Wykorzystanie AI w cyberatakach na uczelnie wyższe

DR HAB. PROF. US

ALEKSANDRA MONARCHA-MATLAK

Nowe technologie rzuciły wyzwanie prawu - jego standardom, regułom, zasadom. Prawo jak wiemy jest centralnym instrumentem porządku prawnego. Ten porządek może zostać zachwiany przez nieumiejętne i niekompetentne zastosowanie narzędzi sztucznej inteligencji.

Należy postawić więc pytanie czy sztuczna inteligencja wykorzystywana przecież przez studentów i pracowników może być narzędziem cyberataku na uczelnię?

Chat GPT odpowiedział, że niestety istnieje taka możliwość np. do ataków typu pishing, generowania fałszywych wiadomości e-mail czy nawet prób przełamania zabezpieczeń systemów uczelni. Dodaje jednocześnie, że AI może być również używana do wykrywania i zwalczania takich zagrożeń, pomagając w wzmocnieniu systemu bezpieczeństwa.

Cyberatak na uczelnię to każda próba nieautoryzowanego dostępu do systemów informatycznych uczelni w celu kradzieży, uszkodzenia lub zakłócenia danych, a także wszelkie działania mające na celu zakłócenie normalnego funkcjonowania uczelni. Mogą to być ataki typu ransomware, wykradanie danych osobowych studentów i pracowników lub ataki mające na celu przerwanie lub zakłócenie działania infrastruktury uczelni.

Istnieje jednak jeszcze jeden niebezpieczny sposób wykorzystania AI, mianowicie w pracach dyplomowych studentów, można to nawet uznać za swoisty cyberatak na uczelnię. Studenci uzyskali potężne narzędzie wspomagające ich w badaniach i pracach dyplomowych, dające im nowe możliwości eksploracji danych, rozwiazywania problemów i tworzenia innowacyjnych rozwiązań. Niestety jednak, jak dotychczas wykorzystywanie miedzy innymi Chata GPT w pracach dyplomowych jest nie do wykrycia, ani przez system Antyplagiat ani przez Jednolity System Antyplagiatowy (JSA). Systemy antyplagiatowe mają różne mechanizmy wykrywania nieuczciwego wykorzystania cudzych treści, ale mogą napotkać trudności w wykrywaniu tekstu wygenerowanego przez Chat GPT.

Chat GPT, generuje unikatowe odpowiedzi na podstawie dostarczonego kontekstu i treści, co oznacza, że w przypadku, gdyby student skorzystał z takiego tekstu, system antyplagiatowy zarejestruje tekst jako oryginalną pracę.

Mówiąc wprost, stosowane na uczelniach systemy antyplagiatowe nie są stanie wykryć treści wygenerowanych technologiami AI. Nie radzą sobie z problemem nawet przy użyciu rozwiązań opartych na modelach oraz wykorzystując AI nauczone wykrywać inne AI.

Dodatkowo zgodnie z aktualnym stanem prawnym treści wygenerowane przez AI nie stanowią plagiatu, nie są również autorstwem osób z nich korzystających.

Sztuczna inteligencja jest również wykorzystywana przez studentów przy zbieraniu i analizowaniu danych, udziela odpowiedzi na pytania studentów, może pomagać w generowaniu celów edukacyjnych, ćwiczeń, materiałów, zmniejszając obciążenie pracą. Wspomaga studentów z niepełnosprawnościami, pozwala na pokonanie barier językowych. Umiejętne korzystanie ze sztucznej inteligencji powinno stać się podstawową umiejętnością cyfrową studentów, którą wyniosą po zakończeniu studiów.

Widać wyraźnie, nawet w takim prostym przypadku, że zastosowanie AI wykracza daleko poza ideę prawa. Nie pomagają nakazy, zakazy oraz inne ograniczenia. Według nowej wizji, pojawiające się tzw. zarządzanie technologiczne spowoduje, że zmieni się tradycyjnie pojmowane prawo. Sztuczna inteligencja sama zacznie opracowywać praktyczną wersję „niezgodności”. Nowymi kanałami postępowania zacznie wprowadzać zupełnie nowa wersję prawa. Dlatego tak ważna jest działalność organów regulacyjnych i regulujących, które mogą decydować o użyciu odpowiednich narzędzi i działać zgodnie ze wskazaniami spójnego rozumowania prawnego. Narzędzia sztucznej inteligencji zostały przeszkolone przez wiele osób, potrafią również uczyć się same, powoduje to że w prostym kontekście prognostycznym mogą nawet przewyższać ludzi.

Nie powinniśmy jednak jak na razie zbytnio się przejmować, ten „gwóźdź technologiczny” jest jeszcze zbyt cienki, narzędzia sztucznej inteligencji nie są lepsze od prawników ocenianych według wymaganego standardu staranności, spójnego rozumowania prawnego oraz doświadczenia i fachowej wiedzy.

Sankcje za cyberataki

Jeszcze jedno ważne zagadnienie związane z tematem czyli sankcje za cyberataki zgodnie z prawem unijnym i prawem polskim.

W maju 2019r. Rada ustanowiła przepisy, które pozwalają nakładać sankcje aby powstrzymać cyberataki stanowiące zagrożenie dla państw członkowskich UE. Sankcje mogą być nakładane na osoby oraz podmioty, które odpowiadają za ataki lub ich próby w związku z tym zapewniają wsparcie finansowe, techniczne, materialne lub angażują się w te działania w inny sposób. Sankcjami mogą być objęte inne powiązane osoby lub podmioty. Przewidziane sankcje to: zakaz wjazdu na teren Unii Europejskiej oraz zamrożenie aktywów należących do tych osób lub podmiotów. Ponadto osoby i podmioty z UE nie mogą udostępniać funduszy tym, których objęły sankcje. Nowy system sankcji dotyczy cyberataków, które wywołują poważne skutki i które zostały przygotowane poza UE lub przeprowadzone spoza terytorium UE lub tez wykorzystują infrastrukturę znajdująca się poza UE. Dotyczy to także cyberataków, które są przeprowadzane przez podmioty lub osoby, mające siedzibę poza UE lub działające poza UE lub są przeprowadzane z pomocą osób lub podmiotów mających siedzibę lub działających poza UE. Nowemu systemowi sankcji podlegają także próby cyberataków o potencjalnie poważnych skutkach.

Według polskiego prawa, za cyberataki i działania związane z naruszeniem systemów informatycznych czy bezprawnym dostępem do danych osobowych mogą być nakładane sankcje karno-administracyjne oraz ponoszenie odpowiedzialności cywilnej. Sankcjami mogą być: grzywny finansowe, kara pozbawiania wolności w przypadku poważniejszych przestępstw oraz obowiązek naprawienia szkody wyrządzonej przez cyberatak. Kary te są ujęte w różnych aktach prawnych, takich jak: kodeks karny, ustawa o ochronie danych osobowych, ustawa o cyberbezpieczeństwie. Należy jeszcze dodać, że skala kar zależy od rodzaju i powagi przestępstwa oraz wyrządzonych szkód.

Dziękuję za uwagę.