Iva Tošić[*]
Olivera Novaković[**]

OSIGURANJE OD INTERNET RIZIKA I NOVA REGULATIVA U OBLASTI ZAŠTITE PODATAKA O LIČNOSTI

Apstrakt

Donošenje Opšte uredbe o zaštiti podataka o ličnosti i po ugledu na nju srpskog Zakona o zaštiti podataka o ličnosti predstavlja prekretnicu u prikupljanju, obradi i skladištenju podataka o ličnosti. Sa druge strane razvoj i sve veća upotreba kompjutera i interneta pored ogromnih prednosti kao što je ušteda vremena i sredstava, sa sobom nose i određene rizike. Ti rizici se odnose pre svega na internet napade koji su sve učestaliji i koji mogu doneti ogromne troškove pogođenoj kompaniji. Otežavajuća okolnost za određene kompanije je činjenica da poseduju podatke koji su prikupljani i skladišteni godinama, a nakon usvajanja nove regulative, prikupljenim podacima je neophodno u kratkom vremenskom roku odrediti svrhu i kategorisati ih u skladu sa novim odredbama. Pored toga, kompanije su sve češće mete internet napada, koja postaje jedna od vodećih kriminalnih aktivnosti u svetu, te se u slučaju eventualnog curenja ličnih podataka zaposlenih i korisnika mogu naći u nezavidnoj situaciji. U tom slučaju troškovi koje bi kompanija morala da pokrije, pogotovo u slučaju da nije u potpunosti usklađena sa novom regulativom, gotovo sigurno bi je dovele do bankrotstva. Upravo iz tih razloga u visokorazvijenim zemljama javilo se osiguranje od internet rizika, koje za cilj ima da smanji troškove koji bi pogodili kompaniju u slučaju da bude meta internet napada i omogućili njeno dalje poslovanje.

U prvom delu rada autori obrađuju ukratko razloge donošenja i značaj nove regulative u oblasti zaštite podataka o ličnosti, kao i poteškoće sa kojima se kompanije susreću u implementaciji novih odredaba, dok se u drugom delu obrađuje uticaj ove regulative na razvoj osiguranja od internet rizika, kao i polemiku da li ta vrsta osiguranja može pokrivati i kazne koje kompanija snosi u slučaju neusklađenosti sa novim odredbama.

***Ključne reči**: lični podaci, GDPR, internet kriminal, osiguravajuća društva, zaštita podataka o ličnosti.*

[*] Istraživač saradnik, Institut za uporedno pravo; *mail: iva_tosic@hotmail.com*

[**] Advokat; mail: *adv.oliveranovakovic@gmail.com*

1. Uvod

Razvoj i primena računara, računarskih mreža i interneta u svim društvenim segmentima doprinela je unapređenju kvaliteta poslovanja i dostupnosti informacija.[1] Međutim, bez obzira na brojne prednosti koje internet donosi, on sa sobom nosi i određene rizike, kako za pojedince tako i za privredna društva. U današnje vreme postoji visok stepen internet rizika i isti predstavlja svakodnevnu pretnju kontinuiranom poslovanju i pružanju usluga u javnom i u privatnom sektoru, a njegovo nastupanje može dovesti do katastrofalnih posledica. Prema rečima Roberta S. Muellera "postoje dve vrste firmi, one koje su hakovane, i one koje će biti hakovane".[2]

S obzirom na sve intenzivniju upotrebu interneta (prema procenama 2020. godine će trilion uređaja biti umreženo)[3] i sveprisutnu opasnost od nastanka štete usled internet napada, u razvijenim zemljama se kao odgovor javilo osiguranje od internet rizika. Na ovaj način se smanjuje zabrinutost kompanije o „samoosiguravanju" i sprečava se da ogromni novčani iznosi u slučaju nastupanja rizika odlaze u nepredviđene svrhe.[4] U vremenu kada internet predstavlja neizostavan deo kako privatnog (individualnog), tako i poslovnog života, nesporno je da će ova vrsta osiguranja postati jedna od najznačajnijih vrsta osiguranja radi obezbeđenje materijalne sigurnosti pojedinaca (fizičkih lica), pravnih lica, kako većih, tako i manjih[5], ali i samih država.

Sa druge strane, globalna upotreba interneta i umrežavanje putem interneta u poslovanju, sve veća međunarodna saradnja i internet kupovina, ubrzanje protoka informacija i nekontrolisana razmena podataka doveli su do potrebe da se na jedinstven i celovit način uredi pitanje koji podaci će se kategorisati kao lični podaci, na koji način takvi podaci mogu pre svega da se prikupljaju, obrađuju, a onda i skladište. Iz navedenih razloga doneta je pre svega Opšta uredba o zaštiti podataka (*General Data Protection*

[1] Za više videti: *Internet i društvo*, Srpsko sociološko društvo, Univerzitet u Nišu – Filozofski fakultet, Institut za uporedno pravo, Beograd 2014.

[2] „There are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.", https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies, 08.06.2020.

[3] Allianz Global Corporate & Specialty, „A guide to Cyber risk- Managing the Impact of Increasing Interconnectivity", 2015., 5.

[4] A. Mukhopadhyay et al., „Insurance for Cyber-risk- A Utility Model", https://www.researchgate.net/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model, 15.04.2020.

[5] Veličina određenog privrednog društva najčešće nije merilo kojim se vode lica koja izvršavaju internet napade, mnogo su značajnije informacije koje određeno društvo poseduje.

Regulation)[6] koja je na unificiran[7] način regulisala ovu oblast u Evropskoj uniji, a koja je bila uzor za donošenje srpskog Zakona o zaštiti podataka o ličnosti (ZZPL).[8] Zahvaljujući donošenju ovih propisa omogućeno je podizanje nivoa poverenja korisnika u servise informacionog društva, uz zaštitu njihovih fundamentalnih prava.[9]

Upravljanje internet rizikom nastaje kao uzrok i posledica usklađivanja sa pravilima nove regulative, s obzirom da pomenuta pravila podstiču kompanije da usvoje znatno strožu praksu zaštite podataka. U jednoj anketi sprovedenoj na 1300 ispitanika, 65% ispitanika je reklo da sada smatraju internet najvećim rizikom. Sprovođenje GDPR-a podstiče kompanije da razviju novi pogled na internet rizik, a ne samo na njihove protokole o privatnosti. Ovo istraživanje je pokazalo da najspremnije kompanije koriste GDPR kao katalizator za poboljšanje njihovog upravljanja internet rizikom, uključujući i ekonomičniju procena njihovih rizika i povećan fokus na izgradnju otpornosti na neizbežne internet incidente .[10]

2. Implementacija GDPR-a u poslovanju i problemi za kompanije

Nova regulativa u oblasti zaštite podataka o ličnosti predstavlja prekretnicu i predviđa niz prava za lice na koje se podaci odnose čime podiže nivo pravne zaštite ovih lica u oblasti prava koja su proklamovana Ustavom. Međutim, čini se da je u želji da se zaštiti lice na koje se podatak odnosi, zakonodavac zanemario i drugog učesnika odnosa koji svoje celokupno poslovanje mora da prilagodi novim propisima.

GDPR je objavljen 27. aprila 2016. godine i ostavljen je rok od dve godine kompanijama da usklade svoje poslovanje sa novom regulativom. Iako na prvi pogled postavljeni zadatak ne deluje komplikovano, kompanije su se

[6] UREDBA (EU) 2016/679 EVROPSKOG PARLAMENTA I VEĆA od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka te o stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka- GDPR)

[7] O povezivanju i unifikaciju u EU: J. Ćeranić, „Redefinisanje koncepta evropskih integracija", *Aktuelna pitanja savremenog zakonodavstva*, Budva 2017., 201-214. ; J. Ćeranić Perišić, „Pravo evropske unije u funkciji razvoja evropskih integracija", *Pravo u funkciji razvoja društva- zbornik radova*, Kosovska Mitrovica 2019., 409-423 ; J. Ćeranić, „Diferencirana integracija- instrument za prevazulaženje različitosti između država članica EU", *Univerzalno i osobeno u pravu- zbornik radova,* Kosovska Mitrovica 2018., 63-79.

[8] *Službeni glasnik RS*, br. 87/2018.

[9] V. W. Gregory. "Looking at European Union data protection law reform through a different prism: The proposed EU General Data Protection Regulation two years later." *Journal of Internet Law* , 2014.,13.

[10] NU perspective, „Companies Getting Ready for GDPR", *Cyber risk management now a top priority as businesses prepare for changes to EU privacy law, Marsh study says*, 2017., 20.

susretale sa brojnim problemima prilikom implementacije. Nova regulativa uvodi strože definisanje profilisanja čime se znatno otežava rad društava koja svakodnevno koriste i obrađuju ogroman broj podataka o ličnosti, a isto tako je dodatno otežavajuća okolnost što takva društva svoje celokupno poslovanje godinama unazad zasnivaju na konstantnom prikupljanju podataka. Davanje širokog spektra prava licima na koja se podaci odnose je znatno otežalo rad društava i opteretilo zaposlene, koji su u periodu implementacije morali da ulože mnogo truda i vremena kako bi najpre podatke koji su se, bez ikakve selekcije, godinama unazad prikupljali, uredili.

Sa druge strane, GDPR je najpre implementiran u zakonodavstva svake pojedinačne zemlje članice EU, zbog čega se obaveze koje se nameću kompanijama značajno razlikuju među zemljama. U tom smislu, primećuju se varijacije u vrsti obaveza koje su nametnute kompanijama koje prikupljaju podatke (npr. pribavljanje saglasnosti; ograničenja, otkrivanja ili odredbe o odjavi u vezi sa upotrebom ili prodajom podataka; zahtevi za prenosivost; obaveze brisanja podataka na zahtev); vrsti ličnih podataka koji su zaštićeni (npr. od precizno određenog tipa podataka do davanja preširoke definicije ličnog podatka), visini i vrsti zaprećene kazne (negde je propisana prekršajna odgovornost za kompaniju, a negde čak i krivična odgovornost). Osim navedenog, međunarodni domet regulative dodaje novi nivo složenosti. GDPR nameće obaveze bilo kojoj kompaniji na svetu koja prikuplja podatke o građanima država članica EU.[11]

Kao što se može zaključiti, najveći problem prilikom implementacije regulacije u svoje poslovanje, bilo je tumačenje pojedinih odredbi, jer se radilo o potpuno novoj regulativi, podjednako za one koje treba da ih se pridržavaju i za one koji kontrolišu njihovu primenu. Zbog toga se u praksi pokazalo da su ostavljeni rokovi za implementaciju norme u poslovanje zapravo bili kratki, dok su sa druge strane zaprećene kazne izuzetno visoke, te ukoliko bi iz kompanije procureo neki podatak, a da kompanija nije ispoštovala neko od pravila predviđenih novom regulativom, mogla bi se naći u izuzetno nepovoljnoj situaciji. Upravo iz tih razloga donošenje nove regulative povećalo je potražnju za osiguranjem od internet rizika[12], a sa druge strane kompanije su osiguravajućim društvima zadale kao glavno pitanje da li polisa osiguranja od internet rizika pokriva i eventualne kazne[13] predviđene GDPR-om.[14]

[11] OECD, „The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage", 2020, 15.

[12] D. Woods, A. Simpson. "Policy measures and cyber insurance: A framework." *Journal of Cyber Policy* , 2017., 214.

[13] Za više videti: S. J. Golla, „Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law.,* 2017., 70-78.

[14] GDPR, čl. 83.

3. GDPR i osiguranje od internet rizika

Uzimajući u obzir ogromne kazne koje pogađaju kompanije u slučaju neusklađenosti sa pravilima GDPR-a, postavilo se pitanje da li polisa osiguranja od internet rizika u slučaju gubitka ličnih podataka pokriva i rizik neusklađenosti sa odredbama GDPR-a, odnosno novčane kazne propisane Direktivom, kao i sve troškove koje bi kompanija zbog toga snosila.[15] Nadalje, ukoliko polisa osiguranja od internet rizika ne pokriva rizik neusklađenosti sa novom regulativom, treba utvrditi da li uopšte postoji mogućnost zaključenja takve vrste osiguranja, kao i da li je to svrsishodno.

Upravo u pogledu navedenog pitanja, javila se najveća polemika, zbog čega se od OECD-a (*Organisation for Economic Co-operation and Development*) tražilo da razjasni ovo pitanje. Regulisanje navedenog najpre zavisi od zakonodavne politike svake zemlje, a zatim od stava osiguravajućih društava, kao i da li su osiguravajuća društva spremna da ovu vrstu osiguranja pruže u okviru polise osiguranja od internet rizika ili je potrebno posebno osigurati ovaj rizik. Treba takođe imati u vidu da kazne propisane Direktivom imaju prekršajni karakter, ali sama Direktiva daje mogućnost svakoj državi da propiše dodatne kazne koje mogu biti kako prekršajne, tako i kivične prirode. Kada su u pitanju novčane kazne iz krivičnog postupka one ne mogu biti osigurane ni u jednoj zemlji. Ovakav stav je zasnovan na principu da lice (pravno ili fizičko) koje je počinilo krivično delo bi trebalo da snosi posledice (kazne) tog dela jer bi u suprotnom odvraćajući efekat kazne bio smanjen.[16] Međutim, kada su u pitanju prekršajne kazne, regulativa se razlikuje od zemlje do zemlje.

U nekim zemljama (npr. Austrija, Danska, Francuska, Italija, Luksemburg, Portugal, Rusija, Švajcarska), je zauzet jasan stav po pitanju osiguranja od odgovornosti za novčane kazne, pa tako ovakva vrsta odgovornosti (bila ona krivična ili prekršajna) ne može biti osigurana, bilo da je to učinjeno direktno tako što je zakonom te zemlje zabranjeno, bilo indirektno tako što je takav stav zauzela sudska praksa smatrajući da je takvo osiguranje nezakonito ili suprotno javnom poretku.[17] Postoje i zemlje koje, premda nemaju jasan stav zakonodavne ili sudske vlasti, ipak ovakvu vrstu osiguranja ne dozvoljavaju, zasnivajući taj stav na suprotnosti javnom poretku kao i principu da nesavesna strana treba da snosi troškove za svoje postupke. U nekoliko zemalja mogućnost

[15] B. Hayretdin, U. Franke, E. Langfeldt Friberg, „The cyber-insurance market in Norway", *Information & Computer Security*, 2019., 5.

[16] OECD, 2020, 18.

[17] Aon and DLA Pipe, *The price of data security: A guide to the insurability of GDPR fines across Europe*, 2018., http://www.aon.com/attachments/risk-services/Aon_DLAPiper-GDPR-Fines-Guide_Final_May2018.pdf, 25.06.2021.

osiguranja kazni zavisi od prirode dela (kao što je da li postoji namera ili gruba nepažnja), ili svrhe novčane kazne.[18]

Uzimajući u obzir da mogućnost da pomenute kazne budu pokrivene polisom osiguranja zavisi od niza faktora, ovde se više radi o sivoj zoni, nego crnoj ili beloj sa različitim stepenima nesigurnosti u zavisnosti od zemlje i politike osiguravajućih društava. [19]

Sa druge strane, nepoštovanje GDPR-a, povlači i niz drugih posledica i troškova. To uključuje troškove i resurse koji su neophodni za odgovor na intervencije i istragu poverenika, prekid poslovanja, zahtevi za kompenzaciju koji su podneli pojedinci na čija prava i slobode je uticalo kršenje GDPR-a i narušavanje reputacije. GDPR daje subjektima podataka građanima EU čiji su podaci ugroženi pravo da zahtevaju naknadu od odgovornih kontrolora i obrađivača podataka. Ovo pravo je široko, a obuhvata i „nematerijalnu štetu", te bi pogođenu kompaniju moglo izložiti ogromnim troškovima. Ukoliko su usled internet incidenta lični podaci klijenata ugroženi, a da stvar bude gora, kompanije ne obavesti poverenika i pogođene klijente, vrlo lako može doći do gubitka reputacije. Polisa internet osiguranja sa posebnim pokrićem prilagođenim GDPR-u mogla bi biti posebno dragocena za rešavanje rizika grupnih zahteva za povredu privatnosti pogođenih pojedinaca.

Osiguranje od internet rizika može pružiti koristan nivo zaštite u pogledu troškova povezanih sa oporavkom kompanije i obnavljanjem podataka. U slučaju internog pada sistema ili prekida usluge, osiguranje može pomoći u pokrivanju troškova povratka na mrežu, neke osiguravajuće kompanije mogu pružiti hitan pristup stručnjacima iz ove oblasti –što je korisno ukoliko kompanija ne poseduje takve stručnjake. Takođe osiguranje pruža pokriće za pravno zastupanje, kao i naknadu troškova za zahteve koje protiv kompanije podnose pojedinci pogođeni prekršajem.

Međutim, pored toga što bi polisa osiguranja od internet rizika pokrila širok spektar troškova u slučaju kršenja odredbi nove regulative, poput troškova povezanih sa istragom, uključujući potencijalne pravne i stručne troškove, zahteva za naknadu štete od pojedinaca podnetih protiv kompanije kao rezultat nepoštovanja GDPR-a i troškova povraćaja narušene reputacije, potencijalna neosiguranost novčanih kazni ili barem trenutna neizvesnost da li se novčane kazne mogu pokriti mogu biti značajan razlog zbog kojeg se kompanija neće okrenuti internet osiguranju kao sredstvu za upravljanje GDPR rizikom.

---

[18] Aon and DLA Piper, *The Price of Data Security (Second Edition*), 2019. https://www.dlapiper.com/fr/france/insights/publications/2019/07/updated-guide-on-theinsurability-of-gdpr-fines-across-europe, 25.06.2021.

[19] Marsh, „GDPR Fines and Penalties: Insurability will Vary by Location, Policy Details, and More", 2018, 1.

Međutim, ukoliko polisa pokriva ovu štetu, za kompaniju ovo neminovno predstavljaju motiv za zaključenje ugovora o osiguranju. Upravo iz tog razloga, kao glavni argument protiv mogućnosti osiguranja od rizika neusklađenosti[20] navodi se moralni hazard, tj. činjenica da kompanije neće imati podsticaj da usklade svoje poslovanje sa novim pravilima ukoliko znaju da neće snositi nikakve posledice za takvo postupanje. Novčane kazne su takve prirode da odvraćaju kompanije od neusaglašavanja sa propisima, međutim ako bi osiguravajuća društva pokrivala ovaj rizik to dejstvo bi se izgubilo. Zakonodavci vrlo često prepoznaju ovaj problem zbog čega postoji već dugo uspostavljena takozvana „odbrana od nezakonitosti" koja sprečava kompanije i pojedince da koriste osiguranje kako bi izbegle posledice svojih nezakonitih radnji. Novčane kazne se smatraju prikladnim i predviđaju se samo u slučajevima kada postoje veliki propusti u poslovanju kompanije, ili gde, uprkos upozorenjima, kompanija nije uskladila svoje poslovanje. Samim tim, zakonodavstvo mnogih zemalja zabranjuje mogućnost da kazne budu obuhvaćene polisom osiguranja. U okviru jedne studije sprovedene na 30 zemalja utvrđeno je da svega u 2 zemlje polisa osiguranja od internet rizika pokriva kazne koje kompanija može snositi u slučaju neusaglašenosti.[21]

Sa svega navedenog, jasno je da na teritoriji Evrope postoji pravna nesigurnost kompanija korisnika osiguranja od internet rizika, a isto tako i velika neusklađenost po pitanju šta je polisom pokriveno. Smatramo da je ovom pitanju potrebno posvetiti više pažnje i unificirati ga, kako svaka kompanija ne bi zavisila od jurisdikcije svake pojedinačne zemlje.

4. Srbija

Ideja regulisanja pitanja zaštite podataka o ličnosti ne predstavlja novinu u srpskom pravnom sistemu, jer su lični podaci uvek predstavljali zaštićenu kategoriju, koja je kao takva proklamovana Ustavom Republike Srbije.[22] Međutim, tek sa pojavom GDPR Direktive po ugledu na koju je u Srbiji donet Zakon o zaštiti podataka o ličnosti (ZZPL), po prvi put je detaljno regulisana ova oblast. Zakonodavac je predvideo odloženu primenu predmetnog zakona od devet meseci, što predstavlja značajno kraći rok od onoga koje su dobile države članice EU i njihova privreda. Niska svest o samom razlogu zaštite privatnosti i činjenica da se kod nas mnoge kompanije još nisu usaglasile ni sa starim pravnim okvirom

[20] Izuzimajući zakonodavnu regulativu u pogledu ovog pitanja, koja u mnogim zemljama zabranjuje mogućnost da osiguranje pokriva kazne.

[21] V. Leemans, D. Molony. „Are GDPR Fines Insurable?", *Risk Management* , 2018., 28-29.

[22] Za više o pojmu i istorijatu podataka o ličnosti videti: S. Andonović, *Zaštita podataka o ličnosti u elekronskoj javnoj upravi u Republici Srbiji- pravni aspekti*, doktorska disertacija, Pravni fakultet u Beogradu, 2019., 87-146.

iz ove oblasti[23], koji mnogi nazivaju „praistorijskim", bile su jasan pokazatelj da su donošenju novog zakona predstojali veliki izazovi kako za privredna društva, javne ustanove i državne organe, tako i za samu kancelariju poverenika koja takođe imala zadatak da se pripremi i dodatno kadrovski pojača za početak primene kompleksnih zakonskih odredbi.

Problematika implementacije ZZPL-a u Srbiji na praktičnom nivou se u najvećoj meri pojavila iz razloga neusaglašenosti ZZPL-a sa domaćim propisima, a pre svega na dosad nedefinisane poslovne pojmove, prakse i mehanizme koji ne postoje ili nisu dovoljno pojašnjeni u domaćem pravnom sistemu, što dovodi u pitanje njegovu potpunu funkcionalnost.

Kako je ZZPL u potpunosti usklađen sa pravilima GDPR-a, postoji neophodnost usaglašavanje propisa koji uređuju određene oblasti sa njegovim odredbama, ali i donošenje podzakonskih akata koje bi trebalo da olakšaju njegovu primenu. Takođe, osim usaglašavanja odredbi zakona kojima se uređuju pojedine oblasti, i donošenja podzakonskih akata, neophodno je i uspostavljanje internih procedura kojima će se olakšati praktična primena njegovih odredbi.

Sa druge strane, osiguranje od internet rizika u Republici Srbiji na žalost, skoro uopšte nije razvijeno. Takva vrsta osiguranja je praktično tek „provirila" među prvima su je ponudili u kompaniji Wiener Stadtische osiguranje. Međutim, primeri internet napada su i u Srbiji mnogobrojni, tako da je nesporno da potreba za ovom vrstom osiguranja svakako postoji, a sa donošenjem nove regulative u oblasti zaštite podataka o ličnosti potreba za ovom vrstom osiguranja će biti sve veća.

Zakon o obligacionim odnosima Republike Srbije, propisuje tri uslova koja ugovor o osiguranju mora da ispuni da bi se smatrao validnim. Osigurani slučaj s obzirom na koji se zaključuje osiguranje mora biti: budući, neizvestan i potpuno nezavisan događaj od isključive volje osiguravača.[24] To bi ukazivalo na to da zakonodavac ne predviđa prepreku da novčane kazne budu osigurane u Republici Srbiji, međutim, ta odgovornost kompanije i pokriće odgovornosti se može naknadno dovesti u pitanje ako je osigurano lice postupilo sa namerom ili grubom nepažnjom.

U Republici Srbiji su vrste osiguranja predviđene Zakonom o osiguranju. Imajući u vidu prirodu novčanih kazni koje bi mogle biti izrečene na osnovu Zakona o zaštiti podataka o ličnosti, verovatno bi ovi proizvodi osiguranja bili klasifikovani kao osiguranje od finansijskih gubitaka. Ovo bi, međutim, zavisilo

[23] Zakon o zaštiti podataka o ličnosti- ZZPL, *Službeni glasnik RS,* br. 97/08, 104/09 - dr. zakon, 68/12 - US i 107/12)

[24] Zakon o obligacionim odnosima, *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. 1/2003 - *Ustavna povelja* i *Službeni glasnik RS*, br. 18/2020, čl. 898, st. 1.

od tačne formulacije polise osiguranja i od toga da li se ona nudi kao zaseban proizvod osiguranja ili kao deo druge postojeće polise koja bi bila izmenjena tako da uključuje pokriće kazni predviđenih novom regulacijom i / ili srodnih finansijskih posledica.[25]

Iako u Srbiji ovo pitanje još uvek nije otvoreno ipak postojeće odredbe Zakona o obligacionim odnosima i Zakona o osiguranju bi mogle da posluže kao model regulacije ovog pitanja na nivou EU, a koje odredbe bi omogućavale osiguravajućem društvu da predvidi da polisa pokriva kazne, osim u slučaju da je do odgovornosti kompanije, došlo usled namere ili grube nepažnje.

5. Zaključak

Nova pravna regulativa u oblasti zaštite podataka o ličnosti, kako na nivou EU, tako i na teritoriji Republike Srbije unapređuje zaštitu lica čiji se podaci obrađuju, ali istovremeno predstavlja ogroman teret za kompanije. Kako je poslovanje putem interneta, čuvanje podataka na online platformama, kao i umrežavanje unutar kompanije, nešto bez čega se u današnje vreme poslovanje praktično ne može ni zamisliti, rizici od internet napada i krađe podataka postali su ogromni. Sa druge strane, ukoliko do krađe podataka dođe, a da kompanija nije ispoštovala sve protokole i odredbe predviđene novom regulativom, pa čak i nenamerno, pored štete koju mora da nadoknadi licima čiji su podaci ukradeni i ostalih troškova koje sa sobom nosi internet napad, biće izložena i ogromnim kaznama. Kao jedan vid zaštite od ovakve vrste napada javilo se osiguranje od internet rizika, za kojim je potražnja naglo porasla nakon donošenja novih odredbi. Međutim, pored toga što ovo osiguranje pokriva većinu troškova sa kojima se kompanija susreće prilikom internet napada postavilo se pitanje da li ono može pokriti i kazne predviđene novim odredbama. Ovakva mogućnost predstavljala bi ogroman motiv za zaključenje ove vrste osiguranja.

Tokom istraživanja došli smo do zaključka da ovo pitanje nije regulisano jednoobrazno, već zavisi od zemlje do zemlje i stava zakonodavca svake zemlje o tome da li kazne mogu biti obuhvaćene polisom osiguranja. Nadalje, čak i ako zakonodavstvo to dozvoljava ostavljena je sloboda osiguravajućim društvima da kreiraju polisu osiguranja i definišu osigurane rizike. Na ovaj način se još jednom stvara pravna nesigurnost i neujednačenost pravila koja se na kompanije koje su u obavezi da implementiraju nove odredbe primenjuje. U Direktivi se ne zauzima nikakva stav po ovom pitanju, dok sudska praksa još uvek nije dovoljno razvijena.

[25] Preparing for the Worst, Hoping for the Best – Can You Insure Your Business for GDPR Fines?, https://sog.rs/2020/06/15/preparing-for-the-worst-hoping-for-the-best-can-you-insure-your-business-for-gdpr-fines/, 30.06.2020.

Mišljenja smo da bi ovo pitanje, barem na nivou EU trebalo da bude regulisano na ujednačen način, te da bi trebalo omogućiti kompanijama da polisa osiguranja pokriva i kazne predviđene Direktivom izuzimajući slučajeve namere ili grube nepažnje, kao i uz preduzimanje mera za umanjenje moralnog hazarda (npr. učestvovanje u kazni, umanjenje premije za ostvaren dobar rezultat itd).

* * *

CYBER RISK INSURANCE AND NEW PERSONAL DATA PROTECTION REGULATION

Summary

The adoption of the GDPR and Law on Personal Data Protection of Serbia certainly represents a turning point in the collection, processing and storage of personal data. On the other hand, the development and increasing use of computers and the Internet, in addition to the huge benefits it brings us, such as saving time and money, also has certain risks. These risks relate primarily to internet attacks which are becoming more frequent and which can bring huge costs to the affected company. The aggravating circumstance for certain companies is the fact that they have data that have been collected and stored for years, and after the adoption of new regulation, it is necessary to determine the purpose of the collected data in a short time and categorize them in accordance with new provisions. In addition, companies are increasingly the target of internet attacks, which is becoming one of the leading business risks in the world, and in the event of personal data breach of employees or customers, they may find themselves in an unenviable situation. In that case, the costs that the company would have to cover, especially if the company is not fully compliant with the new regulation, would almost certainly lead it to bankruptcy. For these reasons, cyber risk insurance has appeared in highly developed countries, which aims to reduce the costs that would hit the company, because otherwise the collapse of the affected company would be almost certain.

In the first part of the paper, the authors briefly discuss the reasons for the adoption and importance of new regulations in the field of personal data protection, as well as difficulties encountered by companies in implementing new provisions, while the second part deals with the impact of these regulations on internet risk insurance and the controversy over whether this type of insurance can also cover the penalties the company incurs in the event of non-compliance with the new provisions.

Keywords: personal data, GDPR, cyber crime, insurance companies, personal data protection.