eBook

WIEDZA i PRAKTYKA

Odpowiedzialność karna informatyka



odpowiedzialność PRAWNA w IT

RAPORTY

Odpowiedzialność administratora za treści umieszczane na stronie internetowej 4

Policja i prokuratura może zażądać zarówno danych, jak również sprzętu stanowiącego dowód w sprawie 6

Samodzielne ustalenie sprawcy może być dowodem w sprawie 7

Dostęp do danych, których nie zabezpieczono żadnymi środkami, nie jest przestępstwem 9

Brak ochrony utrudnia dochodzenie odszkodowania w przypadku cyberwłamania 12

Negatywne pozycjonowanie stron internetowych jest uznawane za czyn nieuczciwej konkurencji 14

Nieetyczne działanie naraża informatyka na wyższą odpowiedzialność 15

Pozycjonowanie strony na nazwę konkurencyjnej firmy jest zagrożone odpowiedzialnością karną 17

Naruszenie bezpieczeństwa informacji nie jest ściągane z urzędu, ale na wniosek poszkodowanego 21

E-mail może być dowodem w sprawie, jeśli jego treść da się zweryfikować 22

Skanowanie portów i całych podsieci może być niezgodne z prawem 23

AUTORZY

Łukasz Bazański
radca prawny, itB Legal Kancelaria Radcy Prawnego

Paweł Gutowski
adwokat, Czyżewscy kancelaria adwokacka

Justyna Plechowska-Łukowska
prokurator

Marcin Sarna
radca prawny

Marcin Szeliga

Microsoft Most Valuable Professional

Odpowiedzialność administratora za treści umieszczane na stronie internetowej

Tylko w określonych sytuacjach administrator jest zobowiązany do zareagowania i usunięcia bezprawnych danych ze strony internetowej, którą zarządza.

Wielu użytkowników korzysta z wolności słowa i komunikacji, czemu sprzyja anonimowość w Internecie. W takich sytuacjach pojawia się problem odpowiedzialności za kontrolowanie publikowanych treści oraz eliminację tych, które naruszają prawo.

Usługodawca nie ma obowiązku kontrolowania treści publikowanych na jego stronach internetowych czy też przekazywanych za pośrednictwem utrzymywanej przez niego sieci. Co więcej, nie ma też obowiązku wdrożenia oprogramowania monitorującego. Argumentem, którym uzasadnia się wprowadzenie takiego rozwiązania w prawie, jest duża problematyczność bieżącego monitoringu zawartości stron. Kwestia ta w szczególności dotyczy sieci operatorskich czy stron internetowych z treściami tworzonymi przez użytkowników (ang. user generated content), jak portale społecznościowe, platformy dyskusyjne czy serwisy internetowe z możliwością komentowania artykułów. W wymienionych przypadkach ilość treści jest tak duża, że ich monitorowanie wymagałoby zaangażowania niewspółmiernych środków.

Zgodnie z prawem administrator strony nie jest odpowiedzialny za treści na niej umieszczane, dopóki nie wie o bezprawnym charakterze danych przechowywanych w podlegających mu serwisach internetowych lub o związanej z tymi danymi bezprawnej działalności. Jego odpowiedzialność powstaje wtedy, gdy otrzyma urzędowe zawiadomienie, np. postanowienie sądu lub prokuratury z żądaniem ujawnienia danych osobowych użytkownika, wyrok nakazujący usunięcie treści itp.

Niewiedza zwalnia z odpowiedzialności

Takie same skutki ma otrzymanie wiarygodnej wiadomości o bezprawnym charakterze danych, tj. gdy administrator dowie się o tym, że przechowuje dane naruszające czyjeś dobra (np. w serwisie są obraźliwe komentarze, zdjęcia, pliki naruszające prawa autorskie).

W wymienionych sytuacjach, aby zwolnić się od odpowiedzialności, należy niezwłocznie uniemożliwić dostęp do tych danych za pośrednictwem strony internetowej. Osoba, której prawa zostały naruszone w sieci, może wystąpić bezpośrednio do administratora serwisu internetowego z żądaniem usunięcia informacji z serwisu i ujawnienia danych osobowych użytkowników, którzy te dane zamieścili.

Zakres odpowiedzialności administratora

Jeżeli administrator nie usunie w odpowiednim czasie kwestionowanych danych, poszkodowana osoba może wystąpić do sądu o zadośćuczynienie lub naprawienie szkody. W wyniku przeprowadzenia postępowania sądowego na administratora może zostać nałożony obowiązek naprawienia tej szkody lub zapłaty zadośćuczynienia za doznaną krzywdę.

TYTUŁ RAMKI

W przypadku pisma z żądaniem usunięcia z serwisu danej treści lub podania danych osobowych autora tego wpisu administrator musi ocenić, czy wystąpienie to należy uznać za wiarygodną wiadomość oraz czy może ona stanowić podstawę do usunięcia materiałów z portalu czy też legalnego przekazania danych osobowych użytkownika. Administrator może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Pamiętać należy, że w takich sytuacjach odpowiedzialny jest podmiot pełniący funkcję administratora. Jeżeli administratorem jest np. spół-

ka z ograniczoną odpowiedzialnością lub inna spółka, sąd nałoży obowiązek na ten podmiot reprezentowany przez upoważnione do tego osoby. Odpowiada zatem osoba reprezentująca dany podmiot, a nie jej pracownik (np. informatyk lub pracownik działu IT, którzy zatrudnieni są w celu wykonywania czynności technicznych, lub bezpośrednio administrują daną stroną internetową). Konkretna osoba mogłaby ponieść odpowiedzialność wtedy, gdyby udowodniono, że to ona osobiście umieściła dane treści na stronie. Jednak wtedy nie byłaby to odpowiedzialność administratora za treści umieszczone przez inne osoby, ale odpowiedzialność indywidualna sprawcy.

Nie wszyscy ponoszą odpowiedzialność

Mamy do czynienia z trzema kategoriami podmiotów świadczących usługi drogą elektroniczną, które w określonych sytuacjach nie ponoszą odpowiedzialności za treści pojawiające się w Internecie. Do pierwszej grupy należą podmioty świadczące usługi transmisji danych oraz usługi dostępu do sieci (najczęściej są to przedsiębiorstwa telekomunikacyjne). Podmioty te nie ponoszą odpowiedzialności za przekazywane dane, jeżeli nie inicjują ich transmisji (nie są np. nadawcą wiadomości), nie wybierają odbiorcy danych oraz nie modyfikują transmitowanych danych (np. dodanie reklamy w przypadku darmowych kont poczty elektronicznej).

Druga grupa to podmioty, które świadczą usługę cachingu, tj. automatycznego i krótkotrwałego pośredniego przechowywania danych w celu przyspieszenia ponownego dostępu do nich. Podmioty te nie ponoszą odpowiedzialności, jeżeli nie modyfikują danych. Jednak należy pamiętać, że istotną cechą cachingu jest krótkotrwałość – każde dłuższe przechowywanie informacji (np. zawartości całych stron internetowych) może powodować powstanie odpowiedzialności za szkodliwe treści. W niektórych przypadkach może to być kilka minut, w niektórych kilka godzin. To niesprecyzowane w przepisach pojęcie powoduje, że usługodawca powinien usunąć dane natychmiast po tym, gdy ich przechowywanie stanie się zbędne.

Może się zdarzyć, że przechowywane na serwerze lokalnym dane zawierające szkodliwe treści zostały usunięte z początkowego źródła lub sąd wyda nakaz ich usunięcia. Wtedy podmiot świadczący usługę cachingu musi je usunąć lub uniemożliwić dostęp do nich, jeśli nie chce ponieść odpowiedzialności za upublicznianie szkodliwych treści.

PRZYKŁAD

ZNIESŁAWIENIE NA FORUM

Firma A prowadzi forum internetowe, na którym umieszczono wpis zniesławiający Jana Kowalskiego. Pan Kowalski napisał do firmy A e-mail z prośbą o usunięcie wpisu, ponieważ narusza on jego dobre imię i może spowodować problemy w miejscu pracy. Pracownik firmy A wyznaczony do obsługi tej strony powinien rozważyć zasadność tej prośby i jeżeli uzna, że rzeczywiście Jan Kowalski ma rację, usunąć kwestionowany wpis. Jeżeli nie usunie, to musi się liczyć z tym, że Kowalski zwróci się do sądu, który może wydać nakaz usunięcia wpisu oraz dodatkowo zasądzić na rzecz Kowalskiego zadośćuczynienie. Sąd ocenia całokształt sprawy i może zadecydować, czy zadośćuczynienie ma zapłacić tylko osoba, która umieściła wpis, czy też kwotą zadośćuczynienia obciążyć również firmę A. Jeżeli sąd nakaże usunąć treści, to jest to decyzja, której firma A musi się podporządkować.

Trzecia grupa to podmioty świadczące usługę hostingu w celu przechowywania różnego rodzaju danych, np. składających się na strony internetowe. Odpowiedzialność takiego dostawcy za treści udostępniane za pośrednictwem Internetu przez usługobiorców jest możliwa jedynie w przypadku uzyskania urzędowego zawiadomienia lub wiadomości z wiarygodnego źródła o bezprawnym charakterze danych lub związanej z nimi działalności. Co istotne, dostawca usługi hostingu nie ma obowiązku sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych. Co za tym idzie, nie ma obowiązku oceny publikowanych danych czy też czuwania nad przestrzeganiem prawa przez użytkowników forum.

Justyna Plechowska-Łukowska

Policja i prokuratura może zażądać zarówno danych, jak również sprzętu stanowiącego dowód w sprawie

W toku postępowania karnego organy ścigania mają prawo i zwracają się do administratorów stron, portali, właścicieli serwerów o udostępnienie danych informatycznych, które mogą się przyczynić do ustalenia tożsamości sprawcy przestępstwa popełnionego za pośrednictwem sieci.

W związku z ogromną popularnością Internetu i występującymi w nim negatywnymi zjawiskami (patrz tabela) stworzono prawne mechanizmy pozwalające na ochronę przed tzw. cyberprzestępczością oraz przeciwdziałanie jej skutkom. Istnieje nie tylko sposobność do ochrony przed szkodami związanymi z funkcjonowaniem Internetu. Ustawodawca zapewnił poszkodowanym również środki odwoławcze oraz możliwość dochodzenia odszkodowania za krzywdy doznane na skutek nadużycia Internetu.

Niestety, ze względu na dużą anonimowość skuteczność tych mechanizmów nie zawsze jest zadowalająca. Wobec coraz większych możliwości podszywania się pod obcy adres IP, korzystania z sieci TOR czy też nawet używania komputerów z tzw. kawiarenek internetowych prawdziwym problemem staje się najważniejszy w postępowaniu karnym element, tj. ustalenie tożsamości sprawcy oraz zebranie dowodów potwierdzających jego sprawstwo.

Informacje dla organów

Policja lub prokuratura mogą zwrócić się o różnorodne informacje, w zależności od rodzaju podmiotu, od którego pochodzą. Z reguły są zawarte w logach systemowych i gromadzone oraz przechowywane głównie w celach technicznych lub administracyjnych. Mogą to być dane podane przy rejestracji różnego rodzaju kont pocztowych czy też profili na forach. Niestety informacje te najczęściej nie są weryfikowane pod kątem ich prawdziwości, co utrudnia identyfikację użytkownika. Inny rodzaj stanowią dane o charakterze technicznym, takie jak numer IP komputera czy też logi systemowe rejestrujące dane na temat aktywności sieciowej. Pozwalają na ustalenie, z jakimi miejscami w sieci łączył się dany użytkownik,

PRZESTĘPSTWA POPEŁNIANE W INTERNECIE

Katalog czynów niezgodnych z prawem, a popełnianych za pośrednictwem Internetu jest naprawdę szeroki:

- Kradzież programu komputerowego.
- Oszustwa za pośrednictwem portali aukcyjnych.
- Znieważanie, zniesławianie, nękanie i kierowanie gróźb.
- Podszywanie się pod inną osobę.
- Uzyskanie nieuprawnionego dostępu do informacji po przełamaniu zabezpieczeń elektronicznych lub informatycznych bądź wykorzystanie w tym celu oprogramowania.
- Uzyskanie bez uprawnień dostępu do systemu informatycznego.
- Niszczenie lub usunięcie bez uprawnień zapisu na informatycznym nośniku danych, niszczenie, usunięcie, zmiana lub utrudnienie dostępu do danych informatycznych albo zakłócenie przetwarzania bądź uniemożliwienie automatycznego przetwarzania czy przekazywania danych.
- Zakłócanie bez uprawnień pracy systemu komputerowego lub sieci teleinformatycznej.
- Produkowanie, utrwalanie albo rozpowszechnianie treści pornograficznych z udziałem małoletnich lub nawiązywanie kontaktu z nieletnim.

Wydawca:
Monika Kijok

Redaktor:
Rafał Janus

Koordynator produkcji:
Mariusz Jezierski

Korekta:
Zespół

ISBN: 978-83-269-2924-3

Wydawnictwo Wiedza i Praktyka sp. z .o.o.
03-918 Warszawa, ul. Łotewska 9a
Tel. 22 518 29 29, faks 22 617 60 10, e-mail: ***e-mail redakcji***
NIP: 526-19-92-256
Numer KRS: 0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy
XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł

Copyright by Wydawnictwo Wiedza i Praktyka sp. z o.o.
Warszawa 2014
„Odpowiedzialność karna informatyka" wraz z przysługującym Czytelnikom innymi elementami dostępnymi w subskrypcji (e-letter, strona www i inne) chronione są prawem autorskim. Przedruk materiałów opublikowanych w „Odpowiedzialność karna informatyka" oraz w innych dostępnych elementach subskrypcji – bez zgody wydawcy – jest zabroniony. Zakaz nie dotyczy cytowania publikacji z powołaniem się na źródło.

Publikacja„Odpowiedzialność karna informatyka" została przygotowana z zachowaniem najwyższej staranności i wykorzystaniem wysokich kwalifikacji, wiedzy i doświadczenia autorów oraz konsultantów. Zaproponowane w publikacji „Odpowiedzialność karna informatyka" oraz w innych dostępnych elementach subskrypcji wskazówki, porady i interpretacje nie mają charakteru porady prawnej. Ich zastosowanie w konkretnym przypadku może wymagać dodatkowych, pogłębionych konsultacji. Publikowane rozwiązania nie mogą być traktowane jako oficjalne stanowisko organów i urzędów państwowych. W związku z powyższym redakcja nie może ponosić odpowiedzialności prawnej za zastosowanie zawartych w publikacji „Odpowiedzialność karna informatyka" lub w innych dostępnych elementach subskrypcji wskazówek, przykładów, informacji itp. do konkretnych przykładów.
Wydawca nie odpowiada za treść zamieszczonej reklamy; ma prawo odmówić zamieszczenia reklamy, jeżeli jej treść lub forma są sprzeczne z linią programową bądź charakterem publikacji oraz interesem Wydawnictwa Wiedza i Praktyka.
Centrum Obsługi Klienta:
Tel: 22 518 29 29
e-mail: cok@wip.pl