



Sposoby wykorzystania usług telekomunikacyjnych, które są niezgodne z prawem lub stanowią rozpowszechnianie szkodliwych treści, w tym przypadki naruszenia praw autorskich i pokrewnych.

Konsekwencje prawne tych czynów.

Sposoby ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych.

Niniejsza informacja Prezesa Urzędu Komunikacji Elektronicznej stanowi wypełnienie obowiązku prawnego wskazanego w art. 62 ust. 1 pkt 3 i 4 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) i została przygotowana w oparciu o dane przekazane przez przedsiębiorców telekomunikacyjnych.

Warszawa, 10 września 2013 r.

Spis treści

Cześć 1. Sposoby wykorzystania usług telekomunikacyjnych niezgodne z prawem lub stanowiące rozpowszechnianie szkodliwych treści, w tym przypadki naruszenia praw autorskich i pokrewnych..	3
1. Sposoby wykorzystania usług telekomunikacyjnych niezgodne z prawem lub stanowiące rozpowszechnianie szkodliwych treści.	3
2. Przykłady nadużyć telekomunikacyjnych. Oszustwa i wyłudzenia.	5
3. Przykłady naruszenia praw autorskich i pokrewnych.	6
Cześć 2. Konsekwencje prawne wykorzystania usług telekomunikacyjnych w sposób niezgodny z prawem lub stanowiący rozpowszechnianie szkodliwych treści.	8
1. Sankcje cywilnoprawne na podstawie prawa autorskiego	8
2. Sankcje karne za naruszenie praw autorskich i pokrewnych.	10
3. Sankcje cywilnoprawne na podstawie przepisów kodeksu cywilnego (art. 24 Kc).....	10
Cześć 3. Sposoby ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych.	13

Cześć 1

Sposoby wykorzystania usług telekomunikacyjnych niezgodne z prawem lub stanowiące rozpowszechnianie szkodliwych treści, w tym przypadki naruszenia praw autorskich i pokrewnych.

1. Sposoby wykorzystania usług telekomunikacyjnych niezgodne z prawem lub stanowiące rozpowszechnianie szkodliwych treści:

- działania powodujące albo mogące powodować zakłócenia pracy urządzeń aktywnych, podłączonych do sieci telekomunikacyjnej lub sieci teleinformatycznej operatora oraz sieci Internet;
- kierowanie, bez zgody operatora, do sieci telekomunikacyjnej lub sieci innych przedsiębiorców telekomunikacyjnych, ruchu pochodzącego z innych sieci telekomunikacyjnych, za pomocą jakichkolwiek urządzeń telekomunikacyjnych przy użyciu abonenckiej karty SIM ;
- uzyskanie nielegalnego dostępu lub wykorzystanie usług telekomunikacyjnych lub infrastruktury telekomunikacyjnej niezgodnie z przeznaczeniem;
- wykorzystanie usług telekomunikacyjnych lub infrastruktury telekomunikacyjnej zgodnie z przeznaczeniem, ale bez zamiaru uiszczenia opłaty za usługi telekomunikacyjne;
- generowanie ruchu nie służącego bezpośredniej wymianie informacji pomiędzy użytkownikami, a mającego na celu uzyskanie jak najwyższych wskazań urządzeń rozliczających ruch międzyoperatorski;
- generowanie ruchu w celu przeciążenia elementów infrastruktury telekomunikacyjnej (tzw. atak „Denial of Service”);
- podawanie przez abonenta nieprawdziwych danych lub posługiwanie się przez niego podrobionymi lub przerobionymi dokumentami, podczas zawierania umowy lub w trakcie wykonywania umowy o świadczenie usług telekomunikacyjnych;
- wykorzystywanie hasła abonenckiego lub hasła dostępu do systemów obsługowych bez zgody uprawnionego użytkownika;
- udostępnianie usług telekomunikacyjnych operatora innym osobom bez zgody operatora, w celu uzyskania korzyści majątkowych;
- używanie karty SIM pochodzącej ze skradzionego telefonu lub telefonu nieposiadającego znaku zgodności z zasadniczymi wymaganiami;

- instalowanie złośliwego oprogramowania w telefonie użytkownika, bez jego wiedzy, (tj. instalowanie rozwiązań i aplikacji, które mogą niszczyć i wykradać dane lub powodować szkody w urządzeniach końcowych) które może doprowadzić do niezamierzonych operacji, a w szczególności:
 - a) samoczynnego restartu urządzenia końcowego (telefonu);
 - b) samoczynnej wysyłki danych lub komunikatów;
 - c) przekierowania SMS-ów bez wiedzy użytkownika;
 - d) przekierowań na płatne numery bez wiedzy użytkownika;
- instalowanie w urządzeniu końcowym użytkownika, bez jego zgody, aplikacji niewiadomego pochodzenia, która może spowodować utratę kontroli użytkownika nad urządzeniem oraz doprowadzić do utraty poufności danych osobowych;
- podmienianie numeru nadawcy (tzw. „Spoofing”) - działanie polegające na fałszowaniu, podmianie numeru nadawcy tak, aby zmylić odbiorcę i w konsekwencji wyłudzić dane, informacje wrażliwe (np. numer karty kredytowej, numery PIN, hasła, itp.);
- kradzież danych z urządzenia końcowego użytkownika, (np. poprzez wykorzystanie Bluetooth);
- wysyłanie informacji handlowych, w tym tzw. „innych niezamówionych informacji” (SPAM-u), do innych użytkowników końcowych, bez ich zgody;
- wysyłanie wirusów do innych użytkowników końcowych;
- zwalczanie programów antywirusowych;
- blokowanie kart pamięci;
- nieuprawnione podsłuchiwanie rozmów telefonicznych;
- nieuprawnione lokalizowanie innych użytkowników;
- nieuprawnione dublowanie karty SIM – tzw. „klonowanie kart SIM” bez wiedzy i zgody operatora;
- wykonywanie jednokrotnych połączeń telefonicznych z numeru telefonicznego o formacie zgodnym z formatem standardowego numeru abonenckiego, w celu skłonienia danego użytkownika do oddzwonienia i wygenerowania tym samym połączenia typu „Premium” (tj. o podwyższonej opłacie) lub połączenia międzynarodowego;
- działania mające na celu nakłanianie użytkowników do generowania bez ich wiedzy połączeń telefonicznych typu „Premium” lub międzynarodowych oraz do wysyłania SMS-ów „Premium” lub międzynarodowych o podwyższonej opłacie;
- wyłudzenie doładowań kont pre-paid, poprzez rozsyłanie SMS-ów z prośbą o kod doładowujący (działanie wprowadza danego użytkownika końcowego w błąd co do tożsamości osoby wysyłającej prośbę);
- prowadzenie działań niezgodnych z prawem i/lub dobrymi obyczajami, w tym promowanie lub rozpowszechnianie nielegalnych i szkodliwych treści, dotyczących rasizmu, faszyzmu, komunizmu, ksenofobii, szerzenia nienawiści lub nakłaniania do przemocy wobec odmiennej rasy, pochodzenia etnicznego, wyznania, płci, wieku, orientacji seksualnej itp.;

- rozpowszechnianie lub propagowanie pornografii, w tym pornografii dziecięcej;
- niszczenie, uszkodzanie, usuwanie, dokonywanie zmian lub utrudnianie dostępu do danych informatycznych albo ich istotne zakłócenie lub uniemożliwienie automatycznego przetwarzania; gromadzenie lub przekazywanie takich danych oraz uzyskiwanie dostępu do całości lub części systemu informatycznego lub informacji nieprzeznaczonej poprzez podłączanie się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenia;
- rozpowszechnienie treści umożliwiających uprawianie lub reklamowanie hazardu (np. zawieranie zakładów bukmacherskich, branie udziału w loteriach, grach liczbowych itp.);
- podejmowanie działań (zaniechań) mających na celu dokuczanie i nękanie innych osób lub instytucji (inaczej tzw. „stalking”);
- przywłaszczanie praw autorskich albo wprowadzanie w błąd co do autorstwa cudzego utworu lub artystycznego wykonania (w całości lub części);
- rozpowszechnianie bez podania nazwiska lub pseudonimu twórcy, cudzego utworu lub artystycznego wykonania w wersji oryginalnej albo w postaci opracowania, publiczne zniekształcanie takiego utworu oraz inne naruszenie cudzego prawa autorskiego lub prawa pokrewnego, określonego w Ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, w celu osiągnięcia korzyści majątkowej bez uprawnienia albo wbrew jego warunkom;
- rozpowszechnianie, zwielokrotnienie nabycia lub pomocy w jego zbyciu, przyjmowanie bądź pomoc w ukryciu - choćby nieumyślnie, cudzego utworu w wersji oryginalnej albo w postaci opracowania, artystycznego wykonania, fonogramu, wideogramu lub nadania;
- uniemożliwianie lub utrudnianie wykonywania prawa do kontroli korzystania z utworu.

2. Przykłady nadużyć telekomunikacyjnych. Oszustwa i wyłudzenia.

a) Użycie urządzeń FCT (inaczej tzw. „Sim-boxing”).

Nadużycie polega na wykorzystaniu różnicy pomiędzy cenami detalicznymi a stawkami za zakończenie połączenia, poprzez skierowanie ruchu międzyoperatorskiego na karty SIM „udające” zwykłego abonenta sieci mobilnej. W tym przypadku poszkodowanym jest najczęściej operator, a skutkiem ubocznym zestawienia połączenia poprzez FCT bez wiedzy abonenta jest zmiana numeru dzwoniącego (numeru A) oraz inne braki w funkcjonalności usługi (takie jak obniżenie jakości czy też nawet brak połączenia).

Standardową procedurą operatorów telekomunikacyjnych w przypadku wykrycia zjawiska kierowania ruchu międzyoperatorskiego przez urządzenia FCT jest zawieszenie świadczenia usług telekomunikacyjnych, a następnie zerwanie umowy i w razie większych strat – dochodzenie odszkodowania na drodze sądowej. Niewykluczone jest również skierowanie zawiadomienie do prokuratury dotyczące popełnienia przestępstwa, np. fałszowania informacji dotyczącej realizacji połączeń (zmiana numeru abonenta dzwoniącego).

b) Prowokowanie oddzwaniania na numer o wysokiej opłacie (tzw. „Wangiri fraud”).

Nadużycie to polega na oszukaniu abonenta, aby oddzwonił na numer, który wyświetla się jako „nieodebrane połączenie”. Numer ten najczęściej jest podobny do numeru krajowego, jest jednak numerem zagranicznym, o cenie za połączenie znacznie wyższej niż cena krajowa. Często wykorzystywane są podobieństwa początku numerów krajowych i międzynarodowych (np. 22 – Warszawa, +22 – kraje afrykańskie). Konsekwencją dla nieświadomych abonentów jest konieczność zapłacenia za zrealizowane połączenia.

c) Wyludzanie kodów doładowania poprzez SMS.

Nadużycie polega na próbie podszycia się pod dostawcę usług i przesłanie do abonenta usług przepłaconych, informacji o rzekomej korzyści (np. o podwójnym doładowaniu, możliwości wygrania drogiego sprzętu, itp.) w zamian za przesłanie zwrotnego kodu doładowującego. Oczywiście, po przesłaniu kodu oszust przejmuje i zużywa doładowanie. Czyn ten może wypełniać znamiona przestępstwa oszustwa lub tzw. „kradzieży impulsów” a jego konsekwencje przewidziane są w ustawie z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r., Nr 88, poz. 553),.

d) Podmiana numerów kont bankowych na fakturach.

Oszustwo polega na dokonaniu kradzieży rachunku/faktury ze skrzynki abonenta i zmianie na tym rachunku numeru konta bankowego operatora na inne. Działanie takie nosi znamiona kilku przestępstw wskazanych w Kodeksie karnym. Należy więc zachować ostrożność w przypadku gdy znaleziony w skrzynce pocztowej dokument zawierający logo operatora wygląda na zmieniony czy przerobiony. Numer konta do zapłaty faktury można zawsze potwierdzić np. poprzez kontakt z infolinią operatora.

e) Wprowadzenie w błąd, co do tożsamości podmiotu zawierającego umowę.

Nadużycie polega na wprowadzeniu klienta w błąd, co do tożsamości podmiotu, z którym klient ma zamiar zawrzeć umowę o świadczenie usług telekomunikacyjnych. Najwięcej tego typu przypadków było związanych z nieuczciwymi przedstawicielami handlowymi niewielkich spółek telekomunikacyjnych, które wykorzystywały podobieństwo nazw do dużych, znanych na rynku przedsiębiorców.

3. Przykłady naruszenia praw autorskich i pokrewnych.

Przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiegokolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór). Ochrona przysługuje twórcy niezależnie od spełnienia jakichkolwiek formalności. Wszystko, co oryginalne, (np. tekst artykułu, projekt strony, wiadomość e-mail lub wpis na forum) zostaje automatycznie objęte ochroną prawa autorskiego. Aby jednak ochrona taka była możliwa, stworzony utwór musi być możliwy do zidentyfikowania jako oryginalne dzieło.

Wszystkie dzieła muzyczne, artykuły, kompozycje graficzne, podobnie jak i inne dzieła artystyczne zamieszczone na stronach WWW lub pobierane za pomocą łączy internetowych jeżeli spełniają przesłanki utworu, podlegają ochronie przewidzianej w prawie autorskim.

Głównym celem tej dziedziny prawa jest ochrona szeroko pojętych dzieł autorów, przed ich kradzieżą i wykorzystaniem bez zezwolenia lub wbrew warunkom zezwolenia twórcy. Dla prawnego autorskiej ochrony utworu nie ma znaczenia, w jaki sposób dokonujący naruszenia wszedł w jego posiadanie lub też w jaki sposób utwór do niego dotarł. W szczególności nie ma znaczenia okoliczność, że utwór stanowiący przedmiot naruszenia dotarł do dokonującego naruszenia, jako niezamawiana korespondencja przesyłana drogą elektroniczną (tzw. spam). Do wyjątków bezwzględnej ochrony autorskiej należy instytucja tzw. dozwolonego użytku (art. 25 – 35 prawa autorskiego), w tym prawo przedruku oraz prawo cytatu.

Poniżej przedstawione zostały przykładowe sposoby wykorzystania usług telekomunikacyjnych (także niekomercyjne), stanowiące przypadki naruszenia praw autorskich i pokrewnych:

- 1) nielegalne ściąganie (tzw. „downloading”) programów z sieci do własnego urządzenia, bez wymaganej zgody uprawnionego na korzystanie z utworów;
- 2) kopiowanie, dystrybuowanie lub udostępnianie zdjęć, filmów, muzyki, gier, programów, artykułów, ilustracji z gazet poza zakresem dozwolonego użytku, bez wymaganej zgody uprawnionego na korzystanie z utworów;
- 3) udostępnianie na własnej stronie internetowej utworów, np. tekstów, artykułów, zdjęć, grafik, makiety strony, poza zakresem wynikającym z dozwolonego użytku;
- 4) zamieszczanie i publikowanie (np. na własnej witrynie) cudzego tekstu i podpisanie go własnym nazwiskiem;
- 5) zamieszczenie cudzego tekstu bez podania autora i źródła utworu;
- 6) rozpowszechnienie opracowań (przeróbek) cudzych utworów (w tym tekstów), bez zezwolenia autora;
- 7) umieszczanie we własnych tekstach, twórczych fragmentów cudzych tekstów jako własnych;
- 8) obchodzenie zabezpieczeń w celu możliwości korzystania z programów komputerowych (np. przez „crackowanie”);
- 9) usuwanie lub zmiana – bez upoważnienia, jakichkolwiek elektronicznych informacji na temat zarządzania prawami autorskimi lub prawami, a także świadome rozpowszechnianie utworów z bezprawnie usuniętymi lub zmodyfikowanymi takimi informacjami.

Cześć 2

Konsekwencje prawne wykorzystania usług telekomunikacyjnych w sposób niezgodny z prawem lub stanowiący rozpowszechnianie szkodliwych treści.

Konsekwencje prawne wykorzystania usług telekomunikacyjnych w sposób niezgodny z prawem lub stanowiący rozpowszechnianie szkodliwych treści mogą być dwojakiego rodzaju: regulaminowe bądź prawne.

Zgodnie z postanowieniami regulaminów świadczenia usług telekomunikacyjnych, w stosunku do użytkowników, którzy dopuszczają się nadużyć wobec przedsiębiorców mogą być wyciągnięte następujące konsekwencje:

- upomnienie telefoniczne lub listowne,
- czasowe zawieszenie świadczenia usług,
- wypowiedzenie umowy abonenckiej.

Konsekwencje prawne naruszeń wskazanych w części 1 w punktach 1 i 2 są określone w szczególności w:

- Ustawie z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 nr 88 poz. 553);
- Ustawie z dn. 4 lutego 1996 r. o prawie autorskim i prawach pokrewnych (Dz. U. 1994, nr 24, poz. 83, tekst jednolity: Dz. U. 2006, nr 90, poz. 631);
- Ustawie z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz.U. z 2010 r. Nr 46, poz. 275, z późn. zm.);
- Ustawie z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 1964 r., Nr 16 poz. 93 z późn. zm.);
- Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Dz.U. 2002 Nr 144 poz. 1204, z późn. zm.);
- Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);

Konsekwencje naruszeń mogą polegać na wymierzeniu kary pozbawienia wolności, ograniczenia wolności lub grzywny oraz odebrania przedmiotów służących do popełnienia przestępstwa. Szczegółowo konsekwencje dla poszczególnych naruszeń są określone w powyżej wymienionych aktach prawnych.

W przypadku, gdy operator stwierdzi powyższe naruszenia, jest uprawniony do blokady inicjowania połączeń lub zawieszenia wszelkich usług wobec użytkownika dopuszczającego się naruszeń. Odbywa się to na zasadach określonych w odpowiednich regulaminach (np. regulaminie świadczenia usług telekomunikacyjnych) lub innych dokumentach

stanowiących integralną część umowy między operatorem a użytkownikiem. Na podstawie tych samych aktów prawnych operator może również rozwiązać umowę o świadczenie usług telekomunikacyjnych, z zachowaniem lub bez zachowania okresu wypowiedzenia.

Niezależnie, w przypadku, gdy dane działanie wypełnia znamiona przestępstwa, operator bądź inna osoba dotknięta naruszeniem może złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa do odpowiednich organów ścigania.

Operator w razie poniesienia szkody w związku z opisanymi powyżej działaniami, może również skorzystać z drogi sądowej, w celu uzyskania odpowiedniego odszkodowania za poniesioną szkodę (postępowanie cywilno-prawne).

Poniżej znajduje się opis konsekwencji prawnych wykorzystywania usług telekomunikacyjnych z naruszeniem praw autorskich i praw pokrewnych:

1. Sankcje cywilno-prawne na podstawie prawa autorskiego.

Twórca, którego autorskie prawa osobiste zostały zagrożone cudzym działaniem, może żądać zaniechania tego działania. W razie dokonanego naruszenia może także żądać, aby osoba która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności aby złożyła publiczne oświadczenie o odpowiedniej treści i formie. Jeżeli naruszenie było zawinione, sąd może przyznać twórcy odpowiednią sumę pieniężną tytułem zadośćuczynienia za doznaną krzywdę lub – na żądanie twórcy – zobowiązać sprawcę, aby uiścił odpowiednią sumę pieniężną na wskazany przez twórcę cel społeczny (art. 78 prawa autorskiego).

Uprawniony, którego autorskie prawa majątkowe zostały naruszone, może żądać od osoby, która naruszyła te prawa:

- a) zaniechania naruszania;
- b) usunięcia skutków naruszenia;
- c) naprawienia wyrządzonej szkody (na zasadach ogólnych albo poprzez zapłatę sumy pieniężnej w wysokości odpowiadającej dwukrotności, a w przypadku gdy naruszenie jest zawinione – trzykrotności, stosownego wynagrodzenia, które w chwili jego dochodzenia byłoby należne tytułem udzielenia przez uprawnionego zgody na korzystanie z utworu);
- d) wydania uzyskanych korzyści;
- e) jednokrotnego albo wielokrotnego opublikowania w prasie oświadczenia odpowiedniej treści i w odpowiedniej formie, lub podania do publicznej wiadomości części albo całości orzeczenia sądu wydanego w rozpatrywanej sprawie, w sposób i w zakresie określonym przez sąd;
- f) zapłaty odpowiedniej sumy pieniężnej (nie niższej niż dwukrotna wysokość uprawdopodobnionych korzyści odniesionych przez sprawcę z dokonanego naruszenia), na rzecz Funduszu Promocji Twórczości, gdy naruszenie jest zawinione i zostało dokonane w ramach działalności gospodarczej wykonywanej w cudzym albo we własnym imieniu, choćby na cudzy rachunek;

- g) odpowiedniego rozporządzenia bezprawnie wytworzonymi przedmiotami oraz środkami i materiałami użytymi do ich wytworzenia (np. ich wycofania z obrotu, przyznania ich na poczet należnego odszkodowania lub zniszczenia).

2. Sankcje karne za naruszenie praw autorskich i pokrewnych.

Sankcje karne za naruszenie praw autorskich i pokrewnych zostały ujęte w następujących przepisach:

a) art. 115 prawa autorskiego

1. Kto przywłaszcza sobie autorstwo albo wprowadza w błąd, co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
2. Tej samej karze podlega, kto rozpowszechnia bez podania nazwiska lub pseudonimu twórcy cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie albo publicznie zniekształca taki utwór, artystyczne wykonanie, fonogram, wideogram lub nadanie.
3. Kto w celu osiągnięcia korzyści majątkowej, w inny sposób niż określony w ust. 1 lub ust. 2 narusza cudze prawa autorskie lub prawa pokrewne określone w art. 16, art. 17, art. 18, art. 19 ust. 1, art. 191, art. 86, art. 94 ust. 4 lub art. 97, albo nie wykonuje obowiązków określonych w art. 193 ust. 2, art. 20 ust. 1-4, art. 40 ust. 1 lub ust. 2, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

b) art. 116 prawa autorskiego

1. Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3.
3. Jeżeli sprawca uczynił sobie z popełnienia przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 5.
4. Jeżeli sprawca czynu określonego w ust. 1 działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

c) art. 117 prawa autorskiego

1. Kto bez uprawnienia albo wbrew jego warunkom w celu rozpowszechnienia utrwala lub zwielokrotnia cudzy utwór w wersji oryginalnej lub w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli sprawca uczynił sobie z popełnienia przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności do lat 3.

d) art. 118 prawa autorskiego

1. Kto w celu osiągnięcia korzyści majątkowej przedmiot będący nośnikiem utworu, artystycznego wykonania, fonogramu, wideogramu rozpowszechnianego lub zwielokrotnionego bez uprawnienia albo wbrew jego warunkom nabywa lub pomaga w jego zbyciu albo przedmiot ten przyjmuje lub pomaga w jego ukryciu, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
2. Jeżeli sprawca uczynił sobie z popełnienia przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od roku do lat 5.
3. Jeżeli na podstawie towarzyszących okoliczności sprawca przestępstwa określonego w ust. 1 lub 2 powinien i może przypuszczać, że przedmiot został uzyskany za pomocą czynu zabronionego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

e) art. 118 (1) prawa autorskiego

1. Kto wytwarza urządzenia lub ich komponenty przeznaczone do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi urządzeniami lub ich komponentami, albo reklamuje je w celu sprzedaży lub najmu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
2. Kto posiada, przechowuje lub wykorzystuje urządzenia lub ich komponenty, o których mowa w ust. 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

f) art. 119 prawa autorskiego

1. Kto uniemożliwia lub utrudnia wykonywanie prawa do kontroli korzystania z utworu, artystycznego wykonania, fonogramu lub wideogramu albo odmawia udzielenia informacji przewidzianych w art. 47, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

3. Sankcje cywilnoprawne na podstawie art. 24 Kodeksu cywilnego.

Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać:

- 1) Zaniechania tego działania, chyba że nie jest ono bezprawne. Ciężar udowodnienia, że działanie nie miało charakteru bezprawnego spoczywa na pozwanym; Powód – twórca nie musi uzasadniać, że działanie pozwanego miało taki charakter, bowiem działa na jego rzecz domniemanie bezprawności tego działania, wyrażone w ustawie;
- 2) W razie dokonanego naruszenia twórca może także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej

formie, na zasadach podobnych jak w przypadku roszczenia uregulowanego przepisami prawa autorskiego;

- 3) Twórca może również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny, jeżeli naruszenie dóbr osobistych było skutkiem działania zawinionego, a więc podjętego mimo tego, że sprawca wiedział lub z łatwością mógł się dowiedzieć o istnieniu praw autorskich;
- 4) Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych, oznacza to, że w przypadku zawinionego działania sprawcy, autor uprawniony będzie do żądania zapłaty sumy pieniężnej, która pozwoli na wyrównanie strat majątkowych, jakich doznał na skutek naruszenia jego autorskich praw osobistych (mogą to być straty już poniesione, albo utracone korzyści).

Cześć 3

Sposoby ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych.

Do sposobów ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych należy zaliczyć m.in.:

- 1) Wykorzystywanie odpowiednio zabezpieczonego komputera (z zainstalowanym aktualnym oprogramowaniem antywirusowym, z najnowszymi wersjami przeglądarek internetowych);
- 2) Regularne skanowanie swojego komputera w celu wykrycia obecności i wyeliminowania szkodliwego oprogramowania;
- 3) Stosowanie bezpiecznych haseł w sieci;
- 4) Zabezpieczenie routerów (firewall);
- 5) Zwracanie uwagi na to, jakich informacji nie należy podawać drogą telefoniczną i elektroniczną w celu zachowania prywatności (np. numeru PESEL, haseł zabezpieczających i numerów kont, numerów PIN, itp.);
- 6) Zdobywanie i rozpowszechnianie informacji o oszustwach sieciowych i nowych metodach działania oszustów (np. dzięki rozpowszechnieniu informacji odkryte i nazwane zostało zjawisko „phishingu”, i abonenci dowiedzieli się, że nie należy wchodzić na portale bankowe, społecznościowe, itd. - z linków, które otrzymali z nieznanych źródeł);
- 7) Ochrona karty SIM przed kradzieżą, zniszczeniem, uszkodzeniem, zagubieniem lub utratą w inny sposób oraz niezwłoczne informowanie operatora przez abonenta/użytkownika w przypadku zagubienia, kradzieży, zniszczenia, uszkodzenia lub utraty karty SIM;
- 8) Ochrona poufności i niedostępności kodu PIN lub kodu PUK do karty SIM osobom trzecim oraz niezwłoczna zmiana przez abonenta/użytkownika kodu PIN w przypadku podejrzenia wejścia w jego posiadanie przez osobę trzecią;
- 9) Blokowanie przez abonenta/użytkownika dostępu do karty SIM, aparatu telefonicznego lub innego urządzenia elektronicznego, umożliwiającego za pośrednictwem karty SIM korzystanie z usług świadczonych przez operatora, w szczególności ustawienie okresu, po którym automatycznie blokowany jest dostęp do aparatu telefonicznego, gdy nie jest on używany;

- 10) Nieudostępnianie przez abonenta/użytkownika osobom trzecim dokumentów lub danych umożliwiających zawarcie w jego imieniu lub na jego rzecz umowy o świadczenie usług telekomunikacyjnych;
- 11) Ochrona poufności i nieudostępnianie osobom trzecim dokumentów lub danych (w szczególności hasła do konta abonenckiego), wykorzystywanych do uwierzytelnienia abonenta/użytkownika przez operatora w procesie sprzedaży lub obsługi klienta oraz niezwłoczna zmiana hasła do konta abonenckiego w przypadku podejrzenia wejścia w jego posiadanie przez osobę trzecią;
- 12) Nieudostępnianie osobom trzecim dokumentów zawierających dane o świadczonych przez operatora usługach telekomunikacyjnych, w szczególności faktur oraz szczegółowych wykazów połączeń (tzw. bilingów);
- 13) Ochrona poufności i nieudostępnianie osobom trzecim danych (w szczególności hasła), wykorzystywanych do uwierzytelnienia dostępu do portali internetowych, umożliwiających przeglądanie poprzez dostęp elektroniczny danych dotyczących abonenta/użytkownika, usług świadczonych mu przez operatora, składania dyspozycji. Zalecana jest niezwłoczna zmiana przez abonenta/użytkownika hasła do portali internetowych w przypadku podejrzenia wejścia w jego posiadanie przez osobę trzecią;
- 14) Korzystanie przez abonenta/użytkownika z mechanizmów umożliwiających potwierdzanie wykonywanych operacji (tokeny, kody SMS lub hasła jednorazowe);
- 15) Możliwość zarządzania przez abonenta/użytkownika zgodami lub sprzeciwami, dotyczącymi przetwarzania jego danych (w tym danych osobowych), takich jak.:
 - dane, o których mowa w art. 161 ust. 3 Prawa telekomunikacyjnego, w tym nazwisk i imion, imion rodziców, miejsca i daty urodzenia, adresu zamieszkania, numeru PESEL czy numeru dokumentu tożsamości;
 - zgoda na umieszczenie danych w publicznie dostępnym spisie abonentów (książce teleadresowej), w tym na przekazywanie danych do podmiotu, o którym mowa w art. 67 prawa telekomunikacyjnego,
 - zgoda na otrzymywanie informacji handlowych za pomocą środków komunikacji elektronicznej, w szczególności przy użyciu automatycznych systemów wywołujących,
 - zgoda na przetwarzanie danych transmisyjnych dla celów marketingu usług telekomunikacyjnych,
 - zgoda na otrzymywanie informacji o treści proponowanych zmian warunków umowy o świadczenie usług telekomunikacyjnych na adres e-mail,
 - sprzeciw wniesiony zgodnie z art. 32 ust. 1 pkt 8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), wobec przetwarzania danych osobowych w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych (tj. operator) zamierza je przetwarzać w celach marketingowych lub wobec przekazywania danych osobowych innemu administratorowi danych;
- 16) Nieoddzwanianie i niewysyłanie komunikatów na nieznane numery;
- 17) Niepodawanie poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub kart kredytowej, nieznanemu rozmówcy lub w miejscach publicznych;

- 18) Systematyczna aktualizacja systemu operacyjnego aparatu telefonicznego lub innego urządzenia elektronicznego, umożliwiającego za pośrednictwem karty SIM korzystanie z usług świadczonych przez operatora;
- 19) Nieprzechowywanie w pamięci wewnętrznej aparatu telefonicznego lub na karcie pamięci niezabezpieczonych (niezaszyfrowanych) poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub kart kredytowych;
- 20) Wyłączanie łączności bezprzewodowej Wi-Fi lub Bluetooth niezwłocznie po zakończeniu korzystania z tego typu połączeń;
- 21) Stosowanie przez abonenta/użytkownika zasad bezpiecznego korzystania z aplikacji mobilnych, w tym:
 - instalowanie lub aktualizacja aplikacji mobilnych tylko z zaufanych źródeł, najlepiej pochodzących od producenta danej aplikacji;
 - dokładna analiza w trakcie instalacji lub aktualizacji aplikacji mobilnych, pod kątem ich uprawnień oraz ich dostępu do usług lub danych abonenta/użytkownika.
 - systematyczna aktualizacja aplikacji mobilnych poprzez instalowanie poprawek i aktualizacji systemowych;
- 22) Korzystanie z aplikacji lub/i usług umożliwiających zdalne zablokowanie aparatu telefonicznego lub zdalne usuwanie danych z aparatu telefonicznego;
- 23) Systematyczne sprawdzanie danych i aplikacji zainstalowanych w aparacie telefonicznym, pod kątem obecności szkodliwego kodu, w szczególności wirusów;
- 24) Usunięcie przed sprzedażą lub przekazaniem aparatu telefonicznego do serwisu z pamięci wewnętrznej lub z karty pamięci poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub karty kredytowej;
- 25) Stosowanie przez abonenta/użytkownika zasad bezpiecznego korzystania z sieci Internet, w tym:
 - zainstalowanie i uruchomienie w aparacie telefonicznym programów zabezpieczających, w szczególności programu antywirusowego,
 - regularna i częsta aktualizacja sygnatur oprogramowania antywirusowego,
 - weryfikacja adresu wpisanego do przeglądarki internetowej,
 - korzystanie z połączeń szyfrowanych z wykorzystaniem protokołu HTTPS, w szczególności w trakcie wykonywania zakupów w sklepach internetowych lub dostępu do usług bankowości elektronicznej,
 - nieotwieranie wiadomości pocztowych pochodzących od nieznanymi nadawców,
 - nieodpowiadanie na wiadomości pocztowe, w których abonent/użytkownik jest proszony o podanie lub zweryfikowanie poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub kart kredytowych,
 - ignorowanie linków przesłanych w wiadomościach pocztowych lub zamieszczonych na stronach WWW, które pochodzą z podejrzanych źródeł, w szczególności zachęcają do zmiany hasła do konta/strony/serwisu internetowego,

- nieotwieranie, nieuruchamianie i nieinstalowanie żadnych plików lub aplikacji nieznanego pochodzenia, pobranych z niezaufanych stron WWW lub otrzymanych pocztą elektroniczną,
- nierejestrowanie się i nieujawnianie bez wyraźnej potrzeby na portalach/serwisach społecznościowych (jak np. Facebook, Twitter), forach dyskusyjnych czy blogach swoich danych osobowych ze względu na ryzyko wykorzystania tych informacji przez osoby nieupoważnione,
- niewyłączanie w trakcie korzystania z sieci Internet programów zabezpieczających, w szczególności aplikacji antywirusowej,
- systematyczne usuwanie plików tymczasowych przeglądarki internetowej,
- wyłączenie w przeglądarce internetowej funkcji zapamiętywania haseł w formularzach,
- nieprzechowywanie haseł do kont w serwisach internetowych w łatwo dostępnych miejscach,
- nieużywanie tego samego hasła do logowania na różnych kontach/stronach/serwisach internetowych,
- nieudostępnianie osobom trzecim identyfikatora i hasła do kont/stron/serwisów internetowych,
- unikanie stron internetowych zachęcających do obejrzenia bardzo atrakcyjnych treści lub ofert,
- zachowanie szczególnej ostrożności w przypadku korzystania z sieci Internet w miejscach publicznych lub za pomocą niezabezpieczonych sieci Wi-Fi. W takim przypadku należy ograniczyć do niezbędnego minimum wykonywanie zakupów w sklepach internetowych lub korzystanie z usług bankowości elektronicznej,
- unikanie kontrahentów, którzy jako jedyną formę płatności akceptują np. Union Money Transfer lub MoneyGram, gdyż nie ma praktycznie żadnej możliwości zidentyfikowania osoby odbierającej pieniądze. Należy wybierać tych, którzy współpracują z firmami obsługującymi płatności w sieci Internet, takimi jak np.: DotPay, eCard, PayPal, Przelewy24, PayU,
- czytanie oraz korzystanie z zasad zawartych w politykach bezpieczeństwa i politykach cookies dostawców usług internetowych.

Opracowanie:

Urząd Komunikacji Elektronicznej, Departament Detalicznego Rynku Telekomunikacyjnego

Zapraszamy do:

Centrum Informacji Konsumenckiej - infolinia 801 900 853, www.cik.uke.gov.pl