

Bezpłatny poradnik

Cyberprzemoc

Prawne aspekty bezpieczeństwa
w środowisku cyfrowym



Dla rodziców, nauczycieli i młodzieży



Opracowanie

adwokat Rafał Rozwadowski
Magdalena Maria Urbańska, MBA



Patronat honorowy



NASK



POLSKA UNIA
EDUKACYJNA

Patronat Strategiczny



Delta Robots



Kancelaria Adwokacka
Rafał Rozwadowski



Ministerstwo
Edukacji Narodowej

Projekt „iPionierzy – Łomianki Miasto Przyszłości” finansowany
ze środków Ministra Edukacji Narodowej w ramach programu
„Odkrywczy”, umowa nr MEN/2025/DK/492.

Cyberprzemoc. Prawne aspekty bezpieczeństwa w środowisku cyfrowym

Opracowanie: adwokat Rafał Rozwadowski, Magdalena Maria Urbańska, MBA

Wydawca: Pionierzy Przyszłości · ipionierzy.pl · kontakt@ipionierzy.pl

Wydanie 1: 2025. Wydanie 2, zmienione graficznie: 2026 (projekt graficzny w systemie Treningu STER, treść bez zmian merytorycznych).

Egzemplarz bezpłatny. Projekt „iPionierzy – Łomianki Miasto Przyszłości” finansowany ze środków Ministra Edukacji Narodowej w ramach programu „Odkrywcy”, umowa nr MEN/2025/DK/492.

Poradnik ma charakter informacyjny i nie stanowi porady prawnej w indywidualnej sprawie.

Spis treści

01

Wstęp

Podstawowe zasady funkcjonowania w środowisku cyfrowym

02

Podstawowe prawa w internecie

Ochrona przed cyberprzemocą, wizerunku i danych osobowych

03

Przepisy prawa karnego

Przestępstwa związane z cyberprzemocą

04

Odpowiedzialność prawna

Zasady odpowiedzialności karnej, cywilnej i nieletnich

05

Ochrona wizerunku i danych

Prawa autorskie i bezpieczne korzystanie z treści online

06

Sztuczna inteligencja

Obowiązki związane z korzystaniem z systemów AI

01

Wstęp

Cyberprzemoc nie ma precyzyjnej prawnej definicji. Ma to jednak znaczenie wtórne, gdyż sama cyberprzemoc jest jedynie pochodną określonych zachowań, które uważamy za niezgodne z prawem lub innymi normami uznawanymi za właściwe.

Różnica pomiędzy przemocą a cyberprzemocą leży w miejscu, gdzie dochodzi do nieakceptowalnych przez nas zachowań. Miejsce to wpływa na sposób postępowania naruszcyciela, na skutki, jakie powstają dla ofiary takich działań, a także na zasady odpowiedzialności za te działania i na sposób ochrony przed przejawami cyberprzemocy.

W dyskusji o cyberprzemocy warto wyjść od uznania podstawowych zasad

Funkcjonowanie w środowisku cyfrowym to dużo szans, ale i zagrożeń.

Zarówno w środowisku wirtualnym, jak i w świecie offline obowiązują przepisy prawa.

Prawo to zbiór przepisów, które określają relacje między ludźmi.

Przepisy określają, co można robić, a czego nie można robić.

Naruszenie tych zasad pociąga za sobą konsekwencje.

Przepisy dostosowują się do rozwoju technologicznego. Regulują zatem naszą obecność w sieci.

W świecie wirtualnym mamy wobec tego takie same prawa i obowiązki jak w świecie offline, ale mamy też dodatkowe prawa i obowiązki w związku ze specyfiką wirtualnej rzeczywistości.

Nieznajomość prawa szkodzi, co oznacza, że brak wiedzy o swoich prawach i obowiązkach nie uchroni nas przed odpowiedzialnością za złamanie prawa.

Świadomość swoich praw i konsekwencji prawnych swoich działań jest ważna zarówno wtedy, kiedy jesteśmy odbiorcą określonych zachowań w sieci, jak i wtedy, kiedy dotyczy to naszego zachowania.

Wyjście od ogólnych twierdzeń pozwala nam dopiero zrozumieć, że środowisko cyfrowe jest jedynie kolejną przestrzenią oddziaływania prawa. Funkcjonowanie w środowisku cyfrowym nie uwalnia nas od odpowiedzialności za działania niezgodne z prawem. Podstawowe znaczenie mają bowiem prawnie zakazane zachowania, które mogą zachodzić zarówno w świecie offline, jak i w świecie cyfrowym.

Ważne

- W sieci dzieci mogą być ofiarami przestępstw.
- Sprawcami przestępstw wobec dzieci mogą być ich rówieśnicy, ale także osoby dorosłe.
- W sieci dzieci mogą dopuszczać się zachowań stanowiących czyny karalne.

02

Podstawowe prawa w internecie

Mamy prawo m.in. do:

Ochrona przed cyberprzemocą

bycia chronionym i zabezpieczonym przed wszelkimi aktami cyberprzemocy

Ochrona wizerunku

ochrony swojego wizerunku i innych dóbr osobistych

Tajemnica korespondencji

ochrony tajemnicy korespondencji

Wolność wypowiedzi

wolności wyrażania swoich poglądów

Wolność sumienia i religii

Ważne

- Funkcjonowanie w środowisku cyfrowym nie ogranicza naszych praw.
- Zachowania, które są zabronione w świecie offline, są również zabronione w świecie cyfrowym.

Ochrona przed cyberprzemocą w internecie

Co to jest cyberprzemoc? Należy przyjąć, że jest to każda forma przemocy, która zachodzi w świecie cyfrowym. NASK (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy) definiuje cyberprzemoc jako przemoc z użyciem urządzeń elektronicznych, najczęściej telefonu bądź komputera.

Ważne

- Katalog zachowań, które mogą stanowić cyberprzemoc, nie jest zamknięty.
- Jest wiele rodzajów przemocy. Jedną z nich jest przemoc psychiczna, która nie musi się wiązać z agresją fizyczną.

Jakie są przykłady cyberprzemocy? Cyberprzemocą będą wszelkie zachowania prawnie zabronione. Będą nią również takie, których nie można zakwalifikować jako konkretnych przestępstw, ale z którymi wiążą się zachowania agresywne, krzywdzące lub nieetyczne.

Cyberprzemocą może być np.:

01**Obrażanie**

za pośrednictwem wszelkiego rodzaju komunikatorów, przy użyciu maili, SMS-ów, komentarzy w internecie itp.

02**Grożenie**

komuś, np. za pośrednictwem SMS-ów lub komunikatorów.

03**Ponizanie**

kogoś, wyśmiewanie kogoś, np. w ramach grupy stworzonej na komunikatorze czy w ramach listy mailingowej.

04**Ujawnianie danych**

czyichś danych osobowych bez zgody, np. przesyłanie innym osobom korespondencji zawierającej imię i nazwisko, adres zamieszkania.

05**Nękanie**

kogoś, np. wielokrotne, uciążliwe przesyłanie wiadomości, SMS-ów bez zgody adresata.

06**Ujawnianie korespondencji**

prywatnej korespondencji prowadzonej w sieci bez zgody, przekazywanie dalej otrzymanej korespondencji.

07**Zmuszanie**

do konkretnego zachowania, szantażowanie za pośrednictwem maili, komunikatorów.

08**Podszywanie się**

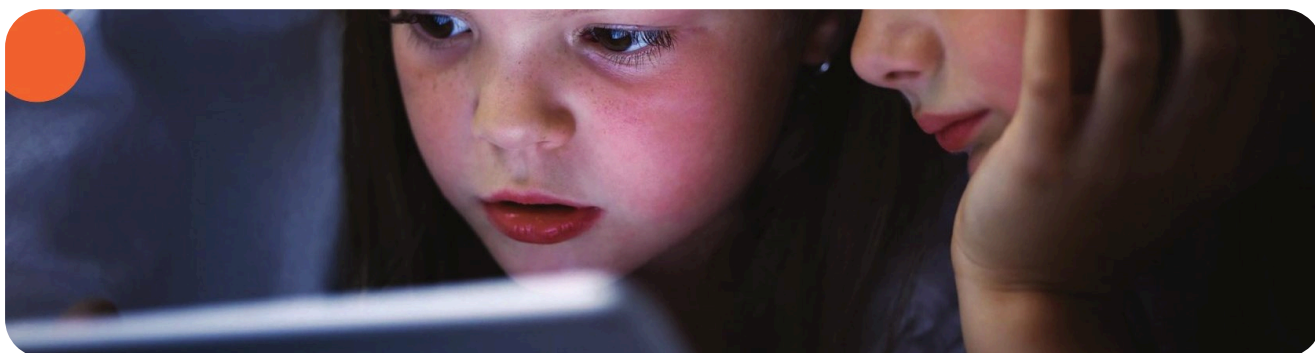
pod inną osobę.

09**Molestowanie**

wszelkie przejawy molestowania seksualnego.

10**Włamanie**

się na czyjąś skrzynkę pocztową lub na konto w mediach społecznościowych, ale także przełamanie zabezpieczeń w telefonie komórkowym.



03

Przepisy prawa karnego

Jakie przepisy prawa karnego dotyczą cyberprzemocy

Co to jest przestępstwo? Czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia, bezprawny, zawiniony, społecznie szkodliwy w stopniu wyższym niż znikomy (za: P. Kozłowska-Kalisz [w:] Kodeks karny. Komentarz aktualizowany, red. M. Mozgawa, LEX/el. 2025, art. 1).

Ważne

- **Przestępstwo ścigane z urzędu:** przestępstwo ścigane przez policję i prokuraturę po uzyskaniu informacji o jego popełnieniu, niezależnie od woli lub działania pokrzywdzonego.
- **Przestępstwo ścigane na wniosek pokrzywdzonego:** przestępstwo ścigane przez policję i prokuraturę wyłącznie po złożeniu wniosku przez pokrzywdzonego, niezależnie od uprzedniej wiedzy organów ścigania o popełnieniu tego przestępstwa.
- **Przestępstwo prywatnoskargowe:** przestępstwo ścigane bez udziału policji i prokuratury, czyli z inicjatywy pokrzywdzonego, poprzez wniesienie do sądu prywatnego aktu oskarżenia.

Przepisy prawa odnoszą się do konkretnych działań, które mogą być kwalifikowane jako cyberprzemoc. Do cyberprzemocy mogą mieć zastosowanie między innymi następujące przepisy.

Art. 190a § 1 Kodeksu karnego: stalking

Treść przepisu

Kto przez uporczywe nękanie innej osoby lub osoby dla niej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność (...)

Ważne: istotne elementy tego przestępstwa

- Nękanie to inaczej uporczywe dręczenie.
- Wymaga powtarzalności.
- Może być zachowaniem jednorodnym, np. wysyłanie niechcianych SMS-ów, lub różnorodnym, np. wysyłanie niechcianych SMS-ów i wystawianie pod domem.
- Aby zaszło, wystarczy, że zajdzie jeden z czterech poniższych skutków.

Poczucie zagrożenia

odczucie niepokoju, obawa o siebie lub swoich najbliższych

Poczucie poniżenia

efektem stalkingu jest naruszenie dóbr osobistych

Poczucie udręczenia

poczucie fizycznego lub psychicznego cierpienia

Naruszenie prywatności

powinno być istotne, np. nachodzenie w domu

**Art. 190a § 2 KK: kradzież tożsamości****Treść przepisu**

Kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, przez co wyrządza jej szkodę majątkową lub osobistą (...)

Ważne: istotne elementy tego przestępstwa

- Podszywanie następuje z wykorzystaniem wizerunku lub innych danych osobowych.
- Skutkiem kradzieży tożsamości jest szkoda majątkowa lub osobista, bądź oba rodzaje szkody łącznie.
- Szkoda majątkowa to uszczerbek, który można wyrazić w pieniądzu, np. utrata środków z konta bankowego.
- Szkoda osobista to uszczerbek, którego nie można wyrazić w pieniądzu, np. utrata dobrego imienia.

Co to są dane osobowe? Zgodnie z RODO oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Art. 190 KK: groźba karalna

Treść przepisu

Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub na szkodę osoby dla niej najbliższej, jeżeli groźba wzbudza w osobie, do której została skierowana lub której dotyczy, uzasadnioną obawę, że będzie spełniona (...)

Ważne: istotne elementy tego przestępstwa

- Grozić komuś to znaczy straszyć go.
- Przedmiotem groźby musi być zapowiedź popełnienia konkretnego przestępstwa.
- Grozić komuś można na wiele sposobów: zachowaniem, słowem, tekstem, SMS-em, mailem.
- Groźba powinna wzbudzić uzasadnioną obawę. Ocenia się to w indywidualnych przypadkach, biorąc pod uwagę, czy przeciętny człowiek o cechach porównywalnych do cech ofiary uznałby spełnienie groźby za realne.

Art. 212 KK: zniesławienie

Treść przepisu

Kto pomawia inną osobę, grupę osób, instytucję, osobę prawną lub jednostkę organizacyjną niemającą osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności (...)

Ważne: istotne elementy tego przestępstwa

- Pomawianie polega na wypowiedzianiu własnych twierdzeń lub rozpowszechnianiu, przytaczaniu twierdzeń innych osób.
- Pomówić kogoś można również SMS-em, mailem czy wpisem internetowym.
- Pomawianie może dotyczyć postępowania, tj. działań, aktywności danej osoby, lub jej cech, np. intelektu, charakteru.

Art. 216 KK: zniewaga

Treść przepisu

Kto znieważa inną osobę w jej obecności albo choćby pod jej nieobecność, lecz publicznie lub w zamiarze, aby zniewaga do osoby tej dotarła (...)

Ważne: istotne elementy tego przestępstwa

- Znieważenie to obelżywe zachowanie się wobec danej osoby.
- Obelżywość zachowania polega na uznaniu, że użyty język lub gest jest wulgarny i społecznie uznawany za nieakceptowalny.
- Nie będzie znieważeniem krytyka czy niezachowanie reguł grzecznościowych.
- Przestępstwo znieważenia można popełnić na trzy podstawowe sposoby.

01**Bezpośrednia zniewaga**

Zniewaga jest skierowana bezpośrednio do osoby znieważanej, np. przez SMS.

02**Zniewaga publiczna**

Zniewaga ma charakter publiczny i nie ma znaczenia, czy w tym publicznym przekazie uczestniczy osoba znieważana.

03**Zniewaga pośrednia**

Zniewaga dotyczy osoby, która jest nieobecna, ale sprawca chce, aby dotarła do osoby znieważanej.

Art. 267 KK: bezprawne pozyskanie informacji**Treść przepisu**

Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie (§ 1). Kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego (§ 2). Kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem (§ 3) (...)

Ważne: istotne elementy tego przestępstwa

- Przestępstwo można popełnić poprzez uzyskanie dostępu do cudzej korespondencji.
- Może to być otwarcie listu, zabranie z szuflady notatek, ale też podłączenie się do niezabezpieczonej hasłem, ale niedostępnej ogólnie sieci Wi-Fi.
- Przełamanie zabezpieczeń to wykorzystanie oprogramowania, aby przełamać zabezpieczenia przed dostępem, np. do konta w mediach społecznościowych, skrzynki pocztowej.
- Wyłudzenie hasła lub uzyskanie go podstępem (np. poprzez tzw. phishing) stanowić będzie tzw. uzyskanie dostępu do całości lub części systemu informatycznego.

Zmuszanie i przestępstwa seksualne**Art. 191 § 1 KK: zmuszanie do określonego działania**

Treść przepisu

Kto, stosując przemoc wobec osoby lub groźbę bezprawną, zmusza ją lub inną osobę do określonego działania, zaniechania lub znoszenia (...)

Ważne: istotne elementy tego przestępstwa

- Przemoc ujęta w tym przepisie związana jest z przemocą fizyczną. W sieci prędzej zatem dojdzie do takiego przestępstwa, jeśli zmusza się inną osobę do określonego zachowania za pomocą groźby bezprawnej, np. grożąc pobiciem lub popełnieniem innego przestępstwa.
- Zmuszanie do określonego działania polega na przełamaniu wolnej woli do podejmowania własnych decyzji.

Cyberprzemocą mogą być również przestępstwa przeciwko wolności seksualnej i obyczajności, takie jak np.:

Art. 191a KK

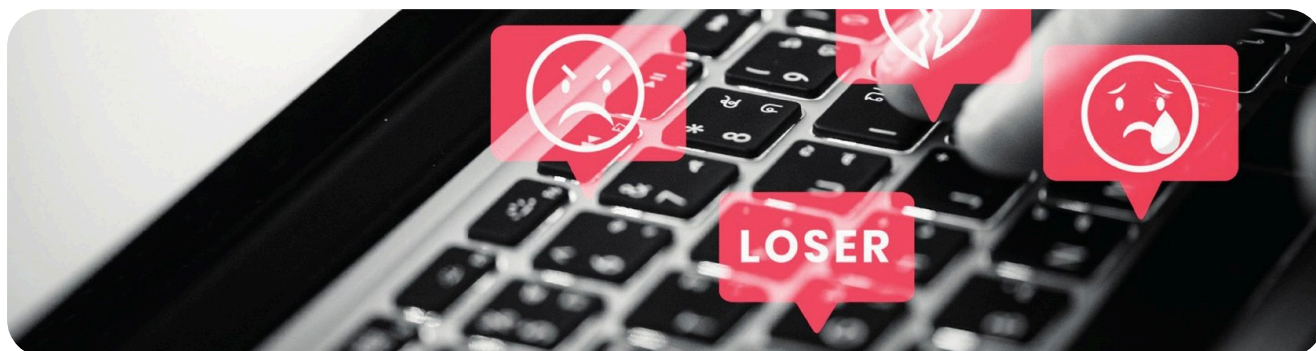
Naruszenie intymności seksualnej

Art. 200 KK

Seksualne wykorzystanie małoletniego

Art. 202 KK

Publiczne prezentowanie treści pornograficznych

**Przestępstwo na szkodę nauczyciela**

Kto to jest nauczyciel? Zgodnie z ustawą z dnia 26 stycznia 1982 r. Karta Nauczyciela przez nauczycieli (wtedy, kiedy nie ma bardziej precyzyjnego określenia w ustawie) rozumie się nauczycieli, wychowawców i innych pracowników pedagogicznych zatrudnionych w przedszkolach, szkołach i placówkach wymienionych w art. 1 ust. 1 tej ustawy.

Ważne

- Zgodnie z art. 63 ustawy Karta Nauczyciela nauczyciel podczas lub w związku z pełnieniem obowiązków służbowych korzysta z ochrony przewidzianej dla funkcjonariuszy publicznych na zasadach określonych w ustawie z dnia 6 czerwca 1997 r. Kodeks karny.
- Organ prowadzący szkołę i dyrektor szkoły są obowiązani z urzędu występować w obronie nauczyciela, gdy ustalone dla nauczyciela uprawnienia zostaną naruszone.
- Dlaczego przyznanie nauczycielowi ochrony jak dla funkcjonariusza publicznego jest tak ważne? Kodeks karny zawiera szereg przestępstw, które mogą być popełnione na szkodę funkcjonariusza publicznego. W rezultacie ochrona prawna nauczycieli jest taka sama jak ochrona np. policjanta, sędziego, posła lub senatora.

Np. art. 226 KK: znieważenie funkcjonariusza publicznego (nauczyciela)**Treść przepisu**

Kto znieważa funkcjonariusza publicznego lub osobę do pomocy mu przybraną, podczas i w związku z pełnieniem obowiązków służbowych (...)

Ważne

- Znieważenie musi nastąpić podczas i w związku z pełnieniem obowiązków służbowych.

Odpowiedzialność prawna

Kto odpowiada za cyberprzemoc?

Ważne

- Na zasadach określonych w Kodeksie karnym odpowiada ten, kto popełnia czyn zabroniony po ukończeniu 17 lat.
- Osoba, która nie ukończyła 17 lat, jest nazywana „nieletnim”. Nie należy mylić tego pojęcia z „małoletnim”, które wynika z przepisów cywilnych i określa osobę poniżej 18. roku życia.

Nieletni nie odpowiadają karnie. Są pewne wyjątki, które dotyczą określonych i bardzo poważnych przestępstw.

Zbrodnia i występki

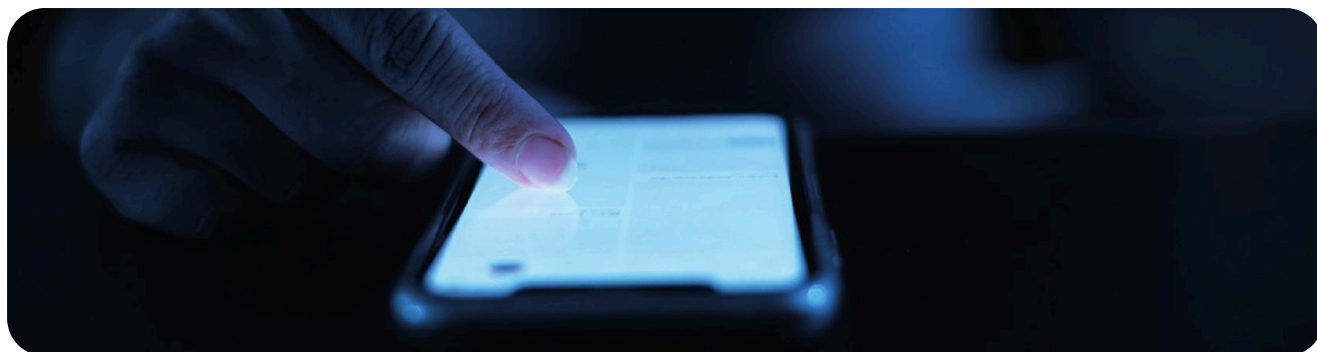
Przestępstwo jest zbrodnią albo występkiem. Zbrodnią jest czyn zabroniony zagrożony karą pozbawienia wolności na czas nie krótszy od lat 3 albo karą surowszą. Występkiem jest czyn zabroniony zagrożony grzywną powyżej 30 stawek dziennych albo powyżej 5000 złotych, karą ograniczenia wolności przekraczającą miesiąc albo karą pozbawienia wolności przekraczającą miesiąc.

Sprawcy pomiędzy 17. a 18. rokiem życia

W stosunku do sprawcy, który popełnił występki po ukończeniu lat 17, lecz przed ukończeniem lat 18, sąd zamiast kary stosuje środki wychowawcze, lecznicze albo poprawcze przewidziane dla nieletnich, jeżeli okoliczności sprawy oraz stopień rozwoju sprawcy, jego właściwości i warunki osobiste za tym przemawiają.

Dlaczego rozmawiamy o przestępstwach z Kodeksu karnego, jeśli wiemy, że odpowiedzialność karną ponoszą co do zasady osoby po ukończeniu 17. roku życia? Czy oznacza to, że osoby, które mają mniej lat, a popełniły czyny, które wypełniają znamiona przestępstw lub wykroczeń, nie ponoszą odpowiedzialności? Czy mogą czuć się bezkarne?

Nie. Ustawodawca przewidział inne formy odpowiedzialności dla młodszych osób, dla których przepisy Kodeksu karnego czy przepisy Kodeksu wykroczeń mogą być tylko pewnym „punktem odniesienia”. Odniesienie to w uproszczeniu polega na tym, że jeżeli osoba młodsza, np. 13-latek, zachowała się w sposób, który jest zabroniony przepisem karnym, np. uporczywie nękała kogoś SMS-ami czy wiadomościami na komunikatorze, to wprowadzie nie poniesie ona odpowiedzialności karnej, ale z racji tego konkretnie opisanego zachowania z Kodeksu karnego może ponieść innego rodzaju odpowiedzialność.



Odpowiedzialność nieletnich

Zasady tej odpowiedzialności określone są w ustawie z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich. Warto wiedzieć, że ustawa ta uchyliła ustawę z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich.

Ważne: przepisy ustawy o wspieraniu i resocjalizacji nieletnich stosuje się w zakresie

1. postępowania w sprawach o demoralizację wobec osób, które ukończyły 10 lat i nie są pełnoletnie;
2. postępowania w sprawach o czyny karalne wobec osób, które dopuściły się takiego czynu po ukończeniu 13 lat, ale przed ukończeniem 17 lat;
3. wykonywania środków wychowawczych, środka leczniczego lub środka poprawczego wobec osób, względem których środki te zostały orzeczone, nie dłużej jednak niż do ukończenia przez te osoby 21 lat, chyba że ustawa stanowi inaczej.

Czyli już nawet 10-latek może odpowiadać w przypadku stwierdzenia demoralizacji.

Co to jest demoralizacja? Nie ma jednolitej definicji demoralizacji. Na podstawie art. 4 ustawy o wspieraniu i resocjalizacji nieletnich okolicznościami świadczącymi o demoralizacji będą w szczególności:

dopuszczenie się czynu zabronionego,

naruszanie zasad współżycia społecznego,

uchylanie się od obowiązku szkolnego lub obowiązku nauki,

używanie alkoholu, środków odurzających, substancji psychotropowych, ich prekursorów, środków zastępczych lub nowych substancji psychoaktywnych, uprawianie nierzędu.

Zgodnie ze wskazówkami Policji przejawami demoralizacji mogą być np.: wulgarne słownictwo, stosowanie agresji, przemocy, wagarowanie, palenie papierosów, wandalizm, spożywanie alkoholu, ucieczki z domu, zażywanie narkotyków, przedwczesne podejmowanie życia seksualnego.

Pojęcie demoralizacji jest szersze niż pojęcie czynu zabronionego. Obejmuje ono bowiem zachowania, które są społecznie czy moralnie nieakceptowalne, ale niekoniecznie muszą wypełniać znamiona czynów zabronionych. Wobec nieletniego mogą być stosowane środki wychowawcze, środek leczniczy i środek poprawczy.

Ważne: sąd rodzinny, który prowadzi sprawy o demoralizację i popełnienie czynów karalnych, może

1. zobowiązać rodziców albo opiekuna nieletniego do poprawy warunków wychowawczych, bytowych lub zdrowotnych nieletniego, a także do ścisłej współpracy ze szkołą, do której nieletni uczęszcza, z poradnią psychologiczno-pedagogiczną, w tym w razie potrzeby wykonania odpowiedniej diagnozy nieletniego, oraz z podmiotem wykonującym działalność leczniczą;
2. zobowiązać rodziców albo opiekuna nieletniego do współpracy z młodzieżowym ośrodkiem socjoterapii w zakresie realizacji obowiązku nauki przez nieletniego, jego socjoterapii i pomocy psychologiczno-pedagogicznej;
3. zobowiązać rodziców albo opiekuna nieletniego do naprawienia w całości albo w części szkody wyrządzonej przez nieletniego lub do zadośćuczynienia za doznaną krzywdę.



Odpowiedzialność cywilna za cyberprzemoc

Odpowiedzialność cywilna w dużym uproszczeniu polega na ponoszeniu konsekwencji majątkowych z powodu swoich działań niezgodnych z prawem.

Poniżej 13 lat

Małoletni, którzy nie ukończyli 13. roku życia, nie ponoszą odpowiedzialności cywilnej za wyrządzoną szkodę na zasadzie winy. Oznacza to, że mogą ponosić odpowiedzialność na zasadzie np. ryzyka czy słuszności.

13–18 lat

Małoletni powyżej 13. roku życia w teorii powinni odpowiadać samodzielnie na zasadzie winy, niemniej zależy to też od oceny, czy można im, z uwagi na indywidualne kryteria, taką winę przypisać.

Powyżej 18 lat

Pełną odpowiedzialność cywilną ponoszą osoby, które ukończyły 18 lat.

Za szkody spowodowane przez małoletnich poniżej 13. roku życia odpowiadają osoby zobowiązane do nadzoru nad takimi osobami. Podobnie jest w sytuacji małoletnich powyżej 13. roku życia przed ukończeniem 18. roku życia, kiedy nie można, z uwagi na ich rozwój emocjonalny, przypisać im winy.

Rodzice mogą ponosić także odpowiedzialność odszkodowawczą na podstawie ustawy o wspieraniu i resocjalizacji nieletnich. Zgodnie z art. 18 ust. 1 pkt 3 tej ustawy sąd rodzinny może m.in. zobowiązać rodziców albo opiekuna nieletniego do naprawienia w całości albo w części szkody wyrządzonej przez nieletniego lub do zadośćuczynienia za doznaną krzywdę.

W przypadku cyberprzemocy odpowiedzialność cywilna może być np. ponoszona w przypadku naruszenia dóbr osobistych. Obrażając kogoś w sieci, musimy liczyć się z tym, że naruszamy dobra osobiste tej osoby i poza odpowiedzialnością karną możemy ponieść odpowiedzialność cywilną za wyrządzoną szkodę.



Jakie kroki podjąć, gdy spotykamy się z podejrzeniem cyberprzemocy?

System prawny wyróżnia powszechny, prawny i społeczny obowiązek zawiadomienia o przestępstwie.

Prawny obowiązek dotyczy tylko niektórych bardzo poważnych przestępstw, np. zabójstwa, spowodowania ciężkiego uszczerbku na zdrowiu, szpiegostwa. Brak dopełnienia tego obowiązku może prowadzić samodzielnie do poniesienia odpowiedzialności karnej przez osobę, która nie zawiadomiła o możliwości popełnienia przestępstwa.

Ważne

- W kontekście cyberprzemocy warto zwrócić szczególną uwagę, że w zakres tego obowiązku wchodzi art. 200 (§ 1, 3, 4, 5: pedofilia, prezentowanie małoletniemu poniżej lat 15 treści pornograficznych, prezentowanie takiemu małoletniemu wykonania czynności seksualnej, prowadzenie reklamy lub promocji rozpowszechniania treści pornograficznych).

Społeczny obowiązek dotyczy pozostałych przestępstw „ściganych z urzędu”. Nie ma prawnej sankcji za niedochowanie obowiązku społecznego zawiadomienia o przestępstwie. Swoistego rodzaju sankcją może być odpowiedzialność społeczna (moralna).

Warto dodać, że prawny obowiązek zawiadomienia o przestępstwie odnosi się w swoisty sposób do instytucji państwowych i samorządowych i dotyczy przestępstw ściganych z urzędu, o których owe instytucje dowiedziały się w związku ze swą działalnością.

Należy też odrębnie odnieść się do obowiązku zawiadomienia odpowiednich organów wynikającego z ustawy o wspieraniu i resocjalizacji nieletnich. Ustawa ta zawiera trzy podstawowe regulacje dotyczące obowiązku zawiadomienia odpowiednich organów (art. 4).

Obowiązek społeczny: demoralizacja

Każdy, kto stwierdzi istnienie okoliczności świadczących o demoralizacji nieletniego, w szczególności dopuszczenie się czynu zabronionego, naruszanie zasad współżycia społecznego, uchylanie się od obowiązku szkolnego lub obowiązku nauki, używanie alkoholu, środków odurzających, substancji psychotropowych, ich prekursorów, środków zastępczych lub nowych substancji psychoaktywnych, zwanych dalej „substancją psychoaktywną”, uprawianie nierzędu, ma społeczny obowiązek odpowiednio przeciwdziałać temu, a przede wszystkim zawiadomić o tym rodziców lub opiekuna nieletniego, szkołę, sąd rodzinny, Policję lub inny właściwy organ.

Obowiązek społeczny: czyn karalny

Każdy, dowiedziawszy się o dopuszczeniu się przez nieletniego czynu karalnego, ma społeczny obowiązek zawiadomić o tym sąd rodzinny lub Policję.

Są to obowiązki, których niedochowanie nie jest zagrożone sankcją prawną. Obowiązkiem prawnym jest natomiast ten skierowany do instytucji w brzmieniu jak niżej:

Obowiązek prawny instytucji

Instytucje państwowe i samorządowe oraz publiczne i niepubliczne szkoły i placówki oświatowe, które w związku ze swoją działalnością dowiedziały się o dopuszczeniu się przez nieletniego czynu zabronionego wyczerpującego znamiona przestępstwa ściganego z urzędu lub przestępstwa skarbowego, są obowiązane niezwłocznie zawiadomić o tym sąd rodzinny lub Policję oraz przedsięwziąć niezbędne czynności, aby nie dopuścić do zatarcia śladów i dowodów popełnienia czynu zabronionego.

Powstanie tego obowiązku np. po stronie szkoły (bo jest to już obowiązek prawny, a nie społeczny) zależne będzie od ustalenia, czy:

01

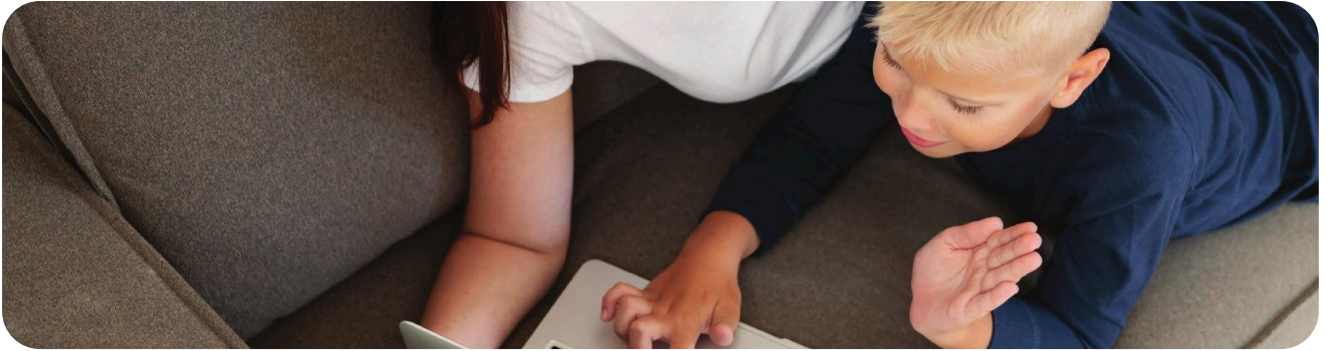
Mamy do czynienia z dopuszczeniem się przez nieletniego czynu zabronionego wyczerpującego znamiona przestępstwa ściganego z urzędu.

02

Wiedzę taką szkoła uzyskała w związku ze swoją działalnością.

Ważne

- W sytuacji podejrzenia cyberprzemocy zaleca się zabezpieczenie materiałów, które mogą w przyszłości stanowić dowód w sprawie. Rekomendowanym rozwiązaniem jest sporządzenie notarialnych protokołów okazania, np. wiadomości mail, co zabezpieczać będzie takie dane na poczet ewentualnego przyszłego postępowania.



Ochrona wizerunku i danych

Ochrona wizerunku w internecie

Co to jest wizerunek? Nie ma jednolitej prawnej definicji wizerunku. Wizerunek należy definiować jako cechy człowieka, które składają się na jego wygląd i pozwalają na indywidualną identyfikację.

W poglądach doktryny i orzecznictwa twierdzi się, że jest to obraz fizyczny zaprezentowany choćby w formie ulotnej, np. emisji nadawanego na żywo programu telewizyjnego (T. Grzeszak [w:] System Prawa Prywatnego, t. 13, s. 783, nt 9), albo w postaci podobizny utrwalonej na odpowiednim nośniku, np. zdjęciu, obrazie, nagraniu filmowym (wyrok SO we Wrocławiu z 13.05.2014 r., I C 1777/12, LEX nr 1541210), w formie portretu, fotografii (wyrok SN z 7.10.2009 r., III CSK 39/09, OSNC-ZD 2010/D, poz. 100) lub wytworu materialnego, który za pomocą środków plastycznych przedstawia podobiznę osoby fizycznej (wyrok SA w Warszawie z 21.04.2005 r., I ACa 566/04, LEX nr 1680186) (również za: B. Janiszewska [w:] Kodeks cywilny. Komentarz. Tom I. Część ogólna, cz. 1 (art. 1–55(4)), red. J. Gudowski, Warszawa 2021, art. 23).

W jaki sposób nasz wizerunek jest chroniony w internecie? Wizerunek jest jednym z naszych dóbr osobistych. W przypadku naruszenia dobra osobistego, zgodnie z art. 24 Kodeksu cywilnego, ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania (chyba że nie jest ono bezprawne).

W razie dokonanego naruszenia może on 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 przewidzianych w Kodeksie cywilnym może on również żądać zadośćuczynienia pieniężnego albo zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.

Wizerunek jest również chroniony przepisami prawa autorskiego. Zgodnie z art. 81 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej, z wyjątkami wskazanymi w tymże przepisie.

Wizerunek można uznać również za daną osobową, stąd zgoda na przetwarzanie danych osobowych w postaci wizerunku jest wymagana. Zgoda ta stanowi inną zgodę aniżeli zgoda na rozpowszechnienie wizerunku, o której mowa w przepisach prawa autorskiego.

Ważne

- Nie można zatem bez zgody rozpowszechniać naszego wizerunku. Nie można też modyfikować przedmiotu ewentualnie udzielonej zgody i np. rozpowszechniać wizerunku w kontekstach naruszających nasze inne dobra osobiste, np. część i godność.

Jakie są przykłady naruszenia praw do naszego wizerunku? Klasycznym przykładem naruszenia naszego prawa do wizerunku będzie jego rozpowszechnienie bez naszej zgody. Może to też być ingerencja w nasz wizerunek i np. zaprezentowanie go w formie poniżającej modyfikacji.

Kto może zgodzić się na rozpowszechnienie wizerunku dziecka? Dzieci, które nie ukończyły lat 13, nie mają zdolności do czynności prawnych, stąd nie mogą same wyrażać zgody na rozpowszechnienie swojego wizerunku. Taką zgodę mogą wyrazić tylko ich przedstawiciele ustawowi, najczęściej będą to rodzice.

Dzieci, które ukończyły lat 13, a nie są pełnoletnie, czyli nie ukończyły 18 lat, mają ograniczoną zdolność do czynności prawnych. Oznacza to, że mogą bez zgody przedstawiciela ustawowego zawierać umowy należące do umów powszechnie zawieranych w drobnych, bieżących sprawach życia codziennego.

Nie ma jednoznacznego stanowiska w zakresie, w jakim bezwzględnie wymaga się, aby zgoda na rozpowszechnienie wizerunku dziecka pomiędzy 13. a 18. rokiem życia udzielana była też przez rodziców. Bezspornie zgoda taka jest niezbędna w sytuacji, gdy wraz z rozpowszechnianiem wizerunku wiążą się określone zobowiązania, np. mamy do czynienia z kontraktem reklamowym lub w innych sytuacjach, w których rozpowszechnianie wizerunku może nieść ze sobą istotne skutki lub zagrożenia dla dziecka.

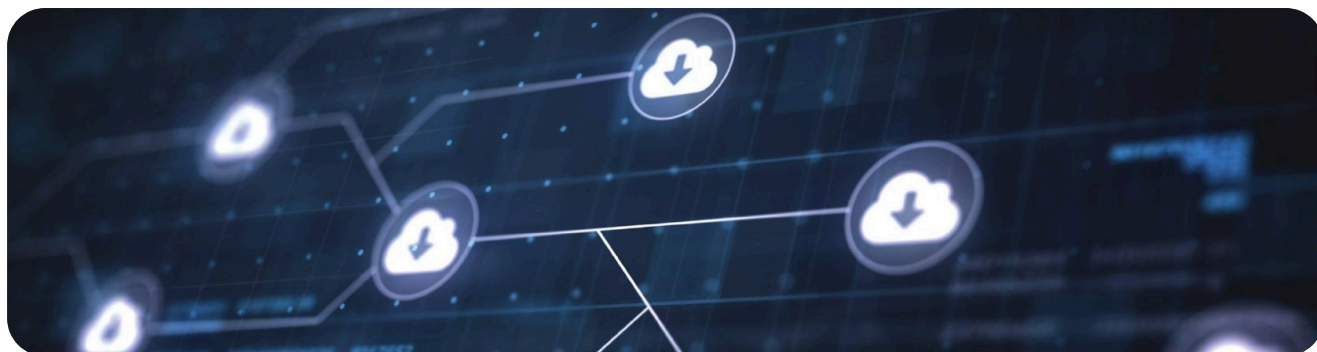
Zasadne jest zatem takie podejście, które nakazuje szeroko interpretować obowiązek uzyskania takiego potwierdzenia lub zgody rodziców, biorąc pod uwagę zarówno obowiązek sprawowania opieki nad dzieckiem, jak i dbania o jego prawidłowy rozwój. Przyznanie bowiem dziecku pomiędzy 13. a 18. rokiem życia całkowitej samodzielności w decydowaniu o prawie do swojego wizerunku może powodować dla niego niepożądane szkody, chociażby z perspektywy niedostatecznego rozeznania konsekwencji rozpowszechnienia jego wizerunku (np. w internecie).

Ważne

- Po ukończeniu 18. roku życia dziecko uzyskuje całkowitą samodzielność w decydowaniu o wykorzystaniu swojego wizerunku.

Poglądowo wskazać należy na regulację RODO, która w art. 8 stanowi, iż jeżeli zastosowanie ma art. 6 ust. 1 lit. a) (chodzi o sytuację, gdy dziecko wyraziło samodzielnie zgodę na przetwarzanie jego danych osobowych), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem, oraz wyłącznie w zakresie wyrażonej zgody.

Co to jest przetwarzanie? Zgodnie z RODO oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.



Ochrona danych osobowych w internecie

Nasze dane osobowe są chronione przepisami prawa i powinniśmy mieć prawo decydować, w jakim zakresie będą przetwarzane.

Ważne

- Brak naszej zgody i innych prawnie uzasadnionych podstaw do przetwarzania naszych danych osobowych (np. rozpowszechnianie w sieci imienia, nazwiska, adresu zamieszkania) może powodować odpowiedzialność prawną.

Zgodne z prawem korzystanie z treści w internecie

Czy są jakieś treści, których nie można publikować w internecie? Tak, między innymi treści:

nawołujące do popełnienia przestępstw,

stanowiące przestępstwa, takie jak groźby, zniewagi itp.,

objęte prawem autorskim, bez zgody twórcy,

zawierające materiały pornografii dziecięcej,

propagujące nazistowski, komunistyczny, faszystowski lub inny totalitarny ustrój państwa lub nawołujące do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość,

propagujące ideologię nazistowską, komunistyczną, faszystowską lub ideologię nawołującą do użycia przemocy w celu wpływania na życie polityczne lub społeczne,

ujawniające dane osobowe bez zgody.

Czy możemy bez ograniczeń korzystać z treści w internecie? Przede wszystkim musimy wiedzieć, że w internecie zamieszczane są treści, które często są chronione prawem autorskim, co oznacza, że nie możemy z nich dowolnie korzystać. Prawa autorskie to ogół praw, które przysługują twórcy i pozwalają mu chronić swój utwór przed niedozwolonym wykorzystywaniem.

Co to jest utwór? Każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia. Będzie to zatem np. wiersz, zdjęcie, artykuł opublikowany w internecie.

Autor ma wobec swojego utworu tzw. prawa osobiste i prawa majątkowe. Autorskie prawa osobiste dają mu wyłączne i niezbywalne prawo np. do oznaczania utworu swoim imieniem lub nazwiskiem, nieingerowania w treść i formę swojego utworu czy też decydowania, kiedy po raz pierwszy zaprezentuje go publicznie. Autorskie prawa majątkowe dają natomiast autorowi prawo do rozporządzania nim w różny sposób i czerpania z niego korzyści.

Ważne

- To, że utwór został zamieszczony w internecie, nie oznacza, że jest zgoda autora na jego wykorzystywanie.

Czy jest możliwość nieodpłatnego korzystania z utworów w sieci? Na początku trzeba zauważyć, że korzystać z utworów można, jeśli zawrze się z autorem umowę. W internecie najczęściej jest to zawarcie umowy licencyjnej, która uprawnia do korzystania z danego utworu w zamian za tzw. opłatę licencyjną.

Darmowe korzystanie z utworów jest możliwe, gdy objęte jest np. darmową licencją (np. freeware), tj. autor zdecydował, że można bez opłat korzystać z jego utworu.

Darmowe korzystanie z utworu jest też możliwe w ramach tzw. dozwolonego użytku osobistego. Zgodnie z art. 23 ustawy o prawie autorskim i prawach pokrewnych bez zezwolenia twórcy wolno nieodpłatnie korzystać z już rozpowszechnionego utworu w zakresie własnego użytku osobistego. Dozwolony użytek jest zatem możliwy, jeśli z utworu korzysta osoba fizyczna i dotyczy to utworu, który został już rozpowszechniony, a korzystanie to jest na własny użytek osobisty lub na użytek osób bliskich.

Ważne

- Jeżeli korzysta się z utworu w ramach dozwolonego użytku, należy podać imię i nazwisko twórcy oraz źródło.

Formą dozwolonego użytku jest również określone w prawie autorskim tzw. „prawo cytatu”. Zgodnie z art. 29 ustawy o prawie autorskim i prawach pokrewnych wolno przytaczać w utworach stanowiących samoistną całość urywki rozpowszechnionych utworów oraz rozpowszechnione utwory plastyczne, utwory fotograficzne lub drobne utwory w całości, w zakresie uzasadnionym celami cytatu, takimi jak wyjaśnianie, polemika, analiza krytyczna lub naukowa, nauczanie lub prawami gatunku twórczości.

Inną kwestią jest tzw. dozwolony użytek publiczny. Odnosi się on do możliwości korzystania z utworów pod określonymi warunkami, np. przez instytucje oświatowe, jednostki naukowe, uczelnie.

Co grozi za niezgodne z prawem korzystanie z treści w internecie? W przypadku nielegalnego korzystania z treści chronionych prawem autorskim uprawnionemu przysługuje szereg roszczeń. Roszczenia te są związane z naruszeniem praw osobistych, jak i majątkowych.

W sytuacji naruszenia praw osobistych można dochodzić od osoby, która dopuściła się naruszenia, aby 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.

W przypadku naruszenia praw majątkowych można żądać od osoby, która naruszyła te prawa: zaniechania naruszania, usunięcia skutków naruszenia, naprawienia wyrządzonej szkody, wydania uzyskanych korzyści.

Nielegalne korzystanie z czyjejś twórczości w sieci może również powodować odpowiedzialność karną.

Sztuczna inteligencja

Czy korzystanie z „systemów AI” wiąże się z dodatkowymi obowiązkami?

Sztuczna inteligencja wiąże się z powstawaniem nowych regulacji prawnych i z próbami nowej interpretacji regulacji już obowiązujących. Spowodowane jest to tym, że możliwości i funkcjonalności AI tworzą często nowe, nierozpoznane dotychczas sytuacje, do których obowiązujące dotychczas przepisy prawa nie są idealnie dopasowane.

Ważne

- Należy pamiętać, iż korzystanie z AI jako narzędzia w działaniach w sieci, które to działania mogą nosić znamiona czynów zabronionych, nie zwalnia nas z odpowiedzialności.

Przykładowo wygenerowany przez AI wpis w komunikatorze, który grozi innej osobie, może stanowić przestępstwo. Nie będzie usprawiedliwiać tego wpisu np. twierdzenie, że nie został on dostatecznie sprawdzony przez autora przed publikacją.

Nieodpowiedzialne korzystanie z narzędzi AI, w tym często bezrefleksyjne przyjmowanie i używanie wytworów AI, może rodzić konsekwencje prawne m.in. z powodu wprowadzania w błąd, szerzenia dezinformacji, fałszywego alarmowania o różnych zdarzeniach itp.

Prawo sztucznej inteligencji jest de facto połączeniem wielu dziedzin prawa, z uwzględnieniem specyfiki funkcjonowania i stosowania narzędzi AI. Ma zatem również wpływ na kwestie związane z prawami autorskimi. Zastanawia się m.in. nad tym, na ile wytwory wygenerowane przez AI mogą stanowić przedmiot prawa autorskiego (obecnie przeważa pogląd, że nie są chronione prawem autorskim).

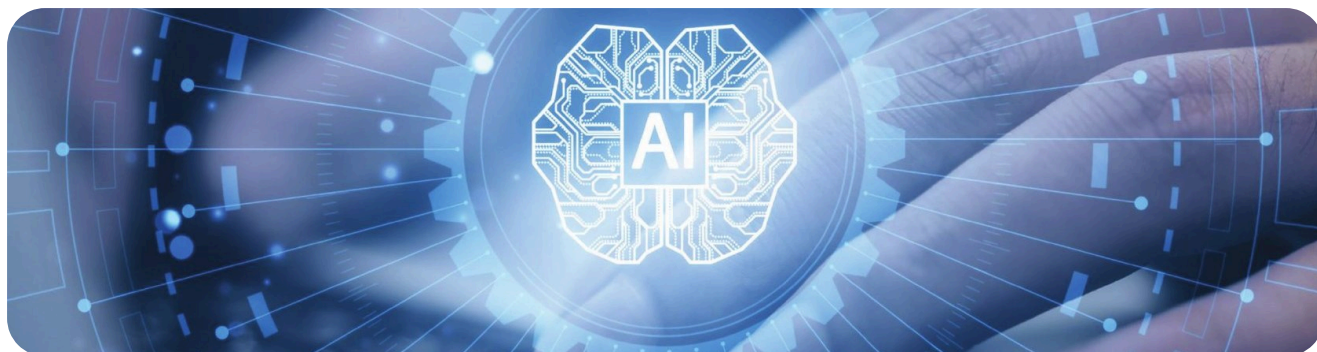
Prawo zajmuje się również szkodliwością nielegalnych deepfake'ów, czyli treści generowanych lub współgenerowanych przez AI, które „pretendują” do tego, aby być uznawane za treści rzeczywiste.

Prawo pochyla się także nad możliwością wykorzystywania AI przy pisaniu własnych prac, które np. są podstawą do uzyskania dyplomu czy innego prawnie istotnego dokumentu. Tutaj dyskusje mogą być prowadzone w kierunku możliwego popełnienia przestępstwa z art. 272 KK, zgodnie z którym kto wyłudza poświadczenie nieprawdy przez podstępne wprowadzenie w błąd funkcjonariusza publicznego lub innej osoby upoważnionej do wystawienia dokumentu, podlega karze pozbawienia wolności do lat 3.

Korzystanie z AI otwiera dyskusję nie tylko prawną, ale również etyczną, i to w wielu aspektach. Stawia pytanie, na ile korzystanie z AI powinno być ujawniane, aby nie wprowadzać w błąd innych osób czy instytucji co do swoich rzeczywistych kompetencji. Na ile możemy polegać na ocenie AI i czy dzisiejsza niedoskonałość i omylność tego narzędzia nie wymaga korzystania z niego w sposób ostrożniejszy i obwarowany dodatkowymi obowiązkami?

Pamiętaj

Dzisiejsze prawo stara się nadążyć za rozwojem technologicznym. Pomimo szeregu zagadnień, które są cały czas w opracowaniu, należy pamiętać, że to człowiek odpowiada za wykorzystywanie AI w swoim życiu codziennym i zawodowym, co oznacza, że użycie lub wykorzystanie go niezgodnie z prawem będzie rodzić odpowiedzialność prawną.



Notatki



Trzymaj ster w cyfrowym świecie

Poradnik powstał w projekcie „iPionierzy – Łomianki Miasto Przyszłości”. Dziś jest częścią materiałów Treningu STER: programu, który uczy dzieci 7–15 lat i ich rodziców samokontroli, bezpiecznego korzystania z technologii, radzenia sobie z emocjami oraz zasad relacji i prawa w sieci.



treningster.pl



ipionierzy.pl

kontakt@ipionierzy.pl

+48 723 680 503

Egzemplarz bezpłatny. Opracowanie: adwokat Rafał Rozwadowski, Magdalena Maria Urbańska, MBA. Wydawca: Pionierzy Przyszłości. Wydanie 1: 2025. Wydanie 2, zmienione graficznie: 2026, projekt graficzny w systemie Treningu STER. Treść poradnika nie stanowi porady prawnej w indywidualnej sprawie.

Patronat honorowy



NASK



POLSKA UNIA
EDUKACYJNA



Ministerstwo
Edukacji Narodowej

Patronat Strategiczny



Delta Robots



Kancelaria Adwokacka
Rafał Rozwadowski



Projekt „iPionierzy – Łomianki Miasto Przyszłości” finansowany ze środków Ministra Edukacji Narodowej w ramach programu „Odkrywczy”, umowa nr MEN/2025/DK/492.