KIBERNETSKA VARNOST IN PREKRŠKI S PODROČJA KIBERNETSKE VARNOSTI

DOI
https://doi.org/10.18690/um.pf.1.2024.9

ISBN
978-961-286-817-8

ANDREJA PRIMEC,[1] BOJAN TIČAR[2, 3]

[1] Univerza v Mariboru, Ekonomsko-poslovna fakulteta, Maribor, Slovenija
andreja.primec@um.si
[2] Univerza v Mariboru, Fakulteta za varnostne vede Ljubljana
bojan.ticar@um.si
[3] Univerza v Mariboru, Pravna fakulteta Maribor, Slovenija
bojan.ticar@um.si

Kibernetska varnost je presegla okvirje informatike in zajema že vsa področja družbenega življenja. Vendar poleg ugodnosti, ki jih prinaša digitalizacija, le-ta predstavlja tudi nevarnost zlorabe elektronskega informacijskega potenciala. V Sloveniji ima pravica do kibernetske varnosti ustavne pravne podlage, sama informacijska varnost kot ožji del kibernetske pa je urejena v uredbah in direktivah EU. Kibernetska varnost igra ključno vlogo v delujoči ureditvi varnega pretoka informacij, integriteti celotnega informacijskega sistema in v preprečevanju zlorab pri uporabi digitalnih informacij. Pravna ureditev kibernetske in informacijske varnosti pomeni zagotavljanje ustreznega normativnega okvira, ki pravno omogoča nemoteni pretok elektronskih informacij brez nepooblaščenega dostopa tretjih, kakor tudi varuje uporabnike pred zlorabo ali uničenjem le-teh. Kibernetska varnost vključuje zaupnost, integriteto in dostopnost informacij, pa naj bodo le-te v digitalni, tiskani obliki ali kakšni drugi obliki. Poleg tega prispevek predstavlja analizo pravne ureditve predpisovanja in sankcioniranja prekrškov na področju kibernetske oz. informacijske varnosti z vidika sodobne slovenske informacijske zakonodaje.

Ključne besede:
kibernetska varnost, kibernetska ureditev, informacijski prekrški, sodobna informacijska zakonodaja, informacijski sistemi

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.1.2024.9

ISBN
978-961-286-817-8

CYBER SECURITY AND MINOR OFFENSES IN CYBER SECURITY

ANDREJA PRIMEC,[1] BOJAN TIČAR[2, 3]

[1] University of Maribor, Economic-Business Faculty, Maribor, Slovenia
andreja.primec@um.si
[2] University of Maribor, Faculty for Criminal Justice and Security, Ljubljana, Slovenia
bojan.ticar@um.si
[3] University of Maribor, Faculty of Law , Maribor, Slovenia
bojan.ticar@um.si

Keywords:
cyber security,
cyber regulation,
information offenses,
modern information
legislation,
information systems

Cybersecurity has expanded beyond IT to encompass all areas of social life. However, in addition to the benefits of digitisation, it also poses a risk of misusing the potential of electronic information. In Slovenia, the right to cybersecurity has a constitutional legal basis and the right to information security as a narrower partsubset of cybersecurity is regulated in the cybersecurity plays a crucial role in a functioning regime for the secure flow of information, the integrity of the entire of the information system and in preventing abuse in the use of digital information. The legal framework for cyber and information security entails ensuring an appropriate normative framework that legally enables the smooth flow of electronic information without unauthorised access by third parties and protects users against misuse or destruction. Cybersecurity includes the confidentiality, integrity and availability of data, whether digital, hard copy or otherwise. In addition, the contribution presents an analysis of the legal regulatory and sanctioning regime of offences in the cyber or information security field from the perspective of contemporary Slovenian information legislation.

University of Maribor Press

1 Uvod

Zaradi nenehnega tehnološkega razvoja postajamo vedno bolj digitalno usmerjena družba. Odvisnost od digitalnih naprav, orodij in od njihove povezljivosti – mednarodnega spleta, se povečuje. Ker se gospodarsko in družbeno življenje vse bolj seli v digitalna okolja, posledično tudi kriminaliteta prerašča standardne okvire. Skrb za varnost družbe in gospodarstva pred kibernetskimi napadi postaja vedno večji izziv tudi za Evropsko unijo (EU).

Komisija EU je aktivno posegla v to dogajanje s Strategijo Varnostne unije EU za obdobje od leta 2020 do 2025.[1] V njej so navedeni glavni ukrepi in orodja za zagotavljanje evropske varnosti v fizičnem in digitalnem svetu. Ključna sestavina strategije varnostne unije je Strategija EU za kibernetsko varnost, ki naj bi EU zagotovila tehnološko suverenost in s tem odpornost celotne EU pred kibernetskimi grožnjami.

Kibernetska varnost je eden izmed ključnih dejavnikov za izgradnjo digitalne Evrope. Poleg varstva podatkov, temeljnih pravic in varnosti, predstavlja kibernetska varnost enega od štirih stebrov družbe, ki izkorišča moč podatkov. EU mora za svoj nadaljnji razvoj in ohranjanje položaja med svetovno najuspešnejšimi gospodarstvi izkoristiti priložnosti digitalne dobe za krepitev industrijskih in inovacijskih zmogljivosti ter hkrati zagotoviti varne in etične okvire za uporabo sodobnih tehnologij, ki omogočajo shranjevanje, obdelovanje in prenašanje ogromne množice podatkov.[2]

Med ukrepi, s katerimi bo uresničila zastavljene cilje, sodi tudi oblikovanje ustreznega regulativnega okvira. Najpomembnejši zakonodajni akt EU s področja kibernetske varnosti je Direktiva 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji[3] (NIS direktiva). Republika Slovenija (RS) je direktivo implementirala leta 2018 z Zakonom o informacijski varnosti[4] (ZinfV). Kako hitro potekajo spremembe na področju kibernetske varnosti dokazuje tudi dejstvo, da je konec leta 2020 Komisija EU predlagala novo direktivo o ukrepih za

[1] Komisija a, 2020.
[2] Komisija b, 2020.
[3] UL L 194, 19. 7. 2016.
[4] Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23.

visoko skupno raven kibernetske varnosti v EU, ki bo nadgradila obstoječa pravila in hkrati razveljavila prvotno direktivo.

V nadaljevanju predstavljamo evropski in slovenski zakonodajni okvir kibernetske varnosti ter njeno institucionalno ureditev v RS. Največ pozornosti namenjamo prekrškom s področja kibernetske varnosti, njihovi materialnopravni ureditvi ter organom, ki na tem področju izvajajo dolžno nadzorstvo in izrekajo sankcije. Posebej izpostavljamo vprašanje odgovornosti za te prekrške. Medtem ko je določitev kazni (ki morajo biti učinkovite, sorazmerne in odvračilne) za kršitve nacionalnih določb, sprejetih na podlagi NIS direktive, v pristojnosti držav članic,[5] nova Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148[6] (NIS 2 direktiva) glede sankcioniranja kršitev prinaša pomembne spremembe. Po vzoru Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES[7] (Splošna uredba o varstvu podatkov, GDPR) predvideva za najhujše kršitve maksimalne kazni, ki so po višini enake kaznim za najhujše kršitve določb GDPR. Tudi to nakazuje, kako pomembno je (in bo) učinkovito izvajanje zahtev, postavljenih v evropski zakonodaji o kibernetski varnosti.

Pri pravni analizi ureditve kibernetskih prekrškov je uvodoma potrebno imeti v mislih tudi ustavno ureditev pravice do varnosti. Sodobno pojmovanje osebne varnosti tako na eni strani zajema osebno varnost pred nasiljem ali škodo, na drugi strani pa dostop do osnovnih človekovih in družbenih dobrin, kamor sodi tudi splet. Med drugim pravica do varnosti vključuje zaščito pred osebnim in strukturnim nasiljem in kriminaliteto ter varstvo pred drugimi družbenimi in naravnimi pojavi, ki ogrožajo posameznikovo osebno varnost. Sodobno razumevanje pojma osebne varnosti je v širšem smislu tesno prepleteno tudi s pojmom trajnostnega človekovega razvoja.[8]

[5] Določbe 21. člena NIS direktive.
[6] UL L 338, 27. 12. 2022.
[7] UL L 119, 4. 5. **2016.**
[8] B. Flander, B. Tičar, The Right to Security - An Outline of the Legal Regulation at the State and Local Levels in Slovenia, 2019, str. 422–438.

V skladu s 34. členom Ustave RS[9] ima vsakdo pravico do varnosti. To ustavno določbo vsebinsko napolnjujeta ustavna teorija in ustavno sodna praksa. Ustavno sodišče RS je v odločbi iz leta 1997[10] med drugim pojasnilo, da je pravica do osebne varnosti v prvi vrsti pravica negativnega statusa. Kot taka ta pravica državi, lokalnim skupnostim, drugim nosilcem javnih pooblastil in na splošno vsakomur nalaga dolžnost vzdržati se naklepnih nedopustnih posegov v integriteto in varnost posameznika, kamor sodi tudi kibernetska dejavnost posameznikov. Po ustavi je prepovedan vsakršen poseg v pravico do osebne varnosti, razen tistih, ki so izrecno dovoljeni.[11]

Po drugi strani pa je pravica do varnosti tudi pravica pozitivnega statusa, na kar je Ustavno sodišče RS opozorilo v odločbi iz leta 2013.[12] Državi in lokalnim skupnostim je naložena dolžnost, da si aktivno prizadeva zagotavljati najvišjo mogočo razumno dosegljivo stopnjo varnosti prebivalcev.

V okviru te dolžnosti morajo vsi organi, tudi na področju kibernetske varnosti, s svojimi pristojnostmi vsem prebivalcem zagotoviti učinkovito pravno varstvo pred posegi v njihovo osebno varnost na spletu.[13]

V prispevku najprej opredelimo pojma kibernetska in informacijska varnost v drugem poglavju. Nadaljujemo s predstavitvijo zakonodajnega okvira kibernetske varnosti v EU in RS v tretjem in četrtem poglavju. Sledi materialno-pravna ureditev prekrškov s področja kibernetske varnosti v slovenski zakonodaji v petem poglavju. V šestem poglavju namenjamo posebno pozornost enemu izmed pomembnejših vprašanj na področju prekrškovnega prava, to je odgovornosti za prekrške. Svoje ugotovitve smo strnili v zadnjem, sedmem poglavju.

[9] Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a.
[10] USRS odločba U-I-25/95 z dne 27. 11. 1997, ECLI:SI:USRS:1997:U.I.25.95.
[11] Prav tam.
[12] USRS odločba Up-1082/12 z dne 2. 4. 2013, ECLI:SI:USRS:1997:U.I.25.95.
[13] Prav tam.

2 Opredelitev pojmov kibernetska in informacijska varnost

Na področju, ki ga proučujemo v prispevku, se srečujemo z dvema pojmoma: kibernetske in informativne varnosti. Izraz kibernetska varnost se uporablja v strategiji za kibernetsko varnost EU in RS, medtem ko se izraz informacijska varnost pojavlja v naslovu temeljnega zakona s področja informacijske varnosti v RS.

S pomočjo jezikovne razlage lahko ugotovimo, da izraz »kibernetska« izvira iz besede kibernetika, ki pomeni: »vedo, ki raziskuje podobnost med delovanjem strojev in živo naravo«,[14] beseda »informacijska« se nanaša na informacijo, le-ta pa v splošnem smislu označuje »kar se o določeni stvari pove, sporoči«, medtem ko izraz varnost označuje »stanje varnega«.[15] Že iz te razlage lahko razberemo, da je pojem kibernetske varnosti bistveno širši od pojma informacijske varnosti, saj se prvi nanaša dejansko na vse, kar povezuje stroje (računalnike) z živo naravo (človekom), medtem ko se drugi »omejuje« na informacije (podatke).

»Kibernetska« predpona (kiber*)* se pogosto uporablja tudi kot sinonim za kibernetski prostor. Izraz kibernetski prostor se danes pojmuje kot zlitje vseh komunikacijskih omrežij, podatkovnih baz in virov informacij v ogromno, zapleteno in raznoliko odejo elektronske izmenjave. Tako se ustvari »omrežni ekosistem«, kraj, ki ni del fizičnega temveč virtualnega sveta. Naloga kibernetske varnosti je, da kibernetski prostor ohranja varen in ga ščiti pred kibernetskimi grožnjami.[16]
Kibernetska varnost je po splošni definiciji:

- skupek aktivnosti in drugih ukrepov, tehničnih in netehničnih, katerih namen je zaščititi računalnike, računalniška omrežja, strojno in programsko opremo ter informacije, ki jih le-ta vsebuje in obravnava, kar vključuje programsko opremo in podatke kot tudi druge elemente kibernetskega prostora pred vsemi grožnjami, vključno z grožnjami nacionalni varnosti;
- stopnja zaščite, ki jo aktivnosti in ukrepi lahko zagotovijo;

[14] Prim. z J. Dokl, Kibernetska varnost omrežij, 2012, str. 35 in 36.
[15] SSKJ, 2014.
[16] M. Dunn, Comparative Analysis of Cybersecurity Initiatives Worldwide, ITU, WSIS Thematic Meeting on Cybersecurity, 2005, str. 3.

– združena področja profesionalnih naporov, vključno z raziskavami in razvojem na področju implementiranja in izboljševanja ukrepov ter dvigovanja kakovosti le-teh.[17]

Informacijska varnost pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem. Informacijska varnost šteje kot zaupnost, neokrnjenost in razpoložljivost podatkov ne glede na njihovo obliko: elektronsko, tiskano ali katero drugo. Informacijska varnost se nanaša na vse vidike varovanja informacij. Zaupnost vključuje zaščito informacij pred razkritjem nepooblaščenim osebam, neokrnjenost ali integriteta pomeni zaščito informacij v tem smislu, da jih nepooblaščene osebe ne morejo spreminjati, medtem ko razpoložljivost omogoča, da so informacije na voljo pooblaščenim strankam, kadar jih le-te zahtevajo.[18]

Tudi iz primerjave obeh definicij je razvidno, da je kibernetska varnost širši pojem od informacijske varnosti ali varnosti podatkov, kljub temu pa je z obema tesno povezana, saj je varnost informacij v ospredju tudi pri kibernetski varnosti.

Ker iz definicije kibernetske varnosti jasno izhaja njen namen zaščititi računalnike, računalniška omrežja, strojno in programsko opremo, informacije, itd. pred kibernetskimi grožnjami, kar je med drugim tudi namen slovenskega ZinfV, lahko zaključimo, da ZInfV kljub svojemu imenu ne posega le na področje informacijske varnosti, temveč obravnava širšo problematiko kibernetske varnosti.

3 Zakonodajni okvir kibernetske varnosti v EU

3.1 Splošno

Konec leta 2020 sta Komisija EU in Visoki predstavnik EU za zunanje zadeve predstavila strategijo EU za kibernetsko varnost. Njen namen je zagotoviti globalni in odprt internet z močnimi zaščitnimi ukrepi, kjer obstajajo tveganja za varnost in temeljne pravice ljudi v Evropi. Uresničevanje strategije bo potekalo z uporabo treh glavnih instrumentov: regulativnimi, naložbenimi in političnimi pobudami.[19]

[17] Prav tam, str. 4.
[18] Dostopno na: https://www.gov.si/teme/informacijska-varnost (30. 10. 2023).
[19] Dostopno na: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies (30. 10. 2023).

Med pomembnejše regulativne ukrepe sodita dva zakonodajna predloga Komisije EU:

- Predlog Direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 (NIS 2 direktiva) in
- Predlog Direktive Evropskega parlamenta in Sveta o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114 (angl.: Critical Entities Resilience; CER direktiva).

Obe predlagani direktivi sta bili sprejeti konec leta 2022.[20] Skladno z njunimi zahtevami morajo članice sprejeti in objaviti ukrepe za uskladitev z NIS 2 in CER direktivo do 17. oktobra 2024. V RS bo to pomenilo predvsem spremembo ZInfV in Zakona o kritični infrastrukturi[21] (ZKI).

Medtem ko je NIS 2 direktiva namenjena »digitalni« varnosti, se CER direktiva ukvarja predvsem z vprašanji »fizične« varnosti (notranje grožnje, pandemije, velike prometne in industrijske nesreče, terorizem itd.).Vključuje tudi digitalna tveganja, posebno nevarnost pa predstavljajo hibridne grožnje, ki bodo za kritične subjekte poseben izziv.[22] Dejstvo, da uporaba novih tehnologij (5G, brezpilotna letala ipd.) prinaša dodatna tveganja, povečuje soodvisnost držav članic in zahteva njihovo usklajeno ravnanje, za kar je potreben enoten zakonodajni okvir. Komisija EU je pri pripravi predlogov direktiv sledila tej zahtevi ter ju vsebinsko uskladila. Tako direktivi pooblaščata pristojne organe za sprejem dopolnilnih ukrepov in izmenjavo informacij o kibernetski in nekibernetski odpornosti »kritičnih« oz. »bistvenih« subjektov. Poleg tega se z NIS 2 direktivo v celoti zagotavlja tudi fizična varnost omrežij in informacijskih sistemov subjektov v sektorju digitalne infrastrukture kot del obveznosti teh subjektov (obvladovanje tveganj in poročanje o kibernetske varnosti). Podobne zahteve veljajo tudi za subjekte iz sektorjev bančništva, infrastrukture finančnih trgov in digitalne infrastrukture. Zaradi tega je bilo treba

[20] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (UL L 338, 27. 12. 2022; NIS 2 direktiva) in Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114 (UL L 333, 27. 12. 2022; CER direktiva).

[21] Uradni list RS, št. 75/17 in 189/21 – ZDU-1M.

[22] C. Pursiainen, E. Kytömaa, From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean?, 2022, str. 97.

bistvene subjekte iz teh sektorjev opredeliti kot enakovredne kritičnim subjektom v CER direktivi, pri čemer jim slednja ne nalaga dodatnih obveznosti.

Pomemben pravni akt EU na področju kibernetske varnosti je Akt EU o kibernetski varnosti, natančneje Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013[23] (Akt EU o kibernetski varnosti). Ta akt zagotavlja ENISI, Agenciji Evropske unije za kibernetsko varnost, trajni mandat in krepi njeno vlogo. Vzpostavlja tudi okvir EU za certificiranje kibernetske varnosti, s čimer se krepi kibernetska varnost digitalnih izdelkov in storitev v Evropi. Kar zadeva vsebino in področje uporabe, je Akt EU o kibernetski varnosti uveden z namenom zagotavljanja pravilnega delovanja notranjega trga ob hkratnem doseganju visoke ravni kibernetske varnosti, kibernetske odpornosti in zaupanja v EU.[24]

Skupina italijanskih raziskovalcev je izvedla študijo različnih pravnih virov EU na področju kibernetske varnosti, na podlagi katere je opredelila tri glavne elemente regulativnega pristopa EU:

- ravnotežje med določbami, ki temeljijo na načelih in tehničnimi pravili,
- različne tehnološke rešitve, ki jih zakonodaja obravnava kot ključne za doseganje ciljev EU na področju varstva in varnosti podatkov, in
- združevanje celotnega pravnega okvira okoli petih temeljnih elementov (ocena tveganja, pristop ob zasnovi, obveznosti poročanja, odpornost in sheme certificiranja).[25]

3.2 Direktivi NIS in NIS 2

NIS 2 direktiva temelji na NIS direktivi in jo razveljavlja. Namen NIS direktive je bil v zagotovitvi visoke skupne ravni varnosti omrežij in informacij z izboljšanjem varnosti interneta ter zasebnih omrežij in informacijskih sistemov, ki podpirajo

[23] UL L 151, 7. 6. 2019.
[24] V. Papakonstantinou, Cybersecurity as Praxis and as a State: The EU Law Path Towards Acknowledgement of a New Right to Cybersecurity?, 2022, str. 9, ki pri tem citira prvi odstavek 1. člena Akta EU o kibernetski varnosti.
[25] A. Mantelaro, G. Vaciago, M. S. Esposito, N. Monte, The Common EU Approach to Personal Data and Cybersecurity Regulation, 2020, str. 328.

delovanje družbe in gospodarstva.[26] V skladu z zahtevami NIS direktive so bili v državah članicah ustanovljeni organi, pristojni za kibernetsko varnost ter centri za odzivanje na računalniške grožnje. Članice so sprejele nacionalne strategije in načrte sodelovanja na področju kibernetske varnosti. Državni organi in podjetja v nekaterih kritičnih sektorjih so morali izdelati ocene tveganj, s katerimi se soočajo, ter sprejeti ustrezne in sorazmerne ukrepe za zagotovitev kibernetske varnosti. Tem subjektom je bilo tudi naloženo, da pristojnim organom poročajo o vseh incidentih, ki resno ogrožajo njihova omrežja in informacijske sisteme ter znatno vplivajo na neprekinjenost kritičnih storitev in dobavo blaga.

Ker se s tehnološkim razvojem povečuje odvisnost delovanja notranjega trga od zanesljivega izvajanja kritične infrastrukture in ker je število kibernetskih napadov, še zlasti med koronavirusno krizo, močno naraslo, je bilo potrebno obstoječa pravila NIS direktive nadgraditi.

Izmed sprememb, ki jih prinaša NIS 2 direktiva, poleg splošnih sprememb (kot je npr. širjenje uporabe direktive na dodatne sektorje, razlikovanje med skupinami zavezancev, ki so dolžni spoštovati določbe direktive), skladno z vsebino poglavja, izpostavljamo spremembe v zvezi z usklajevanjem sistemov sankcioniranja v državah članicah.

NIS 2 direktiva širi področje uporabe NIS direktive na dodatne sektorje, ki so bili izbrani glede na njihov pomen za gospodarstvo in družbo. Priloga I tako določa poleg dosedanjih sedmih (elektrika, promet, bančništvo, infrastruktura finančnega trga, zdravstveni sektor, oskrba s pitno vodo in njena distribucija, digitalna infrastruktura) štiri nove sektorje: odpadna voda, upravljanje storitev IKT med podjetji, javna uprava in vesolje. V Prilogi II so na novo določeni sektorji: poštne in kurirske storitve, ravnanje z odpadki, izdelava, proizvodnja in distribucija kemikalij, pridelava, predelava in distribucija živil, proizvodnja (medicinskih pripomočkov in vitro diagnostičnih medicinskih pripomočkov, računalnikov in elektronskih ter optičnih izdelkov, električnih naprav, strojne opreme, motornih in drugih vozil ter prikolic in polprikolic plovil) in digitalni ponudniki (spletne tržnice, spletni iskalniki in platforme za storitve družbenega mreženja ter raziskave.[27]

[26] Komisija, 2013, str. 2.
[27] Priloga I (visoko kritični sektorji) in priloga II (drugi kritični sektorji) NIS 2 direktive.

Nadalje NIS 2 direktiva odpravlja razlikovanje med izvajalci bistvenih storitev in ponudniki digitalnih storitev. To razlikovanje ni odražalo dejanskega pomena sektorjev ali storitev za družbene in gospodarske dejavnosti na notranjem trgu. Po novem so subjekti razvrščeni v skupino bistvenih subjektov, če izvajajo dejavnost na področju sektorjev iz Priloge I ali v skupino pomembnih subjektov, če izvajajo storitve na področjih iz Priloge II (gl. prejšnji odstavek). Za obe skupini subjektov veljajo enake zahteve glede obvladovanja tveganj in obveznosti poročanja, različno pa je urejen sistem nadzora in sankcioniranja. Prilogi poleg sektorjev in podsektorjev določata tudi »bistvene« (Priloga I) in »pomembne« (Priloga II) subjekte. Tako npr. Priloga I za sektor odpadnih vod kot bistvene subjekte določa podjetja, ki zbirajo, odvajajo ali čistijo komunalno odpadno vodo, odpadno vodo iz gospodinjstev in tehnološko odpadno vodo iz točk 1 do 3 2. člena Direktive Sveta 91/271/EGS z dne 21. maja 1991 o čiščenju komunalne odpadne vode.[28]

NIS 2 direktiva uvaja enotno merilo za podjetja, ki spadajo na področje uporabe direktive. To bi naj bila v bodoče vsa srednja in velika podjetja, kot so opredeljena v Priporočilu Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, majhnih in srednje velikih podjetij,[29] ki delujejo v sektorjih, vključenih v področje uporabe direktive, ali opravljajo storitve, zajete s to direktivo. Mikro in mala podjetja so izključena iz uporabe direktive, razen izjem (podjetja, ki imajo ključno vlogo za gospodarstvo ali družbo držav članic ali za določene sektorje ali vrste storitev).[30]

Od držav članic NIS 2 direktiva zahteva, da bistvenim in pomembnim subjektom naložijo upravne globe za kršitve njenih določb. Hkrati določa nekatere najvišje globe za najhujše kršitve (najmanj 10 000 000 EUR ali 2 odstotka skupnega svetovnega letnega prometa podjetja, ki mu pripada bistveni subjekt, v preteklem proračunskem letu; upošteva se višji znesek).[31] Višina upravne globe iz NIS 2 direktive, kot tudi pogoji za njen izrek, so enaki globi za najhujše kršitve varstva osebnih podatkov, določene z GDPR.[32] Poleg denarnih kazni NIS 2 direktiva uvaja tudi druge sankcije, kot je začasni preklic certifikata ali dovoljenja za del storitev ali vse storitve, ki jih opravlja bistveni subjekt, in začasno prepoved opravljanja vodstvenih funkcij za fizično osebo, ki pa se lahko uporabijo le kot skrajni ukrep

[28] UL L 135, 30. 5. 1991.
[29] UL L 124, 20. 5. 2003.
[30] Podrobneje gl. drugi, tretji in četrti odstavek 2. člena NIS 2 direktive.
[31] Določbe četrtega odstavka 34. člena NIS 2 direktive.
[32] Prim. s četrtim odstavkom 83. člena GDPR.

(*ultima ratio)*, ko so bili uporabljeni vsi drugi »nadzorni« ukrepi, in le dokler subjekti ne sprejmejo potrebnih ukrepov za odpravo pomanjkljivosti ali izpolnitev zahtev pristojnega organa, zaradi katerih so bile takšne sankcije naložene.[33]

Kadar se upravne globe naložijo podjetjem, bi se podjetje v te namene moralo razumeti kot podjetje v skladu s 101 in 102. členom Pogodbe o delovanju EU[34] (PDEU). Kadar se upravne globe naložijo osebam, ki niso podjetje, bi moral nadzorni organ pri določanju ustreznega zneska globe upoštevati splošno raven dohodka v državi članici in ekonomski položaj osebe. Države članice bi morale določiti, ali bi se morale upravne globe uporabljati tudi za javne organe in v kakšnem obsegu. Naložitev upravne globe ne vpliva na uporabo drugih pooblastil pristojnih organov ali drugih sankcij, določenih v nacionalnih pravilih, s katerimi je prenesena NIS 2 direktiva, pri čemer bi bilo potrebno spoštovati načelo *ne bis in idem*.[35]

3.3 Predlog CER direktive

CER direktiva bo nadomestila predhodno Direktivo Sveta (ES) št. 114/2008 z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite.[36] Trenutno veljavna direktiva se uporablja le za energetski in prometni sektor. Osredotoča se zgolj na zaščitne ukrepe t. i. evropskih subjektov kritične infrastrukture ter določa postopek za njihovo opredeljevanje.

Splošni cilj CER direktive je zagotoviti neprekinjeno zagotavljanje bistvenih storitev na notranjem trgu s krepitvijo odpornosti kritičnih subjektov. Po določbah nove direktive se področje uporabe iz prvotnih dveh sektorjev širi na deset sektorjev (na energetiko, promet, bančništvo, infrastrukturo finančnega trga, zdravje, pitno vodo, odpadno vodo, digitalno infrastrukturo, javno upravo in vesolje), ki so skladni s sektorji iz NIS 2 direktive. Direktiva opredeljuje postopek, po katerem države članice opredelijo kritične subjekte z uporabo skupnih meril na podlagi nacionalne ocene tveganja. CER direktiva določa obveznosti za države članice in kritične subjekte, ki jih te opredelijo, vključno s tistimi, ki so posebnega evropskega pomena, tj. kritičnimi subjekti, ki zagotavljajo bistvene storitve več kot šestim ali več državam članicam ali

[33] Podrobneje 32. člen NIS 2 direktive.
[34] UL C 326, 26. 10. 2012.
[35] NIS 2 direktiva, tč. 130.
[36] UL L 345, 23. 12. 2008.

v šestih ali več državah članicah, ki so izpostavljeni posebnemu nadzoru Komisije EU.[37] Komisija EU v ta namen organizira svetovalno misijo za oceno ukrepov, ki jih je kritični subjekt sprejel za izpolnjevanje svojih obveznosti v skladu z direktivo, bodisi na zahtevo države članice, ki je ta kritični subjekt prijavila, bodisi na zahtevo ene ali več držav članic, v katerih kritični subjekt izvaja bistveno storitev ali na lastno zahtevo.[38]

4 Pravna ureditev kibernetske varnosti v RS

4.1 Institucionalna ureditev

Posebni državni organ na področju informacijske varnosti je Urad Vlade RS za informacijsko varnost (v URSIV),[39] ki deluje kot samostojna vladna služba. URSIV deluje kot osrednji koordinacijski organ na strateški ravni nacionalnega sistema zagotavljanja informacijske varnosti, obenem pa je tudi enotna kontaktna točka države pri mednarodnem sodelovanju na tem področju. Sestavni del omenjene službe je tudi skupina za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave (CSIRT organov državne uprave),[40] ki obravnava incidente informacijske varnosti v državni upravi in se nanje odziva.

URSIV je v Sloveniji glavni pristojni nacionalni organ za informacijsko varnost. Njegovo osnovno poslanstvo je dvig odpornosti na kibernetske grožnje, ki lahko ogrozijo posameznike, podjetja, državne organe in družbo v celoti. URSIV v ta namen povezuje deležnike v nacionalnem sistemu informacijske varnosti in na strateški ravni koordinira operativne zmogljivosti v sistemu. Posebno pozornost posveča zavezancem po ZInfV iz skupine izvajalcev bistvenih storitev na področjih energije, digitalne infrastrukture, oskrbe s pitno vodo in njene distribucije, zdravstva, prometa, bančništva, infrastrukture finančnega trga, preskrbe s hrano in varstva okolja, iz skupine ponudnikov digitalnih storitev in iz skupine organov državne uprave. Poleg tega URSIV izvaja naloge enotne kontaktne točke za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU in z evropsko

[37] Določbe 17. člena CER direktive.
[38] Podrobneje gl. 18. člen CER direktive.
[39] Dostopno na: https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/o-uradu/ (1. 10. 2023).
[40] Predlog Zakona o spremembah in dopolnitvah Zakona o informacijski varnosti (ZinfV-A), dostopen na: https://imss.dz-rs.si/IMiS/ImisAdmin.nsf/ImisnetAgent?OpenAgent&2&DZ-MSS-01/156842f84cdd96263e4dcb82fa49756484939dd99d0297546daec874200edd17 (3. 10. 2023), str. 4.

mrežo skupin CSIRT ter druge naloge mednarodnega sodelovanja. Z lastno inšpekcijsko službo izvaja nadzor nad izvajanjem ZInfV.

URSIV je z obveščanjem vlade in Sveta za nacionalno varnost (SNAV) o stanju povečane ogroženosti zaradi verjetnosti realizacije kritičnega incidenta ali kibernetskega napada umeščen v sistem nacionalne varnosti.

Na operativni ravni deluje SI-CERT kot nacionalni odzivni center za kibernetsko varnost pri javnem zavodu Akademska in raziskovalna mreža Slovenije (ARNES), ki je pristojen tudi za priglasitev varnostnih incidentov. Prijave le-teh morajo obvezno sporočati vsi, ki so po sklepu Vlade RS določeni kot izvajalci bistvenih storitev ali ponudniki digitalnih storitev ali operaterji elektronskih komunikacij po Zakonu o elektronskih komunikacijah[41] (ZEKom-2). Vsi ostali (pravne in fizične osebe, javne ustanove) varnostne incidente prijavljajo prostovoljno.

Pomembno vlogo imajo še Uprava RS za zaščito in reševanje s sistemom varstva za zaščito pred naravnimi in drugimi nesrečami (organ v sestavi Ministrstva za obrambo RS), Slovenska obveščevalna agencija na področju protiobveščevalnega delovanja (služba Vlade RS pod neposredno pristojnostjo predsednika Vlade), Policija (organ v sestavi Ministrstva za notranje zadeve) oz. njen Urad za informatiko in telekomunikacije, Uprava kriminalistične policije - predvsem Center za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala.[42]

4.2 Zakonodajni okvir

Temeljni pravni vir na področju kibernetske varnosti v RS je ZInfV. Poleg celovite ureditve področja informacijske varnosti in zagotovitve visoke stopnje varnosti omrežij in informacijskih sistemov v RS je namen zakona tudi v določitvi varnostnih zahtev in obveznosti priglasitve incidentov zavezancev. Zakon o državni upravi[43] (ZDU-1) določa, da naloge na področjih informacijske družbe, elektronskih komunikacij, informatizacije državne uprave, upravljanja informacijsko-komunikacijskih sistemov in zagotavljanja elektronskih storitev javne uprave,

[41] Obveznost priglasitve smiselno velja tudi za izvajalce posebnih obdelav osebnih podatkov, v skladu s 23. členom Zakona o varstvu osebnih podatkov (Zvop-2, Uradni list RS, št. 163/22 (dostopno na: https://www.cert.si/prijava-incidenta/ (1. 10. 2023)).
[42] Vlada RS, 2016, str. 1.
[43] Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 in 18/23.

zagotavljanja delovanja državnega portala eUprava, varnih predalov ter centralne storitve za spletno prijavo in elektronski podpis opravlja Ministrstvo za digitalno preobrazbo.[44]

Poleg ZInfV na področje kibernetske varnosti v RS posega tudi ZEKom-2. Sprejet je bil septembra 2022 in je nadomestil predhodnika ZEKom-1. Glavnina sprememb, ki jih je ZEKom-2 uvedel na področju informacijske varnosti, natančneje v VIII. poglavju (Varnost omrežij in storitev ter delovanje v stanjih ogroženosti), je posledica sprememb regulativnega okvira ter implementacije ukrepov, namenjenih varni uvedbi tehnologije 5G v EU. Za operaterje se krepijo zahteve in pogoji glede varnosti omrežij in storitev v luči varnostnih tveganj, ki jih prinaša tehnologija 5G, še posebej za operaterje mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja določenim subjektom, ki z vidika države in družbe zagotavljajo t. i. kritične storitve.[45]

4.3 Nadzor

Prekrškovni organ je tisti organ, ki po zakonu, ki določa prekrške, izvaja nadzorstvo nad izvajanjem posameznega predpisa.[46] ZInfV določa, da nadzor nad izvajanjem njegovih določb kot tudi določb predpisov, sprejetih na njegovi podlagi in nad izvajanjem upravnih odločb, ki jih izda pristojni nacionalni organ v okviru določil četrtega odstavka 21. člena in četrtega odstavka 22. člena, opravljajo inšpektorji za informacijsko varnost pristojnega nacionalnega organa.[47]

V skladu s citirano zakonsko določbo je pri Upravi RS za informacijsko varnost organizirana posebna enota Inšpekcija za informacijsko družbo. Inšpektorji so osebe s posebnimi pooblastili in odgovornostmi. Pri izvajanju nadzora so dolžni upoštevati določila Zakona o inšpekcijskem nadzoru[48] (ZIN) in določila področne zakonodaje. Pri izrekanju ukrepov na področju informacijske varnosti tako lahko izrekajo tudi ukrepe, predvidene v ZInfV. Delo inšpektorjev kot prekrškovnih organov se bo tako v praksi začelo pri izvajanju njihove nadzorstvene funkcije ob morebitni ugotovitvi kršitve, ki jo ZInfV opredeljuje kot prekršek. Če inšpektor za

[44] Določbe 28. a člena ZDU-1.
[45] Predlog Zakona o elektronskih komunikacijah (ZEKom-2), dostopen na: https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10097 (3. 10. 2023), str. 17.
[46] P. Čas, N. Orel, v: Zakon o prekrških (ZP-1) s komentarjem, 2018, str. 231.
[47] Določbe prvega odstavka 31. člena ZInfV.
[48] Uradni list RS, št. 43/07 – uradno prečiščeno besedilo in 40/14.

informacijsko varnost pri svojem delu ugotovi kršitev varstva osebnih podatkov ali sum te kršitve, o tem obvesti Informacijskega pooblaščenca za varstvo osebnih podatkov.[49]

Nadzor nad izvajanjem določb ZEKom-2 in na njegovi podlagi izdanih predpisov ter splošnih aktov izvaja Agencija za komunikacijska omrežja in storitve Republike Slovenije (Agencija), razen v primerih, ki spadajo v pristojnosti informacijskega pooblaščenca na podlagi 229. člena ZEKom-2 ali organa, pristojnega za informacijsko varnost, na podlagi 128. člena ZEKom-2.

Prekrškovni organi, ki odločajo o prekrških za kršitve ZEKom-2 in na njegovi podlagi izdanih predpisov, so prav tako Agencija, Informacijski pooblaščenec in Inšpekcija za informacijsko varnost. Odločajo v skladu z določbami Zakona o prekrških[50] (ZP-1), vsak na svojem področju nadzora. Prekrškovni postopki potekajo po hitrem postopku, pri čemer je kršitelj lahko sankcioniran z globo v znesku, višjem od najnižje predpisane mere za posamezni prekršek.

5 Prekrški na področju kibernetske varnosti

5.1 Splošno o prekrških

Na splošno je v Sloveniji po veljavnem zakonu prekršek tisto dejanje, ki pomeni kršitev zakona, uredbe vlade ali odloka samoupravne lokalne skupnosti, ki je določeno kot prekršek ter je zanj predpisna sankcija za prekršek.[51]

Pravo o prekrških, ki je del kaznovalnega pravnega sistema RS, daje tudi državi in občinam pooblastilo za predpisovane prekrškov. To sicer veljavno zakonsko pooblastilo v teoriji ni povsem nesporno. Tako je *Jakulin* že leta nazaj opozarjal, da je v zvezi s prekrški problematično dejstvo, da se lahko določajo tudi s podzakonskimi akti.[52] To še zlasti velja za prekrške, ki jih na podlagi pooblastila v 21. členu Zakona o lokalni samoupravi[53] (ZLS) določajo občine z odloki. Vendar

[49] Določbe tretjega odstavka 31. člena ZInfV.
[50] Uradni list RS, št. 29/11 – uradno prečiščeno besedilo, 21/13, 111/13, 74/14 – odl. US, 92/14 – odl. US, 32/16, 15/17 – odl. US, 73/19 – odl. US, 175/20 – ZIUOPDVE in 5/21 – odl. US).
[51] Določbe 6. člena ZP-1.
[52] V. Jakulin, Kazniva dejanja in prekrški zoper javni red in mir, 2002, str. 1457.
[53] Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 76/08, 79/09, 51/10, 40/12 – ZUJF, 14/15 – ZUUJFO, 11/18 – ZSPDSLS-1, 30/18, 61/20 – ZIUZEOP-A in 80/20 – ZIUOOPE.

na področju kibernetske varnosti ni materialnopravne ureditve prekrškov, ki bi jih urejale občine. Vsi prekrški so določeni z državnimi zakoni o informacijski varnosti in elektronskem poslovanju, ki jih obravnavamo v nadaljevanju.

Sicer splošno prekrški pomenijo obliko kršitve družbene discipline oz. družbene vrednote. Po *Tratarju* prekrškovno pravo s pregonom prekrškov nedvomno prispeva tudi k občutku varnosti v družbi in posredno tudi k varovanju ustavnih vrednot oz. človekovih pravic. [54] Država z institucijo prekrškov zagotavlja varnost v družbi kot družbeno in politično vrednoto. *Senčar* poudarja, da je naloga prekrškovnih organov pri obravnavanju prekrškov usmerjena v obravnavanje in po potrebi sankcioniranje oseb, ki ne spoštujejo predpisov in s svojim protipravnim ravnanjem delajo prekrške.[55] Temelj, da govorimo o prekrškovnih organih, je njihova nadzorstvena funkcija, ki je tem organom podeljena z materialnim predpisom, s katerim so urejena posamezna področja in so z njimi določeni prekrški.

V slovenskem pravnem redu je pravo o prekrških sestavljeno iz splošnega in posebnega dela. Določbe posebnega dela so razdrobljene in urejene z zakonskimi in podzakonskimi besedili, ki vsebujejo opise posameznih prekrškov. Kako je to na področju kibernetske varnosti, je prikazano v nadaljevanju.

Splošni del prava o prekrških je enotno zakonodajno urejen na podlagi ZP-1. Gre za sistemski zakon, ki opredeljuje splošne pogoje za predpisovanje prekrškov in sankcije zanje, splošne pogoje glede odgovornosti za storitev prekrškov, za izrekanje in izvrševanje sankcij, prekrškovne postopke ter organe in sodišča za odločanje o njih.[56] Kateri organi so pristojni na področju kibernetske varnosti, smo prikazali v delu poglavja o nadzoru.

[54] B. Tratar, Pomen pregona prekrškov za varnost v družbi, 2009, str. 375.
[55] A. Senčar, Kaznovalna praksa policije za prekrške, 2011, str. 110–125.
[56] L. Selinšek, Predpisovanje prekrškov v odlokih samoupravnih lokalnih skupnosti skladno z ZP-1, 2003, str. 103–119.

5.2 Prekrški, določeni z ZInfV

5.2.1 Kazenske določbe

Kot je bilo navedeno, je ZInfV materialni *lex specialis*, ki določa prekrške v XI. poglavju z naslovom Kazenske določbe v 36. do 39.b členu. ZInfV razlikuje med štirimi skupinami zavezancev,[57] za katere predpisuje tudi različne obveznosti. Posledično tudi ločeno določa prekrške za različne možne kršitelje obveznosti, in sicer: 37. člen določa prekrške za izvajalce bistvenih storitev, 38. člen določa prekrške za ponudnike digitalnih storitev, 39. člen za prekrške organov državne uprave, 39.a pa za prekrške povezanih subjektov. Določena sta tudi dva prekrška upravljavca centralnega informacijsko-komunikacijskega sistema (kadar le-ta ne omogoča vpogleda v delovanje informacijske infrastrukture centralnega informacijsko-komunikacijskega za CSIRT organov državne uprave oz. ne izvede odrejenih ukrepov CSIRT organov državne uprave v svojem informacijsko-komunikacijskem sistemu; kot storilec prekrška je določena odgovorna oseba upravljavca).[58]

5.2.2 Prekrški izvajalcev bistvenih storitev

Izvajalci bistvenih storitev so subjekti, ki izvajajo storitve na (za družbo in gospodarstvo) pomembnih področjih in so bistvene za ohranitev ključnih družbenih in gospodarskih dejavnosti.[59] Pomembna področja oz. sektorji so povzeti po NIS direktivi: energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo, infrastruktura finančnega trga, preskrba s hrano in varstvo okolja.[60]

Vlada RS je z Uredbo o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev[61] na področju energije in prometa določila še podpodročja ter pripravila seznam bistvenih storitev, ki se nahaja v prilogi uredbe.

Kot izvajalci bistvenih storitev štejejo torej subjekti, ki izvajajo (bistvene) storitve, določene z vladno uredbo.

[57] Določbe prvega odstavka 5. člena ZInfV.
[58] Določbe 39. b člena ZInfV.
[59] Določbe 1. točke 4. člena ZInfV.
[60] Določbe drugega odstavka 5. člena ZInfV.
[61] Uradni list RS, št. 39/19.

Kot kršitve, ki jih lahko zagrešijo izvajalci bistvenih storitev, ZInfV[62] določa:

- neizpolnitev obveznosti iz prvega ali petega odstavka 10. člena tega zakona (določitev kontaktne osebe za informacijsko varnost in njenega namestnika ter posredovanje njunih kontaktnih podatkov nacionalnemu pristojnemu organu; posredovanje sprememb o kontaktnih podatkih nacionalnemu pristojnemu organu),
- neizpolnitev obveznosti iz 11. člena tega zakona (neizpolnitev varnostnih zahtev kot npr. določitev ključnih, krmilnih in nadzornih informacijskih sistemov ter delov omrežja, s katerimi zagotavljajo izvajanje bistvenih storitev, vrednotenje tveganj in izvedba ukrepov za obvladovanje tveganj glede varnosti omrežij in informacijskih sistemov),[63]
- neizpolnitev obveznosti iz prvega, drugega ali petega odstavka 12. člena tega zakona (obveznost vzpostavitve in vzdrževanja varnostne dokumentacije; priprava in izvedba potrebnih varnostnih ukrepov (organizacijskih, logično-tehničnih in tehničnih ukrepov; zagotavljanje in ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja za obdobje šestih mesecev na ozemlju RS, razen za področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, glede katerih se lahko zagotavlja na ozemlju EU),
- neizpolnitev obveznosti iz prvega ali drugega odstavka 13. člena tega zakona (priglasitev incidentov SI-CERT-u, ki lahko pomembno vplivajo na neprekinjeno izvajanje bistvenih storitev, ki jih zagotavljajo, zavarovanje dnevniških zapisov oz. revizijskih sledi, če te obstajajo, ob prijavi incidenta),
- neizpolnitev obveznosti iz šestega odstavka 14. člena tega zakona (priglasitev SI-CERT-u znatnega vpliva na neprekinjeno izvajanje bistvenih storitev tistega izvajalca, ki je odvisen od tretjega ponudnika digitalnih storitev, nastalega kot posledica incidenta, ki vpliva na delovanje ponudnika digitalnih storitev),
- neizpolnitev obveznosti iz odločbe, izdane na podlagi četrtega odstavka 21. člena tega zakona (neizpolnitev ukrepov, ki jih zavezancu z odločbo naloži pristojni nacionalni organ za zaustavitev težjega ali kritičnega incidenta ali v primeru kibernetskega napada ali odpravo njegovih posledic),

[62] Določbe prvega odstavka 37. člena ZInfV.
[63] Podrobneje gl. 11. člen ZInfV.

– neizpolnitev obveznosti iz odločbe, izdane na podlagi četrtega odstavka 22. člena tega zakona (neizpolnitev ukrepov, ki jih izvajalcu bistvene storitve v stanju povečane ogroženosti z odločbo naloži pristojni nacionalni organ za preprečitev incidenta kot tudi za zmanjšanje pričakovanih škodljivih posledic ob morebitni realizaciji incidenta).[64]

Naštete prekrške lahko izvrši pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ter njihove odgovorne osebe. Kot sankcija je predvidena globa v višini od 200 do 2.000 eurov za odgovorno osebo (najnižja globa) ter od 10.000 do 50.000 eurov za pravno osebo, ki izpolnjuje merila Zakona o gospodarskih družbah[65] (ZGD-1) za srednjo ali veliko gospodarsko družbo.[66]

Bistveno storitev lahko izvaja tudi državni organ ali organ lokalne skupnosti (ali druga oseba javnega prava),[67] ki pa za prekršek ne odgovarja kot pravna oseba, temveč odgovarja za njegove prekrške le odgovorna oseba.[68]

5.2.3 Prekrški ponudnikov digitalnih storitev

Ponudnik digitalnih storitev je vsaka fizična ali pravna oseba, ki zagotavlja digitalno storitev. ZInfv kot digitalne storitve šteje informacijske storitve, in sicer: storitve spletne tržnice, spletnega iskalnika in računalništva v oblaku.[69] Ponudniki digitalnih storitev so druga skupina zavezancev, ki morajo spoštovati določila ZInfV. Izjema so ponudniki, ki imajo manj kot 50 zaposlenih in imajo letni promet oz. letno bilančno vsoto, ki ne presega deset milijonov eurov.[70]

[64] Prim. A. Primec, Materialnopravna ureditev prekrškov (administrativnih kršitev) na področju informacijske varnosti, 2020, str. 108–120.
[65] Uradni list RS, št. 65/09 – uradno prečiščeno besedilo, 33/11, 91/11, 32/12, 57/12, 44/13 –odl. US, 82/13, 55/15, 15/17, 22/19 – ZPosS, 158/20 – ZIntPK-C, 18/21, 18/23 – ZDU-1O in 75/23.
[66] Določbe 55. člena ZGD-1.
[67] Določbe tretjega odstavka 37. člena ZInfV.
[68] Določbe 13. a člena ZP-1.
[69] Določbe 4. člena ZInfv.
[70] Določbe drugega odstavka 8. člena ZInfV, prim. A. Primec, Odgovornost za prekrške s področja informacijske varnosti, 2021, str. 108–120.

ZInfV[71] določa le dva prekrška za ponudnike digitalnih storitev:

- neizpolnitev obveznosti iz prvega, drugega ali tretjega odstavka 14. člena tega zakona (določitev in sprejem ustreznih tehničnih in organizacijskih ukrepov za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri zagotavljanju teh storitev v EU; sprejem ustreznih ukrepov za preprečitev in zmanjšanje vpliva incidentov, ki ogrožajo varnost njihovih omrežij in informacijskih sistemov, na ponujane storitve, ki jih zagotavljajo v EU, da bi zagotovili neprekinjeno izvajanje teh storitev; priglasitev incidentov, ki imajo pomemben vpliv na zagotavljanje teh storitev, ki jih ponujajo v EU, SI-CERT-u; ta obveznost velja le za ponudnike, ki imajo dostop do informacij, na podlagi katerih lahko ovrednotijo stopnjo vpliva incidenta),
- neizpolnitev obveznosti iz odločbe, izdane na podlagi četrtega odstavka 21. člena tega zakona (neizpolnitev ukrepov, ki jih zavezancu z odločbo naloži pristojni nacionalni organ za zaustavitev težjega ali kritičnega incidenta ali v primeru kibernetskega napada ali za odpravo njegovih posledic).[72]

Storilec prekrškov je lahko pravna oseba, ki se sankcionira z globo v višini 200 do 10.000 eurov ter z globo od 10.000 do 50.000 eurov, če izpolnjuje merila ZGD-1 za srednjo ali veliko gospodarsko družbo; samostojni podjetnik posameznik, za katerega je predvidena globa od 500 do 10.000 eurov, ter odgovorna oseba pravne osebe ali samostojnega podjetnika, ki se sankcionira z globo od 200 do 2.000 eurov. Če primerjamo višino glob, določenih za posamezne kategorije storilcev (pravne osebe, samostojne podjetnike …), za prekrške izvajalcev bistvenih storitev in za prekrške ponudnikov digitalnih storitev, lahko ugotovimo, da so le-te po višini enake.

[71] Določbe prvega odstavka 38. člena ZInfV.
[72] Prim. A. Primec, Materialnopravna ureditev prekrškov (administrativnih kršitev) na področju informacijske varnost, 2020, str. 108–120.

5.2.4 Prekrški organov državne uprave

ZInfV[73] določa pet prekrškov organov državne uprave:

- neizpolnitev obveznosti iz 16. člena tega zakona (na podlagi ocene tveganj izdelati ukrepe, potrebne za obvladovanje tveganj glede varnosti za informacijske sisteme in dele omrežja, s katerimi upravljajo; sprejem potrebnih ukrepov za preprečitev in zmanjšanje vpliva incidentov, ki vplivajo na varnost omrežij in informacijskih sistemov državnih organov, da bi zagotovili neprekinjeno izvajanje storitev organov državne uprave; vzpostavitev potrebnih varnostnih zahtev za posamezne ključne dele nacionalno varnostnega sistema, v primeru, da iz tega sistema črpajo podatke),
- neizpolnitev obveznosti iz prvega, drugega ali petega odstavka 17. člena tega zakona (vzpostavitev in vzdrževanje dokumentiranega sistema upravljanja varovanja informacij in sistema upravljanja neprekinjenega poslovanja; priprava in izvedba potrebnih varnostnih ukrepov (organizacijskih, logično-tehničnih in tehničnih ukrepov); zagotavljanje in ohranjanje dnevniških zapisov o delovanju svojih informacijskih sistemov ali delov omrežja za obdobje šestih mesecev na ozemlju RS),
- neizpolnitev obveznosti iz prvega ali drugega odstavka 18. člena tega zakona (priglasitev incidentov s pomembnim vplivom na neprekinjeno izvajanje storitev organov državne uprave SIGOV-CERT-u oz. pristojnemu nacionalnemu organu, kadar incidente zaznajo organi državne uprave, ki imajo lastne zmogljivosti vsaj na ravni varnostno operativnega centra; ustrezno zavarovanje dnevniških zapisov oz. revizijskih sledi ob prijavi incidenta),
- neizpolnitev obveznosti iz odločbe, izdane na podlagi četrtega odstavka 21. člena tega zakona (neizpolnitev ukrepov, ki jih zavezancu z odločbo naloži pristojni nacionalni organ za zaustavitev težjega ali kritičnega incidenta ali v primeru kibernetskega napada ali odpravo njegovih posledic),
- neizpolnitev obveznosti iz odločbe, izdane na podlagi četrtega odstavka 22. člena tega zakona (neizpolnitev ukrepov, ki jih državnemu organu, ki upravlja z informacijskimi sistemi, v stanju povečane ogroženosti z odločbo naloži pristojni nacionalni organ za preprečitev incidenta kot tudi za

[73] Določbe prvega odstavka 39. člena ZInfV.

zmanjšanje pričakovanih škodljivih posledic ob morebitni realizaciji incidenta.[74]

Kot smo že opozorili, se lahko za prekrške organov državne uprave kaznuje le odgovorna oseba organa državne uprave z globo v višini od 200 do 2.000 eurov, torej je enaka kot v primeru kršitev odgovornih oseb izvajalcev bistvenih storitev in ponudnikov digitalnih storitev.

5.2.5 Prekrški povezanih subjektov

Subjekti, ki se povezujejo s centralnim informacijsko-komunikacijskim sistemom in hkrati še niso zavezanci po ZInfV (državni organi, organi lokalnih skupnosti, javne agencije in nosilci javnih pooblastil ter drugi subjekti, ki niso organi državne uprave), morajo za učinkovito zagotavljanje informacijske in kibernetske varnosti centralnega informacijsko-komunikacijskega sistema izpolnjevati določene obveznosti in minimalne tehnične ukrepe in zahteve, če želijo ostati povezani s tem sistemom, ter hkrati omogočiti učinkovit nadzor in sankcioniranje predvidene ureditve. Ti subjekti so z ZInfV opredeljeni kot povezani subjekti.

Posamezni prekršek izvrši povezana oseba, kadar:

- ne določi kontaktne osebe za informacijsko varnost in njenega namestnika ali ne posreduje njunih kontaktnih podatkov pristojnemu nacionalnemu organu,
- ne pripravi analize obvladovanja tveganj informacijske varnosti z oceno sprejemljive ravni tveganj,
- ne sprejme ali izvaja minimalnega obsega varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki upoštevajo posebne potrebe delovnega področja povezanega subjekta,
- ne pripravi navodil in postopkov za obvladovanje incidentov informacijske varnosti s protokolom obveščanja CSIRT organov državne uprave,

[74] Prim. A. Primec, Materialnopravna ureditev prekrškov (administrativnih kršitev) na področju informacijske varnosti, 2020, str. 108–120.

– ne izvede odrejenih ukrepov CSIRT organov državne uprave v svojem informacijsko-komunikacijskem sistemu.

Če prekršek izvrši pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, se sankcionira z globo od 500 do 10.000 eurov. Če prekršek izvrši odgovorna oseba naštetih oseb, globa znaša od 200 do 2.000 eurov.[75]

5.3 Prekrški, določeni z ZEKom-2

Kršitve s področja informacijske varnosti so v ZEKom-2 določene v prvem odstavku 233. člena.[76] Izvrši jih lahko pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ter odgovorna oseba naštetih oseb. Ker ZEKom-2 operaterjem nalaga precej več obveznosti v primerjavi z ZEKom-1, je večje tudi število možnih kršitev in posledično tudi prekrškov, zato njihovo podrobnejše predstavljanje znotraj prispevka ni smiselno. Primeroma navajamo le nekaj obveznosti operaterjev in možnih posledičnih kršitev: operater ne zagotavlja sistema upravljanja varnosti, kar vključuje sistem upravljanja neprekinjenega poslovanja in sistem upravljanja varovanja informacij; oba sistema morata biti opredeljena kot poslovna skrivnost; operater ju mora v praksi izvajati, posodabljati in nadgrajevati; o incidentih mora poročati tako agenciji kot SI-CERT-u; v primeru stanj ogroženosti mora prednostno zagotavljati delovanje delov omrežja, storitev in povezav, ki so nujni za nemoteno delovanje omrežij ključnih delov sistema varnosti države in komunikacij v sili ter za podporo delovanju kritične infrastrukture, izvajalcev bistvenih storitev ter organov državne uprave itd.[77] Sankcije, ki doletijo storilce teh prekrškov, so precej strožje v primerjavi s sankcijami, ki jih za kršitve svojih določb predvideva ZInfV. Pravne osebe, ki izpolnjujejo merila za srednjo ali veliko družbo po ZGD-1, se sankcionirajo z globo od 50.000 do 400.000 eurov; pravne osebe, ki ne dosegajo kriterijev ZGD-1 za srednje družbe (mikro in majhne družbe), samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, se sankcionirajo z globo od 1.000 do 20.000 eurov; odgovorna oseba pravne osebe, samostojnega podjetnika in posameznika, ki samostojno opravlja dejavnost, se sankcionira z globo od 500 do 10.000 eurov.[78]

[75] Določbe 39. a člena ZInfV.
[76] Natančneje od 22. do 39. točke prvega odstavka 233. člena ZEKom-2.
[77] Podrobneje gl. prav tam.
[78] Določbe prvega, drugega in tretjega odstavka 299. člena ZEKom-2.

6 Odgovornost za prekrške na področju kibernetske varnosti

6.1 Osebe, ki lahko izvršijo prekršek (kategorije storilcev)

V prejšnjem poglavju smo podrobneje opisali zakonske znake prekrškov, določene z ZInfV in ZEKom-2, navedli potencialne storilce ter predstavili sankcije, ki doletijo storilce teh prekrškov. V nadaljevanju pozornost usmerjamo k odgovornosti storilcev. Predpogoj, da se lahko storilcu izreče sankcija za izvršen prekršek, je namreč njegova odgovornost. Vprašanje odgovornosti storilca za prekršek urejajo splošna pravila prekrškovnega prava, zato pri obravnavi odgovornosti storilcev za prekršek izhajamo iz ZP-1.

Iz predstavitve kazenskih določb ZInfV in ZEKom-2 je mogoče razbrati, da se kot storilci prekrška s področja informacijske varnosti lahko obravnavajo pravne osebe, samostojni podjetniki posamezniki, posamezniki, ki samostojno opravljajo dejavnost, ter odgovorne osebe vseh naštetih subjektov.[79]

Kot smo že zapisali, lahko posamezne prekrške, določene z ZInfV, izvršijo tudi državni organi kot izvajalci bistvenih storitev ali kot upravljavci informacijskih sistemov in delov omrežja oz. kot izvajalci informacijskih storitev, nujnih za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti. Prav tako smo opozorili, da državni organi za prekrške ne odgovarjajo, temveč zanje odgovarjajo njihove odgovorne osebe (če zakon tako določi, kar sta ZInfV in ZEKom-2 tudi storila), le-te pa odgovarjajo po splošnih pravilih o odgovornosti odgovornih oseb (pravnih oseb, samostojnih podjetnikov itd.).

Odgovornost za prekršek zaradi boljše preglednosti obravnavamo po posameznih kategorijah storilcev. Kazenske določbe ZInfV in ZEKom-2 na prvo mesto med kršitelji postavljajo pravne osebe, zato tudi pričenjamo s predstavitvijo njihove odgovornosti za prekršek.

[79] Splošno o storilcih prekrškov gl. B. Tičar, A. Primec, Pravna ureditev prekrškov in administrativnih kršitev v gospodarstvu (de lege lata), 2020, str. 205.

6.2 Odgovornost pravnih oseb

Pravna oseba je umetna tvorba, ki z lastnimi dejanji prekrška ne more izvršiti, zato o dejanski odgovornosti pravne osebe ni mogoče govoriti. Njena odgovornost za prekršek se zato navezuje na odgovornost storilca prekrška, ki ga pri opravljanju njene dejavnosti le-ta stori v njenem imenu ali za njen račun ali v njeno korist ali z njenimi sredstvi.[80] V tem primeru govorimo o pridružitveni (akcesorni) odgovornosti pravne osebe, saj se odgovornost pravne osebe »pridružuje« individualni odgovornosti neposrednega storilca, ki je prekršek izvršil pri opravljanju dejavnosti pravne osebe, v njenem imenu ali za njen račun ali v njeno korist ali z njenimi sredstvi. To pomeni, da pravna oseba ne more biti storilka prekrška, temveč je odgovorna za prekršek, ki ga je storila druga (fizična oseba), v njenem interesu.

V praksi je mogoče, da je neposredni storilec odgovorna oseba (ki odgovarja na podlagi prvega odstavka 15. člena ZP-1). Vprašanje, ki se v takšnem primeru zastavlja, je, na podlagi katerih zakonskih določb se presoja odgovornost storilca prekrška: ali po določbah, ki določajo odgovornost neposrednega storilca, ali po določbah, ki se uporabljajo za odgovorno osebo? Po stališču Vrhovnega sodišča RS je potrebno neposrednega storilca prekrška, ki ima status odgovorne osebe po prvem odstavku 15. člena ZP-1, obravnavati po določbah, ki določajo odgovornost odgovorne osebe za prekršek samo v primeru, ko predpis, ki določa prekršek, ne določa tudi odgovornosti neposrednega storilca za storjeni prekršek. V primerih pa, ko predpis o prekršku določa tako odgovornost odgovorne osebe kot odgovornost neposrednega storilca prekrška, storilec prekrška, ki je hkrati neposredni storilec prekrška in odgovorna oseba po prvem odstavku 15. člena ZP-1, za prekršek odgovarja kot neposredni storilec prekrška.[81]

Če storilca ni mogoče odkriti ali ga ni mogoče spoznati za odgovornega (npr. zaradi neprištevnosti ali kadar ga predpis ne določa kot odgovornega za prekršek), je odgovornost pravne osebe utemeljena z opustitvijo dolžnega nadzorstva njenega vodstvenega ali nadzornega organa ali njene odgovorne osebe, ki bi lahko prekršek preprečila.[82] Nadzorstvo obsega kontrolne in sorodne mehanizme, vzpostavljene znotraj pravne osebe z namenom preprečevanja kršitev, ki imajo znake prekrškov. Za utemeljitev samostojne odgovornosti pravne osebe v tem drugem primeru

[80] Določbe prvega odstavka 14. člena ZP-1.
[81] VSRS sodba IV Ips 113/2013 z dne 21. 11. 2013, ECLI:SI:VSRS:2013:IV.IPS.113.2013.
[82] Določbe drugega odstavka 14. člena ZP-1.

zadošča ugotovitev, da ni imela vzpostavljenih ustreznih mehanizmov za preprečitev prekrška oz. niso delovali iz razlogov na strani pravne osebe oz. njenih vodstvenih ali nadzornih organov oz. odgovornih oseb. Opustitev dolžnega ravnanja kot predpostavka odgovornosti pravne osebe za prekršek se v tem primeru domneva in je prekrškovnemu organu ni treba dokazovati – nasprotno, pravna oseba mora dokazati, da ta predpostavka ni podana.[83] Vendar pa je treba dejanja opustitve dolžnega nadzorstva v vsakem posameznem primeru natančno ugotoviti in določno opredeliti že v izreku odločbe o prekršku. Pri dokazovanju opustitve dolžnega nadzorstva ni treba zadostiti standardom kot v primeru opustitve dolžnega nadzorstva kot temelja odgovornosti odgovorne osebe za prekršek, saj fizična oseba odgovarja za svoje ravnanje na podlagi zavesti in volje, ki jo je razvila do tega dejanja, pravna oseba pa odgovarja za ravnanje druge fizične osebe.[84] Zadostiti pa je treba zahtevi po jasni opredelitvi obveznosti, ki jih je bila za preprečitev prekrška dožna izvesti pravna oseba in katerih opustitev se po moči in učinku lahko primerja s storitvijo prekrška v izreku odločbe o prekršku.[85]

V zvezi s pojmom dolžnega nadzorstva je Ustavno sodišče RS ugotovilo: »da je opustitev dolžnega nadzorstva – tako v pomenu iz drugega odstavka 14. člena ZP-1 kot v pomenu iz druge alineje tretjega odstavka 14. člena ZP-1 – predpostavka odgovornosti pravne osebe za prekršek in da 14. člen ZP-1 sam zase konkretnih oblik dolžnega nadzorstva ne opredeljuje. Vendar pa je treba upoštevati, da vseh nadzorstvenih ukrepov, ki jih je v okviru dolžne skrbnosti za zakonitost poslovanja treba izvesti znotraj pravne osebe, s pravnimi akti preprosto ni mogoče predpisati.[86] Odgovornost pravnih oseb za prekrške je predvidena pri različnih prekrških, povezanih z izvajanjem raznovrstnih dejavnosti. Posledično se tudi dolžna ravnanja pravnih oseb, ki so potreba za preprečitev prekrškov, od prekrška do prekrška precej razlikujejo in jih ni mogoče vnaprej taksativno določiti. Po oceni Ustavnega sodišča RS zato ni v neskladju z Ustavo RS, če vsebino pravnega pojma dolžno nadzorstvo iz 14. člena ZP-1 napolnjujejo prekrškovni organi in sodišča pri odločanju v konkretnih primerih. Pomembno pa je, da so ukrepi dolžnega nadzorstva, ki se zahtevajo od pravnih oseb, primerni za preprečitev določenega prekrška (v pomenu, da lahko vplivajo na preprečitev prekrška) in da je podano ustrezno sorazmerje med

[83] VSRS sodba IV Ips 5/2020, z dne 28. 5. 2020, ECLI:SI:VSRS:2020:IV.IPS.5.2020.
[84] L. Selinšek, Razmerje med neposrednim storilcem prekrška in odgovorno osebo po ZP-1, 2014, str. 59–67.
[85] VSRS Sodba IV Ips 32/2019, z dne 19. 5. 2020, ECLI:SI:VSRS:2020:IV.IPS.32.2019.
[86] L. Selinšek, v: P. Čas, 2018, Zakon o prekrških (ZP-1) s komentarjem.

pomenom dobrine, ki jo ščiti posamezna norma, ki določa prekršek, in bremenom, ki ga za pravno osebo pomeni izvajanje zahtevanih ukrepov«.[87]

Pravna oseba se lahko razbremeni odgovornosti za prekršek, če dokaže, da je bil prekršek storjen z namenom škodovanja tej pravni osebi ali z zavestnim kršenjem pogodbe, na podlagi katere storilec opravlja delo ali storitev za pravno osebo, ali s kršenjem navodil ali pravil pravne osebe, ki je v okviru dolžnega nadzorstva pravočasno izvedla vse ukrepe, potrebne za preprečitev prekrška.[88]

6.3 Odgovornost samostojnega podjetnika posameznika in posameznika, ki samostojno opravlja dejavnost

Samostojni podjetnik posameznik in posameznik, ki samostojno opravlja dejavnost, sta fizični osebi, ki se v skladu z zakonskimi pogoji ukvarjata s pridobitno dejavnostjo. To ju postavlja v specifičen položaj tudi na področju prekrškovnega prava. Pogoje njune odgovornosti za prekršek ureja 14. a člen ZP-1, ki pri tem razlikuje med dvema položajema: ko je prekršek izvršil storilec pri opravljanju njune dejavnosti in ko sta prekršek izvršila sama.

Če je bil prekršek storjen pri opravljanju njune dejavnosti, odgovarjata za dejanje drugega kot odgovarjajo pravne osebe. ZP-1 v prvem odstavku 14. a člena tudi izrecno napotuje na uporabo pravil, ki veljajo za ugotavljanje odgovornosti pravne osebe (natančneje na uporabo 14. člena). Samostojni podjetnik kot tudi posameznik, ki samostojno opravlja dejavnost, bosta za prekršek prvenstveno odgovarjala na podlagi »pridružitvene« odgovornosti (ki se navezuje na odgovornost neposrednega storilca). Če pa storilca ne bo mogoče odkriti oz. ni odgovoren, pa na podlagi »samostojne« odgovornosti zaradi opustitve dolžnega nadzorstva (svojega nadzorstva ali nadzorstva odgovorne osebe, če sta jo imenovala).

Kljub sklicevanju na uporabo pravil 14. člena ZP-1 je treba opozoriti na pomembno razliko med postavkami odgovornosti podjetnika in posameznika, ki samostojno opravlja dejavnost, in odgovornostjo pravnih oseb. Oba subjekta praviloma nimata vodstvenega ali nadzornega organa, temveč ta položaj pripada njima kot nosilcema podjema. Če bi njuna odgovornost temeljila na pridružitveni odgovornosti

[87] USRS odločba Up-548/15 z dne 17. 10. 2019, ECLI:SI:USRS:2019:Up.548.15.
[88] Določbe tretjega odstavka 14. člena ZP-1.

neposrednega storilca, bi posledično fizična oseba odgovarjala za dejanje druge fizične osebe, kar bi privedlo do »objektivizirane« odgovornosti za prekršek, ki pa je v slovenskem pravnem redu nesprejemljiva. Zato je treba pri ugotavljanju odgovornosti samostojnega podjetnika in posameznika, ki samostojno opravlja dejavnost (ki imata hkrati položaj vodstvenega in nadzornega organa), ugotavljati tudi njun lasten prispevek k prekršku, ki se kaže v opustitvi dolžnega nadzorstva, s katerim bi prekršek lahko preprečila (subjektivizirana odgovornost). To pomeni, da je potrebno za ugotovitev njune odgovornosti za prekršek, ki ga je izvršila druga oseba pri opravljanju njune dejavnosti,[89] kumulativno upoštevati pogoje iz prvega in drugega odstavka 14. člena ZP-1.[90]

Samostojni podjetnik kot tudi posameznik, ki samostojno opravlja dejavnost, sta fizični osebi, ki velikokrat samostojno izvajata dejavnost in ne zaposlujeta drugih delavcev, zato tudi sama odgovarjata za prekrške. Če prekršek pri opravljanju svoje dejavnosti izvršita sama, se njuna odgovornost po napotilu drugega odstavka 14. a člena ZP-1 presoja po pravilih, ki veljajo za ugotavljanje odgovornosti fizičnih oseb.[91] Splošna pravila ZP-1 o odgovornosti fizičnih oseb se uporabljajo le za ugotavljanje njune odgovornosti, medtem ko se pri izreku sankcije uporabljajo pravila, ki jih za posamezni prekršek določa posebna zakonodaja izrecno zanju (za samostojnega podjetnika in posameznika, ki samostojno opravlja dejavnost) in ne pravila, ki določajo sankcijo za storilca (fizično osebo).

Poleg samostojnega podjetnika in podjetnika, ki samostojno opravlja dejavnost, odgovarja za prekršek tudi njuna odgovorna oseba. Kljub temu, da imata oba subjekta praviloma položaj vodstvenega in nadzornega organa, ju pravo o prekrških ne šteje za odgovorni osebi, temveč se njuna odgovornost presoja na podlagi določil 14. a člena ZP-1. Kot odgovorna oseba obeh subjektov bo torej za prekršek odgovarjala oseba, ki sta jo zaposlila za opravljanje njune dejavnosti in je torej pooblaščena opravljati delo v njunem imenu, za njun račun, v njuno korist ali z njunimi sredstvi.

[89] Določbe prvega odstavka 14. a člena ZP-1.
[90] VSRS sodba IV Ips 5/2017 z dne 18. 4. 2017, ECLI:SI:VSRS:2017:IV.IPS.5.2017.
[91] Določbe 9. člena ZP-1.

6.4 Odgovornost odgovorne osebe

Odgovorna oseba je odgovorna za prekršek, ki ga stori s svojim dejanjem (storitvijo ali opustitvijo) pri opravljanju dejavnosti pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, pri izvrševanju pooblastil državnega organa ali organa samoupravne lokalne skupnosti.[92] Odgovornost odgovorne osebe se presoja kot odgovornost fizične osebe (ugotavlja se njena krivdna odgovornost). Poleg načina izvršitve prekrška (da je prekršek izvršen pri opravljanju dejavnosti pravne osebe) je za ugotavljanje odgovornosti odgovorne osebe pomembna tudi njena pravna opredelitev. Odgovorna oseba je prvenstveno tista oseba, ki je pooblaščena opravljati delo v imenu, na račun, v korist ali s sredstvi pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, državnega organa ali organa samoupravne lokalne skupnosti.[93] Podlaga za opravljanje dela je lahko kakršen koli pravni akt: pogodba o delu, pogodba o zaposlitvi ipd. V praksi to pomeni, da bo odgovorna oseba velikokrat neposredni storilec prekrška in ne oseba, ki v pravni osebi zaseda poseben položaj, npr. zakoniti zastopnik.[94]

Odgovorna oseba pa je tudi tista oseba, ki je pri pravni osebi, samostojnem podjetniku posamezniku ali posamezniku, ki samostojno opravlja dejavnost, državnem organu ali organu samoupravne lokalne skupnosti pooblaščena izvajati dolžno nadzorstvo, s katerim se lahko prepreči prekršek.[95] Kot poudarja stroka, je namen te opredelitve zlasti v določitvi kroga oseb, katerih opustitev dolžnega nadzorstva ima za posledico (samostojno) odgovornost pravne osebe v primeru, ko storilec prekrška ni znan ali ni odgovoren, ne pa identifikaciji storilcev prekrška.[96]

Po zakonski domnevi je za izvajanje dolžnega nadzorstva pooblaščen vodstveni organ, za dolžno nadzorstvo nad vodstvenim organom pa nadzorni organ, razen če je bilo izvajanje dolžnega nadzorstva s pravnim aktom preneseno na drugo osebo ali organ. Če ima vodstveni ali nadzorni organ več članov, odgovarja vsak član zase, razen če je bilo dolžno nadzorstvo s pravnim aktom naloženo le posameznim članom ali ožji skupini članov.[97]

---

[92] Določbe prvega odstavka 15. a člena ZP-1.
[93] Določbe prvega odstavka 15. člena ZP-1
[94] L. Selinšek, Razmerje med neposrednim storilcem prekrška in odgovorno osebo po ZP-1, 2014, str. 61–62.
[95] Določbe drugega odstavka 15. člena ZP-1
[96] L. Selinšek, v: P. Čas, 2018, Zakon o prekrških (ZP-1) s komentarjem, str. 122.
[97] Določbe tretjega in četrtega odstavka 15. člena ZP-1.

Če je odgovorni osebi prenehala zaposlitev ali je subjekt, pri katerem je opravljala delo, prenehal obstajati, s tem njena odgovornost za prekršek ni prenehala. Izvzem odgovornosti za prekršek je mogoč le v primeru, če je ravnala po odredbi nadrejene odgovorne osebe ali vodstvenega ali nadzornega organa pravne osebe, državnega organa ali samoupravne lokalne skupnosti ali po odredbi samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, in je storila vse, kar je bila po zakonu, drugem predpisu ali po notranjem aktu tega subjekta dolžna storiti, da bi preprečila prekršek.[98]

7 Zaključek

Zaradi vedno naprednejših tehnoloških orodij postaja varnost informacijsko-komunikacijskih sistemov in podatkov vedno zahtevnejša naloga. Pomembno vlogo pri zagotavljanju kibernetske varnosti ima tudi regulativni okvir, ki smo ga predstavili v prispevku. Posebej smo se osredotočili na vprašanja, povezana s prekrški s področja kibernetske varnosti, še zlasti na vprašanje odgovornosti storilca za prekršek. To je eno izmed težjih pravnih vprašanj, ki se pojavljajo v prekrškovnem pravu. V prispevku smo tudi na splošno orisali prekrškovno pravo in prikazali, kako deluje na področju sodobne informacijske varnosti, ki se zaradi razvoja tehnologije in posledično vedno strožjih varnostnih zahtev zelo hitro spreminja. ZInfV je bil sprejet leta 2018 in je bil že večkrat spremenjen, nazadnje v letošnjem letu z novelo ZInfV-B.[99] Še več sprememb je bil deležen ZEKom-2, ki je na novo določil kar nekaj prekrškov oz. razširil in nadgradil obstoječe iz ZEKom-1. Naslednja večja sprememba prekrškovnega prava na področju informacijske varnosti se obeta prihodnje leto, ko se izteče rok za implementacijo NIS-2 direktive. Tudi z visokimi globami, primerljivimi z globami, ki jih določa GDPR za kršitve varstva osebnih podatkov, zakonodajalec za najhujše kršitve obveznosti s področja informacijske varnosti izkazuje skrb in pomen tega pomembnega področja.

Sicer na obravnavanem področju splošne pogoje odgovornosti za prekršek ureja ZP-1 (*lex generalis*). Prekrške s področja informacijske varnosti in možne storilce posameznih prekrškov urejajo posebni predpisi, zlasti zakoni (*lex specialis*). V RS sta to ZInfV in ZEKom-2 (*lex specialis*). Poleg opisov prepovedanih ravnanj (materialnih znakov prekrška) določata tudi storilce prekrškov ter sankcije.

[98] Določbe tretjega odstavka 15.a člena ZP-1.
[99] Uradni list RS, št. 49/2003.

ZInfV razlikuje med štirimi skupinami zavezancev, za katere predpisuje tudi različne obveznosti. Posledično tudi ločeno določa prekrške za različne možne kršitelje obveznosti, in sicer: 37. člen določa prekrške za izvajalce bistvenih storitev, 38. člen določa prekrške za ponudnike digitalnih storitev, 39. člen prekrške organov državne uprave, medtem ko 39. a člen določa prekrške povezanih oseb. ZEKom-2 določa prekrške, ki jih lahko izvršijo operaterji[100] in izvajalci govornih komunikacijskih storitev.[101]

Kar je skupno vsem prekrškom, določenih z ZInfV in ZEKom-2, je, da se kot storilec prekrška ne pojavlja posameznik (fizična oseba) ter da se prekrški praviloma izvršijo z opustitvenim ravnanjem (zavezanec ne izvrši zakonskih zahtev – zapovedi). Sicer so kot storilci posameznih prekrškov določene pravne osebe, samostojni podjetniki posamezniki, posamezniki, ki samostojno opravljajo dejavnost, ter njihove odgovorne osebe. ZInfV (dodatno) določa tudi odgovornost odgovorne osebe v državnem organu, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, če ima ta subjekt javnega prava status izvajalca bistvenih storitev, za prekršek, ki ga lahko izvrši ta skupina zavezancev (izvajalci bistvenih storitev). Poleg tega ZInfV določa odgovornost odgovorne osebe državnih organov tudi za prekrške, ki jih izvršijo organi državne uprave.

ZInfV in ZEKom-2 za vsak subjekt (za vsakega storilca) določata različno sankcijo. Odgovornost vseh naštetih subjektov (storilcev prekrškov, določenih z določbami ZInfV in ZEKom-2) pa se ugotavlja po splošnih pravilih ZP-1.

Literatura

Dokl, Jure, Kibernetska varnost omrežij, magistrsko delo, Univerza v Ljubljani, Fakulteta za družbene vede, Ljubljana 2012.

Dunn Myriam, Comparative Analysis of Cybersecurity Initiatives Worldwide. ITU, WSIS Thematic Meeting on Cybersecurity, Ženeva 2005, dostopno na: https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf (1. 9. 2021).

Čas Petra, Orel Nuša, v: Zakon o prekrških (ZP-1) s komentarjem, P. Čas et al. (ur.), GV Založba, Ljubljana 2018.

Flander Benjamin, Tičar Bojan, The Right to Security - An Outline of the Legal Regulation at the State and Local Levels in Slovenia, Revija za kriminalistiko in kriminologijo, Let. 70 (2019), št. 5, str. 422–438.

ISJFR ZRC SAZU, 2014, Slovar slovenskega knjižnega jezika, druga, dopolnjena in deloma prenovljena izdaja, spletna izdaja (SSKJ), dostopna na:

[100] Določbe 22. do 37. točke prvega odstavka 299. člena ZEKom-2.
[101] Določbe 38. in 39. točke prvega odstavka 299. člena ZEKom-2.

https://fran.si/iskanje?View=1&Query=kibernetika&All=kibernetika&FilteredDictionaryIds=133 (1. 9. 2021).

Jakulin Vid, Kazniva dejanja in prekrški zoper javni red in mir, Podjetje in delo, Let. 28 (2002), št. 6-7, str. 1457.

Komisija, 2013, Predlog Direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji. Dostopen na: https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52013PC0048&from=sl (20. 8. 2021).

Komisija a, 2020, Sporočilo Komisije o strategiji EU za varnostno unijo. Dostopno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605 (31. 8. 2021).

Komisija b, 2020, Predlog Direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi direktive (EU) 2016/1148. Dostopen na: https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52020PC0823&from=EN (31. 8. 2021).

Mantelero Alessandro, Vaciago Giuseppe, Esposito Maria Samantha, Monte Nicole, The Common EU Approach to Personal Data and Cybersecurity Regulation, International Journal of Law and Information Technology, Let. 28 (2020), št. 4, str. 297–328.

Ministrstvo za javno upravo, 2021, Predlog Zakona o elektronskih komunikacijah (ZEKom-2), dostopen na: https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10097 (3. 10. 2023).

Papakonstantinou Vagelis, Cybersecurity as Praxis and as a State: The EU Law Path Towards Acknowledgement of a New Right to Cybersecurity?, Computer Law & Security Review, Let. 44 (2022), str. 1–15.

Primec Andreja, Materialnopravna ureditev prekrškov (administrativnih kršitev) na področju informacijske varnosti, v: 1. konferenca prava informacijske varnosti : zbornik 2020, Lexpera, GV založba, Ljubljana 2020.

Primec Andreja, Odgovornost za prekrške s področja informacijske varnosti, v: 2. konferenca prava informacijske varnosti : zbornik 2021, Lexpera, GV založba, Ljubljana 2021.

Pursiainen Christer, Kytömaa Eero, From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does it Mean?, Sustainable and Resilient Infrastructure, Let. 8 (2022), št. 1, str. 85-101.

Selinšek Liljana, Predpisovanje prekrškov v odlokih samoupravnih lokalnih skupnosti skladno z ZP-1, Lex localis, Let. 1 (2003), št. 3, str. 103–119.

Selinšek Liljana, Razmerje med neposrednim storilcem prekrška in odgovorno osebo po ZP-1, v: Zbornik 9. dnevi prekrškovnega prava, GV Založba, Ljubljana 2014.

Selinšek Liljana, v: Zakon o prekrških (ZP-1) s komentarjem, P. Čas et al. (ur.), GV Založba, Ljubljana 2018.

Senčar Alojz, Kaznovalna praksa policije za prekrške, v: Zbornik 6. dnevi prekrškovnega prava, GV Založba, Ljubljana 2011.

Tičar Bojan, Primec Andreja, Pravna ureditev prekrškov in administrativnih kršitev v gospodarstvu (de lege lata), v: 26. Gospodarski subjekti na trgu in evropske dimenzije, V. Rijavec (ur.), Univerzitetna založba Univerze v Mariboru, Maribor 2018.

Tratar Boštjan, Pomen pregona prekrškov za varnost v družbi, v: Varstvoslovje med teorijo in prakso: Zbornik prispevkov, T. Pavšič Mrevlje (ur.), Fakulteta za varnostne vede UM, Ljubljana 2009.

URSIV, 2021 – Urad Republike Slovenije za informacijsko varnost; dostopno na: https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/o-uradu-vlade-za-informacijsko-varnost/ (12. 9. 2021)

Vlada RS, 2016, Predlog zakona o informacijski varnosti. Dostopen na: https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=8587 (obiskano 2. 9. 2021).

Vlada RS, 2021, Predlog sprememb in dopolnitev Zakona o informacijski varnosti (ZInfV-A), dostopen na: https://imss.dz-rs.si/IMiS/ImisAdmin.nsf/ImisnetAgent?OpenAgent&2&DZ-

MSS-01/156842f84cdd96263e4dcb82fa49756484939dd99d0297546daec874200edd17 (3. 10. 2023).

SUMMARY

Cybersecurity has exceeded its original boundaries and expanded to all areas of social life. In addition to all the benefits of digitalisation, it also creates risks of malicious use of electronic information potential. In Slovenia, the right to cyber security has a constitutional legal basis, and information security is regulated in EU regulations and directives as a narrower part of cyber security. Cyber security plays a crucial role in regulating the safe flow of information, the integrity of the entire information system and preventing misuse in the use of digital information. The legal regulation of cyber and information security means ensuring an appropriate normative framework that legally enables the smooth flow of electronic information without unauthorised access by third parties and protects users from misuse or destruction of the same. Cyber security includes the confidentiality, integrity, and accessibility of information, whether in digital, print or some other form.

In addition, the contribution presents an analysis of the legal regulation of prescription and sanctioning of offences in the cyber or information security field in light of contemporary Slovenian information legislation. This is one of the more complex legal issues in tort law. In the article, we also generally outlined misdemeanour law and showed how it works in modern information security, which is changing very quickly due to the development of technology and, as a result, increasingly strict security requirements. The fundamental legal act in Slovenia in information security, the Information Security Act (ZInfV), was adopted in 2018 and has been amended several times, most recently with the amendment ZInfV-B. The Electronic Communications Act (ZEKom-2) underwent even more changes, which newly defined quite a few offences or expanded and upgraded the existing ones from the previous act (ZEKom-1). The following significant shift in misdemeanour law in the field of information security is expected next year when the deadline for the implementation of the NIS-2 directive expires. Even with high fines, comparable to the fines set by the GDPR for violations of personal data protection, the legislator for the most severe violations of obligations in the field of information security shows concern and the importance of this crucial area.

Otherwise, in the area under consideration, the general conditions of responsibility for a misdemeanour are governed by the Misdemeanours Act – ZP-1 (*lex generalis*) 2. Misdemeanours in information security and possible perpetrators of individual misdemeanours are handled by special regulations, especially laws (*lex specialis*). In Slovenia, these are ZInfV and ZEKom-2. In addition to descriptions of prohibited conduct (material signs of a misdemeanour), they also specify the perpetrators of the misdemeanours and the sanctions.

The ZInfV distinguishes between four groups of taxpayers, for which it prescribes different obligations. As a result, it also separately determines offences for various potential violators of obligations, namely: Article 37 determines violations for providers of essential services, Article 38 determines offences for providers of digital services, Article 39 for offences by state administration bodies, while Article 39a determines crimes related to persons. ZEKom-2 defines offences that operators and providers of voice communication services can commit.

What is common to all misdemeanours defined by ZInfV and ZEKom-2 is that an individual (natural person) does not appear as the perpetrator of the misdemeanour. That misdemeanours are generally committed by omission (the obligee does not comply with legal requirements - orders). Otherwise, the perpetrators of individual offences are certain legal entities, self-employed individuals, and their responsible persons. The ZInfV (additionally) also determines the liability of a responsible person in a state body, a self-governing local community, or another public law entity, namely, if this public law entity has the status of a provider of essential services, for an offence that can be committed by this group of liable parties (providers of essential services). In addition, the ZInfV stipulates the

responsibility of the responsible person of state authorities for misdemeanours committed by state administration authorities.

ZInfV and ZEKom-2 determine a different sanction for each entity (for each "perpetrator"). The responsibility of all the listed subjects (perpetrators of offences determined by the provisions of ZInfV and ZEKom-2) is established according to the general rules of ZP-1 (*lex generalis*).