„Krytyka Prawa", tom 16, nr 4/2024, s. 298–313, ISSN 2080-1084, e-ISSN 2450-7938, © 2024 Author.

ZUZANNA GĄDZIK[1]

Catfishing – jako przejaw przestępstwa kradzieży tożsamości[2]

Wpłynął: 6.01.2024. Akceptacja: 13.07.2024

Streszczenie

Przedmiotem artykułu jest prawnokarna ocena *catfishingu* – zachowania polegającego na kradzieży istniejącej tożsamości innej osoby lub stworzenia fałszywej tożsamości dla wykorzystania jej jako własnej – w celu finansowych lub osobistych nadużyć. Zjawisko to należy interpretować dwutorowo – pokrzywdzonym może być zarówno osoba, pod którą sprawca się podszywa, jak i osoby, z którymi ma on kontakt i które wprowadza w ten sposób w błąd. Wobec powyższego, odnosząc się do kwalifikacji prawnej przestępstw, których znamiona może wypełniać powyższe zachowanie, wskazać należy przede wszystkim kradzież tożsamości (art. 190a § 2 k.k.), ale również m.in. stalking (art. 190a § 1 k.k.), oszustwo (art. 286 § 1 k.k.) lub grooming (art. 200a k.k.).

Słowa kluczowe: catfishing, kradzież tożsamości, cyberbezpieczeństwo.

[1] Dr Zuzanna Gądzik, Katolicki Uniwersytet Lubelski Jana Pawła II (Polska), e-mail: zuzanna.gadzik@kul.pl; ORCID: 0000-0002-9121-4658.

[2] Badania wykorzystane w artykule nie zostały sfinansowane przez żadną instytucję.

„Krytyka Prawa", tom 16, nr 4/2024, s. 298–313, ISSN 2080-1084, e-ISSN 2450-7938, © 2024 Author.

ZUZANNA GĄDZIK

Catfishing the behavior of stealing another person's identity[3]

Abstract

The subject of the article is the criminal assessment of catfishing – the behavior of stealing another person's identity or creating a false identity in order to use it as one's own – for the purpose of financial or personal abuse. This phenomenon should be interpreted in two ways – the injured party may be person whom the perpetrator impersonates and the people with whom he/she has contact and whom he/she thus misleads. Therefore, referring to the legal classification of crimes that may constitute the above behavior, first of all it should be mentioned identity theft (Article 190a § 2 of the Penal Code), but also, among others, stalking (Article 190a § 1 of the Penal Code), fraud (Article 286 § 1 of the Penal Code) or grooming (Article 200a of the Penal Code).

Keywords: catfishing, identity theft, cybersecurity.

[3] The research in this article has not been supported financially by any institution.

 DOI: 10.7206/kp.2080-1084.735

Catfishing – znaczenie

Definiując *catfishing*, wskazuje się, że jest to forma internetowego podstępu i oszustwa, polegająca na kradzieży istniejącej tożsamości innej osoby lub stworzenia fałszywej tożsamości, a następnie wykorzystanie tej skradzionej bądź fałszywej tożsamości jako swojej własnej. Cechą charakterystyczną *catfishingu* jest nakłonienie innej osoby do nawiązania relacji online, aby w następstwie tego doprowadzić do jej wykorzystania – w formie finansowych wyłudzeń lub osobistych nadużyć[4]. *Catfishing* jest kojarzony przede wszystkim z portalami randkowymi, lecz może przybierać również inne formy. Najczęściej będzie wiązał się on obecnie z zakładaniem fikcyjnych kont użytkowników portali społecznościowych.

Na chwilę obecną brak polskiej nazwy opisywanego zjawiska. Określenie *catfishing* zostało zaczerpnięte z tytułu filmu dokumentalnego Neva Schulmana *Catfish* (ang. sum). Fabuła filmu opiera się na historii mieszkańca Nowego Yorku, który nawiązał romantyczną relację przez internet z atrakcyjną 19-letnią kobietą – mieszkanką stanu Michigan. Z uwagi na pewne nieścisłości w przedstawionej przez nią historii, postanowił zweryfikować pewne fakty osobiście. Ostatecznie odkrył, że przez cały czas korespondował z 40-letnią gospodynią domową[5].

Biorąc pod uwagę rozwój internetu i mediów społecznościowych, można stwierdzić, że *catfishing* staje się coraz częstszy, a zachowania, które mieszczą się w jego ramach, przybierają coraz poważniejsze formy. Z tego względu zaczęły one stanowić podstawę odpowiedzialności prawnej – zarówno cywilnej (odszkodowawczej)[6], jak i karnej. W kontekście tym należy zaznaczyć, że proceder *catfishingu* trzeba interpretować dwutorowo – pokrzywdzonym może być bowiem zarówno osoba, pod którą sprawca się podszywa, jak i osoby, z którymi ma on kontakt i które wprowadza w błąd co do swojej tożsamości. Zdarza się też, że obie te sfery przenikają się wzajemnie. Zwłaszcza w przypadku odpowiedzialności karnej forma zachowania sprawcy ma kluczowe znaczenie – przekłada się ona bowiem na

---

4 Zob. C. Lauder, E. March, *Catching the catfish: Exploring gender and the Dark Tetrad of personality as predictors of catfishing perpetration*, "Computer in Human Behaviour" 2023, 140.

5 E. McCarthy, *What is catfishing? A brief (and sordid) history*, "The Washington Post", 9 stycznia 2016. Pozyskano z: https://www.washingtonpost.com/news/arts-and-entertainment/wp/2016/01/09/what-is-catfishing-a-brief-and-sordid-history.

6 Jej przykładem może być sprawa Kirat Assi v Simran Kaur Bhogal. Pozyskano z: https://www.5rb.com/news/tortoise-launches-podcast-based-on-cat-fishing-case/.

pociągniecie do odpowiedzialności za różne czyny, a w pewnych przypadkach może wyłączać w ogóle ten rodzaj odpowiedzialności.

Kradzież tożsamości

Analizując zjawisko *catfishingu*, w pierwszej kolejności należy wspomnieć o odpowiedzialności za czyn z art. 190a § 2 k.k. – w brzmieniu obowiązującym od 1 października 2023 roku[7]. Zgodnie z nim karze podlega sprawca, który 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. Czyn ten zagrożony jest karą pozbawienia wolności od 6 miesięcy do lat 8[8].

Biorąc pod uwagę istotę *catfishingu* – sprowadzającą się zazwyczaj do kradzieży tożsamości, można by przyjąć, że jego sprawcy powinni każdorazowo ponosić odpowiedzialność za czyn z art. 190a § 2 k.k. Wniosek ten jest jednak mylny. Wypełnienie znamion powyższego przestępstwa nie zawsze będzie pokrywać się ze sposobem postępowania w ramach *catfishingu.* Konieczna staje się więc każdorazowa weryfikacja, przeciwko komu osoba podszywająca się w rzeczywistości postępuje, jaką formę przybiera jej zachowanie i w jakim celu ma ono miejsce.

Zgodnie z literalnym brzmieniem zachowanie sprawcy przestępstwa z art. 190a § 2 k.k. sprowadza się do fałszywego podawania się za kogoś[9]. Może ono polegać na stworzeniu mylnego przekonania, że jest kimś innym – przez wprowadzanie w błąd co do swojej tożsamości lub czynne utwierdzanie w tym przekonaniu[10]. Ustawodawca określa sposób, w jaki sposób sprawca może wykorzystywać cudzą tożsamość – dotyczy to wykorzystania wizerunku, innych danych osobowych lub innych danych, za pomocą których dana osoba jest publicznie identyfikowana. W doktrynie podkreśla się przy tym, że warunkiem koniecznym do popełnienia przestępstwa stypizowanego w art. 190a § 2 k.k. nie jest skuteczne wprowadzenie

---

7 Przepis art. 190a § 2 k.k. został znowelizowany na gruncie ustawy z dnia 7 lipca 2022 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U., poz. 2600).

8 Jednocześnie warto zaznaczyć, że przepis ten został zmieniony na gruncie ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywoływanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (Dz.U., poz. 568) – poza podniesieniem granic ustawowego zagrożenia ustawodawca dodał do opisu znamion zachowanie związane z wykorzystaniem innych danych, za pomocą których dana osoba jest publicznie identyfikowana.

9 https://sjp.pwn.pl/sjp/podszyc-sie;2502866.html.

10 K. Sowirka, *Przestępstwo „kradzieży tożsamości" w polskim prawie karnym*, „Ius Novum" 2013, 1, s. 67.

 DOI: 10.7206/kp.2080-1084.735

w błąd innej osoby[11]. W większości zachowań mieszczących się w ramach zjawiska *catfishingu* skutek ten będzie jednak zwykle występował – a przynajmniej taki będzie cel jego sprawcy.

Na wstępie należy też zaznaczyć, że zachowania mieszczące się w ramach *catfishingu* nie polegają na nielegalnym pozyskiwaniu dostępu do cudzych kont w serwisach społecznościowych. Zachowanie to stanowi oczywiście czyn zabroniony (np. z art. 267 § 1 k.k.), ale nie wypełnia znamion art. 190a § 2 k.k. Z drugiej jednak strony, może ono stanowić pewien środek do celu – sprawcy *catfishingu* dostają się w sposób nielegalny na konta wybranych użytkowników, aby w ten sposób zdobyć jak największą ilość wstawionych przez nich informacji, dzięki którym stworzony przez nich fałszywy profil w mediach społecznościowych, będzie wyglądał na wiarygodny.

Odnosząc się do samej czynności sprawczej – zarówno w kontekście ogólnym, dotyczącym znamion czynu stypizowanego w art. 190a § 2 k.k., jak i związanym ściśle z *catfishingiem* – sprawca może ponieść odpowiedzialność nawet jeżeli jego zachowanie będzie miało charakter jednorazowy. W odróżnieniu od przestępstwa *stalkingu* (art. 190a § 1 k.k.) ustawodawca nie uzależnił odpowiedzialności karnej za podszywanie się pod kogoś od uporczywości takiego postępowania[12]. Nie można przy tym pominąć faktu, że istota *catfishingu* sprowadza się do stopniowego wprowadzania w błąd swojej ofiary i utwierdzaniu jej w przekonaniu co do fałszywej tożsamości. Pozwala to założyć, że większość przypadków będzie wiązała się z powtarzalnością zachowania sprawcy. W zakresie tym nie można też wykluczyć odpowiedzialności karnej za popełnienie wskazanego przestępstwa w ramach czynu ciągłego (art. 12 § 1 k.k.).

Należy też dodać, że sposób pozyskania przez sprawcę wizerunku pokrzywdzonego lub jego charakterystycznych danych nie musi mieć charakteru bezprawnego. W wielu przypadkach ofiara sama udostępnia pewne informacje na swój temat w sieci (np. wrzucając na publiczny profil swoje zdjęcia lub samodzielnie podając pewne dane na swój temat – m.in. datę urodzenia, miejsce zamieszkania, miejsce pracy itd.). Mimo że pokrzywdzony nie wyraża w ten sposób zgody (nawet w sposób dorozumiany) co do możliwości wykorzystania swojej tożsamości przez kogoś innego, często w pewien sposób przyczynia się do powstania takiej sytuacji[13].

---

11 A. Lach, *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015, s. 93.

12 Por. R. Krajewski, *Przestępstwo nękania innej osoby lub podszywania się pod inną osobę*, „Przegląd Sądowy" 2012, 5, s. 27.

13 Por. J. Sobczak, K. Kakareko, *Nękanie w Internecie*, [w:] *Stalking*, red. M. Mozgawa, Warszawa 2018, s. 198 i nast.; A. Kozień, *Problematyka ochrony danych osobowych w mediach społecznościowych*, [w:] *Prawo a media społecznościowe*, red. R. Markiewicz, Kraków 2022, s. 103 i nast.

Przez wizerunek rozumie się „podobiznę człowieka utrwaloną jako portret, fotografia lub w innej postaci”[14]. Sąd Najwyższy w wyroku z 20 maja 2005 r. doprecyzował ponadto, że „[w]izerunek, poza dostrzegalnymi dla otoczenia cechami fizycznymi, tworzącymi wygląd danej jednostki i pozwalającymi – jak się określa – na jej identyfikację wśród innych ludzi może obejmować dodatkowe utrwalone elementy związane z wykonywanym zawodem jak charakteryzacja, ubiór, sposób poruszania się i kontaktowania z otoczeniem”[15]. Wydaje się, że kwestia kradzieży wizerunku staje się szczególnie problematyczna, w związku ze stosowaniem technik *deepfake*, umożliwiających zmianę twarzy na dowolnym zdjęciu lub nagraniu[16].

Zgodnie z art. 4 pkt 1 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)[17] danymi osobowymi są wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Innymi danymi niż dane osobowe, przez które określona osoba może być publicznie identyfikowana, są natomiast wszelkie inne informacje, które są na tyle charakterystyczne, że pozwalają na wyróżnienie i powiązanie ich w przestrzeni publicznej z określoną osobą[18]. Wśród danych tego rodzaju wymienia się m.in. dane

---

14 Wyrok SN z 7 października 2009 r., III CSK 39/09, Legalis nr 288250.

15 Wyrok SN z 20 maja 2004 r., II CK 330/03, Legalis nr 65950. Na temat pojęcia wizerunku, jako znamienia przestępstwa z art. 190a § 2 k.k. zob. szerzej: A. Błachnio, *Wizerunek jako przedmiot czynności wykonawczej przestępstwa kradzieży tożsamości – uwagi na tle art. 190a § 2 k.k.*, [w:] *Kradzież tożsamości w Internecie*, red. A. Gołębiowska, Warszawa 2017, s. 67 i nast.; N. Święch-Czech, *Ochrona dóbr osobistych w Internecie*, [w:] *Czego nie wolno robić w Internecie. Poradnik dla blogerów, vlogerów, gamerów i instagramowiczów,* red. K. Grzybczyk, Warszawa 2017, s. 156 i nast.

16 Por. np. H. Farid, *Creating, Using, Misusing, and Detecting Deep Fakes,* "Journal of Online Trust and Safety" 2022, 9, s. 1–33.

17 Rozporządzenie 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) Dz. Urz. UE. L Nr 119, s. 1.

18 Por. M. Budyn-Kulik, *Przestępstwo kradzieży tożsamości po zmianach wprowadzonych ustawą z 31 marca 2020 r. nowelizującej przepisy w sprawie COVID-19*, „Studia Prawnicze” 2020, 2, s. 31.

 DOI: 10.7206/kp.2080-1084.735

zanonimizowane, adres e-mail niebędący adresem konkretnego człowieka (tj. niezawierający imienia, nazwiska, pseudonimu itd.) oraz numer KRS[19].

W kontekście odpowiedzialności za czyn z art. 190a § 2 k.k. nie ma znaczenia, którą (i ile) z wymienionych w tym przepisie form wykorzysta sprawca[20]. Może np. posłużyć się fikcyjnym imieniem i nazwiskiem nieistniejącej osoby, lecz wykorzystać przy tym cudze zdjęcie prawdziwego użytkownika, któregoś z portali społecznościowych lub podanie prawdziwych danych osobowych, przy jednoczesnym pominięciu zdjęcia profilowego. Zasadniczo istotne jest to, że sprawca wykorzystuje wizerunek lub charakterystyczne dane innej osoby, którymi nie ma prawa dowolnie dysponować i ich przetwarzać.

Warto również zaznaczyć, że w przypadku mediów społecznościowych podszywanie się pod inną osobę może dotyczyć nie tylko pojedynczych danych, lecz także ich określonych zespołów, których składowe dopiero w zestawieniu z pozostałymi elementami, pozwalają na identyfikację danego użytkownika (np. imię, nazwisko, miejsce zamieszkania i miejsce pracy). Pomimo obowiązku podawania prawdziwych danych, wielu użytkowników mediów społecznościowych celowo zastępuje informacje o sobie danymi, które teoretycznie ograniczają możliwość ich wyszukania przez osoby postronne, a przez to zwiększa ich poczucie anonimowości[21]. Wobec tego często dopiero zestawienie większej liczby tych danych pozwala na ustalenie tożsamości danej osoby, a w pewnych przypadkach jest to wręcz niemożliwe.

W przypadku *catfishingu* określenie katalogu danych, które może w sposób przestępny wykorzystać sprawca czynu z art. 190a § 2 k.k., jest uzależnione w znacznej mierze od treści formularza rejestracji wybranych mediów społecznościowych, jak również dostępnych w nich opcji udostępniania i prezentowania treści. Przykładowo w przypadku serwisu społecznościowego Facebook użytkownik jest identyfikowany przede wszystkim przez swoje imię i nazwisko. Może on jednak upublicznić również inne dane, które pozwolą na jego powiązanie z konkretną osobą – m.in. płeć, datę urodzenia, miejsce zamieszkania, adres e-mail, numer telefonu, powiązania rodzinne z innymi użytkownikami, miejsce pracy, ukończone szkoły itd.[22].

---

19 *Ibidem*, s. 33. Por. także: P. Palichleb, *Zmiany art. 190a K.K.*, „Ius Novum" 2021, 4, s. 68.

20 Por. wyrok SA w Krakowie z 8 stycznia 2019 r., II AKa 194/17, LEX nr 2707539.

21 Przykładowo zamiast podania swojego pełnego imienia i nazwiska, użytkownicy używają pseudonimy, dwukrotnie powtarzają swoje imię (np. Anna Anna), dokonują rozczłonowania swojego imienia, celem nadania drugiemu członowi charakteru nazwiska (np. Kata Rzyna).

22 W literaturze wskazuje się, że gdy zna się tylko imię i nazwisko pokrzywdzonego oraz ewentualnie nazwę miejscowości, w której mieszka, możliwe jest szczegółowe poznanie lub z dużą dozą prawdopodobieństwa przynajmniej domniemanie określonych danych wybranego użytkownika mediów społecznościowych. Zob. szerzej: T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny*, Inowrocław 2013, s. 148 i nast.

W przypadku *catfishingu* w celu pociągnięcia sprawcy do odpowiedzialności karnej za czyn z art. 190a § 2 k.k. konieczne jest, aby osoba, pod którą podszywa się sprawca, w rzeczywistości istniała. Nie wypełni zatem znamion tego czynu podszywanie się pod osoby fikcyjne (np. bohaterów filmów lub gier komputerowych), nawet jeżeli sprawca wykorzysta wizerunek osoby, która wcielała się w taką postać (zwykle aktora). To samo dotyczy podszywania się pod osoby zmarłe. Pokrzywdzonym czynem z art. 190a § 2 k.k. może być wyłącznie osoba żyjąca[23]. Jednocześnie nie jest konieczne, aby sprawca i pokrzywdzony się znali. Sprawca może podszywać się pod zupełnie przypadkową osobę.

Biorąc pod uwagę stronę podmiotową przestępstwa z art. 190a § 2 k.k., nie będzie wypełniało jego znamion, zachowanie sprawcy, który co prawda wykorzystuje fałszywą – fikcyjną tożsamość osoby nieistniejącej, w oparciu o którą ktoś skojarzy ją z prawdziwą, istniejącą osobą. Za problematyczne uznaje się również zachowania, w których sprawca przywłaszcza sobie tylko niektóre elementy tożsamości pokrzywdzonego (np. jego wizerunek), jednocześnie wskazując własne – prawdziwe dane (np. swoje imię i nazwisko). W doktrynie podnoszono, że w takiej sytuacji organ procesowy jest każdorazowo zobowiązany do oceny, czy rodzaj wykorzystywanych danych osobowych, jak również ich zakres pozwalają na przyjęcie, iż doszło do podszywania się pod inną osobę[24]. Może się też zdarzyć, że w celu wprowadzenia danej osoby w błąd co do swojej tożsamości sprawca wykorzystuje wizerunek, dane osobowe lub inne charakterystyczne dane kilku lub wielu osób. Tym sposobem może np. zwiększyć wiarygodność danych przekazywanych pokrzywdzonemu. W przypadku, gdy sprawca podszywa się pod większą liczbę osób, może dojść do realnego zbiegu kilku przestępstw z art. 190a § 2 k.k. – niezależnie od odpowiedzialności za czyny wymierzone w osobę, która jest wprowadzana w błąd.

Co do zasady nie będzie też wypełniała znamion przestępstwa stypizowanego w art. 190a § 2 k.k. odmiana *catfishingu*, jaką jest *kittenfishing.* W tym przypadku użytkownik mediów społecznościowych nie tyle wykorzystuje bowiem cudzą tożsamość, ile wprowadza w błąd co do swojej własnej charakterystyki[25]. Jednocześnie należy dodać, że nie dojdzie do wyłączenia tej odpowiedzialności, jeżeli przedstawiając swój opis, celowo stylizuje się on na inną osobę, w sposób, który mógłby sugerować w sposób obiektywny, że jest on konkretnym użytkownikiem. Oczywiste jest też, że może on ponieść odpowiedzialność za czyny skierowane wobec osób, które w ten sposób wprowadził w błąd (np. oszustwo).

---

23 Jednocześnie należy zaznaczyć, że nie wyklucza to odpowiedzialności sprawcy za inne przestępstwa, np. z art. 286 k.k.

24 A. Lach, *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, 3, s. 34.

25 Por. A. Lim, *Exploring Dating Apps: Catfishing or Kittenfishing.* Pozyskano z: https://etd.ohiolink.edu/acprod/odb_etd/etd/r/1501/10?clear=10&p10_accession_num=akron164977706240253.

 DOI: 10.7206/kp.2080-1084.735

W odniesieniu do odpowiedzialności karnej, istotne jest to, że czyn z art. 190a § 2 k.k. można popełnić wyłącznie umyślnie z zamiarem bezpośrednim lub ewentualnym. Przed wejściem w życie nowelizacji kodeksu karnego z 7 lipca 2022 r. ustawodawca przewidywał pociągnięcie sprawcy do odpowiedzialności wyłącznie w razie wykazania, że działał on z zamiarem bezpośrednim[26]. Nie było zatem wystarczające, aby ten jedynie godził się na to, że poprzez podszywanie się pod inną osobę może wyrządzić jej szkodę majątkową lub osobistą[27]. Takie rozwiązanie było problematyczne, biorąc pod uwagę, że często osoby podszywające się pod kogoś innego, robią to jedynie dla rozrywki, nie mając przy tym żadnego konkretnego celu. Obecne brzmienie przepisu art. 190a § 2 k.k. umożliwia pociągnięcie sprawcy do odpowiedzialności również wówczas, gdy celem zachowania sprawcy nie było wyrządzenie pokrzywdzonemu powyższych szkód – lecz z pewnych przyczyn do tego doszło. Z tych względów nie można wykluczyć odpowiedzialności karnej za wspomniany czyn, w przypadku, gdy sprawca wykorzystuje co prawda cudzy wizerunek, dane osobowe lub inne dane, za pomocą których określona osoba jest publicznie identyfikowana, robiąc to z innych motywów niż wyrządzenie szkody majątkowej lub osobistej. Dopuszczalna jest również odpowiedzialność karna z art. 190a § 2 k.k. za *catfishing* w przypadku, gdy doszło do takiej szkody, choć celem osoby podszywającej się było np. zwiększenie własnej atrakcyjności lub wiarygodności, chęć nawiązania kontaktu z konkretnymi osobami, zdobycie określonych informacji lub przekazanie w pozornie anonimowy sposób jakichś treści – zaś sprawca co najmniej przewidywał możliwość spowodowania szkody majątkowej lub osobistej osobie, pod którą się podszywa.

Wystąpienie negatywnych skutków w przypadku *catfishingu* jest zatem uzależnione od tego, w jakim celu i w jaki sposób jego sprawca podszywał się pod inną osobę. Zasadniczo podejmując takie czynności, powinien on bowiem przewidywać, że jego zachowanie może doprowadzić do poszkodowania osoby, której tożsamość sobie przywłaszcza – zwłaszcza jeżeli robi to w celu wprowadzenia w błąd osób trzecich. Sprawca ma świadomość, że wizerunek lub określone dane nie należą do niego i nie ma prawa się nimi posługiwać. Tymczasem podejmuje takie czynności dla realizacji zachowań, które mogą stanowić inne czyny zabronione lub przynajmniej powinny być uznane za moralnie naganne. W takiej sytuacji wydaje

[26] Zgodnie z wcześniejszym brzmieniem przepisu art. 190a § 2 k.k. odpowiedzialność karną ponosił sprawca, który podszywając się pod inną osobę, wykorzystywał jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej.

[27] Wyrok SN z 27 stycznia 2017 r., V KK 347/16, LEX nr 2269116. Por. także: A. Lach, Kradzież…, *op. cit.*, s. 33.

się, że ryzyko wystąpienia przynajmniej szkody o charakterze osobistym jest wpisane w ten rodzaj zachowań.

Jak wspominano, do znamion przestępstwa z art. 190a § 2 k.k. należy obecnie wyrządzenie pokrzywdzonemu określonego rodzaju szkody – majątkowej lub osobistej. We wcześniejszym stanie prawnym sprawca nie ponosił odpowiedzialności, gdy wymieniony powyżej skutek co prawda wystąpił, nawet gdy sprawca przewidywał, że sytuacja taka może mieć miejsce, lecz nie można było wykazać, że chciał on tę szkodę wyrządzić[28]. Przyjmowano, że przepis art. 190a § 2 k.k. stanowił tzw. kryminalizację na przedpolu skutku[29]. W powyższym kontekście trzeba również dodać, że szkoda, z którą wiąże się zachowanie sprawcy, dotyczy wyłącznie pokrzywdzonego, pod którego ten się podszywa. Jest to istotne, gdyż w przypadku *catfishingu* cel jest szerszy – odnosi się on przede wszystkim do wprowadzania w błąd osób trzecich. W takim przypadku sprawca może ponieść odpowiedzialność karną za inny czyn – wymierzony w dobra tych osób.

Zgodnie z ogólnymi zasadami, wynikającymi z prawa cywilnego, przez szkodę majątkową rozumie się wystąpienie uszczerbku w majątku poszkodowanego. Może ona przybrać jedną z dwóch postaci: straty rzeczywistej (*damnum emergens*) lub utraconych korzyści (*lucrum cessans*)[30]. Szkoda osobista ma natomiast miejsce w razie naruszenia dóbr osobistych poszkodowanego. Może przybrać formę krzywdy (ujemnych przeżyć psychicznych i fizycznych, wynikających ze zdarzenia będącego źródłem szkody niemajątkowej) lub szkody majątkowej[31]. Biorąc pod uwagę specyfikę *catfishingu*, można stowerdzić, że częstszym skutkiem będzie wystąpienie szkody osobistej. Nie można jednak wykluczyć możliwości wystąpienia szkód majątkowych (np. w przypadku podszywania się pod osobę, promującą własne produkty lub markę). Na marginesie warto zaznaczyć, że mimo iż do znamion czynu z art. 190a § 2 k.k. zalicza się wyrządzenie szkody osobistej lub majątkowej, to sam sprawca (ani inna osoba) nie musi odnieść z tego tytułu żadnej korzyści[32].

Wystąpienie szkody majątkowej lub osobistej musi mieć charakter obiektywny. Konieczne jest wykazanie, że skutek taki w rzeczywistości nastąpił. Ocena ta

---

28 W doktrynie pozytywnie ocenia się zmianę polegającą na rozszerzeniu strony podmiotowej wskazanego przestępstwa. Jednocześnie pojawiają się wnioski *de lege ferenda* związane z użyciem w przepisie art. 190a § 2 k.k. sformułowania „w zamiarze wyrządzenia jej szkody", dzięki czemu możliwe byłoby przyjęcie obu postaci zamiaru, przy jednoczesnym zachowaniu formalnego charakteru przestępstwa. Zob. K. Nazar, *Uporczywe nękanie i kradzież tożsamości*, [w:] *Przestępstwa przeciwko wolności*, red. M. Mozgawa, Lublin 2020, s. 352.

29 Por. K. Sowirka, *op. cit.*, s. 73.

30 Zob. np. H. Witczak, A. Kawałko, *Zobowiązania*, Warszawa 2008, s. 40 i nast.

31 Por. szerzej: G. Michalski, *O rozumieniu pojęcia szkody na gruncie prawa karnego*, „Prokuratura i Prawo" 2020, 2, s. 53 i nast.

32 R. Krajewski, *op. cit.*, s. 28.

 DOI: 10.7206/kp.2080-1084.735

powinna mieć miejsce na podstawie zasad analogicznych jak w przypadku postępowań cywilnych, związanych z dochodzeniem odszkodowania lub zadośćuczynienia. W wypadku *catfishingu* wspomniana szkoda może przybrać różne formy – np. ośmieszenia pokrzywdzonego w danym środowisku, przypisania mu sprzecznych z jego przekonaniami poglądów, narażenia go na niechciane relacje społeczne lub roszczenia o charakterze majątkowym. Szkodą o charakterze osobistym może być również poczucie dyskomfortu psychicznego związanego ze świadomością nieautoryzowanego, a przez to często sprzecznego z wolą osoby zainteresowanej, posługiwania się wizerunkiem lub danymi, za pomocą których może być ona identyfikowana.

Na marginesie należy dodać, że przestępstwo stypizowane w art. 190a § 2 k.k. jest ścigane na wniosek pokrzywdzonego (art. 190a § 4 k.k.). Oznacza to, że w wielu przypadkach osoby, które podszywają się pod kogoś innego w ramach zjawiska *catfishingu*, pozostają bezkarne. Część osób, których tożsamość zostaje bezprawnie wykorzystana, często nie zdaje sobie sprawy, że doszło do takiego zdarzenia, a tym samym nie inicjuje postępowania karnego.

Inne formy odpowiedzialności

Oczywiste jest, że odpowiedzialność karna za kradzież tożsamości nie jest jedyną formą przeciwdziałania tego typu zjawisku. Po pierwsze, portale społecznościowe mają własne regulacje, mające na celu przeciwdziałać praktykom polegającym na wykorzystywaniu cudzej tożsamości lub podszywaniu się pod inną osobę. Ich naruszenie może prowadzić do tymczasowego lub stałego zablokowania konta danego użytkownika[33].

Niezależnie od odpowiedzialności karnej w przypadku kradzieży tożsamości – również mieszczącej się w ramach zjawiska *catfishingu* – możliwe jest wystąpienie z roszczeniami odszkodowawczymi, na gruncie przepisów prawa cywilnego. W przepisie art. 23 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny[34] ustawodawca przywołując zakres katalogu otwartego dóbr osobistych, wymienił w nim m.in. nazwisko lub pseudonim oraz wizerunek. Zgodnie z art. 24 k.c. ten, czyje dobro

---

[33] Przykładowo serwis społecznościowy Facebook przewiduje ograniczenie lub zablokowanie konta m.in. w przypadku tworzenia lub używania konta, w których celowo podano błędną tożsamość użytkownika w celu zmylenia innych. Wśród czynników branych w związku z tym pod uwagę wymienia się: wielokrotne lub znaczące zmiany szczegółowych informacji (np. imienia lub wieku); błędne informacje profilowe (np. w biogramie), używanie obrazów z banków zdjęć lub kradzionych zdjęć itd. Zob. *Integralność konta i autentyczność tożsamości*. Pozyskano z: https://transparency.fb.com/pl-pl/policies/community-standards/account-integrity-and-authentic-identity.

[34] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2024 r., poz. 1061), dalej jako: k.c.

osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny (§ 1). Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych (§ 2)[35].

Jak już wspomniano, *catfishing* jest nastawiony na wprowadzenie w błąd osób trzecich i to je należy uznać za główne ofiary jego sprawcy. Można nawet odnieść wrażenie, że pokrzywdzenie osoby, której tożsamość jest przywłaszczana, stanowi w pewnym sensie jedynie środek do celu lub pewnego rodzaju „efekt uboczny" działań sprawcy. Podszywanie się pod inną osobę ma bowiem umożliwić popełnienie innych czynów, które od początku stanowiły jego rzeczywisty zamiar. Spowodowanie szkody majątkowej lub osobistej u osoby innej, niż ta, której tożsamość została bezprawnie wykorzystana, nie mieści się jednak w znamionach czynu z art. 190a § 2 k.k. Nie oznacza to jednak, że tego typu zachowania nie będą wiązały się z odpowiedzialnością karną – choć należy zaznaczyć, iż nie we wszystkich przypadkach faktycznie do tego dojdzie[36]. Ustawodawca określił, w jakich sytuacjach wprowadzenie innej osoby w błąd będzie stanowić przestępstwo. Mimo że żaden przepis nie odnosi się w tej kwestii wprost do mediów społecznościowych, również w przypadku takiego pokrzywdzenia, wynikającego z podszywania się sprawcy pod innego ich użytkownika, możliwa jest odpowiedzialność karna za wybrane przestępstwa. Zwykle wiązać będzie się to z wystąpieniem określonego skutku – odnoszącego się do mienia pokrzywdzonego lub jego dóbr osobistych (zwłaszcza wolności).

Przepis art. 190a § 2 k.k. pozostaje zatem w realnym zbiegu z niektórymi przepisami. Oznacza to, że w przypadku gdy jednocześnie dojdzie do wyrządzenia szkody majątkowej lub osobistej osobie, pod którą podszywa się sprawca, przy jednoczesnym pokrzywdzeniu osób trzecich – wiążącym się z wprowadzeniem

---

35 Na temat ochrony cywilnoprawnej, zob. szczerzej: M.P. Ziemiak, *Kradzież tożsamości osoby fizycznej – wybrane zagadnienia cywilnoprawne*, „Gdańskie Studia Prawnicze" 2018, t. 39, s. 87 i nast.; Por. także: A. Kozień, *Ochrona dóbr osobistych w kontekście mediów społecznościowych*, [w:] *Prawo a media społecznościowe*, red. R. Markiewicz, Kraków 2022, s. 121 i nast.

36 Przykładowo, nie wypełni znamion czynu zabronionego wprowadzanie w błąd co do swojej tożsamości podczas rozmowy za pośrednictwem komunikatora internetowego, jedynie dla zwiększenia własnej atrakcyjności. Pomimo negatywnej oceny moralnej tego typu praktyk, a także częstego wystąpienia poczucia pokrzywdzenia ze strony odbiorcy, zachowania tego typu nie stanowią zasadniczo przestępstwa.

 DOI: 10.7206/kp.2080-1084.735

w błąd co do tożsamości, kwalifikacja prawna czynu powinna uwzględniać zarówno przepis art. 190a § 2 k.k. i odpowiedni przepis, kryminalizujący określone zachowanie. Do zachowań takich zaliczyć należy m.in.:

- **Oszustwo**. Zgodnie z art. 286 § 1 k.k. kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Wydaje się, że wskazany czyn będzie jednym z najczęściej występujących bezprawnych form zachowania, z którymi wiąże się ***catfishing***. Sprawca wprowadza innego użytkownika mediów społecznościowych w błąd co do swojej tożsamości (np. podszywając się pod znaną pokrzywdzonemu osobę) i prosi o przesłanie pewnej sumy pieniędzy. Wykorzystuje w ten sposób zaufanie, jakim rozmówca darzy osobę, której tożsamość została wykorzystana. Należy jednak zwrócić uwagę, że zachowanie takie będzie wypełniać znamiona oszustwa zarówno wtedy, gdy sprawca wykorzysta stworzony od podstaw fałszywy, cudzy profil, jak i gdy uzyska w sposób bezprawny dostęp do cudzego konta i za jego pośrednictwem nakłoni inną osobę do niekorzystnego rozporządzenia mieniem.

  Nie będzie wypełniało znamion oszustwa wprowadzenie innej osoby w błąd w celu osiągnięcia korzyści o charakterze osobistym (np. zdobycie cudzych danych, nawiązanie relacji towarzyskich, przekonanie do bezpłatnego zagłosowania w konkursie internetowym lub kliknięcia w link zawierający szkodliwe oprogramowanie). Mimo że zachowania takie będą mieścić się w potocznym określeniu pojęcia „oszukać", ustawodawca zastrzegł, iż odpowiedzialność za czyn stypizowany w art. 286 § 1 k.k. dotyczy wyłącznie niekorzystnego rozporządzania mieniem;
- ***Phishing***. Do karalnych zachowań, związanych z osiągnięciem innych korzyści niż majątkowe – do popełnienia których może być wykorzystana fałszywa tożsamość sprawcy, zaliczyć należy ataki *phishingowe.* Przyjmuje się, że polegają one na łamaniu zabezpieczeń – poprzez podstępne uzyskiwanie haseł dostępu do chronionych kont internetowych, danych osobowych lub numerów kart kredytowych – za pomocą podszywania się pod inny podmiot (np. przedstawiciela instytucji finansowej). Wynikiem powyższej działalności może być kradzież danych związanych z działalnością finansową, a także zdjęć, dokumentów, utworów itd.[37]. Takie uzyskiwanie dostępu do

[37] A. Kozeń, *Ochrona dóbr…*, s. 124 i wskazana tam literatura.

określonych informacji może wypełniać znamiona przestępstw przeciwko ochronie informacji (przede wszystkim art. 267 k.k.).

- ***Grooming.*** Przejawem zachowania, w którym sprawca może doprowadzić do pokrzywdzenia dzięki wykorzystaniu fałszywej tożsamości jest tzw. *grooming*. Zgodnie z przepisem art. 200a § 1 k.k. kto w celu popełnienia przestępstwa określonego w art. 197 § 4 lub art. 200, jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15, zmierzając, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim, podlega karze pozbawienia wolności do lat 3. Zachowanie sprawcy może w tym przypadku polegać na celowym wprowadzaniu w błąd co do swojego wieku – poprzez podszywanie się pod osobę małoletnią. W ten sposób może on zdobyć zaufanie pokrzywdzonego, które w dalszej kolejności zostanie wykorzystane w celach, o których mowa we wspomnianym przepisie. Zachowanie to stanowi zatem w pewnym sensie karalną formę przygotowania.
- ***Stalking*** (art. 190a § 1 k.k.). Przy wykorzystaniu cudzej tożsamości, sprawca może także uporczywie nękać osobę, z którą nawiązuje w ten sposób kontakt. Zgodnie z art. 190a § 1 k.k., 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. W tym zakresie sprawca może wykorzystywać fikcyjną tożsamość, w celu dotarcia do pokrzywdzonego, przekazywania mu określonych treści, oddziaływania na niego poprzez kreowania fałszywej rzeczywistości, którą ten uznaje za prawdziwą itd.

Zakończenie

Catfishing stanowi jeden z wielu przejawów naruszania bezpieczeństwa i prywatności użytkowników sieci teleinformatycznej. Mimo że nie został on odrębnie stypizowany jako czyn zabroniony, zachowanie to – jak wykazano powyżej – nie może zostać uznane za legalne. Co więcej, może stanowić ono też punkt wyjścia dla dalszych naruszeń, często o wyższej społecznej szkodliwości. Obecnie trudno jednak ocenić jego dokładną skalę. Z uwagi na brak kryminalizacji samego tworzenia fałszywych profili w mediach społecznościowych część jego przejawów nie jest uwzględniana w statystykach kryminalnych. Co więcej, spory odsetek

 DOI: 10.7206/kp.2080-1084.735

pokrzywdzonych nie zdaje sobie często sprawy, że ich dane lub wizerunek zostały wykorzystane w ten sposób – przez co czyn ten nie zostaje zgłoszony organom ścigania. Również sama różnorodność sposobów zachowania sprawców może utrudniać ich jednorodną ocenę i ewentualną konieczność kryminalizacji.

Biorąc pod uwagę powszechność dostępu do internetu – w tym także do mediów społecznościowych, wydaje się, że jest niemal niemożliwe uniknięcie ryzyka kradzieży swojego wizerunku lub odpowiednich danych. Rozwój nowych serwisów i aplikacji, których celem jest pozornie ułatwienie pewnych aspektów życia ich użytkowników, w rzeczywistości może wiązać się z niebezpieczeństwem utraty kontroli nad własnymi danymi lub wizerunkiem. Pomimo istnienia wielu kampanii i programów, mających na celu uświadamianie społeczeństwa co do zagrożeń związanych ze zbyt lekkomyślnym udostępnianiem informacji w sieci, można postawić tezę, że właśnie taki rodzaj zachowania stanowi jedną z podstawowych przyczyn bezprawnego wykorzystywania cudzej tożsamości.

Wydaje się, że na chwilę obecną nie jest konieczne wprowadzanie odrębnych regulacji prawnokarnych, dotyczących zjawiska *catfishingu.* Aktualne rozwiązania uznać należy za wystarczające. Jednocześnie priorytetowe znaczenie przypisać należy prewencji pozytywnej – związanej z bezpiecznym korzystaniem z internetu (m.in. w zakresie świadomego upubliczniania pewnych treści), jak również z uświadamianiem użytkowników, że zachowania mające w świecie wirtualnym mogą mieć swoje poważne konsekwencje w świecie rzeczywistym.

Bibliografia

Błachnio A., *Wizerunek jako przedmiot czynności wykonawczej przestępstwa kradzieży tożsamości – uwagi na tle art. 190a § 2 k.k.*, [w:] A. Gołębiowska (red.), *Kradzież tożsamości w Internecie,* Warszawa 2017. doi: 10.5604/01.3001.0013.5680.

Budyn-Kulik M., *Przestępstwo kradzieży tożsamości po zmianach wprowadzonych ustawą z 31 marca 2020 r. nowelizującej przepisy w sprawie COVID-19*, „Studia Prawnicze" 2020, 2.

Farid, Creating H., Using, *Misusing, and Detecting Deep Fakes,* „Journal of Online Trust and Safety" 2022, 9.

Kozień A., *Ochrona dóbr osobistych w kontekście mediów społecznościowych*, [w:] R. Markiewicz (red.), *Prawo a media społecznościowe*, Kraków 2022.

Kozień A., *Problematyka ochrony danych osobowych w mediach społecznościowych*, [w:] R. Markiewicz (red.), *Prawo a media społecznościowe,* Kraków 2022.

Krajewski R., *Przestępstwo nękania innej osoby lub podszywania się pod inną osobę,* „Przegląd Sądowy" 2012, 5.

Lach A., *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015.

Lach A., *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, 3.

Lauder C., March E., *Catching the catfish: Exploring gender and the Dark Tetrad of personality as predictors of catfishing perpetration,* „Computer in Human Behaviour" 2023, 140. doi: 10.1016/j.chb.2022.107599.

Lim A., *Exploring Dating Apps: Catfishing or Kittenfishing.* Pozyskano z: https://etd.ohiolink.edu/acprod/odb_etd/etd/r/1501/10?clear=10&p10_accession_num=akron164977706240253.

McCarthy E., *What is catfishing? A brief (and sordid) history*, „The Washington Post", 9 stycznia 2016. Pozyskano z: https://www.washingtonpost.com/news/arts-and-entertainment/wp/2016/01/09/what-is-catfishing-a-brief-and-sordid-history.

Michalski G., *O rozumieniu pojęcia szkody na gruncie prawa karnego*, „Prokuratura i Prawo" 2020, 2.

Nazar K., *Uporczywe nękanie i kradzież tożsamości*, [w:] M. Mozgawa (red.), *Przestępstwa przeciwko wolności*, Lublin 2020.

Sobczak J., Kakareko K., *Nękanie w Internecie*, [w:] M. Mozgawa (red.), *Stalking,* Warszawa 2018.

Sowirka K., *Przestępstwo „kradzieży tożsamości" w polskim prawie karnym*, „Ius Novum" 2013, 1.

Święch-Czech N., *Ochrona dóbr osobistych w Internecie,* [w:] K. Grzybczyk (red.), *Czego nie wolno robić w Internecie. Poradnik dla blogerów, vlogerów, gamerów i instagramowiczów*, Warszawa 2017.

Trejderowski T., *Kradzież tożsamości. Terroryzm informatyczny*, Inowrocław 2013.

Witczak H., Kawałko A., *Zobowiązania*, Warszawa 2008.

 DOI: 10.7206/kp.2080-1084.735