

Anna Urbanek*

Ochrona przed piractwem internetowym w prawie Unii Europejskiej i Anticybersquatting Consumer Protection Act

Spis treści

- I. Wprowadzenie
- II. Piractwo internetowe – *cybersquatting* i *typosquatting*
- III. Funkcje i budowa domen internetowych
- IV. Ochrona przed naruszeniami w UE i USA
 1. Prawo amerykańskie
 - 1.1. Anticybersquatting Consumer Protection Act
 - 1.2. Postępowania w związku z naruszeniem ACPA
 2. Prawo Unii Europejskiej
 - 2.1. Wdrażanie i funkcjonowanie Domeny Najwyższego Poziomu „.eu”
 - 2.2. Postępowania w związku z naruszaniem przepisów o domenie „.eu”
- V. Wnioski

Streszczenie

Celem artykułu jest przeanalizowanie form i zakresu piractwa internetowego w związku z przyjęciem rozporządzenia w sprawie wdrażania i funkcjonowania Domeny Najwyższego Poziomu .eu oraz porównanie rozwiązań prawnych amerykańskiej Anticybersquatting Consumer Protection Act (ACPA). Mechanizmy ochrony prawnej stosowane w porządkach prawnych Unii Europejskiej i Stanów Zjednoczonych różnią się od siebie, co może nastroczać problemów w przypadku naruszeń na skalę ogólnoswiatową. Warto rozważyć uzupełnienie prawa UE o pewne rozwiązania przyjęte w ACPA.

Słowa kluczowe: *cybersquatting*; *typosquatting*; piractwo internetowe; prawa przedsiębiorcy; znaki towarowe.

JEL: K2, K3, K4

* Doktorantka w Katedrze Europejskiego Prawa Gospodarczego WPiA UŁ, zatrudniona na stanowisku doktorant-stypendysta w projekcie „Ochrona konsumenta a sztuczna inteligencja. Między prawem a etyką” finansowanym przez Narodowe Centrum Nauki, nr projektu 2018/31/B/HS5/01169; e-mail: anna.urbanek@wpia.uni.lodz.pl; <https://orcid.org/0000-0003-0042-4172>.

I. Wprowadzenie

Współcześnie Internet jest jednym z najważniejszych, o ile nie centralnym, medium działań przedsiębiorcy pozwalającym na komunikację z klientami i kontrahentami. Dlatego ważne jest zagwarantowanie przedsiębiorcom bezpieczeństwa online, uniemożliwiając podszywanie się przez osoby trzecie. Taka przejrzystość i wiarygodność treści internetowych korzystnie wpływa również na pozycję konsumentów, niezależnie od tego, który etap podejmowania decyzji transakcyjnej ma miejsce online, ponieważ mają możliwość bardziej świadomego wyboru towaru lub usługi. Z powodu korzyści, jakie wynikają dla przedsiębiorców z posiadania odpowiedniej domeny, stają się one celem ataków. Zagrożeniem dla rzetelności zawartości stron internetowych jest piractwo w sieci przejawiające się różnego rodzaju naruszeniem praw przedsiębiorców i wprowadzaniem konsumentów w błąd, co do tożsamości właściciela domeny internetowej.

Przyjęte w 2019 roku rozporządzenie w sprawie wdrażania i funkcjonowania Domeny Najwyższego Poziomu .eu ma na celu m.in. zapewnienie skuteczniejszej ochrony przed naruszeniem praw przedsiębiorców online przez wzmocnioną kontrolę rejestrowania domen internetowych. Oceniając trafność wprowadzonych zmian, warto sięgnąć do amerykańskiego systemu prawnego, ponieważ skala problemu piractwa internetowego w Stanach Zjednoczonych odpowiada zakresowi cyberprzestępczości na rynku internetowym Unii Europejskiej. Niniejszy artykuł przedstawia zjawisko *cybersquattingu* i *typosquattingu*, czyli form piractwa internetowego, przez przegląd postępowań prowadzonych w związku z nimi w Unii Europejskiej i Stanach Zjednoczonych.

II. Piractwo internetowe – *cybersquatting* i *typosquatting*

Cybersquatting polega na rejestrowaniu nazwy domeny internetowej wcześniej niż podmiot, dla którego taka domena rzeczywiście miałaby znaczenie gospodarcze. Właściciel domeny kontaktuje się następnie z przedsiębiorcą, który czerpałby korzyści gospodarcze z jej posiadania i proponuje sprzedaż domeny (Curtin, 2010, s. 353–394). Spotyka się również praktyki korzystania z różnych wersji tej samej domeny, np. zmieniając domenę drugiego i trzeciego stopnia – „.net”, „.org” itd. (Tworkowska-Baraniuk, 2016, s. 178–187).

Podobnym naruszeniem jest *typosquatting* polegający na nazywaniu domeny w bardzo podobny sposób do innej, już istniejącej. *Typosquatterzy* korzystają z literówek popełnianych przez użytkowników wyszukiwarek internetowych. Wystarczy zamienić kolejność dwóch liter w nazwie, aby zostać przekierowanym do niewłaściwej strony internetowej. Jeśli obie strony zawierają zbliżone treści, np. prezentują towary i usługi przedsiębiorców prowadzących podobną działalność gospodarczą, konsument może zostać wprowadzony w błąd. W literaturze *typosquatting* traktowany jest niekiedy jako kategoria *cybersquattingu* (Ross, 2000, s. 641).

Często, zanim naruszenie zostanie wykryte, *cybersquatter* dokonuje czynności prawnych na rzecz osób trzecich. W styczniu 2020 r. Sąd Najwyższy w Singapurze (High Court of the Republic of Singapore) wydał wyrok w sprawie z powództwa *3 Corporate Services Pte Ltd* (3 Corporate). Powód zawarł umowę sprzedaży domeny internetowej „grab.co.id” z *Grabtaxi Holdings Pte Ltd* (Grabtaxi). Pozwana spółka zobowiązała się do zapłaty 250 000 dolarów, jednak ostatecznie nie dokonała płatności. 3 Corporate zarzuciło Grabtaxi niewykonanie postanowień umowy. Pozwana twierdziła, że umowa nie ma charakteru wiążącego, ponieważ to nie 3 Corporate jest właścicielem

nazwy domeny, a akcjonariusz tej spółki. Ponadto Grabtaxi podniosło, że powód działa w sprzeczności z porządkiem publicznym, ponieważ on lub jego akcjonariusze są właścicielami takich domen jak „amyswinehouse.com.sg” i „google.com.sg”, które nie mają związku z działalnością prowadzoną przez 3 Corporate. Sąd oddalił powództwo, stwierdzając, że strony nie były związane wiążącą umową, ponieważ powód nie jest właścicielem domeny „grab.co.id”. Jednocześnie Sąd wskazał, że działania 3 Corporate spełniają przesłanki *cybersquattingu*, a celowa błędna pisownia w nazwach domen „amyswinehouse.com.sg” i „google.com.sg” wykazuje cechy *typosquattingu*¹.

III. Funkcje i budowa domen internetowych

Początki Internetu sięgają lat 60. XX wieku. Wówczas występował pod nazwą Wide Area Networks (WAN), co można tłumaczyć jako sieci szerokoprzestrzenne (Pope, Warkentin, Mutchler i Luo, 2012, s. 329–346). Przesyłanie danych między komputerami zapewniają protokoły komunikacji internetowej TCP/IP (*Transmission Control Protocol/Internet Protocol*) odpowiedzialne odpowiednio za zbieranie pakietów danych i wysyłanie ich do właściwego miejsca docelowego². Adresy internetowe pozwalające komputerom podłączyć się do sieci są niepowtarzalne. Tworzą je indywidualne numery IP składające się z ciągu liczb z zakresu od 0 do 255 oddzielonych kropkami, które identyfikują najpierw sieć krajową, następnie miejską, lokalną i finalnie konkretny komputer (Banach, 2006, s. 71–75). W ten sposób możliwe jest precyzyjne przesyłanie danych.

W latach 80. długie ciągi cyfr zostały zastąpione systemem nazw domenowych (*Domain Name System*), co znacznie usprawniło korzystanie z Internetu i ułatwiło pozycjonowanie (Pope, Warkentin, Mutchler i Luo, 2012, s. 329–346). Budowa domeny internetowej nie jest przypadkowa. Składa się z kilku części oddzielonych kropkami, które liczy się od prawej strony. W pierwszej kolejności zwraca się więc uwagę na domenę pierwszego stopnia (*Top Level Domain*, TLD). Może to być m.in.: domena krajowa (*Country Code Top Level Domain*, ccTLD) – „.pl” – oraz domena funkcjonalna (*Generic Top Level Domain*, gTLD) – „.org”. TLD można przyporządkować wiele domen drugiego stopnia (*Second Level Domain*, SLD) (Waty, van Hoolan, Hengchen, Coeckelbergs i De Wilde, 2016, s. 4), np. *ikar.wz.uw.edu.pl*, gdzie domena funkcjonalna drugiego stopnia „.edu” oznacza, że strona internetowa jest związana z edukacją. Początkowo domeny pierwszego stopnia miały siedem rozszerzeń: „.com”, „.edu”, „.gov”, „.int”, „.mil”, „.net” oraz „.org”. Wraz ze wzrostem dostępu do Internetu, liczba domen rosła, aż pojawiła się konieczność rozszerzenia katalogu TLD i SLD. Wśród nowych dostępnych adresów internetowych można wymienić: „.biz”, „.info”, „.name”, „.coop”, „.museum” i „.travel” (Waty, van Hoolan, Hengchen, Coeckelbergs i De Wilde, 2016, s. 4).

Za rejestrowanie domen odpowiedzialne są wyodrębnione instytucje. W Polsce Naukowa i Akademicka Sieć Komputerowa (NASK) prowadzi rejestr domeny krajowej „.pl” oraz domen regionalnych i funkcjonalnych. Według danych z Krajowego Rejestru Domen obecnie zarejestrowanych jest około 2,5 mln domen z sufiksem „.pl”³.

¹ Wyr. SN Republiki Singapuru z 22.01.2020 r. w sprawie *SGHC 2017, 3 Corporate Services Pte Ltd v. Grabtaxi Holdings Pte Ltd*; zob. [https://www.supremecourt.gov.sg/docs/default-source/module-document/judgement/-2020-sghc-17-\(22-1-2020\)-pdf.pdf](https://www.supremecourt.gov.sg/docs/default-source/module-document/judgement/-2020-sghc-17-(22-1-2020)-pdf.pdf).

² <https://www.britannica.com/technology/TCP-IP>.

³ <https://www.dns.pl/>.

IV. Ochrona przed naruszeniami w UE i USA

Konsumenci często zakładają, że znaki towarowe przedsiębiorstw, np. „Disney”, są adresami internetowymi właścicieli znaków towarowych. Niestety wielu przedsiębiorców nie może z tego skorzystać lub może jedynie w sposób ograniczony z powodu piractwa internetowego. Stosowanie *cybersquattingu* i *typosquattingu* można zauważyć na rynkach zarówno UE, jak i ogólnosiwiatowym.

1. Prawo amerykańskie

1.1. Anticybersquatting Consumer Protection Act

Przed wejściem w życie *The Anticybersquatting Consumer Protection Act* (ACPA)⁴ w 1999 r. w sprawach o stosowanie *cybersquattingu* stosowano zasadę pierwszeństwa. Mimo zarejestrowania określonej domeny przez *cybersquattera*, sądy orzekały na korzyść wcześniej uprawnionych do rejestracji znaków towarowych i przyznawały im prawo do rejestracji identycznej lub podobnej nazwy jako domeny internetowej. Jednocześnie, w związku z tą praktyką, obawiano się, co w sytuacji, gdy ktoś dokona jako pierwszy rejestracji domeny, która przypadkowo jest taka sama lub zbliżona do cudzego znaku towarowego (Fisher, 2001, s. 12–25). Remedium na powyższe problemy miało być uchwalenie ACPA, zgodnie z którą, niedozwolone jest czerpanie w złej wierze korzyści ze znaku towarowego, w tym poprzez rejestrowanie, obrót lub korzystanie z nazwy domeny będącej identyczną lub myląco podobną do znaku towarowego. Znak towarowy nie musi przy tym być powszechnie znany, a jedynie mieć charakter odróżniający.

Udowodnienie działania w złej wierze nastęrcza niekiedy problemów, zwłaszcza gdy potencjalny *cybersquatter* nie złożył przedsiębiorcy propozycji odkupienia domeny podobnej lub identycznej z jego znakiem towarowym. ACPA zawiera otwarty katalog czynników, które powinny być brane pod uwagę w rozstrzyganiu występowania złej wiary, m.in.: ewentualne wcześniejsze używanie przez pozwanego nazwy domeny w dobrej wierze; oferty sprzedaży, cesji, przeniesienia nazwy domeny na rzecz właściciela znaku lub osoby trzeciej; rejestracji lub posiadania innych domen podobnych lub identycznych ze znakami towarowymi, do których prawo mają inne podmioty; podawanie wprowadzających w błąd, fałszywych informacji kontaktowych⁵. Co znamienne, przedsiębiorca obligatoryjnie dokonuje oceny prawdopodobieństwa wprowadzenia konsumentów w błąd, niezależnie od żądania pozwu, nawet jeśli zarzuca jedynie osłabianie znaku towarowego. Ten wymóg znacznie osłabia pozycję przedsiębiorcy, ponieważ przy braku prawdopodobieństwa wprowadzenia w błąd, sąd może stwierdzić, że rejestrujący nie działał w złej wierze (Martin, 2000, s. 595–610).

Cyberprzestępczość utrudnia niekiedy ustalenie jurysdykcji sądu. Przed uchwaleniem ACPA często zdarzało się, że rejestrujący nazwy domen podawali nieprawdziwe informacje dotyczące ich tożsamości i lokalizacji w celu ukrycia przed przyszłymi pozwami o naruszenie cudzego znaku towarowego (Fisher, 2001, s. 12–25). W związku z tym w treści ustawy przewidziano wytoczenie powództwa *in rem* przeciwko nazwie domeny według właściwości miejscowej sądu, w którego

⁴ Anticybersquatting Consumer Protection Act, Pub. L. No. 106–113, sekcja 3002(a)(d)(1)(A), 113 Stat. 1501–545 et seq. (1999).

⁵ ACPA sekcja (a)(d)(1)(B)(i).

okręgu znajduje się siedziba organu odpowiedzialnego za rejestrację tej domeny⁶. Warunkiem skutecznego wniesienia pozwu jest wykazanie należytej staranności podczas próby zlokalizowania właściciela domeny (Sadasivan, 2003, s. 237–257). Poza powództwem *in personam* i powództwem *in rem* w myśl przepisów ACPA, przedsiębiorcy przysługują także wszelkie inne sposoby dochodzenia roszczeń cywilnoprawnych.

ACPA przewiduje szereg środków zaradczych w sytuacji stwierdzenia wystąpienia naruszenia w złej wierze w postaci przepadku, anulowania nazwy domeny lub przeniesienia praw na właściciela znaku towarowego⁷. Ustawa zapewnia dodatkową ochronę przedsiębiorcom, ponieważ w przeciwieństwie do innych przepisów chroniących właścicieli znaków towarowych nie wymaga faktycznego używania w obrocie gospodarczym. Jednocześnie ustawa ogranicza odpowiedzialność z tytułu naruszenia prawa do znaku towarowego przez rejestrację domeny. Osoby, które nie są podmiotami rejestrującymi nazwę domeny lub nie posiadają na nią licencji, nie odpowiadają za naruszanie prawa do znaku towarowego⁸. Organy prowadzące rejestry nie ponoszą odpowiedzialności za szkody poniesione w związku z utrzymaniem nazwy domeny w toku postępowania sądowego, ale tylko w przypadku działania w dobrej wierze. Z kolei osoby umyślnie wprowadzający w błąd twierdzeniem, że nazwa domeny narusza lub rozwadnia cudzy znak towarowy, ponoszą odpowiedzialność wobec rejestrującego (Fisher, 2001, s. 12–25).

1.2. Postępowania w związku z naruszeniem ACPA

W sprawie Microsoft v. Fisher pozwanemu zarzucono naruszenie prawa do znaku towarowego Microsoft przez zarejestrowanie domeny „misrosoft.com” (Ross, 2000, s. 641).

Kolejna sprawa związana z Microsoft Corporation dotyczy Kanadyjczyka, Mike’a Rowe (Tworkowska-Baraniuk, 2016, s. 178–187), który w 2003 r. zarejestrował domenę MikeRowSoft.com, reklamującą jego usługi tworzenia stron www. Microsoft zarzucił właścicielowi domeny naruszenie praw patentowych z uwagi na fonetyczne podobieństwo w nazwie strony internetowej. Mimo że Mike Rowe użył w nazwie domeny swojego imienia i nazwiska, a na podobieństwo z Microsoft Corporation można było zwrócić uwagę dopiero na poziomie dźwiękowym, sprawa zakończyła się zawarciem ugody i przejęciem domeny⁹.

Niekiedy zagrożone zostaje dobre imię przedsiębiorcy z powodu zarejestrowania domeny przez *cybersquattera*. W przypadku Habsco Inc., produkującej gry planszowe dla dzieci i używającej znaku towarowego „CANDY LAND”, doszło do osłabienia renomy znaku towarowego. Pozwany zarejestrował domenę „candyland.com” zawierającą treści erotyczne. W efekcie konsumenci zostali wprowadzeni w błąd, co do zawartości strony internetowej „candyland”. Biorąc pod uwagę, że powód produkuje towary przeznaczone dla dzieci, skojarzenie z branżą erotyczną mogło poważnie zaszkodzić funkcjonowaniu jego przedsiębiorstwa. Sąd w Waszyngtonie (United States District Court, W.D. Washington) nakazał natychmiastowe usunięcie treści zawartych na spornej stronie internetowej i zaprzestanie używania znaku „CANDY LAND”¹⁰.

⁶ ACPA, sekcja 3002(a)(2)(C).

⁷ ACPA sekcja (d)(1)(C).

⁸ ACPA sekcja (d)(1)(D).

⁹ https://www.eporady24.pl/orzecznictwo_sadowe_i_ugody_w_sprawach_nazw_domen_internetowych,artykuly,17,106,697.html.

¹⁰ Wyr. SO Stanów Zjednoczonych dla Waszyngton DC z 9.02.1996 r. w sprawie C96–130WD, *Hasbro, Inc. v. Internet Entertainment Group, Ltd.*

2. Prawo Unii Europejskiej

2.1. Wdrażanie i funkcjonowanie Domeny Najwyższego Poziomu „.eu”

Na podstawie rozporządzenia Komisji nr 874/2004 dostęp do rejestracji domeny „.eu” był podzielony na 3 fazy. W każdej kolejnej rozszerzany był krąg podmiotów uprawnionych do rejestracji w domenę „.eu”. Trzecia faza zapoczątkowała otwartą rejestrację domen dla wszystkich, zgodnie z zasadą „kto pierwszy, ten lepszy”. Wciągu pierwszych czterech godzin od umożliwienia rejestracji zanotowano 702 684 zgłoszenia (Banach, 2006, s. 71–75).

W ostatnim kwartale 2019 r. w EURid (European Registry for Internet Domains) zarejestrowano 161 690 domen „.eu”. Całkowita liczba rejestracji spadła z 3 617 536 w trzecim kwartale do 3 606 311 na koniec czwartego kwartału. Jak wskazało EURid tendencja spadkowa spowodowana jest niepewnością związaną z wystąpieniem Wielkiej Brytanii z Unii Europejskiej¹¹. Na początku lutego EURid poinformowało, że w okresie przejściowym – co najmniej do 31 grudnia 2020 – obywatele Wielkiej Brytanii i osoby tam zamieszkałe nadal będą mogli przechowywać i rejestrować nazwę domeny „.eu” zgodnie ze specjalnym planem, który będzie obowiązywał od końca okresu przejściowego¹².

Domena pierwszego stopnia „.eu” została wprowadzona rozporządzeniem 733/2002¹³, które określało zasady funkcjonowania rejestru TLD.eu. Z kolei rozporządzenie Komisji nr 874/2004 określa reguły porządku publicznego dotyczące wprowadzenia w życie i funkcji TLD.eu oraz zasady regulujące rejestrację domeny. Od wejścia w życie obu aktów stopniowo wzrasta liczba domen rejestrowanych z sufiksem „.eu”. W 2017 r. Komisja Europejska rozpoczęła przeprowadzanie konsultacji publicznych w celu zbadania czy ochrona gwarantowana unijnej TLD nadal jest skuteczna. Po przeprowadzeniu oceny, w 2019 r. Parlament Europejski i Rada przyjęły rozporządzenie 2019/517 w sprawie wdrażania i funkcjonowania domeny „.eu”¹⁴.

Zgodnie z art. 3 rozporządzenia 2019/517 wniosek o rejestrację jednej lub kilku nazw domen w ramach TLD.eu może złożyć: obywatel Unii, niezależnie od miejsca jego zamieszkania; osoba fizyczna, która nie jest obywatelem Unii, zamieszkała w państwie członkowskim; przedsiębiorstwo, które ma siedzibę w Unii; organizacja, która ma siedzibę w Unii, bez uszczerbku dla stosowania prawa krajowego. Ponadto, zgodnie z rozporządzeniem 2019/517 nazwa domeny, która jest identyczna z oznaczeniem lub łudząco podobna do oznaczenia, do którego na mocy prawa Unii lub prawa krajowego zostało ustanowione prawo i która została zarejestrowana bez tytułu prawnego do tego oznaczenia lub bez uzasadnionego interesu w odniesieniu do tego oznaczenia, powinna, co do zasady, zostać wycofana, a w razie konieczności przekazana prawowitemu posiadaczowi¹⁵. Nazwę domeny należy wycofać w każdym przypadku, w którym stwierdzono, że została zarejestrowana lub jest używana w złej wierze¹⁶. Ponadto, zgodnie z rozporządzeniem Komisja powołuje Grupę Doradczą Zainteresowanych Stron ds. Domeny .eu, która będzie dawać

¹¹ <https://eurid.eu/en/news/q4-2019-report/>; Sprawozdanie Komisji dla Parlament Europejskiego i Rady na temat wdrożenia, działania i skuteczności domeny najwyższego poziomu .eu od kwietnia 2017 do kwietnia 2019, COM(2020) 63 final.

¹² <https://eurid.eu/en/register-a-eu-domain/brexit-notice/>.

¹³ Rozporządzenie (WE) nr 733/2002 Parlamentu Europejskiego i Rady z 22.04.2002 r. w sprawie wprowadzania w życie Domeny Najwyższego Poziomu.eu (Dz.Urz. UE L 113 z 30.04.2002 r., s. 1–5).

¹⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/517 z 19.03.2019 r. w sprawie wdrażania i funkcjonowania Domeny Najwyższego Poziomu .eu, zmiany i uchylenia rozporządzenia (WE) nr 733/2002 oraz uchylenia rozporządzenia Komisji (WE) nr 874/2004 (Dz.Urz. UE L 91 z 29.03.2019, s. 25–35).

¹⁵ Motyw 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/517.

¹⁶ Art. 4 ust. 4 lit. b) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/517.

wskazówki w kwestiach wykonania rozporządzenia, zarządzania TLD.eu, monitorowania EURid oraz dobrych praktyk w odniesieniu do przeciwdziałania z wszelkimi formami nadużyć podczas rejestracji domeny „.eu”¹⁷.

Rozporządzenie 2019/517 wejdzie w życie w październiku 2022 r. Jego zakres może budzić obawy, ponieważ nie zostały w nim zawarte znaczące zmiany w stosunku do uchylanych rozporządzeń 733/2002 oraz 874/2004.

2.2. Postępowania w związku z naruszeniem przepisów o domenie „.eu”

W 2006 roku miasto Zakopane wystąpiło do EURid o zarejestrowanie domeny „zakopane.eu”. Jednak nazwa została już wykorzystana przez holenderskie przedsiębiorstwo Depmarc posiadające nazwę handlową Z&A&K&O&P&A&N&E. Urząd Miasta wniósł skargę od decyzji EURid do Centrum ADR dla domeny „.eu” przy Czeskim Sądzie Arbitrażowym, zarzucając naruszenie art. 10 w związku z art. 11 rozporządzenia Komisji nr 874/2004¹⁸. Sąd stwierdził, że nie znajduje żadnych powodów, innych niż *cybersquatting*, dla których holenderskie przedsiębiorstwo miałyby zarejestrować domenę. Dokumenty przedstawione przez pozwanego nie wykazały publicznego stosowania przez niego nazwy handlowej Z&A&K&O&P&A&N&E, mimo rejestracji w publicznym rejestrze. Ponadto Depmarc zarejestrował w ten sposób 23 nazwy handlowe składające się z nazw znanych miast lub przedsiębiorstw. Na podstawie zgromadzonych dowodów sąd unieważnił decyzję EURid¹⁹. Choć w tej sprawie nie doszło do złożenia oferty odkupienia domeny, to jednak w działania Depmarc można uznać za świadome zarejestrowanie domeny „zakopane.eu” w złej wierze.

Pod koniec 2019 r. Sąd Polubowny wydał decyzję w sprawie domeny „roccobarocco.eu” na podstawie skargi wniesionej przez włoskiego projektanta Rocco Barocco. Skarżący zarzucił, że sporna domena jest myląco podobna do jego własnej – „roccobarocco.it”, a osoba, która ją zarejestrowała nie miała żadnych podstaw do wybrania takiej nazwy. W treści decyzji sąd wskazał, że „roccobarocco.eu” w pełni zawiera znak towarowy ROCCOBAROCCO i poza domeną pierwszego stopnia „.eu” nazwy są identyczne. Przy porównywaniu spornych domen TLD musi zostać pominięte, ponieważ jest wymogiem technicznym, obligatoryjnym. Ponadto sąd zgodził się ze skarżącym, przyznając, że pozwany nie miał interesu w tym, aby wybrać nazwę „roccobarocco”, która jest fantazyjna, składa się z imienia i nazwiska projektanta, powszechnie znanego od ponad 50 lat. Tym samym jest wysokie prawdopodobieństwo wprowadzenia w błąd potencjalnych klientów i kontrahentów marki. Zgodnie z art. 21 ust. 1 rozporządzenia Komisji nr 874/2004²⁰ przesłanką wycofania nazwy domeny identycznej albo myląco podobnej jest, obok zarejestrowania bezprawnie lub bez uzasadnionego interesu, zła wiara po stronie rejestrującego. Zdaniem Sądu pozwany wiedział o istnieniu znaku towarowego ROCCOBAROCCO i znał włoską markę. Celowo zarejestrował domenę „roccobarocco.eu”, aby czerpać komercyjne zyski z podobieństwa i wprowadzania w błąd oraz zaoferował odsprzedaż domeny za kwotę

¹⁷ Art. 14 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/517.

¹⁸ Rozporządzenie Komisji (WE) nr 874/2004 z 28.04.2004 r. ustanawiające reguły porządku publicznego dotyczące wprowadzenia w życie i funkcji Domeny Najwyższego Poziomu. eu oraz zasady regulujące rejestrację (Dz.Urz. UE L 162 z 30.04.2004 r., s. 40–50).

¹⁹ Dec. Sądu Arbitrażowego w Pradze z 25.11.2006 r. w sprawie 02970, *Urząd Miasta Zakopane v. EURid*; zob: https://eu.adr.eu/adr/decisions/decision.php?dispute_id=2970.

²⁰ Art. 21 ust. 1 rozporządzenia Komisji (WE) nr 874/2004 z 28.04.2004 r. ustanawiające reguły porządku publicznego..., s. 40–50.

7 000 euro. Na tej podstawie sąd zdecydował o przeniesieniu praw do domeny „roccobarocco.eu” na skarżącego²¹.

Podobna sprawa była przedmiotem mediacji przed Centrum Arbitrażu i Mediacji przy WIPO (WIPO Arbitration and Mediation Center) w 2015 roku. Skarżący Marks and Spencer Plc zarzucił naruszenie prawa do znaku towarowego „Marks and Spencer” przez zarejestrowanie domeny „marksandspencer.ir”. W treści decyzji WIPO również poruszyło kwestię podobieństwa między domenami, posiadania praw lub uzasadnionych interesów w zarejestrowaniu domeny oraz złej wiary. Ostatecznie domena została przeniesiona na skarżącego²².

V. Wnioski

Przegląd postępowań toczących się na obszarze Unii Europejskiej i w Stanach Zjednoczonych w związku ze stosowaniem *cybersquattingu* i *typosquattingu* ujawnia skalę zjawiska. Powszechne stają się międzynarodowe spory o nazewnictwo domen internetowych. Analizowane akty prawne – Anticybersquatting Consumer Protection Act oraz rozporządzenie 2019/517 różnią się pod pewnymi względami, jednak zapewniają ochronę przedsiębiorcom i konsumentom w podobnym zakresie.

ACPA przewiduje katalog czynników ułatwiających stwierdzenie występowania złej wiary po stronie rejestrującego. Jednak w rozporządzeniu 2019/517 prawodawca unijny nie zawarł definicji złej wiary.

Ujednolicenie mechanizmów ochrony przed *cybersquattingiem* – w tym w zakresie odpowiedzialności za działanie w złej wierze – wzmocniłoby pozycję przedsiębiorców na rynku internetowym. Amerykańskie *actiones in rem* mogłyby mieć zastosowanie również wobec domeny „.eu” oraz innych TLD. Pojawia się jednak obawa, że przeprowadzenie postępowania w przypadku, gdy naruszcyciel ma siedzibę lub adres zamieszkania w innym państwie okazać się trudne, zwłaszcza może ograniczać udział pozwanego w postępowaniu.

Wobec stale pojawiających się kolejnych przejawów *cybersquattingu* należy postulować zwiększenie kontroli podczas dokonywania rejestracji domeny, np. przez dokładne sprawdzenie w badaniach wstępnych czy proponowana domena może naruszać prawa innych podmiotów.

Bibliografia

- Banach, A. (2006). Domena internetowa. *E-mentor*, (3).
- Curtin, T.J. (2010). *The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites*. *Journal of Law & Policy*, (19).
- Fisher, B.D. (2001). Feature Anticybersquatting Consumer Protection Act – Two Cases Addressing Cybersquatting before and after the Act. *Florida Bar Journal*, (75).
- Martin, N.L. (2000). The Anticybersquatting Consumer Protection Act. *Journal of Corporation Law*, 25(3).
- Nowińska, E. i Szczepanowska-Kozłowska, K. (2018). *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*. Warszawa: Wolters Kluwer.

²¹ Dec. Sądu Arbitrażowego w Pradze z 6.02.2020 r. w sprawie 07703, *Barocco Roma srl, Rocco Barocco v. Virginie Trottier*; zob. https://eu.adr.eu/adr/decisions/decision.php?dispute_id=7703.

²² Dec. Panelu Administracyjnego Centrum Arbitrażu i Mediacji WIPO z 2.06.2015 r. w sprawie DIR2015-0001, *Marks and Spencer Plc v. Ali Ebrahimi*; zob. <https://www.wipo.int/amc/en/domains/decisions/text/2015/dir2015-0001.html>.

- Pope, M.B., Warkentin, M., Mutchler, L.A. i Xin L. (2012). The Domain Name System – Past, Present, and Future. *Communications of the Association for Information Systems*, (30).
- Ross, T.P. (2000). *Intellectual Property Law Damages and Remedies*. New York, N.Y: Law Journal Press.
- Sadasivan, B. (2003). Jurisprudence under the in rem provision of the Anticybersquatting Consumer Protection Act. *Berkeley Technology Law Journal*, (18).
- Tworkowska-Baraniuk, A. (2016). Cybersquatting i Metatagging – ochrona oznaczeń przedsiębiorcy w środowisku internetowym. *Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki humanistyczne, społeczne i Techniczne*, (2).
- Waty, M., van Hoolan, S., Hengchen, S., Coeckelbergs, M. i De Wilde, M. (2016). *How hot is .brussels? Impact of the uptake of the .brussels top-level domain name extension*. Bruksela: Université libre de Bruxelles.