważenia różnych kwalifikacji prawnych.

Problematyka ta wymaga uwzględnienia zarówno zagadnień prawa karnego, jak i podstawowych zagadnień technicznych. Dopiero łączne spojrzenie na te dwa obszary pozwala prawidłowo ocenić stan faktyczny, opisać zachowanie sprawcy oraz rozważyć właściwą kwalifikację prawną.

Z tego względu pierwszy rozdział poświęcono podstawowym definicjom i pojęciom potrzebnym do analizy przejęcia konta w serwisach społecznościowych. Omówiono w nim w szczególności różnicę między kontem a profilem, między danymi informatycznymi a informacją, a także znaczenie terminu hasło oraz system informatyczny. Drugi rozdział dotyczy samego nieuprawnionego przejęcia konta, a więc przede wszystkim uzyskania dostępu do konta lub profilu, możliwego zapoznania się z informacjami nieprzeznaczonymi dla sprawcy czy też jego nieuprawnionej modyfikacji. Trzeci rozdział obejmuje natomiast dalsze zachowania, które mogą nastąpić po przejęciu konta, w szczególności podszywanie się pod pokrzywdzonego oraz wykorzystanie konta do oszustwa.

Oczywiste jest, że kwalifikacja danego przestępstwa zawsze uzależniona jest od konkretnego stanu faktycznego. Nie jest zatem możliwe przypisanie różnych zdarzeń do jednego, niezmiennego schematu. Niejednokrotnie to szczegóły będą

decydować o przyjęciu określonej kwalifikacji prawnej, a także o ewentualnej kwalifikacji dodatkowej. Celem publikacji nie jest zatem zastąpienie samodzielnej analizy materiału dowodowego, lecz wskazanie poprawnego kierunku rozumowania oraz pewnych stałych zasad, które mogą pomóc zwłaszcza początkującym funkcjonariuszom w unikaniu błędów podczas prowadzenia postępowań przygotowawczych.

Ostatnim zastrzeżeniem, które należy poczynić, jest fakt, że w niektórych przypadkach w doktrynie można znaleźć odmienne stanowiska dotyczące ujęcia danego problemu. Celem publikacji nie jest jednak kategoryczne opowiedzenie się za jednym z rozwiązań, lecz przedstawienie zagadnienia w sposób możliwie praktyczny, uporządkowany i przydatny w codziennej służbie.

Rozdział 1.
Definicje

Rozdział ten stanowi istotny element niniejszego opracowania, zwłaszcza dla osób, które na co dzień nie zajmują się zagadnieniami informatycznymi. Obejmuje on zarówno pojęcia występujące w przepisach art. 267, art. 268 czy art. 268a Kodeksu karnego, jak i określenia używane w praktyce funkcjonowania usług cyfrowych, takie jak konto, profil, hasło czy dostęp. Uporządkowanie i zrozumienie tych pojęć ma fundamentalne znaczenie dla prawidłowego opisania zdarzenia oraz późniejszego rozważenia właściwej kwalifikacji prawnej.

1.1. Konto i profil w serwisach społecznościowych

W odniesieniu do serwisów społecznościowych należałoby odróżniać konto od profilu. Należy rozważyć, czy konto nie jest pojęciem szerszym, ponieważ obejmuje dostęp użytkownika do usługi, dane logowania, ustawienia oraz możliwość korzystania z funkcji serwisu. Profil można natomiast rozumieć jako wyodrębnioną reprezentację użytkownika w danej usłudze. Rozróżnienie to widoczne jest m.in. na platformie Facebook, gdzie odróżnia się konto na Facebooku od profilu na Facebooku oraz wskazuje na profil główny i dodatkowe profile tworzone w ramach usługi[1]. Podobną różnicę można zauważyć także w systemie Profil Zaufany, w którym „konto profilu zaufanego" umożliwia m.in. wnioskowanie o potwierdzenie profilu, używanie profilu, przedłużanie jego ważności i jego unieważnianie, natomiast sam „profil zaufany" jest środkiem identyfikacji elektronicznej zawierającym zestaw danych identyfikujących i opisujących osobę fizyczną[2]. Podobne rozróżnienie możemy znaleźć również w innych usługach cyfrowych. W serwisie Netflix w ramach jednego konta mogą funkcjonować odrębne profile, dla których dostępna jest osobna historia oglądania filmów lub seriali[3]. W systemie Android każdy profil użytkownika może mieć na urządzeniu własny obszar, obejmujący m.in. ekrany główne, aplikacje i ustawienia, przy czym konto pozwala korzystać z usług za pomocą jednej nazwy użytkownika i hasła[4]. Można

[1] Różnica pomiędzy kontem na Facebooku a profilem na Facebooku, Centrum pomocy Facebooka, https://www.facebook.com/help/327202558928776?locale=pl_PL (21.06.2026).
[2] Instrukcja Użytkownika systemu Profil Zaufany, wersja 1.1, 2021, s. 5-7.
[3] Netflix, „How to see viewing history and device activity", Netflix Help Center, https://help.netflix.com/en/node/101917, (21.06.2026).
[4] Google, „Usuwanie, przełączanie i dodawanie użytkowników", Android – Pomoc, https://support.google.com/android/answer/2865483?hl=pl (21.06.2026).

więc przyjąć, że konto odnosi się przede wszystkim do dostępu i kontroli nad usługą, a profil do wyodrębnionej przestrzeni użytkownika, jego danych, ustawień, treści albo aktywności.

1.2. Dane informatyczne

Punktem wyjścia dla zdefiniowania pojęcia „danych informatycznych" powinna być definicja zawarta w art. 1 lit. b Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r., której Polska jest stroną[5]. Zgodnie z nią *„dane informatyczne" oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny*[6]. Pod względem technicznym dane informatyczne stanowią więc zasoby cyfrowe, które muszą zostać „zakodowane" w języku binarnym, czyli ciągu zer i jedynek, tak aby były możliwe do przetwarzania przez systemy komputerowe[7]. Jeszcze inaczej – jest to utrwalony w postaci cyfrowej zapis określonej informacji, znajdujący się na dysku komputera, innym nośniku informatycznym albo w systemie umożliwiającym jej przetwarzanie[8]. Już tutaj należy poczynić jedną z najważniejszych uwag: większość autorów stoi na stanowisku, że utożsamianie pojęcia danych informatycznych i informacji na gruncie prawa karnego jest nieuprawnione, chociaż definiowanie ich jako odrębnych kategorii w innych dziedzinach nauki może nastręczać znacznie większych problemów[9]. Rozróżnienie tych pojęć jest kluczowe do określenia różnych przedmiotów czynności wykonawczej, a w konsekwencji prawidłowej kwalifikacji stanu faktycznego. Jako przykłady danych informatycznych można wymienić zapisy cyfrowe przetwarzane na serwerach, techniczny zapis strony internetowej zanim zostanie odczytany jako zrozumiały komunikat czy program komputerowy[10]. Dobrym przykładem na rozróżnienie danych informatycznych od informacji (zob. punkt 1.3) są dane zaszyfrowane mogące mieć postać plików, baz danych, wiadomości,

[5] Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2014 r. poz. 1514).

[6] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., (Dz.U. z 2015 r. poz. 728), Należy zaznaczyć, że Konwencja w języku angielskim posługuje się wyrażeniem *computer data* czyli dane komputerowe, a polskie tłumaczenie zawiera sformułowanie dane informatyczne. Wyrażenia te należy jednak traktować jako tożsame. Zobacz także: F. Radoniewicz, *Dane komputerowe/informatyczne, Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym – propozycje zmian*, 2024, Legalis (10.06.2026).

[7] P. Opitek, *Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych,* s. 24.

[8] Wyrok Sądu Najwyższego – Izba Karna z dnia 30 września 2015 r. II KK 115/15.

[9] P. Opitek, tamże, s. 23.

[10] F. Radoniewicz, *Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym – propozycje zmian*, 2024, Legalis (10.06.2026 r.).

haseł. Zasoby te zostały przekształcone przy użyciu określonego algorytmu kryptograficznego, aby osoba nieuprawniona nie mogła się z nimi zapoznać. Dla osoby nieposiadającej odpowiedniego klucza lub hasła taki zapis może być niezrozumiały, pozornie pozbawiony treści, z którego nie wynika żadna informacja. Nadal jest jednak zapisem cyfrowym, który może być przechowywany, przesyłany, kopiowany, usuwany, uszkadzany albo przetwarzany przez system informatyczny. Dane zaszyfrowane są więc przykładem danych informatycznych w czystym, technicznym sensie: są nośnikiem potencjalnej informacji, ale na etapie zaszyfrowania występują przede wszystkim jako chroniony zapis cyfrowy.

1.3. Informacje

Informacja jest pewną treścią, znaczeniem albo sensem, który można odczytać z określonego zapisu. Aby informacja mogła zostać przekazana, utrwalona, przechowywana lub przetworzona, musi przybrać określoną postać. Taką postacią są dane. Dane pełnią zatem funkcję nośnika informacji. Mogą występować w różnych formach, na przykład jako zapis literowy, dźwiękowy, graficzny albo cyfrowy. Sama informacja jest natomiast tym, co można z tych danych odczytać, zrozumieć albo odkodować[11]. Jeżeli informacja zostanie zapisana w postaci nadającej się do komputerowego przetwarzania staje się danymi informatycznymi (zob. punkt 1.2). Nie każdy ciąg znaków, kod czy szyfr jest informacją. Informacja oznacza treść, sens albo komunikat, który można odczytać. Jeżeli natomiast dany układ znaków pełni jedynie funkcję techniczną w systemie informatycznym, może stanowić tylko dane informatyczne, a nie informację. W postanowieniu z 5 marca 2019 r. Sąd Najwyższy wskazał, że tzw. boxkey (klucz parujący) nie jest kodem dostępu do informacji, lecz technicznym elementem służącym połączeniu składników systemu informatycznego. Klucz taki nie przekazuje więc samodzielnej treści, ale pełni funkcję techniczną. Z tego względu nie można go traktować jako informację, ale jako szczególny rodzaj danych, czyli dane informatyczne[12, 13].

W razie wątpliwości, czy określony zapis należy traktować jako dane informatyczne, czy już jako informację, pomocne może być stanowisko P. Opitka. Autor zwraca uwagę, że znaczenie może mieć nie tylko sam zapis, ale także możliwość jego odczytania przez odbiorcę. Innymi słowy, ten sam ciąg znaków dla jednej osoby może być jedynie danymi, natomiast dla osoby dysponującej odpowiednią wiedzą

[11] F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym,* s. 135.
[12] Postanowienie Sądu Najwyższego z dnia 05.03.2019 r., II KK 208/18.
[13] P. Opitek, tamże, s. 24.

może stanowić źródło informacji. Wspomniany autor podaje tu przykład numeru karty płatniczej. Dla przeciętnego użytkownika jest to przede wszystkim ciąg cyfr, natomiast osoba znająca zasady budowy karty może odczytać z niego dodatkowe informacje, np. dotyczące wystawcy karty, organizacji płatniczej czy identyfikatora rachunku posiadacza karty[14]. Na zakończenie należy jeszcze zwrócić uwagę na zamiar sprawcy. W praktyce istotne może być ustalenie, czy jego działanie było ukierunkowane na uzyskanie dostępu do informacji, czy do danych informatycznych. Jak wskazuje wcześniej przywołany autor, pod względem technicznym uzyskanie dostępu do systemu może wiązać się jednocześnie z dostępem do danych oraz do informacji wyświetlanych użytkownikowi. Organ procesowy powinien więc ustalić, jaki był rzeczywisty cel działania sprawcy oraz czy chciał on uzyskać dostęp do treści jako informacji czy raczej do danych informatycznych jako elementów funkcjonowania systemu informatycznego (zob. punkt 1.4). Oczywiście nie jest wykluczone działanie w obu powyższych zamiarach[15].

1.4. System informatyczny

Na potrzeby oceny prawnokarnej przejęcia konta znaczenie ma pojęcie systemu informatycznego, które występuje m.in. w art. 267 § 2 Kodeksu karnego. Jednak sam Kodeks karny nie zawiera jego definicji. Dlatego przy wyjaśnianiu tego pojęcia należy odwołać się przede wszystkim do Konwencji Rady Europy o cyberprzestępczości oraz dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne. Zgodnie z Konwencją system informatyczny oznacza „każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych”[16]. Dyrektywa 2013/40/UE ujmuje to pojęcie podobnie, wskazując, że chodzi o „urządzenie lub grupę wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych komputerowych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez to urządzenie lub tę grupę urządzeń, w celach ich eksploatacji, użycia, ochrony lub utrzymania”[17].

[14] Tamże, s. 31-32; por. także: Budowa karty płatniczej: numer karty, awers, rewers, CVC, Moneteo, https://moneteo.com/artykuly/budowa-karty-platniczej, dostęp: 22.06.2026 r.

[15] P. Opitek, tamże, s. 27-28.

[16] Art. 1 lit. a Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r.

[17] Art. 2 lit. a dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW, Dz.Urz. UE L 218 z 14.08.2013 r.

Z przywołanych definicji wynika, że pojęcie systemu informatycznego należy rozumieć szeroko. Może nim być zarówno pojedyncze urządzenie, jak i zespół urządzeń, jeżeli przynajmniej jedno z nich, zgodnie z programem, automatycznie przetwarza dane. W komentarzach wskazuje się przykładowo na komputer, tablet, serwer, smartfon, router, system kamer CCTV, rejestrator DVR, urządzenia IoT (ang. Internet of Things), takie jak inteligentne lodówki, kamery, termostaty czy żarówki, a także konsole do gier, SmartTV, inteligentne liczniki energii oraz systemy przemysłowe[18].

Jednocześnie należy dokładnie opisać czyn dotyczący przejęcia konta w serwisie społecznościowym. Systemem informatycznym nie jest samo konto czy profil ani program komputerowy rozumiany w oderwaniu od urządzenia lub infrastruktury, na której działa. W komentarzu do art. 267 k.k. zwrócono uwagę, że przy uzyskaniu dostępu np. do cudzej skrzynki e-mail właściwe jest wskazanie, że sprawca uzyskał dostęp do systemu informatycznego, na przykład serwera, na którym zainstalowano oprogramowanie służące do obsługi poczty elektronicznej, a nie do samej „skrzynki e-mail" jako systemu[19]. Podobnie przy przejęciu konta w serwisie społecznościowym bardziej precyzyjne wydaje się wskazanie dostępu do części systemu informatycznego umożliwiającej logowanie, wyświetlanie profilu, przesyłanie wiadomości lub zmianę ustawień konta, a nie utożsamianie samego profilu z systemem informatycznym.

Warto również wskazać, że system informatyczny nie jest tym samym co system teleinformatyczny. W komentarzach podkreślono, że system informatyczny nie powinien być utożsamiany z systemem teleinformatycznym. System informatyczny służy przede wszystkim wprowadzaniu, przetwarzaniu i odczytywaniu informacji, natomiast system teleinformatyczny obejmuje także przesyłanie i odbieranie danych przez sieci telekomunikacyjne[20].

1.5. Hasło

Hasła komputerowe należy traktować jako przykłady danych, najczęściej przybierających postać ciągu znaków, które pozwalają uzyskać dostęp do informacji znajdujących się m.in. w systemach informatycznych[21]. W literaturze wskazuje się, że z tego względu pojęcie danych w tym kontekście może obejmować również dane biometryczne, takie jak układ linii papilarnych czy obraz tęczówki oka[22]. W przywołanym już wyroku Sąd

[18] M. Mozgawa, *Kodeks karny. Komentarz aktualizowany do art. 267 k.k.* Lex (20.06.2026).
[19] Tamże.
[20] R.A. Stefański, *Kodeks karny. Komentarz do art. 267 k.k.*, 2025, Legalis (10.06.2026).
[21] R.A. Stefański, *Kodeks karny. Komentarz do art. 269b k.k.*, 2025, Legalis (10.06.2026).
[22] F. Radoniewicz, *Odpowiedzialność...,* s. 332.

Najwyższy, odwołując się do pierwszeństwa wykładni językowej, podkreślił różnicę między „informacją" a takimi pojęciami jak „kod dostępu", „hasło", „szyfr" czy „dane"[23].

Nie można jednak całkowicie wykluczyć, że w konkretnym stanie faktycznym hasło będzie miało także znaczenie informacyjne i będzie przekazywać odbiorcy konkretną treść. P. Opitek zwraca uwagę, że w doktrynie i orzecznictwie sporny jest charakter prawny haseł zabezpieczających dostęp do danych lub informacji. Wskazuje też, że dane mogą stać się informacją wtedy, gdy odbiorca potrafi je zinterpretować i odczytać z nich określony sens. Przykładem może być hasło zawierające imię, nazwisko i rok urodzenia użytkownika, ponieważ taki zapis nie tylko pełni funkcję zabezpieczającą dostęp, lecz także pozwala potencjalnemu sprawcy uzyskać informacje o osobie, od której ono pochodzi. Autor zastrzega jednak, że hasło może być traktowane jako informacja tylko wówczas, gdy celem sprawcy było poznanie samego hasła jako poufnej treści, a nie jedynie wykorzystanie go do uzyskania dostępu do innej wiadomości[24].

1.6. Przełamanie i ominięcie zabezpieczenia

Pojęcia przełamania i ominięcia występują w art. 267 § 1 k.k., który penalizuje m.in. uzyskanie bez uprawnienia dostępu do informacji dla sprawcy nieprzeznaczonej przez przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia[25]. Zabezpieczeniem są takie środki ochrony informacji, które realnie utrudniają dostęp osobom nieuprawnionym, a ich pokonanie wymaga specjalistycznej wiedzy, użycia odpowiedniego narzędzia albo posłużenia się kodem[26]. Dane komputerowe mogą być zabezpieczone na dwa sposoby. Bezpośrednio – na przykład przez ich zaszyfrowanie albo wprowadzenie obowiązku podania hasła przed uzyskaniem dostępu. Pośrednio natomiast są chronione wtedy, gdy znajdują się w systemie informatycznym objętym własnymi mechanizmami ochrony, takimi jak firewall, systemy wykrywania lub zapobiegania atakom czy procedura uwierzytelniania użytkownika[27].

Przełamanie zabezpieczenia należy rozumieć jako bezpośrednie oddziaływanie na mechanizm ochronny w sposób, który pozbawia go funkcji zabezpieczającej. Nie musi ono polegać na fizycznym zniszczeniu zabezpieczenia. Wystarczy, że sprawca doprowadzi do tego, że zabezpieczenie przestaje skutecznie blokować dostęp do informacji[28]. W odniesieniu do konta w serwisach społecznościowych takim zabez-

[23] Postanowienie Sądu Najwyższego z dnia 05.03.2019 r., II KK 208/18.
[24] P. Opitek, tamże, s. 35.
[25] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 267 § 1 k.k.
[26] F. Radoniewicz, *Cyberprzestępstwa...*
[27] Tamże.
[28] Tamże.

pieczeniem będzie najczęściej mechanizm logowania. Podstawową formą ochrony jest login i hasło, ale konto może być również chronione przez uwierzytelnianie dwuskładnikowe, np. kod SMS, kod z aplikacji uwierzytelniającej albo klucz zabezpieczeń. W takim przypadku samo poznanie hasła może nie wystarczyć do uzyskania dostępu do konta, ponieważ sprawca musi jeszcze pokonać drugi element zabezpieczenia[29]. Przełamanie zabezpieczenia konta społecznościowego może polegać np. na odgadnięciu albo złamaniu hasła, przechwyceniu danych logowania, użyciu programu zapisującego znaki wpisywane z klawiatury, posłużeniu się złośliwym oprogramowaniem albo wyłudzeniu danych od użytkownika za pomocą fałszywej strony logowania (zależnie od zastosowanej metody technicznej). Jeżeli konto jest objęte uwierzytelnianiem dwuskładnikowym, należy dodatkowo ustalić, czy sprawca uzyskał także kod jednorazowy, dostęp do aplikacji uwierzytelniającej, karty SIM albo innej metody potwierdzania logowania[30].

W odróżnieniu od przełamania, ominięcie zabezpieczenia nie polega na bezpośrednim oddziaływaniu na mechanizm ochronny, lecz na uzyskaniu dostępu mimo jego istnienia, niejako inną drogą[31]. W przypadku konta w serwisach społecznościowych może to polegać np. na wykorzystaniu aktywnej sesji urządzenia, na którym użytkownik był już zalogowany albo procedury odzyskiwania konta. Nie chodzi więc o złamanie hasła, lecz o wejście do konta bez bezpośredniego pokonywania mechanizmu logowania.

Pozostaje jeszcze kwestia samego posłużenia się poprawnym hasłem lub kodem, nawet bez zgody osoby uprawnionej, które nie będzie ani przełamaniem zabezpieczenia ani jego ominięciem[32]. Zagadnienie to wymaga jednak szerszego omówienia i zostanie rozwinięte w dalszej części pracy.

Podsumowując, jeżeli zabezpieczenie było realne i aktywne, a sprawca je pokonał albo obszedł, możemy mówić o realizacji znamienia przełamania lub ominięcia zabezpieczenia. W przypadku kont w serwisach społecznościowych należy zatem ustalić, czy konto było chronione samym hasłem, czy również dodatkowym składnikiem uwierzytelnienia oraz wskazać, jakie dokładnie było to zabezpieczenie, czy było aktywne w chwili zdarzenia oraz w jaki sposób sprawca je pokonał albo obszedł. W opisie czynu należy wskazać jakie zabezpieczenie chroniło konto oraz w jaki sposób sprawca uzyskał dostęp mimo jego istnienia, ale bez jego przełamania lub w jaki sposób je przełamał.

[29] Facebook, Wykorzystywanie aplikacji do uwierzytelniania dwuskładnikowego, Centrum pomocy Facebooka, https://pl-pl.facebook.com/help/fblite/358336074294704 (22.06.2026).
[30] F. Radoniewicz, *Cyberprzestępstwa...*
[31] P. Opitek, tamże, s. 55.
[32] M. Mozgawa, *Kodeks karny. Komentarz aktualizowany do art. 267 k.k.*, Lex (20.06.2026).

1.7. Działanie bez uprawnienia

Zwrot „bez uprawnienia" oznacza, że sprawca nie ma prawa dostępu do danej informacji, konta, systemu informatycznego albo jego części. Chodzi więc o dostęp nielegalny, naruszający prawo innego podmiotu do dysponowania informacją lub decydowania o tym, kto może ją uzyskać[33]. W odniesieniu do art. 267 § 1 k.k. wskazuje się, że sprawca „w ogóle nie ma prawa do zapoznania się z informacją", co odróżnia to znamię od sytuacji, w której dana osoba ma legalny dostęp, lecz wykorzystuje go niezgodnie z celem albo zakresem upoważnienia[34].

[33] Tamże.
[34] P. Opitek, tamże, s. 193.

Rozdział 2.
Prawnokarna ocena nieuprawnionego dostępu do konta w serwisie społecznościowym

Przejęcie konta w serwisach społecznościowych, takich jak Facebook, Instagram czy YouTube nie powinno być traktowane jako jeden prosty i zawsze tak samo kwalifikowany czyn. W praktyce może ono obejmować kilka etapów: uzyskanie danych logowania, wejście na konto, zapoznanie się z wiadomościami albo innymi treściami, zmianę hasła, zmianę danych przypisanych do konta, usunięcie treści lub jej dodanie, ograniczenie właścicielowi dostępu albo całkowite zablokowanie możliwości korzystania z konta. Każdy z tych elementów może mieć znaczenie dla kwalifikacji prawnej, ponieważ inny przedmiot ochrony występuje przy dostępie do informacji, a inny przy dostępie do systemu informatycznego.

2.1. Uzyskanie dostępu do informacji

Dla oceny nieuprawnionego przejęcia konta w serwisie społecznościowym podstawowe znaczenie mają przepisy chroniące dostęp do informacji, dostęp do systemu informatycznego oraz dostępność i integralność danych informatycznych. Z tego względu w pierwszej kolejności należy przywołać treść art. 267, art. 268 i art. 268a k.k., ponieważ to między tymi przepisami najczęściej będzie rozstrzygany problem kwalifikacji prawnej takiego zachowania.

Art. 267 k.k.

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego[35].

Art. 268 k.k.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego[36].

Art. 268a k.k.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego[37].

Zestawienie tych przepisów pokazuje, że w sprawach dotyczących kont w serwisach społecznościowych nie wystarczy ogólne określenie, że doszło do „włamania na konto". Należy ustalić, czy sprawca uzyskał dostęp do informacji dla niego nieprzeznaczonych, czy do systemu informatycznego lub jego części, czy też później ingerował w dane informatyczne albo utrudnił osobie uprawnionej dostęp do informacji lub danych.

Przypomnieć w tym miejscu należy rozróżnienie pomiędzy pojęciami „informacja" i „dane informatyczne". W ocenie P. Opitka w praktyce organów ścigania i sądów

[35] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 267.
[36] Tamże, art. 268.
[37] Tamże, art. 268a.

występują nieścisłości w rozumieniu tych pojęć, co przekłada się na nieprawidłowy opis czynu oraz błędną kwalifikację prawną[38].

W realiach przejęcia konta w serwisie społecznościowym istotne znaczenie mają przede wszystkim przełamanie albo ominięcie zabezpieczenia. Jeżeli sprawca uzyskuje w ten sposób dostęp do treści przeznaczonych wyłącznie dla właściciela konta, np. prywatnych wiadomości, niewidocznych publicznie zdjęć, ustawień prywatności, historii aktywności lub danych kontaktowych, zasadniczo należy rozważyć art. 267 § 1 k.k. Przedmiotem czynności wykonawczej jest wtedy informacja dla sprawcy nieprzeznaczona. Opitek wskazuje, że o zakwalifikowaniu określonego zapisu jako informacji powinno decydować to, czy w konkretnym stanie faktycznym sprawca potrafił sam lub przy użyciu zwykłych środków odczytać z niego sens[39]. Istotne jest to, że informacja nie była przeznaczona dla sprawcy i była chroniona przed nieuprawnionym dostępem. Nie każda sytuacja będzie jednak objęta art. 267 § 1 k.k. Według P. Opitka karanie sprawcy za uzyskanie dostępu do pustej skrzynki poczty elektronicznej albo do informacji powszechnie dostępnych w otwartym Internecie byłoby nieuzasadnione. W takim przypadku można rozważać ewentualnie usiłowanie nieudolne, jeżeli sprawca działał w przekonaniu, że uzyska dostęp do informacji chronionych[40]. Ta uwaga ma znaczenie również przy kontach w serwisach społecznościowych. Jeżeli sprawca uzyskał dostęp wyłącznie do publicznej warstwy profilu, którą każdy użytkownik mógł zobaczyć bez logowania, trudno mówić o uzyskaniu informacji dla niego nieprzeznaczonej. Inaczej będzie wtedy, gdy po zalogowaniu otworzył wiadomości prywatne, archiwum rozmów, niepubliczne zdjęcia albo dane dostępne wyłącznie z poziomu właściciela konta. Wydaje się, że ten pierwszy przypadek będzie miał jednak miejsce niezmiernie rzadko. Należy jeszcze dodać, że jeśli sprawca poznaje treść informacji dla niego nieprzeznaczonej i dochodzi do kwalifikacji z art. 267 § 1 k.k., to razie ujawnienia tej informacji w kwalifikacji należy także zastosować art. 267 § 4 k.k.

2.2. Uzyskanie dostępu do systemu informatycznego

Konto serwisu społecznościowego nie jest samo w sobie systemem informatycznym, ale dostęp do niego może oznaczać dostęp do części systemu informatycznego obsługującego serwis. Art. 267 § 2 k.k. znajduje więc zastosowanie przede wszystkim wtedy, gdy sprawca bez uprawnienia uzyskuje dostęp do całości albo części systemu informatycznego, nawet jeżeli nie przełamuje ani nie omija zabezpieczenia. W odróżnieniu

[38] P. Opitek, tamże, s. 32-33.
[39] Tamże.
[40] Tamże.

od art. 267 § 1 k.k. nie jest tu konieczne wykazanie dostępu do informacji dla sprawcy nieprzeznaczonej. Dlatego przy koncie w serwisie społecznościowym art. 267 § 2 k.k. może mieć znaczenie zwłaszcza wtedy, gdy ustalono samo nieuprawnione zalogowanie się do konta lub panelu użytkownika, ale nie wykazano jeszcze, że sprawca zapoznał się z prywatnymi wiadomościami albo inną konkretną informacją lub nie przełamał ani nie ominął żadnych zabezpieczeń[41,42].

W komentarzach do art. 267 k.k. wskazano, że systemem informatycznym nie jest program komputerowy ani skrzynka e-mail. Z tego wynika, że poprawnie skonstruowany opis kwalifikacji prawnej powinien więc wskazywać, że sprawca uzyskał dostęp do systemu informatycznego, np. serwera, na którym działa oprogramowanie obsługujące daną usługę, czyli zakwalifikować czyn z art. 267 § 2 k.k.[43] Przez analogię przy koncie społecznościowym należy rozważyć czy bardziej właściwe nie będzie wskazanie, że sprawca uzyskał dostęp do części systemu informatycznego usługodawcy umożliwiającej korzystanie z konta, przetwarzanie danych, wysyłanie wiadomości, zmianę ustawień lub zarządzanie profilem.

2.3. Wykorzystanie prawidłowych danych logowania i phishing

Problem kwalifikacyjny powstaje zwłaszcza wtedy, gdy sprawca posługuje się poprawnym loginem i hasłem. Samo posłużenie się prawidłowym loginem lub nawet uzyskanym bez zgody osoby uprawnionej, nie musi oznaczać przełamania albo ominięcia zabezpieczenia w rozumieniu art. 267 § 1 k.k. Dla tego przepisu konieczne jest bowiem uzyskanie dostępu do informacji w jeden ze sposobów wskazanych w jego treści. Jeżeli sprawca loguje się do serwisu przy użyciu poprawnych danych, właściwsze może być rozważenie kwalifikacji z art. 267 § 2 k.k., czyli nieuprawnionego dostępu do całości albo części systemu informatycznego, ponieważ nie sposób wykazać, że wejście w posiadanie prawidłowych danych logowania, nawet przy użyciu podstępu, będzie jakimkolwiek przełamaniem zabezpieczenia[44,45,46]. W tym miejscu należy wskazać, że z poglądem tym nie zgadza się jednak P. Opitek, który porównuje tę sytuację do kradzieży z włamaniem przy użyciu skradzionego klucza

[41] Wyrok Sądu Okręgowego w Elblągu VI Wydział Karny Odwoławczy z dnia 1 sierpnia 2024 r., VI Ka 258/24.
[42] P. Opitek, tamże, s. 73-75.
[43] M. Mozgawa, *Kodeks karny. Komentarz aktualizowany do art. 267 k.k.*, Lex (20.06.2026).
[44] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14.10.2008 r., II AKa 120/08.
[45] Wyrok Sądu Okręgowego w Piotrkowie Trybunalskim z dnia 03.11.2020 r., IV Ka 578/20.
[46] M. Mozgawa, *Kodeks karny. Komentarz aktualizowany do art. 267 k.k.*, Lex (20.06.2026).

i opowiada się za uznaniem takiego zachowania, jako wyczerpującego znamiona przestępstwa z art. 267 § 1 k.k.[47]

Osobno należy omówić tzw. „phishing" jako metoda socjotechniczna polega najczęściej na wyłudzeniu prawidłowych danych logowania między innymi do serwisów społecznościowych, w celu ich późniejszego wykorzystania, jednak to wyłudzenie może przybrać różną formę techniczną. Jeżeli fałszywa strona logowania służy jedynie pozyskaniu loginu i hasła, a następnie sprawca loguje się do serwisu poprawnymi danymi, co do zasady, w ujęciu prezentowanym w części komentarzy, nie dochodzi do przełamania ani ominięcia zabezpieczenia, lecz do nieuprawnionego dostępu z art. 267 § 2 k.k., o czym była mowa w poprzednim akapicie. Jeżeli jednak skutkiem phishingu jest zainstalowanie na urządzeniu pokrzywdzonego programu lub skryptu pozwalającego później przełamać albo ominąć zabezpieczenia, możliwe będzie rozważenie art. 267 § 1 k.k. Natomiast gdy zainstalowany zostaje stealer albo keylogger służący do wykradania loginów, haseł lub innych danych uwierzytelniających, właściwym kierunkiem może być art. 267 § 3 k.k.[48] W praktyce należy zatem precyzyjnie ustalić, chociaż bardzo często jest to mocno utrudnione lub nawet niemożliwe, czy sprawca tylko zalogował się przy użyciu poprawnych danych, czy też wcześniej posłużył się narzędziem przechwytującym dane, programem omijającym zabezpieczenie albo inną metodą pozwalającą dostać się do informacji dla niego nieprzeznaczonej.

2.4. Zmiana hasła, zablokowanie konta i ingerencja w dane

Po uzyskaniu dostępu do konta sprawca często zmienia hasło, adres e-mail, numer telefonu, metodę uwierzytelniania dwuskładnikowego albo inne dane służące odzyskaniu dostępu. Może też usunąć treści, zmienić ustawienia profilu, usunąć konto, zablokować właścicielowi możliwość logowania albo utrudnić mu odzyskanie kontroli. Te zachowania wymagają osobnej oceny, ponieważ mogą wykraczać poza samo uzyskanie dostępu do konta.

Najczęściej w praktyce rozważa się wówczas art. 268a § 1 k.k. Przepis ten obejmuje m.in. zmianę lub utrudnianie dostępu do danych informatycznych. Oznacza to, że np. przy zmianie hasła należy ustalić, czy sprawca zmienił dane informatyczne służące uwierzytelnieniu albo utrudnił osobie uprawnionej dostęp do danych powiązanych z kontem. F. Radoniewicz wskazuje, że przedmiotem ochrony art. 268a k.k. są dane informatyczne, a dokładniej ich integralność i dostępność. Autor podkreśla też, że art. 268a § 1 k.k. jest sformułowany nieprecyzyjnie, ale właściwsza jest interpretacja,

[47] P. Opitek, tamże, s. 36-37.
[48] M. Mozgawa, *Kodeks karny. Komentarz aktualizowany do art. 267 k.k.*, Lex (20.06.2026).

zgodnie z którą niszczeniu, uszkadzaniu, usuwaniu i zmienianiu podlegają dane informatyczne, a nie sam dostęp do danych[49].

Kwalifikację z art. 268a § 1 k.k. przyjęto w wyroku Sądu Rejonowego Poznań-Nowe Miasto i Wilda w Poznaniu z 8 grudnia 2017 r., VI K 358/17. Sąd uznał, że poprzez zmianę haseł do konta oskarżony utrudnił pokrzywdzonej dostęp do danych informatycznych powiązanych z tym kontem. W uzasadnieniu wskazano także, że oskarżony nie był osobą uprawnioną do logowania się do poczty pokrzywdzonej, a zmiana hasła spowodowała konieczność przeprowadzenia procedury odzyskiwania dostępu[50]. Podkreślenia wymaga przy tym, że fakt możliwości późniejszego odzyskania dostępu nie eliminuje karalności takiego zachowania, ponieważ już sama konieczność przeprowadzenia procedury odzyskiwania hasła może stanowić utrudnienie dostępu do danych[51].

Podobnie w wyroku Sądu Rejonowego w Legionowie z 6 października 2020 r., II K 1222/19, usunięcie internetowego profilu (w tym przypadku sąd użył właśnie sformułowania profil) wraz ze znajdującymi się tam danymi informatycznymi zakwalifikowano z art. 268a § 1 k.k.[52] Ten wyrok pokazuje, że usunięcie konta albo danych powiązanych z kontem może być oceniane jako ingerencja w dane informatyczne.

Zakres art. 268a k.k. został ogólnie wyjaśniony także w wyroku Sądu Najwyższego z 30 września 2015 r., II KK 115/15: Przepis art. 268a Kodeksu karnego penalizuje dwa rodzaje zakazanego zachowania sprawcy. Pierwszym z nich jest niszczenie, uszkadzanie, usuwanie, zmiana oraz utrudnianie dostępu do danych informatycznych. Drugi rodzaj zachowania godzi w proces prawidłowego automatycznego przetwarzania, gromadzenia i przekazywania danych informatycznych w stopniu istotnym. Zachowanie to może polegać na zakłócaniu lub uniemożliwianiu działania procesu. Pojęcie zakłócenia automatycznego przetwarzania, przekazywania lub gromadzenia danych informatycznych obejmuje wszelkie czynności oddziałujące na te procesy, których skutkiem jest ich nieprawidłowy przebieg, spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych danych. Uniemożliwienie natomiast oznacza zatrzymanie tych procesów lub niemożność ich podjęcia. Dane informatyczne, o których mowa w przepisie art. 268a Kodeksu karnego, to zapis określonej informacji przechowywanej na dysku komputera lub na innym komputerowym nośniku informacji[53].

[49] F. Radoniewicz, *Odpowiedzialność...*, s. 158.
[50] Wyrok Sądu Rejonowego Poznań-Nowe Miasto i Wilda w Poznaniu z dnia 08.12.2017, VI K 358/17.
[51] A. Sakowicz, S. Zieliński, M. Królikowski, R. Zawłocki (red.), *Kodeks karny. Część szczególna. Tom III. Komentarz do art. 222-316*, 2024.
[52] Wyrok Sądu Rejonowego w Legionowie z dnia 6.10.2020 r., sygn. akt II K 1222/19.
[53] Wyrok Sądu Najwyższego z dnia 30 września 2015 r., II KK 115/15.

Przedstawiony powyżej pogląd, że zmiana hasła lub ingerencja w inne dane, do których sprawca ma dostęp po przejęciu konta zawsze powinny być kwalifikowane z art. 268a k.k. nie znajduje jednak uznania u wszystkich autorów. Według P. Opitka uniemożliwienie zalogowania się do konta oznacza przede wszystkim brak możliwości zapoznania się z informacjami, a nie tylko z danymi informatycznymi. W sprawie, w której sprawca uzyskuje dostęp do konta poprzez wykorzystanie znanego mu hasła, a następnie zmienia to hasło, za prawidłową P. Opitek uznał kwalifikację z art. 267 § 1 k.k. i art. 268 § 2 k.k. w zw. z art. 11 § 2 k.k.[54] W podobnej sprawie Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie, w której sprawca przełamał hasło zabezpieczające skrzynkę pocztową, uzyskał dostęp do informacji dla siebie nieprzeznaczonej, a następnie zmienił hasło dostępu, przyjęto kwalifikację z art. 267 § 1 k.k. P. Opitek wskazuje jednak, że w opisie i kwalifikacji należało uwzględnić również art. 268 § 2 k.k., jeżeli skutkiem było uniemożliwienie osobie uprawnionej zapoznania się z informacjami zapisanymi na informatycznym nośniku danych[55].

Można zauważyć więc dwa odmienne podejścia do problemu kwalifikacji zmiany hasła lub innych danych na koncie serwisu społecznościowego. Z praktycznego punktu widzenia wynika więc, że przy zmianie hasła do konta społecznościowego nie należy automatycznie wybierać jednego przepisu. Jeżeli sprawca zmienia hasło, adres e-mail albo ustawienia uwierzytelniania i w ten sposób utrudnia dostęp do danych konta jako danych informatycznych, uzasadnione może być rozważenie art. 268a § 1 k.k. Jeżeli natomiast ustalono, że działanie sprawcy udaremniło lub znacznie utrudniło właścicielowi zapoznanie się z istotnymi informacjami, np. prywatną korespondencją, dokumentami, zdjęciami albo innymi ważnymi treściami zapisanymi w usłudze, należy rozważyć art. 268 § 2 k.k.

Wydaje się, że możliwy jest zbieg art. 268 § 2 k.k. i art. 268a § 1 k.k., jednak jego charakter jest sporny. P. Opitek opowiada się za kwalifikacją kumulatywną, wskazując na odmienny przedmiot czynności wykonawczej obu przepisów: informację oraz dane informatyczne[56]. Inaczej ujmowane jest stanowisko, zgodnie z którym zachodzi jedynie zbieg niewłaściwy, a art. 268 § 2 k.k. zostaje pochłonięty przez art. 268a § 1 k.k.[57] Dopełniając obraz kwestii zbiegu art. 268 k.k. i 268a k.k. warto przytoczyć w całości komentarz do tego ostatniego: „Jeśli sprawca spełnił znamiona czynu zabronionego określonego w art. 268a k.k. i zarazem art. 268 k.k. wtedy art. 268a k.k. na zasadzie lex consumens wyłączy stosowanie art. 268 k.k., nie będzie więc

[54] P. Opitek, tamże, s. 92-94.
[55] Tamże. s. 100-101.
[56] Tamże, s. 93.
[57] F. Radoniewicz, *Odpowiedzialność...*, s. 148.

kumulatywnego zbiegu przepisów (B. Kunicka-Michalska, Przestępstwa przeciwko ochronie informacji, s. 725). Uważa się również, że w większości przypadków spełnienia znamion przestępstwa z art. 268a § 1 k.k. in principio dojdzie do koniecznego zbiegu art. 268 k.k. W przypadku gdy zachowania sprawcy odnosić się będą do danych informatycznych będących nośnikiem określonych informacji w rozumieniu art. 268 k.k., przepis ten stanowić będzie lex specialis w stosunku do art. 268a k.k. Natomiast w przypadku zbiegu art. 268a § 1 k.k. oraz art. 269 k.k. – ten ostatni będzie miał charakter lex consumens”[58].

[58] *S. Hoc* [w:] *R. A. Stefański* (red.), *Kodeks karny. Komentarz*, wyd. 29, 2026, art. 268a (10.06.2026).

Rozdział 3.
Prawnokarna ocena zachowań następczych po nieuprawnionym przejęciu konta w serwisie społecznościowym

Przejęcie konta w serwisie społecznościowym nie zawsze kończy się na samym uzyskaniu dostępu, zmianie hasła albo zablokowaniu możliwości korzystania osobie uprawnionej. W praktyce sprawca może następnie używać konta tak, jakby był jego właścicielem: publikować wpisy, wysyłać wiadomości, prosić inne osoby o pieniądze, usuwać albo dodawać treści, grozić pokrzywdzonemu czy ujawniać prywatne informacje. Takie zachowania należy oceniać odrębnie. Przejęcie konta może więc realizować znamiona art. 267 k.k., art. 268 k.k. albo art. 268a k.k., ale dalsze wykorzystanie konta może dodatkowo prowadzić do odpowiedzialności za inne przestępstwa, w szczególności podszywanie się, oszustwo, groźby, zniesławienie czy zniewagę[59]. Ze względu na ograniczenia objętościowe opracowania dalsza część pracy nie obejmuje wszystkich możliwych przestępstw, które mogą zostać popełnione po przejęciu konta w serwisie społecznościowym, natomiast wybrano te, które zdaniem autora występują najczęściej w praktyce policyjnej.

3.1. Podszywanie się pod właściciela konta

Pierwszym typowym zachowaniem po przejęciu konta jest podszywanie się pod jego właściciela. Może ono polegać na publikowaniu wpisów w jego imieniu, wysyłaniu wiadomości do jego znajomych, odpowiadaniu na wiadomości, zmianie zdjęcia profilowego lub nazwy profilu czy zamieszczaniu komentarzy. W takim przypadku należy rozważyć kwalifikację dodatkową z art. 190a § 2 k.k.

Art. 190a k.k.
§ 1. Kto przez uporczywe nękanie innej osoby lub osoby dla niej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność,
podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

[59] F. Radoniewicz, *Odpowiedzialność...*, s. 149.

§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, przez co wyrządza jej szkodę majątkową lub osobistą.

§ 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 15.

§ 4. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Po zmianie art. 190a § 2 k.k. obowiązującej od 1 października 2023 r. nieaktualne jest stanowisko, zgodnie z którym przepis ten wymaga zawsze zamiaru bezpośredniego kierunkowego wyrządzenia szkody osobie, pod którą sprawca się podszywa. Obecnie ustawodawca usunął zwrot „w celu wyrządzenia szkody" i zastąpił go znamieniem skutkowym: „przez co wyrządza jej szkodę majątkową lub osobistą". Oznacza to, że przy przejęciu konta w serwisie społecznościowym i wykorzystaniu go do oszustwa należy rozważyć art. 190a § 2 k.k., także wtedy, gdy podszycie się pod właściciela konta było środkiem do wyłudzenia pieniędzy, o ile sprawca co najmniej przewidywał i godził się na wyrządzenie właścicielowi konta szkody majątkowej albo osobistej[60,61].

3.2. Wykorzystanie przejętego konta do oszustwa „na Blika"

Drugim częstym zachowaniem następującym po przejęciu konta jest wykorzystanie go do oszustwa. Sprawca może wysyłać wiadomości do znajomych lub rodziny właściciela konta, prosząc np. o opłacenie rzekomej przesyłki przez podanie kodu Blik i autoryzację transakcji. W takim przypadku samo przejęcie konta jest etapem przygotowującym dalsze przestępstwo przeciwko mieniu. Jeżeli sprawca działa w celu osiągnięcia korzyści majątkowej, wprowadza inną osobę w błąd i doprowadza ją do niekorzystnego rozporządzenia mieniem, a tak dzieje się w podanym przykładzie, należy rozważyć w kwalifikacji art. 286 § 1 k.k.[62]

Art. 286 k.k.

§ 1. Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą

[60] https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s/212272%2CSkutecznosc-karnoprawnej-regulacji-kradziezy-tozsamosci-w-sprawach-z-zakresu-cyb.html

[61] M. Królikowski, A. Sakowicz [w:] M. Królikowski, R. Zawłocki (red.), *Kodeks Karny. Część szczególna. Tom II. Komentarz do art. 190a k.k.*

[62] F. Radoniewicz, *Odpowiedzialność...*, s. 147 i 159.

wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania,
podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
§ 2. Tej samej karze podlega, kto żąda korzyści majątkowej w zamian za zwrot bezprawnie zabranej rzeczy.
§ 3. W wypadku mniejszej wagi, sprawca
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 4. Jeżeli czyn określony w § 1-3 popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

F. Radoniewicz wskazuje jako przykład sytuację, w której sprawca uzyskuje nieuprawniony dostęp do konta innego użytkownika w serwisie aukcyjnym, a następnie za jego pomocą dokonuje oszustw. Ten sam mechanizm może wystąpić przy koncie w serwisie społecznościowym. Nie należy również zapominać o rozważeniu w tym przypadku dodatkowej kwalifikacji z art. 268a § 1 k.k., jeżeli doszło do zablokowania korzystania z konta i zmiany danych[63].

Mając na uwadze rozważania dwóch poprzednich podrozdziałów, warto przytoczyć komunikat Prokuratury Okręgowej w Krakowie dotyczący sprawy wyłudzania środków pieniężnych przy wykorzystaniu kodów Blik. Wynika z niego, że sprawcy przejmowali konta użytkowników Facebooka, a następnie podszywali się pod właścicieli przejętych profili i prosili ich znajomych o pomoc finansową. Pokrzywdzeni realizowali płatności, generując i zatwierdzając kody Blik. Mechanizm ten potwierdza, że takie zachowanie nie powinno być oceniane wyłącznie przez pryzmat oszustwa, ponieważ obejmuje ono także wcześniejsze bezprawne uzyskanie dostępu do konta oraz podszywanie się pod jego właściciela. W opisanej sprawie prokurator przedstawił podejrzanym zarzuty obejmujące m.in. art. 286 § 1 k.k., art. 190a § 2 k.k. oraz art. 267 § 1 k.k. w zw. z art. 11 § 2 k.k.[64]

3.3. Groźby, zniewagi i zniesławienie z wykorzystaniem przejętego konta

Krótko należy również wspomnieć, że przejęcie konta w serwisie społecznościowym może być wykorzystane nie tylko do oszustwa albo podszywania się pod właściciela profilu, lecz także do zachowań wymierzonych bezpośrednio w jego wolność, cześć

[63] Tamże.

[64] Rozbicie grupy przestępczej, zajmującej się wyłudzaniem środków pieniężnych od użytkowników portalu społecznościowego przy wykorzystaniu kodów płatności, Komunikat rzecznika z dnia 04.02.2026 https://www.gov.pl/web/po-krakow/funkcjonariusze-centralnego-biura-zwalczania-cyberprzestepczosci-rozbili-zorganizowana-grupe-przestepcza (23.06.2026).

lub dobre imię. Sprawca, mając dostęp do konta, może wysyłać wiadomości zawierające groźby albo rozpowszechniać treści godzące w reputację właściciela konta.

Jeżeli sprawca kieruje do pokrzywdzonego albo osoby mu najbliższej zapowiedź popełnienia przestępstwa i groźba ta wzbudza uzasadnioną obawę spełnienia, należy rozważyć art. 190 § 1 k.k.

Art. 190 k.k.

§ 1. Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub na szkodę osoby dla niej najbliższej, jeżeli groźba wzbudza w osobie, do której została skierowana lub której dotyczy, uzasadnioną obawę, że będzie spełniona, podlega karze pozbawienia wolności do lat 3.

§ 2. Ściganie następuje na wniosek pokrzywdzonego.

Dla kwalifikacji nie wystarczy jednak samo użycie agresywnego i wulgarnego języka. Trzeba oczywiście pamiętać, że należy ustalić, czy wypowiedź rzeczywiście zawierała groźbę popełnienia przestępstwa oraz czy po stronie adresata powstała uzasadniona obawa jej spełnienia[65].

W przypadku gdy sprawca wykorzystuje przejęte konto do publikowania albo wysyłania treści naruszających cześć pokrzywdzonego, należy w pierwszej kolejności ustalić, czy chodzi o zniewagę czy o zniesławienie.

Art. 212 k.k.

§ 1. Kto pomawia inną osobę, grupę osób, instytucję, osobę prawną lub jednostkę organizacyjną niemającą osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności, podlega grzywnie albo karze ograniczenia wolności.

§ 2. Jeżeli sprawca dopuszcza się czynu określonego w § 1 za pomocą środków masowego komunikowania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. W razie skazania za przestępstwo określone w § 1 lub 2 sąd może orzec nawiązkę na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.

§ 4. Ściganie przestępstwa określonego w § 1 lub 2 odbywa się z oskarżenia prywatnego.

[65] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 190 § 1.

Art. 216 k.k.

§ 1. Kto znieważa inną osobę w jej obecności albo choćby pod jej nieobecność, lecz publicznie lub w zamiarze, aby zniewaga do osoby tej dotarła, podlega grzywnie albo karze ograniczenia wolności.

§ 2. Kto znieważa inną osobę za pomocą środków masowego komunikowania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. Jeżeli zniewagę wywołało wyzywające zachowanie się pokrzywdzonego albo jeżeli pokrzywdzony odpowiedział naruszeniem nietykalności cielesnej lub zniewagą wzajemną, sąd może odstąpić od wymierzenia kary.

§ 4. W razie skazania za przestępstwo określone w § 2 sąd może orzec nawiązkę na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.

§ 5. Ściganie odbywa się z oskarżenia prywatnego.

Zniewaga z art. 216 k.k. będzie dotyczyć przede wszystkim wyzwisk, obelg i innych wypowiedzi uwłaczających godności osobistej[66], natomiast zniesławienie z art. 212 k.k. polega na przypisaniu pokrzywdzonemu określonych zachowań lub właściwości mogących poniżyć go w opinii publicznej albo narazić na utratę zaufania[67]. W realiach serwisu społecznościowego znaczenie ma także sposób udostępnienia treści: wpisy, komentarze albo publikacje dostępne dla szerszego kręgu odbiorców mogą uzasadniać rozważenie art. 212 § 2 k.k. albo art. 216 § 2 k.k., natomiast wiadomości prywatne wymagają ostrożniejszej oceny, ze względu na znamię środków masowego komunikowania[68]. Dlatego w opisie czynu należy wskazać nie tylko fakt przejęcia konta, lecz także konkretną treść wpisu lub wiadomości, jej adresatów oraz zakres dostępności dla innych użytkowników[69].

[66] M. Mozgawa [w:] M. Budyn-Kulik, P. Kozłowska-Kalisz, M. Kulik, M. Mozgawa, *Kodeks karny. Komentarz aktualizowany*, art. 216.
[67] J. Kulesza [w:] A. Behan i in., *Kodeks karny. Komentarz*, art. 212.
[68] Wyrok SN z 7.11.2014 r., V KK 231/14, LEX nr 1583243.
[69] F. Radoniewicz, *Odpowiedzialność...,* s. 147.

Rozdział 4.
Zestawienie modelowych wariantów kwalifikacji

Wariant zachowania	Modelowa kwalifikacja	Warunki zastosowania / uwagi
Dostęp do prywatnych treści konta	art. 267 § 1 k.k.; przy ujawnieniu także art. 267 § 4 k.k.	Informacje dla sprawcy nieprzeznaczone: wiadomości prywatne, niepubliczne zdjęcia, historia rozmów, dane kontaktowe.
Nieuprawnione zalogowanie do konta	art. 267 § 2 k.k.	Dostęp do całości albo części systemu informatycznego, bez konieczności wykazywania uzyskania konkretnej informacji.
Phishing i użycie poprawnych danych logowania	sporne: art. 267 § 2 k.k. albo art. 267 § 1 k.k.; przy keyloggerze art. 267 § 3 k.k.	Część komentarzy wyklucza przełamanie przy samym użyciu poprawnego hasła, a część dopuszcza art. 267 § 1 k.k. przy podstępnym pozyskaniu hasła.
Zmiana hasła, e-maila, telefonu lub 2FA	najczęściej art. 268a § 1 k.k.; możliwy art. 268 § 2 k.k.; spór co do zbiegu	Art. 268a przy utrudnieniu dostępu do danych; art. 268 § 2 przy udaremnieniu lub znacznym utrudnieniu zapoznania się z istotną informacją.
Usunięcie profilu, konta lub danych	art. 268a § 1 k.k.	Usunięcie danych informatycznych albo utrudnienie dostępu do danych powiązanych z kontem.
Podszywanie się pod właściciela konta	art. 190a § 2 k.k.; zwykle w zbiegu z art. 267 k.k.	Wykorzystanie wizerunku, danych osobowych lub innych danych identyfikujących oraz wyrządzenie szkody majątkowej albo osobistej.
Oszustwo „na Blika" z przejętego konta	art. 286 § 1 k.k.; często art. 190a § 2 k.k. i art. 267 § 1 albo § 2 k.k.	Podszycie się pod właściciela konta i doprowadzenie pokrzywdzonego do przekazania kodu Blik i zatwierdzenia transakcji.
Groźby, zniewagi lub zniesławienie z konta	art. 190 § 1 k.k., art. 216 § 2 k.k. albo art. 212 § 2 k.k.; możliwy zbieg z art. 267 k.k.	Wymaga oceny treści wiadomości lub wpisu. Przy § 2 art. 212 i 216 istotny jest publiczny charakter publikacji lub użycie środka masowego komunikowania.

Bibliografia

Akty prawne:

- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 2025 poz. 383).
- Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2014 r. poz. 1514).
- Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728).
- Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218 z 14.08.2013 r.).

Literatura i komentarze:

- Hoc S. [w:] Stefański R.A. (red.), *Kodeks karny. Komentarz*, wyd. 29, 2026, art. 268a, Legalis, dostęp: 10.06.2026.
- Królikowski M., Sakowicz A. [w:] M. Królikowski, R. Zawłocki (red.), *Kodeks Karny. Część szczególna. Tom II. Komentarz do art. 190a k.k.*, 2023.
- Kulesza J. [w:] Behan A. i in., *Kodeks karny. Komentarz*, Warszawa 2025, art. 212.
- Mozgawa M., *Kodeks karny. Komentarz aktualizowany do art. 267 k.k.*, LEX, dostęp: 20.06.2026.
- Mozgawa M. [w:] Budyn-Kulik M., Kozłowska-Kalisz P., Kulik M., Mozgawa M., *Kodeks karny. Komentarz aktualizowany*, Gdańsk 2026, art. 216.
- Opitek P., *Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych*, Wydawnictwo Krajowej Szkoły Sądownictwa i Prokuratury, Kraków 2023.
- Radoniewicz F., *Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym – propozycje zmian*, 2024, Legalis, dostęp: 10.06.2026.
- Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wolters Kluwer, Warszawa 2016.
- Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, Prawo w Działaniu. Sprawy karne 2013, nr 13.
- Sakowicz A., Zieliński S. [w:] Królikowski M., Zawłocki R. (red.), *Kodeks karny. Część szczególna. Tom III. Komentarz do art. 222-316*, 2024.
- Stefański R.A., *Kodeks karny. Komentarz do art. 267 k.k.*, 2025, Legalis, dostęp: 10.06.2026.

- Stefański R.A., *Kodeks karny. Komentarz do art. 269b k.k.*, 2025, Legalis, dostęp: 10.06.2026.

Orzecznictwo:

- Postanowienie Sądu Najwyższego z dnia 5 marca 2019 r., II KK 208/18.
- Wyrok Sądu Najwyższego z dnia 7 listopada 2014 r., V KK 231/14, LEX nr 1583243.
- Wyrok Sądu Najwyższego – Izba Karna z dnia 30 września 2015 r., II KK 115/15.
- Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r., II AKa 120/08.
- Wyrok Sądu Okręgowego w Elblągu VI Wydział Karny Odwoławczy z dnia 1 sierpnia 2024 r., VI Ka 258/24.
- Wyrok Sądu Okręgowego w Piotrkowie Trybunalskim z dnia 3 listopada 2020 r., IV Ka 578/20.
- Wyrok Sądu Rejonowego Poznań-Nowe Miasto i Wilda w Poznaniu z dnia 8 grudnia 2017 r., VI K 358/17.
- Wyrok Sądu Rejonowego w Legionowie z dnia 6 października 2020 r., II K 1222/19.

Źródła internetowe i dokumenty elektroniczne:

- Budowa karty płatniczej: numer karty, awers, rewers, CVC, Moneteo, https://moneteo.com/artykuly/budowa-karty-platniczej, dostęp: 22.06.2026.
- Facebook, Różnica pomiędzy kontem na Facebooku a profilem na Facebooku, Centrum pomocy Facebooka, https://www.facebook.com/help/327202558928776?locale=pl_PL, dostęp: 21.06.2026.
- Facebook, Wykorzystywanie aplikacji do uwierzytelniania dwuskładnikowego, Centrum pomocy Facebooka, https://pl-pl.facebook.com/help/fblite/358336074294704, dostęp: 22.06.2026.
- Google, Usuwanie, przełączanie i dodawanie użytkowników, Android – Pomoc, https://support.google.com/android/answer/2865483?hl=pl, dostęp: 21.06.2026.
- Instrukcja Użytkownika systemu Profil Zaufany, wersja 1.1, 2021.
- Netflix, How to see viewing history and device activity, Netflix Help Center, https://help.netflix.com/en/node/101917, dostęp: 21.06.2026.
- Prokuratura Okręgowa w Krakowie, Rozbicie grupy przestępczej zajmującej się wyłudzaniem środków pieniężnych od użytkowników portalu społecznościowego przy wykorzystaniu kodów płatności, komunikat rzecznika z dnia 04.02.2026, https://www.gov.pl/web/po-krakow/funkcjonariusze-centralnego-biura-zwalczania-cyberprzestepczosci-rozbili-zorganizowana-grupe-przestepcza, dostęp: 23.06.2026.

- Skuteczność karnoprawnej regulacji kradzieży tożsamości w sprawach z zakresu cyberprzestępczości, Gazeta Policyjna, https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s/212272%2CSkutecznosc--karnoprawnej-regulacji-kradziezy-tozsamosci-w-sprawach-z-zakresu-cyb.html.

Zakład Służby Kryminalnej

st. asp. Konrad Kędzierski

Szkoła Policji w Katowicach
ul. gen. Jankego 276
40-684 Katowice-Piotrowice
www.katowice.szkolapolicji.gov.pl