MIRJANA GLINTIĆ

SAJBER OSIGURANJE KAO NOVA VRSTA OSIGURANJA – POSTOJI LI POTREBA ZA NOVOM KLASIFIKACIJOM OSIGURANJA –

Sve veći broj sajber napada učinio je proizvod sajber osiguranja vrlo popularnim, jer se radi o proizvodu koji osiguraniku može da ponudi ponovno uspostavljanje i održavanje stabilnosti poslovanja nakon napada. Obaveze i osiguravača i osiguranika kod ovog osiguranja su nešto drugačije koncipirane nego što je to slučaj sa drugim vrstama imovinskih osiguranja, u koja se ovo osiguranje nesumnjivo ubraja. Posledično su se javili stavovi da se na ovo osiguranje ne mogu primeniti propisi iz oblasti ugovornog prava osiguranja, jer predstavljaju posebnu vrstu osiguranja. Stoga autorka centralni deo rada posvećuje analizi određenih obaveza ugovornih strana sa ciljem da ispita ispravnost navedenog stava. Pozitivnopravna i uporednopravna analiza signalizirale su da je pristup i srpskog zakonodavca, ali i nekih stranih zakonodavaca, takav da dozvoljava poimanje ovog osiguranja kao imovinskog osiguranja i da posledično nije potrebno zasebno regulisati ugovor o sajber osiguranje. Zaključni deo rada posvećen je argumentima za nastavak regulisanja ovog osiguranje isključivo putem opštih uslova osiguranja.

Ključne reči: *sajber osiguranje, prijava okolnosti, povećanje rizika, imovinska osiguranja, opšti uslovi osiguranja*

Dr Mirjana Glintić, naučni saradnik Instituta za uporedno pravo u Beogradu, e-mail: *m.glintic@iup.rs*. Rad je nastao kao rezultat naučnoistraživačkog rada Instituta za uporedno pravo koji finansira Ministarstvo nauke, tehnološkog razvoja i inovacija Republike Srbije prema Ugovoru o realizaciji i finansiranju naučnoistraživačkog rada NIO u 2023. godini (evidencioni broj: 451-03-47/2023-01/200049 od 3. 2. 2023).

UVOD

Istovremeno sa rastom sajber kriminala, raste i ulaganje u IT bezbednost, za koje se procenjuje da će u 2025. godini biti u vrednosti oko 400 milijardi dolara. Kompleksni međusobni odnosi modernih informacionih sistema rezultiraju u velikoj izloženosti sajber rizicima, iako pojedinačne kompanije investiraju u mere preventivne zaštite od sajber rizika. Deo ulaganja u povećanje bezbednosti odlazi i na premije za sajber osiguranje.[1] U poslednjih nekoliko godina, a naročito posle svakog sajber napada, sve veći broj privrednih društava se okreću sajber osiguranju kako bi zaštitili svoje poslovanje od brojnih negativnih ekonomskih posledica[2] koje bi sajber napad doneo sa sobom.[3] Svaki prijavljeni incident povrede podataka ili neuspeh u funkcionisanju informacionih sistema koji su rezultirali finansijskim gubitkom ili gubitkom reputacije podiže stepen svesti o tome koliko je neophodno posedovanje sajber osiguranja.[4] Kada su se počeli događati sajber napadi, osiguranici koji su imali zaključene ugovore o osiguranju od odgovornosti i osiguranju imovine, ostajali su zatečeni kada su shvatali da štete nastale usled sajber napada nisu bile pokrivene njihovim polisama. Tada je postalo jasno da je potreban novi proizvod osiguranja koji će pružiti zaštitu osiguranicima, odnosno njihovim privrednim društvima.[5] Razvoj ovog osiguranja sa sobom je doneo širenje palete obaveza i osiguravača i osiguranika usled stalnih tehnoloških promena. Počelo se stoga postavljati pitanje da li ipak određene karakteristike ovog osiguranja onemogućavaju jedinstvenu primenu zakonskih

---

[1] Prema nekim procenama, sadašnja vrednost globalnog tržišta sajber osiguranja je više od sedam milijardi dolara, a do 2025. će dostići vrednost veću od 20 milijardi. Severna Amerika je i dalje najjače tržište sa vrednošću od 5,3 milijarde dolara, a snažan rast se predviđa i u Aziji, kao i u Evropi gde je vrednost ovog tržišta sada oko milijardu dolara. V. *https://www.marketsandmarkets.com/Market-Reports/cyber-insurance-market-47709373.html?gclid=CjwKCAjwseSoBhBXEiwA9iZtxlNah6zF2zKy5IyCZtKtsx2Mnw4duAwasSoTvtSkLJ53k403TQXEwRoCbtYQAvD_BwE*, 23. 9. 2023.

[2] Samo tokom 2021. godine na nemačkom tržištu je šteta od sajber napadala iznosila preko 200 milijardi evra, podatak preuzet od Bitkom, *Angriffsziel deutsche Wirtschaft: mehr als 220 Mrd. € Schaden pro Jahr*, *https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr*, 29. 9. 2023.

[3] Od 2016. godine značajno je porastao broj uplaćenih premija za sajber osiguranje. Nicolai Wojciechowski, „Aufsätze Cyberversicherung: Vorvertragliche Anzeigepflicht und Gefahrerhöhung", *Versicherungsrecht,* 2022, 341.

[4] U prilog tome govori i činjenica da su najzainteresovaniji za zaključenje ugovora o osiguranju oni koji su preživeli sajber napad. *Willis Fortune 500 Cyber Disclosure Study*, 2013, *https://cyberforsikring.willisweb.dk/dyn/Normal1/5/215/Default_Model_Normal1_Sidebar/file/317/1401708954/willis-cyber-disclosure-2013.pdf*, 23. 9. 2023.

[5] Tom Baker, Anja Shortland, „Insurance and enterprise: cyber insurance for ransomware", *The Geneva Papers on Risk and Insurance – Issues and Practice*, Vol. 48, 2023, 280.

propisa iz oblasti ugovornog prava osiguranja, ali i statusnog prava osiguranja jer, kako ističu, ovo osiguranje se ne može razvrstati prema postojećim kriterijumima klasifikovanja osiguranja. Neki od glasova odlaze tako daleko da se čak razmišlja o koncipiranju ovog osiguranja kao zasebne grane osiguranja, naročito u kontekstu nadzora nad poslovanjem osiguravajućeg društva.[6] Prilikom apostrofiranja navedenih stavova, polazi se prvenstveno od posebnosti obaveza osiguravača i osiguranika, koje se u određenoj meri razlikuju od uobičajenih obaveza ugovornih strana kod ugovora o osiguranju.[7] Ispravnije bi ipak bilo reći da nisu ugovorne obaveze te koje su *per se* drugačije, već da je priroda sajber rizika, o kome nedostaju empirijski podaci i koji je vrlo promenljiv, takav da zahteva malo drugačije tumačenje obaveza ugovornih strana. Ponekad promene sajber rizika nastupaju vrlo iznenada i drastično usled tehničkog progresa i upotrebe novih uređaja, pa postoji strepnja i od velikih promena propisa primenjivih na osiguranje takvih gubitaka, jer to može imati značajne implikacije na izmene strategija poslovanja i upravljanja rizicima osiguranika.

Upravo da bi „izašli na kraj" sa navedenim izazovima koje sajber osiguranje donosi na tržište osiguranja, osiguravači su koncipirali proizvod osiguranja koji zahteva dodatno angažovanje i jedne i druge ugovorne strane, svake u svom domenu. Stava smo da navedene dopune ovog proizvoda ne predstavljaju dovoljan osnov da se o ovom osiguranju govori kao posebnoj vrsti osiguranja, koje se ni na koji način ne uklapa u postojeće zakonske odredbe. Kao što će sledeći redovi pokazati, to se naročito odnosi na ugovorno pravo osiguranje, čije postojeće odredbe se i dalje mogu primenjivati na sajber osiguranje.

OBAVEZE OSIGURAVAČA KOD SAJBER OSIGURANJA

Kao osnovni sajber rizici prepoznaju se krađa identiteta, otkrivanje poverljivih podataka i prekid poslovanja,[8] u skladu sa čim se i dalje definišu osnovno

---

[6] Ovaj stav je iznela nemačka Savezna uprava za nadzor finansijskih usluga, BaFin, *BaFin Journal*, No. 9, 2021, 6, *https://www.bafin.de/SharedDocs/Downloads/DE/BaFin-Journal/2021/bj_2109.pdf?__blob=publicationFile&v=3*.

[7] *Ibidem*.

[8] Potrebno je naglasiti da postoje različite definicije sajber rizika i da su ove samo najuobičajenije. Tako se pod sajber rizikom može razumeti ona vrsta rizika proistekla iz upotrebe zlonamernog softvera, koji dovode do prekida poslovanja i finansijskih gubitaka. Druge pak definicije ovaj rizik povezuju sa rizikom po informacionu sigurnost ili kao rizik koji rezultira uništenjem informacionih sistema, što predstavlja širi koncept sajber rizika. U skladu sa regulativom Bazel II i Solventnost II, sajber rizici se mogu posmatrati kao rizici proistekli iz postupaka ljudi, rizici usled sistemskih i tehnoloških kvarova, neuspelih unutrašnjih procesa i spoljnih događaja. V. Christian Biener, Martin Eling, Jan Hendrik Wirfs, „Insurability of Cyber Risk: An Empirical Analysis",

i dodatno pokriće kod ovog osiguranja. Osnovno pokriće kod sajber osiguranja obuhvata kako stručne usluge u vidu tehničke pomoći kada dođe do sajber incidenta, obnove softvera i podataka, usluge eksperta, tako i finansijske u vidu povraćaja oduzetih novčanih sredstava, naknade odštetnih zahteva trećih lica, ali i zahteva proisteklih iz odgovornosti osiguranika za kršenje poverljivosti i privatnosti i mrežnu bezbednost.[9]

Rizici koji mogu biti dodatno ugovoreni, uz osnovni paket, jesu: prekid rada osiguranika, čime je pokrivena smanjena neto dobit odnosno uvećani troškovi poslovanja koji su posledica sajber incidenta; odgovornost za odštetne zahteve trećih lica koje osiguranik nije u mogućnosti da ispuni; sajber ucena; naknada materijalne štete na oštećenoj ili uništenoj opremi (hardver) i obnova softvera.[10]

Kada se pogleda gore predstavljeni katalog usluga osiguravača, dolazi se do prve karakteristike sajber osiguranje, usled koje se ovo osiguranje razlikuje u odnosu na ostala osiguranja. Radi se o obavezi osiguravača da osiguraniku pruži stručne savete kada dođe do gubitka usled sajber napada, ali i da osiguraniku daje savete preventivno, kako bi se sprečili gubici.[11] Isplaćivanje šteta za osiguranje naime čisto je reaktivna aktivnost, koja predstavlja značajno finansijsko opterećenje za osiguravača, posebno kada se radi o sajber osiguranju. Zato osiguravači po osnove polise sajber osiguranja imaju proaktivni pristup sajber bezbednosti, aktivno pomažući klijentima da preuzmu bolji pristup sajber bezbednosti. Međutim, osiguranici uglavnom ne koriste te usluge preventivnog delovanja,[12] jer znaju da su zaključili ugovor o osiguranju koji će im obezbediti finansijsku pomoć u slučaju da dođe do ostvarenja osiguranog slučaja, *ransomware, phishing, fund transfer fraud attacks*. Jedino kada postoje izgledi da osiguranik postupi po savetima

---

The Geneva Papers on Risk and Insurance. Issues and Practice, No. 1, Vol. 40, 2015, 133; Hulisi Oğüt, Srinivasan Raghunathan, Nirup Menon, „Cyber security risk management: Public policy implications correlated risk, imperfect ability to prove loss, and observability of self-protection", *Risk Analysis*, No. 3, Vol. 31, 2011, 497–512.

[9] Preuzeto sa sajta *https://www.generali.rs/pravna_lica/imovina/sajber_osiguranje.3546.html*, 26. 9. 2023.

[10] U nekim zemljama osiguravač preuzima na sebe i plaćanje otkupnine u slučaju *ransomware*, što se percipira kao loše rešenje jer se na taj način daje podsticaj za sve veći broj ovih ovakvih napada, kao i za nepreduzimanje sigurnosnih mera od strane osiguranika. V. *https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-supporting-fight-against-ransomware.html*, 13. 9. 2023.

[11] Tom Baker, Sean Grifth, *Ensuring corporate misconduct: How liability insurance undermines shareholder litigation*, University of Chicago Press, Chicago, 2010, 58.

[12] Brayan Cunningham, Shauhin A. Talesh, „Uncle Sam RE: Improving cyber hygiene and increasing confdence in the cyber insurance ecosystem via government backstopping", *University of Connecticut Insurance Law Journal*, No. 1, Vol. 28, 2021, 1–84.

osiguravača jeste onda kad bi im u izgleda stavljena niža premija kao „nagrada" za preventivno delovanje u domenu sajber bezbednosti.[13]

Potom, kada dođe do osiguranog slučaja, osiguravač pruža osiguraniku i tehničku podršku kako bi se oporavio od sajber napada, uz pružanje finansijske podrške u vidu naknade ugovorenih troškova, koji su nastali usled narušavanja bezbednosti, uključujući povrat podataka, sistemsku forenziku, kao i troškove pravne odbrane. Dakle, osiguravač se upušta u određene troškove, bez da prejudicira ishod postupka kojim će osiguranik zahtevati isplatu sume osiguranja, što znači da će se tek forenzičkim ispitivanjem ustanoviti da li će i koliko će biti obaveza osiguravača. Navedeni aspekt obaveze osiguravača može biti izazovan iz vizure nadzora nad poslovanjem osiguravajućeg društva, jer određene finansijske obaveze osiguravača mogu nastupiti i pre trenutka kada je ustanovljeno da li postoji njegova obaveza prema osiguraniku i koliko ta njegova obaveza iznosi. Dodatni problem predstavlja što ovako koncipirano sajber osiguranje takođe sadrži elemente i osiguranja od odgovornosti i osiguranja poverenja,[14] što delimično vodi i pitanju da li se na jedinstven način mogu primenjivati odredbe i ugovornog prava osiguranja. Navedeno pitanje će naročito doći do izražaja u onim pravnim sistemima kod kojih propisi iz ugovornog prava osiguranja zakonski regulišu pojedinačne vrste osiguranja.[15] Iako više puta iz različitih razloga osporavana podela u našem ZOO, u ovom slučaju se ispostavila kao dobro rešenje jer se kreće od načelne, opšte podele na osiguranja lica i osiguranja imovine, spram koje se može izvršiti klasifikacija većine postojećih i budućih vrsta osiguranja. Naročito kada se uzme u obzir da zakon posvećen statusnom pravu osiguranja, Zakon o osiguranju,[16] polazi od potpuno druge podele osiguranja kao pravnorelevantne.[17]

OBAVEZE OSIGURANIKA KOD SAJBER OSIGURANJA

Pored specifičnosti pokrića koje nudi sajber osiguranje u pogledu prilično širokog kruga prestacija koje je osiguravač u obavezi da ponudi, sledeća specifičnost ovog osiguranja ogleda se u tome da se svaki osiguranik, svako privredno društvo,

---

[13] Kenneth Abraham, Daniel Schwarcz, „The limits of regulation by insurance", *Indiana Law Review*, No. 1, Vol. 98, 2022, 224.

[14] Mirjana Glintić, „Osiguranje poverenja kao instrument zaštite imovine privrednih društava", *Pravo i privreda*, br. 7–9, 2019, 539–552.

[15] Mirjana Glintić, „Pravna priroda prava na isplatu osigurane sume kod osiguranja lica", doktorska disertacija odbranjena na Pravnom fakultetu Univerziteta u Beogradu, Beograd, 2019, 100–106.

[16] Zakon o osiguranju, *Službeni glasnik RS*, br. 139/14, 44/21.

[17] *Ibidem*, 32–37.

suočava sa rizicima koji su specifični za njih, što zahteva individualan pristup prilikom sastavljanja polisa osiguranja. Veličina kompanije, broj korisnika njihovih usluga, obim upotrebe interneta u poslovanju, kao i vrsta podataka koji koriste i čuvaju predstavljaju važne odrednice vrste polise sajber osiguranja i visine premije. Sajber rizici koji pogađaju različita privredna društva nisu međusobno povezani,[18] što govori u prilog tome da se slučajnost ostvarivanja rizika mora posmatrati u vezi sa jednim konkretnim slučajem.[19] Stoga određivanje visine premija sajber osiguranja ne predstavlja jednostavan zadatak, što je dodatno otežano činjenicom da portfelji sajber rizika nisu dovoljno veliki i da rizik nije optimalno diversifikovan unutar riziko grupe, sa jedne strane. Sa druge strane, specifičnost osiguranog rizika postavlja pred osiguravače i zadatak da ustanove da li je osiguranik prilagodio svoje poslovanje potencijalnom riziku preduzimajući potrebne mere i da li njegovi IT sistemi ispunjavaju određene minimalne tehničke uslove.

Iz tog razloga je faza procene rizika kod ovog osiguranja ključni element odluke osiguravača da li da zaključi ugovor o osiguranju. Međutim, usled informacione asimetrije i stalnog menjanja sajber rizika usled tehničkog progresa,[20] osiguravači ne poseduju dovoljno informacija u odnosu na pojedinačne firme, što za posledicu može imati izuzetno visoke premija osiguranja i visoke franšize. Posledično se kod sajber osiguranja naročito bitnom pokazala predugovorna obaveza prijave okolnosti od strane osiguranika.[21] Ono što je posebno interesantno i što je dodatno apostrofiralo pitanje posebnosti ove vrste osiguranja jeste strogo

---

[18] Upor. Jean Bolot, Marc Lelarge, „Cyber insurance as an incentive for internet security", *Managing Information Risk and the Economics of Security* (ed. Eric Johnson), Springer, New York, 2009, 269–290; Annette Hofmann, Hidajet Ramaj, „Interdependent risk networks: The threat of cyber-attack", *International Journal of Management and Decision Making*, No. 5/6, Vol. 11, 2011, 312–323.

[19] C. Biener, M. Eling, J. H. Wirfs, op. cit., 141.

[20] Andreas Haas, Annette Hofmann, „Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit", *FZID Discussion Paper*, No. 74, 2013, *http://opus.uni-hohenheim.de/volltexte/2013/853/pdf/fzid_dp_2013_74_Schiller.pdf*, 14. 9. 2023.

[21] Jedna mogućnost za eliminisanje ovog nedostatka jeste skupljanje empirijskih podataka o slučajevima kada je došlo do ostvarenja sajber rizika, kao i podataka o podnetim zahtevima za naplatu pokrića iz osiguranja. Osiguravači bi čak mogli i da kombinuju izvore i da razmenjuju podatke, kao što se to radi sa operativnim rizicima u bankarskom sektoru ili bi čak mogla da se uspostavi zajednička platforma za razmenu podataka. Tu bi postojao izvesni prostor za uključivanje nacionalnih vlada jer bi one imale ovlašćenje da zahtevaju pristup informacijama u slučaju kada nezavisni osiguravači to pravo nemaju i pri čemu bi takvo postupanje vlade više bilo usklađeno sa javnim interesom. O konceptu javnog interesa v. Vladimir Đurić, „Upravnopravni aspekti konkursnog ostvarivanja javnog interesa u Republici Srbiji", *Aktuelna pitanja savremenog zakonodavstva i pravosuđa*, Beograd 2023, 459–461.

insistiranje na značaju informacija koje osiguranik pruža osiguravaču. Ipak, svestan značaja informacija koje su mu potrebne, osiguravač je taj koji sastavlja vrlo precizne upitnike u vezi sa rizikom na koje osiguranik ima da odgovori. Na taj način je u potpunosti ispoštovan savremeni trend prebacivanja obaveze na osiguravača da zahteva od osiguranika podatke koje su mu nužni o svom kompjuterskom sistemu, primenjenoj zaštiti, načinu prenosa i skladištenja podataka, ali i finansijske podatke, informacije o uticaju na redovno poslovanje, o broju i prirodi ličnih podataka trećih lica.[22] Ovaj trend je uočen u praksi osiguravača, čak i u pravnim sistemima kao što je naš, gde je ova obaveza drugačije zakonski koncipirana.[23] Uvid u uslove osiguranja osiguravača ukazuje da je formulisana i navedena obaveza osiguravača.

Nesposobnost osiguranika da poseduje sva stručna, tehnička i pravna znanja naročito dolazi do izražaja kod sajber osiguranja, što objašnjava zašto se toliko insistira na obavezi osiguravača da prikupi sve informacije relevantne za procenu rizika. Upravo insistiranje na nešto strožim zahtevima prema osiguravačima da postave precizna pitana u svom upitniku, i prema osiguraniku da da tačne odgovore na postavljena pitanja, dovelo je do pitanja da li je ovo osiguranje različitog ugovornopravnog režima.

Prijava okolnosti relevantnih za ocenu rizika

Predugovorna obaveza prijave okolnosti relevantnih za procenu rizika obavezuje osiguranika da osiguravaču prijavi okolnosti koje su mu poznate ili koje mu nisu mogle biti nepoznate, a koje su relevantne iz vizure osiguravača da odluči da li će želeti da sa konkretnim osiguranikom zaključi ugovor o osiguranju ili ne.[24]

---

[22] Čl. 2:101 Principi ugovornog prava osiguranja.

[23] Naime, čl. 907 Zakona o obligacionim odnosima – ZOO, *Službeni list SFRJ*, br. 29/78, 39/85, 45/89 – odluka USJ i 57/89, *Službeni list SRJ*, br. 31/93, *Službeni list SCG*, br. 1/03 – Ustavna povelja i *Službeni. glasnik RS*, br. 18/20 predviđa obavezu ugovarača osiguranja da osiguravaču prijavi sve okolnosti koje su relevantne za procenu rizika a koje su mu poznate ili koje mu nisu mogle biti nepoznate prilikom zaključenja ugovora. Dakle, osiguranik će imati pravo na pokriće iz ugovora o osiguranju samo ako je osigurani slučaj nastao iz uzroka koji ugovaraču nije bio poznat ili mu nije mogao biti poznat u trenutku zaključenja ugovora (tako i presuda Privrednog apelacionog suda, Pž. 658/2010(2) od 7. 4. 2010). U našem pravu osiguravač nema nikakvu obavezu da postavi pitanja osiguraniku. Na ovaj način je ostavljena velika diskreciona ocena osiguravaču i sudovima koji se uvek mogu pozvati na činjenicu da osiguranik nije prijavio okolnosti koje mu nisu mogle biti nepoznate u trenutku zaključenja ugovora. Nataša Petrović Tomić, *Zaštita potrošača usluga osiguranja: analiza i predlog unapređenja regulatornog okvira*, Pravni fakultet, Centar za izdavaštvo i informisanje, Beograd, 2015, fn. 920.

[24] Peter Reusch, „Die vorvetragliche Anzeigepflichten im neuen VVG 2008", V*ersicherungsrech*t, Heft 28, 2007, 1313.

Sa jedne strane, osiguranik je taj koji najbolje poznaje sopstvene okolnosti i zato je on odgovorno lice. Sa druge strane, osiguranik ne može jasno i precizno znati koje su to tačno okolnosti koje mora da prijavi, jer ih ima isuviše, a njemu nedostaje stručnog i pravničkog znanja da izabere relevantne. Zato, kao što je već istaknuto, osiguravač sastavlja upitnik u kome navodi koje su to za njega relevantne okolnosti, odnosno za procenu rizika.

Obim upitnika često korespondira veličini privrednog društva koje želi da se osigura. Tako se kraći upitnici primenjuju kod malih i srednjih privrednih društava. Kod velikih multinacionalnih privrednih društava upitnici su obimniji, a procena rizika često obuhvata i razgovore sa odgovarajućim stručnjacima.[25] Fokus upitnika se nalazi na sledećim riziko kategorijama: bezbednosti pristupa, zaštita od malvera, bezbednost podataka i bezbednosna ažuriranja. To znači da postavljanjem pitanja osiguravač nastoji da ustanovi kakva je početna situacija osiguranika u pogledu ispunjenosti određenih tehničkih uslova.

Preporuka osiguravačima je svakako da njihova pitanja budu što preciznija kako bi se izbeglo pozivanje na zabunu i pogrešnu ocenu. Istovremeno, sa zahtevom za preciziranjem pitanja o riziku ne sme se preterivati, posebno ako opšti uslovi osiguranja sadrže definicije. Moguće je zahtevati od osiguranika da pojmove i formulacije iz ugovora o sajber osiguranju shvata ne samo u datom kontekstu, već u sveukupnom kontekstu datog ugovora, u onoj meri u kojoj je njemu taj kontekst prepoznatljiv.[26]

Zahtev da pitanje mora takođe biti takvo da ga osiguranik razume ne sme biti postavljen isuviše nisko kod sajber osiguranja.[27] Kod sajber osiguranja ne radi se o prosečnom, „normalnom" osiguraniku potrošaču, već je reč o iskusnim i poslovno angažovanim poslovnim ljudima. Stoga bi se od osiguranika moglo zahtevati posedovanje određenog tehničkog znanja.[28] U pojedinim opštim uslovima osiguranja se ipak nalaze i opširnije definicije, što je posebno značajno iz vizure transparentnosti. Ono što svakako predstavlja izazov u vezi sa tumačenjem pojmova kod sajber osiguranja jeste da se osnovno znanje u kontekstu za IT specifičnih termina stalno proširuje. Stoga se postavlja pitanje kada se može reći da neko vlada svim

---

[25] Najčešće je to *Cyber-Underwriter* ili *Cyber Risk Engineer*.

[26] O tome već postoji praksa nemačkih sudova, v. primera radi, BGH v. 4. 4. 2018 – IV ZR 104/17, VersR 2018, 532.

[27] Theo Langheid, „§19 Anzeigepflicht", *Versicherungsvertragsgesetz: VVG mit Einführungsgesetz und VVG-Informationspflichtenverordnung* (Hrsg. Theo Langheid, Roland Rixecker), C. H. Beck, München, 2022, 165–211.

[28] Paul Malek, Camila Schütz, „Cyberversicherung: rechtliche und praktische Herausforderungen", *Recht und Schaden,* 2019, 421, 424.

potrebnim pojmovima iz ove oblasti.[29] Tako su pojmovi kao što što *cloud*, Trojanac, *ransomware* danas daleko uobičajeniji u svakodnevnom govoru nego što su bili pre par godina i zato se ta granica tolerantnosti stalno pomera. Takođe, u onoj meri u kojoj postoji obaveza osiguranika da odgovora na pitanja iz upitnika, tu postoji i obaveza osiguravača da pitanja koju su mu potrebna postavi, jer ne može zahtevati da dobije određene podatke o kojima nije postavio pitanja u upitniku.[30]

U vezi sa ovom obavezom osiguranika postavlja se pitanje: Kada će se smatrati da je osiguranik dao netačne odgovore i gde je granica njegove obaveze? Ova pitanja se postavljaju kako bi se dobio deo odgovora na pitanje da li je sajber osiguranje toliko različito od ostalih imovinskih osiguranje usled posebnosti obaveze prijave okolnosti relevantnih za procenu rizika. Da li osiguranik ikad ima mogućnost da se pozove na okolnost da nije zaista znao za određene okolnosti ili je u obavezi da uvek sve zna i da prijavi? Postoje li granice njegove obaveze, pogotovu što osiguravač može da angažuje forenzičara i uvek obezbedi dokaze da je objektivno nastupila povreda obaveze prijave okolnosti od strane osiguranika?[31] S obzirom na to da je potrebno i znanje i svest da daje pogrešne informacije, da li će postojati namerno postupanje ako postoje minimalna odstupanja od pravila o lozinkama i njihovoj jačini?[32] Da li će tada osiguravač imati pravo da traži poništaj, odnosno raskid?[33] Ili se nužno mora praviti razlika između ove situacije i situacije kada je dat pogrešan odgovor na više pitanja?

Kako bi se sva navedena pitanja i njihovi dometi bolji razumeli, poći ćemo od jednog praktičnog primera. Tako, primera radi, da li će se smatrati da je osiguranik dao netačne odgovore ako je u upitniku naveo da su koristili složene šifre za pristup sistemu, a oni su koristi šifru „1234", ako su prevelika administratorska ovlašćenja data prevelikom broju nedovoljno obučenih zaposlenih i ako navede da koriste sisteme koji imaju odgovarajuću podršku, a ispostavi se da njihov sistem nema podršku od 2015. godine? Da li će u navedenim slučajevima osiguranik izgubiti svoja prava iz ugovora o osiguranju, jer je netačno odgovorio ili zato što nije posedovao dovoljno tehničko znanje da zna da su ove dve gorenavedene okolnosti od velikog značaja za bezbednost njihovog poslovanja? Ako se prihvati da obaveza osiguranika počiva na strožim, tehnički preciznim zahtevima, da li to znači da je

---

[29] P. Malek, C. Schütz, op. cit., 421, 424.

[30] Dan Schilbach, „Typische Deckungseinwendungen in der Regulierung von Cyberschäden im Spannungsfeld zwischen Cyber- und D&O-Versicherung", *VersicherungsPraxis*, No. 2, 2023, 10.

[31] N. Wojciechowski, op. cit., 344.

[32] *Ibidem*, 345.

[33] Čl. 908, 909 ZOO.

kod ovog osiguranja obaveza osiguranika (i osiguravača) drugačije koncipirana? I to u tolikoj meri koja bi opravdalo njihovo tretiranje kao zasebne vrste osiguranja koje zahteva posebno zakonsko regulisanje.

U ovakvom jednom slučaju, kao što je prethodno prikazani, gde su korišćene slabe šifre, osiguranik bi trebalo da bude svestan rizika od izbora neadekvatnih lozinki koje ne ispunjavaju minimum zahteva. Iz tog razloga bi se moglo reći da je povređena obaveza prijave okolnosti od značaja za procenu rizika. Pogotovu što se takve šifre mogu odgonetnuti i otkriti i zahvaljujući alatima koji su besplatno *online* dostupni i koji ne zahtevaju nikakva posebna znanja i veštine. Da slabe šifre predstavljaju ozbiljnu opasnost na internetu, poznato je već i prosečnim osiguranicima. Ovi primeri jasno pokazuju da se rizik kod sajber osiguranja ocenjuje spram okolnosti konkretnog slučaja i da će sudovi u svakom pojedinačnom slučaju morati da ocenjuju da li su pruženi podaci bili dovoljni da osiguravač izvrši procenu rizika.

Povećanje rizika

Predugovorna procena rizika i u skladu sa njom prijava okolnosti od strane osiguranika samo odražava IT sigurnosni standard u trenutku zaključenja ugovora. Ako tokom trajanja ugovora dođe do promene standarda, to će rezultirati povećanjem rizika. Povećanje rizika po pravilu nastaje kada se usled neke okolnosti, uzimajući u obzir moguće uzročne procese, povećava mogućnost nastupanja osiguranog slučaja. Povećanje rizika mora biti takvo da bude relevantno iz aktuarskih razloga u smislu da bi bila naplaćena veća premija da se za takve okolnosti znalo u trenutku zaključenja ugovora o osiguranju.[34] Povećanje rizika se odnosi situacije kada dođe do naknadne promene okolnosti koje su relevantne za ocenu rizika i koje su bile relevantne u trenutku zaključenja ugovora, i koje utiču na povećanje verovatnoće nastupanja osiguranog slučaja ili koje utiču na povećanje nivoa nastale štete.[35] To se može oceniti uzimajući u obzir celokupnu situaciju i moguću kompenzaciju za odgovarajuće rizike. Stoga je potrebno utvrditi da se verovatnost nastupanja osiguranog slučaja promenila na štetu osiguravača nakon prijave okolnosti od strane osiguranika.[36] Tako, na primer, ako osiguranik upravlja delimično zastarelim (proizvodnim) sistemima za koje proizvođač više ne osigurava sigurnosna ažuriranja u trenutku sklapanja ugovora o sajber osiguranju, njihov daljnji rad ne menja nužno situaciju rizika.

---

[34] Manfred Wandt, *Versicherungsrecht*, Carl Heymanns Verlag, Frankfurt am Main, 2010, 275.

[35] *Ibidem.*

[36] *Ibidem.*

I u vezi sa ovom obavezom osiguranika se postavilo pitanje da li ova vrsta osiguranja poseduje određene karakteristike koje bi opravdale njegov poseban tretman. Pitanje se odnosi na situacije kada osiguravač insistira da okolnosti koje nisu obuhvaćene predugovornom obavezom mogu biti okolnosti koje utiču na povećanje rizika kod sajber osiguranja, uz opravdanje da u ovoj oblasti stalno nastupaju određene promene. Posledično, prema nekim stavovima u literaturi se počelo isticati da nije moguće osloniti se samo na one okolnosti koje su relevantne u trenutku zaključenja ugovora, već i na one koje nastupaju i nakon toga.[37] Ipak, stava smo da bi prilikom ocene treba voditi računa o opštoj i trenutnoj situaciji sa sajber rizicima i opasnostima koje donose. Postupanje suprotno tome bi značilo preveliko opterećenje po osiguranika koji bi bio izložen samovolji osiguravača.

Isto tako, postavlja se pitanje predstavlja li i pod kojim uslovima neinstaliranje postojećih sigurnosnih ažuriranja povećanje rizika bi osiguranik bio u obavezi da prijavi osiguravaču.[38] Pitanje se postavlja iz dva razloga: prvo zato što se često dešava da se sigurnosni sistemi ne ažuriraju, što hakeri koriste kao „prozor" u kom mogu da izvrše napad, a drugi razlog je pravne prirode. Naime, s obzirom da je za promenu rizika u smislu njegovog povećanja potrebno da postoji aktivno činjenje osiguranika,[39] pitanje je da li i propuštanje da se nešto preduzima, odnosno nečinjenje, dovoljno da se formira osnov za povećanje rizika ili je nužno da je reč o aktivnom postupku. Ipak, ako postojeća sigurnosna ažuriranja nisu instalirana, moglo bi se reći da postoji aktivno postupanje osiguranika ako se nastavi sa korišćenjem sigurnosnih sistema koji nisu ažurirani. Samo po sebi postojanje neažuriranog bezbednosno sigurnosnog sistema ne stvara situaciju povećanja rizika, već povećanje rizika nastaje ako se takav sistem dugoročno koristi.

U meri u kojoj karakter povećanja rizika nije takvog karaktera da se ima posmatrati kao trajan, ponašanje osiguranika – neažuriranje softvera – može se promatrati iz perspektive izazivanja osiguranog slučaja namerno ili prevarom.[40]

---

[37] Kao čest primer u prilog ovoj tezi jeste pozivanje na situaciju tokom pandemije kada je većina ljudi radila od kuće, na sopstvenim računarima, što je stvorilo mogućnosti za brojne hakerske napade. Upor. „Home-Office vergrößert Angriffsfläche für Cyber-Kriminelle", *https://www.bsi.bund-de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210415_HO-Umfrage.html*, 15. 9. 2023. Takođe, Iva Tošić, „Uticaj pandemije virusa kovid 19 na osiguranje od internet rizika", *Pandemija Kovida 19: pravni izazovi i odgovori* (ur. Vladimir Đurić, Mirjana Glintić), Institut za uporedno pravo, Beograd 2021, 161–162.

[38] Čl. 914 ZOO, par. 23 nemačkog Zakona o ugovornom pravu osiguranja – Versicherungsvertragsgesetz vom 23. November 2007 (BGBl. I S. 2631).

[39] Predrag Šulejić, *Pravo osiguranja*, Beograd, 2005, 235. Takođe, D. Schilbach, op. cit., 11.

[40] Ovo pitanje je u našem pravu regulisano čl. 920 ZOO.

Dakle, i ova situacija, koja na prvi pogled odstupa od zakonski regulisane materije, zapravo je pokrivena postojećim zakonskim normama i ne zahteva nove norme.

Do gubitka ili smanjenja prava osiguranika može doći i ako on iz svoje krivice dovede do nastupanja osiguranog slučaja. Osiguranik je, dakle, dužan da preduzme mere da spreči nastupanje osiguranog slučaja, a ako nastupi osigurani slučaj, potrebno je da preduzme sve što je u njegovoj moći kako bi posledice osiguranog slučaja bile što manje. O postupanju sa krajnjom nepažnjom[41] u kontekstu sajber osiguranja možemo govoriti kada osiguranik ne preduzima nekoliko neophodnih sigurnosnih mera. To bi bio slučaj kada osiguranik ne bi tražio alternative kada podrška servera prestane ili kada ne reaguje na bezbednosna upozorenja proizvođača softvera.

Stav suda o sajber osiguranju

U ovom trenutku smo uspeli da naiđemo na jednu sudsku odluku u pogledu obaveze osiguranika da prijavi okolnosti od značaja od procene rizika i sa tim povezanog povećanja rizika. Radi se o odluci suda u Tibingenu,[42] a tiče se štete koja je nastala usled virusa Trojanac.[43] Ukupna nastala šteta je iznosila skoro tri miliona evra koje je osiguravač odbijao da plati usled pogrešno popunjenog upitnika i zato što sigurnosni sistemi nisu apdejtovani. Ova odluka je vrlo bitna jer je sud presudio u korist tužilje, i pritom potvrdio stav da ovo osiguranje podleže svim pravilima kao i svaki drugi proizvod osiguranja, i da, iako još uvek postoje neke nejasnoće u pogledu razumevanja uslova osiguranja, njihovo tumačenje ne zahteva posebne moći.

U slučaju se radilo o tome da se odbrana osiguravača sastojala u pozivanje na to da sigurnosna ažuriranja za server koji je tužilja koristila nisu dostupna već godinama, što je tužilji bilo poznato. Sve je to uticalo na obim pretrpljene štete,

[41] U ZOO se ne govori o konkretnom stepenu krivice koji mora postojati da bi postupanje osiguranika bilo sankcionisao. Uslovi osiguranja pak isključuju lakši stepen krivice osiguranika, što bi značilo da je osiguravač oslobođen svoje obaveze ako je osiguranik postupao sa namerom ili velikom nemarnošću.

[42] Urteil vom 26. 5. 2023, Az. 4 O 193/21.

[43] Zaposleni je na poslovnom računaru otvorio mejl koji je sadržao virus i to tako što je otvorio prilog (*attachment*), za koji je u mejl pisalo da je faktura. Taj poslovni računar je preko VPN bio povezan sa mrežom tužilje. Trojanac je tako ušao u IT sistem i zaključao sve servere. Ponovo pokretanje sistema nije bilo moguće zbog enkripcije i svim zaposlenima se samo pojavila poruka na ekranu da se traži otkupnina u bitkoinima za otključavanje sistema. Tužilja nije ispunila navedeni zahtev, već se obratila policiji, koja još uvek nije našla izvršioca. Ceo sistem je stoga ostao zaključan, tužilja je morala da pravi novi IT sistem, usled čega su troškovi bili tako visoki.

jer bi savremeniji sistemi pružili bolju zaštitu. Da je tačno odgovoreno na pitanja iz osiguravačevog upitnika, onda osiguravač ne bi ni zaključio ugovor o osiguranju. Osim toga, tuženi se pozvao na povećanje rizika koje je povezao sa prouzrokovanjem osiguranog slučaja grubom nepažnjom jer tužilja nije preduzela mere zaštite od sajber napada. Povećanje opasnosti se ogleda u tome što nakon zaključenja ugovora tužilja nije izvršila zamenu servera Microsoft Windows 2003 i što se nije bavila ažuriranjem bezbednosnih sistema.

Sud je stao na stanovište niti da ima povrede predugovorne obaveze prijave okolnosti niti da ima prouzrokovanja nesrećnog slučaj usled grube nepažnje. Što se tiče povrede predugovorne obaveze, osiguranik je uspela da dokaže da netačni odgovori nisu bili uzrok nastanka osiguranog slučaja.

Tu je zapravo veštak odigrao ključnu ulogu kada je konstatovao da Windows ima postojeću slabost koju su hakeri iskoristili i koja bi svakako postojala nezavisno od toga da li je sistem apdejtovan ili ne. Ono što je naročito interesantno jeste da je sud zaključio da je osiguravač sam zapravo donekle kriv jer njegova pitanja nisu ukazivala jasno na to da je reč o osiguravaču koji ima visoke zahteve u pogledu sigurnosnih mera koje se imaju ispuniti. Da je to bio slučaj i da je tih zahteva bilo, onda bi osiguravač tako formulisao svoja pitanja u upitniku! U literaturi pak ima i drugačijih shvatanja, koja idu u pravcu opravdanja osiguravača i toga da on nije u mogućnosti da u upit unese sve relevantne okolnosti u oblasti sajber osiguranja, usled svih promena koje nastupaju, i da zato postoji opravdanje da se pravila ustanovljena za klasične vrste osiguranja ne mogu primeniti na nove vrste osiguranja.[44] Međutim, navedeni stavovi bi isuviše poremetili ionako labilnu ugovornu ravnotežu kod ugovora o osiguranju, nezavisno od toga li se osiguranik ima smatrati potrošačem ili ne.

ZAKLJUČAK

Nakon sprovedene analize nekih osnovnih načela koja vladaju sajber osiguranjem i njihovog upoređivanja sa osnovnim načelima „klasičnih" osiguranja, može se reći da se početna situacija kod sajber osiguranja razlikuje od početne situacije kod klasičnih osiguranja. Tako je, primera radi, kod osiguranja od požara početno stanje, u trenutku zaključenja ugovora, rizik stabilan, što kod sajber osiguranja nije moguće usled redovnih novih tehničkih otkrića. Opasnost od rizika se

[44] Peter Reusch, „§23 Gefahrerhöhung", *Münchener Kommentar Versicherungsvertragsgesetz: VVG, Band 1: §§ 1-99, VVG-InfoV* (Hrsg. Theo Langheid, Manfred Wandt), C. H. Beck, München, 2022, 700–701.

u vrlo kratkom periodu može povećati i učiniti mogućnost od sajber napada vrlo verovatnom.[45] Iz tog razloga su ugovorne obaveze, one koje proizilaze iz uslova osiguranja, nešto drugačije i možda preciznije u odnosu na takve obaveze kod ostalih osiguranja.[46]

Razlog zašto osiguravači tako pooštravaju svoje uslove osiguranje se najverovatnije sastoji u tome da u poslednjih nekoliko godina ima sve više i više sajber napada, usled čega stalno nastaju obaveze osiguravača koje se dovele da u određenim zemljama i u određenim trenucima posluju u zoni gubitka.[47] Osiguravači pokušavaju da ograniče visinu svoje obaveze, pa nije iznenađujuće da se ta ograničenja odgovornosti primenjuju na područja koja osiguravajuća društva smatraju posebno kritičnima. Ranije je kao standard korišćeno „stanje tehnike"[48] na koji su se osiguravači pozivali u uslovima osiguranja. Međutim, nešto što je preko nekog vremena predstavljalo i potpadalo pod taj standard, danas više ne predstavlja nekakvu posebnu prepreku za hakere. Stoga i osiguravajuća društva zahtevaju od osiguranika dalji i stalni razvoj i primenu zaštitnih mera. Tipični osiguranik u sajber osiguranju će biti vremenom uvežban u postupanju sa uslovima osiguranja i imaće iskustva. Od njega će se očekivati da ima određeno tehničko znanje.

Ipak, sve to ne znači da se radi o nekoj novoj vrsti osiguranja, koja je toliko drugačija da zahteva posebne članove zakona. Teoretski je zamislivo osigurati se protiv svakog rizika, ako to ne bi bilo protivno javnom poretku.[49] Potreba za lakšom sistematizacijom zahteva kategorizaciju poslova osiguranja. Osim toga, svrstavanje osiguranja u neku od postojećih vrsta osiguranja ima i svoj praktični značaj. Naime, u slučajevima kada ne postoji odgovarajuće pravno pravilo za neku vrstu osiguranja, pripadnost ili sličnost sa nekom vrstom osiguranja omogućava primenu pravila važećih za tu vrstu osiguranja.[50] Na taj način se popunjavaju pravne praznine, koje su neminovnost usled velike raznolikosti osiguranja. Iako bi bila poželjna, potpuna uniformnost se ne može postići, tako da se može desiti da se jedna vrsta osiguranja razlikuje kod različitih osiguravača. Pored praktičnog

---

[45] Lena Rudkowski, „Versicherungsrechtliche Probleme des vernetzten Zuhauses ('Smart Home')", *Versicherungsrech*t, 2017, 1, 4.

[46] Tako se u uslovima osiguranja insistira na dnevnom pohranjivanju podataka i ažuriranju sigurnosnih sistema.

[47] Podaci za nemačke osiguravače: *https://www.gdv.de/gdv/medien/medieninformationen/cyber-ver-si-che-rer-machen-erst-mals-ver-luste-markt-legt-wei-ter-zu-89766*, 27. 9. 2023.

[48] D. Schilbach, op. cit., 12.

[49] John F. Dobbyin, *Insurance Law in a Nutshell,* West Publishing Co, St. Paul, 1966, 6.

[50] Vladimir Jovanović, *Osiguranje u privredi*, Zagreb, 1962, 19.

značaja podele osiguranja na različite vrste, time se značajno olakšava naučno i teoretsko izučavanje pojedinačnih vrsta osiguranja.

Svakako da je ranije postojao manji broj vrsta osiguranja, jer određenih rizici nisu postojali ili im se nije dovoljno davalo na značaju.[51] Ukorak sa novim opasnostima koje su se javljale, razvijali su se novi oblici osiguranja. Istovremeno su neke druge vrste vremenom izgubile na značaju, tako da je preambiciozno očekivati da se mogu pobrojati sve vrste osiguranja. Manje-više sva osiguravajuća društva prihvataju i nude tipične vrste osiguranja uprkos dispozitivnosti pravila prava osiguranja i ovlašćenja osiguravača da stvara posebne vrste osiguranja i donosi sopstvena pravila. To je jedan od razloga zašto zakonska pravila u pravu osiguranja treba da budu formulisana na takav način da omoguće svoju primenu i na neke nove vrste osiguranja koje će se tokom vremena razviti. Upravo je to slučaj i sa sajber osiguranjem, koje nije takvo da postoji potreba za njegovim posebnim zakonskim regulisanjem. Ono se vrlo jasno može sagledati u kontekstu već postojećih podela osiguranja i u okviru tih podela primenjivih pravila.

Kao što je već istaknuto, nadzorni organ koji vrši kontrolu poslovanja nad osiguravajućim društvom (Narodna banka Srbije u Republici Srbiji) verovatno će imati izazov na koji način će primenjivati statutarne propise.[52]

Na samom kraju ne treba ispuštati iz vida da se ispitane obaveze osiguraniku imaju regulisati opštim uslovima osiguranja, koji se donose unapred za pojedinačne grane osiguranja ili pojedine vrste osiguranja i kojima se određuje sadržina budućih ugovora o osiguranju.[53] Menjanje zakona kada bi nastajao svaki novi proizvod osiguranja imalo bi kontraproduktivno dejstvo, jer bi se odustajalo od razvijanja odnosa osiguranja. Prinudne i poluprinudne norme zakona ostavljaju dovoljno prostora za regulisanje ugovornih odnosa u skladu sa autonomijom volja, a veći deo prostora je popunjen uslovima osiguranja, koji preciziraju obaveze ugovornih strana, kako u predugovornoj, tako i ugovornoj fazi.

Nesporno je da je potrebno da postoje odgovarajuće ugovorne obaveze koje predviđaju postojanju ovakvih standarda ponašanja. Dakle, nije nužna da svaka obaveza bude zakonski regulisana, već je dovoljno da proizilaze iz uslova osiguranja.[54]

---

[51] Tako su nekad u Americi postojale samo tri vrste osiguranja: osiguranje života, osiguranje od požara i ostale vrste osiguranja stvari i osiguranje na unutrašnjim vodama. J. F. Dobbyin, op. cit., 6.

[52] Konkretno u Republici Srbiji mali je broj osiguravača koji se uopšte odlučio da ponudi ovaj proizvod osiguranja. v. detaljnije Iva Tošić, „Osiguranje od internet rizika", *Prouzrokovanje štete, naknada štete i osiguranje* (ur. Vladimir Čolović, Zdravko Petrović), Beograd, Valjevo, 2020, 447–448.

[53] P. Šulejić, op. cit., 52.

[54] Nemačka literatura stoga pravi razliku između *Pflichten* i *Obligheiten* kako bi se napravila razlika između izvora ovih obaveza. M. Wandt, op. cit., 201–208.

U pogledu navedenih uslova tržište je vrlo heterogeno. Uslovi osiguranja idu od toga da ne sadrže nikakve tehničke odredbe, preko predviđanja čitavog spiska obaveza, pa do opštih formulacija u vidu klauzula koje obavezuju osiguranika na poduzimanje tehničkih organizacijskih mera u skladu s najnovijim dostignućima.[55] Ono što pak jeste uočeno kao trend, bar na inostranim tržištima, jeste da su se počeli razvijati koncepti pokrića osiguranja, koji se u potpunosti odriču predviđanja obaveza uslovima osiguranja.[56] Posledično se počelo postavljati pitanje pravnih posledica neispunjenja određenih obaveza od strane osiguranika u takvim slučajevima. Stava smo da je vrlo bitno da nadzorni organi kontrolišu ovaj izvor prava osiguranja, jer će u velikoj meri od njega zavisiti ishod sudskih sporova, pa stoga ne bi trebalo podržati navedeni trend.

I pred domaćim i stranim sudovima veliki je put dok se ne uspostavi konsolidovana sudska praksa u pogledu sajber osiguranja, a koje će biti sve više i više s obzirom na sve veću učestalost sajber napada. Heterogenost u pogledu različitih ponuda pokrića od različitih osiguravača samo je znak da će do željene pravne sigurnosti i transparentnosti doći postepeno. S obzirom na ukazane karakteristike ovog osiguranja, za koje je ustanovljeno da se u velikoj meri poklapaju sa karakteristikama drugih osiguranja, nesumnjivo smo stava da će se sudovi moći osloniti na svoju dosadašnju praksu.

Dr. MIRJANA GLINTIĆ
Research Fellow, Institute of Comparative Law
Belgrade

CYBER INSURANCE AS A NEW TYPE OF INSURANCE
– IS THERE A NEED FOR A NEW INSURANCE CLASSIFICATION –

Summary

Demand for cyber insurance has drastically increased due to the increasing number of cyber-attacks and due to the fact that this insurance is crucial for maintaining business stability. Opting for this insurance product, policyholders are entitled to different forms of assistance provided by the insurer, which enables sustainable protection from losses caused by cyber-attacks. The duties of both the insurer and the insured stemming from the cyber insurance contract differ in certain aspects from the duties of contractual parties in other property insurance contracts. Consequently, voices from

[55] D. Schilbach, op. cit., 11. U tom kontekstu postoji mnogo prostora za (tehničke) rasprave, koje se, u slučaju sumnje, mogu razjasniti samo kada dođe do konkretnog pravnog spora.

[56] N. Wojciechowski, op. cit., 342.

both practitioners and academia can be heard, claiming that regulations from the field of insurance contract law cannot be applied to this insurance, because they represent a special type of insurance. Therefore, the author devotes the central part of the paper to the analysis of certain duties of the contracting parties in cyber insurance in order to examine the validity of the stated positions. Positive legal and comparative legal analysis signaled that the approach of the Serbian legislator is such that it allows this insurance to be understood as property insurance and that consequently, it is not necessary to regulate cyber insurance separately. The concluding part of the paper is devoted to arguments for the further regulation of this insurance exclusively through the general conditions of insurance.

Key words: cyber insurance, disclosure duty, risk increase, property insurance, general insurance conditions

Literatura

Abraham K., Schwarcz D., „The limits of regulation by insurance", *Indiana Law Review*, No. 1, Vol. 98, 2022.

BaFin, *BaFin Journal*, No. 9, 2021, *https://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2021/bj_2109.pdf?__blob=publicationFile&v=3*.

Baker T., Grifth S., *Ensuring corporate misconduct: How liability insurance undermines shareholder litigation*, University of Chicago Press, Chicago, 2010.

Baker T., Shortland A., „Insurance and enterprise: cyber insurance for ransomware", *The Geneva Papers on Risk and Insurance – Issues and Practice*, Vol. 48, 2023.

Biener C., Eling, M., Wirfs J. H., „Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance. Issues and Practice*, No. 1, Vol. 40, 2015.

Bolot J., Lelarge, M., „Cyber insurance as an incentive for internet security", *Managing Information Risk and the Economics of Security* (ed. Eric Johnson), Springer, New York, 2009.

Cunningham B., Talesh S. A., „Uncle Sam RE: Improving cyber hygiene and increasing confdence in the cyber insurance ecosystem via government backstopping", *University of Connecticut Insurance Law Journal*, No. 1, Vol. 28, 2021.

Dobbyin J. F., *Insurance Law in a Nutshell*, West Publishing Co, St. Paul, 1966.

Đurić V., „Upravnopravni aspekti konkursnog ostvarivanja javnog interesa u Republici Srbiji", *Aktuelna pitanja savremenog zakonodavstva i pravosuđa*, Beograd, 2023.

Haas A., Hofmann A., „Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit", *FZID Discussion Paper*, No. 74, 2013.

Hofmann A., Ramaj H., „Interdependent risk networks: The threat of cyber-attack", *International Journal of Management and Decision Making*, No. 5/6, Vol. 11, 2011.

Glintić M., „Osiguranje poverenja kao instrument zaštite imovine privrednih društava", *Pravo i privreda*, br. 7–9, 2019.

Glintić M., „Pravna priroda prava na isplatu osigurane sume kod osiguranja lica", doktorska disertacija odbranjena na Pravnom fakultetu Univerziteta u Beogradu, Beograd, 2019.

Jovanović V., *Osiguranje u privredi*, Zagreb, 1962.

Langheid T., „§19 Anzeigepflicht", *Versicherungsvertragsgesetz: VVG mit Einführungsgesetz und VVG-Informationspflichtenverordnung* (Hrsg. Theo Langheid, Roland Rixecker), C. H. Beck, München, 2022.

Malek P., Schütz C., „Cyberversicherung: rechtliche und praktische Herausforderungen", *Recht und Schaden*, 2019.

Oğüt H., Raghunathan S., Menon N., „Cyber security risk management: Public policy implications correlated risk, imperfect ability to prove loss, and observability of self-protection", *Risk Analysis*, No. 3, Vol. 31, 2011.

Petrović Tomić N., *Zaštita potrošača usluga osiguranja: analiza i predlog unapređenja regulatornog okvira*, Pravni fakultet, Centar za izdavaštvo i informisanje, Beograd, 2015.

Reusch P., „Die vorvetragliche Anzeigepflichten im neuen VVG 2008", V*ersicherungsrech*t, Heft 28, 2007.

Reusch P., „§23 Gefahrerhöhung", *Münchener Kommentar Versicherungsvertragsgesetz: VVG, Band 1: §§ 1–99, VVG-InfoV* (Hrsg. Theo Langheid, Manfred Wandt), C. H. Beck, München, 2022.

Rudkowski L., „Versicherungsrechtliche Probleme des vernetzten Zuhauses ('Smart Home')", *Versicherungsrech*t, 2017.

Schilbach D., „Typische Deckungseinwendungen in der Regulierung von Cyberschäden im Spannungsfeld zwischen Cyber- und D&O-Versicherung", *VersicherungsPraxis*, No. 2, 2023.

Tošić I., „Osiguranje od internet rizika", *Prouzrokovanje štete, naknada štete i osiguranje* (ur. Vladimir Čolović, Zdravko Petrović), Beograd, Valjevo, 2020.

Tošić I., „Uticaj pandemije virusa kovid 19 na osiguranje od internet rizika", *Pandemija Kovida 19 : pravni izazovi i odgovori* (ur. V. Đurić, M, Glintić), Institut za uporedno pravo, Beograd 2021.

Šulejić P., *Pravo osiguranja*, Beograd, 2005.

Wandt M., *Versicherungsrecht*, Carl Heymanns Verlag, Frankfurt am Main, 2010.

Wojciechowski N., „Aufsätze Cyberversicherung: Vorvertragliche Anzeigepflicht und Gefahrerhöhung", *Versicherungsrecht*, 2022.

ORIGINALAN NAUČNI RAD