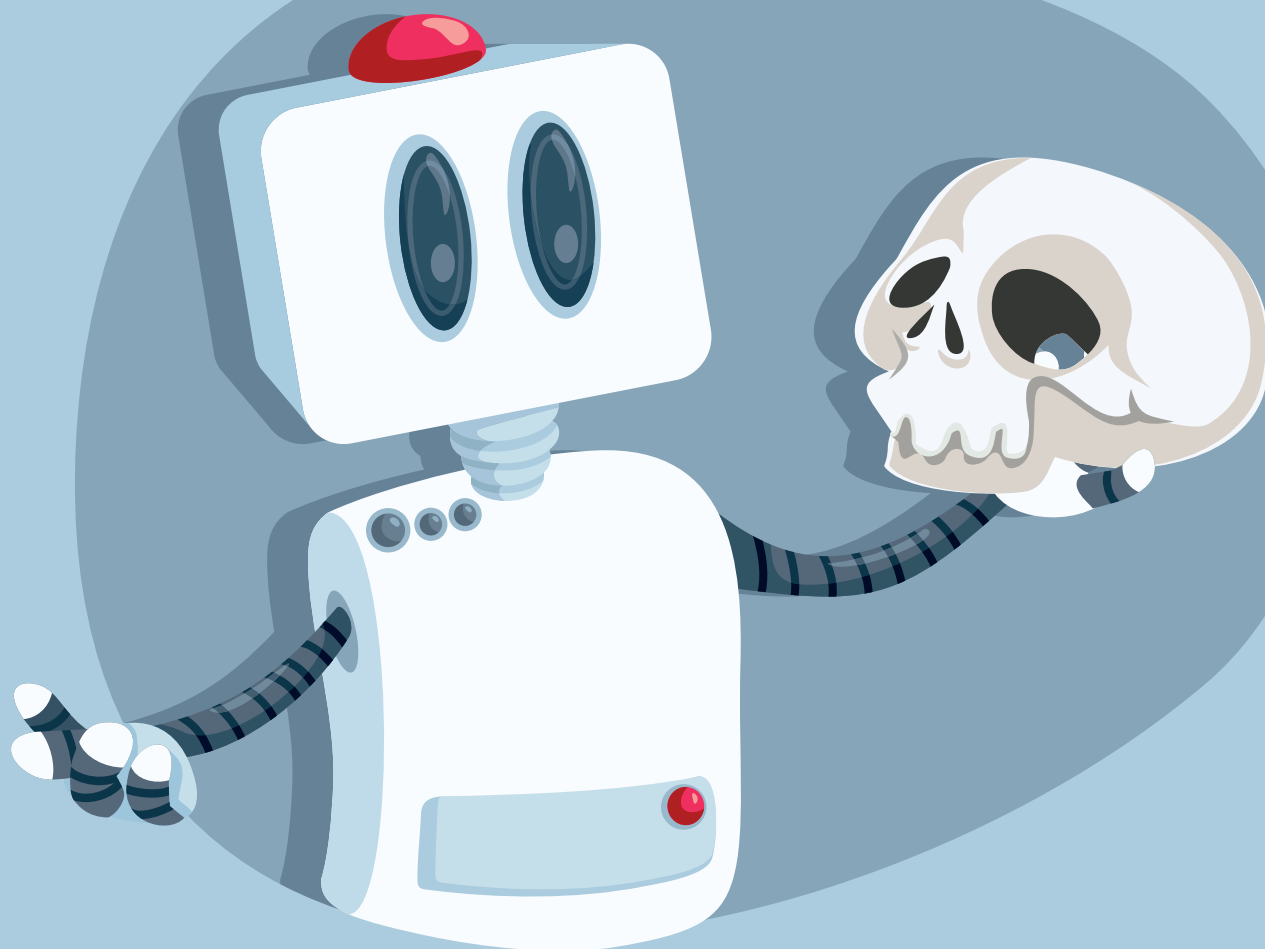


# Miesięcznik

# Ubezpieczeniowy

ISSN 1732-2413 • WSZYSTKO, CO TRZEBA WIEDZIEĆ O RYNKU UBEZPIECZEŃ • TOM 19 I NUMER 7/8 I LIPIEC/SIERPIEŃ 2022 • 20 LIPCA 2022



© nicoletaionescu/stock.adobe.com

W N U M E R Z E :

## Technologia:

insurtechy, automatyzacja, digital marketing, sztuczna inteligencja

Resolution w ubezpieczeniach/Polisa skarbowe vs D&O/Oczekiwania inwestorów



**MATEUSZ BARTOSZCZE**  
zastępca dyrektora Oddziału Kraków EIB,  
radca prawny.

## Problematyka nowych technologii, uczenia maszynowego i sztucznej inteligencji w umowie ubezpieczenia

Nowe technologie, uczenie maszynowe, sztuczna inteligencja (SI) stają się istotnymi elementami ubezpieczeniowej codzienności. Z całą pewnością proces ten będzie trwał i co do zasady nie ma od niego ucieczki. – **MATEUSZ BARTOSZCZE**

**W** swoim tekście chciałbym poruszyć parę aspektów związanych z technologiami obecnymi w naszej branży i implikacjami, jakie wynikają lub mogą wynikać z ich zastosowania. Problematykę tę ujmę w kilku płaszczyznach. Z jednej strony mamy czynności związane z codzienną pracą i ułatwienia oferowane przez nowoczesne rozwiązania. Jesteśmy użytkownikami i korzystamy z dobrodziejstw technologii. Oprogramowanie, które organizuje proces likwidacji, a w niektórych przypadkach realizuje go całkowicie autonomicznie, bez udziału człowieka, jest już faktem. Wsparcie procesów underwritingowych również. Coraz lepiej funkcjonuje także analiza i wykrywanie fraudów z użyciem nowoczesnych technologii i narzędzi wykorzystujących SI. Zważywszy na fakt, że szkody spowodowane fraudami na rynku europejskim szacuje się na około 13 mld euro, to odzyskanie części z tych środków znacząco wpłynie na pozostałych uczestników rynku ubezpieczeniowego. Jest to aspekt ważny, ale wewnętrzny, związany z funkcjonowaniem i organizacją procesów ubezpieczycieli, który, choć emanuje na zewnątrz, chciałbym jednak zostawić na boku w swoich rozważaniach. Podobnie poza zakresem niniejszej analizy pozostawiam kwestie wpływu technologii na szybkość, jakość oraz organizację naszej codziennej pracy. To się już dzieje i jest naturalnym procesem.

### POTRZEBA NOWYCH ROZWIĄZAŃ UBEZPIECZENIOWYCH?

Kolejną płaszczyzną, jest tworzenie produktów ubezpieczeniowych, które mają za zadanie zapewnić ochronę ubezpieczeniową

dla ciągle rozwijającej się technologii. Procesowi temu towarzyszy jednak nieustająca dyskusja wśród prawników – czy przepisy polskiego kodeksu cywilnego są wystarczające dla ujęcia nowych technologii w ramy prawne. Czy współczesny kontrakt ubezpieczeniowy znajdzie oparcie w aktualnie obowiązujących przepisach? Jest to jeden z kierunków obecnych rozważań. Dlaczego tak istotny? Użytkowane pojazdy mają coraz większą liczbę funkcji autonomicznych. Co więcej, instalacja systemów monitorujących wilgotność, przepływ wody, czy też temperaturę w domach to także coraz powszechniejsze elementy naszej codzienności. Ponadto, ubezpieczyciele coraz częściej oferują klientom korporacyjnym wsparcie w ramach systemów monitorujących i predykcyjnych. Wszystko w celu minimalizacji zagrożenia szkodą, wcześniejszego rozpoznania nadchodzącego zdarzenia.

### NOWE TECHNOLOGIE NA NOWYCH WARUNKACH

To, co jest dla mnie interesujące, to sfera zewnętrzna, gdzie z jednej strony mamy aspekt relacji ubezpieczyciel-ubezpieczony w kontekście prawnym, a z drugiej wyzwania, którym rynek ubezpieczeniowy będzie musiał stawić czoła w związku z rozwojem nowoczesnych technologii i związanymi z tym potrzebami ubezpieczeniowymi klientów. Moim zdaniem **umowa ubezpieczenia przyszłości będzie musiała zawierać odrębną sekcję, która ureguluje kwestie związane z użytkowaniem wspierających użytkownika nowoczesnych technologii**. Dostrzegam też kilka możliwych korelacji, interesujących z punktu widzenia osoby zajmującej się

na co dzień ubezpieczeniami korporacyjnymi. Na boku pozostawiam aspekt przetwarzania danych i związane z nim skutki w sferze administracyjnoprawnej.

Wracając do głównego wątku, przykładowo, stosownie do art. 815 kodeksu cywilnego ubezpieczający zobligowany jest do podania określonych informacji, ponosi również odpowiedzialność za niezgodne z dyspozycją normy zaniechania poczynione w tym procesie, jak i za rzetelność przedstawionych informacji. Jak powinna wyglądać ta regulacja, kiedy część informacji będzie dostępna w publicznych otwartych zbiorach danych? Czy informacje o konstrukcji budynku istotne z punktu widzenia oceny ryzyka nie mogą być zebrane i przeanalizowane przez SI ze skutkiem dla ubezpieczonego? Wystarczy spojrzeć na zastosowanie takich systemów, choćby zesty.ai. To system, który ocenia ryzyko, mając dostęp do map satelitarnych, zdjęć obiektu i innych dostępnych baz danych oraz informacji własnych. Co więcej, pewne dane mogą być zbierane i monitorowane w trakcie trwania ochrony ubezpieczeniowej. Z całą pewnością istnieć będzie potrzeba regulacji we wskazanym zakresie. Jak wspominałem uprzednio, **bardzo mocno rozwijającym się sektorem jest infrastruktura związana z predykcją zdarzeń oraz monitorowaniem parametrów parku maszynowego**. Zawarto już nawet pierwsze umowy ubezpieczenia, które uwzględniają czynnik technologiczny. Ubezpieczony otrzymuje od ubezpieczyciela urządzenia, które w sposób ciągły monitorują ustalone uprzednio parametry. Cel jest oczywisty, chodzi o ograniczenie rozmiarów mogącej wystąpić szkody lub nawet jej uniknięcie. W konsekwencji może to prowadzić bądź do obniżenia ceny, bądź do objęcia ochroną ubezpieczeniową ryzyka, które jeszcze niedawno było oceniane, jako nieakceptowalne.

#### KTO BĘDZIE ODPOWIEDZIALNY ZA SZTUCZNĄ INTELIGENCJĘ?

To rozwiązanie ze wszech miar słuszne i pożądane. Jednak rodzi pytania o określenie zasad odpowiedzialności za działanie bądź niezadziałanie konkretnych urządzeń. Rzecz jasna mamy reżim odpowiedzialności producenta za swój produkt, ale co w sytuacji, w której samo urządzenie działa poprawnie a brak informacji zwrotnej, która winna zostać przekazana wynika z błędów po stronie ubezpieczyciela? Na dodatek zdarzenie nie mieści się w zakresie ubezpieczenia? Ponadto same urządzenia IoT mogą stanowić element wprowadzający nowe dodatkowe ryzyko cybernetyczne. Rynek ubezpieczeniowy reguluje przedmiotową problematykę w formie odpowiednich postanowień i póki co sam wypracowuje własne standardy. Zgodnie z art. 826 kodeksu cywilnego ubezpieczony ma określone obowiązki prewencyjne. Materializują się jednak one dopiero w razie wypadku. Przedstawiciele doktryny prawa ubezpieczeniowego spierają się, czy aby przedmiotowe postanowienie nie dotyczy również zabezpieczenia mienia przed szkodą i przed wystąpieniem szkody niejako wbrew literalnemu brzmieniu przepisu z powołaniem się na funkcję i cel umowy ubezpieczenia. Już samo nieprecyzyjne pojęcie wypadku stanowi problem z uchwyceniem czasowego zakresu materializacji obowiązku. **Nowe technologie mogą z pewnością lepiej i dokładniej przewidzieć etap „przedwypadkowy”**. Co zatem z sytuacją, w której wiemy, że do wypadku może dojść? Czy koszty zapobieżenia szkodzie winny stanowić potencjalny element umowy ubezpieczenia, który stanowiłby również świadczenie ubezpieczyciela? Umowa ubezpieczenia wykraczałaby wtedy poza jej aktualny charakter prawny, jakim jest udzielanie ochrony ubezpieczeniowej. Byłaby również umową, która wskutek doskonałości technologii nie materializowałaby

zdarzenia, jakim jest wypadek ubezpieczeniowy lub też minimalizowałaby jego wystąpienie.

#### WĄTPLIWOŚCI NIE TYLKO PRAWNE, ALE I ETYCZNE

Kolejny element dyskusji to całokształt sfery związanej z odpowiedzialnością za użytkowanie i wprowadzanie w życie gospodarcze nowoczesnych technologii, uczenia maszynowego czy wreszcie sztucznej inteligencji. **Systemy autonomiczne sprawiają, że zarówno etycy, jak i prawnicy mają wiele zagadnień do przemyślenia**. Czy aktualne rozwiązania i prawodawstwo są wystarczające, czy też należy poszukiwać nowych rozwiązań prawnych dla określenia zasad i charakteru odpowiedzialności? Jest oczywiste, że w następstwie pojawi się zapotrzebowanie i nowe produkty ubezpieczeniowe. I nie chodzi tylko o pojazdy autonomiczne. Jakiś czas temu EU postanowiła skodyfikować całość problematyki SI w jednym akcie. Artificial Intelligence Act jest dokumentem, który doczekał się już kilku poprawionych wersji. W aktualnej, w sposób bardzo ogólny wskazuje on, że należy rozważyć kwestię ubezpieczenia i odpowiedzialności. Dokonuje on również podziału systemów SI. Kryterium jest stopień ryzyka wyrządzenia szkód, ingerencji i zakresu możliwej ingerencji w życie publiczne oraz społeczne. Wyróżniono więc systemy niosące wysokie ryzyko dla zdrowia, bezpieczeństwa oraz praw i wolności osobistych. Jako systemy wysokiego ryzyka zostały określone m.in. systemy znajdujące zastosowanie w służbie zdrowia, pojazdy autonomiczne, systemy wyborcze.

#### JAKIE BĘDĄ SUMY GWARANCYJNE DLA UBEZPIECZEŃ SI?

W roku 2020 przyjęta została rezolucja Parlamentu Europejskiego dotycząca reżimu odpowiedzialności (2020/2014(INL)) (2021/C 404/05). W odniesieniu do systemów wysokiego ryzyka zaprojektowano obowiązkowe ubezpieczenie odpowiedzialności użytkowników końcowych (operatorów) lub producentów, w zakresie, w jakim odpowiedzialność nie mieściłaby się, lub wykraczała, poza regulacje dotyczące odpowiedzialności za produkt. Sugerowane sumy gwarancyjne określone zostały na 2 miliony euro na zdarzenie w przypadku szkód na osobie oraz 1 miliona euro w przypadku szkód rzeczowych. Z ciekawostek warto odnotować, iż projektowana regulacja odpowiadała na pytanie, co w sytuacji, w której suma gwarancyjna nie wystarczy na zaspokojenie wielu poszkodowanych, wprowadzając ogólne założenie proporcjonalnej redukcji świadczenia. Wydaje się jednak, że obecnie przeważa koncepcja zakładająca wyłącznie odświeżenie dyrektywny o odpowiedzialności za produkt bez tworzenia odrębnej regulacji. Ocenia się, iż systemowo dyrektywa zdała egzamin i wystarczające będzie wprowadzenie nowych definicji, które w sposób jednoznaczny zakwalifikują oprogramowanie i systemy SI do kategorii podlegających dyrektywie. Warto przy tym wskazać na jedną ze spraw sądowych, która toczyła się w Stanach Zjednoczonych, gdzie wskutek działania algorytmu doszło do zwolnienia z aresztu osoby, która dzień później dokonała morderstwa. Na kanwie tego sporu rozstrzygano, czy tego typu oprogramowanie jest produktem i stwierdzono, że w tym konkretnym przypadku jednak nie. Warto jednak odnotować, jakie potencjalnie zagrożenie może nieść wadliwe działanie podobnych systemów na szeroką skalę. Już samo wyobrażenie sobie zdarzenia polegającego na zderzeniu się dwóch pojazdów autonomicznych każe zastanowić się nad charakterem i zasadami odpowiedzialności. Który system „zawinił”? A może odpowiedzialność solidarna? Są to ciekawe i istotne rozważania, które z całą pewnością będą musiały znaleźć swoją odpowiedź. □