Tomasz Fołta, Andrzej Mucha

Zniesławienie i znieważenie w internecie

Z roku na rok liczba użytkowników globalnej sieci informacyjnej – internetu w naszym kraju gwałtownie rośnie. Techniczne możliwości, jakie oferuje internet, sprzyjają popełnieniu wielu typów czynów zabronionych, w tym również ściganych z oskarżenia prywatnego. Przyjrzyjmy się zatem w sposób bardziej szczegółowy przestępstwom zniesławienia i znieważenia dokonanym za pomocą internetu. Parafrazując słowa poety, należy również zapytać, jakie ma pokrzywdzony „tanki przeciw włóczni złego" w obecnym stanie prawnym. Czy rzeczywiście ma pełny wachlarz obrony swojego dobrego imienia z uwagi na specyfikę nośnika informacji, jakim jest internet?

I. Zagadnienia karnomaterialne

Rozważając problematykę popełniania przestępstw pomówienia (art. 212 k.k.) i znieważenia (art. 216 k.k.) za pomocą internetu, w pierwszej kolejności należy skupić się na samej ich konstrukcji normatywnej. Zastosowany przez ustawodawcę sposób budowy tychże typów ma niewątpliwie doniosłe znaczenie dla omawianego zagadnienia. Jego doniosłość wynika z samej specyfiki popełniania przestępstw z art. 212 k.k. i 216 k.k. „za pomocą" tak specyficznego medium, jakim jest internet.

Wbrew temu, co może się wydawać, sam sposób skonstruowania przepisów art. 212 k.k. i 216 k.k. ma w świetle omawianej tu problematyki doniosłe znaczenie tak teoretyczne, jak i praktyczne. Tymczasem komentatorzy kodeksu karnego, poruszając problematykę przestępstw pomówienia i znieważenia, w części, w jakiej dotyczą one kwestii znamion określających czynność sprawczą, ograniczają się do zdawkowego stwierdzenia, że przestępstwa te mogą być popełnione także przez internet[1]. Co więcej, we wszystkich publikacjach stanowiska takie przedstawiane są przy okazji omawiania typów kwalifikowanych tychże przestępstw, które dotyczą sytuacji, gdy są one popełniane „za pomocą środków masowego komunikowania". Tymczasem sprawa nie jest tak jednoznaczna.

[1] Por. A. Zoll, Kodeks karny. Komentarz. Część szczególna, Kantor Wydawniczy Zakamycze, Kraków 1999 s. 647 i n.; R. Góral, Kodeks karny. Praktyczny komentarz, Warszawa 2000, s. 288 i n.; O. Górniok, Kodeks karny. Komentarz, Warszawa 2004, s. 647 i n.; A. Marek, Kodeks karny. Komentarz, Warszawa 2005, s. 478 i n.

Analizując w tym miejscu przepisy art. 212 k.k. i 216 k.k., należy ograniczyć rozważania jedynie do omówienia kwestii ściśle powiązanych z przedmiotem niniejszego artykułu.

Z punktu widzenia możliwości wyczerpania przez sprawcę znamion przestępstw pomówienia i znieważenia „przez internet" istotne jest wskazanie możliwych sposobów popełnienia każdego z tych czynów. Ma to doniosłe znaczenie dla prowadzenia dalszych rozważań.

Zarówno w przypadku przestępstwa z art. 212 k.k. i art. 216 k.k. mamy do czynienia z niejako dwoma ogólnymi sposobami ich popełnienia, a w konsekwencji z dwoma kategoriami podmiotów, do jakich kierowana jest zabroniona prawem treść. Wyróżnić bowiem można tu: „publiczny sposób" popełnienia wskazanych wyżej przestępstw, np. znieważenie innej osoby publicznie oraz „sposób niepubliczny", np. znieważenie innej osoby niepublicznie i w jej nieobecności, lecz z zamiarem, aby zniewaga do tej osoby dotarła oraz znieważenie innej osoby w jej obecności, które, jak się słusznie przyjmuje, także nie ma charakteru publicznego[2].

Tak więc w przypadku przestępstwa pomówienia, jak i znieważenia, wyraźnie rysują się nam dwie ich kategorie zbiorcze o charakterze ogólnym, wyodrębnione z uwagi na podmiot (indywidualny lub zbiorowy), który staje się odbiorcą zakazanej treści i warunkuje realizację znamion określonego typu czynu zabronionego.

Analizując techniczny sposób skonstruowania przez ustawodawcę omawianych przepisów dochodzimy do wniosku, iż zarówno w art. 212 k.k. i art. 216 k.k. w ich § 1 opisane zostały typy podstawowe przestępstwa – odpowiednio – pomówienia i znieważenia. W art. 212 § 2 k.k. i art. 216 § 2 k.k. zawarte natomiast zostały typy kwalifikowane, wyodrębnione z uwagi na charakter środka, jakim posłużył się sprawca dla ich dokonania. Elementem kwalifikującym jest okoliczność, iż sprawca działał „za pomocą środków masowego komunikowania".

Mając na uwadze przedstawione wyżej uwagi na temat „publicznego" i „niepublicznego" popełnienia przestępstw z art. 212 i 216 k.k., stwierdzić należy, iż w ich typie podstawowym możliwe są oba wyżej omówione sposoby ich popełnienia.

W przypadku typów kwalifikowanych przestępstwa pomówienia i znieważenia stwierdzić należy natomiast, iż mogą zostać one popełnione – odmiennie niż wskazane wyżej typy podstawowe – tylko w jeden z wyróżnionych wyżej sposobów, a mianowicie tylko i wyłącznie „publicznie" (poprzez skierowanie zakazanej treści do szeroko pojętej opinii publicznej).

Na taki tylko możliwy sposób popełnienia tych typów przestępstw z art. 212 i 216 k.k. wskazują dwie okoliczności. Po pierwsze, wyraźną ku temu

[2] A. Zoll, Komentarz…, s. 668.

przesłanką jest użycie przez ustawodawcę zarówno w art. 212 § 2 k.k., jak i w art. 216 § 2 k.k. określenia „masowego" przy opisie środka komunikowania, którym posłużenie się kwalifikuje dany typ czynu zabronionego. Po drugie, na taki jedynie możliwy sposób popełnienia typów kwalifikowanych wskazuje właśnie to, że ustawodawca zdecydował się przypadki posłużenia się przy dokonaniu przestępstwa zniesławienia i znieważenia za pomocą środków masowego komunikowania zaliczyć właśnie do typów kwalifikowanych. Uznanie jakiegoś typu za kwalifikowany wskazuje bowiem, iż zdaniem ustawodawcy niesie on ze sobą znacznie poważniejszy ładunek bezprawia w stosunku do typu podstawowego. Niewątpliwie zaś, w przypadku art. 212 § 2 k.k. i art. 216 § 2 k.k., taka postawa ustawodawcy połączona jest z oceną, że wykorzystanie przez sprawcę środków masowego komunikowania się dla realizacji omawianych przestępstw, spowoduje, że treści przez prawo zakazane trafią do szerokiej opinii publicznej i przez to będą miały silniejszy negatywny oddźwięk społeczny. Jak przyjmuje się w literaturze przedmiotu, znamieniem wpływającym na zwiększenie się bezprawia i w konsekwencji zaliczenie danego typu do typu kwalifikowanego jest m.in. popełnienie czynu w szczególnych okolicznościach modalizujących, a więc np. publicznie[3]. Z taką sytuacją mamy do czynienia właśnie w przypadku art. 212 § 2 k.k. i art. 216 § 2 k.k.

Przechodząc do niejako głównego nurtu rozważań, zauważyć należy, że w literaturze słusznie przyjmuje się, iż jednym ze środków masowego komunikowania, o jakim mowa w analizowanych przepisach art. 212 § 2 k.k. i art. 216 § 2 k.k., jest internet.

Za poważny błąd uznać należy jednakże to, iż komentatorzy kodeksu karnego oraz wypowiedzi doktryny dotyczące szeroko rozumianej przestępczości internetowej[4] w części dotyczącej omawianej tu problematyki zniesławienia oraz znieważenia wspominają o internecie jedynie we wskazanym wyżej kontekście, uznając go *ex definitione* za środek masowego komunikowania. W konsekwencji, posłużenie się przez sprawcę internetem dla dokonania przestępstwa zniesławienia lub znieważenia niejako z urzędu traktowane jest jako wyczerpanie przez taką osobę znamion typu kwalifikowanego czynu zabronionego określonego w § 2 art. 212 k.k. i § 2 art. 216 k.k.

Tymczasem sieć internetowa z uwagi na możliwości, jakie oferuje, posiada niejako dwa gatunkowo różniące się od siebie „oblicza". Ze względu na sposób wykorzystania internetu w celu komunikowania się, występuje on jako „środek masowego komunikowania" oraz jako „środek hermetycznej komunikacji interpersonalnej".

---

[3] K. B u c h a ł a, A. Z o l l, Polskie prawo karne, Warszawa 1997, s. 130.
[4] M. S o w a, Ogólna charakterystyka przestępczości internetowej, Palestra 2001, nr 5–6, s. 31.

Jako „środek masowego komunikowania" internet występuje wówczas, gdy wykorzystywany jest w celu przekazywania informacji do ściśle nieokreślonego lub też określonego, ale odpowiednio liczebnego gremium podmiotów, któremu to gremium jesteśmy w stanie przypisać określenie – „wielość odbiorców". Taki charakter internet przybiera np. wtedy, gdy treści zabronione przez art. 212 k.k. i art. 216 k.k. umieszczone zostały przykładowo na forum danego serwisu internetowego lub gdy treści takie umieszczono na witrynie internetowej www (World Wide Web). Dostępne są wtedy nieograniczonej liczbie podmiotów odwiedzających daną stronę internetową. W takim właśnie kontekście internet występuje w przepisach art. 212 § 2 k.k. i art. 216 § 2 k.k. Analiza danego stanu faktycznego, która prowadzi do wniosku, że internet dla popełnienia przestępstwa zniesławienia lub znieważenia użyty został jako środek, który umożliwił dotarcie zakazanej przez te przepisy treści do bliżej nieokreślonej liczby odbiorców lub też określonej ale znaczącej liczby (przestępstwo z art. 212 i 216 k.k. dokonane publicznie), powoduje konieczność uznania tegoż medium w takiej sytuacji za „środek masowego komunikowania", o jakim mowa w art. 212 § 2 k.k. i art. 216 § 2 k.k. W konsekwencji, sprawca w takiej sytuacji realizuje znamiona typu czynu zabronionego w jego postaci kwalifikowanej.

Możliwości, jakie aktualnie oferuje sieć internetowa w zakresie komunikowania się i przekazywania pomiędzy osobami treści informacyjnych, umożliwia wyodrębnienie także drugiej jego „twarzy" – „środka hermetycznej komunikacji interpersonalnej". Chodzi w tym przypadku przede wszystkim o pocztę elektroniczną wykorzystywaną do przesłania pojedynczej osobie lub wąskiej grupie osób (takiej ażeby nie wyczerpywała znamienia „publicznie", o jakim mowa w art. 212 k.k. i art. 216 k.k.) tzw. listu elektronicznego oraz komunikatory internetowe (*instant messenger*). Poczta elektroniczna – inaczej e-mail – to system transmisji wiadomości oraz danych pomiędzy komputerami za pośrednictwem łączy internetowych. Za pomocą e-maili można przesyłać zarówno wiadomości tekstowe, jak i wszelkiego rodzaju pliki komputerowe[5]. Natomiast komunikatory internetowe to oprogramowanie umożliwiające bezpośrednią rozmowę na monitorze komputera z inną osobą w czasie rzeczywistym (popularne GaduGadu, Tlen, Akuku, Gush, Hapi, FomineWinPopup, ICQ, AOL Instant Messenger, Odigo, Hello). Rozmowa odbywa się za pomocą krótkich komunikatów tekstowych. Przekazywanie w ten sposób treści o charakterze zniesławiającym lub znieważającym niczym nie różni się od wysłania określonej osobie tradycyjnego listu napisanego na kartce papieru lub przekazanie mu takowej treści podczas rozmowy „w cztery oczy", czy podczas rozmowy telefonicznej. Jako porównanie można podać przykład popełnienia przestępstwa znieważenia przez wysła-

[5] *Ibidem,* s. 26.

nie zwykłego listu drogą pocztową oraz wysłanie listu e-mail drogą elektroniczną. Długopisem staje się klawiatura, kartką papieru ekran monitora komputerowego, numerem domu adresata adres jego skrzynki pocztowej, a listonoszem przewody czy światłowody. Komputery tworzące sieć internet spełniają po prostu rolę przekaźników informacji w stosunku do wysłanego listu elektronicznego, tak jak odpowiednio Poczta Polska jest pośrednikiem w doręczaniu danego materialnego listu. Oczywiście chodzi o takie wykorzystanie wskazanych wyżej narzędzi internetowych, które nie ma charakteru „publicznego" przekazania informacji, a więc nie wchodzi w obszar typów kwalifikowanych zawartych w art. 212 § 2 k.k. i art. 216 § 2 k.k. W sytuacji, gdy warunek ten zostanie spełniony, posłużenie się internetem we wskazany wyżej sposób do przekazania treści zniesławiających lub znieważających nie uczyni z tego medium „środka masowego komunikowania", albowiem treści przekazywane za jego pośrednictwem nie są kierowane do takiej grupy osób, która powodowałaby, że zniesławienie lub znieważenie nastąpiły „publicznie". Treści te, w takiej sytuacji, kierowane są do ściśle określonej osoby lub wąskiej grupy osób (np. e-mail do zarządu spółki). Wykorzystanie przez sprawcę internetu jako „środka hermetycznej komunikacji interpersonalnej" podczas popełnienia przestępstwa zniesławienia lub znieważenia powoduje, że zachowanie jego wyczerpuje znamiona przestępstwa z art. 212 § 1 k.k. lub art. 216 § 1 k.k. Internet wykorzystany do takiej komunikacji nie staje się więc narzędziem kwalifikującym typ czynu zabronionego i posłużenie się nim wyczerpuje znamiona typu podstawowego omawianych przestępstw. Ma to ogromne znaczenie praktyczne dla zastosowania odpowiedniej kwalifikacji prawnej danego czynu. Przekłada się to bezpośrednio na sytuację procesową sprawcy, albowiem typ kwalifikowany zarówno przestępstwa zniesławienia, jak i znieważenia, jest zagrożony odpowiednio wyższymi w stosunku do podstawowego sankcjami karnymi.

Reasumując, przeprowadzone powyżej rozróżnienie wydaje się jak najbardziej uzasadnione. Zaliczenie internetu – w jednej z jego postaci – do „środków masowego komunikowania" wymuszających typ kwalifikowany czynu zabronionego podyktowane jest posiadaniem przez takie środki (oprócz internetu zalicza się tu również radio, prasę, telewizję, czy nawet rozplakatowanie zakazanych treści w miejscach powszechnie dostępnych[6]) niezwykle szerokiego pola rażenia przejawiającego się w możliwości dotarcia z przekazem informacyjnym do praktycznie nieograniczonej liczby osób. Z drugiej jednakże strony, internet daje możliwość komunikacji indywidualnej, pozbawionej charakteru masowości odbiorców przekazywanych treści. W takiej sytuacji internet wymyka się z ram znamienia „środek masowego komunikowania" i staje się innym gatunkowo środkiem umożliwiającym ko-

[6] A. Z o l l, Komentarz..., s. 647.

munikowanie się – staje się „środkiem hermetycznej komunikacji interpersonalnej".

II. Zagadnienia karnoprocesowe

Zarówno przestępstwo zniesławienia, jak i znieważenia, należą do grupy przestępstw prywatnoskargowych. Biorąc pod uwagę ich charakter, ustawodawca w rozdziale 52 k.p.k. zatytułowanym „Postępowanie w sprawach z oskarżenia prywatnego" przewidział dla nich szczególny tryb postępowania. Charakteryzuje się on w szczególności tym, że uprawnienia oskarżyciela wykonuje sam pokrzywdzony, względnie osoby, które mogą działać za pokrzywdzonego. Pokrzywdzony może sam wnosić i popierać akt oskarżenia aż do upływu okresu przedawniania ścigania danego przestępstwa.

W rozdziale 52 k.p.k. unormowane są dwie z trzech możliwości przeprowadzenia postępowania. Po pierwsze, pokrzywdzony może skierować uproszczony akt oskarżenia (spełniający wymagania formalne określone w przepisie art. 487 k.p.k.) bezpośrednio do właściwego sądu, który od tej chwili staje się gospodarzem postępowania i podejmuje przewidziane prawem czynności. Po drugie, pokrzywdzony może skierować ustną lub pisemną skargę bezpośrednio do Policji, która zgodnie z treścią art. 488 § 1 k.p.k. w razie potrzeby zabezpiecza dowody, po czym przesyła tą skargę do właściwego sądu. Trzecią z kolei drogą ścigania przestępstw z oskarżenia prywatnego jest droga z aktywnym udziałem prokuratora, który na mocy art. 60 k.p.k. z uwagi na interes społeczny wszczął postępowanie lub wstąpił do postępowania już wszczętego. Z chwilą ingerencji prokuratora postępowanie toczy się z urzędu.

Przedstawione poniżej rozważania dotyczyć będą jedynie dwóch pierwszych z przedstawionych powyżej trzech możliwości postępowania w sprawach o przestępstwa ścigane z oskarżenia prywatnego. Ten sposób postępowania w sprawach z oskarżenia prywatnego – odnośnie przestępstw z art. 212 k.k. i art. 216 k.k. popełnionych „przez internet" – niesie ze sobą szereg problemów, które w konsekwencji mogą niweczyć samą zasadność prowadzenia takiego postępowania w tych sprawach.

Na wstępie, pokrótce i w konsekwencji ogólnie, przedstawić należy podstawowe techniczne zasady korzystania z internetu w aspekcie interesujących nas kwestii.

Na serwerach portali internetowych znajdują się liczne serwisy typu forum, listy dyskusyjne, czaty, księgi gości, blogi itp., w których wprowadzane przez użytkownika treści (opinie, poglądy, informacje itp.) stają się publicznie dostępne dla nieograniczonej liczby osób. Użytkownik może publikować swoje treści w tych serwisach w zasadzie w sposób dowolny, sam decydując o tym, jak mają one być podpisywane. Zazwyczaj jest to pseudonim, zwany

w żargonie sieciowym „nick-iem". Zapewnia to poczucie całkowitej anonimowości, dając zarazem użytkownikom internetu poczucie swoistej bezkarności. Wynikające z ogólnej zasady połączeń realizowanych w internecie informacje zawarte w logach systemowych (takie jak np. adres IP), będące pomocne w ustaleniu sprawcy, są przez administratorów serwerów przechowywane i wykorzystywane głównie w celach technicznych oraz administracyjnych. Również dane konieczne do założenia elektronicznego konta pocztowego – adresu e-mail czy komunikatora internetowego nie są weryfikowane co do ich prawdziwości i nie są ujawniane osobom trzecim.

Każdy komputer podłączony bezpośrednio do internetu ma przypisany swój indywidualny, niepowtarzalny w danej chwili, adres IP (Internet Protocol Adress). Adres ten, co do zasady, składa się z czterech 8-bitowych członów, z których każdy może przybierać wartości od 0 do 255 (np. 83.17.115.14). Jest to niejako „numer rejestracyjny" danego komputera. Każdy z członów w takim adresie oznacza co innego i pozwala na zakreślenie coraz to mniejszego obszaru, w którym można poszukiwać dany komputer. Zatem poprzez jeden człon odnajdziemy określoną sieć, poprzez następny odnajdziemy mniejszą sieć, już w ramach tej dużej sieci, i następnie któryś z komputerów w tej sieci. Taka struktura wynika ze specyfikacji protokołu IP. Pule (zakresy) adresów IP tworzących tzw. klasy, które są przydzielane firmom będących dostarczycielami połączeń internetowych (ISP – Internet Service Provider). Ze względu na swoją chwilową unikalność – adres IP w połączeniu z dokładnym określeniem czasu – jednoznacznie identyfikuje urządzenie w sieci Internet oraz firmę, z której puli pochodzi[7]. Do odczytania konkretnego adresu IP potrzebne są natomiast logi systemowe (cyfrowe) serwerów internetowych. Log systemowy jest informacją, jaką przekazuje serwerowi komputer przy każdym połączeniu z siecią Internet.

Logi te rejestrują dane na temat aktywności sieciowej swoich klientów i pozwalają stwierdzić, z jakimi miejscami w sieci się łączyli, dokąd wysyłali wiadomości, skąd i kiedy je otrzymywali, oraz jakiego rodzaju transakcji dokonywali. Przykładowo można wymienić: transfer plików (wysyłanie i ściąganie), udział w grupie dyskusyjnej czy wejście na daną stronę www. Pliki rejestrów są generowane przez dostawców dostępu do Internetu i zawierają dane, które stanowić mogą „elektroniczny trop" sprawcy przestępstwa popełnionego za pomocą komputera. Ma to szczególnie istotne znaczenie w przypadku użytkowników internetu, którzy nie są na stale włączeni do sieci, lecz korzystają z tzw. protokółów komunikacyjnych umożliwiających im doraźne połączenie z internetem przy pomocy modemu i linii telefonicznej. Z chwilą nawiązania połączenia modemowego z dostawcą dostępu do inter-

[7] M. Kliś, A. Stella-Sawicki, Identyfikacja użytkownika komputera na podstawie logów cyfrowych, Prokuratura i Prawo 2001, nr 7–8, s. 52.

netu, jego serwer automatycznie przyznaje abonentowi tej usługi adres IP z tzw. puli adresowej będącej w dyspozycji dostawcy internetu[8]. Sygnał z informacjami przesyłany jest, mniej więcej, za pomocą tych samych elementów, co rozmowa telefoniczna. Za każdym razem, gdy posiadacz modemu chce połączyć się z internetem, operator sieci telefonicznej przydziela mu numer IP. Jest to numer, który nie jest przypisany raz na zawsze jakiemuś użytkownikowi. Oddawany jest jedynie danemu użytkownikowi na czas jego aktywności w sieci. W takiej sytuacji, aby określić jaki komputer korzystał z danego adresu IP, należy przyporządkować datę i godzinę korzystającemu z takiego adresu IP. Tym samym wszelka aktywność danego komputera w sieci będzie związana właśnie z jego adresem IP.[9]

Pomocnym w ustaleniu powyższego są tzw. bilingi, które zawierają informację o numerze stacji abonenta, adresie abonenta, liczbie jednostek taryfikacyjnych zaliczonych na rzecz danej stacji w przyjętym okresie rozliczeniowym, numerach, z którymi abonent uzyskał połączenie, dacie uzyskania i czasie trwania połączenia oraz o jego rodzaju (międzynarodowe, krajowe, lokalne, czy właśnie połączenie z internetem). Operator jest zobowiązany do rejestracji danych wykonanych usług telekomunikacyjnych, w zakresie umożliwiającym ustalenie należności za wykonanie tych usług[10].

Należy w tym miejscu nadmienić, że również niektóre z komputerowych sieci lokalnych korzystają z mechanizmu tzw. dynamicznej alokacji adresu IP, a więc przydzielanej na dane połączenie z siecią Internet. Fakt ten może utrudniać zestawienie danego adresu IP z konkretnym komputerem, który w chwili bycia w sieci go używał. Dane bilingowe, jako informacje dotyczące zrealizowanych połączeń telekomunikacyjnych pomiędzy stacjami abonenckimi, objęte są tajemnicą komunikacyjną wynikającą z ustawy – Prawo telekomunikacyjne z dnia 16 lipca 2004 r.[11]. Ujawnienie tych informacji objętych tajemnicą może nastąpić jedynie mocą postanowienia sądu, prokuratora lub na podstawie odrębnych przepisów.

Każdy użytkownik sieci internet może ponadto, bez większych problemów, stworzyć własną stronę www, a także umieścić ją w sieci oraz prezentować na niej dowolne treści, w tym zniesławiające czy znieważające inną osobę.

Strony www to obszerny zbiór powiązanych odsyłaczami dokumentów oraz innych plików umiejscowionych na komputerach połączonych poprzez Internet, umożliwiający dostęp, użytkowanie oraz kopiowanie informacji, danych oraz programów. Strony te, aby były dla innych użytkowników sieci internet dostępne, muszą zostać zapisane w postaci pliku komputerowego

[8] A. A d a m s k i, Prawo karne komputerowe, Warszawa 2000, s. 204 i n.
[9] M. K l i ś, A. S t e l l a - S a w i c k i, Identyfikacja..., s. 53.
[10] A. L a c h, Dowody elektroniczne. Pojęcia i klasyfikacja, Security Magazine 2001, nr 4, s. 24.
[11] Dz. U. z 2004 r., Nr 171, poz. 1800.

na twardym dysku serwera, czyli komputera nie będącego, w zdecydowanej większości przypadków, własnością autora strony. Miejsce na serwerach udostępniane jest przez szereg firm odpłatnie, ale także nieodpłatnie[12].

Pokrzywdzony może sam „na własną rękę" próbować podjęcia czynności zmierzających do wykrycia sprawcy przestępstwa znieważenia bądź zniesławienia. Wybierając jednakże taką drogę, skazany jest niejako już „z góry" na niepowodzenie.

Tak więc pokrzywdzony przez innego użytkownika sieci znać może co najwyżej jedynie jego internetowy pseudonim, adres poczty elektronicznej lub numer komunikatora internetowego. W celu uzyskania adresu IP, bądź danych osobowych danego użytkownika konkretnego adresu IP, który zrealizował, posługując się internetem, znamiona przestępstwa z art. 212 k.k. lub 216 k.k., pokrzywdzony musi podjąć dalsze kroki. Przede wszystkim należy zwrócić się do administratora serwera, na którego przykładowo forum został umieszczony obraźliwy wpis i żądać ujawnienia adresu IP przyporządkowanego danemu wpisowi. Z uwagi na fakt, iż w zdecydowanej większości przypadków administrator serwera nie będzie posiadał oprócz adresu IP dalszych danych osobowych (imię i nazwisko, adres) użytkownika określonego adresu IP należy w celu ich uzyskania zwrócić się do dostawcy internetu dla tegoż adresu IP, aby udostępnił takie dane. Dane te chronione są ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 r.[13].

Zgodnie z art. 29 ust. 1–3 tejże ustawy dane osobowe mogą być udostępnione osobom trzecim, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Dane te udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek ten powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Jednakże art. 30 wskazanej ustawy upoważnia administratora danych osobowych do odmowy udostępnienia tych danych. Należy przy tym zaznaczyć, że dla czynności tej nie jest przewidziana forma decyzji administracyjnej ani postanowienia. Odmowa następuje w formie pisma, które nie jest także aktem lub czynnością z zakresu administracji publicznej, dotyczącymi przyznania, stwierdzenia albo uznania uprawnienia lub obowiązku wynikających z przepisów prawa. W razie takiej odmowy pokrzywdzony ma prawo zainicjowania postępowania przed Generalnym Inspektorem Ochrony Danych Osobowych, które to postępowanie, jak wynika z art. 18 ustawy, jest szczególnym i jedynym trybem orzekania w sprawach z zakresu danych osobo-

[12] M. S o w a, Odpowiedzialność karna sprawców przestępstw internetowych, Prokuratura i Prawo 2002, nr 4, s. 44.
[13] Dz. U. z 1997 r., Nr 133, poz. 883.

wych[14]. W przypadku negatywnej dla pokrzywdzonego decyzji GIODO pozostaje skarga do Wojewódzkiego Sądu Administracyjnego.

Dużo poważniejszy problem powstaje dla pokrzywdzonego, gdy osoba szkalująca jego dobre imię łączyła się z siecią internet przy pomocy modemu i linii telefonicznej, uzyskując chwilowy adres IP. W tym przypadku konieczne jest zwrócenie się do operatora telekomunikacyjnego celem uzyskania danych billingowych, które chronione są jednak tajemnicą telekomunikacyjną. W takim przypadku pokrzywdzony może więc dysponować jedynie adresem IP, który jest niewystarczający do wniesienia uproszczonego aktu oskarżenia. Zgodnie z treścią przepisu art. 487 k.p.k. taki akt oskarżenia zawierać musi co najmniej oznaczenie osoby oskarżonego, opis zarzucanego mu czynu, a także wskazanie dowodów na poparcie oskarżenia. Oznaczenie osoby oskarżonego powinno być takie, aby można było zindywidualizować tę osobę i móc doręczyć jej wezwanie na rozprawę, a więc powinno zawierać imię, nazwisko i adres oskarżonego[15]. Zarówno adres IP, jak i adres poczty internetowej, taką indywidualizacją osoby oskarżonego nie jest, co w konsekwencji powoduje bezskuteczność takiego aktu oskarżenia.

W tym miejscu przejdźmy do zasadniczego problemu, czyli do sytuacji, gdy pokrzywdzony jako drogę dochodzenia swoich praw wybiera złożenie skargi na Policję w trybie art. 488 § 1 k.p.k.

Skarga ta w odróżnieniu od uproszczonego aktu oskarżenia nie musi zawierać danych osoby sprawcy czynu zabronionego, którego ustalenie jest rolą właśnie Policji. W tym celu Policja nie wszczyna sformalizowanego postępowania przygotowawczego, dochodzenia czy śledztwa, nie prowadzi również postępowania w niezbędnym zakresie ani postępowania sprawdzającego, lecz podejmuje czynności procesowe, z zachowaniem wszelkich rygorów przewidzianych w k.p.k., mające za zadanie zabezpieczenie dowodów.

Zabezpieczanie dowodów może być połączone z poszukiwaniem dowodów oraz podejmowaniem przez Policję czynności zmierzających do wykrycia sprawcy przestępstwa[16].

Należy podkreślić, że k.p.k. nie określa wprost jakie konkretne czynności w ramach uprawnienia wynikającego z art. 488 § 1 k.p.k. Policja może podejmować. Mając na względzie wykładnię systemową wydaję się, że ustawodawca wprowadził pewną gradację uprawnień organów w zależności od rodzaju postępowania (oczywiście chodzi o sytuacje przed wstąpieniem

[14] Por. Wyrok Naczelnego Sądu Administracyjnego – Ośrodek Zamiejscowy w Katowicach z dnia 19 listopada 2001 r., II SA/Ka 346/2000, opubl. LEX.

[15] T. Grzegorczyk, Kodeks postępowania karnego. Komentarz, Kantor Wydawniczy Zakamycze, Kraków 2004, s. 1245.

[16] R. A. Stefański, (w:) Kodeks postępowania karnego. Komentarz, Z. Gostyński (red.), Warszawa 2004, s. 403.

w fazę sądową). Najszersze uprawnienia procesowe związane są z prowadzeniem śledztwa, nieco mniejsze przy dochodzeniu. Natomiast w postępowaniu w niezbędnym zakresie czy postępowaniu sprawdzającym napotykamy już na liczne ograniczenia przedmiotowe. Idąc tym tokiem myślenia, dochodzimy do konkluzji, że czynności procesowe wykonywane przez Policję na podstawie art. 488 § 1 k.p.k. mają najmniejszy zakres przedmiotowy.

W literaturze wymienia się tu przykładowo: legitymowanie osoby wskazanej przez pokrzywdzonego, ustalenie jej tożsamości i adresu, oględziny miejsca przestępstwa lub ciała, ustalenie nazwisk i miejsca zamieszkania świadków, przesłuchanie świadków, zwłaszcza tych, którzy nie będą mogli złożyć zeznań na rozprawie, np. z powodu wyjazdu za granicę[17]. Generalnie, stwierdzić należy, iż chodzi o takie czynności, których nie może wykonać sam pokrzywdzony, a które zrealizować może Policja w ramach swych kompetencji. Co więcej, jak wynika z samej istoty przepisu art. 488 § 1 k.p.k., czynności te powinny być wykonane przez Policje w jak najkrótszym czasie od momentu wystąpienia potrzeby ich realizacji.

Wydaje się zatem, że w ramach uprawnień z art. 488 § 1 k.p.k. nie jest dopuszczalne podejmowanie czynności, które wymagają jakiejkolwiek decyzji prokuratora. W artykule tym prezentowany jest pogląd, iż w sytuacji, gdy pokrzywdzony wybiera – jak to określono wyżej – drugą drogę postępowania, a więc decyduje się na złożenie skargi bezpośrednio do Policji, wyłączona jest jakakolwiek aktywność prokuratora przy podejmowaniu czynności zmierzających do wykrycia sprawcy przestępstwa ściganego z oskarżenia prywatnego. Prokurator, zgodnie z brzmieniem art. 60 k.p.k., może tu zaistnieć tylko i wyłącznie wtedy, gdy doszuka się w swojej ingerencji interesu społecznego. Istotą postępowania określonego w rozdziale 52 k.p.k. jest bowiem brak udziału w nim w jakiejkolwiek postaci prokuratora. Gdyby uznać, że prokurator może podjąć jakąkolwiek czynność w takim postępowaniu (np. wydanie postanowienia o przeszukaniu, czy postanowienia o zwolnieniu z tajemnicy służbowej), musiałoby się to wiązać z uprzednim uznaniem przez niego, że istnieje interes społeczny w takiej interwencji. Dokonanie przez niego takiej nawet tylko jednostkowej czynności byłoby *de facto* poprzez czynność faktyczną daniem wyrazu, że zachodzą przesłanki do jego ingerencji w ramach art. 60 k.p.k. Oznaczałaby to automatyczne wkroczenie postępowania na drogę postępowania z urzędu (art. 60 § 2 k.p.k.) i wyjście poza zakres wskazanej „drugiej" drogi postępowania, co ostatecznie wypaczałoby istotę unormowania art. 488 § 1 k.p.k. Zaakceptowanie takiej ingerencji prokuratora doprowadziłoby do niedopuszczalnych konsekwencji. Mianowicie, z „postępowania" określonego w art. 488 § 1 k.p.k., które w swym założeniu konstruowane było jako „postępowanie"

[17] *Ibidem*, s. 403.

szybkie i odformalizowane, zrobiłoby się nam rzeczywiste postępowanie, ograniczone jedynie terminem przedawnienia, w którym można by podejmować każdą dowolną czynność (z uwagi na „cichy" udział prokuratora) i które w istocie niczym nie różniłoby się od postępowania zwyczajnego, a nawet wykraczałoby zdecydowanie poza jego gwarancyjne uregulowania. Tak więc, czynności z art. 488 § 1 k.p.k. prowadzi tylko i wyłącznie Policja, bez nadzoru i jakiegokolwiek udziału prokuratora. Przemawia za tym również fakt, iż postępowanie prywatnoskargowe jest szczególnym rodzajem postępowania sądowego, które – jak to wskazano wyżej – co do zasady wyłączać ma udział prokuratora, zostawiając samemu pokrzywdzonemu dążenie do pociągnięcia do odpowiedzialności karnej za określone przestępstwa.

Wobec powyższego nie tylko sam pokrzywdzony, ale również Policja po przyjęciu skargi pokrzywdzonego w trybie art. 488 § 1 k.p.k., nie mają procesowych możliwości zdobycia wykazu połączeń telekomunikacyjnych, czyli bilingu, a w konsekwencji ustalenia danych osobowych abonenta – internauty korzystającego z modemu i linii telefonicznych, a chronionych tajemnicą telekomunikacyjną. Z tajemnicy takiej zwolnić może w tym przypadku jedynie prokurator, którego udział w tak prowadzonym postępowaniu – o czym wyżej – jest wyłączony i nie może on wykonywać w nim jakichkolwiek czynności.

Idąc dalej, stwierdzić należy, że zarówno adres IP komputera, adres poczty elektronicznej, numer komunikatora internetowego, jak również numer abonenta sieci telekomunikacyjnej w przypadku łączenia się z siecią internet przez modem, stanowią dane mogące stać się bardzo wartościowymi dowodami w postępowaniu karnym, które przy tego rodzaju postępowaniach, z uwagi na ich specyfikę (internet), w większości przypadków są praktycznie jedyną drogą prowadzącą do zidentyfikowania sprawcy.

Ustalenie numeru stacji abonenckiej lub identyfikatora serwera, z których zainicjowano połączenie lub przesłano wiadomość, nie zawsze jest wystarczająca do identyfikacji konkretnej osoby nawiązującej dane połączenie, jak również nie przesądza o prawdziwości adresu nadawcy wiadomości przesłanej pocztą elektroniczną.

Możliwość manipulowania danymi transakcyjnymi, które zawiera nagłówek komunikatu e-mail, są praktycznie nieograniczone, a techniki „podszywania się w poczcie elektronicznej" są szeroko opisane w literaturze przedmiotu. Ponadto, korzystanie z dostępnych w internecie tzw. anonimowych remailerów, które usuwają z nagłówka komunikatu e-mail oryginalne dane adresowe – pozwala osobie przesyłającej wiadomość na zachowanie całkowitej anonimowości[18]. Zatem w niektórych przypadkach koniecznie jest zestawienie z innymi dowodami, które pozwolą na identyfikację sprawcy. Pewnym sposobem zdobycia pozostałych dowodów może być przeszukanie

[18] A. A d a m s k i, Prawo ..., s. 198.

pomieszczeń i zatrzymanie znajdujących się w nich komputerów lub nośników informacji, celem odczytania i utrwalenia znajdujących się w pamięci dyskowej komputera danych.

Szczególne problemy mogą pojawić się w przypadku systemu komputerowego składającego się z wielu stacji roboczych, serwerów i urządzeń służących do archiwizowania danych, które służą do prowadzenia przykładowo działalności gospodarczej, czy znajdują się w miejscu, gdzie z komputerów przyłączonych do sieci pracuje wiele osób. Często w przypadku rozbudowanych sieciach korporacyjnych, w których istnieje duża liczba podłączonych komputerów, to jednym z najczęstszych sposobów zapewnienia bezpieczeństwa danych jest oddzielenie komputerów wewnętrznych od internetu za pomocą serwera *firewall*. Jest to komputer, którego adres IP jest widoczny na zewnątrz, a wszelka komunikacja między komputerami zabezpieczonymi w ten sposób a siecią odbywa się za jego pośrednictwem, poprzez tzw. serwer *proxy*. Bezpośrednim skutkiem takiej konfiguracji jest zarówno niemożność nieautoryzowanego dostępu do sieci wewnętrznej, jak i braku dokładnej informacji w logach serwera o adresie IP komputera, który korzystał z jakiejś usługi na tym serwerze, np. zamieścił znieważający wpis na forum. W logach zostanie bowiem zapisany adres IP serwera *firewall*. Przedstawiając te sytuację obrazowo, to jeśli ktoś z pracowników danej firmy czy użytkowników takiej sieci ukrytej za *firewallem* chce połączyć się choćby z jakąś witryną www, to serwer zarządzający tą stroną i notujący adres IP, z którego pochodzi określone żądanie, zanotuje adres IP tego serwera *proxy*, a nie adres IP konkretnego komputera pracownika czy użytkownika. Adres ten pozostanie po prostu nie ujawniony. W każdym zatem takim przypadku należy dokładnie poddać badaniom komputery znajdujące się pod serwerem *proxy*[19]. Zatrzymanie niekiedy dużej ilości komputerów, o ile jest to technicznie możliwe, naruszać będzie zasadę proporcjonalności, a badanie ich zawartości będzie kosztowne i w naszych realiach czasochłonne. Alternatywą dla zatrzymania komputera jest skopiowanie całej zawartości jego twardego dysku i zabezpieczenie do dalszych badań kryminalistycznych[20]. Trzeba mieć również na uwadze fakt, że log systemowy, identyfikujący adres IP komputera, nie może stanowić dowodu, jeśli został wykorzystany przez hakera jako pośrednik do przestępnego działania, przez co wykrycie sprawcy stanie się jeszcze bardziej skomplikowane.

Kodeks postępowania karnego zastrzega decyzję o zatrzymaniu rzeczy i o przeszukaniu właściwości sądu lub prokuratora, dopuszczając tylko wyjątkowo, w wypadkach nie cierpiących zwłoki, niezbędne działania Policji lub innego organu (art. 217 k.p.k. i art. 220 k.p.k.). Jedynie w przypadkach nie-

[19] M. Kliś, A. Stella-Sawicki, Identyfikacja..., s. 61 i n.
[20] Por: A. Adamski, Prawo..., s. 208.

cierpiących zwłoki przepis art. 220 § 3 k.p.k. dopuszcza wyjątkowy tryb przeszukania. Może być ono przeprowadzane przez Policję bez postanowienia prokuratora lub sądu o przeszukaniu wyłącznie na podstawie nakazu kierownika jednostki Policji lub legitymacji służbowej. Następnie Policja ma zwrócić się niezwłocznie do prokuratora lub sądu celem zatwierdzenia przeszukania. Nadto, postanowienie sądu lub prokuratora w przedmiocie zatwierdzenia należy doręczyć także osobie, u której dokonano przeszukania, w terminie 7 dni od daty czynności na zgłoszone do protokołu żądanie tej osoby. Również w sytuacjach szczególnych z żądaniem wydania rzeczy może wystąpić Policja lub inny uprawniony organ, także wówczas, gdy nie dysponuje postanowieniem sądu lub prokuratora. Gwarancją legalności zatrzymania rzeczy, dokonanego przez Policję lub inny uprawniony organ na podstawie nadzwyczajnego uprawnienia przewidzianego w przepisie art. 217 § 4 k.p.k., jest określony tryb zatwierdzania tej czynności przez sąd lub prokuratora[21]. Należy przy tym wyraźnie podkreślić, że w przypadku zniesławienia bądź znieważenia przez internet trudno mówić o wystąpieniu wypadku niecierpiącego zwłoki, który usprawiedliwiałby Policję do zastosowania tego wyjątkowego trybu przeszukania.

Tak więc niejako nieodzowny jest udział prokuratora w tych czynnościach (postępowanie nie jest jeszcze w stadium jurysdykcyjnym, więc działanie sądu jest tu wyłączone).

Zatem, jeżeli uznajemy, że w ramach uprawnień z art. 488 § 1 k.p.k. nie jest możliwe podejmowanie przez Policję czynności, które wymagają decyzji prokuratora, to zarówno przeszukanie, jak i zatrzymanie rzeczy w trybie czynności podejmowanych na podstawie art. 488 § 1 k.p.k., są prawnie niedopuszczalne. Podobnie jak nie jest możliwe uzyskanie postanowienia o zwolnieniu z tajemnicy służbowej.

W tym świetle ustalenie sprawcy przestępstwa znieważenia bądź zniesławienia i pociągnięcie go do odpowiedzialności karnej jest w pewnych przypadkach niemożliwe.

Pociągnięcie do odpowiedzialności karnej jest również niemożliwe, gdy sprawca korzystał z sieci internet z popularnych kafejek internetowych. Mimo faktu, że sprawca nie został wykryty w trybie czynności z art. 488 § 1 k.p.k., Policja ma ustawowy obowiązek przesłać skargę sądowi. Skarga ta, jako zawierająca braki formalne, będzie oczywiście bezskuteczna.

III. Zakończenie

[21] W. G r z e s z c z y k, Kodeks postępowania karnego. Komentarz, Warszawa 2003, s. 600 i n.

Wskazana w niniejszym artykule istota popełniania przestępstw zniesławienia i znieważenia za pośrednictwem tak szczególnego medium, jakim jest internet, powoduje, że bez czynności procesowych w postaci zwolnienia z tajemnicy służbowej lub przeszukania i zatrzymania sprzętu komputerowego celem poddania go ekspertyzie kryminalistycznej, ustalenie sprawcy w przeważającej większości przypadków jest niemożliwe.

Wymienione czynności, pozwalające na wykrycie sprawcy, wymagają jednakże udziału prokuratora. W ramach art. 488 § 1 k.p.k., co wskazano wyżej, nie jest natomiast dopuszczalne podejmowanie czynności procesowych wymagających decyzji prokuratora. Teoretycznie wydaje się więc, że rozwiązaniem jest uznanie przez prokuratora, iż z uwagi na powyżej wykazaną „nieporadność procesową" pokrzywdzonego zachodzi interes społeczny, o jakim mowa w art. 60 k.p.k., co pociąga za sobą jego ingerencję w postępowanie prywatnoskargowe.

Pamiętać jednak należy, że interes społeczny jest zawsze kategorią ocenną i w sytuacji, gdy prokurator nie uzna, że w danej sytuacji zachodzi interes społeczny, to pokrzywdzony – z uwagi na przedstawione problemy z wykryciem sprawcy – traci faktyczną możliwość skutecznej ochrony swoich praw.

W związku z powyższym zachodzi potrzeba zmiany uregulowań kodeksowych, która pozwoliłaby wyeliminować wskazane w niniejszym artykule problemy. Konieczne zatem jest dodanie § 5 do art. 60 k.p.k. w brzmieniu: „W sytuacji gdy prokurator nie znajduje podstaw do wszczęcia postępowania lub wstąpienia do już wszczętego postępowania, może na wniosek Policji wydawać postanowienia, które są niezbędne dla realizowanych przez nią czynności w trybie art. 488 § 1 k.p.k.".