Piotr Modrzejewski
Uniwersytet Warszawski
ORCID: 0000-0002-4987-4951

Sposoby naruszania dóbr osobistych w Internecie – zagadnienia wybrane

Wstęp

W polskim systemie prawnym, w art. 23 Kodeksu cywilnego[1], została przyjęta koncepcja otwartego katalogu dóbr osobistych. Wyliczenie dóbr osobistych zawarte w tym przepisie nie jest wyczerpujące. W związku z tym można wyróżnić dobra bezpośrednio wymienione w ustawie i dobra, o których istnieniu przesądziła doktryna lub judykatura. Do pierwszej kategorii, w myśl art. 23 k.c., należą zdrowie, wolność, cześć, swoboda sumienia, nazwisko, pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska. Do drugiej kategorii, podążając za dorobkiem doktryny[2], należą życie, nietykalność cielesna, integralność seksualna, dobre imię osoby prawnej, nazwa osoby prawnej, firma, nazwa zespołu, stan cywilny, poczucie przynależności do określonej płci, kult po zmarłej osobie bliskiej, prawo do prywatności, ochrona danych osobowych, możliwość korzystania z walorów środowiska naturalnego oraz ochrona przed hałasem.

Jednym z podziałów dóbr osobistych jest podział na dobra, które mogą być naruszone w Internecie oraz te, które w taki sposób naruszone być nie mogą. Podział ten ma istotne znaczenie z punktu widzenia potrzeb niniejszego opracowania. Niestety, jest podziałem niejednoznacznym i wywołującym wiele wątpliwości. Zgodnie z poglądem J. Sadomskiego, dobrami osobistymi, które najczęściej są naruszane przez media (czyli również w Internecie) są cześć, wizerunek i prywatność[3]. Autor ten wprawdzie nie wyklucza, że za pomocą środków masowego przekazu można naruszyć również inne dobra osobiste, ale nie precyzuje, których dóbr to dotyczy. Powszechnie uważa się,

[1] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, Dz. U. 1964 nr 16 poz. 93 – dalej jako „k.c."

[2] M. Pazdan, [w:] M. Safjan (red.), *System prawa prywatnego. Prawo cywilne – część ogólna*, tom 1, Warszawa 2007, s. 1119–1149.

[3] J. Sadomski, *Naruszenie dóbr osobistych przez media*, Warszawa 2003, s. 26.

że istnieją dobra osobiste, które można naruszyć jedynie w świecie rzeczywistym. W doktrynie wskazuje się, że przykładem takiego dobra jest nietykalność mieszkania[4]. Z kolei M. Pazdan uważa, że w systemie komunikacji elektronicznej może dojść do naruszenia wizerunku[5] oraz tajemnicy korespondencji[6]. Co do możliwości naruszenia jakichkolwiek innych dóbr osobistych za pomocą środków masowego przekazu (w tym również Internetu) nie zabiera głosu. Według P. Waglowskiego, praktycznie wszystkie dobra osobiste wymienione w art. 23 k.c. mogą być zagrożone lub naruszone w Internecie[7]. Przykładowo, życie i zdrowie przez umieszczenie migającej grafiki na forum internetowym często odwiedzanym przez osoby chore na epilepsję. Nazwisko przez bezprawne umieszczenie go w domenie internetowej. Wizerunek przez opublikowanie zdjęcia osoby bez jej zgody. Tajemnica korespondencji przez przeglądanie cudzej poczty elektronicznej. Prywatność przez monitorowanie czynności innych osób w Internecie. Jak również wolność, cześć, pseudonim, firma i twórczość.

Moim zdaniem, praktycznie każde dobro osobiste może zostać zagrożone lub naruszone w Internecie, na co wskazują chociażby przykłady wymienione powyżej. Co więcej, stoję na stanowisku, że nawet nietykalność mieszkania może być przedmiotem naruszeń w Internecie. Należy pamiętać, że naruszenie nietykalności mieszkania nie wymaga fizycznego wtargnięcia do cudzego mieszkania[8]. Może polegać na zainstalowaniu ukrytych kamer czy urządzeń podsłuchowych. Współcześnie powszechnie dostępne są programy lub aplikacje, dzięki którym, przy wykorzystaniu Internetu i urządzeń elektronicznych, możemy oglądać obraz z kamery lub słuchać nagrywanych rozmów niezależnie od miejsca, w którym się znajdujemy (może to być miejsce oddalone nawet o setki kilometrów). W ten sposób, przez zamontowanie odpowiedniego urządzenia w cudzym mieszkaniu, można obserwować, nagrywać, odtwarzać i udostępniać każdy ruch i każde słowo osób tam przebywających – zarówno domowników, jak i osób trzecich. Niewątpliwie będzie to stanowiło naruszenie nietykalności mieszkania, zgodnie z orzeczeniem Sądu Apelacyjnego w Gdańsku[9], który stwierdził, że przy ustalaniu treści prawa nietykalności mieszkania powinien być brany pod uwagę aspekt niematerialny. W uzasadnieniu orzeczenia Sąd Apelacyjny w Gdańsku, odnosząc się do aspektu niematerialnego nietykalności mieszkania, zwrócił uwagę, iż „chodzi w nim o ochronę przed bezprawnym wtargnięciem osoby trzeciej

[4] P. Waglowski, *Ochrona dóbr osobistych i danych osobowych*, Warszawa 2009, s. 4.
[5] M. Pazdan, [w:] M. Safjan (red.), op. cit., s. 1132.
[6] Ibidem, s. 1135.
[7] P. Waglowski, *Ochrona dóbr osobistych*…, op. cit., s. 4–5.
[8] M. Pazdan, [w:] M. Safjan (red.), op. cit., s. 1138.
[9] Wyrok Sądu Apelacyjnego w Gdańsku z dnia 29 grudnia 2000 r., I CA 910/00, Orzecznictwo Sądów Apelacyjnych 2002, Nr 2, poz. 11.

w sferę określonego stanu psychicznego i emocjonalnego, jaki daje człowiekowi poczucie bezpiecznego i niezakłóconego korzystania z własnego kąta, w którym ześrodkowana jest jego aktywność życiowa i z którym związana jest jego prywatność".

Dobra osobiste mogą zostać naruszone na wiele różnych sposobów. Niemożliwe wydaje się wskazanie wszystkich. Katalog dóbr osobistych, które mogą zostać naruszone w Internecie, niczym się nie wyróżnia, ale sposoby ich naruszeń są inne. Stawiam sobie zadanie wskazania podstawowych sposobów, które mogą prowadzić do naruszenia dóbr osobistych w Internecie.

Cookies

Pierwszym sposobem, za pomocą którego może dojść do naruszenia dóbr osobistych w Internecie jest używanie tzw. *cookies*, czyli, jak charakteryzuje je A. Rogacka-Łukasik w odniesieniu do prawa do prywatności, małych plików tekstowych umieszczanych na komputerze użytkownika w chwili połączenia się ze stroną internetową[10]. Dzięki tym plikom można prześledzić i zgromadzić wszelkiego rodzaju działania użytkownika Internetu. Informacje nazywane ciasteczkami (ang. *cookies*) są wysyłane przez odwiedzany serwis internetowy i zapisywane na używanym do tego urządzeniu (np. komputerze, laptopie czy smartfonie). Ciasteczka umożliwiają zapamiętanie preferencji użytkownika i personalizowanie stron internetowych w zakresie wyświetlanych treści, dopasowanie reklam, rejestrowanie produktów i usług czy głosowanie w internetowych ankietach. Niewątpliwie dzięki ciasteczkom korzystanie ze stron internetowych jest łatwiejsze i szybsze, ale stwarza też szerokie możliwości naruszania dóbr osobistych człowieka, przede wszystkim prawa do prywatności.

Należy zauważyć, że w znowelizowanej w 2013 r. ustawie Prawo telekomunikacyjne[11] przyjęta została procedura uzyskiwania zgody na stosowanie plików *cookies* (w art. 173 tej ustawy). Użytkownik podczas łączenia się ze stroną internetową używającą omawianych plików otrzymuje automatyczny komunikat, zgodnie z którym ma możliwość (nie obowiązek) wyrażenia zgody na przechowywanie i używanie tych plików. Wydaje się na pozór, że można bez żadnych konsekwencji odmówić takiej zgody. Niestety tak nie jest, ponieważ brak zgody powoduje zablokowanie ciasteczek, co oznacza, że strona nie będzie funkcjonować poprawnie. W związku z tym, większość użytkowników stron internetowych udziela zgody na korzystanie z plików *cookies*

[10] A. Rogacka-Łukasik, *Prawo do prywatności w dobie współczesnej ekspansji Internetu*, [w:] A. Kalisz (red.), *Prawa człowieka. Współczesne zjawiska, wyzwania, zagrożenia*, tom 2, Sosnowiec 2015, s. 66.

[11] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. 2004 nr 171 poz. 1800.

na ich urządzeniach, pozostając w nieświadomości co do potencjalnych naruszeń ich dóbr osobistych.

Sniffing, *phishing* i *heartbleed bug*

Do naruszenia dóbr osobistych w Internecie może dojść także przez *sniffing* (po polsku węszenie), który, według A. Rogackiej-Łukasik, stanowi jedną z najskuteczniejszych technik przechwytywania danych przesyłanych w sieci[12]. *Sniffing* umożliwia nie tylko monitorowanie czy słuchanie transmisji danych komputerowych, ale również pozyskiwanie cudzych haseł dostępu do poczty elektronicznej, portali społecznościowych, a nawet kont bankowych. Ten sposób naruszania jest szczególnie groźny, ponieważ pozostaje niezauważony przez użytkownika i jest bardzo trudny do wykrycia nawet przez informatyków. Warto wspomnieć, że *sniffing* może być wykorzystywany legalnie jako narzędzie do zarządzania i usuwania problemów z siecią[13].

Kolejnym sposobem, za pomocą którego może dojść do naruszenia dóbr osobistych w Internecie jest *phishing* (określany też jako *spoofing*, po polsku podszywanie się). A. Rogacka-Łukasik wskazuje, że *phishing* można określić jako kradzież tożsamości, ponieważ polega na podszywaniu się pod znane użytkownikom osoby lub instytucje w celu uzyskania od nich poufnych danych osobowych, przede wszystkich numerów kart kredytowych oraz haseł do kont bankowych, ale nie tylko[14]. Równie dobrze może dojść do ujawnienia innych poufnych danych, które mogą zostać wykorzystane do naruszenia dóbr osobistych, jak choćby zdjęć, wyników prac naukowych czy danych dotyczących stanu zdrowia. W celu pozyskania danych służących np. wykorzystaniu cudzej karty kredytowej, tworzone są specjalne strony internetowe[15]. Na tych stronach można nabywać różne towary. W momencie sfinalizowania zakupu przez użytkownika, wszystkie dane dotyczące transakcji zostają przechwycone przez nieuprawniony podmiot, o czym użytkownik oczywiście nie wie. Szczególną odmianą *phishingu* jest *SMiShing*, który również polega na podszywaniu się pod znane użytkownikom osoby lub instytucje w celu uzyskania od nich poufnych danych osobowych, ale przez wykorzystanie telefonu komórkowego (również smartfona), a nie komputera lub laptopa[16].

---

[12] A. Rogacka-Łukasik, op. cit., s. 67.

[13] M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4 (113), s. 5.

[14] A. Rogacka-Łukasik, op. cit., s. 67.

[15] P. Waglowski, *Prawo w sieci. Zarys regulacji internetu*, Gliwice 2005, s. 353.

[16] M. Nowak, op. cit., s. 5.

Naruszenie prawa do prywatności oraz przyczynek do naruszania innych dóbr osobistych stanowi zjawisko *heartbleed bug* (po polsku „krwawienie z serca")[17]. Błąd bezpieczeństwa, który często wyświetla się na ekranach mobilnych urządzeń, może spowodować odczyt pamięci systemu. W efekcie naruszyciel uzyskuje dostęp do wszelkich danych zgromadzonych w pamięci systemowej atakowanego urządzenia (np. kluczy szyfrujących, nazw i haseł użytkownika). Specyficzną nazwę tego zjawiska można uzasadnić tym, że pamięć systemowa stanowi serce każdego elektronicznego urządzenia, a więc nieuprawniony dostęp można określić jako „krwawienie z serca".

Google Maps

Google Maps (po polsku mapy Google) to serwis internetowy (lub aplikacja na smartfony) umożliwiający oglądanie map i sprawdzanie położenia określonych obiektów[18]. Pozornie tylko wydaje się, że przez użycie tego programu nie może dojść do naruszenia dóbr osobistych. Było tak do 2007 roku, w którym to została dodana do Map Google usługa Street View (pl. widok ulicy). Dzięki tej usłudze można wirtualnie „spacerować" po wielu miastach na świecie, między innymi po Warszawie. Zdjęcia satelitarne wykorzystane do usługi Street View mają bardzo wysoką rozdzielczość, a więc ich jakość jest doskonała. Poza budynkami i ulicami można bez problemu obejrzeć postacie sfotografowanych osób, samochody, ogródki oraz wszystkie inne przedmioty, które w momencie robienia zdjęcia znajdowały się w zasięgu obiektywu. W związku z tym w Internecie swobodnie krążą zdjęcia określonych osób w określonych miejscach, z którymi to miejscami te osoby być może nie chciałyby być kojarzone. Stanowi to również doskonałą bazę danych dla złodziei, którzy mogą wykorzystać tę usługę do planowania różnego rodzaju przestępstw[19]. Należy stwierdzić, że Street View może być szeroko wykorzystywany przez użytkowników Internetu do naruszania dóbr osobistych innych osób, o ile już samo istnienie tej usługi nie narusza prywatności czy wizerunku osób na nich widniejących.

Spam

Jednym z podstawowych celów korzystania z Internetu jest możliwość używania poczty elektronicznej, powszechnie określanej jako e-mail czy po

[17] A. Rogacka-Łukasik, op. cit., s. 69.

[18] Ibidem, s. 68.

[19] W. Lis, *Prawo do prywatności a rozwój nowych technologii informatycznych. Szanse i zagrożenia*, [w:] J. Mucha (red.), *Nie tylko Internet. Nowe media, przyroda i „technologie społeczne" a praktyki kulturowe*, Kraków 2010, s. 180.

prostu mail[20]. Dzięki niej można, między innymi, wysyłać, odbierać i przekazywać wiadomości elektroniczne między użytkownikami. Problem pojawia się wtedy, gdy otrzymana wiadomość elektroniczna jest niepotrzebna czy wręcz niechciana, a więc jest tzw. spamem. Spam, występujący najczęściej w postaci informacji reklamowej, stanowi zazwyczaj zbędną dla adresata wiadomości informację. Warto dodać na marginesie, że poczta elektroniczna jest atrakcyjniejszym nośnikiem komercyjnych danych niż strony WWW, ponieważ dociera do adresata w sposób nieuchronny[21]. Jednakże szkodliwość spamu nie ogranicza się jedynie do marnowania czasu użytkowników poczty elektronicznej na odbieranie zbędnych wiadomości, choć z pewnością ten czas mogliby spożytkować w inny sposób. Przede wszystkim spam może doprowadzić do blokady poczty elektronicznej w ogóle, blokady pożądanej korespondencji, zakłócenia działania sieci internetowej przez nadmierne obciążenie serwerów wywoływane ogromną ilością i rozmiarem spamu, wywołania awarii w komputerze (i w każdym innym urządzeniu elektronicznym używanym do obsługi poczty elektronicznej) oraz narażenia użytkownika na ponoszenie zwiększonych kosztów dostępu do jego poczty[22]. Zwiększenie kosztów powoduje konieczność zainstalowania odpowiednich programów antyspamowych, w które wciąż wiele komputerów nie jest wyposażonych. Takie programy stanowią, co do zasady, skuteczne zabezpieczenie wszelkich urządzeń służących do obsługi poczty elektronicznej przed spamem, co nie oznacza, że są niezawodne. Dostawcy Internetu pracują nad wdrożeniem specjalnych mechanizmów filtrujących pocztę elektroniczną i odrzucających listy pochodzące z jednego źródła, a adresowane do tysięcy użytkowników Internetu, ale pojawiają się coraz to nowe, oszukańcze metody omijania tych mechanizmów, polegające na mylącym formułowaniu tytułów listów (tak, aby nie wskazywały na reklamową treść), zmienianiu źródła ich nadania czy wykorzystywaniu adresu osoby nieistniejącej. Wywołanie szkód w komputerze polega zazwyczaj na możliwości przesyłania za pomocą spamu wirusów komputerowych, które mogą służyć do niszczenia danych lub zdobycia informacji poufnych przez podmioty nieuprawnione.

Według D. Kasprzyckiego, w zasadzie każda niezamawiana przesyłka (czyli każdy spam, który bywa też określany mianem *junk e-mail*[23]) stanowi naruszenie sfery prywatności odbiorcy przez zakłócenie swobodnego i płynnego korzystania przez niego z Internetu. Istotą zjawiska *spammingu* jest

[20] A. Rogacka-Łukasik, op. cit., s. 68–69.

[21] D. Kasprzycki, *Spam, czyli niezamawiana komercyjna poczta elektroniczna: zagadnienia cywilnoprawne*, Kraków 2005, s. 24–39.

[22] P. Waglowski, *Spam a prawo. Próba wskazania kierunków badawczych,* „Prawo i Ekonomia w Telekomunikacji" 2003, nr 4, s. 64.

[23] Pochodzenie terminu „spam" oraz szeroka gama jego możliwych rozwinięć, jak również synonimów jest warta uwagi, lecz nie mieści się w ramach niniejszego opracowania. W związku z tym proponuję zapoznanie się z następującą publikacją: D. Kasprzycki, op. cit., s. 30–33.

korespondencja elektroniczna przesyłana masowo do wielu użytkowników Internetu, którzy jej nie zamawiali. Praktyki spammingowe nie są związane wyłącznie z działalnością gospodarczą, lecz mogą być również stosowane w działalności politycznej, kulturalnej, religijnej i społecznej. Spam, poza naruszaniem dobra osobistego w postaci sfery prywatności, może naruszać również wolność człowieka[24]. Wolność należy w tym przypadku rozumieć jako wolność od złośliwego, uciążliwego niepokojenia, od obawy i strachu, a także od wszelkich nieuprawnionych nacisków krępujących swobodne dysponowanie wartościami osobistymi[25]. Słusznie wskazuje się w literaturze[26], że spam, mimo iż dotyczy poczty elektronicznej, nie narusza tajemnicy korespondencji, ponieważ jego istotą nie jest zapoznanie się z informacją kierowaną do innego podmiotu, ani ujawnienie informacji otrzymanej poufnie.

Domeny internetowe

Domeny internetowe, inaczej nazywane adresami internetowymi, są jednym z najważniejszych i najczęściej stosowanych narzędzi w Internecie[27]. Na świecie zarejestrowanych jest około trzydzieści milionów domen internetowych, które służą przede wszystkim do identyfikacji stron WWW oraz lokalizacji kont pocztowych używanych w korespondencji elektronicznej. Zarejestrowanie i używanie domen internetowych, których częścią jest cudze nazwisko, pseudonim, firma czy nazwa, może prowadzić do naruszenia dóbr osobistych tych podmiotów[28]. Co więcej, w związku z wykorzystaniem w adresach internetowych wskazanych danych, może dojść do naruszenia takich dóbr osobistych jak wizerunek, cześć, dobre imię czy renoma[29]. Warto mieć świadomość, że większość dóbr osobistych osób fizycznych i osób prawnych może zostać naruszona przez używanie ich nazwisk, pseudonimów, firm i nazw w adresach stron WWW oraz adresach poczty elektronicznej.

Należy poczynić uwagę, że niemożliwe jest funkcjonowanie dwóch identycznych domen internetowych na jednym poziomie domen (są trzy poziomy domen internetowych – globalny, unijny i krajowy) ze względu na koniecz-

---

[24] D. Kasprzycki, op. cit., s. 307–311.

[25] Z. Radwański, *Glosa do postanowienia Sądu Najwyższego z dnia 18 października 1967 r., II CZ 92/67*, „Orzecznictwo Sądów Polskich i Komisji Arbitrażowych" 1968, z. 10, poz. 208, s. 447.

[26] P. Drewniak, *Wybrane problemy regulacji antyspamowych w Polsce*, „Prawo Mediów Elektronicznych" 2007, nr 6.

[27] J. Ożegalska-Trybalska, *Adresy internetowe. Zagadnienia cywilnoprawne,* „Prace Instytutu Prawa Własności Intelektualnej Uniwersytetu Jagiellońskiego" 2003, z. 84, s. 18.

[28] O. Sztejnert, *Ochrona praw do domeny w procesie cywilnym*, „Monitor Prawniczy" 2000, nr 10, dodatek: Internet i komputer w kancelarii, s. 12.

[29] J. Ożegalska-Trybalska, *Adresy internetowe*…, op. cit., s. 223–243.

ność jednoznacznej identyfikacji urządzeń w Internecie[30]. Dopuszczenie do sytuacji, w której miałyby istnieć dwa identyczne adresy internetowe zapisane w systemie domenowym na tym samym poziomie, uniemożliwi należytą identyfikację urządzeń, a zatem uniemożliwi należyte działanie Internetu. W konsekwencji każdy podmiot, który zarejestruje nazwę domeny internetowej, uzyska jednocześnie pewność, że żadna osoba nie dokona rejestracji tożsamej nazwy. Jednakże w pełni dopuszczalne i niewywołujące żadnych problemów w funkcjonowaniu Internetu jest rejestrowanie nazw domen internetowych różniących się od siebie nieznacznie, a nawet łudząco do siebie podobnych (np. firma.pl i frima.pl)[31]. Tak samo za w pełni dopuszczalne należy uznać zarejestrowanie identycznych nazw domen internetowych, ale na różnym poziomie domen (np. firma.com i firma.com.pl)[32].

Należy zauważyć, że nie każda forma posługiwania się cudzym nazwiskiem lub pseudonimem prowadzi do naruszenia dóbr osobistych. Konieczne jest, poza istnieniem innych przesłanek odpowiedzialności z tytułu naruszenia cudzych dóbr osobistych, aby posługiwanie się cudzym nazwiskiem lub pseudonimem w adresie strony internetowej naruszało sferę identyfikacji osoby fizycznej. Nie może dotyczyć to danego nazwiska lub pseudonimu w ogólności. Musi odnosić się do konkretnej osoby o tym nazwisku lub pseudonimie. Samo użycie cudzego nazwiska lub pseudonimu nie umożliwia zidentyfikowania tej osoby. Dopiero powiązanie tego nazwiska lub pseudonimu z dodatkowymi informacjami lub osadzenie go w odpowiednim kontekście sytuacyjnym pozwala na identyfikację konkretnej osoby noszącej to nazwisko lub używającej tego pseudonimu. Według J. Ożegalskiej-Trybalskiej[33], do naruszenia cudzego nazwiska lub pseudonimu przez bezprawne użycie ich w adresie strony internetowej, może dojść w dwóch sytuacjach. Po pierwsze, gdy za pośrednictwem tej strony rozpowszechniane są nieprawdziwe informacje, ujemne oceny, fałszywe zarzuty, krytyczne uwagi w stosunku do osoby noszącej to nazwisko lub używającej tego pseudonimu, w celu jej poniżenia w oczach opinii publicznej lub narażenia na utratę zaufania potrzebnego do sprawowania określonego stanowiska czy wykonywania określonego zawodu. Tytułem przykładu można wskazać na wykorzystanie nazwiska

[30] P. Wilczak, *Skutki zawarcia umowy o rejestrację i utrzymywanie nazwy domeny .pl w sferze uprawnień i sytuacji faktycznej abonenta*, „Prawo Mediów Elektronicznych" 2007, nr 6.

[31] W prawie nieuczciwej konkurencji takie zjawisko określane jest mianem *typosquatting*. Stanowi formę naruszenia uprawnień do oznaczeń odróżniających w Internecie. Traktowane jest jako odmiana *cybersquattingu*. Szerzej na ten temat: M. Modrzejewska, *Wykorzystanie w nazwie domeny internetowej cudzych oznaczeń identyfikacyjnych jako czyn nieuczciwej konkurencji,* [w:] M. Pazdan (red.), M. Jagielska (red.), E. Rott-Pietrzyk (red.), M. Szpunar (red.), *Rozprawy z prawa prywatnego. Księga jubileuszowa dedykowana Profesorowi Wojciechowi Popiołkowi,* Warszawa 2017, s. 1122–1124.

[32] Szerzej o możliwościach rejestracji różnych domen, o sposobie zawierania umów dotyczących korzystania z domeny oraz o nadzorze nad domeną „.pl" sprawowanym przez instytut badawczy NASK (Naukowa i Akademicka Sieć Komputerowa): M. Modrzejewska, op. cit., s. 1109–1114.

[33] J. Ożegalska-Trybalska, *Adresy internetowe*…, op. cit., s. 238–239.

znanego polityka w adresie strony internetowej, która zawiera ośmieszające i kompromitujące go treści albo wykorzystanie nazwiska nobliwego duchownego w adresie strony WWW, reklamującej towary pornograficzne. Po drugie, gdy strona służy do celów reklamowych, a nazwisko lub pseudonim powszechnie znanej osoby ma na celu zwrócenie uwagi odbiorców. W takim przypadku przeciętny użytkownik Internetu, skojarzy adres strony internetowej z nazwiskiem lub pseudonimem sławnych osób ze świata sportu, mody, filmu, mediów czy polityki.

W przypadku osób prawnych, tak jak w przypadku osób fizycznych, najbardziej narażona na naruszenia spowodowane używaniem adresów stron internetowych jest sfera identyfikacji osoby prawnej. Używanie nazwy lub firmy osoby prawnej będzie stanowiło naruszenie jej dóbr osobistych, gdy podmiot nieuprawniony wywołuje niebezpieczeństwo pomyłek wśród użytkowników Internetu co do tożsamości osoby prawnej i dysponenta adresu lub co do związku dysponenta adresu z osobą prawną[34]. Warto zauważyć, że do naruszenia dóbr osobistych osoby prawnej w postaci jej nazwy lub firmy może również dojść, gdy w adresie strony internetowej zostanie wykorzystana część (skrót lub akronim) nazwy lub firmy, ale tylko pod warunkiem, że ta część jest wystarczająca do identyfikacji tej osoby prawnej oraz odróżnienia jej od innych podmiotów. W praktyce używanie przez osoby prawne w adresach stron internetowych skrótów ich oznaczeń odróżniających jest powszechne (np. podmiot National Aeronautics and Space Administration używa skrótu NASA).

Deep links

Poddać pod rozwagę należy problem możliwości naruszenia dóbr osobistych, zwłaszcza prawa do wizerunku, przez stosowanie tzw. głębokich odesłań (ang. *deep links*) z innych stron internetowych. W doktrynie zostało postawione pytanie, czy umieszczenie na stronie internetowej głębokiego odesłania do wizerunku znajdującego się na linkowanej stronie internetowej bez zgody dysponenta wizerunku może naruszać jego prawo do wizerunku i ewentualnie inne dobra osobiste. Odpowiedź twierdząca na to pytanie wywołuje wątpliwość co do kwalifikacji takiego odesłania jako bezpośredniego naruszenia[35]. Zagadnienie to było przedmiotem rozstrzygnięcia Sądu Apelacyjnego w Kra-

---

[34] R. Skubisz, *Glosa do wyroku Sądu Najwyższego z dnia 26 września 1991 r., II CR 753/90*, „Przegląd Sądowy" 1993, nr 1, s. 95.

[35] K. Włodarska, *Naruszenie prawa do wizerunku w Internecie przez podmiot stosujący tzw. głębokie odesłania*, [w:] J. Barta, A. Matlak (red.), *Prawo własności intelektualnej wczoraj, dziś i jutro*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace Instytutu Prawa Własności Intelektualnej" 2007, z. 100, s. 603–627.

kowie, który zajął stanowisko, że działanie polegające na zamieszczeniu na stronie internetowej głębokiego odesłania, umożliwiającego użytkownikom tej strony bezpośrednie otwarcie rekomendowanej witryny, stanowi rozpowszechnienie wizerunku zamieszczonego w tej witrynie[36]. Sąd uznał, że użycie takiej techniki elektronicznej zwiększa ilość osób, które mogą zapoznać się z zawartością strony, do której prowadzi głębokie odesłanie. W dalszej części uzasadnienia Sąd stwierdził, że należy odróżnić sytuację powstałą na tle omawianego zagadnienia, od sytuacji stosowania zwykłych odesłań do innych stron internetowych. Za odesłania zwykłe uznaje się takie, które nie umożliwiają bezpośredniego dostępu do określonych treści, lecz wymagają dodatkowych czynności ze strony użytkownika Internetu (mówiąc kolokwialnie – wymagają kilku dodatkowych kliknięć). Rozstrzygnięcie Sądu Apelacyjnego w Krakowie spotkało się z negatywną oceną niektórych przedstawicieli doktryny[37]. Ich zdaniem celem stosowania głębokich odesłań jest szybkie i łatwe zapoznawanie się z materiałami dostępnymi pod linkiem. Istotą tego narzędzia jest możliwość bezpośredniego dostępu do informacji zawartych na stronie, na którą użytkownik zostaje przekierowany. Uznanie, że na posługiwanie się takimi odesłaniami konieczna jest zgoda podmiotu, na którego stronę następuje odesłanie, nakłada na podmioty je umieszczające dodatkowy obowiązek obserwowania i weryfikowania treści znajdujących się na stronie, do której prowadzi odesłanie oraz obowiązek uzyskiwania zgód od odpowiednich podmiotów na rozpowszechnianie ich wizerunku za pomocą odesłania. Warto zauważyć, że treści znajdujące się na stronie, do której prowadzi odesłanie, zazwyczaj ulegają zmianom, a zgoda podmiotów na rozpowszechnianie ich wizerunku może zostać cofnięta czy unieważniona, co jeszcze bardziej komplikuje prawne aspekty stosowania głębokich odesłań i prowadzi do dalszych pytań i problemów, na które próżno szukać jednoznacznych odpowiedzi.

Niezależnie od tego, czy w następnych orzeczeniach, dotyczących omawianego zagadnienia, sądy wesprą pogląd ukształtowany przez Sąd Apelacyjny w Krakowie, czy zmienią go i jakie będzie ich uzasadnienie, a także jakie będą na ten temat wypowiedzi doktryny, to *deep links* są kolejnym sposobem, za pomocą którego może dojść do naruszenia dóbr osobistych w Internecie. Czy w danym stanie faktycznym rzeczywiście dojdzie do naruszenia prawa do wizerunku lub innego dobra osobistego przez stosowanie głębokich odesłań rozstrzygnie każdorazowo sąd, lecz warto mieć świadomość, że również w taki sposób dobra osobiste mogą zostać naruszone.

---

[36] Wyrok Sądu Apelacyjnego w Krakowie z dnia 20 lipca 2004 r., I ACa 564/04, „Transformacje Prawa Prywatnego" 2004, nr 3–4, s. 155; Zob. podobnie Wyrok Sądu Apelacyjnego w Warszawie z dnia 9 grudnia 2015 r., VI ACa 1772/14, LEX 2009536.

[37] J. Ożegalska-Trybalska, *Naruszenie dóbr osobistych w Internecie w świetle orzecznictwa sądowego*, [w:] J. Balcarczyk (red.), *Dobra osobiste w XXI wieku. Nowe wartości, zasady, technologie*, Warszawa 2012, s. 380.

Cloud Computing

Cloud Computing, tłumaczony na język polski jako usługa „w chmurze", stał się narzędziem dostępnym dla każdego, kto nie chce inwestować w drogi sprzęt elektroniczny (przede wszystkim dyski pamięci), lecz wystarczy mu dostęp do współdzielonych, wirtualnych zasobów umieszczonych na zewnętrznych serwerach[38]. Rozwój sprzętu komputerowego, połączeń internetowych oraz usług świadczonych przez producentów aplikacji mobilnych spowodował, że współcześnie każdy może udostępniać i przechowywać dane „w chmurze". Dotyczy to zarówno wszystkich danych prywatnych, jak i służbowych, które mogą być zapisane na komputerach i innych urządzeniach elektronicznych (np. tabletach czy smartfonach). Powszechnie „chmura" jest używana przez osoby korzystające z internetowych i mobilnych usług konsumenckich, takich jak Facebook, Bing, Google czy Office 365[39]. Jednak nie może zostać niezauważone, że taki sposób udostępniania i przechowywania danych powoduje znaczne ryzyko dla ich prywatności i bezpieczeństwa. Nieodpowiednie zarządzanie systemem, mogące doprowadzić do niekontrolowanego „wycieku" danych, a także ataki hakerów, będą niewątpliwie stanowiły naruszenie prawa do prywatności. Co prawda przy użyciu tej usługi wprost może dojść do naruszenia tylko jednego dobra osobistego, jakim jest prawo do prywatności, jednakże informacje pozyskane w ten sposób przez nieuprawnione podmioty mogą zostać wykorzystane do naruszenia innych dóbr osobistych, jak choćby wizerunku, czci czy dobrego imienia. *Cloud Computing* stanowi kolejny, możliwy do zrealizowania jedynie w cyberprzestrzeni, sposób naruszenia dóbr osobistych.

Zakończenie

Warto zasygnalizować daleko idące konsekwencje, jakie rodzi korzystanie z Internetu przez jego użytkowników. W niniejszym opracowaniu zostały omówione podstawowe sposoby naruszeń, które można kwalifikować jako godzące w dobra osobiste w Internecie. Należy zaznaczyć, że nie stanowią one zamkniętego katalogu, lecz jedynie najczęściej spotykane przykłady. Używanie tzw. *cookies*, *sniffing*, *phishing*, *heatbleed bug*, spam, *deep links*, *Cloud Computing*, korzystanie z aplikacji typu Google Maps oraz rejestrowanie i używanie domen internetowych mogą stanowić źródło naruszeń dóbr

[38] E. Molenda-Kropielnicka, *„Cloud Computing" – zagadnienia prawne*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace z Prawa Własności Intelektualnej" 2013, nr 1 (119), s. 109

[39] S. Ahmed, R. Zalewska, *Przetwarzanie w chmurze obliczeniowej (cloud computing): kwestie umów i zgodności z prawem z perspektywy prawnika wewnętrznego*, „Monitor Prawniczy" 2014, nr 22, s. 1213.

osobistych. Wszystkie wymienione wyżej sposoby naruszeń powstały wraz z rozwojem cyberprzestrzeni, która, jak słusznie wskazuje A. Rogacka-Łukasik, jest symbolem najnowocześniejszej technologii[40]. Technologii, bez której gatunek ludzki nie potrafiłby w dzisiejszych czasach funkcjonować. Jak słusznie wskazuje się w doktrynie, korzystanie z komputerów i Internetu, w życiu prywatnym i zawodowym, wpływa pozytywnie na ogólny rozwój i postęp[41]. Należy jednak zdawać sobie sprawę, że ogromny potencjał Internetu stanowi jednocześnie rzeczywiste zagrożenie naruszeń dóbr osobistych. Całkowicie uzasadnione są obawy wielu użytkowników Internetu, którzy obserwują jak wraz z jego rozwojem następuje coraz brutalniejsze wkraczanie w ich życie prywatne.

Wykaz literatury

Ahmed S., Zalewska R., *Przetwarzanie w chmurze obliczeniowej (cloud computing): kwestie umów i zgodności z prawem z perspektywy prawnika wewnętrznego*, „Monitor Prawniczy" 2014, nr 22.

Drewniak P., *Wybrane problemy regulacji antyspamowych w Polsce*, „Prawo Mediów Elektronicznych" 2007, nr 6.

Kasprzycki D., *Spam, czyli niezamawiana komercyjna poczta elektroniczna: zagadnienia cywilnoprawne*, Kraków 2005.

Lis W., *Prawo do prywatności a rozwój nowych technologii informatycznych. Szanse i zagrożenia*, [w:] J. Mucha (red.), *Nie tylko Internet. Nowe media, przyroda i „technologie społeczne" a praktyki kulturowe*, Kraków 2010.

Modrzejewska M., *Wykorzystanie w nazwie domeny internetowej cudzych oznaczeń identyfikacyjnych jako czyn nieuczciwej konkurencji*, [w:] M. Pazdan (red.), M. Jagielska (red.), E. Rott-Pietrzyk (red.), M. Szpunar (red.), *Rozprawy z prawa prywatnego. Księga jubileuszowa dedykowana Profesorowi Wojciechowi Popiołkowi*, Warszawa 2017.

Modrzejewski P., *Odpowiedzialność innych podmiotów niż sprawca za naruszenie dóbr osobistych w Internecie*, „Przegląd Prawa Handlowego" 2017, nr 3.

Molenda-Kropielnicka E., *Cloud Computing – zagadnienia prawne*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace z Prawa Własności Intelektualnej" 2013, nr 1 (119).

Nowak M., *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4 (113).

Ożegalska-Trybalska J., *Adresy internetowe. Zagadnienia cywilnoprawne*, „Prace Instytutu Prawa Własności Intelektualnej Uniwersytetu Jagiellońskiego" 2003, z. 84.

Ożegalska-Trybalska J., *Naruszenie dóbr osobistych w Internecie w świetle orzecznictwa sądowego*, [w:] J. Balcarczyk (red.), *Dobra osobiste w XXI wieku. Nowe wartości, zasady, technologie*, Warszawa 2012.

[40] A. Rogacka-Łukasik, op. cit., s. 71

[41] P. Modrzejewski, *Odpowiedzialność innych podmiotów niż sprawca za naruszenie dóbr osobistych w Internecie*, „Przegląd Prawa Handlowego" 2017, nr 3, s. 58

Pazdan M., [w:] M. Safjan (red.), *System Prawa Prywatnego, Prawo cywilne – część ogólna*, tom 1, Warszawa 2007.
Radwański Z., *Glosa do postanowienia Sądu Najwyższego z dnia 18 października 1967 r., II CZ 92/67*, Orzecznictwo Sądów Polskich i Komisji Arbitrażowych 1968, z. 10, poz. 208.
Rogacka-Łukasik A., *Prawo do prywatności w dobie współczesnej ekspansji Internetu*, [w:] A. Kalisz (red.), *Prawa człowieka. Współczesne zjawiska, wyzwania, zagrożenia*, tom 2, Sosnowiec 2015.
Sadomski J., *Naruszenie dóbr osobistych przez media*, Warszawa 2003.
Skubisz R., *Glosa do wyroku Sądu Najwyższego z dnia 26 września 1991 r., II CR 753/90*, „Przegląd Sądowy" 1993, nr 1.
Sztejnert O., *Ochrona praw do domeny w procesie cywilnym*, „Monitor Prawniczy" 2000, Nr 10, dodatek: Internet i komputer w kancelarii.
Waglowski P., *Ochrona dóbr osobistych i danych osobowych*, Warszawa 2009.
Waglowski P., *Prawo w sieci. Zarys regulacji internetu*, Gliwice 2005.
Waglowski P., *Spam a prawo. Próba wskazania kierunków badawczych*, „Prawo i Ekonomia w Telekomunikacji" 2003, nr 4.
Wilczak P., *Skutki zawarcia umowy o rejestrację i utrzymywanie nazwy domeny .pl w sferze uprawnień i sytuacji faktycznej abonenta*, „Prawo Mediów Elektronicznych" 2007, nr 6.
Włodarska K., *Naruszenie prawa do wizerunku w Internecie przez podmiot stosujący tzw. głębokie odesłania*, [w:] J. Barta, A. Matlak (red.), *Prawo własności intelektualnej wczoraj, dziś i jutro*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace Instytutu Prawa Własności Intelektualnej" 2007, z. 100.

Summary

Ways of violating personal rights on the Internet – selected issues

Key words: personal rights, Internet, ways of violating personal rights, consent of the rights holder, internet domains.

One of the many divisions of personal rights was the division into rights which can be infringed on the Internet and those that cannot be violated in this way. Nowadays, it should be assumed that practically all personal rights may be endangered or violated on the Internet. Moreover, the role of identifying, indicating and describing the basic ways that violate personal rights in cyberspace is increasing. The use of cookies, sniffing, phishing, the Heartbleed bug, spam, deep links, Cloud Computing, the use of the Google Maps application, and the registration and use of Internet domains are just the most common examples. The development of these cutting-edge technologies has led to significant violations of privacy rights.