Vilniaus universiteto Teisės fakulteto
Privatinės teisės katedra

Dominyko Kulako,
V kurso, civilinės ir verslo teisės
studijų šakos studento

Kursinis darbas

Kibernetinių incidentų rizikos valdymas: bendrovių teisės aspektai

Vadovė: doc. dr. Lina Mikalonienė

Recenzentas: doc. dr. Paulius Miliauskas

Vilnius
2022

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojama kibernetinė rizika kylanti bendrovėms, nagrinėjami atskiri šios rizikos elementai bei galimi jos valdymo – mažinimo būdai. Darbe taip pat nagrinėjamos bendrovių vadovų pareigos, susijusios su bendrovės kibernetinio saugumo užtikrinimu bei šių pareigų prigimtis ir vadovų civilinės atsakomybės klausimai, susiję su netinkamu kibernetinio bendrovės saugumo užtikrinimu.

Pagrindiniai žodžiai: kibernetinis incidentas, vadovo pareigos, civilinė vadovo atsakomybė, bendrovių teisė, fiduciarinės pareigos, civilinė atsakomybė

This paper analyzes the cyber risk the companies are facing, examines the individual elements of this risk and possible ways to manage and reduce it. The study also looks into the responsibilities of the company executives related to ensuring the cyber security of the company, the nature of these responsibilities and the issues of civil liability of executives related to cyber security of the company.

Main words: cyber incident, executives duties, executives civil liability, company law, fiduciary duties, civil liability

TURINYS:

ĮVADAS

Nagrinėjamos temos aktualumas. Sparčiai plintant informacinių ryšių technologijų panaudojimui tiek viešajame, tiek privačiajame sektoriuose, proporcingai didėja ir neteisėtų prisijungimų, bandymų perimti, pakeisti ar kitaip neteisėtai paveikti duomenis, perduodamus informacinėje erdvėje. Vien per 2020 m. Lietuvoje buvo užfiksuota 4330 kibernetinių incidentų, tuo tarpu kibernetinių incidentų kiekis per metus (nuo 2019 m.) pakilo net ketvirtadaliu. Toks ženklus kibernetinių incidentų augimas gali būti paaiškinamas sparčiu verslo taikomų duomenų apdorojimo, gamybinių ir kitų procesų skaitmenizavimu, t.y. nuolat didėjant skaitmeniniu būdu tvarkomų duomenų kiekiams, atitinkamai didėja ir neteisėtų bandymų paveikti šiuos procesus. Pažymėtina, kad verslo sektoriaus „perkėlimą“ į skaitmeninę erdvę paskatino ir 2019 m. prasidėjusi Covid-19 pandemija. Nuolat didėjantis kibernetinių incidentų skaičius tiek Lietuvoje, tiek visame pasaulyje verčia verslininkus vis labiau susimąstyti valdomų bendrovių kibernetiniu saugumu. Atitinkamai, tikėtini ir nauji, iki šiol teismų dar nenagrinėti ginčai dėl bendrovių vadovų pareigų, susijusių su kibernetiniu bendrovės saugumu.

Darbo tikslas. Apibrėžti kibernetinę riziką kylančią bendrovėms, bei nustatyti, kokios pareigos, susijusios su kibernetinio bendrovių saugumo užtikrinimu, kyla bendrovių vadovams. O taip pat, nustatyti ar šios pareigos vykdymas gali būti pavedamas kitiems asmenims

Darbo uždaviniai. Darbo tikslui pasiekti keliami šie uždaviniai: 1) Atskleisti, kuo pasireiškia bendrovėms kylanti kibernetinė rizika; 2) Nustatyti, kokios pareigos susijusios su kibernetiniu saugumu kyla bendrovės vadovui bei atskleisti šių pareigų pobūdį; 3) Nustatyti, ar vadovas turi teisę pavesti kitiems asmenims vykdyti pareigas, susijusias su kibernetinio saugumo užtikrinimu bei išanalizuoti susijusius atsakomybės klausimus.

Objektas ir tyrimo metodai. Darbe nagrinėjama bendrovių vadovo pareiga užtikrinti kibernetinį bendrovės saugumą, bei vadovo teisė šias pareigas vykdyti kitiems asmenims. Siekiant atskleisti šios pareigos turinį ir kilmę, apibrėžiama, kibernetinė rizika kylanti bendrovėms, bei atskirai nagrinėjama pareiga užtikrinti kibernetinį saugumą kylanti: (i) bendrovių, kurioms kyla tam tikri papildomi reikalavimai susiję su kibernetiniu saugumu, vadovams; bei (ii) bendrovių, kurių kibernetinio saugumo nereglamentuoja papildomi teisės aktai, vadovams. Taip pat, pažymėtina, kad darbe nebus vertinamas techninių priemonių, išdėstytų Kibernetinio saugumo reikalavimų apraše, tinkamumas ir pakankamumas, kadangi išsamiam vertinimui atlikti reikalingos išsamios informacinių

technologijų ir kitos techninės kibernetinio saugumo žinios, kurios nėra susijusios su teisės fakultete dėstomomis disciplinomis.

Šio darbo tikslui siekti buvo naudojami šie metodai:

Sintezės metodas – analizuojant vadovo pareigas pasitelktas, siekiant apibendrinti ir, atsižvelgiant į esamą reguliavimą, suformuotą teismų praktiką bei teorinius šaltinius, apibrėžti bendrovės vadovo pareigos, užtikrinti kibernetinį saugumą, kilmę, turinį bei intensyvumą.

Aprašomasis metodas – buvo pasitelktas siekiant perteikti techninę, pareigos užtikrinti kibernetinį bendrovės saugumą, pusę. Taip pat perteikiant ir sisteminant įvairiuose šaltiniuose pateiktą techninę statistinę ir kitą medžiagą.

Lingvistinis metodas – buvo naudojamas analizuojant įvairius įstatymus, siekiant atskleisti jų normų reikšmę ir praktinį pritaikomumą.

Apibendrinimo ir analogijos – pasitelktas aiškinant ir taikant panašių ir susijusių institutų požymius ir jiems būdingus principus.

Darbo originalumas. Informacinių technologijų pažanga lemia naujų ir dar teisės kontekste nenagrinėtų klausimų atsiradimą bei kuria naują realybę, kuriai tampa aktualūs nauji, iki šiol teisės nenagrinėti institutai ar jų aspektai. Iki šiol, Lietuvos Respublikoje nebuvo nei vieno mokslinio darbo nagrinėjančio bendrovių kibernetinio saugumo temą.

Svarbiausi šaltiniai. Lietuvos Respublikos Civilinis Kodeksas, Lietuvos Respublikos akcinių bendrovių įstatymas, kibernetinio saugumo įstatymas, Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679 (Bendrasis duomenų apsaugos reglamentas), Lietuvos Aukščiausiojo Teismo praktika, įvairių užsienio teisės ir kibernetinio saugumo ekspertų straipsniai bei publikacijos, Lietuvos Respublikos krašto apsaugos ministerijos ir Nacionalinio kibernetinio saugumo centro leidiniai.

1. KIBERNETINĖS RIZIKOS SAMPRATA BENDROVIŲ TEISĖS KONTEKSTE

Nagrinėjant kibernetinius incidentus ir su jais susijusias bendrovių pareigas, visų pirma svarbu nustatyti, kas yra kibernetinių incidentų rizika bendrovių teisės kontekste (toliau ir **kibernetinė rizika**). Lietuvos Respublikos Kibernetinio saugumo įstatymas (Lietuvos Respublikos Kibernetinio saugumo įstatymas, TAR, 2014-12-23, Nr. 20553) (toliau **Kibernetinio saugumo įstatymas**) , yra specialusis įstatymas, kuriame apibrėžiami kibernetinio saugumo principai, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos, šių institucijų įgaliojimai kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigos, tarpinstitucinis bendradarbiavimas, ryšių ir informacinių sistemų spragų paieškos ir pranešimo apie jas ir kibernetinius incidentus pagrindai, taip pat nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijos ir įgaliojimai. Be kita ko, šiame įstatyme apibrėžiama ir kibernetinio incidento sąvoka. Kibernetinio saugumo įstatymo 2 str. 9 d. kibernetinį incidentą apibrėžia kaip įvykį ar veiką kibernetinėje erdvėje[1], galintį sukelti arba sukeliantį grėsmę, arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintis trikdyti arba trikdantis ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą. Kibernetinio saugumo įstatymas duodą gerą atspirties tašką apibrėžiant kibernetines rizikas bendrovių teisės kontekste, t.y. šis įstatymas išskiria tam tikras sritis, kurios gali būti pažeistos įvykus kibernetiniam incidentui.

Vertinant kibernetines rizikas, svarbu atsižvelgti į jų specifiką ir nuolatinį kitimą bei dažniausiai pasitaikančių kibernetinių incidentų rūšis. Krašto apsaugos ministerija 2020-ųjų metų Nacionalinėje Kibernetinio saugumo būklės ataskaitoje nurodo, kad didžiausią grėsmę asmenų skaitmeniniam turtui kelia duomenis šifruojanti ir išpirkos reikalaujanti kenkimo programinė įranga (angl. *ransomware*), ryšių ir informacinėmis sistemomis teikiamų paslaugų trikdymas (angl. *distributed denial of service (DDoS)* atakos), duomenų vagystės (angl. *phishing*), kitokio pobūdžio sukčiavimas internete. 2020 m. didžiausią nusikalstamų veikų kibernetinėje erdvėje dalį (virš 90 proc.), kaip ir 2019 m., sudarė elektroninis sukčiavimas, neteisėtas prisijungimas prie informacinės sistemos ir neteisėtas elektroninių duomenų perėmimas ir panaudojimas. <...> Lietuvos bankų

[1] Kibernetinė erdvė – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija (Kibernetinio saugumo įstatymo 2 str. 6 d.).

asociacijos duomenimis, 2020 m. elektroninių sukčių Lietuvoje gyventojams padaryta žala perkopė 4,5 mln. eur. <...> dažniausiai vykdė socialine inžinerija pagrįstas duomenų vagystes. Taip pat pažymėtina, kad vienas sparčiausiai plintančių sukčiavimo internete būdų – investicinis sukčiavimas, sukeliantis didžiulių nuostolių. (Krašto apsaugos ministerija, 2020. NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA 2020). Kibernetinio saugumo specialistai nurodo, kad kasdien sukuriama apie 230 000 naujų kenkėjiškų programų pavyzdžių (Purplesec, 2021. Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends [interaktyvus, žiūrėta 2022-04-06]. Prieiga per internetą: https://purplesec.us/resources/cyber-security-statistics/) Taigi, galime matyti, kad kibernetinių incidentų spektras, iš tiesų, yra labai platus, be to, nuolat didėjantis. Atsižvelgiant į nuolat didėjantį kibernetinių rizikų spektrą ir kenkėjiškos programinės įrangos tobulėjimą, kibernetinio saugumo specialistai, teisininkai, draudimo rizikų vertintojai ir kt. pradėjo naudoti *nulinės dienos pavojaus* sąvoką (angl. *zero day theat*), kuri naudojama apibūdinti tam tikrą kenkėjišką programą, kuri iki šiol dar nebuvo aptikta ir neatitinka jokių žinomų kenkėjiškų programų aprašų. Kibernetinio saugumo specialistai TrendMicro nurodo, kad pasitaiko ir tokių situacijų, kai tam tikrą kibernetinio saugumo spragą atradę subjektai parduoda informaciją apie šią spragą kibernetinio saugumo nusikaltėliams. Pastarieji bando pasipelnyti pasinaudodami spraga, kol ji nėra užfiksuojama ir išleidžiami tam tikri sistemos atnaujinimai, kurie užkardo tolimesnį kibernetinio saugumo spragos išnaudojimą (TrendMicro. CAN YOU BE READY FOR A YOU DON'T KNOW ABOUT? The Art of Zero-Day Threat Coverage [interaktyvus. Žiūrėta: 2022-03-28]. Prieiga per internetą: https://resources.trendmicro.com/rs/945-CXD-062/images/Trend-Micro_eBook_The-Art-of-Zero-Day-Threat-Coverage.pdf). Taigi, vien atskirtos nulinės dienos pavojaus sąvokos buvimas parodo informacinių ryšių ir kibernetinių technologijų diktuojamą vystymosi tempą, kuriam atitinkamą atsaką turi pateikti ir valstybių teisinės sistemos, kuriose veikiantys viešieji ir privatieji subjektai nuolat susiduria su kibernetiniais incidentais bei tam tikru būdu valdo jų rizikas. Kibernetinių incidentų neišvengiamumą dar 2012 m. vykusios RSA kibernetinio saugumo konferencijos metu yra pabrėžęs ir Jungtinių Amerikos Valstijų federalinių tyrimų biuro vadovas Robert Mueller teigdamas, kad „yra dviejų tipų bendrovės: tos, į kurių informacinių technologijų ir ryšių sistemas jau buvo įsilaužta ir tos, į kurių dar bus įsilaužta" (Robert Mueller kalba per 2012 m. RSA kibernetinio saugumo konferenciją [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą:

https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies).

Apibrėžiant kibernetinę riziką ir nagrinėjant kitus kibernetinio saugumo klausimus, verta išskirti ir specialiuosius, Kibernetinio saugumo įstatyme įtvirtintus, kibernetinio saugumo principus. Iš esmės, šie principai taikytini Kibernetinio saugumo įstatyme apibrėžtiems kibernetinio saugumo subjektams, tačiau Kibernetinio saugumo įstatymo 16 str. 1 d. įtvirtina visų asmenų teisę savanoriškai pranešti apie kibernetinius incidentus jų valdomose ryšių ir informacinėse sistemose. Atitinkamai NKSC tokius pranešimus tvarko pagal Nacionaliniame kibernetinių incidentų valdymo plane[2] (Nutarimas dėl kibernetinio saugumo strategijos patvirtinimo) nustatytą tvarką. Taigi, tokiu būdu įstatymų leidėjas išplečia kibernetinį saugumą reguliuojančių teisės aktų pritaikomumą, t.y. šie teisės aktai gali būti taikomi praktiškai visiems subjektams (tame tarpe ir bendrovėms, nepriklausomai nuo vykdomos veiklos pobūdžio), kurie gali būti paveikti kibernetinių incidentų. Minėtieji kibernetinio saugumo principai yra įtvirtinti Kibernetinio saugumo įstatymo 3 str. Jame nustatomi pagrindiniai principai, kuriais grindžiamas kibernetinis saugumas, t.y.: (i) kibernetinės erdvės nediskriminavimo principas – pagal šį principą teisiniai gėriai kibernetinėje erdvėje turi būti saugomi tokia pat apimtimi kaip ir teisiniai gėriai fizinėje erdvėje. Šis principas parodo įstatymų leidėjo požiūrį ir ypatingą svarbą, teikiamą naujai atsirandančių technologijų reiškiniams, tačiau taip pat ir valią reguliuoti kibernetinėje erdvėje vykstančius reiškinius; (ii) kibernetinio saugumo rizikos valdymo principas – kibernetinio saugumo rizika turi būti nuolat vertinama bei atitinkamai turi būti imamasi reikiamų saugumo priemonių. Detalesnė šio principo reikšmė ir susijusios subjektų pareigos detalizuojamos Nutarime dėl kibernetinio saugumo strategijos. Apibendrintai galima teigti, kad šis principas įpareigoja Kibernetinio saugumo subjektus periodiškai vertinti kibernetinio saugumo riziką ir atlikti kitus susijusius veiksmus; (iii) kibernetinio saugumo proporcingumo principas – saugumo priemonės neturi, iš esmės, riboti subjektų veiklos daugiau, negu tai yra būtina siekiant užtikrinti saugumą kibernetinėje erdvėje. Nors galėtumėme sakyti, kad tai ir yra bendrasis teisinis principas, tačiau įstatymų leidėjas jam suteikia ypatingą svarbą, kadangi kibernetinio saugumo reikalavimų apimtis priklauso nuo subjekto vykdomos veiklos. Būtų neprotinga iš nedidelės parduotuvėlės reikalauti įsidiegti pažangiausias saugumo technologijas, kurių įdiegimas ir palaikymas gali kainuoti net daugiau nei atitinkamas verslo subjektas uždirba. Todėl, ypatingas dėmesys turi būti

[2] Nacionalinis kibernetinių incidentų valdymo planas nustato kibernetinių incidentų kategorijas, informavimo apie kibernetinius incidentus, kibernetinių incidentų tyrimo ir kibernetinių incidentų analizės baigus kibernetinių incidentų tyrimą tvarką, valdant kibernetinius incidentus.

skiriamas konkretaus subjekto veiklos vertinimui; (iv) viešojo intereso viršenybės principas – nepažeidžiant atskirų vartotojų teisių, turi būti užtikrinama viešojo intereso apsauga. Dėl plataus subjektų, kuriuos jungia informacinių ir ryšių technologijų tinklai, pavienių subjektų interesai negali ir neturėtų būti keliami bendrų – viešųjų interesų. (v) standartizacijos ir technologinio neutralumo principas – įgyvendinant kibernetinio saugumo priemones, subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės. Šio principo įtvirtinimas yra sveikintinas, ypač, atsižvelgiant į nuolatinį informacinių technologių tobulėjimą, kadangi įstatymų leidėjas neturėtų galimybės eiti koja kojon su naujausiomis technologijomis, bei nurodyti, kokią konkrečią programinę įrangą privalo būti įsidiegę tam tikri subjektai. Šiuo atveju pažymėtina, kad kibernetinio saugumo klausimai Europos Sąjungos lygmenyje paprastai yra reglamentuojami tam tikromis gairėmis, kurios priskirtinos negriežtosios teisės (angl. *soft law*) šaltiniams, kurių laikymasis ar atitikimas keliamiems standartams paprastai nėra privalomas. (vi) subsidiarumo principas - už ryšių, informacinių sistemų bei jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas jomis teikiantys subjektai. Autoriaus nuomone, šis sistemas valdančių ir paslaugas teikiančių subjektų atsakomybės klausimas, kelia nemažai abejonių, kadangi numatant tokį reguliavimą, šalys praranda galimybę apsibrėžti savo teises ir prisiimamas pareigas ir riziką (pvz. sudarant tam tikras informacinių technologijų paslaugų teikimo sutartis), kadangi įstatymas įpareigoja subjektus atsakyti subsidiariai. Tuo pačiu galimi ir prieštaravimai kitiems teisinės valstybės principams. Įtvirtinus šį principą galime įžvelgti griežtą įstatymų leidėjo toną, kuris liečia klausimus susijusius su kibernetiniu saugumu, t.y. įtvirtindamas tokį principą, įstatymų leidėjas aiškiai leidžia suprasti, kad kiekvienas susijęs subjektas privalės atsakyti už kibernetinio saugumo spragas, taip įtvirtinant „nulinę kibernetinių saugumo pažeidimų toleranciją“. Apibendrinant, vertėtų paminėti ir tai, kad nei vienam iš nurodytų principų nėra teikiama pirmenybė prieš kitus, o visi principai turi būti aiškinami *in corpore*, bei derinami tarpusavyje.

Atsižvelgiant į Kibernetinio incidento įstatyme pateikiamus rizikos ir kibernetinio incidento apibrėžimus, kibernetinių incidentų rizika bendrovių teisės kontekste galėtų būti apibrėžta, kaip tikimybė, kad konkrečioje bendrovėje, atsižvelgiant į jos (ne)naudojamas kibernetinio saugumo priemones, įvyks kibernetinis incidentas, kuris sukels žalą bendrovei ar tretiesiems asmenims. Svarbi kibernetinės rizikos valdymo dedamoji yra bendrovės kibernetinio saugumo užtikrinimas ir tam pasitelktos priemonės, įrankiai ar sprendimai,

vykdomi procesai. Nagrinėjant kibernetinius incidentus, būtina atsižvelgti ir įvertinti, ar atsakingi asmenys ėmėsi visų būtinų ir protingų priemonių, kad kibernetinio saugumo rizikos būtų tinkamai identifikuotos, galimybės kilti kibernetiniams incidentams minimizuojamos (iki bendrovės toleruojamo lygio), o įvykus incidentui mažinti jo padarinius ir imtis kitų veiksmų susijusių su kibernetinio incidento padarinių šalinimo organizavimu, o taip pat, informuoti atitinkamas valstybines institucijas. Klasifikuojant kibernetinės rizikos objektą pagal CK 1.97 str. 1 d., galime teigti, kad kibernetinės rizikos objektu turėtų būti laikoma informacija saugoma bendrovių duomenų bazėse ar kitose skaitmeninėse laikmenose. Praktiškai kibernetinės rizikos objektas galėtų apimti įvairių formų neigiamą įtaką bendrovės vykdomai ūkinei komercinei veiklai bei bendrovės sutartinių ir įstatymais nustatytų pareigų vykdymui.

Kibernetinė rizika bendrovių kontekste, kaip ir dauguma kitų institutų, gali būti klasifikuojama pagal kriterijus. Atsižvelgiant į tai, kad Lietuvos Respublikos ir užsienio teisės aktai, doktrina ir kita literatūra nepateikia aiškių kriterijų, pagal kuriuos galėtų būti apibrėžta kibernetinė rizika bendrovių teisės kontekste, toliau autorius pateikia keletą kriterijų, pagal kuriuos galėtų būti skirstoma ir detaliau nagrinėjama kibernetinė rizika, kylanti bendrovėms.

Vienas iš galimų kibernetinės rizikos skaidymo ar detalizavimo variantų, galimas pagal subjektą, kuriam kyla žala įvykus kibernetiniam incidentui. Tokiu atveju, autorius siūlytų kibernetinę riziką skirstyti į tokius elementus:

i) **Žalą kylančią pačiai bendrovei**

Žalą kylančią pačiai bendrovei paprastai sudaro dar bent keletas savarankiškų elementų, t.y.:

a**) žala kylanti praradus bendrovės veiklai svarbią informaciją** (pvz.: komercinę paslaptį, konfidencialią ar kt. informaciją). Kaip jau buvo nurodyta NKSC kibernetinio saugumo būklės ataskaitoje, kibernetiniai incidentai gali pasireikšti įvairiomis formomis, tačiau vieną didžiausių pavojų ir toliau kelia duomenis šifruojanti ir išpirkos reikalaujanti kenkimo programinė įranga (angl. *ransomware*). Tokio kibernetinio išpuolio metu yra užšifruojami bendrovės kompiuteriuose ir/ar net serveriuose/debesijoje esantys duomenys. Tokiu būdu bendrovė bent tam tikram laikui (kol/jei duomenys buvo saugomi išorinėse laikmenose ir gali būti atkurti) netenka prieigos prie jautrios klientų, darbuotojų, techninės ar kitos informacijos. Tačiau tai tik viena medalio pusė, įsilaužėlių naudojančių *ransomware* tikslas, apribojus informacijos valdytojo prieigą prie tam tikrų duomenų, už jų (galimai tariamą) atkodavimą gauti tam tikrą išpirką. Paveiktos bendrovės kompiuteriuose paprastai atsiranda tekstas, kuriuo įsilaužėliai reikalauja sumokėti tam tikrą

pinigų sumą (dažnu atveju suma gali būti net neatskleidžiama, tačiau bendrovei tampa žinoma tik susisiekus su įsilaužėliais), taip pat pažymėtina, kad beveik visada reikalaujama atsiskaityti Bitcoin ar kita elektronine valiuta. Pasitaiko atvejų, kai įsilaužėliai, siekdami užtikrinti savo saugumą ir susirašinėjimo slaptumą, susisiekimui su jais reikalauja naudoti atvirojo kodo TOR naršyklę skirtą informacijai anonimiškai siųsti ir gauti internetu, ar nurodo komunikacijai naudoti tam tikrą konkrečią elektroninio pašto dėžutę, kurią palaiko konfidencialumą garantuojantys elektroninio pašto paslaugų teikėjai. Įvykus tokiam kibernetiniam incidentui, bendrovėms rekomenduotina susilaikyti nuo įsilaužėlių reikalaujamos išpirkos sumokėjimo, kadangi net sumokėjus išpirką, negaunama jokių garantijų, kad duomenys bus saugiai atkoduoti pilna apimtimi ir/ar nebus kopijuojami ar perkeliami. Tokias rekomendacijas teikia ir dauguma teisininkų bei verslo konsultantų (pvz.: Gartner, 2021. When it Comes to Ransomware, Should Your Company Pay? [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://www.gartner.com/en/articles/when-it-comes-to-ransomware-should-your-company-pay), kibernetinio saugumo specialistų (pvz.: Kyle Johnson, 2021. Should companies pay after ransomware attacks? Is it illegal? [interaktyvus, žiūrėta 2022-04-03]. Prieiga per internetą: https://www.techtarget.com/searchsecurity/tip/Should-companies-pay-ransomware-and-is-it-illegal-to) ir valstybinių institucijų (pvz.: NKSC, 2021. Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) įspėja apie pavojingų „ransomware“ tipo virusų suaktyvėjimą [interaktyvus, žiūrėta 2022-04-05]. Prieiga per internetą: https://www.nksc.lt/naujienos/demesio_plinta_virusai_uzsifruojantys_failus.html; Nacionalinis JK kibernetinio saugumo centras, 2020. Mitigating malware and ransomware attacks [interaktyvus, žiūrėta 2022-04-05]. Prieiga per internetą: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks) Taigi, nors vertinant žalą kylančią pačiai bendrovei nereiktų pamiršti ir aptartos išorinės žalos, susijusios su išpirkos reikalavimu, tačiau ne mažiau svarbūs gali būti ir patys duomenys, kurie yra prarandami/užkoduojami, ir t.t. Pavyzdžiui bendrovė vykdanti tam tikrą veiklą praradusi naudojamus brėžinius ar kitą techninę informaciją vargu ar galėtų sėkmingai tęsti pelningą veiklą, jei šie duomenys negalėtų būti atkurti pasitelkiant protingus kaštus. Taip pat, pažymėtina ir bendrovės veiklai ypač svarbi reputacinė žala. Tikėtina, kad potencialūs bendrovės klientai ir kontrahentai vengtų bendrovės nesirūpinančios savo informacinių technologijų sistemų saugumu.

b) **žalą kylančią dėl bendrovės veiklos nutraukimo ar laikino sustabdymo**. Daugumos kibernetinių incidentų atveju, bendrovių veikla sutrikdoma iki tokio lygio, kai bendrovė nebegali tęsti savo vykdomos ūkinės komercinės veiklos, kadangi įsilaužėliai apriboja prieigą prie tam tikrų duomenų bazių (jos gali būti ir užšifruojamos). Taip pat, galima rizika, kad tęsiant veiklą gali būti paveikta ir didesnė dalis kompiuteriuose esančių duomenų ar įsilaužėliai pašalins duomenis dėl atsisakymo su jais bendradarbiauti. Todėl galima teigti, kad įvykus kibernetiniam incidentui, yra didelė rizika, kad bendrovei teks stabdyti savo veiklą ar tam tikrą laiką (kol kibernetinis incidentas bus suvaldytas) ją vykdyti mažiau kompiuterizuotu būdu, jei tai įmanoma, atsižvelgiant į bendrovės vykdomą ūkinę komercinę veiklą. Nepaisant to, tikėtina, kad įvykus kibernetiniam incidentui, bendrovė patirs nuostolių dėl negautų pajamų;

c) kaip netiesioginė bendrovei kylanti žala gali būti įvardijami ir trečiųjų asmenų ieškiniai dėl žalos atlyginimo (t.y. juose keliami reikalavimai bendrovei), tačiau plačiau apie trečiųjų asmenų patiriamą žalą žr. sekančiame punkte.

ii) **Žalą kylančią kitiems asmenims**

Priklausomai nuo bendrovės vykdytos veiklos, tretieji asmenys, patyrę tam tikrą žalą, gali būti tiek fiziniai asmenys (pvz. vartotojai, kurių duomenis valdė bendrovė), tiek ir juridiniai asmenys (pvz. nuo kibernetinio incidento nukentėjusios bendrovės verslo partneriai ar kontrahentai).

Viena jautriausių duomenų kategorijų – tai asmens duomenys. Galime konstatuoti, kad pastaruoju metu, ženkliai išaugus kompiuterinių technologijų panaudojimui, didelė dalis bendrovių yra asmens duomenų valdytojos. Taigi įvykus kibernetiniam incidentui tokioje bendrovėje, kyla pavojus ir bendrovės valdomiems duomenims. Nepaisant to, kad asmenys, kurių asmens duomenys buvo prarasti ar kitaip paveikti kibernetinio incidento, turi teisę kreiptis dėl turtinės ir neturtinės žalos atlyginimo ieškinio tvarka, Lietuvos Respublikos teisės aktai numato galimybę teikti ir grupės ieškinį.

Kaip jau buvo minėta, kiti duomenys, kurie gali būti prarandami kibernetinio incidento metu bei sukelti žalą tretiesiems asmenims, yra konfidenciali informacija, kurią bendrovei patikėjo jos kontrahentai, pvz. tam tikri sandorio elementai, kaip kaina, vykdymo terminas, ar kita informacija, kurią šalys sutartyse apibrėžė kaip konfidencialią.

Kibernetinio saugumo reikalavimų apraše (Nacionalinis kibernetinių incidentų valdymo planas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“ (toliau - **Nutarimas dėl kibernetinio saugumo strategijos patvirtinimo**)) (plačiau žr. 2.2. dalyje)

numatoma kibernetinės rizikos vertinimo tvarka, kuri grindžiama grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus. Kibernetinio saugumo subjektai[3], organizuodami ryšių ir informacinių sistemų rizikos vertinimą yra įpareigoti: (i) paskirti už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingą asmenį arba asmenis ir nustatyti jiems taikomus kvalifikacinius reikalavimus; (ii) nustatyti reikalavimus rizikos vertinimo procesui, rizikos išdėstymo pagal prioritetus kriterijus ir apibrėžti priimtiną rizikos lygį[4]; (iii) nustatyti grėsmes ir pažeidžiamumus, galinčius turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, ir nustatyti galimo grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritis; (iv) įvertinti ryšių ir informacinių sistemų pažeidimo grėsmių tikimybę ir pasekmes, nustatyti rizikos lygį, įvertinti identifikuotas grėsmių tikimybes ir jas išdėstyti prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą; (v) Aprašo nustatyta tvarka, atsižvelgiant į atliktą rizikos vertinimą, rengti ir peržiūrėti patvirtintus teisės aktus, reglamentuojančius valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo politiką ir jos įgyvendinimą, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisykles, paslaugų kibernetinio saugumo valdymo taisykles, ir nustatyti, kuriuos ,iš juose nustatytų kibernetinio saugumo reikalavimų, būtina atnaujinti ir (ar) įgyvendinti pirmiausia, siekiant užtikrinti ryšių ir informacinių sistemų kibernetinį saugumą. Šiame apraše taip pat pabrėžiama, kad organizuojant ryšių ir informacinių sistemų rizikos vertinimą, rekomenduojama vadovautis Lietuvos Respublikos ir tarptautiniais standartais ar metodikomis (plačiau apie kibernetinio saugumo standartų taikymą žr. 2.1. dalyje),

[3] **Kibernetinio saugumo subjektas** - subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas (Kibernetinio saugumo įstatymo 2 str. 8 d.). Šio darbo kontekste, darytina išvada, kad bendrovėms, atitinkančioms Kibernetinio saugumo subjektų apibrėžimą taikomas papildomos įstatyme numatytos pareigos susijusios su kibernetinio saugumo užtikrinimu.

[4] Kibernetinio saugumo ekspertai paprastai pabrėžia, kad praktiškai neįmanoma užtikrinti šimtaprocentinio kibernetinio saugumo, taigi subjektai yra priversti nuolat toleruoti tam tikrą riziką. Šį argumentą patvirtina ir Krašto apsaugos ministerija bei NKSC pabrėždamas, kad kibernetinis saugumas nėra baigtinis procesas ir jokia įmonė negali užtikrinti visiško atsparumo kibernetinėms grėsmėms (Krašto apsaugos ministerija, NKSC, 2020. KIBERNETINIS SAUGUMAS IR VERSLAS Ką turėtų žinoti kiekvienas įmonės vadovas [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://kam.lt/download/68737/kibernetinio%20saugumo%20vadovas%20verslui.pdf).

reglamentuojančiais rizikos valdymą, ir įtraukti ryšių ir informacinių sistemų rizikos vertinimą į kibernetinio saugumo subjektų veiklos rizikos vertinimo procesus.

Taigi, atsižvelgiant į tai kas buvo išdėstyta šioje darbo dalyje, galime daryti išvadą, kad kibernetinė rizika bendrovių teisės kontekste, yra tam tikra tikimybė, kad bendrovė patirs kibernetinį incidentą (kuris atitinkamai sukels neigiamus padarius bendrovei ir kitiems asmenims). Būtina pabrėžti, kad šios rizikos vertinimas praktikoje yra ypač sudėtingas, kadangi ir pati rizika gali būti vadinama „tarpdisciplinine“. Apsibrėžus šią riziką ir kitus su ja susijusius klausimus, galima pereiti prie bendrovių vadovų pareigų, susijusių su bendrovių kibernetinės erdvės apsauga, analizės.

2. BENDROVĖS VADOVO PAREIGA UŽTIKRINTI KIBERNETINĮ SAUGUMĄ

Šioje darbo dalyje bus nagrinėjamos bendrovės vadovo pareigos, susijusios su kibernetiniu bendrovės saugumu, šių pareigų apimtis bei iš šių pareigų nevykdymo ar netinkamo vykdymo kylančios pasekmės. Siekiant aiškumo, bus išskirti keli atvejai, t.y.: (i) kai bendrovė nepriklauso tam tikram specifiškai reguliuojamam sektoriui (pvz. tam tikra bendrovė užsiimanti įprasta ūkine komercine veikla, kuri nėra papildomai reguliuojama Lietuvos Respublikoje); (ii) kai bendrovė priklauso tam tikram reguliuojamam sektoriui (pvz.: sveikatos priežiūros, finansų, ir t.t.).

Vadovo atsakomybės klausimo analizę vertėtų pradėti nuo vadovo atsakomybės pobūdžio, kurį būtina apibrėžti konkrečiu darbe nagrinėjamu atveju dėl Lietuvos Aukščiausiojo Teismo nustatyto, vadovo teisinio statuso prigimties dualizmo. Kadangi ABĮ 37 str. 1 dalyje nustatyta, jog bendrovės vadovas yra vienasmenis bendrovės *valdymo* organas, o pagal ABĮ 37 str. 4 dalį toks yra įmonės *darbuotojas,* nes su juo sudaroma darbo sutartis (Lietuvos Aukščiausiojo Teismo 2008 m. gegužės 12 d. nutartį, priimtą civilinėje byloje Nr. 3K-3-267/2008). Vadovas laikytinas ne tik juridinio asmens darbuotoju, tačiau ir juridinio asmens vienasmeniu valdymo organo nariu, kurio pareigos numatytos Civilinio kodekso, kitų norminių teisės aktų, juridinio asmens įstatuose. CK 2.87 str. 7 dalyje įtvirtinta juridinio asmens *valdymo* organo nario (nagrinėjamu atveju - vadovo), nevykdančio arba netinkamai vykdančio savo pareigų, nurodytų CK 2.87 str. ar steigimo dokumentuose, prievolė padarytą žalą atlyginti juridiniam asmeniui visiškai, jei įstatymai, steigimo dokumentai ar sutartis nenumato kitaip. Tai, kad vadovą ir bendrovę sieja civiliniai teisiniai santykiai, reiškia, jog bendrovės vadovo civilinė atsakomybė bendrovei neribojama materialinės atsakomybės taisyklėmis, jei jis padaro žalą vykdydamas valdymo

funkciją, t. y. pažeisdamas jam, kaip valdymo organui, civiliniuose įstatymuose nustatytas pareigas. Kiekvienu konkrečiu atveju, bendrovės vadovui taikytinos atsakomybės rūšis nustatoma atsižvelgiant į vadovo veiksmo, sukėlusio žalą, pobūdį ir pažeistų pareigų rūšį – jei vadovas padaro žalos veikdamas pagal savo, kaip valdymo organo, kompetenciją, jis pažeidžia jam, kaip valdymo organui, o ne darbuotojui nustatytą pareigą, todėl jam taikoma civilinė atsakomybė. (Lietuvos Aukščiausiojo Teismo 2016 m. birželio 3 d. nutartis, priimta civilinėje byloje Nr. 3K-3-298-701/2016). Taigi, vertinant vadovo pareigas užtikrinti kibernetinį saugumą, bei atsižvelgdami anksčiau nurodytus vadovų pareigų pagrindus, galime teigti, kad, vadovo pareigos užtikrinti kibernetinį saugumą kyla iš civilinių, o ne darbo santykių, todėl už vadovo pareigos užtikrinti kibernetinio saugumo nevykdymą ar netinkamą vykdymą vadovui kyla civilinė atsakomybė.

Šio darbo 2.1. ir 2.2. dalyse, siekiant atskleisti bendrovių ir jų valdymo organų pareigas kylančias bendrovėms veikiančioms tam tikruose reguliuojamuose bei nereguliuojamuose sektoriuose, bus detaliau nagrinėjami atskiri bendrovių, jų valdymo organų pareigų ir atsakomybės atvejai ir šių pareigų kilmės klausimai.

2.1. Bendrovės vadovo pareiga užtikrinti kibernetinį bendrovės saugumą nereguliuojamuose sektoriuose

Šioje dalyje bus analizuojamos bendrosios bendrovių pareigos, susijusios su kibernetinio saugumo užtikrinimu, t.y. nebus vertinamas specialusis reguliavimas, taikomas tik tam tikroje sferoje, konkrečioje srityje veikiančioms bendrovėms ir / ar taikomas tik Kibernetinio saugumo subjektams. Vertinant atsakomybę, kylančią už kibernetinius incidentus, visų pirma svarbu nustatyti: (i) ar bendrovėms bei jų valdymo organams kyla specifinės pareigos užtikrinti kibernetinį saugumą; (ii) jeigu būtų nustatyta, kad pareiga užtikrinti kibernetinį saugumą kyla, svarbu nustatyti, kas yra atsakingas už tinkamą šių pareigų vykdymą, t.y. ar ši pareiga keliama pačioms bendrovėms ar atitinkamiems jų valdymo organams bei koks yra šios pareigos turinys.

Paprastai, bendrovių teisėje bendrovės organų teisės ir pareigos suvokiamos pagal jų apimtį, numatytą Lietuvos Respublikos akcinių bendrovių įstatymo (Lietuvos Respublikos akcinių bendrovių įstatymas, Valstybės žinios, 2000-07-31, Nr. 64-1914) (toliau - **ABĮ**) 20 (Visuotinio akcininkų susirinkimo kompetencija), 32 (Stebėtojų tarybos kompetencija ir sprendimų priėmimas), 34 (Valdybos kompetencija) ir 37 (Bendrovės vadovas) str. bei Lietuvos Respublikos Civilinio Kodekso (Lietuvos Respublikos Civilinis Kodeksas, Valstybės žinios, 2000-09-06, Nr. 74-2262) (toliau - **CK**) 2.87 str., kuriame

numatomos bendrovės valdymo organų fiduciarinės pareigos. Pažymėtina, kad pagal ABĮ 37 str. 8 dalį, bendrovės vadovas organizuoja kasdieninę bendrovės veiklą, pagal ABĮ 37 str. 12 d. 1 p., bendrovės vadovas yra atsakingas už bendrovės veiklos organizavimą bei jos tikslų įgyvendinimą.

Pradedant nagrinėti konkrečius vadovų civilinės atsakomybės klausimus, tikslinga būtų pradėti nuo konkrečių Lietuvos Respublikos teisės aktų nuostatų, apibrėžiančių bendrovės organų pareigas ir atsakomybę. CK 2.82 str. 3 d. numato, kad valdymo organas atsako už juridinio asmens dalyvių susirinkimo sušaukimą, pranešimą juridinio asmens dalyviams apie esminius įvykius, turinčius reikšmės juridinio asmens veiklai, juridinio asmens veiklos organizavimą, juridinio asmens dalyvių apskaitą, bei kitus veiksmus, nurodytus CK 2.4 str. 3 dalyje <...>, tuo tarpu CK 2.4 str. 3 dalyje nurodyta, kad kiekvienas asmuo, kuris verčiasi verslu ar profesine veikla, privalo tvarkyti savo turtą ir visą kitą, kas susiję su jo verslu ar profesine veikla, taip pat saugoti dokumentus ir kitą informaciją apie savo turtą, verslą ar profesinę veiklą taip, kad kiekvienas turintis teisinį interesą asmuo bet kada galėtų gauti visapusišką informaciją apie to asmens turtines teises ir pareigas. Taigi, iš šios CK normos galime daryti išvadą, kad juridinio asmens valdymo organai atsako už tinkamą, informacijos susijusios su vykdomu verslu, saugojimą. Kitą vertus, toliau matome, kad minimame straipsnyje numatyta saugoti su verslu susijusią informaciją yra siejama su šios informacijos atskleidimu teisinį suinteresuotumą turintiems asmenims „<...> kad kiekvienas turintis teisinį interesą asmuo bet kada galėtų gauti visapusišką informaciją apie to asmens turtines teises ir pareigas“, taigi darbo autoriaus nuomone, šios normos tikslas nėra informacijos apsaugos nuo neteisėto trečiųjų asmenų poveikio užtikrinimas, bet greičiau bendrovės pareiga saugoti su vykdoma ūkine komercine veikla susijusius dokumentus (pvz.: pirkimą patvirtinančius finansinius dokumentus, sudarytas sutartis ir t.t.) ir tinkamai tvarkyti bendrovės apskaitą. Ši vadovo pareiga galėtų būti priskirta prie priemonių siekiant išvengti žalos pačiai bendrovei[5]. Taigi, darytina išvada, kad CK eksplicitiškai nenumato bendrovių ar jų organų pareigos užtikrinti kibernetinį saugumą.

ABĮ detalizuoja akcinių bendrovių valdymo organų pareigas. Tačiau, išanalizavus ABĮ 37 str. 12 dalį numatančią bendrovės vadovo pareigas, galime daryti išvadą, kad ABĮ taip pat, eksplicitiškai neįpareigoja vadovo rūpintis bendrovės informacinių technologijų ir ryšių perdavimo sistemų saugumu. Kita vertus, ABĮ numato bendrovės vadovo pareigą organizuoti bendrovės veiklą bei jos tikslų įgyvendinimą, todėl reikėtų įvertinti, ar

[5] kaip tai buvo apibrėžta ir paaiškinta šio darbo 1. dalyje.

bendrovės veiklos organizavimas neturėtų apimti ir kibernetinio saugumo organizavimo ir užtikrinimo. Taigi, darbo autoriaus nuomone, tais atvejais, kai teisės aktuose bendrovei eksplicitiškai nėra nustatoma pareiga užtikrinti tam tikro lygio kibernetinį saugumą, manytina, kad šią pareigą turėtų vykdyti vadovas, vykdydamas aukščiau paminėtas jam priskirtas pareigas, kadangi dažnu atveju (pažymėtina: kai bendrovė naudoja kompiuterines sistemas ir jos yra ypač svarbi bendrovės veiklos organizavimui, pvz. vykdoma e-prekyba, ar teikiamos skaitmeninės paslaugos) neužtikrinus kibernetinio saugumo, bendrovės veikla gali būti nutraukta ar bendrovė gali patirti ženklius nuostolius. Kibernetinis saugumas po truputį tampa neatsiejama verslo gyvybingumo ir plėtros dalimi. Kibernetinio incidento padariniai bendrovėms gali būti itin skaudūs, kartais net lemtingi (ypač smulkioms ar vidutinėms bendrovėms) verslo pranašumui ar tęstinumui. NKSC ir Krašto apsaugos ministerijos duomenimis, net 3 iš 4 smulkiojo ir vidutinio verslo vadovų sutinka, kad kibernetinis saugumas jų įmonei yra svarbus. (Krašto apsaugos ministerija, NKSC, 2020. KIBERNETINIS SAUGUMAS IR VERSLAS Ką turėtų žinoti kiekvienas įmonės vadovas [interaktyvus]. Prieiga internete: https://kam.lt/download/68737/kibernetinio%20saugumo%20vadovas%20verslui.pdf [žiūrėta 2022-04-01]). Todėl, šiame darbe yra koncentruojamasi būtent į vadovo, kaip vienasmenio valdymo organo, pareigą užtikrinti kibernetinį bendrovės saugumą.

Lietuvos Aukščiausiasis Teismas yra pažymėjęs, kad bendrovės vadovas, kaip vienasmenis valdymo organas, *ex officio* organizuoja kasdienę bendrovės veiklą (ABĮ 37 str. 8 d.), atsako už bendrovės veiklos organizavimą bei jos tikslų įgyvendinimą (ABĮ 37 str. 12 d. 1 p.). Šios funkcijos ir yra pagrindinės funkcijos, kurios identifikuoja bendrovės vadovą, kaip vieną svarbiausių figūrų, dalyvaujančių juridinio asmens veikloje. Todėl, vien aptariamų funkcijų apibrėžimai rodo, kad bendrovės vadovas, kaip vienasmenis valdymo organas, turi plačius įgaliojimus bendrovės valdymo procese. Vis dėlto, kad ir kokie platūs yra bendrovės vadovo, kaip vienasmenio valdymo organo, įgaliojimai, nereiškia, jog šio subjekto atsakomybė yra neribota ir kartu neindividualizuota, t. y. kad jis automatiškai atsako pagal visas prievoles, kurios atsiranda kaip juridinio asmens vykdomos veiklos pasekmė. Pažymėtina, kad, sprendžiant civilinės atsakomybės taikymo bendrovės vadovui klausimą, būtina identifikuoti, ar pareigos, kurių pažeidimas yra įrodinėjamas reikalaujant žalos atlyginimo, priskirtos vadovo kompetencijai, ar bendrovės vadovas pažeidė šias (jo kompetencijai priskirtas) pareigas ir ar įrodinėjama žala yra būtent bendrovės vadovui tenkančių pareigų pažeidimo pasekmė (Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus 2018 m. rugsėjo 21 d. nutartis civilinėje byloje Nr. 3K-3-326-1075/2018). Lietuvos Aukščiausiasis Teismas, pasisakydamas dėl bendrovės valdymo organų pareigų

taip pat yra nurodęs, kad organizuodamas ir vykdydamas bendrovės kasdienę veiklą, bendrovės vadovas, be kita ko, yra saistomas įstatyme įtvirtintų fiduciarinių pareigų, t. y. veiklos principų, kuriais jis turi vadovautis, priimdamas konkrečius verslo sprendimus, ir kuriais iš esmės apibūdinamas bendrovės vadovo veiklos standartas (Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus 2021 m. gruodžio 2 d. nutartis civilinėje byloje Nr. e3K-3-300-313/2021). Pasisakydamas dėl konkretaus standarto, kurį turėtų atitikti vadovas, Kasacinis teismas yra nurodęs, kad įmonės vadovas privalo dirbti rūpestingai ir kvalifikuotai bei daryti viską, kas nuo jo priklauso, kad jo vadovaujama įmonė veiktų pagal įstatymus ir kitus teisės aktus. Įmonės vadovas privalo rūpintis, kad įmonė laikytųsi įstatymų, nustatytų jos veiklos apribojimų ir kt. Vadovą ir jo vadovaujamą įmonę sieja fiduciariniai santykiai, nuo pat tapimo bendrovės vadovu momento vadovas turi elgtis rūpestingai, atidžiai ir apdairiai. Ar vadovas konkrečiu atveju šią pareigą įvykdė, nustatoma pagal tam tikrus objektyvius elgesio standartus – rūpestingo, apdairaus, protingo vadovo elgesio matą (Lietuvos Aukščiausiojo Teismo 2006 m. gegužės 25 d. nutartis, civilinėje byloje Nr. 3K-7-266/2006). T.y. pasisakymas dėl vadovo pareigos organizuoti bendrovės veiklą Kasacinis teismas šią pareigą sieja su fiduciarinėmis vadovo pareigomis, o tuo tarpu fiduciarinės pareigų vykdymas nustatomas pagal *bonus pater familias* standartą.

Apibendrindamas suformuotą praktiką, Lietuvos Aukščiausiasis Teismas yra nurodęs, kad taikant verslo sprendimų priėmimo taisyklę pirmiausia būtina nustatyti, ar priimtas sprendimas buvo verslo sprendimas. Verslo sprendimu laikomas toks vadovo (ar valdybos) veiksmas, kurio atlikimas nebuvo susijęs su imperatyvų, nustatytų įstatymuose ir įmonės dokumentuose, įvykdymu, t. y. vadovas turėjo diskreciją priimti konkretų sprendimą ir tuo metu nebuvo žinoma, ar šis pasiteisins (Bendrovės valdymo organų civilinę atsakomybę reglamentuojančių teisės normų taikymo Lietuvos Aukščiausiojo Teismo praktikoje apžvalga). Taigi, nustačius, kad vadovo pareigos užtikrinti kibernetinį bendrovės saugumą kildinamos iš ABĮ numatyto bendrovės veiklos organizavimo, galime daryti išvadą, kad verslo sprendimo taisyklė nebūtų taikoma, kadangi laikytina, kad šių veiksmų atlikimas yra susijęs su imperatyvų nustatytų įstatyme įvykdymu.

Taigi, vertinant aukščiau nurodytą Lietuvos Aukščiausiojo Teismo suformuotą praktiką, galime daryti išvadą, kad ABĮ 37 str. 12 d. 1 p. numatytų bendrovės vadovo pareigų vykdymas bei bendrovės kibernetinio saugumo užtikrinimas glaudžiai susijęs su bendrovės vadovo fiduciarinėmis pareigomis. Apibrėždamas vadovo fiduciarines pareigas V. Mikelėnas nurodo, kad vykdydamas savo pareigas įmonės vadovas pagal savo pareigas privalo veikti maksimaliai apdairiai ir rūpestingai, kad būtų visokeriopai užtikrinti jo vadovaujamos įmonės interesai. Kadangi vadovą ir jo vadovaujamą įmonę sieja

fiduciariniai santykiai, <...> vadovas turi elgtis rūpestingai, atidžiai ir apdairiai. Šios pareigos turinys yra platus ir iš esmės reiškia, kad įmonė bei jos akcininkai turi teisę reikalauti iš įmonės vadovo veikti įmonės interesais kvalifikuotai, protingai, rūpestingai ir apdairiai. Ar įmonės vadovas konkrečiu atveju šią pareigą įvykdė, ar ne, nustatoma pagal tam tikrus objektyvius elgesio standartus. Daugumos užsienio valstybių teisė ir teismų praktiką pripažįsta, kad įmonės vadovo veiklai turi būti taikomas objektyvus, „rūpestingos šeimos galvos“ elgesio standartas (*bonus pater familias*). Šis kriterijus reiškia, kad sprendžiant administracijos vadovo atsakomybės klausimą, turi būti aiškinamasi, ar būdamas asmens, kurio atžvilgiu gali būti taikoma atsakomybė, vietoje rūpestingas, apdairus, protingas vadovas toje pačioje situacijoje būtų pasielgęs analogiškai. Jeigu daroma išvada, kad analogiškoje situacijoje protingas, apdairus ir rūpestingas vadovas būtų pasielgęs kitaip ir dėl to įmonė būtų išvengusi nuostolių, tai reiškia, kad įmonės vadovas pažeidė savo pareigą veikti apdairiai (Abramavičius A., Mikelėnas V. 1999, *Įmonių vadovų teisinė atsakomybė*, antras leidimas, VĮ Teisinės informacijos centras, Vilnius). Vertinant vadovo veiklos tinkamumą, tokiu atveju pasitelkiamas *bonus pater familias* standartas, kuris tam tikru atspirties tašku. Numačius tam tikrą standartą, pagal kurį vertinami vadovo veiksmai, galima spręsti ar vadovas konkrečioje situacijoje veikė tinkamai. Nustačius, kad bendrovės vadovo atsakomybė turi būti vertinama pagal *bonus per familias* standartą, galima būtų išsiaiškinti, ar nustatyti objektyvią sistemą, pagal kurią galima būtų vertinti kokio lygio kibernetinę apsaugą privalo užtikrinti tam tikrus parametrus (pvz. vykdomos veiklos pobūdis, darbuotojų skaičius, apyvartos dydis ir kt.) atitinkančios bendrovės. Be kita ko, tokį reguliavimą bei kibernetinio saugumo užtikrinimo metodiką skatina ir Kibernetinio saugumo įstatymo 3 str. v p. įtvirtintas standartizacijos ir technologinio neutralumo principas, pagal kurį subjektai (įskaitant bendroves) skatinami vadovautis ir taikyti Europos Sąjungos ir kitus tarptautinius ryšių ir informacinių sistemų kibernetinio saugumo standartus.

Taip pat, svarbu pabrėžti, kad vertinant bendrovės vadovų pareigų klausimą, vertėtų atsižvelgti ir į vadovų civilinės atsakomybės pagrindus bei sąlygas, esant skirtingai vadovo civilinės atsakomybės kilmei. Manytina, kad bendrovės vadovui, civilinė atsakomybė už netinkamą kibernetinio saugumo užtikrinimo pareigos vykdymą (kai tokia pareiga kyla), galėtų kilti delikto pagrindu, kadangi kaip jau buvo minėta anksčiau, laikytina, kad bendruoju atveju, vadovo pareiga užtikrinti kibernetinį saugumą kyla iš pareigos numatytos ABĮ t.y. ABĮ 37 str. 12 d. 1 p. Taigi, pagal CK 6.246–6.249 str., civilinei vadovo atsakomybei kilti būtina įstatyme nustatytų sąlygų visuma: neteisėti vadovo veiksmai (išskyrus įstatyme nustatytas išimtis), priežastinis ryšys tarp neteisėtų veiksmų ir nuostolių,

vadovo kaltė (išskyrus įstatyme ar sutartyje nustatytas išimtis), žala (nuostoliai). Apie vadovo veiksmų neteisėtumą ir kaltę sprendžiama pagal tai, ar vadovas laikėsi bendrųjų (CK 2.87 str.) ir specialiųjų teisės normų, reglamentuojančių jo pareigas atliekant valdymo organo ar jo nario pareigas (nagrinėjamo darbo kontekste koncentruojantis į vadovo pareigas) valdant įmonę. <...> bendrovės valdymo organų (vienasmenio ir kolegialaus) nariai turi elgtis rūpestingai ir sąžiningai bendrovės atžvilgiu. Taip pat, pažymėtina, kad vertinant bendrųjų ir specialiųjų teisės normų pažeidimo santykį būtina pabrėžti, kad vadovų kaltės laipsnis taikant civilinę atsakomybę pagal minėtus pagrindus skiriasi. T.y. tais atvejais, kai pažeidžiamos fiduciarinės vadovo pareigos ar vadovas priima tam tikrą nenaudingą verslo sprendimą, atsakomybė vadovui kyla tik nustačius didelį jo neatsargumą ar tyčią (Lietuvos Aukščiausiojo Teismo 2013 m. lapkričio 20 d. nutartis civilinėje byloje Nr. 3K-3-581/2013; 2013 m. gruodžio 20 d. nutartis civilinėje byloje Nr. 3K-3-699/2013), pagal Kasacinio formuojamą praktiką, didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina duotomis aplinkybėmis, tuo tarpu civilinė atsakomybė už imperatyvių – specialiųjų normų pažeidimus, galima ir esant vadovo neatsargumui. (Lietuvos Aukščiausiojo Teismo 2017 m. spalio 16 d. nutartis civilinėje byloje Nr. 3K-7-177-701/2017). Fiduciarinių ir imperatyvių pareigų pažeidimai yra savarankiški valdymo organo nario atsakomybės pagrindai, t. y. ir nepažeidus konkrečių įstatymuose įtvirtintų imperatyviųjų normų valdymo organų veiksmai gali būti neteisėti dėl fiduciarinių pareigų pažeidimo. (Bendrovės valdymo organų civilinę atsakomybę reglamentuojančių teisės normų taikymo Lietuvos Aukščiausiojo Teismo praktikoje apžvalga).

Apibendrinant šioje dalyje nagrinėtą vadovų pareigos užtikrinti kibernetinį saugumą kilmę, galime daryti išvadą, kad atsakomybė už kibernetinio saugumo užtikrinimą bendruoju atveju turėtų būti vertinama pagal pagal *bonus pater familias* elgesio standartą. Atsižvelgiant į kibernetinių rizikų naujumą ir tam tikrą neapibrėžtumą (kadangi ši rizika yra stipriai įtakojama trečiųjų asmenų ir technologijų pažangos) vadovams turėtų būti suteikta teisė patiems įvertinti bendrovės vykdomą veiklą, jos pobūdį, ir t.t., bei atitinkamai priimti protingus sprendimus, kurie konkrečiu atveju būtų naudingiausi bendrovei. Vertinant ar vadovas ėmėsi pakankamų priemonių ir tinkamai užtikrino kibernetinį saugumą bendruoju atveju, būtina vadovautis *bonus pater familias* rūpestingumo standartu, kadangi šiai dienai neturime kito instituto, kuri padėtų įvertinti vadovo veiksmų ir rūpestingumo (ne)pakankamumą. Skaidant kibernetinę riziką į atskirus jos elementus (t.y. pritaikant šį institutą konkrečiai situacijai), galimos ir kitos išvados, kadangi kiekvienas elementas gali turėti atskirą atsakomybės pagrindą. Štai pavyzdžiui įmonės vadovui

neužtikrinus vidinių bendrovės dokumentų apsaugos (pagal 1 dalyje aptartą skirstymą tokį atvejį galėtumėme priskirti ir žalai, bendrovei praradus jos veiklai svarbius dokumentus), t.y. galima konstatuoti CK 2.4 str. 3 d. įtvirtintos normos (ir iš jos kylančių pareigų numatytų Lietuvos Respublikos buhalterinės apskaitos įstatyme (Lietuvos Respublikos buhalterinės apskaitos įstatymas, Valstybės žinios, 2001-11-28, Nr. 99-3515)) pažeidimą. Tuo tarpu jei bendrovės vadovas nepasirūpino ugniasienių, antivirusinių ar kitų kibernetinio saugumo priemonių įdiegimu, tikėtina, kad toks elgesys būtų laikomas nerūpestingu (vertinimas ar toks neveikimas galėtų būti laikomas dideliu nerūpestingumu ar tyčia turėtų būti atliekamas atsižvelgiant į bendrovės vykdomos veiklos pobūdį, kibernetinės rizikos dydį ir specialiuosius teisės aktus numatančius konkrečias pareigas susijusias su kibernetiniu saugumu, kurios plačiau nagrinėjamos 2.2. dalyje), tačiau kaip jau buvo minėta, toks sprendimas turės būti vertinamas pagal *bonus pater familia* standartą.

Be jokios abejonės, kad vienokio ar kitokio saugumo standarto taikymą ir jo taikymo apimtį lemia bendrovės vykdoma veikla ir jos pobūdis. Tikriausiai visi sutiktų, kad advokatų kontoros, valdančios ypač jautrius klientų duomenis ir nedidelės parduotuvėlės prekiaujančios maisto produktais, kibernetinio saugumo užtikrinimo standartai turėtų ženkliai skirtis. Šį teiginį pagrindžia ir V. Mikelėno išsakyta mintis, kad vadovo rūpestingumo ir apdairumo laipsnį gali apspręsti daugybė faktorių. Pavyzdžiui didelę įtaką gali turėti bendrovės veiklos pobūdis. <...> tai, ką vienu atveju galima pripažinti normalia gamybine – ūkine rizika, kitu atveju bus pripažinta neapdairiu, neprotingu ir nerūpestingu, t.y. kaltu vadovo elgesiu. Taip pat, nurodoma, kad atidumo ir rūpestingumo pareigos pažeidimai dažniausiai pasireiškia: <...> 3) elementarių verslo administravimo standartų nesilaikymu; <...> 10) nesaugojamos ar nepakankamai saugojamos įmonės komercinės paslaptys ar kitokia konfidenciali informacija; <...> 16) kitokio pobūdžio aplaidumu, nerūpestingumu, neapdairumu arba nepakankamu domėjimusi įmonės reikalais (Abramavičius A., Mikelėnas V. 1999, *Įmonių vadovų teisinė atsakomybė*, antras leidimas, VĮ Teisinės informacijos centras, Vilnius). Taigi, vertinant vadovo atsakomybę, ypač svarbu nustatyti, ar pasirinktas informacinių technologijų sistemų apsaugos standartas yra pakankamas ir proporcingas, atsižvelgiant į bendrovės vykdomą ūkinę komercinę veiklą. Informacinių ir ryšių technologijų saugumo standartų pasirinkimas turėtų priklausyti išimtinai nuo bendrovės vykdomos veiklos, veiklos skaitmenizavimo lygio, pažeidžiamumo, saugomos informacijos kiekio ir pobūdžio ir kitų objektyvių kriterijų. Dauguma šių atsparumo kibernetinių incidentų rizikoms standartų yra viešinami įvairių ES ar nacionalinių institucijų negriežtosios teisės (angl. *soft law*) šaltiniais, tokiais kaip gairės ar rekomendacijos. Štai pavyzdžiui Europos draudimo ir profesinių pensijų institucija

(toliau - **EIOPA**) parengė Informacinių ir ryšių technologijų saugumo ir valdymo gaires Nr. EIOPA-BoS-19/600 (toliau - **ITR saugumo gairės**), kuriomis rinkos dalyviams siekiama paaiškinti apie būtiniausią pageidaujamą informacijos ir kibernetinio saugumo pajėgumą, t. y. bazinį saugumo lygį. Šiomis gairėmis pateikiamos rekomendacijos valdymo reikalavimus informacinių ir ryšių technologijų, saugumo ir valdymo srityje. 2-oji ITR saugumo gairė nurodo, kad administracinis, valdymo arba priežiūros organas turėtų užtikrinti, kad įmonių valdymo sistemoje, visų pirma rizikos valdymo ir vidaus kontrolės sistemoje, būtų tinkamai valdoma įmonių informacinių ryšių technologijų ir saugumo rizika. Pažymėtina, kad „tinkamo valdymo“ sąvoka šiose gairėse nėra išaiškinta, taip pat, ši definicija plačiai naudojama ir kituose teisės aktuose (pvz. 2.2. dalyje nagrinėjamame Elektroninių ryšių įstatyme ar BDAR), tačiau jos aiškinimo ir taikymo praktika nėra suformuota. Plačiau apie šios definicijos aiškinimą žr. 2.2. dalyje.

Dalis įmonių, siekdama gauti dar aukštesnį kibernetinių rizikų atsparumo patvirtinimą siekia tam tikrų konkrečių standartų. Informacinių sistemų saugumo sertifikavimas pagal tam tikrus standartus leidžia parodyti priežiūros institucijai, esamiems bei potencialiems klientams ir partneriams sertifikuotos bendrovės įsipareigojimą užtikrinti valdomos informacijos saugumą, konfidencialumą ir prieinamumą reikiamu metu. Taip pat, dažnu atveju šis sertifikatas gali patvirtinti viešųjų pirkimo kvalifikacinių reikalavimų laikymąsi tais atvejais, kai konkurso dalyvių atrankos kriterijumi yra informacijos saugos sistemų turėjimas. Štai pavyzdžiui ISO 27001:2013 yra tarptautinis standartas, kurį įgyvendinus bendrovėje sukuriama patikima informacinių technologijų saugos sistema, nustatomos informacijos ir duomenų saugumo rizikos ir numatomos būtinos priemonės užkirsti joms kelią bei sumažinti jų poveikį ateityje.

Tiek literatūroje tiek praktikoje, bendrovėms, kurių kibernetinių incidentų rizika yra aukšta, rekomenduojama suburti tam tikrą vidinę kibernetinių incidentų valdymo komandą, kuri būtų pasiskirsčius konkrečius vaidmenis ir pareigas, ir žinotų ką privalo atlikti įvykus kibernetiniam incidentui. Štai pavyzdžiui Belgijos kibernetinio saugumo centras yra parengęs Kibernetinio saugumo incidentų valdymo vadovą (Centre for Cyber Security Belgium, 2021. CYBER SECURITY INCIDENT MANAGEMENT GUIDE [interaktyvus, žiūrėta 2022-03-22], prieiga per internetą: https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf). Kaip vienas iš pasiruošimo ir vidinių bendrovės tvarkų parengimo žingsnių nurodytas minėtos komandos, atsakingos už kibernetinių incidentų valdymą, subūrimas ir tinkamas apmokymas. Paprastai tokią komandą turėtų sudaryti: (i) kibernetinio incidento valdymo vadovas, atsakingas už visus procesus susijusius su

kibernetinio incidento valdymu nuo pat jo pradžios iki pabaigos, paprastai šias pareigas atlieka bendrovės vadovas ar informacinių technologijų padalinio vadovas (plačiau apie vadovo atsakomybė dalį funkcijų pavedant vykdyti informacinių technologijų specialistams žr. 3 darbo dalyje); (ii) akcininkai, turintys galimybę sutelkti reikalingus resursus ir priimti strateginius bendrovės valdymo sprendimus; (iii) informacinių technologijų ekspertai, kurie galėtų analizuoti ir administruoti techninius informacinio saugumo procesus, atkurti prarastus ar užkoduotus duomenis, riboti tolimesnę įsilaužėlių prieigą prie tam tikrų sistemų ar jos dalių, pradėti įprastos bendrovės veiklos atkūrimo procesus. Ypač svarbu, kad šie specialistai būtų nuodugniai susipažinę su bendrovės informacinių technologijų ūkiu, naudojamais sprendimais, ir kt. Jei samdomi išoriniai informacinių technologijų specialistai, rekomenduojama parengti trumpas instrukcijas ar gaires, kuriose būtų detalizuota informacija susijusi su informacinėmis technologijomis naudojamomis konkrečioje bendrovėje. Informacinių technologijų specialistams keliama ir kita ypač svarbi pareiga – tai kibernetinio incidento įvykių protokolavimas ir tinkamas jų aprašymas ir įforminimas tokiu būdu, kad ši informacija vėliau galėtų būti teikiama tam tikroms tyrimus atliekančioms institucijoms, teismui ar draudimo bendrovėms; (iv) teisininkai (tiek išoriniai, tiek vidiniai bendrovės teisininkai, priklausomai nuo bendrovės dydžio ar veiklos pobūdžio), kurie galėtų įvertinti kibernetinio incidento poveikį sutartinių ir įstatymais nustatytų pareigų vykdymui. Teisininkai paprastai įvertina ir atrenka reikalingą informaciją, bei parengia dokumentus, kurie yra teikiami tam tikroms valstybinėms institucijoms (pvz. Valstybinei duomenų apsaugos inspekcijai (toliau - **VDAI**), Lietuvos Respublikos Kibernetinio saugumo centrui, policijai ar kitos valstybės atsakingai institucijai atliekančiai tyrimą); (v) Komunikacijos ar viešųjų ryšių specialistai, kurie galėtų atsakyti į visuomenei rūpimus klausimus susijusius su kibernetiniu incidentu, tai ypač aktualu didesnėms bendrovėms, kai nutekinami dideli kiekiai fizinių asmenų asmens duomenų; (vi) fizinės apsaugos atstovas turėtų organizuoti fizinę tam tikrų bendrovės patalpų apsaugą, kadangi įvykus kibernetiniam incidentui, galimi ir signalizacijos ar kitų bendrovės saugumo sistemų sutrikimai, todėl svarbu užkardyti trečiųjų asmenų patekimą į bendrovės valdomas patalpas. Taigi, bendrovių vadovai (atsižvelgdami į vykdomos veiklos pobūdį) turėtų apsvarstyti galimybę sukurti tam tikrą komandą, kuri galėtų reaguoti į kibernetinius incidentus įvykusius minėtoje bendrovėje. Tačiau nepaisant to, kad bendrovėms rekomenduojama burti minėtas komandas, nereiktų pamiršti ABĮ nuostatų numatančių vadovo pareigą organizuoti bendrovės veiklą. Taigi, būtina įvertinti ir nustatyti, ar bendrovės veiklos organizavimas apima ir kibernetinių rizikų apsaugos organizavimą. Ketvirtoji ITR saugumo gairė nurodo, kad administraciniam,

valdymo arba priežiūros organui tenka bendra atsakomybė sukurti veiksmingą IRT ir saugumo rizikos valdymo sistemą, kuri būtų įmonės bendros rizikos valdymo sistemos dalis. Tai apima priimtinos rizikos nustatymą šios rizikos atžvilgiu pagal įmonės rizikos strategiją ir reguliarią rašytinę ataskaitą apie rizikos valdymo proceso rezultatus, skirtą administraciniam, valdymo arba priežiūros organui. Taip pat, toliau patikslinama, kad rengdamos bendrą rizikos valdymo sistemą, įmonės informacinių ryšių technologijų ir saugumo rizikos atžvilgiu turėtų įtraukti bent šiuos elementus: a) įmonės turėtų sudaryti ir reguliariai atnaujinti savo verslo procesų ir veiklos, veiklos funkcijų, vaidmenų ir išteklių (pvz., informacinių ir informacinių ryšių technologijų išteklių) planus, kad nustatytų jų svarbą ir tarpusavio priklausomybės ryšius su informacinių ryšių technologijų ir saugumo rizika; b) įmonės turėtų nustatyti ir vertinti visą susijusią informacinių ryšių technologijų ir saugumo riziką, su kuria jos susiduria, ir suklasifikuoti nustatytus verslo procesus ir veiklą, veiklos funkcijas, vaidmenis ir išteklius (pvz., informacinius ir informacinių ryšių technologijų išteklius) pagal svarbą. Nesigilinant į negriežtosios teisės šaltinių taikymo klausimą, ITR saugumo gairės galėtų būti laikomos tam tikro imperatyvaus teisės akto, numatančio konkrečias vadovų pareigas susijusias su bendrovės kibernetiniu saugumu, užuomazga. Įmonės taip pat turėtų įvertinti apsaugos reikalavimus, susijusius su bent tų verslo procesų ir veiklos konfidencialumu, vientisumu ir prieinamumu, veiklos funkcijomis, vaidmenimis ir ištekliais (pvz., informaciniais ir informacinių ryšių technologijų ištekliais). Turėtų būti nurodyti išteklių savininkai, atsakingi už išteklių klasifikavimą; c) metodai, skirti reikalingos apsaugos svarbai ir lygmeniui nustatyti, ypač atsižvelgiant į apsaugos tikslus, susijusius su vientisumu, prieinamumu ir konfidencialumu, turėtų užtikrinti, kad nustatomi apsaugos reikalavimai būtų nuoseklūs ir išsamūs.

Taigi, darbo autoriaus nuomone, vertinant bendrąsias vadovų pareigas susijusias su kibernetiniu saugumu, reikėtų pabrėžti, kad ekspertai rekomenduoja bendrovėje: (i) turėti suformuotą kibernetinių incidentų valdymo komandą, bei parengtus reagavimo į kibernetinius incidentus planus – veiklos tęstinumo planus ir kitus vidinės tvarkos dokumentus, susijusius su kibernetinio saugumo užtikrinimu; (ii) yra nuolat stebima kibernetinė aplinka, atliekamas savalaikis kibernetinio saugumo rizikų vertinimas; (iii) bendrovė naudoja proporcingas kibernetinio saugumo užtikrinimo priemones, t.y. priklausomai nuo bendrovės vykdomos veiklos, turėtų būti naudojamos antivirusinės programos, ugniasienės, atliekamas duomenų kopijos, periodiškai atliekami informacinių sistemų auditai. Vertinant vadovo pareigų intensyvumą ir šių pareigų apimtį, turėtų būti atsižvelgiama į *bonus pater familias* standartą ir vertinama, kokias kibernetinio saugumo

priemones rinktųsi protingas verslininkas atitinkamoje situacijoje būdamas atsakingas ir atitinkamai konsultuodamasis su informacinių technologijų ir kitų sričių specialistais.

Apibendrinant šią dalį galima paminėti ir Susan Moore rinkos pokyčių spėjimus – prognozes, kuriuose nurodoma, kad plintant informacinių technologijų, išmaniųjų pastatų ar net ištisų miestų, ir autonominių transporto priemonių panaudojimui kibernetiniai incidentai visame pasaulyje turės daug didesnį poveikį fiziniam pasauliui, nes rizika, grėsmės ir pažeidžiamumas (atsižvelgiant į sparčiai didėjantį informacinių technologijų naudojimą ir įvairių procesų skaitmenizavimą) egzistuoja dvikrypčiu kibernetinės ir fizinės veiklos spektru. Ji taip pat pažymi, kad 75% vadovų bus asmeniškai atsakingi už kibernetinio saugumo incidentus dar iki 2024 m. (Susan Moore (2020), Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024 [interakyvus, žiūrėta 2022-03-22]], prieiga per internetą: https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl) Tiesa reikėtų pabrėžti, kad šiame straipsnyje kalbama būtent apie kibernetinius incidentus sukeliančius fizinį poveikį. Nepaisant to, galima įžvelgti aiškią tendenciją ir kryptį, kuria galimai judės vadovų atsakomybės už kibernetinį saugumą institutas.

Pažymėtina, kad praktiškai vertinant bendrovių valdymo organų pareigas, nereiktų apsiriboti vien šioje dalyje išdėstytomis bendrosiomis bendrovių valdymo organų pareigomis susijusiomis su kibernetiniu saugumu, tačiau taip pat reikėtų atsižvelgti ir į bendrovės įstatuose ar kituose specialiuosiuose teisės aktuose (daugiau apie specialiaisiais teisės aktais bendrovėms sukuriamas pareigas žr. 1.2. dalį) bendrovės valdymo organams priskiriamas pareigas.

2.2. Bendrovės vadovo pareiga užtikrinti kibernetinį bendrovės saugumą reguliuojamuose sektoriuose

Nagrinėjant bendrovių valdymo organų atsakomybės klausimus vertėtų išskirti tam tikras įstatymų leidėjo ypatingai reguliuojamas rinkas. Dėl ypatingos svarbos valstybės ekonomikai, tam tikros sritys patiria platesnio mąsto įstatymų leidėjo įsikišimą į tokių bendrovių steigimo, valdymo, ūkinės veiklos vykdymo procesus, ir kt. Nepaisant to, kad Lietuvoje funkcionuoja laisvos rinkos santykiais grįsta rinkos ekonomika, ir toliau išlieka nemažai valstybės aktyviai reguliuojamų sričių (rinkų), pvz.: telekomunikacijos, energetika (elektra, gamtines dujos, šiluma), vandens tiekimas, finansinės institucijos ir rinkos (bankai, draudimo kompanijos), transportas (geležinkelių, oro, jūrų), medicinos paslaugos

ir farmacinė veikla, žemės ūkis ir kt. Be kitų jau paminėtų reguliuojamų procesų, dažnu atveju nustatomos ir papildomos pareigos šioms įmonėms, kurios be kita ko yra susijusios su ryšių ir komunikacijos sistemų ar kibernetinio saugumo sritimi.

Kibernetinio saugumo įstatymo 5 str. 4 p. numato, kad Vyriausybė tvirtina organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus kibernetinio saugumo subjektams. Įgyvendindama savo pareigą numatytą Kibernetinio saugumo įstatyme, Vyriausybė priėmė Nutarimą dėl kibernetinio saugumo strategijos patvirtinimo, kuriame numatyti ypatingos svarbos sektoriai, subsektoriai, paslaugos ir atsakingos institucijos (toliau – **Ypatingos svarbos sektorių sąrašas**); organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų Kibernetinio saugumo subjektams, Kibernetinio saugumo reikalavimų aprašas, ir t.t. Į Ypatingos svarbos sektorių sąrašą yra įtraukta 14 sektorių, tarp kurių: sveikatos priežiūros, informacinių technologijų ir elektroninių ryšių, finansų sektorius ir kiti. Taigi, atsižvelgiant į šį sąrašą, galime daryti išvadą, kad šie sektoriai yra laikomi ypatingos svarbos, dėl to juose veikiantys subjektai laikytini Kibernetinio saugumo subjektais, kuriems priskiriamos tam tikros papildomos pareigos, susijusios su aukštesnio kibernetinio saugumo lygio užtikrinimu.

Šioje darbo dalyje bus nagrinėjamas specialusis sektorinis reguliavimas susijęs su kibernetiniu saugumu, nustatytas šių sektorių veiklą reguliuojančiuose įstatymuose, o apibendrinant - dalies gale bus paminėti ir visiems Kibernetinio saugumo subjektams taikomi techniniai kibernetinio saugumo reikalavimai numatyti Kibernetinio saugumo reikalavimų apraše.

Lietuvos Respublikos sveikatos sistemos įstatymo (toliau – **Sveikatos sistemos įstatymas**) (Lietuvos Respublikos sveikatos sistemos įstatymas, Valstybės žinios, 1994-08-17, Nr. 63-1231) 52 str. 2 d. numato, kad informacijos apie asmens sveikatą kompiuteriuose apsauga privalo garantuoti jos konfidencialumą. Kitais žodžiais, naudojamos informacinių tinklų apsaugos sistemos turi garantuoti, kad saugomi duomenys netaps žinomi tretiesiems asmenims. Atsižvelgiant į nuolatinį administracinių medicinos įstaigų vykdomų procesų skaitmenizavimą, ši norma įgauna ypatingą reikšmę, kai visi (ar didžioji dalis) asmens sveikatos duomenys jau yra laikomi elektroninėse laikmenose, tame tarpe ir sveikatos priežiūros įstaigų naudojamuose kompiuteriuose. Įstatymų leidėjas nedetalizuoja, kam tenka Sveikatos priežiūros įstatyme numatyta pareiga užtikrinti asmens sveikatos duomenų konfidencialumą, tačiau atsižvelgiant į ankstesnėje darbo dalyje padarytas išvadas galime teigti, kad konkrečios sveikatos priežiūros įstaigos vadovas turėtų būti laikomas atsakingu už tokio pobūdžio (kasdienės bendrovės veiklos organizavimo) bendrovei priskiriamų pareigų tinkamą įvykdymą. Visgi, nors šiame įstatyme ir pastebime

papildomų pareigų susijusių su informacijos apsauga kibernetinio saugumo kontekste, tačiau jų apimtis yra ypač siaura, kadangi numatoma tik informacijos konfidencialumo pareiga. CK 6.164 str. 1 d. numatanti sutartinės informacijos konfidencialumo pareigas nurodo, kad šalis, sužinojusi ar gavusi šią informaciją, privalo jos neatskleisti ar nenaudoti savo tikslams neteisėtu būdu. Kembridžo universiteto žodyne žodis konfidencialus (angl. *confidential*) apibūdinamas kaip slaptas ir privatus, laikomas paslėptas nuo kitų žmonių (angl. *secret and private, kept hidden from other people*) (Kembridžo žodynas [interaktyvus, žiūrėta: 2022-04-01]. Prieiga per internetą: https://dictionary.cambridge.org/dictionary/english/confidential). Pacientų teisės yra detalizuojamos ir kituose teisės aktuose, pavyzdžiui Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymo 8 ir 9 str., detalizuojamos pacientų teisės į privataus gyvenimo neliečiamumą (Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymas, Valstybės žinios, 1996-10-23, Nr. 102-2317).

Taip pat, pažymėtina ir tai, kad asmenų sveikatos duomenys priskirtini specialiųjų kategorijų duomenims (pagal BDAR 9 str. 2 dalį). Minėtiems duomenims, kurie pagal savo pobūdį yra susiję su pagrindinėmis teisėmis ir laisvėmis bei dėl to neskelbtini, turėtų būti užtikrinta ypatinga apsauga, nes atsižvelgiant į jų tvarkymo aplinką galėtų kilti didelis pavojus pagrindinėms teisėms ir laisvėms (Zaleskis, J., 2019. Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija, Vilnius: Registrų centras). BDAR 4 str. 15 p. apibrėžta sveikatos duomenų sąvoka (asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugų teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę) iš esmės atitinka Sveikatos sistemos įstatyme minimą duomenų kategoriją „Informacija apie asmens sveikatą“, todėl darytina išvada, kad šiai duomenų kategorijai ir jos apsaugai reglamentuoti taikytinas ir BDAR.

Todėl, galime daryti išvadą, kad sveikatos priežiūros įstaigoms kyla pareiga užtikrinti informacijos apsaugą, kuri turėtų pasireikšti ir šios informacijos pasiekiamumo ribojimu tretiesiems asmenims. Autoriaus nuomone, vertinant konfidencialumo pareigą nurodytą Sveikatos sistemos įstatyme ir BDAR kibernetinio saugumo užtikrinimo kontekste, sveikatos priežiūros įstaigos vadovas turėtų būti laikomas atsakingu už reikiamų informacinių sistemų apsaugos parinkimą, jų įdiegimo ir priežiūros organizavimą, t.y. duomenų saugos užtikrinimą plačiąja prasme. Nepaisant to, pastebima, kad paminėti teisės aktai neįpareigoja sveikatos priežiūros įstaigų vadovų imtis priemonių, reikalingų sveikatos

priežiūros įstaigos veiklos tęstinumui užtikrinti[6], t.y. vadovams nėra keliami reikalavimai susiję su galima žala pačiai sveikatos priežiūros įstaigai, aptarti šio darbo 1 dalyje (žala bendrovei). Tačiau atsižvelgiant į ypatingą sveikatos priežiūros įstaigų svarbą visuomenėje, sveikatos priežiūros įstaigos yra laikomos Kibernetinio saugumo subjektais, kuriems taikomi papildomi techniniai reikalavimai (plačiau apie techninius reikalavimus keliamus Kibernetinio saugumo subjektams žr. žemiau) susiję su kibernetinio saugumo užtikrinimu, kuriuose įtvirtintos priemonės apima ir priemones reikalingas išvengti žalos pačiai bendrovei.

Specialusis (sektorinis) reguliavimas, gali būti pastebimas Lietuvos Respublikos elektroninių ryšių įstatyme (toliau - **Elektroninių ryšių įstatymas**) (Lietuvos Respublikos elektroninių ryšių įstatymas, Valstybės žinios, 2004-04-30, Nr. 69-2382). Šio įstatymo 74 str. 1 d. numato, kad Viešųjų elektroninių ryšių paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų elektroninių ryšių paslaugų saugumui užtikrinti, o prireikus kartu su viešųjų elektroninių ryšių tinklų teikėjais imtis tokių pačių priemonių viešųjų elektroninių ryšių tinklų saugumui užtikrinti. Šios priemonės turi atitikti BDAR nustatytus reikalavimus, užtikrinti saugumo lygį, atitinkantį iškilusią grėsmę, ir užtikrinti: 1) kad su asmens duomenimis galėtų susipažinti tik tokią teisę turintys viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjo įgalioti darbuotojai teisėtais tikslais; 2) tvarkomų asmens duomenų apsaugą nuo atsitiktinio arba neteisėto sunaikinimo, atsitiktinio praradimo ar pakeitimo ir neteisėto saugojimo, tvarkymo, susipažinimo ar atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo; 3) kad būtų įgyvendinama asmens duomenų saugumo politika asmens duomenų tvarkymo srityje. Lyginant šio įstatymo bei Sveikatos sistemos įstatymo formuluotes susijusias su informacinių technologijų sistemų saugumu, akivaizdu, kad Elektroninių ryšių įstatymas daug detaliau nurodo, kokios pareigos kyla šiuo įstatymu reguliuojamiems subjektams. Pažymėtina ir tai, kad Elektroninių ryšių įstatymas reguliuojamiems juridiniams asmenims sukuria daugiau pareigų, t.y. galime daryti išvadą, kad Elektroninių ryšių įstatymas, lyginant su Sveikatos sistemos įstatymu, yra šiuolaikiškesnis, labiau pritaikytas ir geriau parengtas plačiam informacinių technologijų sistemų panaudojimui. Be kita ko, galime įžvelgti normų perkėlimą ar nuorodas į BDAR: pavyzdžiui Elektroninių ryšių įstatymo 74 str. 1 d. 2 p. galime įžvelgti BDAR 4 str. 12 p. įtvirtinto Duomenų saugumo pažeidimo apibrėžimą, 3 p. įtvirtinama bendroji pareiga laikytis duomenų saugos reikalavimų, 74 str.

[6] Pažymėtina, kad sveikatos priežiūros įstaigų vadovų pareigos susijusios su siekiu užtikrinti bendrovės veiklos tęstinumą, galėtų būti priskiriamos ir prie bendrųjų vadovų pareigų veikti *bona fidei,* geriausiais bendrovės interesais.

1 dalyje be kita minima ir BDAR naudojama „tinkamų techninių ir organizacinių priemonių“ konstrukcija. Vertinant šį įstatymą kibernetinio saugumo užtikrinimo kontekste, galima padaryti išvadą, kad Elektroninių ryšių įstatymas kaip ir aukščiau nagrinėtas Sveikatos sistemos įstatymas apibrėžia kibernetinio saugumo reikalavimus per duomenų apsaugos prizmę, t.y. į įstatymą perkeliami BDAR reikalavimai. Esminis šių įstatymų skirtumas – reguliavimo konkrečiuose nacionaliniuose teisės aktuose intensyvumas. Atsižvelgiant į nacionaliniuose teisės aktuose eksplicitiškai įtvirtintas pareigas, galime daryti prielaidą, kad įstatymų leidėjas jų apsaugai skiria ypač didelį dėmesį. Taip pat, pažymėtina ir tai, kad Lietuvos Respublikos Administracinių nusižengimų kodekso (Lietuvos Respublikos Administracinių nusižengimų kodeksas, TAR, 2015-07-10, Nr. 11216) 83 str. numato vadovų atsakomybę už Elektroninių ryšių įstatymo pažeidimus, o Kibernetinio saugumo reikalavimų aprašas detalizuoja technines priemones taikomas tame tarpe ir sveikatos priežiūros, finansų bei kitoms įstaigoms.

Panašus reguliavimas susijęs su kibernetinės aplinkos apsauga gali būti pastebimas Lietuvos Respublikos finansų įstaigų įstatyme (toliau - **Finansų įstaigų įstatymas**) (Finansų įstaigų įstatymas, Valstybės žinios, 2002-09-18, Nr. 91-3891). Finansų įstaigų įstatymo 8 str. 1 d. 4 p. numato, kad finansų įstaiga gali teikti finansines paslaugas tik tuo atveju, jeigu ji turi tinkamas technines, informacines, technologines apsaugos užtikrinimo priemones ir patalpas. Taigi, Finansų įstaigų įstatymas eksplicitiškai nurodo, kad techninės, informacinės ir technologinės apsaugos užtikrinimas yra neatsiejama finansų institucijų veiklos sąlyga. Be to, minėto įstatymo 10 str. 2 d. 4 p. nurodo, kad priežiūros institucija taip pat, turi teisę atšaukti finansų įstaigai išduotą licenciją teikti licencines finansines paslaugas, jeigu finansų įstaiga pažeidė Lietuvos Respublikos teisės aktuose nustatytus finansinės apskaitos, valdymo ir kontrolės reikalavimus, šio Įstatymo bei kitų teisės aktų nuostatas ar priežiūros institucijos nurodymus dėl finansų įstaigos saugios ir patikimos veiklos. Atsižvelgdami į tai, galime teigti, kad įstatymų leidėjas nurodo ne tik prieš tai jau minėtus apsaugos užtikrinimo reikalavimus, bet ir numato galimas sankcijas už šių, bei kitų nuostatų nesilaikymą, t.y. licencijos atšaukimą. Šis įstatymas nurodo gan abstraktų rezultatą, kurį privalo pasiekti finansų priežiūros įstaigos. Finansų įstaigų įstatyme, kaip ir prieš tai minėtame Elektroninių ryšių įstatyme galime matyti aiškią nuorodą į BDAR. Įpareigojimas užtikrinti tinkamas technines informacines, technologines apsaugos užtikrinimo priemones kyla iš BDAR 24 str. 1 d. ir 32 str. 1 d.

Formuluotė „tinkamas technines, informacines, technologines apsaugos užtikrinimo priemones“ teismų dar nebuvo išaiškinta ir nėra iki galo aišku, kokį saugumo lygį, standartą ar etaloną ji implikuoja. Todėl, verta paminėti, kad 2021 m. birželio 2 d.

Bulgarijos Aukščiausiasis Administracinis Teismas kreipėsi į Europos Sąjungos Teisingumo Teismą su prašymu priimti prejudicinį sprendimą (2021 m. birželio 2 d. Bulgarijos Aukščiausiojo Administracinio Teismo prašymas priimti prejudicinį sprendimą, Europos Sąjungos Teisingumo Teismo byloje Nr. C-340/21 [interaktyvus, žiūrėta 2022-03-29], prieiga per internetą: https://curia.europa.eu/juris/documents.jsf?oqp=&for=&mat=or&lgrec=en&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-340%252F21&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=en&avg=&cid=1758136). Jame prašoma išaiškinti BDAR 32 str. numatytas duomenų valdytojui tenkančios pareigas, susijusias su tvarkymo saugumu, kurios yra reikšmingos kalbant apie duomenų tvarkytojo atsakomybę pagal 24 str. ir prašome detalizuoti kriterijus pagal kuriuos turi būti taikomos tinkamos techninės ir organizacinės priemonės, kad būtų užtikrintas pavojų atitinkančio lygio saugumas. Nors šis prašymas ir susijęs su BDAR normos aiškinimu, tačiau akivaizdu, kad perkėlus šios BDAR normos esmę į nacionalinius teisės aktus, jos aiškinimas turėtų išlikti nepakitęs, taigi jis teismo išaiškinimas bus aktualus ir Elektroninių ryšių bei Finansų įstaigų įstatymų ir jose numatytoms apsaugos priemonėms keliamų reikalavimų aiškinimą. Šiame prašyme pažymima, kad BDAR nėra apibrėžta sąvoka „tinkamos techninės ir organizacinės priemonės“. BDAR preambulės 74 dalyje nurodyta, kad duomenų valdytojas turi įgyvendinti tinkamas ir veiksmingas priemones ir galėti įrodyti, kad duomenų tvarkymo veikla atitinka šį reglamentą, įskaitant priemonių veiksmingumą. Remiantis tuo, kas išdėstyta, darytina išvada, kad duomenų valdytojas privalo įvertinti riziką pagal reglamento 32 str. nustatytus kriterijus, į kurią atsižvelgdamas jis imasi tinkamų techninių ir organizacinių priemonių, kad būtų užtikrintas būtinas ir pavojų atitinkančio lygio asmens duomenų saugumas. Įdiegdamas atitinkamas technines ir organizacines priemones duomenų valdytojas užtikrina, kad asmens duomenys bus tvarkomi pagal BDAR. Atsižvelgdamas į tai, kas išdėstyta, Bulgarijos Aukščiausiasis Administracinis Teismas klausia, ar BDAR 24 ir 32 str. aiškintini taip, kad vien neteisėtų pasekmių, kaip antai asmens duomenų atskleidimas be leidimo arba prieigos prie jų gavimas be leidimo, kaip tai suprantama pagal BDAR 4 str. 12 p., atsiradimas įrodo, kad techninės ir organizacinės priemonės, kurių ėmėsi duomenų valdytojas, buvo netinkamos.

Tikėtina, kad teismui patvirtinus šią hipotezę, būtų patvirtinta, kad bet koks duomenų saugumo pažeidimas (nepriklausomai nuo įdiegtų saugumo priemonių, *nulinės dienos rizikos* ir kitų aplinkybių) būtų laikomas atitinkamų (pvz. Elektroninių ryšių ir

Finansų įstaigų) įstatymų normų, sukuriančių pareigas vadovui pažeidimu. Taigi, tai suponuotų ir vienos iš vadovo civilinės atsakomybės sąlygų – kaltės atsiradimą[7]. Šis prejudicinis sprendimas neabejotinai turės įtakos ir tolimesniam kibernetinio ir duomenų saugos lygio standarto formavimui, kadangi tikėtina, kad bus išaiškinta, kas turėtų būti laikoma tinkamomis techninėmis ir organizacinėmis priemonėmis, kurios yra pakankamos saugumui užtikrinti. Visgi darbo autoriaus nuomone, šiai dienai turime konstatuoti, kad techninių ir organizacinių priemonių tinkamumas turėtų būti nustatomas šio darbo 2. ir 2.1. dalyse detaliau nagrinėta tvarka, t.y. pagal *bonus pater familias* standartą.

Apibendrinant galime daryti išvadą, kad detalesnė specialiųjų įstatymų, reglamentuojančių atskiras sritis, analizė parodė, kad pareigų, susijusių su informacinių technologijų saugumu, lygis skirtingose srityse (reguliuojamuose rinkose) yra gan panašus. Iš esmės visi trys analizuoti įstatymai įpareigoja juridinius asmenis užtikrinti valdomų duomenų apsaugą, o Finansų įstaigų įstatymas numato ir papildomas priemones susijusias su, tame tarpe ir veiklos tęstinumo užtikrinimu. Pagrindinis skirtumas tarp bendruoju atveju taikomos bendrovių vadovų atsakomybės ir bendrovių vadovų atsakomybės reguliuojamuose sektoriuose yra šių pareigų kilmė ir atitinkamai iš to kylantys padariniai vertinant vadovų atsakomybės klausimą (kurių esminis yra vadovo kaltės laipsnis). T.y. bendruoju atveju vadovas galėtų atsakyti už netinkamai užtikrintą bendrovės kibernetinį saugumą tik esant dideliam neatsargumui ar tyčiai, tuo tarpu reguliuojamuose sektoriuose esant tam tikram reguliavimui įpareigojančiam vadovus užtikrinti tam tikro lygio ar apimties kibernetinį saugumą, vadovo atsakomybė galima ir dėl neatsargių veiksmų.

Taip pat, gali būti daroma išvada, kad dauguma specialiųjų teisės reguliuojančių tam tikrų specifinių sferų veiklą koncentruojasi į duomenų apsaugą ir konfidencialumo užtikrinimą. Toks reguliavimas nekelia didelės nuostabos, atsižvelgiant į BDAR įsigaliojimą ir ypatingą institucijų dėmesį asmens duomenų apsaugai, tačiau pastebima tendencija, kad nagrinėtieji teisės aktai nereglamentuoja kitų kibernetinės rizikos elementų (pvz. žalos pačiai bendrovei), dauguma šių elementų reguliuojami Vyriausybės, tvirtinant tam tikrus techninius aprašus. Tuo tarpu bendruoju atveju – nereguliuojamuose rinkose bendrovės savarankiškai vertindamos galimai joms kylančią žalą turi galimybę pasirinkti, kokias kibernetinio saugumo priemones naudoti, bei kokią riziką jos gali toleruoti. Pasirenkamos saugumo priemonės turėtų stipriai priklausyti nuo juridinio asmens vykdomos veiklos. Pavyzdžiui vertinant tam tikrą bendrovę užsiimančia smulkia prekyba,

[7] Autoriaus nuomone atsakomybės be kaltės instituto taikymas kibernetinio saugumo kontekste yra abejotinas, kadangi kibernetinio saugumo specialistai vienbalsiai skelbia, kad paprastai neįmanoma užtikrinti visiško kibernetinio saugumo.

toks reguliavimas gali būti laikomas tinkamu. Tačiau vertinant juridinius asmenis vykdančius tam tikrą visuomenei itin svarbią veiklą (pvz. sveikatos priežiūra), darbo autoriaus nuomone yra sveikintinas esamas reguliavimas, kai tam tikros veiklos sferos, sektoriai, ir kt. yra pripažįstami turintys ypatingą svarbą ir priskiriami tam tikrai Kibernetinio saugumo subjektų kategorijai, kuriai keliami aukštesni techninių ir organizacinių priemonių reikalavimai, kurie šiems subjektams turėtų padėti užtikrinti duomenų saugumą ir vykdomos veiklos tęstinumą nepriklausomai nuo įvykusių kibernetinių incidentų.

Kaip jau buvo minėta, Kibernetinio saugumo reikalavimų apraše, yra išdėstyti tam tikri techniniai reikalavimai taikomi Kibernetinio saugumo subjektams. Nors šių reikalavimų pobūdis ir yra techninis, tačiau jie gali būti aktualūs vertinant konkrečias bendrovių pareigas, bet suteikti galimybę įvertinti 2.1. dalyje išdėstytas bendrąsias vadovų pareigas. Kibernetinio saugumo reikalavimų aprašo 5 p. nurodoma, kad subjektai, <...>, ypatingos svarbos informacinės infrastruktūros valdytojai: (i) ne rečiau kaip kartą per metus ar po esminių organizacinių pokyčių organizuoja ir atlieka rizikos vertinimą; (ii) atsižvelgdami į atlikto rizikos vertinimo rezultatus, taip pat jeigu nustatoma kibernetinių incidentų valdymo ir šalinimo, organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, tobulina informacinių išteklių veiklos tęstinumo valdymo planus ar kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus, rengia nustatytų trūkumų ataskaitas, kurios teikiamos NKSC; (iii) kartu su NKSC tvirtina kibernetinio saugumo politikos įgyvendinimo dokumentus, kuriuose be kita ko numatoma: kibernetinio saugumo politikos ir jos įgyvendinimo dokumentų taikymas ir naudojimas, sistemų naudotojų pareigos ir funkcijos, susijusios su kibernetiniu saugumu, bei šių naudotojų, kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, mokymai kibernetinio saugumo klausimais, įsibrovimų aptikimas ir prevencija, naudotojų vardų ir slaptažodžių sudarymas, apsauga ir keitimo tvarka, duomenų šifravimo nuostatos, dokumentai susiję su nustatytais pažeidžiamumais, ir užfiksuotais kibernetiniais incidentais, elektroninio pašto naudojimo tvarka, ir kt.; (iv) ne rečiau kaip kartą per metus organizuojamas atitikties reikalavimams vertinimas, naudotojų veiksmų audito įrašų analizė, šalinamos pastebėtos neatitiktys ir vykdomi naudojamų priemonių naudotojų vardų ir slaptažodžių sudarymas, apsauga ir keitimas, ir kita.

Taigi, atsižvelgdami į techninių pareigų išsamumą, galime tik konstatuoti faktą, kad Lietuvos Respublikos teisės aktai numato išsamų techninių priemonių skirtų Kibernetinio saugumo subjektų kibernetinio saugumo užtikrinimui. Akivaizdu, kad šios priemonės yra

daug išsamesnės ir konkretesnės, lyginant su bendrosiomis bendrovių pareigomis susijusiomis su kibernetiniu saugumu išdėstytomis šio darbo 2.1. dalyje.

3. PAVEDIMAS VYKDYTI KIBERNETINIO SAUGUMO UŽTIKRINIMO IR SUSIJUSIAS PAREIGAS BEI ŠIŲ PAREIGŲ VYKDYMO PRIEŽIŪRA

Pažymėtina, kad Lietuvos Respublikoje, skirtingai nei daugelyje kitų ES valstybių, bendrovės gali turėti tik vieną juridinio asmens vadovą. Todėl, praktiškai visa atsakomybė už bendrovės veiklos organizavimą yra koncentruojama administracijos vadovui (bendrovėse paprastai vadinamam direktoriumi). Bendruoju atveju, bendrovės valdymas yra pareigų ir tam tikrų funkcijų, kurias vykdo už įmonę atsakingi asmenys (pvz.: vadovas, valdyba ar stebėtojų taryba), visuma, siekiant bendrovei suteikti strateginę kryptį, užtikrinti, kad būtų pasiekti užsibrėžti tikslai, įsitikinti, kad rizikos valdomos tinkamai, ir patikrinti, ar įmonės ištekliai naudojami atsakingai. Atsižvelgiant į tokį reguliavimą kyla klausimas dėl vadovo atsakomybės, kai tam tikras funkcijas, pavyzdžiui nagrinėjamo darbo kontekste svarbią kibernetinio saugumo užtikrinimo funkciją, vadovas perduoda kitiems asmenims – įmonės darbuotojams (pvz. IT specialistams) ar tretiesiems asmenims teikiantiems informacinių technologijų ar kibernetinio saugumo paslaugas. Bendrovės valdoma rizika ir ištekliai gali būti siejami su tam tikromis skirtingomis sritimis (pvz.: informacinėmis technologijomis, finansais, rinkodara ir t.t.), tačiau skirtingų sričių rizikoms vertinti ir valdyti reikia specialių žinių. Taigi atitinkamai turėtų būti organizuojamas ir įmonės valdymas – paskirstant tam tikrų rizikų valdymą. Šioje dalyje bus nagrinėjama vadovo teisė pavesti tam tikras funkcijas vykdyti bendrovės darbuotojams ar tretiesiems asmenims, bei susiję vadovo ir asmenų, kuriems buvo pavestas šių funkcijų vykdymas, atsakomybės klausimai.

3.1. Vadovo teisė pavesti vykdyti kibernetinio saugumo užtikrinimo pareigas vidiniuose bendrovės santykiuose

Didėjant informacinių technologijų panaudojimui, ar jų panaudojimui tampant beveik neišvengiamu siekiant išlaikyti konkurencingumą rinkoje, daugelis vadovų supranta kibernetinio saugumo svarbą, tačiau ne visada žino, kaip turėtų būti vertinamos kibernetinio saugumo rizikos, bei kokia infrastruktūra yra reikalinga siekiant padidinti atsparumą

kibernetiniams incidentams. Nepaisant kibernetinio saugumo temos naujumo ir žinių stokos, galime išvesti paralelę tarp kibernetinio saugumo užtikrinimo ir kitų bendrovės vadovo veiklos krypčių, kurios reikalauja tam tikrų specifinių žinių ar įgūdžių, pvz. finansais, viešaisiais pirkimais, sandoriais, ir t.t. Dažnu atveju, bendrovės vadovas paveda šiuos uždavinius vykdyti kitiems bendrovės darbuotojams ar tretiesiems asmenims, todėl nagrinėtas ir vadovo pareigų, susijusių su kibernetiniu bendrovės saugumu pevedimas, bei atitinkami atsakomybės klausimai.

Kibernetinio saugumo reikalavimų aprašo 3.1. dalyje nurodoma, kad Kibernetinio saugumo subjektai paskiria už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingą asmenį arba asmenis ir nustato jiems taikomus kvalifikacinius reikalavimus. Atsakingu asmeniu gali būti skiriamas Kibernetinio saugumo subjekto darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu. Atsižvelgiant į tokią aprašo formuluotę, galime daryti išvadą, kad atsakomybės už kibernetinio saugumo užtikrinimą paskirstymas bendrovėje (perduodant šią atsakomybę kitiems nei vadovas asmenims) ar perdavimas tretiesiems asmenims yra įprasta praktika, bent jau tarp Kibernetinio saugumo subjektų (atsižvelgiant į paprastai ženkliai didesnį bendrovės darbuotojų kiekį ir vykdomų procesų sudėtingumą). Tuo tarpu manytina, kad pareiga skirti šiuos asmenis, bei atsakomybė tais atvejais kai tokie asmenys nėra skiriami tenka bendrovės veiklą organizuojančiam vadovui.

Pažymėtina, kad nors ABĮ ar kituose teisės aktuose nėra eksplicitiškai nustatyta vadovo teisė tam tikras pareigas pavesti vykdyti kitiems bendrovės darbuotojams ar tretiesiems asmenims, tačiau nepaisant to, ir remiantis civilinėje teisėje dominuojančiu dispozityvumo principu, įstatymas nedraudžia tam tikras funkcijas perduoti darbuotojams ar kitiems asmenims, pavyzdžiui sudarant darbo sutartis, atitinkamas funkcijas pavedant bendrovės įstatuose, pareigų aprašymuose ar kituose vidiniuose teisės aktuose ar sutarties pagrindu. Praktikoje tokie darbuotojai, kuriems perduodamos teisės ir pareigos tvarkyti tam tikrą bendrovės veiklos sritį (pvz. bendrovės rinkodarą, finansus, informacinių technologijų saugumą, ir t.t.), paprastai vadinami funkciniais arba tam tikrų (pvz. informacinių technologijų) padalinių vadovais. Nustatant funkcinio/padalinio vadovo pareigų ir atsakomybės klausimą, ypač svarbu atsižvelgti, ar konkrečios pareigos buvo tinkamai perduotos darbuotojui. T.y. turėtų būti atsižvelgiama į konkretaus asmens paskyrimo vykdyti tam tikras pareigas nustatančių dokumentų turinį bei faktą, kad asmuo kuriam skiriamos papildomos pareigos yra su jomis supažindintas, su jomis sutinka bei patvirtina, kad objektyviai gali (turi reikiamą išsilavinimą, kompetencijos ir žinių tam tikroje srityje)

jas eiti, bei yra gautas tai patvirtinantis rašytinis sutikimas. Paprastai siekiant išvengti ginčų, tokio darbuotojo vykdomos funkcijos ir atsakomybės klausimai turėtų būti aiškiai ir išsamiai aprašyti pareigybės aprašyme ar kituose bendrovės vidaus tvarkos dokumentuose. Pažymėtina, kad funkcinių vadovų sąvoka yra minima ir Lietuvos Vyriausiojo Administracinio Teismo praktikoje, pavyzdžiui nutartyje priimtoje administracinėje byloje Nr. eA-324-442/2022, kurioje buvo nagrinėjamas juridinio asmens atsakomybės, už personalo vadovės atliktus neteisėtus veiksmus klausimas (Lietuvos Vyriausiojo Administracinio Teismo 2022 m. vasario 23 d. nutartis administracinėje byloje Nr. eA-324-442/2022).

Tais atvejais, kai valdyba (ar nagrinėjamu atveju - vadovas) tinkamai (t.y. laikantis tam nustatytų procedūrų, bendrovės įstatų, ir kt.) pavedė kitam asmeniui atlikti tam tikras pareigas ar konkrečius veiksmus, laikytina, kad tai savaime nepažeidžia vadovo pareigos elgtis rūpestingai, protingai ir kvalifikuotai. Tinkamas pavedimo laipsnis yra leistinas ir dažnai būtinas, o tam tikras darbų pasidalinimas, pavedimai bei atitinkamas atsakomybės pasidalijimo laipsnis bendrovėje paprastai yra neišvengiamas. Pažymėtina, kad tam tikrų pareigų pavedimas neatleidžia vadovo nuo pareigos, prižiūrėti kaip yra vykdomos pavestos funkcijos, o šios pareigos nevykdymas gali būti laikomas vadovo pareigų pažeidimu. Todėl bet koks funkcijų pavedimas turi būti pagrįstas, o funkcijas pavedantis asmuo turi įsitikinti, kad atitinkamas darbuotojas yra pajėgus atlikti pavestus uždavinius. Tai, kokias funkcijas yra tikslinga pavesti vykdyti kitiems asmenims, iš esmės priklauso nuo įmonės dydžio ir vykdomos veiklos pobūdžio. Pavyzdžiui, didelės įmonės valdyba vadovas greičiausiai bus priverstas pavesti daugiau funkcijų. Vadovas (pavesdamas atitinkamas funkcijas), pažeidžiantis pareigą elgtis protingai, rūpestingai ir kvalifikuotai gali būti atsakingas bendrovei už sukeltos žalos atlyginimą (Michael Currie 2017. Delegation of Company Directors' Power [interaktyvus, žiūrėta 2022-03-31], prieiga per internetą: https://www.dallasmcmillan.co.uk/Blog/Corporate/delegation.html).

Nagrinėjant konkrečius pareigų pavedimo ir vadovo atsakomybės klausimus, vertėtų sugrįžti ir prie 2 dalyje nagrinėtos pareigos, užtikrinti kibernetinį bendrovės saugumą, kilmės klausimų. Nustačius, kad reguliuojamuose sektoriuose pareiga užtikrinti kibernetinį saugumą kyla pagal įstatymą, galime daryti išvadą, kad vadovo pareigos prižiūrėti pavestų funkcijų vykdymą intensyvumas atitinkamai padidėja, t.y. civilinė atsakomybė vadovui galėtų kilti ir dėl nerūpestingo jo elgesio.

Tuo tarpu vertinant vadovo atsakomybę už pavestas kibernetinio saugumo užtikrinimo funkcijas nereguliuojamuose sektoriuose, galime teigti, kad pavestos funkcijos vykdymo priežiūros pareigos intensyvumas turėtų būti nustatomas pagal *bonus pater*

familias standartą, o civilinė atsakomybė vadovui kiltų tik nustačius didelį jo neatsargumą ar tyčią.

Nagrinėjant užsienio šalių vadovų teisę pavesti tam tikras pareigas vykdyti kitiems asmenims, galima paminėti ir Harvardo universiteto bendrovių valdymo forume išsakytą poziciją, pagal kurią valdyba įgaliojimus ir atsakomybę už įmonės veiklą perduoda direktoriui, o per generalinį direktorių - vadovybei. <...> Vadovybė, vadovaujama generalinio direktoriaus, yra atsakinga už bendrovės strategijų nustatymą, valdymą ir įgyvendinimą. <...> Valdyba turėtų sukurti rizikos priežiūros ir atsakomybės komitetams bei vyresniajai vadovybei pavedimo, tvarką <...> Vadovybė nustato pagrindines įmonės verslo ir veiklos rizikas, įskaitant susijusias su stichinėmis nelaimėmis, valdymo spragomis, fiziniu ir kibernetiniu saugumu, reguliavimo pokyčiais ir kt. (Harvard Law School Forum on corporate governance, 2016. Principles of Corporate Governance [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://corpgov.law.harvard.edu/2016/09/08/principles-of-corporate-governance/). Atsiribojant nuo bendrovių valdymo modelių skirtumų ir atskirų bendrovių vadovybės struktūros aspektų, darbo autoriaus nuomone, šis pavyzdys parodo, kad bendrovės turėtų siekti pareigų pasidalinimo, o bendrovės vadovo teisė pavesti tam tikras pareigas tretiesiems asmenims yra neišvengiama ir net sveikintina. Kibernetinio saugumo klausimas gali būti laikomas neblogu pavyzdžiu iliustruojančiu bendrovės vadovo poreikį pavesti tam tikras funkcijas kitiems asmenims. Dėl kibernetinio saugumo klausimų specifiškumo, bendrovės, kurioms atsižvelgiant į jų vykdomą veiklą kyla didelė kibernetinė rizika (pvz. Kibernetinio saugumo subjektai), paprastai yra sudariusios atitinkamas sutartis su informacinių technologijų specialistais, t.y. tokios bendrovės samdo išorinius šių paslaugų teikėjus - profesionalus, kurie tvarko bendrovės kompiuterinių technologijų ūkį ir su jo saugumu susijusius klausimus. Šie atvejai bei atitinkami atsakomybės klausimai bus aptariami sekančioje darbo dalyje.

3.2. Asmenų atsakomybė už jiems pavestą vykdyti bendrovės kibernetinio saugumo užtikrinimą

Vertinant darbuotojo, kuriam buvo pavesta pareiga užtikrinti kibernetinio saugumo atsakomybės klausimus, būtina pabrėžti, kad nepriklausomai nuo to, kad atitinkamą pareigą darbuotojui paveda vadovas, tai savaime nesukuria prielaidų šiam darbuotojui taikyti civilinės atsakomybės instituto, kuris būtų pritaikytas aptariamas pareigas vykdant pačiam vadovui. Pažymėtina, kad turtinė darbuotojų atsakomybė galima tik pagal darbo teisės normas, o Lietuvos Respublikos darbo kodekso (Lietuvos Respublikos Darbo Kodeksas,

TAR, 2016-09-19, Nr. 23709) (toliau – **Darbo kodeksas**) 153 str. numato, kad darbuotojas privalo atlyginti visą padarytą turtinę žalą, bet ne daugiau kaip jo trijų vidutinių darbo užmokesčių dydžio, o jeigu turtinė žala padaryta dėl darbuotojo didelio neatsargumo, – ne daugiau kaip jo šešių vidutinių darbo užmokesčių dydžio. Taigi, priešingai nei civilinė atsakomybė, kuriai galioja visiško žalos atlyginimo principas, žalos atlyginimas pagal darbo teisės normas yra ribojamas[8].

Nagrinėjant asmenų, kuriems pavedamos teises ir pareigos susijusios su kibernetiniais incidentais ir duomenų apsauga, vertėtų skirti dėmesio tretiesiems asmenims teikiantiems informacinių technologijų paslaugas. Bendrovės vykdančios tam tikrą ūkinę - komercinę veiklą kurioje naudojamos pažangios informacinės technologijos, paprastai naudojasi tam tikromis ryšio, serverių, informacinių technologijų infrastruktūros, techninių sistemų darbo priežiūros ar kitomis panašiomis paslaugomis. Atsižvelgiant į tai, kad minėtų paslaugų teikėjai yra susiję su bendrovei teikiamomis informacinių technologijų paslaugomis, nagrinėtinas klausimas, dėl šių paslaugų teikėjų pareigų ir civilinės atsakomybės susijusios su kibernetiniais incidentais. Paprastai, bendrovės siekiančios gauti tam tikras informacinių technologijų paslaugas sudaro sutartis su atitinkamų informacinių technologijų paslaugų teikėjais, todėl galime daryti išvadą, kad šalis sieja sutartiniai teisiniai santykiai. Todėl asmenims teikiantiems kibernetinio saugumo paslaugas gali kilti sutartinė atsakomybė už konkrečių sutartyje numatytų sąlygų pažeidimą, bet deliktinė civilinė atsakomybė pagal bendrąsias deliktinės atsakomybės sąlygas.

Kibernetinio saugumo principai numato, kad už ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai. T.y. šiuo principu įtvirtinama subsidiari informacinių technologių paslaugas gaunančių ir jas teikiančių subjektų atsakomybė, įvykus kibernetiniam incidentui[9]. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo ir Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480, 589 str. ir priedo pakeitimo įstatymo projektų aiškinamajame rašte (Nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. Xii-1428 pakeitimo įstatymo ir Lietuvos Respublikos administracinių nusižengimų

[8] Atsakomybės ribojimo išimtys numatytos Darbo kodekso 154 str..

[9] Pažymėtina, kad skolininkų atsakomybės klausimas šiame darbe nebus nagrinėjamas iš esmės, kadangi siekiant atlikti detalesnę analizę reikėtų nagrinėti konkrečią šalių sudarytą sutartį, tačiau atsižvelgiant į tokio pobūdžio sutartyse dominuojančias konfidencialumo sąlygas, išsamesnė analizė tampa negalima. Visgi, siekiant atskleisti Kibernetinio saugumo įstatyme įtvirtinto subsidiarumo principo esmę, gali būti nagrinėjama bendroji, teorinė skolininkų subsidiarumo problematika kibernetinių incidentų kontekste.

kodekso 479, 480, 589 str. ir priedo pakeitimo įstatymo projektų pateikimo Lietuvos Respublikos Seimui, TAR, 2018-03-29, Nr. 4776) nurodoma, kad atsižvelgiant į besikeičiantį kibernetinio saugumo teisinį reguliavimą, kibernetinio saugumo principų sąrašą siūloma papildyti ir subsidiarumo principu, kurio esmė: už ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas teikiantys kibernetinio saugumo subjektai, o srityse, kurios priklauso išimtinei Kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas teikiantys kibernetinio saugumo subjektai. Pažymėtina, kad teismai šiuo klausimu nėra suformulavę praktikos, tačiau darbo autoriaus nuomone, toks subsidiarumo principo perkėlimo į įstatymą išaiškinimas nėra pakankamas, kadangi nėra aišku, kokiu būdu jis turėtų būti taikomas, bei ar šis principas yra taikytinas civilinės atsakomybės klausimams už kibernetinio saugumo pažeidimus spręsti, atsižvelgiant į tai, kad Kibernetinio saugumo įstatymas reguliuoja ir „<...>viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų pareigas“.

Iš dalies gali būti pateisinamas įstatymų leidėjo siekis proteguoti nuo kibernetinių incidentų nukentėjusius asmenis (kurių duomenys buvo paskleisti ar kitaip paveikti), tačiau subsidiarumo principo taikymas informacinių paslaugų teikėjo (kaip antrinio kreditoriaus subsidiarioje prievolėje) atžvilgiu neproporcingai apsunkina informacinių paslaugų teikėją. Sudarydamas tam tikrą paslaugų sutartį teikti konkrečia sutartimi apibrėžtas paslaugas, šių paslaugų teikėjas prisiima riziką, kurios visiškai negali ir neturi teisės kontroliuoti. Štai pavyzdžiui įmonė A suteikia įmonei B informacinių technologijų – kompiuterinės prieglobos (angl. *hosting*) paslaugas. Teoriškai, įmonės atitinka Kibernetinio saugumo įstatyme numatytą situaciją, taigi A ir B įmonės prieš nukentėjusius trečiuosius asmenis atsakytų subsidiariai. Atkreiptinas dėmesys, kad kibernetinių incidentų sukeliama žala paprastai yra kompleksinė ir susideda iš daugelio dedamųjų, tačiau ekspertams atlikus informacinių technologijų auditą, paprastai įmanoma nustatyti kokie veiksmai ar jų neatlikimas nulėmė galimybę kilti incidentui, t.y. paprastai nekyla sunkumų nustatant priežastinį ryšį[10] (Microtrend, Bridging Cybersecurity Gaps with Managed Detection and Response, 2018 [interaktyvus, žiūrėta 2022-04-09]. Prieiga per internetą: https://www.trendmicro.com/vinfo/hk-en/security/news/security-technology/bridging-

[10] Kibernetinio saugumo specialistai tam naudoją ir specialią „pagrindinės priežasties analizės“ sąvoką (angl. *root cause analysis*), kurios tikslas nustatyti konkrečią priežastį, kuri leido kilti kibernetiniam incidentui.

cybersecurity-gaps-with-managed-detection-and-response). Darbo autoriaus nuomone, subsidiarumo principo pritaikymas civiliniuose teisiniuose santykiuose įvykus kibernetiniam incidentui gali būti problematiškas ir ne visais atvejais atitikti kitus teisinės valstybės principus. Nors kibernetiniai incidentai ir gali pasireikšti ypač sudėtingais reiškiniais vykstančiais skaitmeninėje – kompiuterinėje erdvėje, tačiau nepaisant to, informacinių paslaugų teikėjo ir jų gavėjo pareigos susijusios su kibernetiniu saugumu yra gan aiškios ir paprastai gali būti atskirtos. Nustačius priežastinį ryšį tarp konkrečių veiksmų / neveikimo ir kilusių padarinių, gali būti nustatomas ir subjektas, kuriam teko pareiga imtis atitinkamų priemonių, kad užkirsti kelią kibernetiniam incidentui. Taigi, kibernetinio saugumo užtikrinimo procesų kompleksiškumas nesuponuoja būtinybės taikyti subsidiarią atsakomybę.

Taip pat, subsidiarumo principo taikymas kritikuotinas ir dėl to, kad kibernetinių incidentų metu kilusios žalos dydis gali stipriai priklausyti nuo kibernetinio incidento šalinimo spartos. T.y. galimos situacijos, kai kibernetinio incidento sukelta žala eksponentiškai didėja vien dėl to, kad kibernetinio incidento paveikta bendrovė B gaunanti pavyzdyje minėtas prieglobos paslaugas nesiima tam tikrų veiksmų ar nebuvo iš anksto pasirengus kibernetiniam incidentui (pvz. nebuvo iš anksto parengtas verslo tęstinumo planas, atliktos duomenų kopijos ar suburta kibernetinio incidento valdymo komanda, ir kt.), kurie dažnu atveju gali priklausyti ir nuo komercinių bendrovės sprendimų (pvz. bendrovė apsisprendė neinvestuoti papildomų lėšų į atsarginių duomenų kopijų saugojimą). Tokiu atveju bendrovei B neatsiskaičius su savo kreditoriais (pvz. nukentėjusiais asmenimis), bendrovė A kaip subsidiari skolininkė būtų priversta atlyginti kreditorių patirtą žalą.

Kita vertus, galimos ir tokios situacijos kai informacines paslaugas teikianti bendrovė netinkamai vykdė savo sutartinius įsipareigojimus (pvz. laiku neįdiegtos reikalingos serverių apsaugos sistemos), ar dėl įvykusio pažeidimo kalti abu kontrahentai. Tačiau pabrėžtina, kad tokiu atveju bendroji kontrahentų atsakomybė galima ir pagal bendrąsias civilinės atsakomybės normas, t.y. nėra būtinas šio principo perkėlimas į Kibernetinio saugumo įstatymą, nenumatant jo pritaikomumo gairių ar paaiškinimų.

Pažymėtina, kad subsidiarumo principas nėra įprastas ar plačiai taikomas ir kitose valstybėse, štai pavyzdžiui pagal JAV reguliavimą, duomenų savininkas yra atsakingas už nuostolius, atsiradusius dėl kibernetinio duomenų pažeidimo, net jei dėl saugumo sutrikimų kaltas duomenų saugotojas (debesijos paslaugų teikėjas) (Thomson Reuters, Who is liable

then a data breach occurs? [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://legal.thomsonreuters.com/data-breach-liability).

Darbo autoriaus nuomone, subsidiarumo principas numatytas kibernetinio saugumo įstatyme turėtų būti taikomas ypač ribotai ir atsižvelgiant į konkrečią situaciją, kadangi platus šio principo pritaikymas sudėtingose kibernetinio saugumo situacijose gali prieštarauti civilinės atsakomybės instituto prasmei, protingumo, sąžiningumo ir teisinės valstybės principams.

IŠVADOS

1. Kibernetinių incidentų rizika bendrovių teisės kontekste gali būti apibrėžiama kaip tikimybė, kad konkrečioje bendrovėje, atsižvelgiant į jos (ne)naudojamas kibernetinio saugumo priemones, įvyks kibernetinis incidentas. Svarbi kibernetinės rizikos valdymo dedamoji yra bendrovės kibernetinio saugumo užtikrinimas ir tam pasitelktos priemonės, įrankiai ar sprendimai, vykdomi procesai. Svarbu pažymėti, kad kibernetinė rizika ir iš kibernetinio incidento kylanti žala gali pasireikšti ne tik pačiai bendrovei, bei jos vykdomai veiklai, bet ir bendrovės kontrahentams ir tretiesiems asmenims.
2. Bendruoju atveju (bendrovėms, kurių kibernetinio saugumo pareigų nereguliuoja papildomi teisės aktai), bendrovių vadovams gali kilti pareiga užtikrinti kibernetinį bendrovės saugumą, tačiau šios pareigos kilmė priklauso nuo bendrovės vykdomos veiklos. Manytina, kad dėl ypač didelės įvairių bendrovių vykdomų procesų skaitmenizacijos, kibernetinio saugumo užtikrinimas galėtų būti priskiriamas prie bendrovės vadovo pareigos organizuoti bendrovės veiklą. Kadangi nėra kito objektyvaus kriterijaus, pagal kurį galėtų būti nustatomas vadovo pareigos užtikrinti kibernetinį saugumą intensyvumas ir pritaikomumas, taikytinas *bonus pater familias* standartas.
3. Sektorinio reguliavimo atveju ar bendrovių, kurios yra priskiriamos Kibernetinio saugumo subjektams, vadovams kyla konkrečios pareigos numatytos specialiuosiuose, konkrečių bendrovių veiklą reglamentuojančiuose įstatymuose, o taip pat, vadovams tenka pareiga užtikrinti konkrečių techninių priemonių, įtvirtintų Kibernetinio saugumo reikalavimų apraše, įgyvendinimą.
4. Bendrovių vadovai turi teisę pavesti bendrovės darbuotojams ar tretiesiems asmenims vykdyti pareigas susijusias su kibernetinio saugumo užtikrinimu.
5. Bendrovių vadovai, pavedę kibernetinio saugumo užtikrinimo pareigų vykdymą darbuotojams ar tretiesiems asmenims privalo tinkamai prižiūrėti šių funkcijų vykdymą. Priežiūros pareigos intensyvumas priklauso nuo to, ar bendrovė, kurios vadovas pavedė tam tikrų funkcijų vykdymą: (i) priklauso nereguliuojamam sektoriui (kai bendrovei nėra keliami papildomi – specialieji kibernetinio saugumo užtikrinimo reikalavimai) – atsakomybė vadovui nustatoma pagal *bonus pater familias* strandartą ir kyla dėl vadovo didelio neatsargumo ar tyčios; ar reguliuojamam sektoriui (kuriam pagal įst. numatytos specialiosios su kibernetiniu saugumu susijusios pareigos) – atsakomybė tokiu atveju kyla ir dėl imperatyvių įstatymo normų pažeidimo, o šie veiksmai gali būti (ne)atliekami ir neatsargiai.

6. Nėra iki galo aiškus kibernetinio saugumo įstatyme įtvirtinto kibernetinio saugumo subsidiarumo principo panaudojimas. Darbo autoriaus nuomone, šio principo pritaikomumas civiliniuose teisniuose santykiuose gali būti problematiškas ir prieštarauti kitiems bendriesiems teisės principams.

ŠALTINIŲ SĄRAŠAS

I. NORMINIAI ŠALTINIAI

Lietuvos Respublikos teisės aktai

1. Lietuvos Respublikos Administracinių nusižengimų kodeksas, TAR, 2015-07-10, Nr. 11216.
2. Lietuvos Respublikos Civilinis kodeksas, Valstybės žinios, 2000-09-06, Nr. 74-2262.
3. Lietuvos Respublikos Darbo Kodeksas, TAR, 2016-09-19, Nr. 23709.
4. Lietuvos Respublikos akcinių bendrovių įstatymas, Valstybės žinios, 2000-07-31, Nr. 64-1914.
5. Lietuvos Respublikos elektroninių ryšių įstatymas, Valstybės žinios, 2004-04-30, Nr. 69-2382.
6. Finansų įstaigų įstatymas, Valstybės žinios, 2002-09-18, Nr. 91-3891.
7. Lietuvos Respublikos kibernetinio saugumo įstatymas, TAR, 2014-12-23, Nr. 20553.
8. Lietuvos Respublikos sveikatos sistemos įstatymas, Valstybės žinios, 1994-08-17, Nr. 63-1231.
9. Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymas, Valstybės žinios, 1996-10-23, Nr. 102-2317.
10. Nacionalinis kibernetinių incidentų valdymo planas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“.

II. SPECIALIOJI LITERATŪRA

11. Zaleskis, J., 2019. Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija, Vilnius: Registrų centras.
12. Abramavičius A., Mikelėnas V. 1999, Įmonių vadovų teisinė atsakomybė, antras leidimas, VĮ Teisinės informacijos centras, Vilnius.

III. TEISMŲ PRAKTIKA

13. Lietuvos Aukščiausiojo Teismo 2006 m. gegužės 25 d. nutartis, civilinėje byloje Nr. 3K-7-266/2006.

14. Lietuvos Aukščiausiojo Teismo 2008 m. gegužės 12 d. nutartis civilinėje byloje Nr. 3K-3-267/2008.
15. Lietuvos Aukščiausiojo Teismo 2013 m. lapkričio 20 d. nutartis civilinėje byloje Nr. 3K-3-581/2013.
16. Lietuvos Aukščiausiojo Teismo 2013 m. gruodžio 20 d. nutartis civilinėje byloje Nr. 3K-3-699/2013.
17. Lietuvos Aukščiausiojo Teismo 2016 m. birželio 3 d. nutartis civilinėje byloje Nr. 3K-3-298-701/2016.
18. Lietuvos Aukščiausiojo Teismo 2017 m. spalio 16 d. nutartis civilinėje byloje Nr. 3K-7-177-701/2017.
19. Lietuvos Aukščiausiojo Teismo 2018 m. rugsėjo 21 d. nutartis civilinėje byloje Nr. 3K-3-326-1075/2018.
20. Lietuvos Aukščiausiojo Teismo 2021 m. gruodžio 2 d. nutartis civilinėje byloje Nr. e3K-3-300-313/2021.
21. Lietuvos Vyriausiojo Administracinio Teismo 2022 m. vasario 23 d. nutartis administracinėje byloje Nr. eA-324-442/2022.
22. Bendrovės valdymo organų civilinę atsakomybę reglamentuojančių teisės normų taikymo Lietuvos Aukščiausiojo Teismo praktikoje apžvalga.

IV. TRAVAUX PRÉPARATOIRES

23. 2021 m. birželio 2 d. Bulgarijos Aukščiausiojo Administracinio Teismo prašymas priimti prejudicinį sprendimą, Europos Sąjungos Teisingumo Teismo byloje Nr. C-340/21 [interaktyvus, žiūrėta 2022-03-29], prieiga per internetą: https://curia.europa.eu/juris/documents.jsf?oqp=&for=&mat=or&lgrec=en&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-340%252F21&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=en&avg=&cid=1758136.
24. Nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. Xii-1428 pakeitimo įstatymo ir Lietuvos Respublikos administracinių nusižengimų kodekso

479, 480, 589 str. ir priedo pakeitimo įstatymo projektų pateikimo Lietuvos Respublikos Seimui, TAR, 2018-03-29, Nr. 4776.

V. KITA LITERATŪRA

25. Krašto apsaugos ministerija, 2020. NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA 2020 [interaktyvus, žiūrėta 2022-04-06]. Prieiga per internetą: https://kam.lt/download/70748/2020%20m.%20nacionalinio%20kibernetinio%20saugumo%20b%C5%ABkl%C4%97s%20ataskaita%20el.%20versija.pdf.
26. Purplesec, 2021. Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends [interaktyvus, žiūrėta 2022-04-06]. Prieiga per internetą: https://purplesec.us/resources/cyber-security-statistics/.
27. Michael Currie 2017. Delegation of Company Directors' Power [interaktyvus, žiūrėta 2022-03-31], prieiga per internetą: https://www.dallasmcmillan.co.uk/Blog/Corporate/delegation.html
28. TrendMicro. CAN YOU BE READY FOR A YOU DON'T KNOW ABOUT? The Art of Zero-Day Threat Coverage [interaktyvus, žiūrėta: 2022-03-28]. Prieiga per internetą: https://resources.trendmicro.com/rs/945-CXD-062/images/Trend-Micro_eBook_The-Art-of-Zero-Day-Threat-Coverage.pdf).
29. Robert Mueller kalba per 2012 m. RSA kibernetinio saugumo konferenciją [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.
30. Krašto apsaugos ministerija, NKSC, 2020. KIBERNETINIS SAUGUMAS IR VERSLAS Ką turėtų žinoti kiekvienas įmonės vadovas [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://kam.lt/download/68737/kibernetinio%20saugumo%20vadovas%20verslui.pdf.
31. Susan Moore (2020), Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024 [interakyvus, žiūrėta 2022-03-22]], prieiga per internetą: https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl.
32. Centre for Cyber Security Belgium, 2021. CYBER SECURITY INCIDENT MANAGEMENT GUIDE [interaktyvus, žiūrėta 2022-03-22], prieiga per internetą:

https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf.

33. Thomson Reuters, Who is liable then a data breach occurs? [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://legal.thomsonreuters.com/data-breach-liability.
34. Microtrend, Bridging Cybersecurity Gaps with Managed Detection and Response, 2018 [interaktyvus, žiūrėta 2022-04-09]. Prieiga per internetą: https://www.trendmicro.com/vinfo/hk-en/security/news/security-technology/bridging-cybersecurity-gaps-with-managed-detection-and-response.
35. Kembridžo žodynas [interaktyvus, žiūrėta: 2022-04-01]. Prieiga per internetą: https://dictionary.cambridge.org/dictionary/english/confidential.
36. Harvard Law School Forum on corporate governance, 2016. Principles of Corporate Governance [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://corpgov.law.harvard.edu/2016/09/08/principles-of-corporate-governance/).
37. Gartner, 2021. When it Comes to Ransomware, Should Your Company Pay? [interaktyvus, žiūrėta 2022-04-01]. Prieiga per internetą: https://www.gartner.com/en/articles/when-it-comes-to-ransomware-should-your-company-pay.
38. Kyle Johnson, 2021. Should companies pay after ransomware attacks? Is it illegal? [interaktyvus, žiūrėta 2022-04-03]. Prieiga per internetą: https://www.techtarget.com/searchsecurity/tip/Should-companies-pay-ransomware-and-is-it-illegal-to.
39. NKSC, 2021. Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) įspėja apie pavojingų „ransomware“ tipo virusų suaktyvėjimą [interaktyvus, žiūrėta 2022-04-05]. Prieiga per internetą: https://www.nksc.lt/naujienos/demesio_plinta_virusai_uzsifruojantys_failus.html.
40. Nacionalinis JK kibernetinio saugumo centras, 2020. Mitigating malware and ransomware attacks [interaktyvus, žiūrėta 2022-04-05]. Prieiga per internetą: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

SANTRAUKA

Kibernetinė rizika yra neišvengiama praktiškai kiekvienos bendrovės veiklos dalis, kuri gali būti mažinama (tačiau negali būti visiškai eliminuojama) pasitelkiant tam tikras kibernetinio saugumo priemones. Bendrovėms kylanti kibernetinė rizika gali pasireikšti ne tik žala pačiai bendrovei (prarasta informacija, reputacinė žala, ir kt.) tačiau ir žala kontrahentams – verslo partneriams (konfidenciali informacija) ir tretiesiems asmenims (prarasti duomenys). Atsakingi bendrovių vadovai (papildomai nereguliuojamuose sektoriuose) organizuodami bendrovės veiklą ir vykdydami savo fiduciarines pareigas bendrovei, turėtų laikytis *bonus pater familias* standarto ir apsvarstyti bei vertinti jų bendrovei kylančią kibernetinę riziką, o atlikus vertinimą taikyti atitinkamas rizikos mažinimo priemones, bei ruoštis galimam kibernetiniam incidentui. Tuo tarpu bendrovių, kurių veikla priskiriama tam tikriems papildomai reguliuojamiems sektoriams (pvz. finansų įstaigos) ir tam tikrų valstybės ekonomikai ypač svarbių subjektų, kurie yra priskiriami Kibernetinio saugumo subjektų sąrašui, vadovams kyla griežtesnės, imperatyviomis įstatymų normomis bei techniniais aprašais įtvirtintos kibernetinio saugumo užtikrinimo pareigos. Nepaisant to, kad pareiga užtikrinti kibernetinį bendrovės saugumą kyla bendrovės vadovui, organizuojančiam bendrovės veiklą, vadovai turi teisę šias pareigas pavesti vykdyti bendrovės darbuotojams (pvz. informacinių technologijų ar kt. rizikų valdymo specialistui) ar tretiesiems asmenims (pvz. išoriniams informacinių technologijų ar kibernetinio saugumo paslaugų teikėjams). Pažymėtina, kad vadovui pavedusiam pareigų vykdymą, išlieka pareiga prižiūrėti kaip šios pareigos yra vykdomos, o priežiūros pareigos intensyvumas ir apimtis nustatoma pagal pavedamos vykdyti pareigos kilmę. Už pavestas kibernetinio saugumo užtikrinimo pareigas bendrovės darbuotojas atsako Darbo Kodekse nustatyta tvarka, o trečiojo asmens civilinė atsakomybė gali kilti iš sutarties arba delikto.

SUMMARY

Cyber risk is an unavoidable part of virtually every business activity that can be reduced (but not completely eliminated) through certain cyber security measures. Cyber risk for companies can include not only damage to the company itself (lost information, reputational damage, etc.) but also damage to contractors - business partners (confidential information) and third parties (lost data). Responsible company executives (in sectors where there is no additional cyber regulation) should adhere to the bonus pater familias standard when organizing the company's activities and performing their fiduciary duties also consider and assess the cyber risks the managed company faces, and apply appropriate risk mitigation measures, prepare for a possible cyber incident. Meanwhile, the executives of companies operating in certain additionally regulated sectors (eg financial institutions) and certain entities of particular importance to the state economy, which are included in the list of cyber security entities, are subject to wider range of cyber security obligations established by mandatory legal norms and technical specifications. Although the obligation to ensure the cyber security of the company rests with the executive of the company, while organizing the company's activities, the executives have the right to entrust these responsibilities to the company's employees (eg information technology or other risk management specialist) or third parties (eg external information technology or cyber security service providers). It should be noted that the executive, which have entrusted performance of some the duties to other parties retains the duty to supervise the performance of these duties, while the intensity and scope of the duty of supervision shall be determined according to the origin of the assigned duty. An employee of the company shall be liable for the assigned cyber security duties in accordance with the procedure established in the Labour Code, and the civil liability of a third party may be subject contract or tort liability.