Dariusz Skrzyński

Cyberprzestępczość szkolna – zasady odpowiedzialności

Cyberprzestępczość to zbiór wielu różnych przestępstw związanych z funkcjonowaniem systemów i sieci teleinformatycznych, w tym Internetu. W doktrynie prawa, literaturze fachowej i języku potocznym określane są jako „cyberprzestępstwa", „przestępstwa komputerowe" lub „przestępstwa internetowe". Cyberprzestępczość szkolna to nic innego, jak zbiór przestępstw uczniów związanych z ich działalnością komputerową i internetową.

1. Rodzaje cyberprzestępstw

Do najważniejszych cyberprzestępstw szkolnych zaliczamy: *hacking*, *cracking* i *cyberbullying*. Większość z nich nie istnieje samodzielnie, przenikają się nawzajem i uzupełniają. Dlatego, w praktyce, w przypadku odpowiedzialności karnej, sprawcy podlegają kilkunastu zarzutom.

1.1 Hacking

Komputer może być nie tylko narzędziem przestępstwa, ale również stanowić przedmiot ataku. *Hacking*, czyli włamanie do systemów komputerowych, m.in. do serwerów szkoły, jest jednym z najpowszechniejszych przestępstw komputerowych. Stanowi element konieczny do zaistnienia innych cyberprzestępstw, np. oszustw czy kradzieży. Polega na zainfekowaniu komputera ofiary np. koniem trojańskim lub innym programem typu *backdoor* w celu przechwycenia określonych informacji czy ominięcia zabezpieczeń.

1.2 Cracking

Niejednokrotnie działalność sieciowa uczniów dotyczy łamania praw autorskich. Związana jest nie tylko z nielegalnym pozyskiwaniem materiałów z sieci i ich późniejszym wykorzystywaniem (np. tekstów, muzyki, filmów, zdjęć), ale przede wszystkim z łamaniem zabezpieczeń programów komputerowych. Za łamanie zabezpieczeń, oprócz np. kary umownej za naruszenie postanowień umowy lub odpowiedzialności za wyrządzoną szkodę, kodeks karny oraz ustawa o prawie autorskim i prawach pokrewnych przewiduje sankcje karne. Producenci komercyjnego oprogramowania stosują wiele technik zabezpieczających je przed nieuprawnionym użyciem. Sprawca, w celu usunięcia zabezpieczeń, najczęściej tworzy mały program automatyzujący to zadanie, tzw. *crack*. Może być on umieszczony w Internecie lub na nośniku obok programu. Innym rozwiązaniem jest stworzenie generatora kluczy licencyjnych – *keygena*. *Cracker* oraz osoby korzystające z rezultatów jego pracy mają możliwość używania programu nielegalnie lub w sposób niedozwolony przez producenta.

1.3 Cyberbullying

Działaniem bezprawnym uczniów jest w dużej mierze przemoc internetowa, czyli tzw. *cyberbullying*. Jest to prześladowanie, szykanowanie, zastraszanie lub dręczenie innych osób (najczęściej z najbliższego otoczenia sprawcy) z wykorzystaniem Internetu i narzędzi elektronicznych (e-maila, komunikatorów tekstowych typu Gadu-Gadu czy SMS lub głosowych typu Skype, forów internetowych, blogów, a nawet całych stron WWW). Mimo że jest to przede wszystkim poważny problem psychologiczno-społeczny, to dotyczy on również szeregu działań, które są przestępstwami. Oznacza to, że choć cyberprzemoc nie jest zabroniona wprost przepisami prawa, to karalne jest takie zachowanie, które wypełnia znamiona tradycyjnego czynu zabronionego (np. zniewagi, oszustwa, pomówienia, kradzieży, niszczenia danych informatycznych). Przykładowo, jeżeli sprawca wysyła złośliwe SMS-y czy e-maile, takie działania mogą być uznane za przestępstwo gróźb karalnych. Do najczęstszych form *cyberbullyingu* zaliczamy:

- zamieszczanie w sieci filmów nagrywanych np. telefonami komórkowymi, gdzie bohaterami są zarówno koledzy, jak i nauczyciele,
- włamania na konta pocztowe lub konta komunikatorów w celu rozsyłania kompromitujących wiadomości,

- włamania do kont znajomych w portalach internetowych,
- włamania na szkolne serwery w celu skopiowania materiałów egzaminacyjnych,
- kradzież tożsamości z kont społecznościowych,
- tworzenie kompromitujących i ośmieszających stron internetowych.

2. Identyfikacja sprawcy

Złudzenie anonimowości nieletnich sprawców utrwala poczucie bezkarności. Nie oznacza to jednak, że sprawcy nie można zidentyfikować. Ofiary cyberprzemocy często potrafią wskazać sprawcę, którym najczęściej okazuje się kolega ze szkoły, bądź przynajmniej mają przypuszczenie, kto może nim być. Jeżeli jednak nie znają danych sprawcy, powinni skorzystać z uprawnienia do wniesienia skargi na policję, która na tej podstawie zabezpiecza niezbędne dowody oraz kieruje skargę do właściwego sądu. W ramach tych czynności policja jest uprawniona m.in. do ustalenia adresu IP komputera. Może także w toku dalszych czynności służących zabezpieczeniu dowodów próbować ustalić, kto w danym czasie korzystał z danego komputera. W tym celu może zwracać się do dostawców usług internetowych, kawiarenek internetowych, administratorów serwerów, a nawet do administratorów stron czy forów internetowych o udostępnienie takich danych, wyręczając w tym pokrzywdzonego. Dane te są objęte ustawą o ochronie danych osobowych oraz tajemnicą telekomunikacyjną.

Komputer z dostępem do Internetu, co do zasady, posiada własny niezmienny adres IP, na podstawie którego policja w przypadku złamania prawa może ustalić właściciela. Adres IP w połączeniu z dokładnym określeniem czasu jednoznacznie identyfikuje urządzenie w sieci Internet. A to pozwala zidentyfikować użytkownika. W przypadku użytkowników, którzy nie są na stałe włączeni do sieci, lecz korzystają z modemu i linii telefonicznej z chwilą nawiązania połączenia domenowego z dostawcą Internetu otrzymują adres IP. W takiej sytuacji, aby określić, który komputer korzystał z danego adresu IP, należy przyporządkować datę i godzinę korzystającemu z takiego adresu IP. Korzystanie z mechanizmów dynamicznego przydzielania adresu IP może utrudniać zidentyfikowanie konkretnego komputera z danym adresem IP. Pomocne są w tym przypadku dane billingowe, które zawierają informacje m.in. o adresie abonenta, liczbie jednostek taryfowych połączenia, numerach, z którymi uzyskał połączenie, dacie i czasie trwania połączenia. Operator jest obowiązany do rejestracji danych wykonywanych usług telekomunikacyjnych w zakresie umożliwiającym ustalenie należności za wykonanie tych usług. Informacje te są tajemnicą komunikacyjną na podstawie ustawy o prawie telekomunikacyjnym. Ujawnienie tych informacji może nastąpić mocą postanowienia sądu, prokuratora lub na podstawie odrębnych przepisów, np. ustawy o policji.

3. Odpowiedzialność karna a cywilna

W polskim prawie wyróżniamy odpowiedzialność karną i cywilną. Odpowiedzialność karna wynika z przepisów kodeksu karnego oraz innych ustaw, które zawierają przepisy karne (np. ustawy o prawie autorskim). Natomiast odpowiedzialność cywilna wynika z przepisów kodeksu cywilnego. Pomiędzy nimi istnieją istotne różnice. Odpowiedzialność cywilna ma postać wyłącznie majątkową i powstaje dopiero wtedy, gdy zostanie wyrządzona szkoda. Odpowiedzialność karna ma postać osobistą i majątkową. Te dwa rodzaje odpowiedzialności mogą być dochodzone równolegle. Jedna nie wyklucza drugiej.

4. Odpowiedzialność karna nieletnich

Odpowiedzialność karna uczniów z uwagi na ich wiek jest ograniczona. Prawo karne w stosunku do uczniów posługuje się pojęciem nieletniego, czyli osoby, która w momencie popełnienia czynu zabronionego nie ukończyła 17 lat. Dzieci do lat 13 nie mogą być ukarane za popełnione czyny będące przestępstwami. Jeżeli sprawca znajduje się między 13 a 17 rokiem życia, ma wobec niego zastosowanie ustawa o postępowaniu w sprawach nieletnich. W tym przypadku orzeka sąd rodzinny, a najdotkliwszą sankcją z możliwych do zastosowania jest umieszczenie w zakładzie poprawczym. Kodeks karny dotyczy uczniów, którzy ukończyli lat 17. W wyjątkowych sytuacjach możliwe jest pociągnięcie do odpowiedzialności sprawców, którzy ukończyli lat 15. Oznacza to, że uczeń szkoły ponadgimnazjalnej za popełnienie czynów będących przestępstwami będzie odpowiadać na takich samych zasadach, jak każda osoba dorosła. Natomiast uczeń gimnazjum będzie odpowiadał na podstawie ustawy o postępowaniu w sprawie nieletnich (np. w sytuacji włamania do kont pocztowych, komunikatorów lub portali internetowych). Większość nielegalnych działań uczniów to sprawy podlegające powództwu cywilnemu. Oznacza to, że poszkodowany może wystąpić z prywatnym aktem oskarżenia (np. w przypadku zniewagi lub pomówienia). Może jednak zwrócić się do policji, by pomogła ustalić sprawcę. Jeżeli następstwem działań uczniów jest ujawnienie danych osobowych, to wystarczy tylko złożyć zawiadomienie o podejrzeniu

popełnienia przestępstwa, bowiem tego typu przestępstwo jest ścigane z urzędu. Ofiarami przemocy internetowej uczniów są przede wszystkim inni uczniowie. Poszkodowanymi mogą być również osoby dorosłe, w tym nauczyciele. W przypadku nielegalnych działań tego typu w stosunku do nauczycieli zastosowanie ma również przepis art. 63 Karty Nauczyciela. Zgodnie z tym przepisem nauczyciel, podczas lub w związku z pełnieniem obowiązków służbowych, korzysta z ochrony przewidzianej dla funkcjonariuszy publicznych na zasadach określonych w kodeksie karnym. Ochrona ta zapewnia surowsze kary za znieważenie, naruszenie nietykalności cielesnej oraz czynną napaść na ich osobę. Czyny te stają się przestępstwami w momencie, gdy są wymierzone w nauczyciela wykonującego swoje obowiązki. Organ prowadzący szkołę i dyrektor szkoły są obowiązani z urzędu występować w obronie nauczyciela, gdy ustalone dla nauczyciela uprawnienia zostaną naruszone.

5. Odpowiedzialność cywilna małoletnich

Prawo cywilne w stosunku do uczniów posługuje się pojęciem małoletniego, czyli osoby, która nie ukończyła lat 18. Inaczej jednak kształtuje się odpowiedzialność małoletniego, który nie ukończył lat 13, a inaczej małoletniego w wieku od 13 do 18 roku życia. Małoletni, który nie ukończył lat 13, nie posiada zdolności do czynności prawnych oraz nie ponosi odpowiedzialności za wyrządzoną szkodę (nie można mu przypisać winy). Związane jest to z tym, iż osoby takie ze względu na swój stopień rozwoju psychofizycznego nie są w stanie właściwie kierować swym postępowaniem czy też ocenić skutków swoich czynów. Takiej oceny dokonał ustawodawca, tworząc kodeks cywilny. Nie oznacza to jednak, że małoletni poniżej 13 roku życia są całkowicie bezkarni. Odpowiedzialność ta jest przeniesiona na osoby sprawujące opiekę nad nim (rodziców, prawnych opiekunów, nauczycieli, instruktorów). Ich odpowiedzialność wynika ze sprawowanego nadzoru. Nadzorujący może uwolnić się od odpowiedzialności, gdy udowodni, że nadzór był sprawowany należycie. W sytuacjach wyjątkowych, gdy nie da się dowieść winy nadzoru, gdy ściągnięcie odszkodowania od osoby winnej z tytułu nadzoru jest niemożliwe lub utrudnione, jeżeli brak jest osób zobowiązanych do nadzoru, można dochodzić odszkodowania bezpośrednio od dziecka.

Małoletni, który ukończył lat 13, a nie ukończył 18 roku życia, z uwagi na ograniczoną zdolność do czynności prawnych może, ale nie musi, odpowiadać za wyrządzoną szkodę na zasadzie winy. O tym decyduje każdorazowo ocena sądu, czy z uwagi na wiek osiągnął on dostateczną dojrzałość, by w pełni przypisać mu winę. Małoletni musi mieć rozeznanie własnego działania i jego skutków oraz zdawać sobie sprawę z naganności swojego zachowania. W przypadku uznania winy, problemem jest brak własnego majątku małoletniego – najczęściej ciężar naprawienia szkody ponoszą rodzice.

Z *cyberbullyingiem* związany jest temat ochrony wizerunku. Obraz człowieka może być na różne sposoby utrwalany, np. na fotografii, plakacie, rzeźbie, filmie, co rozszerza także możliwość jego bezprawnego wykorzystania. Takie zdarzenia niejednokrotnie powodują naruszenie praw osobistych i majątkowych osoby portretowanej. W praktyce szkolnej takiego rodzaju sytuacje mają miejsce w przypadku zamieszczania na stronach internetowych wizerunku osoby sfotografowanej lub sfilmowanej. Zarówno postanowienia kodeksu cywilnego, jak i ustawy o prawie autorskim zakazują rozpowszechniania wizerunku bez zgody osoby przedstawianej. W praktyce zatem wymagana jest zgoda na rozpowszechnianie wizerunku na stronie internetowej, np. utrwalonego zdjęciem lub nagraniem filmowym (również telefonem komórkowym). Należy pamiętać, że nawet „zamazanie" twarzy lub ukrycie jej za czarnym paskiem nie zwalnia nas z odpowiedzialności. W takiej sytuacji może również dojść do ujawnienia danych osobowych, co jest już przestępstwem.

Autor jest prawnikiem, specjalistą z zakresu prawa oświatowego, prawa pracy i prawa autorskiego

Nagabywanie dzieci dla celów seksualnych, tzw. grooming

Z dniem 8 czerwca 2010 roku weszła w życie nowelizacja kodeksu karnego. Wprowadziła nowy typ przestępstwa seksualnego wobec małoletnich poniżej lat 15.

Nowelizacja wynika z konieczności dostosowania polskiego prawa do postanowień Konwencji Rady Europy z Lanzarote o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, podpisanej przez Polskę w dniu 25 października 2007 roku. Jest również próbą reakcji na wzmagające się zjawisko wykorzystywania seksualnego dzieci przez osoby dorosłe, możliwe dzięki nawiązywaniu za pomocą technologii komunikacyjnych kontaktu z dziećmi i doprowadzaniu do spotkania z nimi. Zjawisko to, znane jako *grooming*, wiąże się z zachęcaniem dziecka do udziału w czynności seksualnej, np. poprzez obietnicę nagrody, dyskutowanie na temat intymnych zachowań, prezentowanie treści o charakterze pornograficznym w celu przełamania oporu czy też zahamowań dotyczących sfery seksualnej.

Wykorzystanie seksualne dziecka w kontekście *groomingu* może przybierać różne formy, obejmujące również wykorzystanie w celach związanych z pornografią. Stąd wprowadzenie karalności czynu polegającego na nawiązywaniu kontaktu z małoletnim poniżej 15 lat za pośrednictwem Internetu lub telefonu i podejmowaniu czynności zmierzających do spotkania z nim w celu popełnienia przestępstwa gwałtu, obcowania płciowego lub produkowania bądź utrwalania treści pornograficznych z jego udziałem.

Karane jest również samo złożenie propozycji obcowania płciowego lub udziału w produkowaniu lub utrwalaniu treści pornograficznych dziecku poniżej 15 roku życia.

Przestępstwa te zagrożone są karą do 3 lat pozbawienia wolności.

◀

Operator witryny internetowej lub portalu oferującego gry może korzystać z oznaczenia PEGI OK. Podstawą jest oświadczenie złożone PEGI, że gra nie zawiera materiałów wymagających formalnego *ratingu*.

Gry kwalifikujące się do oznaczenia PEGI OK **nie mogą** zawierać żadnego z poniższych elementów:

- przemoc,
- czynności seksualne lub aluzje o charakterze seksualnym,
- nagość,
- wulgaryzmy,
- hazard,
- popularyzacja lub zażywanie narkotyków,
- popularyzacja alkoholu lub tytoniu,
- przerażające sceny.

Logo PEGI OK umieszczane jest na grach internetowych (do 250 MB), które nie zawierają treści nieodpowiednich dla dzieci w wieku 3 lat.