Dr Justyna Jasińska-Rudzka
e-mail: jasinska.justyna@o2.pl
Uniwersytet Jana Długosza w Częstochowie

DOCHODZENIE ROSZCZEŃ Z TYTUŁU NARUSZEŃ CYBERBEZPIECZEŃSTWA – ZASYGNALIZOWANIE PROBLEMÓW I WYZWAŃ PROCESOWYCH

Streszczenie

W treści niniejszego artykułu omówione zostały cywilnoprawne aspekty dochodzenia roszczeń wynikających z naruszeń cyberbezpieczeństwa. W kontekście wspomnianych roszczeń, analizie poddano zarówno aspekty materialnego prawa cywilnego, jak i prawa procesowego, koncentrując się na trudnościach m.in. dowodowych czy jurysdykcyjnych. Poruszono także kwestię odpowiedzialności odszkodowawczej oraz specyfiki szkody wyrządzonej wskutek np. cyberataku. Artykuł uwzględnia dorobek doktryny i orzecznictwa.

Słowa kluczowe: roszczenia cywilnoprawne, odpowiedzialność odszkodowawcza, dowody elektroniczne, postępowanie cywilne, jurysdykcja, opinia biegłego.

WSTĘP

W dobie powszechnej cyfryzacji, w tym także działalności gospodarczej jak i administracyjnej, cyberbezpieczeństwo staje się jednym z najważniejszych obszarów ochrony prawnej. Wzrost liczby incydentów, takich jak nieuprawniony dostęp do systemów informatycznych, kradzież danych osobowych, wycieki informacji objętych tajemnicą przedsiębiorstwa czy celowe zakłócanie ciągłości działania systemów, przekłada się bezpośrednio na wzrost zainteresowania skutecznymi mechanizmami ochrony prawnej. Tego rodzaju naruszenia mogą prowadzić do poważnych konsekwencji zarówno majątkowych, przez które rozumieć należy np. utratę przychodów, koszty przywracania sprawności funkcjonowania systemów czy obowiązek zapłaty

odszkodowań, jak i niemajątkowych, takich jak naruszenie dobrego imienia, utrata zaufania klientów czy obniżenie pozycji konkurencyjności na rynku. Oczywistym pozostaje, że osoby poszkodowane poszukują środków prawnych, które pozwoliłyby im dochodzić swoich praw i uzyskać rekompensatę za poniesione straty. Należy jednak zauważyć, że dochodzenie roszczeń z tytułu naruszeń cyberbezpieczeństwa, w ramach postępowania cywilnego wiąże się z szeregiem poważnych trudności. Problemy pojawiają się już na etapie ustalania właściwej jurysdykcji, szczególnie gdy działania sprawcy mają charakter transgraniczny. Wątpliwości mogą budzić także kwestie odpowiedzialności za szkodę, zwłaszcza w sytuacjach, gdy dochodzi do pośrednich skutków incydentu lub gdy winę ponosi więcej niż jeden podmiot. Dodatkowym wyzwaniem pozostaje zebranie i przedstawienie w sądzie adekwatnego materiału dowodowego, który często ma charakter wysoce specjalistyczny, dynamiczny i trudny do jednoznacznej interpretacji. W efekcie, postępowania dotyczące cyberincydentów cechują się znacznym stopniem skomplikowania, wymagają interdyscyplinarnej wiedzy oraz ścisłej współpracy prawników z ekspertami z zakresu informatyki, bezpieczeństwa sieciowego i ochrony danych. Wszystko to sprawia, że poszukiwanie efektywnych i praktycznych rozwiązań w tej dziedzinie staje się jednym z pilnych wyzwań współczesnego prawa cywilnego. Treść artykułu opisuje najistotniejsze zdaniem autora aspekty procesowe dochodzenia roszczeń z tytułu naruszeń natury cyberbezpieczeństwa, które potwierdzają niedoskonałość aktualnych przepisów i potrzebę pilnej nowelizacji dostosowanej do aktualnych realiów cyberrozwoju.

CHARAKTERYSTYKA ROSZCZEŃ CYWILNOPRAWNYCH ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM

Odpowiedzialność odszkodowawcza za naruszenie cyberbezpieczeństwa może mieć swoje źródło zarówno w zobowiązaniach wynikających z umowy (*ex contractu*), jak i w działaniach niedozwolonych stanowiących naruszenie

powszechnie obowiązującego porządku prawnego (*ex delicto*)[1]. Oba wskazane modele odpowiedzialności znajdują zastosowanie w zależności od charakteru relacji łączącej strony oraz rodzaju i okoliczności danego naruszenia. W przypadku odpowiedzialności *ex contractu* mamy do czynienia z sytuacją, w której naruszenie obowiązków związanych z zapewnieniem cyberbezpieczeństwa stanowi niewykonanie lub nienależyte wykonanie zawartej umowy. Dotyczy to w szczególności umów o świadczenie usług cyfrowych, outsourcing IT czy umów powierzenia przetwarzania danych osobowych, w których strony wyraźnie określiły zasady zabezpieczania systemów i danych. W razie niewywiązania się z tych obowiązków, poszkodowany może dochodzić odszkodowania za szkodę poniesioną w wyniku naruszenia warunków kontraktu. Przesłankami tej odpowiedzialności pozostają: istnienie ważnej umowy, naruszenie jej postanowień przez choćby jedną ze stron, wystąpienie szkody oraz związek przyczynowy między naruszeniem a szkodą. Z kolei odpowiedzialność *ex delicto* opiera się na ogólnych zasadach prawa cywilnego dotyczących czynów niedozwolonych, takich jak działanie bezprawne, zawinione i szkodliwe, naruszające dobra osobiste lub majątkowe innego podmiotu. Przykładami mogą być: nieuprawnione pozyskanie lub ujawnienie danych, celowe zakłócenie działania systemu informatycznego czy rozpowszechnienie informacji objętych tajemnicą przedsiębiorstwa. Odpowiedzialność ta może powstać również niezależnie od istnienia uprzedniego stosunku zobowiązaniowego między sprawcą a poszkodowanym, co czyni ją szczególnie istotną w relacjach pozaumownych, np. pomiędzy konkurencyjnymi przedsiębiorstwami. W praktyce często mamy do czynienia z tzw. odpowiedzialnością mieszaną, w której elementy obu podstaw przenikają się. Za przykład rzeczonej, może posłużyć sytuacja, w której wykonawca usług cyfrowych dopuszcza się naruszenia, które z jednej strony stanowi niewypełnienie warunków umowy, a z drugiej wyczerpuje znamiona czynu niedozwolonego tj. rażące niedbalstwo

[1] Zob. P. Kaniewski, K. Kowacz, Odpowiedzialność cywilna za szkody spowodowane funkcjonowaniem sztucznej inteligencji – uwagi de lege lata i de lege ferenda, „Palestra" 2024, nr 11, s. 6-33; M. Wałachowska, Sztuczna inteligencja a zasady odpowiedzialności cywilnej, [w:] L. Lai, M. Świerczyński, Prawo sztucznej inteligencji, Legalis.

skutkujące ujawnieniem danych osobowych. W konsekwencji cyberincydenty bardzo często prowadzą do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, zwłaszcza art. 82 RODO, który przewiduje możliwość dochodzenia od administratora lub podmiotu przetwarzającego odszkodowania za szkodę poniesioną w wyniku naruszenia przepisów rozporządzenia[2]. Jest to szczególna forma odpowiedzialności cywilnej, która może mieć charakter zarówno kontraktowy, jak i deliktowy, w zależności od relacji prawnej między stronami.

Specyfika roszczeń związanych z naruszeniami cyberbezpieczeństwa przejawia się w licznych wyzwaniach natury materialnoprawnej i procesowej. W praktyce trudności sprawia precyzyjne określenie zakresu i rodzaju szkody, w szczególności w przypadku szkód niemajątkowych, takich jak naruszenie prywatności czy utrata reputacji. Równie problematyczna może być identyfikacja podmiotu odpowiedzialnego za szkodę, zwłaszcza w sytuacjach, gdy działania sprawcy były ukryte, rozproszone technologicznie lub miały charakter transgraniczny. Ustalenie związku przyczynowego między konkretnym zachowaniem, a powstałą szkodą bywa również znacząco utrudnione, szczególnie gdy cyberatak nastąpił przy współudziale różnych podmiotów lub był skutkiem następujących po sobie zdarzeń. Wszystkie te okoliczności wpływają na przebieg i efektywność postępowań cywilnych dotyczących naruszeń cyberbezpieczeństwa, czyniąc je czasochłonnymi, kosztownymi i często trudnymi do skutecznego przeprowadzenia. Tym samym konieczne staje się nie tylko pogłębianie wiedzy prawniczej w tym obszarze, ale także rozwijanie praktycznych mechanizmów pozwalających na skuteczne dochodzenie roszczeń w warunkach współczesnego świata cyfrowego.

JURYSDYKCJA KRAJOWA I WŁAŚCIWOŚĆ SĄDU PRZY ROSZCZENIACH WYNIKAJĄCYCH Z NARUSZEŃ CYBERBEZPIECZEŃSTWA

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), dalej: RODO.

W dobie globalizacji działalności gospodarczej i powszechnej cyfryzacji, w której podmioty funkcjonują w ramach wzajemnych powiązań międzynarodowych oraz współpracują w wirtualnej przestrzeni niezależnie od granic państwowych. W związku z powyższym zagadnienia jurysdykcji krajowej i wyboru prawa właściwego nabierają kluczowego znaczenia w kontekście dochodzenia roszczeń związanych z naruszeniami natury cyberbezpieczeństwa.

W przypadku transgranicznych sporów cywilnych i handlowych w ramach Unii Europejskiej, podstawowe znaczenie ma rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (przekształcenie)[3]. Zgodnie z jego przepisami, a w szczególności treścią art. 7, w sprawach dotyczących czynu niedozwolonego lub czynu podobnego do czynu niedozwolonego, roszczenia dochodzi się przed sądem miejsca, w którym nastąpiło lub może nastąpić zdarzenie wywołujące szkodę. Ponadto w sprawach dotyczących umowy, roszczenia rozpatrywane są przez sądy miejsca wykonania danego zobowiązania, a w sprawach dotyczących roszczeń cywilnoprawnych o odszkodowanie lub przywrócenie stanu poprzedniego, które wynikają z czynu zagrożonego karą, właściwy pozostaje sąd, do którego wniesiono akt oskarżenia, o ile sąd ten może według swojego prawa rozpoznawać roszczenia cywilnoprawne. W konsekwencji oznacza to konieczność precyzyjnego ustalenia, gdzie miało miejsce naruszenie. Niestety w przypadku ataków rozproszonych, wielopłaszczyznowych takich jak np. phishing precyzyjne ustalenie miejsca naruszenia bywa wyjątkowo utrudnione. Niejednokrotnie bowiem poszczególne elementy incydentu cyberbezpieczeństwa rozproszone są na terytoriach różnych państw, co w istotny sposób komplikuje przypisanie jurysdykcji sądowi konkretnego

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz. U. UE. L. z 2012 r. Nr 351, str. 1 z późn. zm.).

państwa i utrudnia jednoznaczne ustalenie sądu właściwego do rozpoznania sprawy[4].

Kolejnym istotnym zagadnieniem jest ustalenie prawa właściwego dla rozpoznania roszczenia. W przypadku braku uprzedniego wyboru prawa przez strony, dla roszczeń deliktowych sytuację reguluje Rozporządzenie (WE) nr 864/2007 Parlamentu Europejskiego i Rady z dnia 11 lipca 2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych (Rzym II)[5]. Zgodnie z treścią rzeczonego Rozporządzennia „Chociaż zasada *lex loci delicti commissi* jest podstawowym rozwiązaniem stosowanym dla zobowiązań pozaumownych prawie we wszystkich państwach członkowskich, jej zastosowanie w praktyce, w przypadku gdy elementy stanu faktycznego sprawy powiązane są z wieloma państwami, jest różne. Sytuacja taka powoduje brak pewności w zakresie prawa właściwego." Co za tym idzie, zgodnie z treścią art. 4 wspomnianego Rozporządzenia „Jeżeli niniejsze rozporządzenie nie stanowi inaczej, prawem właściwym dla zobowiązania pozaumownego wynikającego z czynu niedozwolonego jest prawo państwa, w którym powstaje szkoda, niezależnie od tego, w jakim państwie miało miejsce zdarzenie powodujące szkodę, oraz niezależnie od tego, w jakim państwie lub państwach występują skutki pośrednie tego zdarzenia." I tutaj również pojawia się szereg trudności praktycznych, ponieważ w środowisku cyfrowym granice terytorialne mają charakter umowny i często rozmyty. Może się zdarzyć, że skutki naruszenia będą odczuwane w wielu krajach jednocześnie, co rodzi pytania o możliwość kumulacji podstaw prawnych lub o wybór właściwej jurysdykcji.

W kontekście problemów związanych z jurysdykcją krajową oraz stosowaniem odpowiedniego prawa, należy również podkreślić, iż udział podmiotów mających siedzibę poza terytorium Unii Europejskiej rodzi dodatkowe komplikacje. Okoliczność ta może skutkować znaczną niepewnością co do wykładni oraz zakresu stosowania poszczególnych

[4] Szerzej: J. Worona-Vlugt, Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Warszawa 2020, s. 64-92.
[5] Rozporządzenie (WE) NR 864/2007 Parlamentu Europejskiego i Rady z dnia 11 lipca 2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych ("Rzym II") (Dz. U. UE. L. z 2007 r. Nr 199).

regulacji prawnych, prowadząc do rozbieżności w poziomie ochrony prawnej, jak również do problemów związanych z brakiem wzajemnego uznawania i wykonywania orzeczeń sądowych pomiędzy zaangażowanymi państwami.

Wszystkie te okoliczności czynią postępowania dotyczące cyberincydentów szczególnie trudnymi z perspektywy formalnoprawnej. Wymagają one nie tylko znajomości przepisów krajowych i unijnych, ale także umiejętności analizy złożonych stanów faktycznych, w których granice pomiędzy miejscem działania a miejscem skutku są płynne i dynamiczne. Z tego względu *de lege ferenda* postuluje się rozwój bardziej spójnych mechanizmów jurysdykcyjnych oraz pogłębioną współpracę międzynarodową w zakresie rozpoznawania i dochodzenia roszczeń wynikających z naruszeń cyberbezpieczeństwa.

WYZWANIA W ZAKRESIE POSTĘPOWANIA DOWODOWEGO

Jednym z najbardziej złożonych i wymagających aspektów postępowań cywilnych dotyczących naruszeń cyberbezpieczeństwa pozostaje wykazanie przesłanek odpowiedzialności odszkodowawczej, i to zarówno na gruncie kontraktowym, jak i deliktowym. Szczególne trudności występują w odniesieniu do udowodnienia powstania szkody oraz istnienia adekwatnego związku przyczynowego pomiędzy zachowaniem (działaniem bądź zaniechaniem) sprawcy, a zaistniałą szkodą natury majątkowej lub niemajątkowej.

Szkoda będąca skutkiem incydentu o charakterze cybernetycznym nierzadko przybiera postać rozproszoną, trudną do jednoznacznego ujęcia w tradycyjnych kategoriach finansowych, zwłaszcza gdy dotyczy utraty integralności danych, naruszenia poufności informacji lub czasowego braku dostępności zasobów systemowych. Problematyka dowodowa dodatkowo komplikuje się w sytuacjach, gdy działania sprawcy miały charakter zautomatyzowany i zamaskowany bądź miały miejsce w wielu krajach jednocześnie, co znacząco utrudnia identyfikację odpowiedzialnego podmiotu oraz przypisanie mu realizację konkretnych czynów.

W praktyce sądowej coraz większą wagę przykłada się do tzw. dowodów elektronicznych, zwanych niekiedy także cyfrowymi[6], obejmujących, w kontekście roszczeń z tytułu naruszeń cyberbezpieczeństwa w szczególności: dane systemowe i serwerowe, treść korespondencji e-mailowej, czy zapisy aktywności użytkowników w systemach informatycznych. Uwzględniając myśl K. Wręczyckiej, zasadne wydaje się stwierdzenie, że dane komputerowe potwierdzające naruszenie natury cyberbezpieczeństwa stanowią dopuszczalny dowód w postępowaniu cywilnym. Należy podkreślić możliwość zakwalifikowania dowodów elektronicznych jako dokumentów. Niestety „problemy praktyczne w postępowaniu cywilnym budzi określenie sposobu zapoznania się z ich treścią przez sąd oraz strony. Dokumenty w postaci elektronicznej mogą bowiem być przedstawione w trzech różnych postaciach — jako dane zapisane na elektronicznych nośnikach informacji, jako wizualizacja na monitorze komputera lub jako wydruk komputerowy."[7] I choć poczynione w ostatnich latach nowelizacje Kodeksu postępowania cywilnego wiele zmieniły w postrzeganiu dowodów elektronicznych, *de lege ferenda* zasadne wydaje się wprowadzenie regulacji poświęconej *stricte* rzeczonemu typowi dowodu. Dużym wyzwaniem procesowym pozostaje fakt, że dowody elektroniczne stanowią materiał łatwy do modyfikacji, usunięcia lub fałszowania. Niezbędne jest zatem przeprowadzenie odpowiednich czynności w celu zabezpieczenia i zachowania dowodów w pierwotnej formie.

Podejmując się analizy kolejnych środków dowodowych, w kontekście dochodzenia roszczeń cywilnoprawnych wynikających z naruszeń cyberbezpieczeństwa, dowód z opinii biegłego stanowi szczególnie doniosły środek dowodowy, który obok dowodów elektronicznych *sensu stricto* pełni funkcję komplementarną, a niejednokrotnie wręcz kluczową dla wykazania przesłanek odpowiedzialności odszkodowawczej.

Zgodnie z treścią art. 278 § 1 k.p.c.[8], „w wypadkach wymagających wiadomości specjalnych sąd po wysłuchaniu wniosków stron co do liczby

[6] J. Kudła, Dopuszczalność wykorzystania dowodów cyfrowych w postępowaniu cywilnym, LEX/el. 2020.
[7] K. Wręczycka, Dowody elektroniczne w postępowaniu cywilnym, Acta Uniersitatis Wratislaiensis, „Przegląd Prawa i Administracji" nr CXXXIII, Wrocław 2023, s. 197.
[8] Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2024 r. poz. 1568 z późn. zm.).

biegłych i ich wyboru może wezwać jednego lub kilku biegłych w celu zasięgnięcia ich opinii.”. Cyberincydenty, jako zjawiska o wysokim stopniu technicznego skomplikowania, niemal zawsze wymagają przeprowadzenia specjalistycznej analizy informatycznej, celem wyjaśnienia istoty zdarzenia, jego przyczyn, mechanizmu działania sprawcy, a także ewentualnych skutków dla poszkodowanego. Z tej perspektywy dowód z opinii biegłego z zakresu informatyki śledczej, cyberbezpieczeństwa lub inżynierii systemów informatycznych jest niezbędny dla przekształcenia materiału elektronicznego w materiał procesowo użyteczny. Uwzględniając opisywany temat, opinia biegłego może obejmować między innymi: wykrycie nieautoryzowanego dostępu do systemu informatycznego, identyfikację luk bezpieczeństwa, które umożliwiły dokonanie naruszenia, ocenę skali oraz zakresu naruszenia integralności lub poufności danych, określenie prawdopodobieństwa wystąpienia szkody oraz jej związku przyczynowego z działaniem podmiotu odpowiedzialnego.

Dowód z opinii biegłego może również służyć do oceny, czy określone zachowania stanowiły naruszenie należytej staranności po stronie administratora danych lub dostawcy usług cyfrowych, co ma znaczenie dla przypisania winy lub ustalenia stopnia zawinienia. Opinia ta może być też istotna w kontekście wykazania braku staranności w implementacji rozwiązań organizacyjnych i technicznych służących zapewnieniu cyberbezpieczeństwa, co ma istotne znaczenie w świetle art. 82 ust. 1 RODO oraz art. 471 k.c.[9]

Warto również podkreślić, że sąd, w razie potrzeby posiada uprawnienie do powołania więcej niż jednego biegłego, albo zlecenia sporządzenia opinii instytucji naukowej lub specjalistycznej, co znajduje zastosowanie w sprawach o szczególnie wysokim poziomie technicznego zaawansowania lub naruszeń o charakterze transgranicznym.

Reasumując, dowód z opinii biegłego stanowi nieodzowny instrument w rekonstrukcji zdarzenia naruszenia cyberbezpieczeństwa oraz w uwiarygodnieniu i procesowej legalizacji innych środków dowodowych, przede

[9] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061 z późn. zm.).

wszystkim dowodów elektronicznych. Bez jego wsparcia skuteczne dochodzenie roszczeń z tego tytułu może okazać się praktycznie niemożliwe.

Dodatkowo w postępowaniach dotyczących naruszeń cyberbezpieczeństwa istotne znaczenie dowodowe mają także dokumenty wewnętrzne podmiotu, w którym doszło do naruszenia, w szczególności polityki bezpieczeństwa informacji, procedury reagowania na incydenty oraz rejestry działań operacyjnych. Pomocne są również zapisy zgłoszeń i interwencji. W sprawach tego rodzaju często wykorzystuje się także dowody zgłoszeń incydentów do organów publicznych, w tym Prezesa Urzędu Ochrony Danych Osobowych lub organów ścigania, a także wszelkie komunikaty i zalecenia wydane przez podmioty nadzorcze. Cenne źródło informacji stanowią zeznania świadków, przede wszystkim pracowników działu IT, administratorów oraz osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji. Świadkowie mogą potwierdzić okoliczności samego incydentu oraz wskazać na ewentualne niedopatrzenia w zakresie zabezpieczeń. Uzupełnieniem tych dowodów jest przesłuchanie stron, zwłaszcza w kontekście stosowania wymaganych środków technicznych i organizacyjnych. Dowód ten może pomóc w ustaleniu, czy strona pozwana dochowała należytej staranności. Dla wykazania rozmiaru szkody konieczne może okazać się przedłożenie np. dokumentacji księgowej i operacyjnej potwierdzającej straty finansowe. Równie ważne są dowody odnoszące się do szkód niemajątkowych, takich jak naruszenie reputacji lub dóbr osobistych. Kompleksowość tego materiału dowodowego ma kluczowe znaczenie dla skuteczności roszczeń wynikających z cyberincydentów.

W kontekście opisywanego postępowania dowodowego, szczególnego znaczenia nabiera instytucja zabezpieczenia dowodu, o której mowa w art. 310 i nast. k.p.c. Zastosowanie regulacji może okazać się istotnym elementem przebiegu procesu w przypadkach, gdy istnieje uzasadniona obawa, że dowód ulegnie zniszczeniu, zniekształceniu bądź stanie się niedostępny w toku właściwego postępowania rozpoznawczego. Szybka reakcja strony wnioskującej, polegająca na skierowaniu do sądu żądania zabezpieczenia materiału dowodowego, nierzadko decyduje o możliwości skutecznego dochodzenia roszczeń wynikających z cyberincydentów.

PODSUMOWANIE

Dochodzenie roszczeń cywilnoprawnych w związku z naruszeniami cyberbezpieczeństwa wiąże się z wieloaspektowymi wyzwaniami natury procesowej, które w istotny sposób rzutują na skuteczność ochrony prawnej przysługującej podmiotom poszkodowanym. Złożoność ta przejawia się nie tylko w trudnościach dowodowych, takich jak ustalenie sprawcy, zebranie i zabezpieczenie dowodów elektronicznych czy wykazanie przesłanek odpowiedzialności, lecz także w barierach wynikających np. z charakteru transgranicznego cyberincydentów, konieczności rozstrzygania kolizji jurysdykcyjnych i normatywnych oraz braku jednolitych standardów orzeczniczych. Ustalenie odpowiedzialności w tego rodzaju sprawach wymaga często sięgnięcia po narzędzia techniczne, procesowe i prawnomiędzynarodowe, których dostępność i skuteczność pozostają ograniczone. Ponadto, niedostosowanie klasycznych instrumentów procedury cywilnej do specyfiki zjawisk cyfrowych oraz trudności w oszacowaniu szkód, zwłaszcza niematerialnych, znacząco utrudniają realizację roszczeń poszkodowanych. W tym kontekście niezbędne wydaje się dalsze dostosowywanie krajowego i unijnego porządku prawnego do wymogów współczesnej gospodarki cyfrowej, a także rozwój orzecznictwa, które stopniowo wypracuje standardy właściwe dla tej nowej i dynamicznie rozwijającej się dziedziny.

De lege ferenda, Z uwagi na szczególny charakter spraw odszkodowawczych wynikających z naruszeń cyberbezpieczeństwa, zasadne wydaje się rozważenie wprowadzenia do Kodeksu postępowania cywilnego przepisów kategoryzujących rzeczone sprawy do postępowania odrębnego. Wspomniane postępowania wyróżniają się znaczącym stopniem złożoności, nietypowym zakresem materiału dowodowego oraz koniecznością stosowania specjalistycznych środków technicznych, w tym dowodów elektronicznych, których pozyskanie i zabezpieczenie wymaga odrębnych mechanizmów procesowych.

W kontekście dynamicznie rosnącej liczby incydentów cybernetycznych, które generują poważne skutki prawne i finansowe, regulacja ustawowa w postaci postępowania odrębnego umożliwiłaby nie tylko ujednolicenie praktyki orzeczniczej, ale także zapewnienie stronom skuteczniejszej i bardziej efektywnej ochrony prawnej. Wyodrębnienie takiego postępowania pozwoliłoby na precyzyjne określenie zasad przeprowadzania dowodów elektronicznych, dopuszczania dowodów z opinii biegłych z zakresu informatyki, a także uregulowanie wniosków o zabezpieczenie powództwa, służącego np. zabezpieczeniu danych cyfrowych przed ich utratą lub modyfikacją. Wprowadzenie wyspecjalizowanej procedury byłoby ponadto zgodne z kierunkiem modernizacji wymiaru sprawiedliwości w zakresie spraw gospodarczych i technologicznych, odpowiadając na rosnące potrzeby praktyki i ochrony interesu publicznego w erze cyfrowej.

Bibliografia:

Kaniewski, P., Kowacz, K. (2024). Odpowiedzialność cywilna za szkody spowodowane funkcjonowaniem sztucznej inteligencji – uwagi de lege lata i de lege ferenda, Palestra, nr 11, s. 6-33;

Kudła, J. (2020), Dopuszczalność wykorzystania dowodów cyfrowych w postępowaniu cywilnym, LEX/el.;

Rozporządzenie (WE) NR 864/2007 Parlamentu Europejskiego i Rady z dnia 11 lipca 2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych ("Rzym II") (Dz. U. UE. L. z 2007 r. Nr 199);

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.);

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz

ich wykonywania w sprawach cywilnych i handlowych (Dz. U. UE. L. z 2012 r. Nr 351, str. 1 z późn. zm.);
Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2024 r. poz. 1568 z późn. zm.);
Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061 z późn. zm.);
Wałachowska, M. (2020). *Sztuczna inteligencja a zasady odpowiedzialności cywilnej.* W: L. Lai, M. Świerczyński (red.), Prawo sztucznej inteligencji, Legalis;
Worona-Vlugt, J. (2020), Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Warszawa, s. 64-92;
Wręczycka, K. (2023). Dowody elektroniczne w postępowaniu cywilnym, Acta Uniersitatis Wratislaiensis, Przegląd Prawa i Administracji nr CXXXIII, Wrocław, s. 197.

CLAIMING CYBERSECURITY BREACHES – REPORTING PROCESS ISSUES AND CHALLENGES

Abstract

W treści niniejszego artykułu omówione zostały cywilnoprawne aspekty dochodzenia roszczeń wynikających z naruszeń cyberbezpieczeństwa. W kontekście wspomnianych roszczeń, analizie poddano zarówno aspekty materialnego prawa cywilnego, jak i prawa procesowego, koncentrując się na trudnościach m.in. dowodowych czy jurysdykcyjnych. Poruszono także kwestię odpowiedzialności odszkodowawczej oraz specyfiki szkody wyrządzonej wskutek np. cyberataku. Artykuł uwzględnia dorobek doktryny i orzecznictwa.

The article discusses the civil law aspects of pursuing claims arising from cybersecurity breaches. In the context of such claims, both substantive civil law and procedural law are analyzed, with particular focus on challenges such as evidentiary issues and jurisdictional questions. The paper also addresses the matter of liability for damages and the specific nature of harm caused by

cyberattacks. The analysis takes into account relevant legal doctrine and case law.

Keywords: civil claims, liability for damages, electronic evidence, civil procedure, jurisdiction, expert opinion.