Katarzyna Malinowska

Aspekty prawne ubezpieczenia cyber ryzyk

W niniejszym opracowaniu dokonano analizy charakteru prawnego ubezpieczenia cyber ryzyk z punktu widzenia prawa cywilnego oraz prawa ubezpieczeń, co umożliwilo podjęcie próby zakwalifikowania go do określonego typu ubezpieczenia. Przedstawiono także interakcję cyber ryzyka z otoczeniem prawnym w dziedzinie ubezpieczeń i cyber bezpieczeństwa. Jest to istotne w szczególności z tego powodu, że obydwie te dziedziny podlegają w 2018 r. bardzo dynamicznym legislacyjnym przemianom. Ubezpieczenie cyber ryzyk warto poddać analizie nie tylko z punktu widzenia zarządzania ryzykiem, czy też techniczno-ubezpieczeniowej oceny ryzyka, lecz także z prawnego punktu widzenia. Na tej podstawie będzie można stwierdzić, z jakim typem ubezpieczenia mamy do czynienia i jakie przepisy mogą mieć do niego zastosowanie.

Słowa kluczowe: cyber ryzyko, cyber ubezpieczenie, umowa ubezpieczenia, ochrona danych, cyber bezpieczeństwo.

1. Wprowadzenie

Cyber ubezpieczenie stało się w ostatnim czasie „modnym" tematem, a to za sprawą istotnych zmian ustawodawczych w obszarze ochrony danych osobowych, w szczególności zaś sankcji grożących potencjalnie podmiotom przetwarzającym dane osobowe na podstawie rozporządzenia RODO[1]. Zwróciło ono baczną uwagę zarówno pośredników ubezpieczeniowych, jak i ubezpieczających oraz ubezpieczycieli na to, że we współczesnym świecie już od dość dawna mamy do czynienia z postępującą zależnością od technologii informacyjnych i komunikacyjnych, a w tym nasilającym się przenoszeniem ciężaru aktywów z materialnych na niematerialne, co nie mogło pozostać bez wpływu na rodzaj związanych z nimi zagrożeń.

Wydaje się, że występuje tu swoiste sprzężenie zwrotne. Ubezpieczenia cyber rodzą świadomość co do istnienia ryzyka i skali zagrożenia, w tym zwłaszcza co do konieczności wdrażania narzędzi poprawiających bezpieczeństwo w cyber przestrzeni, to zaś prowadzi do faktycznej poprawy sytuacji, powodującej zwiększenie dostępności ubezpieczenia, buduje jego statystyki, obniża składki i wspomaga jego rozwój.

[1] 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); (dalej: rozporządzenie RODO). Rozporządzenie to obowiązuje bezpośrednio w porządku prawnym. Zwrócić także należy uwagę na projekt rozporządzenia UE o prywatności i łączności elektronicznej opublikowany przez Komisję Europejską 10 stycznia 2017 r. – COM(2017)10.

Celem artykułu jest więc, po pierwsze, udzielenie odpowiedzi na pytanie, co oznacza w istocie cyber ryzyko w kontekście przedmiotu ochrony ubezpieczeniowej, jakie są jego źródła i faktory oraz jakie są konsekwencje realizacji cyber zagrożeń. Dopiero wówczas możliwe jest sprecyzowanie przedmiotu i zakresu ubezpieczenia cyber ryzyk, szacowania ryzyka i szkody, specyfiki obowiązków stron i wreszcie koncepcji uczestniczenia ubezpieczyciela w procesie naprawienia szkody. Rola pośrednika ubezpieczeniowego w tym kontekście jest nie do przecenienia. Mając na uwadze przepisy ustawy o dystrybucji ubezpieczeń w zakresie analizy potrzeb klienta, dotyczyć to będzie nie tylko brokera, lecz także agenta.

2. Natura cyber ryzyka jako przedmiotu ubezpieczenia

Na początku należy stwierdzić, że brak jest jednej utrwalonej, a tym bardziej wiążącej definicji cyber ryzyka[2]. Dla celów niniejszego opracowania najbardziej przydatne, jak się wydaje, są definicje stworzone na potrzeby ochrony ubezpieczeniowej, choć należy także brać pod uwagę bardziej ogólne jego rozumienie. Poza poszukiwaniem definicji samego cyber ryzyka, konieczne wydaje się też przedstawienie dodatkowych jego czynników (faktorów ryzyka), jego źródeł oraz skutków. Te ostatnie w szczególności przeniosą nas na grunt przedmiotu i zakresu ochrony ubezpieczeniowej.

Cyber ryzyko utożsamiane jest z ryzykiem informatycznym i określane jako ryzyko operacyjne związane z użyciem, posiadaniem, zarządzaniem, wpływaniem lub wdrażaniem technologii informatycznych w przedsiębiorstwie. Określane jest także jako ryzyko nieuprawnionego zdobycia i wykorzystania informacji różnego rodzaju. Takie szerokie ujęcie jest uzasadniane tym, że podobne konsekwencje realizacji ryzyka IT mogą nastąpić bez względu na to, czy przyczyną było celowe działanie, czy też nie, lub czy jego źródłem są zewnętrzne wobec przedsiębiorstwa zasoby Internetu, czy też ma swoje źródło wewnątrz podmiotu.

Najbardziej przydatna wydaje się być definicja cyber ryzyka przyjęta przez Geneva Association, zgodnie z którą **cyber ryzyko to każde ryzyko wynikające z wykorzystywania technologii informatycznych i komunikacyjnych[3], które zakłada poufność, dostępność i integralność danych lub usług**. Zaburzenie technologii operacyjnych prowadzi do zakłócenia działalności, załamania działania infrastruktury (w tym krytycznej), materialnych szkód osobowych i rzeczowych. Cyber ryzyko w takim ujęciu jest powodowane w sposób naturalny przez cechy technologii lub przez działanie ludzkie, takie

[2] T. Grabowska, „Cyber przestępczość w świecie finansów – ryzyka cybernetyczne", Rozprawy Ubezpieczeniowe 18 (1/2015).

[3] National Institute of Standards and Technology (NIST, 2013) definiuje przestrzeń cybernetyczną jako: „*Globalna przestrzeń w środowisku informacyjnym składająca się z współzależnej sieci infrastruktur systemów informatycznych, w tym Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz wbudowanych procesorów i kontrolerów*". Zob. The Geneva Association, „Ten key questions on Cyber Risk and Cyber Risk Insurance", 7 December 2016.

jak: błąd ludzki, działania o charakterze przestępczym (wymuszenie, fałszerstwo), wojnę cybernetyczną lub cyber terroryzm. Charakteryzuje się ono współzależnością zdarzeń i ich skutków, ich potencjalnie katastroficznym rozmiarem, wysoką niepewnością pod względem podejścia do modelowania oraz dużym potencjałem wahań. Taka definicja zawiera wiele czynników, które umożliwiają wyodrębnienie z niej elementów stanowiących źródło ryzyka (zagrożenie) oraz jego konsekwencji (straty).

Natomiast pod kątem czynników mających wpływ na cyber ryzyko wymienia się występujące w obecnym świecie zjawisko określane jako współzależność działalności i systemów, które mogą prowadzić do wewnętrznego zakłócenia działalności, ale także większej podatności na skutki zewnętrznych zjawisk. Skutki tego mogą być pogłębiane przez wzrost współzależności nie tylko w obszarze wymiany danych pomiędzy sektorem prywatnym i publicznym (np. rejestry publiczne dostępne *online*), lecz także na poziomie funkcjonowania infrastruktury krytycznej. Z tego powodu można powiedzieć, że cyber zagrożenia leżą w obszarze publicznym i prywatnym ujmowanych łącznie, a zapobieganie im polega na zapewnieniu indywidualnym odbiorcom (obywatelom) nieprzerwanego dostępu do usług podstawowych dla życia oraz ciągłości funkcjonowania gospodarki i administracji publicznej[4].

Analizując źródła zagrożeń pod względem ich kategoryzacji, trzeba posłużyć się kryteriami, obejmującymi: rodzaj zdarzenia (celowe działanie lub zdarzenia nieumyślne), podmiot dokonujący (terroryści, przedsiębiorcy, wyspecjalizowani przestępcy cybernetyczni, podmioty sponsorowane przez państwa – szpiegowskie działania, aktywiści oraz pracownicy zarówno obecni, jak byli).

Działania umyślne określane są popularnie ogólnym **pojęciem cyber ataku**, **definiowanego przez Lloyd's jako celowy akt elektroniczny, będący bezpośrednią przyczyną szkody**[5].

Innym kryterium jest **natarczywość działania**, pod względem którego podzielić można je na: przypadkowe i krótkoterminowe, automatyczne, niezdefiniowane skanowanie, jak też najgroźniejsze – długoterminowe uporczywe działania.

---

[4] Patrz np. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego", Bruksela, 5.07.2016, COM (2016) 410 final. Szerzej na temat infrastruktury krytycznej i zarządzania kryzysowego: W. Skomra, „Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego, Rządowe Centrum Bezpieczeństwa, http://www.archiwalna.powiat-wloszczowa.pl/ochrona_ludnosci/OIK_w_systemie_zarzadzania_kryzysowego.pdf. Patrz też definicja infrastruktury krytycznej w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn. Dz. U. z 2017 r. poz. 209, z późn. zm.). W. Skomra, w: „Zarządzanie ryzykiem. Przegląd wybranych metodyk, praca zbiorowa, D. Wróblewski (red.), Warszawa 2015, s. 295 i n. O aspektach ekonomicznych cyber bezpieczeństwa szerzej: R. Anderson, T. Moore, „The Economics of Information Security: A survery and open questions", https://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf

[5] The Geneva Association, „Ten key questions...", *op.cit*.

Kolejnym kryterium jest **zasięg działania podmiotu atakującego**, gdzie wyróżnić można działania w zasięgu tej samej sieci *wi-fi*, działania wewnętrzne (*insider*), fizyczny dostęp do sprzętu IT, jak również zdalne działania za pomocą Internetu.

Niewątpliwie do cyber zagrożeń należą nie tylko działania celowe, lecz także zdarzenia o charakterze niecelowym, gdzie można mieć do czynienia z błędem w działaniu sprzętu lub oprogramowania lub też błędy wynikające z działania ludzkiego (np. utrata laptopa z danymi). **Innym kryterium analizy jest przedmiot narażony na zdarzenie, a więc osoba, nośnik, system, poszczególne informacje lub cała sieć**[6]. Ta różnorodność zagrożeń powoduje, że są one trudne do zidentyfikowania i zwalczania. Z perspektywy ubezpieczyciela zagrożenia powyższe są niekiedy porównywalne do ryzyka terroryzmu lub ryzyka katastroficznego, choć w miarę zdobywania doświadczenia, w tym gromadzenia danych o cyber ryzyku, stanie się ono zapewne ryzykiem jak każde inne[7]. Identyfikując zaś dodatkowe faktory cyber ryzyka można je podzielić na wewnętrzne, a wśród nich na szpiegostwo, wyciek danych, zmiany personelu oraz oszustwo, a także zewnętrzne (które jednak łączą się z wewnętrznymi, tam gdzie mówimy o przestępstwie, w szczególności o celowym wyrządzeniu szkody)[8].

Mając na uwadze powyższe, konieczne jest wyodrębnienie konsekwencji, jakie mogą powodować te zagrożenia. W myśl bowiem przyjętej koncepcji ryzyka definiowane jest ono jako wypadkowa prawdopodobieństwa określonego zdarzenia – zagrożenia i konsekwencji, jakie może powodować wystąpienie owego zdarzenia[9]. **Przechodząc zaś na płaszczyznę skutków, jakie mogą powodować cyber zagrożenia, można wyróżnić kilka cech charakterystycznych dla cyber ryzyka**, nieobecnych w ogóle lub w nieporównywalnie mniejszym stopniu w innego rodzaju ubezpieczeniach. Obejmują one swoisty publiczny charakter skutków realizacji cyber ryzyka, a więc zagrożenie dla reputacji przedsiębiorstwa i międzynarodowy charakter zagrożenia z uwagi na transgraniczny przepływ danych. Ponadto zaś występuje niespotykane, wręcz krytyczne, znaczenie czasu w reagowaniu na realizację cyber ryzyka oraz wspomniana już wysoka współzależność pomiędzy wszystkimi uczestnikami gospodarki, zarówno publicznymi, jak i prywatnymi. Ma to także znaczenie z punktu widzenia ubezpieczyciela, jako że na skutek jednego zdarzenia mogą powstać szkody u ogromnej liczby podmiotów, rozmieszczonych w różnych częściach świata, co implikuje m.in. specyfikę likwidacji takich szkód. To powoduje też możliwy scenariusz agregowania

[6] „UK Cyber security, the role of insurance in managing and mitigating the risk" March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.; dostęp 5 lutego 2018.

[7] Insurance 2020 and beyond: Reaping the dividends of cyber resilience, https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

[8] M. Vos, „Handling of cyber risks claims. Presentation", June 2015, Lloyd's (materiał niepublikowany).

[9] Więcej na temat różnych koncepcji ryzyka E. Vaughan, T. Vaughan, „Fundamentals of Risk and Insurance", 2008 John Wiley& Sons, Inc., s. 3 i n.

szkód w wymiarze globalnym, a tym samym ich katastroficzny rozmiar z punktu widzenia ubezpieczyciela i reasekuratora. Scenariusze szkód katastroficznych są brane pod uwagę w szczególności w takich rodzajach szkód, jak naruszenie danych, przerwa w działalności, naruszenie systemów płatności, przerwa w dostawie energii na skalę krajową[10].

Podobnie jak skutki, także **stopień prawdopodobieństwa** ich wystąpienia trzeba uznać za poważny. Raporty w tej dziedzinie wskazują na zajście ponad 100 000 zdarzeń dziennie w skali światowej, przy jednocześnie wzrastającej wysokości szkody nimi spowodowanej. Rzeczywisty rodzaj i zakres ryzyka, z którym powinno się zmierzyć dane przedsiębiorstwo, zależy od przedmiotu i zakresu jego działalności. Choć jest oczywiste, że na cyber zagrożenia narażone są obecnie niemal wszystkie podmioty obecne na rynku w przestrzeni wirtualnej bądź nie, z pewnością przedsiębiorstwa w obszarze *e-commerce* narażone są w dwójnasób[11].

Próbując dokonać kwalifikacji skutków, jakie powoduje realizacja zagrożenia, należy rozważyć kilka możliwych kryteriów. Pod względem przedmiotowym, będziemy mieli do czynienia z utratą kontroli lub naruszenia integralności systemu *hardware* i *software*, a także naruszenia danych. W konsekwencji zaś, wśród najczęściej wymienianych znajduje się konieczność poniesienia kosztów naprawy naruszenia[12], przerwa w działalności, utrata wartości akcji przedsiębiorstwa lub odpowiedzialność cywilna wobec osób trzecich oraz odpowiedzialność administracyjna. Podchodząc zaś systematycznie do szkód, jakie mogą być wyrządzone, można je podzielić aż na jedenaście kategorii rozpatrywanych łącznie jako wynikające z cyber ataków lub nieumyślnych szkód w systemie IT[13].

Po pierwsze, możemy mieć do czynienia **z kradzieżą własności intelektualnej oraz ewentualnie wrażliwych komercyjnie danych**. Ten rodzaj szkody uznaje się za najbardziej dotkliwy dla dużych przedsiębiorstw, w szczególności tak wrażliwych pod względem wartości danych, jak w przemyśle kosmicznym, chemicznym, farmaceutycznym lub medialnym. Z kolei wśród małych i średnich przedsiębiorstw największym problemem wydaje się być ryzyko szkód wynikłych z naruszenia bezpieczeństwa oprogramowa-

---

[10] Także z tej przyczyny ubezpieczyciele biorący udział w ostatnim *Banana skin survey* uznali cyber ryzyko za największe zagrożenie dla prowadzonej przez nich działalności. Zob. Insurance 2020 and beyond..., *op. cit.*

[11] Koszt ponoszony zaś przez globalną gospodarkę oscyluje rocznie w granicach 400 bilionów dolarów, 2015 Information Security Breaches Survey. Department for Business, Innovation and Skills/PwC, www.pwc.co.uk/services/audit-assurance/insights/2015-information-securitybreaches-survey.html; zob. także P. Low, „Insuring against cyber-attacks.",Insurance 2020 and beyond..., *op. cit.*

[12] Szacuje się, że średni koszt naruszenia wynosił 561 495,6 dolarów amerykańskich, 2011 Annual Cost of a Data Breach report, the Ponemon Institute. „2011 Cost of Data Breach Study" Symantec and Ponemon Institute, March 2012, www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf.; dostęp 5 lutego 2018.

[13] „UK Cybersecurity; the role of insurance in managing and mitigating the risk", March 2015; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.

nia i danych, w tym danych osobowych klientów, tym bardziej że w przeciwieństwie do dużych przedsiębiorstw brak jest wdrożonych awaryjnych planów działalności. Szkoda polegająca na przerwie w działalności lub wykonywaniu zobowiązań przez podmiot dotknięty atakiem, utrata danych lub oprogramowania stwarzają największe zagrożenie dla firm zajmujących się obrotem oprogramowania (np. sprzedaż gier komputerowych *online*). Wśród pozostałych, mających największe znaczenie dla gospodarki, wymienia się bezpośrednie straty finansowe polegające na kradzieży środków pieniężnych, lub wymuszeniu płatności, a także szkody pośrednie lub bezpośrednie, dotykające osób lub dóbr materialnych. Ten ostatni rodzaj szkody budzi coraz więcej niepokoju, a to z uwagi na strategiczne znaczenie dla wielu gałęzi gospodarki.

Dość szczególnym typem szkody, mogącym występować dodatkowo do każdej z powyższych, jest **szkoda reputacyjna,** dość szczególna w kontekście trudności jej oszacowania i zarządzania ryzykiem jej powstania. Na ryzyko takiej szkody najbardziej narażone są duże przedsiębiorstwa. W obecnej chwili najmniejsze prawdopodobieństwo szkód dotyczy szkód osobowych, jednak i takich nie można wykluczyć wraz ze wzrostem zastosowania technologii w życiu prywatnym.

Do szkód spowodowanych cyber ryzykiem niewątpliwie należy także zaliczyć koszty innego rodzaju, a w tym przede wszystkim wynikające z odpowiedzialności wobec kontrahentów i osób trzecich. W kontekście tych pierwszych realizacja cyber ryzyka może oznaczać niewykonanie lub nienależyte wykonanie zobowiązania i związane z tym roszczenia odszkodowawcze (którymi można zarządzać przez odpowiednie klauzule kontraktowe i właśnie ubezpieczenie). Należy brać pod uwagę również roszczenia pracowników, których dane zostały wykorzystane, a także roszczenia o charakterze D&O kierowane przez udziałowców spółki. Te same czynniki obecne będą na płaszczyźnie odpowiedzialności wobec osób trzecich.

Reasumując więc, możemy mieć do czynienia z przerwą w działalności, odpowiedzialnością za wadliwy produkt lub usługę, szkodą rzeczową, czystą stratą finansową, a także odpowiedzialnością członków zarządu (D&O oraz E&O).

Szkody te można podzielić także według innych kryteriów, a mianowicie biorąc pod uwagę kryterium podmiotowe, tj. ze względu na relacje podmiotowe, w których występuje strata. Po pierwsze, będzie to więc podmiot, który bezpośrednio doznaje straty, a więc ryzyko utraty własnych aktywów (*first party risk*), po drugie, będzie to ryzyko utraty aktywów podmiotów powiązanych (także kontraktowo) (*second party risk*), po trzecie zaś, ryzyko związane z odpowiedzialnością wobec osób trzecich (*third party risk*).Wszystkie one charakteryzują się różnorodnym potencjałem rozciągliwości w czasie, w tym także *long tail risks*, a to z powodu silnych współzależności systemów, które mogą być dotknięte szkodą. Jedno zdarzenie może więc być źródłem zarówno szkody w aktywach własnych, którego wykrycie i konsekwencje następują od razu, jak i źródłem postępo-

wania administracyjnego, skutkującego po pewnym dopiero czasie nałożeniem sankcji na podmiot, a także źródłem odpowiedzialności wobec osób trzecich, odciągniętej nawet znacznie w czasie, w zależności od czasu wystąpienia konsekwencji[14].

Przedstawione powyżej cechy cyber zagrożeń są istotne dla identyfikacji, z jakim rodzajem ubezpieczenia mamy w istocie do czynienia. Oczywistą konstatacją jest, że należy ono do grona ubezpieczeń majątkowych, zarówno w regulacji umowy ubezpieczenia w kodeksie cywilnym, jak i w ustawie o działalności ubezpieczeniowej i reasekuracyjnej, jako ryzyko należące do ubezpieczeń działu II. Można wyróżnić następujące rodzaje szkód:

1) szkody rzeczowe rozumiane jako uszkodzenie, zniszczenie lub utrata rzeczy (na skutek realizacji zagrożeń związanych z tzw. internetem rzeczy lub zarządzaniem infrastrukturą kryzysową),
2) czyste straty finansowe,
3) inne rodzaje straty finansowej związanej z przerwą w działalności, w tym w szczególności z utratą zysku,
4) odpowiedzialność wobec osób trzecich, przy czym należy ją zakwalifikować do odpowiedzialności cywilnej ogólnej.

Jak wynika z powyższych rozważań, ubezpieczenie cyber ryzyk pod względem przedmiotowym będzie można zakwalifikować do ubezpieczenia z **grupy 9 –** ubezpieczenia pozostałych szkód rzeczowych (jeżeli nie zostały ujęte w grupach 3, 4, 5, 6 lub 7), wywołanych przez grad lub mróz oraz inne przyczyny (jak np. kradzież), jeżeli przyczyny te nie są ujęte w grupie 8; **grupy 13** – ubezpieczenia odpowiedzialności cywilnej (ubezpieczenie odpowiedzialności cywilnej ogólnej) nieujętej w grupach 10–12; a wreszcie do **grupy 16 –** ubezpieczenia ryzyk finansowych, w tym: m.in. utraty zysków, stałych wydatków ogólnych, nieprzewidzianych wydatków handlowych oraz innych strat finansowych; **grupy 17 –** ubezpieczenia ochrony prawnej.

3. Zakres ochrony prawnej i jego wpływ na prawną kwalifikację umowy ubezpieczenia

Kwalifikacja przedmiotu ubezpieczenia cyber nie przesądza jeszcze jednak o zakresie ochrony. Zasadniczą rolę w kształtowaniu zakresu ochrony ubezpieczeniowej odgrywa praktyka, dynamika cyber zagrożeń i konieczność elastycznego reagowania na nie także pod względem konstrukcji zakresu ochrony w określonych powyżej ramach przedmiotowych. Zakres cyber ubezpieczenia będzie więc wypadkową techniki ubezpieczeniowej i informatycznej, z przewagą tych ostatnich elementów, a to z uwagi na małą jeszcze statystykę szkodową i ograniczone możliwości zastosowania prawa wielkich liczb w tym rodza-

[14] Wynika to z faktu, że odpowiedzialność wobec osób trzecich wymaga spełnienia kilku przesłanek, a ostatnią z nich jest zazwyczaj poniesienie szkody możliwej do oszacowania w pieniądzach. Zob. chociażby art. 361 k.c., zgodnie z którym naprawieniu podlega każda szkoda (strata rzeczywista i utrata korzyści), o ile pozostaje w normalnym związku przyczynowym ze zdarzeniem ją wyrządzającym.

ju ubezpieczenia[15]. Stanowi to o jego specyfice, gdzie ubezpieczyciel musi wciąż jeszcze być raczej specjalistą z zakresu nowych technologii bardziej niż techniki ubezpieczeniowej. Dynamiczny rozwój tych ubezpieczeń przypuszczalnie zmieni tę sytuację w dość szybkim tempie.

Zaznaczyć należy, że przez długi okres ochrona przed cyber ryzykami była zapewniana w ramach ubezpieczenia mienia, *business interruption*, ogólnej odpowiedzialności cywilnej, a także profesjonalnej odpowiedzialności cywilnej (*Errors and omissions/Professional indemnity*). Jednak z uwagi na fakt, że nie były one konstruowane z myślą o tych cyber ryzykach, pomimo przedmiotowej zgodności, zakres ich był w istocie niedostosowany do specyfiki ryzyka, stąd najbardziej krytyczne ryzyka objęte są wyłączeniem odpowiedzialności ubezpieczyciela. Odpowiedzią rynku ubezpieczeń na wzrastający poziom cyber zagrożeń było wypracowanie dedykowanego zakresu ubezpieczenia cyber ryzyk i oferowanie go jako odrębnego produktu ubezpieczeniowego, który kompleksowo może zapewnić kompatybilny z zagrożeniem poziom ochrony[16]. Zakwalifikowanie ubezpieczenia cyber ryzyk, jako wyodrębnionego produktu ubezpieczeniowego, wymaga odniesienia się, choćby do definicji tego pojęcia. W polskim systemie prawa przyjęło się mianowicie za produkt uważać *„projektowany/tworzony lub oferowany przez Zakład produkt rozumiany jako typ umów ubezpieczenia lub gwarancji ubezpieczeniowych, identyfikowanych przez odrębne warunki ubezpieczenia lub wewnętrzne oznaczenie stosowane w Zakładzie, zawieranych na podstawie tych samych wzorców umownych, dedykowanych temu produktowi”*[17]. Jak widać, jest to pojęcie funkcjonalne, nie zaś prawne.

Zakres ubezpieczenia obejmuje zazwyczaj **trzy podstawowe typy zdarzeń** składających się na cyber ryzyka, tj. odpowiedzialność cywilną, ryzyka finansowe związane z przerwą w działalności ubezpieczającego lub innego rodzaju kosztami, stanowiącymi czystą stratę finansową, a także ubezpieczenia kosztów ochrony prawnej.

Szczególnie interesujące są tym względzie postanowienia umów ubezpieczenia, definiujące zdarzenia implikujące odpowiedzialność cywilną ubezpieczającego. Zakres ubezpieczenia znacząco różni się od tzw. ubezpieczenia ogólnej odpowiedzialności cywilnej, obejmując tylko wycinek potencjalnej odpowiedzialności

---

[15] Więcej na temat prawa wielkich liczb E. Vaughan, T. Vaughan, „Fundamentals of Risk and Insurance”, 2008 John Wiley&Sons, Inc., s. 36.

[16] P. Low, „Insuring against cyber-attacks…”, *op. cit.* Przykładem może być np. ubezpieczenie odpowiedzialności pracodawcy, w którym zakresem ochrony mogą być objęte także roszczenia wynikające z korzystania z Internetu przez pracownika. Z kolei ubezpieczenie odpowiedzialności członków zarządu (D&O) mogłoby obejmować roszczenia wynikające z nienależytej oceny przez ubezpieczonego ryzyka związanego z handlem elektronicznym. K. Burden, Barlow Lyde&Gilbert, „E-Risk and Insurance”, Computer Law & Security Report 2000/16(4).

[17] W takim brzmieniu definicja ta została zaproponowana w Rekomendacjach dotyczących systemu zarządzania produktem ubezpieczeniowym wydanych przez KNF 22 marca 2016 r. Patrz więcej: K. Malinowska, „Pojęcie zarządzania produktem ubezpieczeniowym w świetle dyrektywy o dystrybucji ubezpieczeń i przepisów implementacyjnych, Wiadomości Ubezpieczeniowe, 2017, nr 1, s. 9 i n.

ubezpieczonego[18]. Biorąc pod uwagę rodzaj szkód, jakie mogą zostać wyrządzone osobom trzecim, zakresem ubezpieczenia objęte są zdarzenia polegające na naruszeniu prywatności[19], danych[20], bezpieczeństwa[21] i skutków z tym związanych. Zakresem ubezpieczenia objęte może być zarówno świadczenie odszkodowawcze, zgodnie z art. 822 k.c., jak również koszty ochrony przed roszczeniem, a także tzw. koszty reakcji na zdarzenie, które powinny być kwalifikowane jako koszty ratownictwa, ujęte w sposób ogólny w art. 826 k.c. O ile jednak objęcie kosztów ochrony przed roszczeniem jest wynikiem praktyki kontraktowej z uwagi na dobrowolność ubezpieczenia (i należące do innej grupy ubezpieczeń)[22], o tyle koszty ratownictwa, polegające na ratowaniu przedmiotu ubezpieczenia oraz zapobieżeniu szkodzie lub zmniejszeniu jej rozmiarów, leżą w granicach zobowiązania ubezpieczyciela wynikającego z art. 826 § 4 k.c. (*„Ubezpieczyciel obowiązany jest, w granicach sumy ubezpieczenia, zwrócić koszty wynikłe z zastosowania środków, o których mowa w § 1, jeżeli środki te były celowe, chociażby okazały się bezskuteczne. Umowa lub ogólne warunki ubezpieczenia mogą zawierać postanowienia korzystniejsze dla ubezpieczającego”*).

Praktyka rynkowa wskazuje na praktyczne zastosowanie powyższego przepisu, choć naprawienie szkody spowodowanej realizacją cyber ryzyka powoduje niejednokrotnie trudności w ocenie, czy mamy do czynienia z kosztami ratownictwa, czy już naprawieniem szkody *sensu stricto*. W jednym i drugim przypadku wspólnym mianownikiem powinno być, w miarę możliwości, przywrócenie stanu poprzedniego, sprzed zajścia wypadku ubezpieczeniowego (np. przywrócenie funkcjonalności systemu komputerowego, technicznego odtworzenia, odzyskania lub ponownego zainstalowania danych bądź programów komputerowych, w tym koszty zakupu licencji na oprogramowanie niezbędne do odtworzenia tych danych lub programów komputerowych). Niemniej jednak należy uznać, że konstrukcja zakresu ochrony pozwalająca na pokrycie kosztów ekspertów, których celem jest zapobieżenie zwiększaniu się szkody, zbliża charakter świadczenia z tego tytułu do kosztów ratownictwa. Dotyczy to tych działań, które są podejmowane po ujawnieniu naruszenia danych, prywatności lub bezpieczeństwa, a mają na celu zapobieżenie ich skutkom lub zmniejszenie

[18] M. Krajewski, „Ubezpieczenie odpowiedzialności cywilnej według kodeksu cywilnego”, Warszawa 2011, s. 40–42; M. Serwach, „Komentarz do art. 822 k.c., w: M. Serwach (red.), M. Glicz (red.), „Komentarz do niektórych przepisów ustawy – Kodeks cywilny, w: „Prawo ubezpieczeń gospodarczych”. Tom II. Komentarz, wyd. II, LEX 2010.

[19] Definiowane jako nieuprawnione ujawnienie przez ubezpieczonego danych osobowych poszkodowanego; lub nieuprawniony dostęp lub wykorzystanie danych osobowych przechowywanych w systemie informatycznym ubezpieczonego stanowiące naruszenie przepisów o ochronie danych osobowych.

[20] Zazwyczaj definiowane jako ujawnienie informacji o kliencie przez ubezpieczonego lub nieuprawniony dostęp czy też wykorzystanie informacji o kliencie przechowywanych w systemie informatycznym ubezpieczonego.

[21] Definiowane jako działanie lub zaniechanie ubezpieczonego, na skutek którego doszło do cyber ataku.

[22] Koszty ochrony definiowane są zazwyczaj jako opłaty sądowe, koszty oraz wydatki poniesione przez ubezpieczonego w związku z postępowaniem przygotowawczym, repliką, obroną, środkiem zaskarżenia lub ugodą dotyczącą roszczenia wniesionego przez osobę trzecią.

ich zakresu (takich jak zabezpieczenie danych, informowanie poszkodowanych, organizowanie *call center*, analiza przyczyn i skutków zdarzenia itp.).

W zakres ochrony ubezpieczeniowej wchodzą także koszty doradztwa na rzecz ubezpieczonego w zakresie ustawowych obowiązków publiczno-prawnych, związanych z ujawnieniem naruszenia i pomocy w wypełnianiu takich obowiązków. Świadczenia w tym zakresie można kwalifikować zarówno jako ubezpieczenie kosztów ochrony prawnej, jak i ubezpieczenie strat finansowych, w zależności od charakteru podejmowanych czynności oraz kwalifikacji podmiotu je podejmującego (prawnik czy ekspert IT).

Pod względem podmiotowym konstrukcja ubezpieczenia odpowiedzialności cywilnej w zakresie cyber ryzyka może obejmować zarówno samego ubezpieczającego, jak również przyjmować postać ubezpieczenia na rzecz osoby trzeciej w taki sposób, że ochrona dotyczy nie tylko odpowiedzialności, którą ponosi ubezpieczający (za czyny własne lub czyny innych osób na podstawie art. 429, 430 lub 474 k.c.), lecz także odpowiedzialności powiązanych podmiotów trzecich. Powyższe rozróżnienie jest bardzo istotne, także w kontekście odpowiedzialności pracowników i członków zarządu spółki, za których ubezpieczający będący osobą prawną nie zawsze będzie ponosił odpowiedzialność na podstawie przepisów prawa (cywilnego, pracy, handlowego). Objęcie ich osobistej odpowiedzialności jako odrębnego zakresu ubezpieczenia może więc być kluczowe dla zaspokojenia interesu ubezpieczeniowego organizacji jako całości.

Poza odpowiedzialnością cywilną, zakres ochrony ubezpieczeniowej może obejmować koszty nałożonych na ubezpieczonego grzywien i kar oraz koszty reprezentacji ubezpieczonego w postępowaniu administracyjnym lub karnym toczącym się w sprawie lub przeciwko ubezpieczonemu w związku z zajściem wypadku ubezpieczeniowego (lub tylko niektórych zdarzeń kwalifikowanych jako wypadek ubezpieczeniowy). Ten typ ryzyka objęty zakresem ochrony ubezpieczeniowej należy zakwalifikować jako ubezpieczenie ryzyk finansowych, co oznacza, że z punktu widzenia cywilnoprawnego zastosowania nie mają przepisy o umowie ubezpieczenia odpowiedzialności cywilnej, lecz ogólne przepisy o ubezpieczeniach majątkowych.

Drugi typ ochrony w ramach ubezpieczenia cyber ryzyka dotyczy strat finansowych. W tym względzie, zakres ubezpieczenia obejmuje przede wszystkim skutki przerwy w działalności i związanych z tym strat poniesionych przez ubezpieczającego. Podobnie jak wyżej wymieniona ochrona dotycząca kosztów kar i grzywien, stanowi to rodzaj ubezpieczenia ryzyk finansowych. W tym zakresie ochrona ubezpieczeniowa obejmuje straty z tytułu przerwy w działalności określanej zazwyczaj jako konieczne i całkowite przerwanie lub spowolnienie działalności produkcyjnej lub usługowej ubezpieczonego, poniesione przez ubezpieczonego w związku (zazwyczaj bezpośrednim) z brakiem dostępności systemu informatycznego, a także koszty wznowienia działalności poniesione w bezpośrednim związku ze zdarzeniem powodującym przerwę w działalności, a polegające zasadniczo na poniesieniu kosztów zaangażowania ekspertów w celu przywrócenia funkcjonalności systemu informatycznego ubezpieczającego, w tym odtworzenia danych lub oprogramowania albo naby-

cia nowych. Charakter czystych strat finansowych ma także ochrona z tytułu szkód poniesionych na skutek ataków hakerskich na systemy informatyczne, a także ochrona z tytułu szkód wywołanych cyber wymuszeniem, poniesionych w celu usunięcia zdarzenia powodującego naruszenie danych lub prywatności[23], a także koszty wynikające z omyłkowo wypłaconych kwot na skutek cyber ataku czy też wykorzystanie systemu informatycznego ubezpieczającego do realizowania przepływów finansowych. Pod względem prawnym, tę samą konstrukcję przyjmuje zakres ubezpieczenia polegający na pokryciu kosztów poniesionych na tzw. *public relations* w związku z koniecznością ochrony reputacji ubezpieczonego, polegających na pokryciu kosztów konsultantów z zakresu *public relations* lub tzw. komunikacji kryzysowej[24].

Ważnym aspektem zakresu ubezpieczenia jest tzw. *trigger*, czyli czynnik czasowy warunkujący ochronę ubezpieczeniową. Stanowi on „czasowy" element wypadku ubezpieczeniowego, który – zgodnie z art. 805 i 806 k.c. – musi zajść w okresie ubezpieczenia. W praktyce ubezpieczeniowej mamy do czynienia najczęściej z *triggerem* opartym na wniesieniu roszczenia (*claims made*), powstaniu szkody (*loss occurrence*) lub zdarzeniu wyrządzającym szkodę (*act committed*), a rozróżnienie tych zdarzeń ma największe znaczenie w ubezpieczeniu odpowiedzialności cywilnej, w sposób wynikający z treści art. 822 § 2 i 3 k.c., zgodnie z którym, jeżeli strony nie umówiły się inaczej, umowa ubezpieczenia odpowiedzialności cywilnej obejmuje szkody, będące następstwem przewidzianego w umowie zdarzenia, które miało miejsce w okresie ubezpieczenia. Jednak strony mogą postanowić, że umowa będzie obejmować szkody powstałe, ujawnione lub zgłoszone w okresie ubezpieczenia. Wobec faktu, że ubezpieczenie cyber ryzyk łączy w sobie cechy różnych ubezpieczeń, definicja wypadku ubezpieczeniowego pod względem czasowym będzie się różnić w poszczególnych zakresach ochrony. I tak więc w części dotyczącej ochrony od odpowiedzialności cywilnej możemy mieć do czynienia z wypadkiem ubezpieczeniowym, polegającym na zajściu zdarzenia powodującego odpowiedzialność w okresie ubezpieczenia, np. naruszenia danych, prywatności lub bezpieczeństwa (*act committed*), lub też powstania szkody z tego tytułu (*loss occurrence*), albo zgłoszenia roszczenia odszkodowawczego w okresie ubezpieczenia (*claims made*). Specyfika cyber ryzyka wskazuje jednak na nieraz znaczne trudności w identyfikacji momentu zajścia zdarzenia wyrządzającego szkodę, a także skomplikowany proces identyfikowania momentu powstawania szkody. Z tego powodu dość częstym *triggerem* stosowanym w ubezpieczeniu odpowiedzialności cywilnej jest *trigger claims made*, przewidujący ochronę z tytułu roszczeń odszkodowawczych zgłoszonych po raz pierwszy w okresie ubezpieczenia lub ewentualnie w okresie dodatkowym, jeżeli taki będzie miał zastosowanie.

---

[23] W tym względzie ochrona obejmuje zarówno koszty ekspertów zarządzających zdarzeniem i prowadzących np. negocjacje, jak i kwoty wypłacone tytułem okupu.

[24] Definiowane jest to jako negatywny rozgłos wynikający z wypadku ubezpieczeniowego; czasem ujmowane jako koszty komunikacji kryzysowej.

Takie ujęcie wypadku ubezpieczeniowego nie będzie miało zastosowania do części ochrony ubezpieczeniowej, polegającej na kompensacji skutków przerwy w działalności lub innych strat finansowych, wynikłych z zajścia cyber zdarzenia. W tym zakresie wypadkiem ubezpieczeniowym będzie ujawnienie zajścia zdarzenia objętego ubezpieczeniem, a więc ujawnienie naruszenia danych, prywatności lub bezpieczeństwa. Jest to ujęcie także nieco odbiegające od popularnych form ubezpieczenia mienia lub ryzyk finansowych, w których wypadek ubezpieczeniowy obejmuje zazwyczaj zajście, a nie ujawnienie określonego zdarzenia w okresie ubezpieczenia. Różnica ta wynika w sposób oczywisty z natury cyber ryzyka. Stwierdzenie momentu zajścia naruszenia jest niezwykle trudne, jeżeli nawet nie niemożliwe. Kluczowe jest jego ujawnienie, co jest zbieżne także z ujawnieniem skutków szkodowych. Dodatkowo, w przypadku ubezpieczenia przerwy w działalności, będziemy mieli do czynienia z pojęciem okresu odszkodowawczego, który oznacza okres zajścia (lub ujawnienia) zdarzenia skutkującego przerwaniem działalności ubezpieczającego, a który musi rozpocząć się w okresie ubezpieczenia – wówczas bowiem musi mieć miejsce wypadek ubezpieczeniowy, w zależności od jego definicji. Okres odszkodowawczy zwykle jest ograniczony czasowo, np. do 180 dni, o ile przerwa w działalności nie skończy się wcześniej.

Niewątpliwie istotną częścią oceny zakresu ochrony jest zakres wyłączeń proponowany przez ubezpieczycieli. Jako że ubezpieczenie to nie ma charakteru *all risk*, ograniczenie zakresu ochrony powinno być analizowane przez pryzmat co najmniej dwóch rodzajów postanowień. Są to nie tylko postanowienia opatrzone tytułem „wyłączenia", lecz także specyfika konstrukcji definicji zdarzeń objętych ubezpieczeniem, np. ograniczenie pojęcia szkody lub zakresu świadczenia odszkodowawczego. Ryzyka podlegające wyłączeniu spod ochrony ubezpieczeniowej można pogrupować według kilku kategorii. Jak się wydaje, stanowią one powtarzalną praktykę rynkową.

Ryzykiem nieubezpieczalnym w każdych warunkach jest działanie umyślne lub rażące niedbalstwo ubezpieczonego, które podlega wyłączeniu także na podstawie przepisów prawa (art. 827 k.c.). Wyłączenie to dotyczy zarówno ubezpieczającego (a więc także osób działających w imieniu ubezpieczającego, który jest osobą prawną), jak i ubezpieczonego w myśl art. 827 § 4 k.c. Dotyczy to zatem także takich zdarzeń, które z natury rzeczy mogą zaistnieć tylko na skutek umyślnego działania, a więc naruszenia własności intelektualnej osób trzecich, takich jak: plagiat, naruszenie tajemnicy handlowej, patentów, znaków towarowych, nazw handlowych, praw autorskich, licencji bądź jakiejkolwiek innej formy praw własności intelektualnej, ponadto celowego gromadzenia danych lub dystrybucji informacji o charakterze spamu.

Wyłączenia dotyczące sankcjonowania określonego zachowania ubezpieczonego należą do najbardziej problematycznych. Wynika to chociażby z różnic pomiędzy przepisami prawa systemów kontynentalnych (lub tzw. kultury alpejskiej w ubezpieczeniach) a systemem anglosaskim, spośród których ten ostatni pozwala na stosowanie tzw. *warranties* lub *conditions precedents* w postaci określonego zachowania ubezpieczonego i sankcjonowanie każdej postaci

i przyczyny niedochowania powinności poprzez możliwość odmowy wypłaty świadczenia, pierwszy typ zaś ogranicza taką możliwość. Polski system prezentuje niewątpliwie podejście kontynentalne, czego konsekwencją jest przeważające stanowisko orzecznictwa i doktryny co do możliwości ograniczenia prawa do świadczenia tylko w sytuacji, gdy naruszenie powinności miało miejsce z winy umyślnej lub rażącego niedbalstwa[25]. Klauzule tego typu nie powinny więc być konstruowane w sposób sugerujący ograniczenie ubezpieczalności zdarzeń wynikłych z winy zwykłej ubezpieczonego, takich jak np. brak staranności w monitorowaniu systemu zabezpieczeń[26].

Do kolejnej kategorii wyłączeń można zaliczyć ryzyko szkody w samym oprogramowaniu lub innych aktywach IT, przez które nastąpił atak, polegającej na ich utracie, zniszczeniu lub utracie wartości handlowej. Spowodowane jest to bardzo trudnym szacowaniem takich strat. Ryzykiem nieubezpieczalnym w ramach ubezpieczenia cyber ryzyk jest też ryzyko szkód osobowych, choć jak wynika z doświadczeń międzynarodowych, istnieje możliwość indywidualnego negocjowania zakresu takiego wyłączenia, w szczególności gdy mowa o odpowiedzialności cywilnej wobec poszkodowanej osoby trzeciej. Brak objęcia zakresem ubezpieczenia cyber ryzyk odpowiedzialności za szkody osobowe może wymagać uzupełnienia ochrony w tym zakresie na podstawie ubezpieczenia odpowiedzialności cywilnej ogólnej.

Innym popularnym wyłączeniem jest awaria urządzeń mechanicznych lub elektronicznych. Polega ono na wyłączeniu spod ochrony zdarzeń polegających na mechanicznym wyłączeniu urządzeń, odłączeniu zasilania itp.[27], jednak powinno dotyczyć tylko zdarzeń niemających charakteru cyber ataku (za pomocą wirusa, spamu itp.). Szczególnej uwadze należy poddać wyłączenia dotyczące ryzyk wojennych i terrorystycznych (wyłączenie takie dotyczy wojny, inwazji oraz powstania) w powiązaniu z ich szeroką definicją. Nie można bowiem zaprzeczyć, że celowe ataki terrorystyczne niejednokrotnie będą miały charakter terroryzmu[28]. Kolejnym rodzajem częstego wyłączenia o charakterze przedmiotowym jest brak ochrony urządzeń przenośnych, takich jak laptopy. W niektórych umowach ubezpieczenia zniesienie tego wyłączenia jest możliwe na indy-

[25] Np. K. Malinowska, „Konsekwencje niedochowania powinności ubezpieczeniowych w świetle art. 827 k.c." Prawo Asekuracyjne 2013, nr 3, s. 28–41; J. Woronkiewicz, „Granice swobody kształtowania obowiązków prewencyjnych w umowie ubezpieczenia w świetle art. 826 i 827 k.c.", Prawo Asekuracyjne 2016, nr 1.

[26] Armerding T., „Cyber insurance: Worth it, but beware of the exclusions", https://www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber-insurance-worth-it-but-beware-of-the-exclusions.html.

[27] Zob. https://securenow.in/insuropedia/what-are-common-exclusions-cyber-risk-insurance.

[28] Terroryzm definiowany przez rynek londyński obejmuje: „Act(s), including but not limited to the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organisation(s) committed for political, religious, ideological or similar purposes including the intention to influence any government and/or to put the public, or any section of the public, in fear", http://www.cyberriskinsuranceforum.com/content/cyber-insurance-and-terrorism-exclusion (dostęp: 27.12.2017 r.).

widualnych warunkach, np. pod warunkiem szyfrowania danych znajdujących się w takich urządzeniach[29].

Klasycznym wyłączeniem jest ograniczenie ochrony z tytułu odpowiedzialności cywilnej do tej regulowanej przepisami prawa, a więc w zakresie wykraczającym poza podstawowy zakres odpowiedzialności za niewykonanie lub nienależyte wykonanie zobowiązań w obszarze nierozszerzonym na podstawie art. 473 k.c. Ponadto, w obrębie odpowiedzialności cywilnej, wyłączeniu mogą podlegać roszczenia pomiędzy ubezpieczonymi[30], co powoduje konieczność odrębnej ochrony, np. typu D&O w przypadku, gdy ubezpieczenie od cyber ryzyk obejmuje jako ubezpieczonych zarówno spółkę, jak i jej członków zarządu.

Oprócz wyłączeń charakterystycznych dla cyber ryzyka, umowy ubezpieczenia zawierają też standardowy zakres wyłączeń dotyczący różnych rodzajów ubezpieczeń, a to właśnie z uwagi na stwierdzone wcześniej łączenie różnych typów ryzyk w jednej umowie ubezpieczenia (produkcie ubezpieczeniowym). Do takich wyłączeń należą ryzyka wojenne i terrorystyczne (choć z zastrzeżeniem ewentualnej możliwości objęcia ochroną cyber terroryzmu), ryzyka zanieczyszczenia środowiska, ryzyka naturalnego zużycia systemów informatycznych, korzystania z eksperymentalnych i niezatwierdzonych do obrotu produktów infrastruktury informatycznej, a także szereg ryzyk finansowych związanych z obrotem papierami wartościowymi (w szczególności na terytorium USA).

4. Otoczenie prawne w zakresie dystrybucji ubezpieczeń i ochrony danych osobowych i jego wpływ na konstrukcję ubezpieczenia cyber ryzyk

Omawiając przedmiot i zakres ubezpieczenia od cyber ryzyk nie można pominąć zmian legislacyjnych, które wchodzą w życie w 2018 r., w tym przede wszystkim ustawy o dystrybucji ubezpieczeń[31], jak i rozporządzenia RODO.

Wejście w życie rozporządzenia RODO przyczyni się do wzrostu popularności ubezpieczenia od cyber ryzyk, a to za sprawą potencjalnie wysokich sankcji ekonomicznych grożących przedsiębiorcy/ubezpieczającemu. Ryzyko poniesienia straty o charakterze finansowym w postaci zapłacenia kary administracyjnej, które na podstawie umowy ubezpieczenia ubezpieczający chciałby przenieść (choć w części) na ubezpieczyciela, trudno jednak uznać za wpływ na naturę prawną tego ubezpieczenia. Nie zmienia to też charakteru ryzyka obejmowanego przedmiotem ubezpieczenia cyber, a stanowić może raczej głównie tzw. hazard moralny w zawieraniu umów ubezpieczenia w tym przedmiocie. Jednocześnie zaś, biorąc pod uwagę możliwość różnego rodzaju odpowiedzial-

[29] B. Moorcraft, Tricky exclusions in cyber policies could hinder claim process, https://www.insurancebusinessmag.com/ca/news/cyber/tricky-exclusions-in-cyber-policies--could-hinder-claim-process-73995.aspx.

[30] Association of British Insurers, *Making Sense of Cyber Insurance: A Guide for SMEs*, https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2016/cyber-insurance/making-sense-of-cyber-insurance-a-guide-for-smes.pdf.

[31] Ustawa z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń (Dz. U. z 2017 r. poz. 2486, z późn. zm.).

ności, nie tylko administracyjnej, lecz także cywilnej i karnej, wydaje się oczywiste, że wzrasta tym samym ryzyko odpowiedzialności nie tylko samego podmiotu/przedsiębiorcy, lecz także jego organu zarządzającego i osób na stanowiskach kierowniczych. Kompleksowe podejście do ryzyka cyber może więc oznaczać, że jego zakresem (np. w ramach dodatkowej opcji) zostanie też objęta odpowiedzialność członków zarządu, będąca dotychczas domeną wyodrębnionego typu ubezpieczenia, zwanego popularnie ubezpieczeniem D&O.

Należy także postawić pytanie o wpływ przepisów ustawy o dystrybucji ubezpieczeń na ubezpieczenia cyber ryzyk. O ile ustawa ta nie ingeruje w sam przedmiot i zakres ubezpieczenia, to niewątpliwie będzie miała wpływ na sposób jego oferowania. Warto zwrócić uwagę na nowe przepisy mające zastosowanie do wszystkich rodzajów dystrybutorów (pośredników i ubezpieczycieli), a więc w szczególności art. 7, który wprowadza z pozoru ogólną, lecz w istocie fundamentalną zasadę, kierowania się najlepiej pojętym interesem klienta. Przez ten pryzmat powinno odbywać się oferowanie klientom cyber ubezpieczenia. Kluczową rolę może także odgrywać art. 8, wprowadzający obowiązek analizy potrzeb klienta i zakaz zawierania umowy ubezpieczenia nieodpowiadającej takim potrzebom. To spowoduje, że każdy pośrednik i ubezpieczyciel pragnący zaangażować się w dystrybucję tego ubezpieczenia będzie musiał posiadać wiedzę odpowiednią do przeprowadzenia takiej analizy potrzeb. Obowiązek ten z natury rzeczy jest rozwinięty wobec brokerów w przepisach art. 32, poprzez konieczność opracowania rekomendacji na podstawie analizy odpowiedniej liczby produktów danego rodzaju. Obowiązki powyższe są jedynie nieznacznie rozluźnione w sytuacji, gdy umowa ubezpieczenia obejmuje ryzyka duże. Biorąc pod uwagę grupy ubezpieczeń, do których przynależy ubezpieczenie cyber ryzyk, nie jest ono immanentnie ryzykiem dużym, a jego kwalifikacja jako takie może być oparta jedynie na statusie ubezpieczającego, jego przynależności do grona klientów profesjonalnych lub spełniających parametry zatrudnienia, sumy bilansowej i obrotów[32]. Biorąc pod uwagę zawarcie kilku rodzajów ubezpieczeń w jednej umowie ubezpieczenia, kryteria te powinny być stosowane jednolicie w sposób jak najbardziej korzystny dla ubezpieczonego (zgodnie z dyrektywą art. 7 ustawy o dystrybucji ubezpieczeń).

5. Wnioski

Rozważania zawarte w niniejszym artykule można zakończyć wnioskami na kilku płaszczyznach. Po pierwsze, wydaje się, że ubezpieczenie cyber ryzyk, pomimo swej złożonej natury, łączącej ryzyka charakterystyczne dla różnych ty-

[32] Art. 3 ust. 1 pkt 6 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (tekst jedn. Dz. U. z 2017 r. poz. 1170, z późn. zm.), definiuje duże ryzyka jako ryzyka, o których mowa w dziale II załącznika do ustawy: a) w grupach 4–7, 11 i 12, b) w grupach 14 i 15 – w przypadku gdy ubezpieczający wykonuje działalność gospodarczą lub wolny zawód, a ryzyko wiąże się z tą działalnością, c) w grupach 3, 8, 9, 10, 13 i 16 – w przypadku gdy ubezpieczający przekracza co najmniej dwa z następujących progów w roku obrotowym: sumę aktywów bilansu w wysokości równowartości w złotych 6,2 mln euro, łączne przychody netto ze sprzedaży towarów i usług oraz operacji finansowych w wysokości równowartości w złotych 12,8 mln euro, średnioroczne zatrudnienie w przeliczeniu na pełne etaty w liczbie 250 osób.

pów ubezpieczeń, jest oferowane w ramach jednej umowy ubezpieczenia. To powoduje, że można próbować już teraz kwalifikować je jako jeden określony typ umowy ubezpieczenia, w którym decydującą, łączącą rolę odgrywa źródło ryzyka, a nie rodzaj szkód. W konsekwencji moglibyśmy mówić o produkcie ubezpieczeniowym w znaczeniu prawnym, uregulowanym w art. 11 ustawy o dystrybucji ubezpieczeń, podlegającym jako taki także regulacji rozporządzenia delegowanego dotyczącego zarządzania produktem ubezpieczeniowym. Praktyka i doktryna w tym zakresie dopiero się tworzą. Cyber ubezpieczenia czeka więc, oprócz zmagań z rynkiem, także poligon doświadczalny nowych, wymagających regulacji prawnych.

Na jego rozwój zdecydowanie ma wpływ przyjęcie rozporządzenia RODO, choć stanowić ono będzie jedynie przyczynek i niewielki wycinek całego *spectrum* ryzyk związanych z cyber przestrzenią, daleko wykraczających poza ochronę danych osobowych. W tym względzie regulacje w zakresie ochrony danych osobowych niewątpliwie spełnią funkcję edukacyjną w zakresie ogólnego obrazu cyber ryzyka.

Wreszcie nie sposób po raz kolejny nie zauważyć, jak bardzo niedostosowane do zmieniającej się dynamicznie rzeczywistości pozostają przepisy kodeksu cywilnego o umowie ubezpieczenia. Widać to wyraźnie na gruncie ubezpieczenia cyber ryzyk. Znakomita część specyfiki przedmiotu ubezpieczenia cyber ryzyk w ogóle nie znajduje odzwierciedlenia w przepisach art. 805–829 k.c., choć z pewnością wypełnia *essentialia negotii* wskazane w art. 805 k.c. Po raz kolejny warto zatem podnieść postulat prac nad rozbudową przepisów, chociażby w kontekście praw i obowiązków ubezpieczonego oraz sankcji za ich niedopełnienie, czasu trwania ochrony (*triggerów*) nie tylko w ubezpieczeniu OC, oraz powiązanych z tym okresów przedawnienia roszczeń z ubezpieczenia.

dr Katarzyna Malinowska
radca prawny

Bibliografia

Anderson R., Moore T., „The Economics of Information Security: A survery and open questions", https://www.cl.cam.ac.uk/ ~rja14/ Papers/ toulouse-summary.pdf

Armerding T., „Cyber insurance: Worth it, but beware of the exclusions", https://www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber--insurance-worth-it-but-beware-of-the-exclusions.html

Burden K., Barlow Lyde&Gilbert, „E-RISK AND INSURANCE", Computer Law & Security Report 2000/16(4).

Grabowska T., „Cyber przestępczość w świecie finansów – ryzyka cybernetyczne", Rozprawy Ubezpieczeniowe 18 (1/2015).

The Geneva Association, „Ten key questions on cyber risk and cyber risk insurance", November 2016, https://www.genevaassociation.org/sites/default/files/research--topics-document-type/pdf_public//cyber-risk-10_key_questions.pdf

Insurance 2020 and beyond: Reaping the dividends of cyber resilience, https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends--cyber-resilience.pdf.

Krajewski M., „Ubezpieczenie odpowiedzialności cywilnej według kodeksu cywilnego", Warszawa 2011.
Malinowska K., „Pojęcie zarządzania produktem ubezpieczeniowym w świetle dyrektywy o dystrybucji ubezpieczeń i przepisów implementacyjnych", Wiadomości Ubezpieczeniowe, 2017, nr 1.
Malinowska K., „Konsekwencje niedochowania powinności ubezpieczeniowych w świetle art. 827 k.c.", Prawo Asekuracyjne 2013, nr 3.
Molęda M., „Jak zrobić ISMS", Miesięcznik Ubezpieczeniowy, 2017, nr 6.
Molęda M., „Cyber is the new black", wyd. specjalnie, Miesięcznik Ubezpieczeniowy 2018.
Molęda M., „Cyber defense matrix", Miesięcznik Ubezpieczeniowy, 2018, nr 1.
Moorcraft B., „Tricky exclusions in cyber policies could hinder claim process", https://www.insurancebusinessmag.com/ca/news/cyber/tricky-exclusions-in--cyber-policies-could-hinder-claim-process-73995.aspx
OECD, enhancing the role of insurance in cyber risk management, Paris 2017.
Serwach M., „Komentarz do art. 822 k.c., w: M. Serwach (red.), M. Glicz (red.), „Komentarz do niektórych przepisów ustawy – Kodeks cywilny", w: „Prawo ubezpieczeń gospodarczych". Tom II. Komentarz, wyd. II, LEX 2010.
Skomra W., „Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego", Rządowe Centrum Bezpieczeństwa, http://www.archiwalna.powiat-wloszczowa.pl/ochrona_ludnosci/OIK_w_systemie_zarzadzania_kryzysowego.pdf
Skomra W., w: „Zarządzanie ryzykiem. Przegląd wybranych metodyk", praca zbiorowa, D. Wróblewski (red.), Warszawa 2015.
UK Cybersecurity: the role of insurance in managing and mitigating the risk, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf
Vaughan E., Vaughan T., „Fundamentals of Risk and Insurance", 2008, John Wiley & Sons, Inc.
Woronkiewicz J.,"Granice swobody kształtowania obowiązków prewencyjnych w umowie ubezpieczenia w świetle art. 826 i 827 k.c.", Prawo Asekuracyjne 2016, nr 1.
Vos M., „Handling of cyber risks claims. Presentation", June 2015, Lloyd's
Association of British Insurers, *Making Sense of Cyber Insurance: A Guide for SMEs*, https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2016/cyber-insurance/making-sense-of-cyber-insurance-a-guide-for-smes.pdf.

Legal Aspects of Cyber Risk Insurance

This article analyses the legal nature of cyber risk insurance from civil and insurance law perspectives, which enables to qualify it as a particular type of insurance. It also examines an interaction of cyber risks with the legal environment in the insurance industry and cyber security. This is particularly important due to the fact that these areas are undergoing dynamic legislative changes in 2018. Cyber risk insurance is worth investigating not only from the point of view of risk management or technical risk assessment, but also from a legal perspective. On this basis, it will be possible to determine what type of insurance is being dealt with and which regulations may be applied.

Keywords: cyber risk, cyber insurance, insurance contract, data protection, cyber security.