Zakres skuteczności regulacji art. 190a § 2 KK dla zwalczania działań sprawczych związanych z tzw. kradzieżą tożsamości w sieci Internet

dr *Piotr Siemkowicz*[1]

Celem niniejszego opracowania jest analiza art. 190a § 2 KK, a w szczególności próba odpowiedzi na pytanie, jaka jest w praktyce skuteczność przedmiotowego przepisu dla zwalczania przestępstw, które wiążą się z wcześniejszym przejęciem danych dotyczących tożsamości innej osoby za pośrednictwem sieci Internet, a następnie wykorzystania tych danych dla działań przestępczych. Autor zwraca także uwagę na przykładowe techniki, którymi posługują się przestępcy w celu wyłudzania danych osobowych bądź ich przejęcia, a także sygnalizuje potencjalne zagrożenia istniejące w sieci Internet, a wiążące się z udostępnianiem danych osobowych oraz wizerunku przez użytkowników, w tym zwłaszcza na tzw. portalach społecznościowych. W opracowaniu przedstawiono także analizę nowego zjawiska, którym jest podszywanie się przez sprawców pod tzw. wirtualne postacie funkcjonujące w ramach gier typu MMORPG. Ostatecznie w opracowaniu wskazano na postulowaną konieczność dokonania zmian legislacyjnych w zakresie regulacji czynu z art. 190a § 2 KK, które mogą przyczynić się do poprawy skuteczności tego przepisu w zakresie ścigania sprawców przestępstwa „kradzieży tożsamości".

Uwagi wstępne

Nowe zdobycze technologiczne, w tym zwłaszcza wiążące się z rozwojem sieci Internet i udogodnieniami komunikacji elektronicznej, niosą za sobą także zagrożenia, które faktycznie nie istniały u schyłku XX w. Zagrożenia te, w tym także związane z tzw. kradzieżą tożsamości, stawiają w pierwszej kolejności przed ustawodawcą, a następnie organami ścigania i sądami, nowe wyzwania. Wymaga to z jednej strony stworzenia nowych i skutecznych narzędzi legislacyjnych do zwalczania tego rodzaju przestępczości, z drugiej zaś odpowiedniego przeszkolenia prokuratorów i sędziów pozwalającego na operowanie nie tylko niezbędnym zakresem wiedzy prawniczej, ale w szczególności także technicznej i informatycznej. Dopiero bowiem połączenie warsztatu pracy prawnika z niezbędnym zakresem wiedzy informatycznej pozwala na skuteczne wykrycie, a także ocenę określonych typów działań przestępczych podejmowanych najczęściej za pośrednictwem sieci Internet, a zmierzających między innymi do wejścia w posiadanie danych dotyczących tożsamości innej osoby, a następnie wykorzystania tych danych do celów przestępczych.

Kradzieży tożsamości jako przestępstwo

Wprowadzenie ustawą z 25.2.2011 r. o zmianie ustawy Kodeks karny[2] art. 190 a § 2 KK, dotyczącego tzw. kradzieży tożsamości, który wszedł w życie 6.6.2011 r., bez wątpienia było krokiem w dobrym kierunku. Przed wprowadzeniem do Kodeksu karnego omawianej regulacji wiele zachowań o charakterze przestępczym pozostawało bowiem poza możliwością ich kryminalizacji. Przytoczyć warto w tym miejscu chociażby za *F. Radoniewiczem* opisywany przez niego przypadek założenia przez nieznaną osobę profilu na Facebooku z danymi osobowymi znanego aktora, gdzie sprawca, podszywając się pod niego, korespondował z jego znajomymi z branży artystycznej oraz dokonywał wpisów komentujących aktywność podejmowaną przez innych użytkowników, czym szkodził reputacji oraz dobremu imieniu pokrzywdzonego[3]. Jak przy tym podkreślał wskazany autor, w przedmiotowej sprawie zostało ostatecznie wydane postanowienie z 29.12.2010 r. o odmowie wszczęcia dochodzenia w przedmiocie „zmiany zapisu na informatycznym nośniku danych poprzez utworzenie na portalu społecznościowym profilu pokrzywdzonego bez jego wiedzy i zgody", tj. w zakresie czynu z art. 268 § 2 KK, z uwagi na przyjęcie, że zachowanie sprawcy nie wyczerpywało znamion czynu zabronionego, przy czym faktycznie w aktualnym stanie prawnym (po 6.6.2011 r.) mogłoby to zostać zakwalifikowane jako czyn z art. 190a § 2 KK.

Oczywiste jest przy tym, że przywłaszczenie czyjejś tożsamości przez przestępcę, zwłaszcza w ramach możliwości stwarzanych przez sieć Internet, może stać się dla pokrzywdzonego faktycznym utrapieniem, z uwagi na możliwość wykorzystania takich danych osobowych przez sprawcę w ramach innych czynów karalnych, w tym głównie z art. 212

[1] Autor jest adwokatem, specjalizującym się w sprawach karnych. W zakresie zainteresowań naukowych autor zajmuje się głównie problematyką tzw. przestępstw komputerowych, w tym popełnianych za pośrednictwem sieci Internet.

[2] Dz.U. Nr 72, poz. 381.

[3] *F. Radoniewicz*, Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warszawa 2016, s. 449.

§ 2 oraz z art. 286 § 1 KK. Wszak sprawca, który wszedł w nieuprawnione posiadanie czyichś danych osobowych bądź wizerunku, może, posługując się nimi, założyć „na rachunek" pokrzywdzonego fałszywe konto e-mail (rejestrując się jako pokrzywdzony), a następnie wysyłać z niego pomawiające inne osoby treści bądź też zdjęcia i filmy objęte np. normą art. 202 § 3 i 4b KK – co może spowodować wszczęcie przeciwko tej osobie postępowania karnego oraz konieczność procesowego wykazywania, iż treści te zostały faktycznie rozpowszechnione bez wiedzy pokrzywdzonego. Osoba dysponująca danymi osobowymi innej osoby może dokonywać na jej rachunek zakupów w sieciach sklepów internetowych, a często nawet zawrzeć umowę pożyczki bądź umowę kredytową – podszywając się pod dane pokrzywdzonego, zwłaszcza jeżeli weryfikacja autentyczności pożyczkodawcy lub kredytobiorcy dokonywana przez określoną instytucję finansową nie będzie odpowiednio wnikliwa. Przestępca może ostatecznie po uzyskaniu danych osobowych pokrzywdzonego założyć w oparciu o te dane fałszywy profil na portalu społecznościowym i zamieszczać w jego ramach szkalujące pokrzywdzonego bądź inne osoby informacje, a nawet założyć – podszywając się pod niego – blog internetowy w celu zamieszczenia na nim informacji naruszających np. normę art. 256 § 1 lub art. 257 KK.

Artykuł 190a § 2 KK stanowi w szczególności, iż karze pozbawienia wolności do lat trzech podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. Z kolei art. 190a § 3 KK przewiduje formę kwalifikowaną przestępstwa „kradzieży tożsamości", zagrożoną karą pozbawienia wolności od roku do lat 10, w sytuacji gdy następstwem czynu określonego także w § 2 jest targnięcie się pokrzywdzonego na własne życie.

Ściganie przestępstwa określonego w § 2 art. 19a KK następuje przy tym na wniosek pokrzywdzonego.

Czyn z art. 190a § 2 KK jest przestępstwem formalnym – bezskutkowym, które jak słusznie zauważa się w doktrynie, zostaje dokonane w chwili, gdy sprawca przystąpił już do „robienia użytku" z danych osobowych lub wizerunku, nawet gdy szkody jeszcze nie wyrządził[4]. Przestępstwo to może zostać popełnione jedynie w zamiarze bezpośrednim kierunkowym, gdzie działanie sprawcy musi zostać podjęte w celu wyrządzenia pokrzywdzonemu konkretnej szkody materialnej lub osobistej. Tym samym do realizacji przedmiotowego przestępstwa w żadnym zakresie nie jest wystarczające działanie podjęte przez sprawcę w zamiarze ewentualnym – a więc aby sprawca jedynie godził się na wyrządzenie swoim działaniem szkody osobie, pod którą się podszywa przy wykorzystaniu jej wizerunku lub danych osobowych[5]. Podobne stanowisko wyraził także SN w wyroku z 27.1.2017 r., wskazując w tezie przedmiotowego orzeczenia, iż „przestępstwo określone w art. 190a § 2 KK może być popełnione wyłącznie w zamiarze bezpośrednim, tak więc dla realizacji jego znamion nie jest wystarczające, aby sprawca jedynie godził się na wyrządzenie swoim działaniem szkody osobie, pod którą się podszywa, wykorzystując jej wizerunek lub dane osobowe"[6].

W przypadku natomiast formy kwalifikowanej skutkiem – z art. 190a § 3 KK, jak zauważa się w doktrynie, przedmiotowy skutek w postaci targnięcia się pokrzywdzonego na własne życie niekoniecznie musi być objęty zamiarem sprawcy, natomiast musi być on obiektywnie przewidywalny, a tym samym sprawca musi co najmniej przewidywać następstwa swojego czynu[7].

Przestępstwo z art. 190a § 2 KK nie będzie możliwe do popełnienia przez zaniechanie, ponieważ użycie w nim znamienia czasownikowego „podszywać się" wymaga od sprawcy podjęcia określonego działania[8]. Stroną przedmiotową przestępstwa z art. 190a § 2 KK jest przy tym podszywanie się pod inną osobę poprzez wykorzystanie jej wizerunku lub innych jej danych osobowych w celu wyrządzenia jej szkody majątkowej lub osobistej.

Pojęcie podszywania się nie jest zdefiniowane w Kodeksie karnym. Należy więc przyjąć, że oznaczać ono będzie każdą formę wykorzystania cudzych danych osobowych lub wizerunku, która będzie stwarzała wrażenie, że użycie tych danych dokonane zostało przez ich faktycznego dysponenta, nie zaś przez osobę fikcyjnie podającą się za pokrzywdzonego. Jak słusznie zauważa przy tym *A. Lach*, zachowanie sprawcy może być bezpośrednio nakierowane na inną osobę – np. przez podanie jej danych osobowych lub też może ono oddziaływać na określone urządzenie informatyczne, weryfikujące dostęp do niego na podstawie podawanych danych[9].

Zauważyć należy, że nie zawsze „podszycie się", a więc naśladowanie danej osoby, będzie mieściło się w gestii zainteresowania prawa karnego. Jak zauważa *K. Sowirka*, samo naśladowanie kogoś, w szczególności poprzez upodobnienie się do niego strojem, wyglądem czy zachowaniem, jednakże bez zamiaru wprowadzenia w błąd innej osoby, nie będzie podlegało penalizacji na podstawie art. 190a § 2 KK[10]. Cytowany autor podaje przy tym przykłady sobowtórów oraz fanów gwiazd, którzy starają się upodobnić lub wręcz wyglądać jak ich idole, a także satyryków, parodystów i komików, którzy w ramach swojej pracy artystycznej wręcz naśladują określone osoby.

[4] *M. Filar*, [w:] *M. Filar* (red.), Kodeks Karny Komentarz, Warszawa 2016, s. 1175.

[5] *M. Królikowski*, *A. Sakowicz*, [w:] *M. Królikowski*, *R. Zawłocki* (red.), Kodeks karny część szczególna, t. I, Warszawa 2017, s. 592.

[6] V KK 347/16, Legalis.

[7] *J. Sobczak*, Wpływ internetu na zjawisko samobójstwa, [w:] *M. Mozgawa* (red.), Samobójstwo, Warszawa 2017, s. 291.

[8] *K. Sowirka*, Przestępstwo „kradzieży tożsamości" w polskim prawie karnym, IUS NOVUM 2013, Nr 1, 2013, s. 70.

[9] *A. Lach*, Kradzież tożsamości, Prokuratura i Prawo 2012, Nr 3, s. 33.

[10] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 67.

W praktyce możliwa jest również sytuacja, gdy sprawca będzie posługiwał się częściowo swoimi danymi osobowymi, częściowo zaś danymi osobowymi innej osoby – a więc np. własnym adresem i telefonem oraz imieniem i nazwiskiem innej osoby. Jak słusznie zauważa się w doktrynie, w przedmiotowej sytuacji to organ procesowy będzie musiał ocenić, czy rodzaj i zakres wykorzystanych danych osobowych pozwala na przyjęcie, iż sprawca faktycznie podszył się pod inną osobę[11].

Przestępstwo z art. 190a § 2 KK zostało przez ustawodawcę umieszczone w rozdziale XXIII Kodeksu karnego – a więc w ramach przestępstw przeciwko wolności. Umieszczenie art. 190a § 2 KK zaraz po przestępstwie stalkingu z art. 190a § 1 KK może sugerować, iż czyn z art. 190a § 2 KK jest także pewną formą przestępstwa stalkingu – co uznać należy za rozwiązanie nietrafne. W szczególności bowiem przestępstwo stalkingu z art. 190a § 1 KK wymaga dla jego realizacji „uporczywości nękania", a więc powtarzających się działań sprawcy w określonym okresie, podczas gdy czyn z art. 190a § 2 KK może być zrealizowany nawet przez jednorazowe podszycie się sprawcy pod inną osobę – poprzez wykorzystanie jej wizerunku lub innych jej danych osobowych, pod warunkiem że działanie to wiąże się z zamiarem sprawcy wyrządzenia tej osobie szkody majątkowej lub osobistej.

W doktrynie wysuwane były także uprzednio – między innymi z uwagi na wskazaną powyżej odmienność czynu z art. 190a § 2 KK od tzw. przestępstwa stalkingu opisanego w art. 190a § 1 KK – postulaty w zakresie umieszczenia czynu typizowanego w art. 190a § 2 KK w innym rozdziale Kodeksu karnego, w tym jako samodzielne (niepowiązane ze stalkingiem) przestępstwo. W szczególności *A. Lach* opowiadał się za umieszczeniem przestępstwa „kradzieży tożsamości" w rozdziale XXVII Kodeksu karnego, zawierającego przestępstwa przeciwko czci i nietykalności cielesnej[12], natomiast *K. Sowirka*, postulując zaliczenie przedmiotowego przestępstwa z art. 190a § 2 KK do przestępstw przeciwko ochronie informacji bądź do przestępstw przeciwko czci i nietykalności cielesnej, także opowiadał się za przeniesieniem przestępstwa opisanego w art. 190a § 2 KK do odrębnego artykułu w kodeksie, bez formalnego związania tego czynu ze stalkingiem[13]. Postulaty obu cytowanych autorów w pełni należy przy tym zaaprobować jako podkreślające odmienność czynu z art. 190a § 2 KK „kradzieży tożsamości" od przestępstwa stalkingu z art. 190a § 1 KK.

Wizerunek jako dobro osobiste

Pojęcie wizerunku osoby zostało uregulowane w ramach art. 23 KC dotyczącego ochrony dóbr osobistych. Przepis ten stanowi zwłaszcza, że dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Dodatkowo art. 81 ust. 1 ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych[14] wskazuje, iż rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie. Zgodnie natomiast z treścią art. 81 ust 2 PrAutU zezwolenia nie wymaga rozpowszechnianie wizerunku:

1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Jak podkreśla się także w doktrynie, pojęciu wizerunku osoby nadaje się dwa znaczenia: wąskie – związane z przedmiotem, na którym istnieje fizyczne utrwalenie wyglądu danej osoby, oraz szerokie – a więc w rozumieniu wytworu niematerialnego, który za pomocą środków plastycznych przedstawia rozpoznawalną podobiznę danej osoby, zawierając zarazem istotną wartość identyfikacyjną poszczególnych elementów takich jak kolor oczu, stale noszone okulary, fryzura, makijaż, ubiór, a nawet sposób poruszania się, zachowania czy też gestykulacji, jeśli w oderwaniu lub w łączności z innymi cechami są one dla tej osoby charakterystyczne[15].

Wizerunkiem osoby w rozumieniu art. 190a § 2 KK będzie przy tym – jak się wydaje – jedynie przedstawienie bądź też wyobrażenie określonej osoby fizycznej w postaci graficznej, a więc w postaci zdjęcia, rysunku, karykatury, w tym także we wszelkich formach przetworzonych w systemie elektronicznym. Niezbędnym wymogiem będzie jednak każdorazowo możliwość powiązania takiego wizerunku z określoną osobą fizyczną, pozwalającego na jej identyfikację.

Z uwagi na znamię czasownikowe „wykorzystania przez sprawcę wizerunku" osoby, poza zakresem kryminalizacji art. 190a § 2 KK, pozostaną zatem wszelkie inne formy posługiwania się wizerunkiem innej osoby, nieposiadającym jednak swojego wyznacznika w formie graficznej – a więc np. poprzez jedynie słowne przedstawienie tzw. wizerunku publicznego, politycznego, artystycznego związanego ze sposobem postrzegania określonej osoby przez społeczeństwo jako człowieka, polityka, naukowca itp. Oczywiste jest jednak, że posłużenie się opisem danej osoby w formie niegraficznej (opisem słownym) może skutkować realizacją przez sprawcę

[11] *A. Lach*, Kradzież tożsamości…, s. 34.
[12] *Ibidem*, s. 32.
[13] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 65–66 oraz s. 78.
[14] T.j. Dz.U. z 2017 r. poz. 880 ze zm.; dalej jako: PrAutU.
[15] *J. Barta*, *R Markiewicz*, [w:] *J. Barta, M. Czajkowska-Dąbrowska*, *Z. Ćwiąkalski*, *R. Markiewicz*, *E. Traple*, Prawo autorskie i prawa pokrewne. Komentarz, Kraków 2005, s. 626.

innego czynu karalnego, w szczególności czynu z art. 212 § 1 KK – a więc przestępstwa zniesławienia, jeżeli dodatkowo ze słownym opisem „wizerunku" danej osoby połączone będzie pomówienie jej 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. W sytuacji gdy sprawca przedstawi w sposób pejoratywny, a tym samym zniesławiający słowny opis „wizerunku" danej osoby za pośrednictwem środków masowego komunikowania się, zamieszczając taki opis np. na stronie internetowej lub też w ramach komunikatora społecznościowego, może zrealizować on swoim działaniem dyspozycję art. 212 § 2 KK.

Dane osobowe a tożsamość osoby fizycznej

Pojęcie danych osobowych uregulowane jest w art. 6 ust. 1 ustawy z 29.8.1997 r. o ochronie danych osobowych[16]. Przepis ten stanowi, iż w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Dodatkowo art. 6 ust. 2 OchrDanychU wskazuje, że osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Równocześnie art. 6 ust. 3 OchrDanychU stanowi, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Tym samym za dane osobowe w rozumieniu ustawy o ochronie danych osobowych należy uznać w szczególności adres zamieszkania, imiona i nazwiska rodziców, numer PESEL i NIP, linie papilarne, wzór siatkówki oka, a także wiele informacji dotyczących danej osoby, takich jak wykształcenie, stan cywilny, wykonywany zawód, pełnione funkcje[17]. Należy zgodzić się także z *A. Lachem*, iż imię i nazwisko danej osoby będą stanowić dane osobowe jedynie wówczas, gdy samodzielnie umożliwią identyfikację danej osoby lub też umożliwią tę identyfikację w powiązaniu z innymi informacjami[18]. Cytowany autor słusznie bowiem zauważa, że w sytuacji gdy sprawca posłuży się popularnym i często występującym imieniem i nazwiskiem (np. *Jan Kowalski*), same te dane nie będą jeszcze pozwalały na identyfikację konkretnej osoby.

Danymi osobowymi w rozumieniu ustawy o ochronie danych osobowych mogą być także adresy e-mail, adresy stron WWW bądź też loginy do określonych portali lub też usług internetowych, w sytuacji gdy samoistnie lub też w połączeniu z innymi informacjami pozwolą na zidentyfikowanie danej osoby, a więc w szczególności gdy w swojej treści zawierają imię i nazwisko użytkownika[19].

Z pojęciem danych osobowych nierozerwalnie jest związane także pojęcie tożsamości osoby ludzkiej. Tożsamość związana jest przy tym z tzw. pojęciem identyczności – oraz oznacza bycie tym samym w znaczeniu ciągłości, a także świadomość siebie oraz własnej odrębności[20]. Na pojęcie tożsamości w jej ujęciu prawnym składają się przy tym dane określające osobę, a więc jej dane osobowe, pseudonimy oraz inne dane, które bądź samodzielnie użyte, bądź też w połączeniu z innymi danymi pozwalają na jej identyfikację[21].

W ramach sieci Internet tożsamość może być przy tym postrzegana jako tożsamość rzeczywista – będąca odzwierciedleniem wszystkich danych danej osoby w świecie realnym, jako tożsamość fikcyjna – tzw. pseudonim lub nick używane w ramach czatów lub grup dyskusyjnych oraz jako tożsamość anonimowa[22]. Jak zauważa przy tym *A. Lach*, każda osoba może dysponować kilkoma tożsamościami, w tym jedną rzeczywistą i kilkoma fikcyjnymi lub anonimowymi, które tworzone są dla różnych obszarów aktywności życiowej[23].

W tym miejscu należy wskazać, że w ramach sieci Internet przetwarzane są oraz gromadzone na określonych serwerach, portalach społecznościowych, portalach sklepów internetowych, stronach WWW, w ogólnie dostępnych bazach danych, a nawet w ramach komunikatorów internetowych, ogromne ilości danych, w tym także bezpośrednio danych osobowych pozwalających na prostą identyfikację osoby, jak też danych dotyczących wizerunku osób fizycznych. Część danych osobowych i wizerunków osoby udostępniana jest dobrowolnie przez użytkowników w ramach powszechnie dostępnych usług Web 2.0 oraz wpisów na portalach społecznościowych takich jak Facebook, Twitter, nk.pl itp. Dane osobowe, takie jak imię i nazwisko właściciela firmy, a także NIP i adres prowadzonej działalności gospodarczej (często tożsamy z miejscem zamieszkania), a także numer telefonu i adres e-mail, zamieszczane są oficjalnie na stronach internetowych administrowanych przez instytucje państwowe lub publiczne, takich jak np. CEIDG. Numer PESEL każdej osoby będącej właścicielem nieruchomości odnaleźć możemy także oficjalnie w ramach ogólnie dostępnej elektronicznej bazy Ksiąg Wieczystych. Faktycznie więc uznać należy, że

[16] T.j. Dz.U. z 2016 r. poz. 922 ze zm.; dalej jako: OchrDanychU.
[17] *A. Lach*, Kradzież tożsamości…, s. 35.
[18] *Ibidem*, s. 35.
[19] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 70.
[20] *A. Lach*, Karnoprawna reakcja na zjawisko kradzieży tożsamości, Warszawa 2015, s. 1–16.
[21] *M. Romańczuk-Grącka*, Prawnokarna ochrona tożsamości elektronicznej w perspektywie przeciwdziałania nielegalnym rynkom finansowym, [w:] *W. Pływaczewski* (red.), Przeciwdziałanie patologiom na rynkach finansowych. Od edukacji ekonomicznej po prawnokarne środki oddziaływania, Warszawa 2015, s. 238.
[22] *A. Lach*, Karnoprawna reakcja…, s. 18.
[23] *Ibidem*, s. 19.

wejście w posiadanie danych osobowych określonej osoby fizycznej za pośrednictwem sieci Internet, w tym nawet za pośrednictwem wyszukiwarek internetowych, nie stanowi żadnego problemu.

Jak słusznie zauważa *T. Trejderowski*[24], w sytuacji znajomości jedynie imienia i nazwiska pokrzywdzonego i ewentualnie nazwy miasta, w którym zamieszkuje, potencjalny sprawca może uzyskać na portalu społecznościowym następujące dane dotyczące tej osoby:

- zobaczyć jej zdjęcia oraz zdjęcia jej rodziny i znajomych;
- poznać wiek, a także przybliżoną datę urodzenia;
- poznać jej znajomych, przyjaciół i kolegów z pracy oraz członków rodziny;
- uzyskać dane dotyczące tej osoby – czym się aktualnie zajmuje, gdzie pracuje lub studiuje;
- poznać przebieg jej edukacji, w tym ukończone szkoły, uczelnie oraz odbyte kursy;
- poznać numer Gadu-Gadu, Skype'a oraz telefonu;
- poznać stan cywilny na podstawie analizy nazwiska, fotografii lub porównując nazwiska znajomych;
- poprzez analizę fotografii i listy znajomych dowiedzieć się, czy dana osoba posiada dzieci, ich liczbę oraz poznać ich płeć i oszacować wiek;
- w przypadku publikacji zdjęć ze ślubu – ustalić, gdzie dana para miała uroczystość weselną;
- poprzez szczegółowe porównanie nazwisk na liście znajomych można ustalić powiązania rodzinne, w tym rodzeństwo, kuzynów, bliższych i dalszych krewnych oraz powinowatych;
- porównując szkoły i uczelnie, w których uczy się dana osoba razem ze swoimi znajomi, poznać jej znajomych z konkretnych szkół i uczelni;
- poprzez analizę podpisów pod fotografiami oraz komentarze do nich i do profilu można poznać wiele szczegółów z życia prywatnego danej osoby, a więc gdzie spędzała wakacje, w jakich klubach się bawi, jak spędza wolny czas, jakie ma hobby itp.;
- poprzez analizę dat i godzin dodawania kolejnych zdjęć lub udzielania odpowiedzi na komentarze, ustalić, w jakich porach dana osoba korzysta z Internetu, a także czy ma do niego dostęp w pracy.

Cytowany autor zwraca również uwagę, że poprzez tzw. mechanizm „like" – a więc zaznaczanie jako „lubię to" określonych wpisów czy też zdjęć np. na Facebooku, potencjalny sprawca może z łatwością ustalić, co dana osoba lubi, jakie są jej zainteresowania i poglądy[25].

Nie może jednak budzić wątpliwości, że w zakresie wskazanym powyżej na ujawnienie swojej tożsamości w sposób bezpośredni lub też co najmniej dorozumiany, a tym samym na wejście w posiadanie danych zamieszczanych na publicznych portalach – zwłaszcza o charakterze społecznościowym, wyraża zgodę sam użytkownik. Tym samym powinien on przynajmniej godzić się z tym, że inne osoby dane te poznają. W przedmiotowym wypadku potencjalny pokrzywdzony wyzbywa się niejako przysługującego mu prawa do prywatności. Poza dyskusją pozostaje ocena takiego zachowania, które bez wątpienia może narazić potencjalnego pokrzywdzonego na daleko idące i negatywne dla niego konsekwencje, także w sferze wiktymologicznej, a więc tzw. podatności na stanie się ofiarą przestępstwa. Nie ulega bowiem wątpliwości, że poza możliwością przejęcia danych osobowych takiej osoby przez potencjalnego sprawcę przestępstwa z art. 190 a § 2 KK, tego rodzaju aktywność w sferze portali społecznościowych narazić może ich użytkownika na inne niebezpieczeństwa, w tym np. na potencjalne dokonanie na jego szkodę przestępstwa z art. 279 § 1 KK, a więc kradzieży z włamaniem do jego mieszkania, w sytuacji gdy zamieści na portalu społecznościowym informację, że we wskazanym okresie przebywać będzie z całą rodziną na zaplanowanym urlopie, poza miejscem swojego zamieszkania.

Oczywistym jest także, że zdobycie przez sprawcę określonej kategorii danych osobowych innej osoby, w tym w szczególności numeru PESEL, imion rodziców i panieńskiego nazwiska matki, może umożliwić sprawcy – o czym wspomniano powyżej, popełnianie innych przestępstw bezpośrednio na szkodę osoby, której dane osobowe uzyskał, lub też na szkodę innych pokrzywdzonych, w tym w szczególności przestępstwa oszustwa z art. 286 § 1 KK, gdzie sprawca, podając się za inną osobę, może uzyskać od określonej instytucji finansowej pożyczkę kredytową lub też np. dokonać zakupów za pośrednictwem sklepu internetowego. Zauważyć także należy, iż w ramach sieci Internet weryfikacja danych osobowych następuje bez osobistego kontaktu pomiędzy osobą podającą określone dane osobowe a osobą dane te weryfikującą[26]. W ramach interakcji pomiędzy użytkownikiem – klientem a podmiotem świadczącym określone usługi w sieci Internet tożsamość danej osoby najczęściej weryfikowana jest także przy użyciu takich danych, jak login i hasło lub też token czy karta dostępu[27]. Także w przypadku dokonywania transakcji kartami płatniczymi za pośrednictwem sieci Internet brak jest możliwości faktycznej weryfikacji tego, czy osoba podająca dane niezbędne do transakcji jest faktycznym właścicielem karty płatniczej, a także czy kartą tą rzeczywiście dysponuje, czy też weszła jedynie w posiadanie numeru tej karty i danych osobowych osoby, na którą kartę wystawiono. Brak jest bowiem w tym wypadku fizycznej obecności karty płatniczej w punkcie akceptanta w chwili dokonywania

[24] *T. Trejderowski*, Kradzież tożsamości. Terroryzm informatyczny, cyberprzestępstwa, internet, telefon, Facebook, Warszawa 2013, s. 148–150.
[25] *Ibidem*, s. 151.
[26] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 65.
[27] *A. Lach*, Kradzież tożsamości…, s. 29–30.

transakcji, a także nie dochodzi do bezpośredniego kontaktu sprzedającego z kupującym[28].

Wykorzystanie cudzego wizerunku i danych osobowych a przestępstwo z art. 190a § 2 KK

Nie można także nie zauważyć, że w ramach portali społecznościowych mogą być często tworzone fałszywe konta – dotyczące faktycznie nieistniejących w rzeczywistości osób, gdzie poprzez zaproszenie potencjalnego pokrzywdzonego do tzw. grona znajomych, a następnie dokonywanie przez niego określonych wpisów, dochodzi do zbierania informacji o tej osobie, w tym także bezpośrednio w zakresie danych osobowych[29].

Czyn z art. 190a § 2 KK, w brzmieniu nadanym mu przez ustawodawcę, pozwala faktycznie na ściganie jedynie tych sprawców, którzy podszywając się pod inną osobę oraz wykorzystując w tym celu jej wizerunek lub inne dane osobowe, działają w celu wyrządzenia jej szkody majątkowej lub osobistej. Oznacza to, iż poza zainteresowaniem art. 190a § 2 KK pozostają wszelkie te działania potencjalnych sprawców, które nie są nakierowane na wyrządzenie szkody majątkowej lub osobistej.

Wobec powyższego samo pozyskiwanie i gromadzenie czyichś danych osobowych za pośrednictwem sieci Internet bądź też wizerunków danej osoby fizycznej, w sytuacji gdy sprawca dopiero w przyszłości zamierza przy ich pomocy podszywać się pod tę osobę w celu wyrządzenia jej szkody majątkowej lub osobistej, nie podlega faktycznie penalizacji w ramach czynu z art. 190a § 2 KK. Działanie takie pozostaje więc bezkarne, a to z uwagi na to, iż ustawodawca przy nowelizacji z 25.2.2011 r. nie włączył do Kodeksu karnego przepisu penalizującego także formę stadialną przestępstwa „kradzieży tożsamości" – a więc przygotowania do czynu z art. 190a § 2 KK[30]. Bez wątpienia natomiast już samo gromadzenie danych osobowych określonej osoby fizycznej lub też ściąganie i zapisywanie np. na twardym dysku komputera ewentualnego przyszłego sprawcy wizerunków takiej osoby, w sytuacji gdy czyni on to w celu popełnienia dopiero w przyszłości czynu zabronionego związanego z wyrządzeniem danej osobie przy użyciu tych danych szkody majątkowej lub osobistej, wypełnia dyspozycję art. 16 § 1 KK – a więc przygotowania do realizacji przestępstwa z art. 190a § 2 KK. *De lege ferenda* należałoby się więc zastanowić, czy przy najbliższej nowelizacji Kodeksu karnego nie byłoby pożądanym zabiegiem legislacyjnym także penalizowanie samego przygotowania do czynu z art. 190a § 2 KK.

Nie można przy tym tracić z pola widzenia, że nie zawsze sprawca zbierający dane osobowe określonej osoby lub osób będzie czynił to w celu wyrządzenia jej bezpośrednio szkody majątkowej lub osobistej, pomimo iż jego działania związane z gromadzeniem tych danych będą faktycznie nastawione na uzyskanie korzyści majątkowej. Dane osobowe stanowią bowiem aktualnie często przedmiot obrotu handlowego, a sprawca może je gromadzić w celu np. odsprzedaży określonemu podmiotowi[31].

Zauważyć przy tym należy, że poza faktyczną penalizacją czynu z art. 190a § 2 KK, z uwagi na brak karalności przygotowania do tego przestępstwa, pozostają także te działania sprawcy, które za pośrednictwem określonych metod socjotechnicznych bezpośrednio zmierzają do uzyskania danych osobowych danej osoby, w sytuacji gdy nie realizują one zarazem znamion czynu z art. 267 § 1 KK. Wskazany przepis stanowi bowiem, że odpowiedzialności karnej za przestępstwo z art. 267 § 1 KK podlega ten, 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. Tym samym, jeżeli sprawca uzyska takie dane osobowe pokrzywdzonego, jednakże bez otwierania zamkniętej korespondencji bądź bez podłączenia się w tym celu do sieci telekomunikacyjnej lub też bez przełamania czy też ominięcia elektronicznych, magnetycznych, informatycznych lub innych szczególnych jej zabezpieczeń, nie będzie ponosił w tym zakresie zazwyczaj odpowiedzialności karnej, w szczególności gdy następnie tymi danymi osobowymi nie posłuży się w celu podszywania się pod inną osobę, a zarazem wyrządzenia jej w ten sposób szkody majątkowej lub osobistej.

Poza zainteresowaniem art. 190a § 2 KK pozostaje także posłużenie się przez sprawcę danymi osobowymi lub wizerunkiem osoby zmarłej, co jest związane z brakiem możliwości zidentyfikowania jako osoby fizycznej człowieka po jego śmierci[32]. Jak podkreśla się bowiem w doktrynie, kult i pamięć o osobie zmarłej jest jednym z dóbr osobistych człowieka, które po jego śmierci przysługują rodzinie zmarłego, co daje podstawę w przypadku naruszenia tych dóbr dochodzenia ochrony cywilnoprawnej[33].

Przestępstwo z art. 190a § 2 KK nie może zostać także zrealizowane w sytuacji, gdy sprawca posłuży się fikcyjnymi danymi osobowymi lub fikcyjnym wizerunkiem nieistniejącej osoby. Oczywiście działania takie mogą natomiast nosić znamiona czynu z art. 286 § 1 KK, w sytuacji gdy sprawca

[28] *R. Kaszubski*, *Ł. Obzejta*, Karty płatnicze w Polsce, Warszawa 2012, s. 401.

[29] *E. Całus*, Przestępstwo kradzieży tożsamości w Internecie – uwagi na tle art. 190a § 2 KK, [w:] *M. Gdula* (red.), Ochrona prywatności w nowych technologiach, Wrocław 2015, s. 5.

[30] *A. Lach*, Karnoprawna reakcja..., s. 99.

[31] *M. Siwicki*, Kradzież tożsamości – pojęcie i charakterystyka zjawiska, Część I, Edukacja Prawnicza 2009, Nr 11, s. 36.

[32] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 68.

[33] *Ibidem*, s. 68.

wprowadzi w błąd, posługując się takimi fikcyjnymi danymi osobowymi, inną osobę oraz doprowadzi ją do niekorzystnego rozporządzenia swoim mieniem[34].

W literaturze przedmiotu oraz w literaturze informatycznej opisywane są przy tym liczne metody działań sprawców, zmierzające do uzyskania dostępu do danych osobowych określonych osób fizycznych, w tym także do tzw. danych wrażliwych – pozwalających następnie na dokonywanie określonych przestępstw, w tym z art. 190a § 2 KK czy też z art. 286 § 1 KK – a więc przestępstw oszustwa. Poza oczywistymi i prostymi metodami pozyskiwania cudzych danych osobowych, takimi jak przeglądanie wyrzuconych – bez wcześniejszego ich zniszczenia dokumentów, w tym faktur czy też listów przewozowych, jedną z częściej spotykanych metod wyłudzania danych osobowych jest tzw. *phishing*. Działanie to sprowadza się zazwyczaj do wysyłania wiadomości e-mail na pocztę użytkownika spreparowanych w taki sposób, aby stwarzały one wrażenie, iż pochodzą z określonej instytucji, np. banku lub urzędu (ZUS, Urząd Skarbowy itp.)[35]. Wiadomość ta sugeruje także zazwyczaj wystąpienie określonego problemu technicznego, który wymaga zweryfikowania przez użytkownika na wskazanej stronie internetowej danych osobowych, a także loginów i haseł dostępu. Zazwyczaj także, jak zauważa *E. Całus*, wiadomość taka posiada wpisany w jej treść link, o skorzystanie z którego proszony jest użytkownik w celu przekierowania np. na stronę banku, przy czym w przypadku kliknięcia we wskazany link użytkownik przekierowywany jest na fałszywą stronę internetową – do złudzenia przypominającą stronę określonego banku lub instytucji, gdzie pojawia się miejsce do wpisania danych uwierzytelniających, takich jak login, hasło, PIN, bądź też danych uwierzytelniających transakcję w postaci kodów jednorazowych[36].

Jak słusznie podkreśla się przy tym w doktrynie, opisywane powyżej działanie sprawcy mające postać *phisingu*, a polegające na wysyłaniu e-maili pochodzących rzekomo od innej osoby bądź instytucji (banku, podmiotu świadczącego usługi internetowe), z prośbą o podanie danych osobowych przez odbiorcę, nie będzie karalne[37]. W szczególności bowiem obecnie czynności mające na celu uzyskanie takich danych osobowych w celu wyrządzenia później szkody odbiorcy można potraktować jedynie jako formę niekaralnego przygotowania[38].

Aktualnie inną, a zarazem trudniejszą do wykrycia techniką zmierzającą także do przejęcia danych osobowych, w tym loginów i haseł dostępu, jest tzw. *pharming*, stanowiący pewną modyfikację *phisingu*, który polega na przekierowaniu użytkownika z autentycznej strony WWW określonej instytucji na stronę stworzoną przez przestępców[39].

Pharming jest poprzedzony przy tym zazwyczaj wcześniejszym złamaniem przez sprawcę zabezpieczeń określonego serwera DSN, np. banku, oraz zmianą adresów na tym serwerze, co powoduje, że użytkownik po wejściu na prawdziwą stronę WWW jest następnie przekierowywany na inną podszywającą się pod nią stronę stworzoną przez hackera, gdzie dochodzi do przejęcia wpisywanych danych osobowych, a także np. loginów, haseł, numerów kart kredytowych czy też kodów jednorazowych do operacji bankowych[40]. *Pharming* może także przybierać inną formę – sprawca infekuje najpierw komputer ofiary wirusem komputerowym lub innym złośliwym oprogramowaniem, po czym wskazany wirus lub program przekierowuje pokrzywdzonego ze strony autentycznej np. banku lub sklepu internetowego na fałszywą stronę WWW, która wygląda identycznie jak strona, którą pokrzywdzony zamierzał otworzyć[41].

W praktyce dane osobowe mogą być uzyskiwane przez potencjalnych sprawców przestępstwa z art. 190a § 2 KK, także poprzez stosowanie innych metod socjotechnicznych, w tym poprzez zwykły kontakt telefoniczny – po uzyskaniu numeru telefonu potencjalnego pokrzywdzonego np. z bazy CEIDG, gdzie poprzez fałszywe podanie się np. za operatora sieci telefonicznej w celu przedstawienia fikcyjnej oferty rozmówca przeprowadzi rzekomą weryfikację abonenta i poprosi go o podanie danych osobowych takich jak imię, nazwisko, adres zamieszkania, numer PESEL, imiona rodziców bądź panieńskiego nazwiska matki. Przedmiotowe techniki działania sprawców, związane z telefonicznym wyłudzaniem danych osobowych oraz numerów kart płatniczych, często są określane mianem *phone phisingu* bądź też *vishingu*[42].

Zauważyć przy tym należy, że numer PESEL i panieńskie nazwisko matki, jako dane zwyczajowo ujawniane jedynie w niektórych dokumentach, są często podstawą weryfikacji tożsamości danej osoby w kontakcie z autentycznymi operatorami telefonii, dostawcami Internetu czy też w telefonicznych kontaktach z bankami lub instytucjami finansowymi. W przypadku zatem wejścia w posiadanie takich danych osobowych przez potencjalnego sprawcę istnieje obawa, iż może on, wykorzystując wskazane dane ofiary, przejść następnie pomyślnie telefoniczną weryfikację np. w określonym banku, co do którego posiada informację, iż pokrzywdzony posiada tam rachunek bankowy. Oczywiste jest także, że dane dotyczące rachunku bankowego pokrzywdzonego często bez trudu można uzyskać w sieci Internet, np. poprzez analizę strony WWW związanej z działalnością gospodarczą prowadzoną przez pokrzywdzonego.

[34] *K. Chałubińska-Jentkiewicz*, *M. Karpiuk*, Prawo nowych technologii. Wybrane zagadnienia, Warszawa 2015, s. 382.
[35] *M. Romańczuk-Grącka*, Prawnokarna ochrona…s. 246–247.
[36] *E. Całus*, Przestępstwo kradzieży..., s 5–6.
[37] *A. Lach*, Kradzież tożsamości…, s. 37.
[38] *Ibidem*, s. 37.
[39] *R. Kaszubski*, *Ł. Obzejta*, Karty płatnicze w Polsce…, s. 402–403.
[40] *M. Ziarek* (analityk, Kaspersky Lab Polska), Phising, pharming i sieci zombie – to czego nie wiesz o swoim komputerze, https://www.securelist.pl/threats/5883,phishing_pharming_i_sieci_zombie_to_czego_nie_wiesz_o_swoim_komputerze.html (dostęp z 11.3.2018 r.).
[41] https://www.avast.com/pl-pl/c-pharming (dostęp z 11.3.2018 r.).
[42] *R. Kaszubski*, *Ł. Obzejta*, Karty płatnicze w Polsce…, s. 402.

Kolejnymi metodami socjotechnicznymi opisywanymi przez *E. Całus* jest tzw. oszustwo nagrodowe oraz oszustwo rekrutacyjne[43]. W pierwszym wypadku sprawca informuje potencjalną ofiarę w wiadomości e-mail lub też telefonicznie o określonej wygranej, prosząc zarazem o podanie danych osobowych „niezbędnych do odebrania nagrody", co często wiąże się z ujawnieniem wskazanych danych osobowych przez pokrzywdzonego. W drugim wypadku opisywanym przez cytowaną wyżej autorkę sprawca przesyła do pokrzywdzonego wiadomość e-mail zawierającą informację o fikcyjnej ofercie zatrudnienia. W ramach takiej oferty, jak zauważa autorka, sprawca często zwraca się również o nadesłanie CV oraz skanu dowodu osobistego pokrzywdzonego, przy czym w rzeczywistości rzekoma firma mająca zatrudnić pokrzywdzonego nie istnieje.

Do uzyskania danych osobowych pokrzywdzonego dojść może także poprzez fizyczny kontakt sprawcy z pozostawionymi w biurze ofiary dokumentami, fakturami lub poprzez wgląd do niezabezpieczonego komputera w miejscu pracy – do którego sprawca uzyskuje dostęp z uwagi na zatrudnienie w tym samym miejscu lub z uwagi na wykonywanie tam doraźnych czynności np. serwisanta, pracownika ochrony lub pracownika personelu sprzątającego. Do przejęcia danych osobowych przez potencjalnego sprawcę czynu z art. 190a § 2 KK dojść może także poprzez uzyskanie dostępu do dokumentów poszkodowanego, np. w sytuacji zagubienia przez niego dowodu osobistego.

Zauważyć przy tym należy, że w ramach sieci Internet użytkownicy często przyporządkowują do siebie określone „wirtualne postacie", tworzone na potrzeby np. gier sieciowych (online), gdzie dany użytkownik funkcjonuje jako określona postać graficzna (avatar), z którą często się utożsamia. Gry takie zaliczane są do kategorii gier MMORPG, przy czym użytkownik po uzyskaniu najczęściej darmowego konta na serwerze dostawcy usługi w postaci przedmiotowej gry online – co wymaga zazwyczaj podania podstawowych danych osobowych (imię, nazwisko, data urodzenia, państwo i miasto użytkownika, adres e-mail), uzyskuje login i hasło dostępowe do konta, a zazwyczaj także dodatkowo kod dla odzyskania utraconego konta „Recovery Key". Po uzyskaniu dostępu do konta użytkownik wciela się w określoną postać wirtualną, np. rycerza, trolla, czarnoksiężnika itp., a także jako wskazana postać wirtualna uczestniczy w przedmiotowej grze, do której dostęp posiada faktycznie nieograniczona liczba użytkowników występujących w niej pod postacią innych fikcyjnych, wirtualnych avatarów. Każda postać w miarę czasu trwania gry uzyskuje określone sprawności i atrybuty związane z poziomem gry, na którym się znajduje, a także zdobywa wirtualną walutę, uzyskiwaną za wygrane pojedynki w postaci np. wirtualnych złotych monet lub brylantów. Zarówno za wirtualną walutę uzyskaną w trakcie gry, jak i często za realne płatności dokonywane najczęściej za pośrednictwem karty płatniczej, użytkownik może także nabywać od administratora gry dodatkowe wirtualne przedmioty i artefakty, takie jak np. miecze, topory, tarcze, części zbroi, które w określony sposób wzmacniają jego postać oraz dostarczają jej nowych „mocy". Tym samym po odpowiednio długim okresie uczestniczenia w grze oraz po uzyskaniu lub zakupieniu określonych atrybutów wirtualnej postaci staje się ona faktycznie „niezwyciężona", w tym w szczególności dla nowych użytkowników, dopiero rozpoczynających grę, których wirtualne avatary nie są jeszcze odpowiednio „silne". Przedmiotowa „wirtualna postać" – avatar uzyskuje zatem z biegiem czasu określoną wartość, przekładającą się na wartość pieniężną. Użytkownicy przedmiotowych gier często także odsprzedają następnie określone atrybuty swojego avatara, np. w postaci części uzbrojenia, na aukcjach internetowych innym użytkownikom. W sieci znane jest również zjawisko tzw. *pushingu* sprowadzające się do odsprzedaży przez jednego użytkownika innemu pełnej wirtualnej postaci wraz z kontem, do którego ta postać jest przypisana, bądź też np. przelania określonej ilości wirtualnej waluty na nowo utworzone konto przez użytkownika, co pozwala mu już na wstępie gry nabyć od administratora określoną ilość atrybutów wzmacniających jego avatara. Zauważyć także należy, że zjawisko to jest najczęściej nielegalne, z uwagi na zakaz tego rodzaju działań dokonywanych przez użytkowników, wpisany w treść większości regulaminów administratorów gier gatunku MMORPG.

Zbliżony charakter może mieć również tzw. zjawisko *cheatingu* będącego formą oszustwa w grze typu MMORPG, sprowadzającego się najczęściej do nieuprawnionego (wbrew woli operatora) kopiowania wirtualnych przedmiotów oraz waluty używanej w grze[44].

Także tego typu „wirtualne postacie" stały się od pewnego czasu przedmiotem zainteresowania przestępców, którzy uzyskując różnymi metodami dane do konta innego użytkownika (login, hasło), a często także jego dane osobowe, przejmują kontrolę nad jego kontem i tym samym avatarem. W następstwie tego może dojść bądź do zniszczenia wirtualnej postaci, którą dysponował pokrzywdzony użytkownik, bądź też do przeniesienia jej na inne konto, innego użytkownika lub też odsprzedaży wirtualnej postaci oraz przypisanych do niej atrybutów i wirtualnej waluty zgromadzonych na koncie pokrzywdzonego, za co sprawca uzyskuje wymierne korzyści finansowe od nabywcy. W przypadku przejęcia „wirtualnej postaci" przez sprawcę, który następnie nadal z niej korzysta, dochodzi przy tym faktycznie do pewnej formy „podszycia się" pod poprzedniego użyt-

[43] *E. Całus*, Przestępstwo kradzieży…, s. 5–6.

[44] *K. Gienas*, Prawo autorskie w ramach „wirtualnych światów", CBKE e-BIULETYN 2007, Nr 4, http://www.bibliotekacyfrowa.pl/Content/22502/Prawo_autorskie_w_ramach.pdf (dostęp z 14.3.2018 r.).

kownika, który dotychczas dysponował tą postacią, a więc stanowiła ona jego avatar.

Do przejęcia kont użytkowników gier MMORPG oraz przypisanych do nich wirtualnych postaci dochodzi przy tym najczęściej za pomocą tych samych metod, które wykorzystują sprawcy przestępstwa z art. 190a § 2 KK. Metodą tą może być zatem *phising*, gdzie sprawca w wiadomości e-mail przesłanej do użytkownika podaje się za administratora gry i prosi o weryfikację danych tego użytkownika oraz hasła dostępu i loginu do konta. Sprawca może posłużyć się także dla zdobycia wskazanych danych dostępu do konta użytkownika metodą hackingu, poprzez zainfekowanie komputera użytkownika koniem trojańskim, najczęściej poprzez otworzenie przez takiego użytkownika załącznika w wiadomości e-mail w tym celu do niego przesłanej. Przedmiotowe zagrożenie, związane z infekowaniem koniem trojańskim komputerów użytkowników gier MMORPG w celu wykradania haseł i loginów dostępowych do ich kont, określane jest mianem zagrożenia Win32/PSW.OnLineGames, przy czym po zainstalowaniu przedmiotowego konia trojańskiego na komputerze użytkownika działa on jak typowy keylogger rejestrujący wszystkie znaki, które użytkownik wprowadza podczas logowania się do gry[45].

Opisywane są przy tym przypadki faktycznego przejęcia konta użytkownika gier typu MMORPG w celu uzyskania kontroli nad „wirtualną postacią". W szczególności warto odwołać się do zdarzenia mającego swój finał sądowy, gdy 20-letni mieszkaniec Płocka sprzedał mieszkańcowi Warszawy wirtualną postać rycerza z gry Tibia na aukcji internetowej za kwotę kilkuset złotych, po czym po pewnym czasie postanowił odzyskać swoją wirtualną postać oraz po zdobyciu kodów dostępu ponownie przejął kontrolę nad kontem, do którego przypisany był sprzedany przez niego rycerz, a także usunął go w tym celu z konta nabywcy[46]. Ostatecznie sprawa zakończyła się wyrokiem skazującym, gdzie sprawca dobrowolnie poddał się karze pięciu miesięcy pozbawienia wolności z warunkowym zawieszeniem jej wykonania na okres trzech lat próby i karze grzywny, przy czym sąd zobowiązał go dodatkowo do zwrotu wirtualnej postaci pokrzywdzonemu oraz do zwrotu pieniędzy, które uprzednio nabywca zainwestował w wyposażanie wirtualnego rycerza[47].

Również wyrokiem skazującym wydanym w sierpniu 2010 r. przez SR w Sławnie, 20-letni *Patryk S.* oskarżony o to, że „działając w celu wyrządzenia szkody innej osobie (…), po uzyskaniu za pomocą programu szpiegującego dostępu do konta usunął dane informatyczne w postaci wirtualnych przedmiotów" (którymi były faktycznie miecz, zbroja i tarcza w grze Metin2), został skazany na karę roku pozbawiania wolności z warunkowym zawieszeniem wykonania tej kary na okres próby oraz na karę grzywny[48].

Jak się wydaje, przedmiotowe zachowania sprawcze, związane z opisanym powyżej zjawiskiem kradzieży tzw. wirtualnych postaci, w większości wypadków realizować będą znamiona czynu z art. 286 § 1 KK, a więc przestępstwa oszustwa, z uwagi na doprowadzenie pokrzywdzonego do niekorzystnego rozporządzenia mieniem – w sytuacji gdy sprawca zarazem wprowadzi go w błąd np. co do faktycznego zamiaru nabycia lub odsprzedaży postaci wirtualnej, a w niektórych wypadkach także znamiona czynu z art. 267 § 1 KK, gdy sprawca w celu uzyskania kodów dostępu do konta pokrzywdzonego uzyska bez uprawnienia dostęp do tych danych, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne zabezpieczenia. Brak jest natomiast obecnie możliwości zakwalifikowania przedmiotowych zachowań sprawczych jako przestępstwa z art. 190a § 2 KK, a to z uwagi na okoliczność, iż przepis ten wymaga „podszycia się pod inną osobę", a więc co do zasady pod osobę fizyczną. Oczywiste jest przy tym, że „wirtualna postać", nawet w sytuacji gdy pokrzywdzony z nią się utożsamia, nie posiada atrybutów osoby fizycznej.

Inna sytuacja zachodziłaby natomiast wówczas, gdyby sprawca w celu przejęcia „wirtualnej postaci" uzyskał np. metodą *phisingu* nie tylko dostęp do loginu i hasła pokrzywdzonego, ale także do jego danych osobowych, udostępnionych uprzednio administratorowi gry, a następnie podawałby się za poprzedniego użytkownika, np. w odpowiedzi na zapytanie administratora gry przesłane do niego wiadomością e-mail. Jak się wydaje, w takiej sytuacji mogłoby dojść do wypełnienia normy art. 190a § 2 KK, w szczególności jeżeli równocześnie przyjmiemy, że osoba, która utraciła w ten sposób swojego avatara i pod którą aktualnie sprawca się podszywa, poniosła z tego tytułu wymierną szkodę majątkową.

W tym miejscu należy zauważyć, że ustawowy zakres ujęcia szkody w ramach art. 190a § 2 KK nie chroni w sposób wystarczający wszystkich osób, którym na skutek działania sprawcy podszywającego się pod inną osobę szkoda taka zostaje wyrządzona. Szkodę zarówno w ujęciu majątkowym, rozumianym jako *damnum emergens* oraz *lucrum cessans*, jak i szkodę osobistą, rozumianą jako szkoda na osobie oraz tzw. krzywda, w ramach czynu z art. 190a § 2 KK można bowiem wywołać wyłącznie w odniesieniu do bezpośredniego pokrzywdzonego tym przestępstwem, a więc osoby fizycznej, pod którą w celu wyrządzenia takiej szkody podszył

[45] *M. Maj*, Kradzież tożsamości w grze… i co dalej, Dziennik Internautów. Internauci z 4.6.2008 r., http://di.com.pl/kradziez-tozsamosci-w-grze-i-co-dalej-21124 (dostęp z 12.3.2018 r.).

[46] Zatrzymano sprawcę kradzieży wirtualnego rycerza w grze Tibia, Dziennik Internautów. Biznes i prawo, 29.7.2011 r., http://di.com.pl/zatrzymano-sprawce-kradziezy-wirtualnego-rycerza-w-grze-tibia-39410 (dostęp z 12.3.2018 r.).

[47] *M. Gajewski*, Do więzienia za wirtualną kradzież. W Polsce!, CHIP z 29.7.2011 r., https://www.chip.pl/2011/07/kradziez-postaci-w-grze-mmo-skonczyla-sie-wyrokiem-sadowym/ (dostęp z 12.3.2018 r.).

[48] *D. Szyller*, *M. Fabiański*, Kradzież w krainie demonów, Rzeczpospolita z 25.8.2012 r., http://www.rp.pl/artykul/925892-Kradziez-w-krainie-demonow.html (dostęp z 12.3.2018 r.).

się sprawca. Jak słusznie podkreśla się natomiast w doktrynie, przestępstwo kradzieży tożsamości z art. 190a § 2 KK może naruszać nie tylko dobra osoby, której dane osobowe są faktycznie przywłaszczone, ale także może naruszać dobra prawne innych osób[49]. W przypadku bowiem podszycia się pod określoną osobę szkoda – w szczególności o charakterze osobistym – może zaistnieć także w dobrach innej osoby. Jako przykład można przedstawić fikcyjną sytuację, gdy sprawca, wykorzystując wizerunek członka danej rodziny, np. ojca, i podszywając się pod ten wizerunek w celu zamieszczenia na portalu społecznościowym wpisu mającego stworzyć wrażenie, iż osoba ta posiada określone, pejoratywne cechy (np. sprzedaje narkotyki), doprowadza do napiętnowania społecznego także pozostałych członków tej rodziny, a nawet czasowego ich wykluczenia społecznego. Bez wątpienia szkoda osobista w opisanej sytuacji, związana z działaniem sprawcy nakierowanym na jedną osobę, może zaistnieć także w odniesieniu do innych osób, pod które faktycznie sprawca się nie podszywał.

Podkreślić także należy, że zgodnie z treścią art. 49 § 1 KPK za pokrzywdzonego uważa się osobę fizyczną lub prawną, której dobro prawne zostało bezpośrednio naruszone lub zagrożone przez przestępstwo. Tym samym już z samej definicji pokrzywdzonego – będącego osobą fizyczną wynika, że także w przypadku innej osoby niż ta, pod którą sprawca bezpośrednio się podszył (w celu wyrządzenia jej szkody majątkowej lub osobistej), jeżeli dochodzi do faktycznego naruszenia lub zagrożenia jej dóbr prawnych wyrządzeniem szkody majątkowej lub osobistej, powinna być ona włączona do kręgu osób pokrzywdzonych czynem z art. 190a § 2 KK. Z uwagi na użycie jednak w dyspozycji art. 190a § 2 KK jednoznacznego sformułowania „kto podszywając się pod inną osobę wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej", brak jest możliwości bez stosownej zmiany legislacyjnej zastosowania wykładni rozszerzającej w tym zakresie – zwłaszcza w kontekście bezpośrednio wynikającego z zasady *nullum crimen sine lege* (art. 1 § 1 KK) postulatu *nullum crimen sine lege stricta*, a więc zakazu stosowania niekorzystnej dla sprawcy analogii oraz wykładni rozszerzającej.

Podsumowanie

Jak się wydaje, poprzez użycie w dyspozycji przedmiotowego art. 190a § 2 KK sformułowania „kto podszywając się pod inną osobę wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej lub też innej osobie szkody majątkowej lub osobistej" doszłoby do pożądanego z punktu widzenia następstw przedmiotowego przestępstwa rozszerzenia odpowiedzialności sprawcy czynu z art. 190 a § 2 KK, także za ewentualną szkodę (majątkową lub osobistą) wyrządzoną innej osobie niż jedynie ta, pod którą sprawca bezpośrednio się podszył. Co oczywiste, postulat ten ma charakter wyłącznie propozycji *de lege ferenda*.

Tym samym uznać należy, że aktualny brak kryminalizacji przygotowania do przestępstwa z art. 190 a § 2 KK, uznającego w szczególności za takie przygotowanie pozyskiwanie bądź też gromadzenie danych osobowych lub wizerunków danej osoby, w celu wykorzystania ich następnie do podszycia się pod określoną osobę i wyrządzenia jej przez to szkody majątkowej lub osobistej, jak też brak możliwości uznania za pokrzywdzoną czynem z art. 190a § 2 KK także innej osoby niż ta, pod którą sprawca faktycznie się podszywa, stanowią istotne mankamenty przedmiotowej regulacji.

Bez wątpienia wprowadzenie postulowanych w treści niniejszego opracowania zmian legislacyjnych przyczyniłoby się do skuteczniejszego zwalczania przestępstw kradzieży tożsamości, i to już w ich stadium początkowym, gdzie sprawca faktycznie czyni przygotowania do popełnienia przedmiotowego przestępstwa, a także do zwiększenia bezpieczeństwa ofiar tego przestępstwa, rozumianych w szerokim, a nie jak dotychczas jedynie wąskim zakresie.

Oczywiście nie można tracić z pola widzenia także konieczności podejmowania działań w zakresie kryminologicznym, w szczególności poprzez stałe zwiększanie świadomości potencjalnych ofiar przestępstw z art. 190a § 2 KK odnośnie do występujących w ramach sieci Internet zagrożeń będących następstwem bezkrytycznego często udostępniania swoich danych osobowych i wizerunku graficznego np. na portalach społecznościowych. Konieczne wydają się w tym zakresie działania podejmowane na szczeblu rządowym – w szczególności przez Ministerstwo Sprawiedliwości, a sprowadzające się do określonych kampanii medialnych w tym telewizyjnych i prasowych, a także poprzez stosowne publikatory internetowe, które mogą zwiększyć poziom ostrożności i wyczulenia społecznego na tego rodzaju bezprawne działania podejmowane przez przestępców.

Przedmiotowe działania, a tym samym zwiększenie świadomości społecznej w zakresie skutków, które niesie za sobą ewentualne przejęcie tożsamości danej osoby przez przestępcę przyczynić mogą się także do większej wykrywalności przestępstw kradzieży tożsamości, które często obecnie pozostają w sferze tzw. ciemnej liczby przestępstw. W szczególności bowiem, jak zauważa się w doktrynie, często sami pokrzywdzeni przedmiotowymi przestępstwami nie podejmują działań w zakresie zawiadomienia o nich organów ścigania pomimo często dotkliwych szkód z nimi związanych, a to z uwagi na świadomość tych pokrzywdzonych, że do pozyskania ich danych osobowych bądź wizerunku doszło w wyniku ich własnych zaniedbań, w tym niewłaściwego zabezpieczenia danych i dokumentów[50].

[49] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 73.
[50] *M. Siwicki*, Kradzież tożsamości – pojęcie i charakterystyka…, s. 32.

Podkreślić należy przy tym, że w literaturze przedmiotu od dawna postulowane są określone działania profilaktyczne, które powinny być objęte w szerokim zakresie także informacjami w ramach kampanii społecznych. W szczególności warto w tym miejscu przytoczyć postulat *M. Kowalczyk-Ludzia* oraz *K. Pruszkiewicz-Słowińskiej* wskazujący na konieczność niszczenia dokumentów zawierających dane identyfikujące przed wyrzuceniem ich do śmieci, przechowywanie ważnych dokumentów w zamkniętych pomieszczeniach, przechowywanie poufnych informacji w plikach i katalogach chronionych hasłami, wzmożonej czujności w zakresie rozpoznawania fałszywych wiadomości e-mail bądź też stron WWW, a także poprzez przeprowadzanie finansowych transakcji online wyłącznie na bezpiecznych stronach[51].

Metody zabezpieczenia się przed określonymi formami działań podejmowanych przez sprawców w sieci Internet, a zmierzających do przejęcia danych osobowych, sprowadzają się przy tym często do tzw. zwykłej przezorności i rozwagi oraz znajomości podstawowych zasad działania określonych instytucji, w tym zwłaszcza banków. W szczególności bowiem banki nigdy nie wysyłają do swoich klientów pytań dotyczących haseł, loginów lub innych danych, a także nie podają w swoich wiadomościach linków do stron transakcyjnych[52].

Tym samym podstawowa zasada ograniczonego zaufania w sieci Internet, sprowadzająca się między innymi do nieotwierania e-maili nieznanego pochodzenia oraz unikania nieznanych stron WWW, na których może występować złośliwe oprogramowanie, może uchronić nas przed możliwością przejęcia naszych danych osobowych bądź innych danych wrażliwych przez przestępców. Zasada ograniczonego zaufania w sieci Internet ma swoje odzwierciedlenie także w potrzebie powstrzymania się przed zamieszczaniem danych osobowych, zdjęć oraz wszelkich innych informacji pozwalających na kradzież naszej tożsamości, na portalach społecznościowych bądź też udostępniania tych danych niesprawdzonym dostawcom usług internetowych.

Wskazane działania profilaktyczne, niezależnie od ochrony prawnokarnej, jaką stwarza art. 190a § 2 KK, mogą skutecznie uchronić nas przed możliwością stania się ofiarą przedmiotowych działań przestępczych.

[51] *M. Kowalczyk-Ludzia*, *K. Pruszkiewicz-Słowińska*, Wybrane zagadnienia dotyczące kradzieży tożsamości na gruncie przepisów prawa karnego i prawa medycznego – studium przypadku, Przegląd Policyjny 2016, Nr 2, s. 87.

[52] *R. Kaszubski*, *Ł. Obzejta*, Karty płatnicze w Polsce…, s. 406.

Słowa kluczowe: kradzież tożsamości, wizerunek, dane osobowe, wirtualna postać, sieć Internet, podszywanie się pod inną osobę

Scope of effective law regulations of art. 190a § 2 of the Penal Code on combating actions concerning the so-called Internet-related identity thief

The subject of the analysis in this paper is the art. 190a § 2 of the Penal Code. Based on this, an attempt has been made to give the answer about effectiveness of regulation against online identity fraud and subsequent criminal acts. The author also takes notice of exemplary methods used by criminals trying to capture or bilk personal data and potential threats of sharing personal information or effigy by Internet users, especially on social networking websites. Moreover this work provides analysis of the new phenomenon which is "online identity impersonation" taking place within games known as MMORPG. Finally, this article points the importance of postulated changes to legislation concerning regulations from the art. 190a § 2 of the Penal Code, which could gain pursuing effectiveness of "identity thief" perpetrators.

Keywords: identity thief, effigy, personal data, online identity, Internet, impersonation.