Usporedba engleskog i američkog pravnog uređenja kibernetičke sigurnosti

Rebernak, Julija

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Law / Sveučilište u Zagrebu, Pravni fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:199:420792

PRAVNI FAKULTET SVEUČILIŠTA U ZAGREBU
KATEDRA ZA PRAVA INFORMACIJSKIH TEHNOLOGIJA I INFORMATIKU

Julija Rebernak

DIPLOMSKI RAD

USPOREDBA EUROPSKOG I AMERIČKOG PRAVNOG UREĐENJA KIBERNETIČKE SIGURNOSTI

Mentor:
izv. prof. dr. sc. Hrvoje Lisičar

Zagreb 2024.

IZJAVA O IZVORNOSTI

Ja, Julija Rebernak, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio/-la drugim izvorima do onih navedenih u radu.

Julija Rebernak, v.r.

SADRŽAJ

SAŽETAK

Cilj ovog rada je usporediti pravne okvire Europske Unije i Sjedinjenih Američkih Država u području kibernetičke sigurnosti. Započinje objašnjavanjem pojma kibernetičke sigurnosti kroz različite definicije i gledanja na to što sve ulazi u ovo područje. Zatim iznosi pregled europskog uređenja pojedinačnih akata kroz detaljnu analizu područja primjene, obveza i prava koje proizlaze iz odredaba, predviđenih kazni za nepoštivanje te tijela koje nadziru provedbu akata. Obrađuju se akti značajniji za kibernetičku sigurnost poput GDPR-a, AI akta, DORA-e i ostalih, te funkcije europske agencije ENISA-e. Poslije prelazi na isti takav pregled i analizu pravnih akata u SAD-u. Kod SAD-a posebno se obrađuju savezni zakoni poput COPPA-e, sektorski zakoni kao GLBA i zakoni specifični za određenu državu kao što je CCPA. Također obrađuje ulogu i funkcije regulatornih agencija. Na kraju se uspoređuju ta dva pravna sustava temeljem izložene analize te isticanjem sličnosti i različitosti akata koji uređuju ista područja u oba sustava. Uspoređuju se i ovlasti regulatornih agencija i mogućnost agencije da nadzire propise i izriče kazne. Zaključno se izvodi konkluzija o bitnim elementima kod uspredbe pravnih okvira.

SUMMARY

The aim of this thesis is to compare the legal frameworks of the European Union and the United States of America in the field of cyber security. It begins by defining cyber security through different definitions and looking at all that goes into this field. It then provides an overview of the European regulation of individual acts through a detailed analysis of the areas of application, obligations and rights arising from the provisions, the prescribed penalties for non-compliance and the bodies that supervise the implementation of the act. Acts more significant for cyber security such as the GDPR, AI Act, DORA and others and the functions of the European agency ENISA. Afterwards, it moves on to the same review and analysis of legal acts in the USA. In the USA, federal laws such as COPPA, sectoral laws such as GLBA, and state-specific laws such as CCPA are specifically addressed. It also addresses the role and functions of regulatory agencies. At the end, the two legal systems are compared based on the presented analysis and highlighting the similarities and differences of acts that regulate the same areas in both systems, and the powers of regulatory agencies and the agency's ability to monitor regulations and impose penalties are compared. In conclusion, judgement is made about the essential elements in the development of legal frameworks.

1. UVOD

S obzirom na sve veću pojavu kibernetičkih prijetnji, povreda podataka i malicioznih programa te mrežnih napada, kibernetička sigurnost postala je značajna tema za skoro sva poduzeća koja pohranjuju različite vrste podataka i koriste mrežne sustave te njihove korisnike i kupce čiji su podaci česta meta kibernetičkih napada. Ukoliko pogledamo globalni prosječni trošak koji poduzeće snosi nakon povrede podataka uvidjet ćemo zašto je kibernetička sigurnost posebice bitna iz gospodarskog aspekta. Prema IBM-ovom izvješću iz 2024. godine, taj trošak iznosi 4.88 milijuna američkih dolara.[1] To je povećanje od čak deset posto u odnosu na prošlu godinu te je najveći prosječni iznos dosad. Trend povećanja tog iznosa zasad nastavlja rasti te ne možemo predvidjeti hoće li se ubrzo krenuti smanjivati. Potrebno je pravno regulirati prostor kibernetičke sigurnosti, kao što to uvijek slijedi nakon nove pojave u društvu. Razlika u odnosu na ostale društevene trendove tijekom povijesti i njihovoj regulaciji je u brzini razvoja materije koju je potrebno regulirati. Tehnologija se razvija iznimno brzo na slobodnom tržištu te ju pravo mora nastojati pratiti. Zakonodavna tijela država donijela su različite zakone i propise o kibernetičkoj sigurnosti kako bi zaštitila osjetljive podatke fizičkih i pravnih osoba, osigurala nacionalnu sigurnost i smanjila prijetnje kibernertičkoj sigurnosti. Problem koji se ovdje javlja je postojanje značajnih razlika u pristupu regulacije kibernetičke sigurnosti, posebice između Sjedinjenih Američkih Država i Europske unije. Ova razlika u regulatornim pristupima može rezultirati poteškoćama za multinacionalna poduzeća koja posluju na područjima obaju jurisdikcija te postavlja pitanje o učinkovitosti ta dva pristupa. Cilj ovog rada prvenstveno je što preglednije sustavno prikazati pravno uređenje kibernetičke sigurnosti u Europskoj Uniji te u Sjedinjenim Američkim Državama. Nakon dobivenog cjelokupnog pregleda obaju pravnih okvira uspoređujemo sličnosti i razlike te zaključno donosimo mišljenje o njihovoj učinkovitosti. Obrađivat će se bitni propisi poput Opće Uredbe o zaštiti podataka, NIS Direktive, CISA i NIST okvira, te ćemo obraditi načine i sustave njihova provođenja i nadziranja primjene. Pritom ćemo primijenjivati pristup komparativne pravne analize. Kada govorimo o regulaciji kibernetičkih prijetnji na svjetskoj razini, potrebno je uzeti u obzir cjelokupno pravno uređenje svih država u kojima se te prijetnje pojavljuju, ali za potrebe ovog rada stavljen je primarni fokus na transatlantskom odnosu između navedenih dvaju regija. Pitanja poput kibernetičke špijunaže, kibernetičkog ratovanja i drugih potencijalnih zlouporaba

[1] IBM, *Cost of a Data Breach Report*, 30. srpnja 2024., dostupno na: https://www.ibm.com/reports/data-breach (15. rujna 2024.).

u kibernetičkom prostoru nisu obuhvaćena ovim radom kako bi se suzio predmet istraživanja i detaljnije obradilo navedeno.

2. DEFINIRANJE KIBERNETIČKE SIGURNOSTI

Pravo kibernetičke sigurnosti nije još precizno definirano kao što su to recimo, autorska prava. Kada se govori o pravu kibernetičke sigurnosti, najčešće se misli na pravila sigurnosti podataka koja primjenjuju poduzeća radi sprječavanja povreda, pravila o privatnosti te pravila za sprječavanje hakerskih napada. Američko Ministarstvo nacionalne inicijative domovinske sigurnosti za karijere i studije u području kibernetičke sigurnosti definira kibernetičku sigurnost kao: "strategija, politika i standardi u vezi sa sigurnošću i operacijama u kibernetičkom prostoru, koji obuhvaćaju cijeli raspon aktivnosti smanjenja prijetnji, smanjenja ranjivosti, odvraćanja, međunarodnog angažmana, odgovora na incidente, otpornosti i oporavka, uključujući operacije računalnih mreža, osiguranje informacija, provođenje zakona, diplomaciju, vojne i obavještajne misije, u kontekstu sigurnosti i stabilnosti globalne informacijske i komunikacijske infrastrukture.".[2] Pojednostavljeno, Agencija za kibernetičku sigurnost i sigurnost infrastrukture nudi definiciju koja glasi ovako: "kibernetička sigurnost je vještina zaštite mreža, uređaja i podataka od neovlaštenog pristupa ili kriminalne upotrebe, kao i praksa osiguravanja povjerljivosti, integriteta i dostupnosti informacija."[3] Prema Međuresornom odboru za sigurnost, kibernetičku sigurnost možemo podijeliti u 8 kategorija: sigurnost i upravljanje rizicima, sigurnost imovine, sigurnosna arhitektura i inženjerstvo, sigurnost komunikacije i mreže, upravljanje identitetom i pristupom, procjena sigurnosti i sigurnosno testiranje, sigurnosne operacije, sigurnost razvoja softvera.[4] Kada govorimo o definiranju kibernetičke sigurnosti u Republici Hrvatskoj, Zakon o kibernetičkoj sigurnosti NN 14/24 upućuje nas na vrlo široku i šturu definiciju iz Uredbe 2019/881 Europskog parlamenta i Vijeća: "kibersigurnost znači sve aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava."[5] Na stranicama Središnjeg državnog ureda za razvoj digitalnog

[2] NICCS, *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases*, 18. travnja 2024., dostuono na: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c (16. rujna 2024.).
[3] CISA, *What is cybersecurity?*, 1. veljače 2021., dostupno na: https://www.cisa.gov/news-events/news/what-cybersecurity (16. rujna 2024.).
[4] ISC2, *CISSP Certification Exam Outline Summary* , 15. travnja 2024., dostupno na: https://www.isc2.org/Certifications/cissp/Certification-Exam-Outline (17. rujna 2024.).
[5] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), SL L 151, 7.6.2019.

društva Republike Hrvatske, kibernetička sigurnost definira se kao "skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada tome značajno pridonosi."[6] Kako bismo bolje razumjeli pojam kibernetičke sigurnosti, potrebno je proučiti tzv. CIA trokut za koji stručnjaci često govore da je u njemu sadržan cilj kibernetičke sigurnosti kao takve. Nije poznato tko je prvi kreirao ovaj pojam, ali se mnogi zakonodavni akti u SAD-u njime koriste. C u trokutu predstavlja engl. *confidentiality*, tj. povjerljivost koja osigurava da informacije budu dostupne samo ovlaštenim korisnicima te sprječava neovlašteni pristupa. I označava engl. *integrity*, tj. integritet mora garantirati da će podaci ostati ispravni i cjelokupni bez promjena ili oštećenja tijekom njihove pohrane ili prijenosa. Te A za engl. *availability*, tj. da podaci trebaju biti dostupni korisnicima kada su im potrebni, bez kašnjenja ili ometanja u pristupu tim podacima.

[6] Središnji državni ured za razvoj digitalnog društva, *Kibernetička sigurnost*, https://rdd.gov.hr/kiberneticka-sigurnost/1436 (19. rujna 2024.).

3. PREGLED ZAKONA O KIBERNETIČKOJ SIGURNOSTI U EUROPSKOJ UNIJI

Europska Unija na porast prijetnji u kibernetičkom prostoru odgovara donošenjem Strategije za kibersigurnost u prosincu 2020. godine. Nju zajednički donose Europska komisija i Europska služba za vanjsko djelovanje. Strategija za kibersigurnost te Strategija jedinstvenog digitalnog tržišta Europske Unije skupa čine širi pravni okvir za uređenje kibernetičke sigurnosti na području Unije. U njoj se postavljaju načela uređenja kibersigurnosti i pet strateških prioriteta te odgovarajuće akcije. Također, ona određuje uloge i odgovornost dijeli zajednički među nadležnim tijelima prema NIS direktivama, tijelima za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava (dalje u tekstu: CERT) te tijelima za provedbu zakona.[7] Strategija Unije za kibernetičku sigurnost donijela je mnogo novih pravila koja će morati slijediti i subjekti koji u prošlosti možda uopće nisu pridavali poseban značaj kibernetičkoj sigurnosti. Također, kao što ćemo vidjeti kod određenih akata, propisane su novčane kazne koje mogu biti vrlo visokog iznosa. Ova strategija objedinjuje sve akte Europske Unije o kibernetičkoj sigurnosti koje ćemo obrađivati u ovome poglavlju. Republika Hrvatska donijela je svoju Nacionalnu strategiju kibernetičke sigurnosti sukladnu onoj Europske Unije te određene provedbene propise za primjenu europskih akata.

3.1. Opća uredba o zaštiti podataka (dalje u tekstu: GDPR)

GDPR nastoji fizičkim osobama pružiti mogućnost kontrole nad svojim osobnim podacima te ujednačiti akte o zaštiti podataka na području Europske Unije. Uredba je obvezujuća za sve države članice te se izravno primjenjuje u njima od 2018. godine. Materijalno se primjenjuje na automatiziranu obradu osobnih podataka ili na neautomatiziranu obradu tih podataka ukoliko oni čine dio sustava pohrane ili su namijenjeni biti dijelom sustava pohrane. Kako bismo određene podatke smatrali osobnima oni se moraju odnositi na pojedinca utvrđenog identiteta ili čiji je identitet moguće utvrditi izravno ili neizravno, posebice pomoću identifikatora kao što su to ime, lokacija, osobni identifikacijski broj, mrežni identifikator ili jedan ili više određenih čimbenika specifičnih za tu osobu. Voditeljem obrade smatra se fizička osoba, pravna osoba te tijelo javne vlasti ili drugo tijelo ukoliko utvrđuje svrhu i način obrade

[7] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Document 52013JC0001, 7. veljače 2013., dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001 (19. rujna 2024.).

osobnih podataka. Ova se Uredba teritorijalno primjenjuje na voditelja ili izvršitelja obrade ako imaju poslovni nastan u Europskoj Uniji, neovisno o tome gdje se odvija obrada podataka. Primjenjuje se i na poduzeće bez poslovnog nastana u Uniji ako je procesuiranje podataka "povezano s nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje; ili praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar Unije."[8] Europski službenici razjasnili su da se ne radi o nuđenju dobara i usluga samo zato što je web stranica poduzeća dostupna u nekoj državi članici Unije, već se gledaju neki drugi čimbenici poput valute ili korištenja jezika strane države ili spominjanja kupaca te države. Europski odbor za zaštitu podataka objasnio je da se na poduzeće primjenjuju pravila GDPR-a ukoliko to poduzeće cilja na kupce određene države time što im nudi dobra ili usluge. Također su ustanovili kako postoji mogućnost da se uredba primjenjuje na neko poduzeće ako ono promatra i prati ponašanje ispitanika neke države, ali uz to da se razmotri svrha tog promatranja ponašanja ispitanika. Od 5. do 11. članka razlažu se načela procesuiranja osobnih podataka: zakonitost brade, smanjenja količine podataka, ograničenje svrhe, točnost podataka, ograničenje pohrane, cjelovitosti i povjerljivosti podataka te odgovornosti voditelja obrade podataka. Također se zahtjeva od poduzeća, da već u samom dizajnu prilikom kreiranja nove aplikacije ili sustava, sastavni dio budu privatnost i sigurnost podatka (engl. *privacy by design*). Privatnost prema zadanim postavkama (eng. privacy *by default*) pretpostavlja da su postavke privatnosti automatski podešene na najvišu moguću razinu zaštite bez da ih korisnik mora ručno prilagođavati. Uredba iscrpno definira prava ispitanika, način na koji se ona ostvaruju te mogućnost njihova ograničenja. Ispitanici imaju pravo na pristup podacima, brisanje i ispravak podataka, ograničenje obrade, prenosivost podataka, pravo na prigovor i pojedinačno automatizirano donošenje odluka. Pravila o obvezama voditelja obrade i izvršitelja obrade postavljaju visoke standarde za obrađivanje osobnih podataka. Od poduzeća se zahtjeva korištenje naprednijih metoda kibernetičke sigurnosti poput enkripcije, redovitih sigurnosnih provjera i kontrolu pristupa podacima. GDPR je uveo obvezu prijavljivanja kibernetičkih napada ili povrede podataka nadležnim tijelima najčešće u roku 72 sata od otkrivanja incidenta. Ona ne nalaže određeni skup mjera kibernetičke sigurnosti, već zahtjeva od subjekata na koje se primjenjuje da poduzmu odgovarajuće mjere zaštite.[9] U slučaju nepostupanja prema Uredbi propisane su novčane kazne u maksimalnom iznosu od 10 milijuna eura te minimalnom od 2%

[8] UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, SL L 119/1, 4. svibnja 2016.

[9] National Cyber Security Centre, *General Data Protection Regulation (GDPR)*, 18. svibnja 2018., dostupno na: https://www.ncsc.gov.uk/information/gdpr (20. rujna 2024.).

što sigurno rezultira motiviranošću subjekata da poduzmu sve potrebne mjere. Može se zaključiti da ova Uredba kao jedini sveobuhvatni akt o zaštiti svih vrsta osobnih podastaka ima najznačajniji utjecaj unutar cjelokupnog uređenja kibernetičke sigurnosti.

3.2. Direktiva (EU) 2016/1148 Europskog Parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih informacijskih sustava širom Unije (dalje u tekstu: NIS1 direktiva)

"Cilj Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća bio je izgradnja kibersigurnosnih kapaciteta širom Unije, ublažavanje prijetnji mrežnim i informacijskim sustavima koji se upotrebljavaju za pružanje osnovnih usluga u ključnim sektorima i osiguravanje kontinuiteta takvih usluga u slučaju incidenata, čime se doprinosi sigurnosti Unije i učinkovitom funkcioniranju njezina gospodarstva i društva."[10] NIS1 direktiva donesena je 2016. godine te ju van snage uskoro stavlja direktiva NIS2. Direktiva NIS1 državama članicama nametnula je obvezu donošenja nacionalne strategije za sigurnost mrežnih i informacijskih sustava, osnivanje jednog ili više nacionalnog nadležnog tijela i nacionalne jedinstvene kontaktne točke za sigurnost mrežnih i informacijskih sustava te timove za odgovor na računalne sigurnosne incidente (dalje u tekstu: CSIRT). Ova se direktiva primjenjivala na dvije kategorije subjekata: operatore ključnih usluga te pružatelje digitalnih usluga. Operatori ključnih usluga pružaju usluge u tzv. kritičnim sektorima koji su od značajne važnosti za funkcioniranje države i njezinu ekonomiju i gospodarstvo. To su: sektor energetike, prijevoza, bankarstva, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba vodom za piće i njezina distribucija te digitalna infrastruktura. Pružatelji digitalnih usluga su oni čije su vrste digitalnih usluga: internetsko tržište, internetska tražilica te usluge računalstva u oblaku.[11] Subjekti koji potpadaju pod ove kategorije obvezni su poduzeti tehničke i organizacijske mjere za upravljanje rizicima, odgovarajuće mjere osiguranja svojih mrežnih i informacijskih sustava kako bi spriječili incidente i sveli njihove učinke na što manju razinu te osigurali kontinuirano korištenje tih usluga. Ti subjekti također su dužni obavijestiti nadležno tijelo ili CSIRT o incidentima značajnog učinka koji onemogućavaju pružanje usluga. Nakon provedbe NIS1 direktive 2018. godine, Europska komisija ocijenila je i revidirala direktivu zbog poteškoća s

[10] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2), SL L 333/80, 27. prosinca 2022.
[11] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, SL L 194/1, 19. srpnja 2016.

provedbom kod nekoliko država članica. Procjena Komisije analizirala je direktivu s obzirom na njezin značaj, dodanu vrijednost za Eurospku Uniju, koherentnost, djelotvornost i učinkovitost. Glavni nalaz govori da je područje primjene ove direktive previše ograničeno u smislu sektora koji potpadaju pod njega, uglavnom zbog pojačane digitalizacije posljednjih godina i višeg stupanja međusobne povezanosti, zbog toga što opseg direktive više nije odražavao sve digitalizirane sektore koji pružaju ključne usluge te zbog nejednake otpornosti diljem Europske Unije koja proizlazi iz nedostatka zajedničkog razumijevanja primarnih prijetnji.[12]

3.3. Direktiva (Eu) 2022/2555 Europskog Parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (dalje u tekstu: Direktiva NIS2)

Direktiva NIS2 donesena je krajem 2022. godine te zamjenjuje Direktivu NIS1. Europska Unija zahtjeva od država članica da se implementiraju smjernice nove direktive od 18. listopada 2024. godine. Predmet ove direktive je "utvrditi mjere čiji je cilj postići visoku zajedničku razinu kibersigurnosti unutar Unije kako bi se poboljšalo funkcioniranje unutarnjeg tržišta."[13] Dakle, nastoji se dodatno povećati razina kibernetičke sigurnosti na području Europske Unije. Direktiva se fokusira na izgradnju sposobnosti zaštite kibernetičke sigurnosti, ublažavanje prijetnji mrežnim i informacijskim sustavima kojima se koriste pružatelji kritičnih infrastruktura. Pokušava osigurati kontinuitet pružanja takvih usluga kad su pružatelji suočeni sa određenim incidentima, pojačati otpornost tržišta na kibernetičke prijetnje. Njome se određuju obveze država članica o donošenju nacionalnih strategija za kibersigurnost i o uspostavljanju i imenovanju nadležnih tijela, tijela za upravljanje kiberkrizama, jedinstvene kontaktne točke za kibersigurnost i timove za odgovor na računalne sigurnosne incidente.[14] Razlika u odnosu na prethodnu NIS Direktivu je u području primjene koje je sada značajno prošireno. Veličina entiteta i područje pružanja usluga entiteta su odlučujući faktori kod primjene Direktive NIS2. Čak i bez obzira na njihovu veličinu, ova direktiva primjenjuje se na

[12] Koelemij S., *Securing Process Automation Systems in the European Union: An Overview of the NIS1 Directive and NIS2 Directive*, Industrial Cyber, 25. travnja 2024., dostupno na: https://industrialcyber.co/expert/securing-process-automation-systems-in-the-european-union-an-overview-of-the-nis1-directive-and-nis2-directive/ (25. rujna 2024.).
[13] *op.cit.* u bilj. 10., Direktiva NIS2.
[14] *op.cit.* u bilj. 10. i 13., Direktiva NIS2.

“pružatelje javnih elektroničkih komunikacijskih mreža ili javno dostupne elektorničke komunikacijske usluge, pružatelje usluga povjerenja, pružatelji usluga sustava naziva domena, ako je subjekt u nekoj državi članici jedini pružatelj usluge koja je ključna za održavanje ključnih društvenih ili gospodarskih djelatnosti, ako bi poremećaj u funkcioniranju usluge koju pruža subjekt mogao imati znatan učinak na javnu sigurnost, javnu zaštitu ili javno zdravlje, ako bi poremećaj u funkcioniranju usluge koju pruža subjekt mogao uzrokovati znatne sistemske rizike, posebno u sektorima u kojima bi takav poremećaj mogao imati prekogranični učinak, ako je subjekt ključan zbog svoje posebne važnosti na nacionalnoj ili regionalnoj razini za određeni sektor ili vrstu usluge ili za druge međuovisne sektore u državi članici te ako se radi o subjektu javne uprave.”[15] Također, bez obzira na veličinu primjenjuje se na subjekte utvrđene kao kritične u samoj direktivi. Ostali entiteti koji pružaju usluge unutar pojedinih sektora ulaze u polje primjene ukoliko se smatraju barem srednjim poduzećima ili koji prelaze gornje granice za srednja poduzeća i pružaju svoje usluge ili obavljaju svoje djelatnosti unutar Unije. Srednja poduzeća su ona koja imaju do 250 zaposlenih, promet do 50 milijuna EUR ili ukupnu bilancu do 43 milijuna EUR.[16] Prethodna direktiva uglavnom se fokusirala na sektore energetike, transporta, zdravstva i digitalne infrastrukture te vidimo koliko nova direktiva proširuje to područje primjene na druge subjekte. S novom direktivom pomiče se fokus sa određene esencijalne usluge unutar nekog subjekta koji potpada pod navedene sektore. To znači da obavezno propisano upravljanje rizicima nije ograničeno na mrežne i informacijske sustave koje subjekt koristi za poslovanje kritičnim infrastrukturama već se odnosi na cijeli subjekt koji nudi usluge u relevantnom sektoru koji potpada pod područje primjene direktive. Subjekt mora osigurati da svi njegovi mrežni i informacijski sustavi budu pokriveni mjerama upravljanja kibersigurnosnim rizicima prema smjernicama. Zahtjevi za usklađenosti sa smjernicama će se *ex lege* primjenjivati na subjekte koji zadovoljavaju navedene kriterije u direktivi bez dodatnog akta kojim se određuje primjenjivost od strane državne vlasti. Subjektima je propisana dužnost obavještavanja nadležnog tijela o značajnom incidentu koji se dogodio prema pravilima o prijavljivanju takvih incidenata koja se sastoje od više razina. Još jedna od bitnih razlika koja se pojavljuje u ovoj direktivi je u vrsti odgovornosti koja je predviđena. Prema NIS2 direktivi članovi upravljačkih tijela kritičnih subjekata mogu odgovarati subjektu osobno za povrede vezane uz uvjete za upravljanje rizicima.[17]

[15] *op.cit.* u bilj. 10., 13. i 14., Direktiva NIS2.
[16] Ured za publikacije Europske unije, *Mala i srednja poduzeća*, 22. veljače 2022., dostupno na: https://eur-lex.europa.eu/HR/legal-content/glossary/small-and-medium-sized-enterprises.html (26. rujna 2024.).
[17] Wolf Theiss Rechtsanwälte, *Digital Law: EU's comprehensive cybersecurity framework*, 4. srpnja 2024., dostupno na: https://www.youtube.com/watch?v=-eiGfa4BcAA (26. rujna 2024.).

3.4. Zakon o kibernetičkoj otpornosti (Cyber Resilience Act, dalje u tekstu: CRA)

Vijeće Europske Unije je usvojilo Zakon o kibernetičkoj otpornosti u listopadu 2024. godine sa ciljem postavljanja visokih standarda sigurnosti digitalnih proizvoda i softvera koji se nalaze na tržištu Unije. Prijedlog ovog akta bio je izložen već 2022. godine u sklopu Strategije Europske Unije za kibersigurnost. CRA se primjenjuje na proizvode s digitalnim elementima. To se odnosi na uređaje u fizičkom obliku koji su povezani s internetom te prikupljaju i razmjenjuju podatke s drugim uređajima putem mreže (engl. *internet of things*), poput povezanih televizora, usisavača ili frižidera. Značajan element u definiranju ovih proizvoda je u tome da je proizvod povezan s drugime ili na neku mrežu radi razmjene informacija. Povezanost može biti izravna ili neizravna, fizička ili bežična te virtualna. To također uključuje procesuiranje podataka na daljinu, primjerice pametne kućne uređaje koji se kontroliraju korištenjem mobilne aplikacije. Ova se uredba primjenjuje na navedene proizvode s digitalnim elementima koji su ponuđeni na tržištu Europske Unije, bez obzira gdje je proizvod razvijen ili proizveden te bez obzira gdje se nalazi korisnik proizvoda.[18] Uredba dijeli proizvode s digitalnim elementima na četiri kategorije: prozivodi s niskim, normalnim, visokim te kritičnim rizikom. Prema svakoj kategoriji propisani su određeni standardi koje proizvođači moraju zadovoljiti te svaka država članica imenuje tijelo koje provodi prijavljivanje za postupke ocjenjivanja sukladnosti. Navedeni proizvodi moraju ispunjavati osnovne sigurnosne zahtjeve, uključujući zaštitu od kibernetičkih prijetnji i ranjivosti te proizvođači moraju provesti procjene sigurnosti prije puštanja proizvoda na tržište. Kad se govori o obvezi informiranja misli se na nedvosmisleno informiranje korisnika od strane proizvođača o sigurnosnim značajkama proizvoda, potencijalnim sigurnosnim rizicima i uputama o održavanju. Proizvođači su dužni provoditi sigurnosna ažuriranja tijekom cijelog životnog vijeka proizvoda kako bi se ispravile eventualne ranjivosti u proizvodima. Unutar 24 sata od saznanja za ranjivost, proizvođači ju moraju prijaviti ENISA-i. Ukoliko proizvodi koji nisu u sukladnosti sa zahtjevima dovedu do kibernetičkog napada, proizvođač može biti odgovoran. Novčane kazne koje se izdaju poduzećima koja ne ispune propisane zahtjeve slične su onima kod GDPR-a te mogu doseći i do 15 milijuna eura ili 2,5% globalnog godišnjeg prometa, ovisi o tome koji je iznos veći.[19]

[18] Canonical Ubuntu, *What is the Cyber Resilience Act?*, 3. rujna 2024., dostupno na: https://www.youtube.com/watch?v=ltBtIDvav6c (28. rujna 2024.).
[19] Prijedlog uredbe europskog parlamenta i vijeća o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020, COM/2022/454 final, 15. rujna 2022.

3.5. Agencija Europske Unije za kibernetičku sigurnost (dalje u tekstu: ENISA)

Agencija je osnovana 2004. Godine. Njezino djelovanje uređeno je donošenjem Uredbe br. 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe br. 526/2013. ENISA je tijelo Unije sa pravnom osobnošću koje zastupa izvršni direktor. Ona se sastoji od upravljačkog odbora, izvršnog odbora, izvršnog direktora, savjetodavne skupine, ad hoc radnih skupina te mreže nacionalnih časnika za vezu. Bitno je napomenuti postojanje interesne skupine za kibersigurnosnu certifikaciju koja pruža savjete i pomoć Komisiji o strateškim pitanjima u vezi s europskim okvirom za kibersigurnosnu certifikaciju. Djelovanje ENISA-e utvrđeno je u skladu s jedinstvenim programskim dokumentom u kojem su njezini godišnji ili višegodišnji programi sa svim planiranim aktivnostima.[20] Ona utvrđuje europski okvir za kibersigurnosnu certifikaciju, poznat pod nazivom ENISA okvir. On djeluje pod nadzorom upravnog odbora, Europske komisije i drugih relevantnih sudionika. Strateške odluke donosi izvršni odbor, a izvršni direktor osigurava da se učinkovito provode ciljevi okvira. Okvir za certificiranje omogućit će uspostavu certifikacijskih programa na razini EU-a, koji će obuhvaćati skup pravila, tehničkih zahtjeva, standarda i postupaka. Temeljit će se na zajedničkom dogovoru unutar Europske Unije o procjeni sigurnosnih značajki određenih ICT proizvoda ili usluga. Certifikacija će potvrditi da ICT proizvodi i usluge, koji su certificirani prema takvom programu, ispunjavaju propisane zahtjeve. Svaki europski certifikacijski sustav treba navesti kategorije obuhvaćenih proizvoda i usluga, kibersigurnosne zahtjeve kao norme ili tehničke specifikacije, vrstu evaluacije kao samoprocjenu ili procjenu treće strane i razinu jamstva koja može biti osnovna, značajna ili visoka. Razine jamstva pomažu korisnicima razumjeti kibernetički rizik proizvoda u smislu vjerojatnosti i učinka nesreće. Certifikat će biti priznat u svim državama članicama EU-a, što olakšava prekograničnu trgovinu i informira kupce o sigurnosnim osobinama proizvoda ili usluge.[21] ENISA ujedno organizira edukativne konferencije, podiže svijest kroz osiguravanje resursa za jačanje vještina te provodi vježbe kibernetičke sigurnosti kako bi testirala spremnost i otpornost institucija na moguće kibernetičke napade. Ona analizira prijetnje i rizike uz pružanje savjeta i preporuka za rješavanje istih. Također pomaže u koordinaciji odgovora na kibernetičke incidente te razmjeni informacija među članicama Unije. Na temelju izloženog

[20] *op. cit.* u bilj. 5., Akt o kibersigurnosti.
[21] Europska komisija, *Okvir EU-a za kibersigurnosnu certifikaciju*, 7. veljače 2024., dostupno na: https://digital-strategy.ec.europa.eu/hr/policies/cybersecurity-certification-framework (1. listopada 2024.).

možemo zaključiti da ENISA ima ključnu ulogu u jačanju cjelokupne kibernetičke sigurnosti na području Europske Unije.

3.6. Uredba 2019/881 europskog Parlamenta i Vijeća od 17. travnja 2019. o ENISA-i te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe br. 526/2013 (engl. *Cybersecurity Act*)

Ova uredba donesena je 2019. godine s ciljem jačanja kibersigurnosti Unije i povećanja povjerenja korisnika digitalnih usluga. Glavni ciljevi ove uredbe su osiguravanje pouzdanih ICT proizvoda i usluga sa visokom razinom kibersigurnosti, zaštita europskog tržišta putem standardiziranih kibersigurnosnih certifikata te poboljšanje koordinacije između država članica, institucija Unije, privatnog sektora i stručnjaka na području kibersigurnosti. Uredbom se daje trajni mandat ENISA-i kako bi izradila sveobuhvatan okvir za certifikaciju na razini Unije. Proširuju se njezine ovlasti i odgovornosti, utvrđuju se njezini ciljevi, način na koji doprinosi razvoju i provedbi politike Unije te operativnoj suradnji. Također se određuje od kojih se dijelova sastoji struktura ENISA-e, kako se pojedini odbori sastaju te njezino cjelokupno funkcioniranje koje smo detaljnije obradili u prethodnom potpoglavlju ovog rada. Druga značajna stvar koja se utvrđuje ovom uredbom je okvir za uspostavu europskih programa kibersigurnosne certifikacije za potrebe osiguranja prikladne razine kibersigurnosti ICT proizvoda, ICT usluga i ICT procesa u Uniji.[22] Taj okvir uključuje certifikacijske programe sa normama, tehničkim zahtjevima i postupcima za ocjenjivanje sigurnosnih značajki ICT proizvoda. U sklopu okvira predviđene su ujedno i tri razine osiguranja temeljene na procjeni rizika s različitim vrstama procjena. Osnovna vrsta može uključivati samoprocjenu, značajna procjena je od strane neovisne treće strane, a visoka razina uključuje obavezno penetracijsko testiranje. Svaka razina osiguranja određuje koja je potrebna razina otpornosti određenog proizvoda ili usluge na kibernetičke napade. Unutar okvira uključeno je i priznavanje certifikata na području Unije za koje smo već napomenuli da značajno olakšava prekograničnu trgovinu.

[22] *op.cit.* u bilj. 5. i 20., Akt o kibersigurnosti.

3.7. Uredba 2024/1689 europskog Parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/182 (dalje u tekstu: AI Uredba)

AI uredba stupila je na snagu u kolovozu 2024. godine ali se velik dio obveza počinje primjenjivati tek od kolovoza 2026. godine. Ona ima nekoliko ključnih ciljeva koji se sastoje od uspostavljanja usklađenih pravila za primjenu i korištenje sustava umjetne inteligencije (dalje u tekstu: UI sustavi), osiguravanja transparentnosti i odgovornosti u procesima donošenja odluka pomoću umjetne inteligencije te smanjenja potencijalnih rizika povezanih s UI tehnologijama. Uredba se primjenjuje na UI sustave i na UI modele opće namjene te daje preciznu definiciju za oba. To znači da se neće primjenjivati na sve pametne sustave ili aplikacije koji imaju na tržištu naziv AI, već samo na one koji ispunjavaju sve značajke navedenih definicija. Uredba propisuje obveze isključivo za UI sustave i modele koji se: smatraju zabranjenima, su klasificirani kao visokorizična prema nekim kriterijima i smatraju se AI modelom opće namjene sa sistemskim rizikom.[23] Propisano je da će se UI sustavi smatrati visokorizičnima u dva slučaja: proizvoda ili sigurnosnoj komponenti proizvoda, koji su regulirani određenim propisima navedenima u prilogu Uredbe te koji se odnose na biometriju, kritičnu infrastrukturu, obrazovanje, radne odnose, ključne privatne i javne usluge, policiju, granična pitanja i migracije ili pravosuđe i demokratske postupke. Prema ovoj Uredbi, neke od stvari koje su zabranjene su stavljanje na tržište, u upotrebu ili korištenje UI sustava koji primjenjuju subliminalne tehnike radi manipulacije ponašanjem osobe, iskorištavaju ranjivosti ili slabosti fizičke osobe, klasificiraju fizičke osobe na temelju društvenog rejtinga zbog njihovog ponašanja ili obilježja, predviđaju potencijalno počinjenje kaznenog djela u odnosu na fizičku osobu, kreiraju ili šire baze prepoznavanja lica prikupljanjem podataka s interneta ili snimaka CCTV sustava nadzora, omogućuju biometrijsku kategorizaciju.[24] Te odredbe o zabranjenim postupanjima počinju se primjenjivati od veljače 2025. godine. U kolovozu iste godine stupaju na snagu odredbe o nadzoru tržišta i uspostavljanju mehanizama kontrole poput lokalnih agencija država članica za nadzor te ured Europske Unije za AI. U istom će se

[23] Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji), SL L 2024/1689, 12. srpnja 2024.

[24] Span, *Na koga se odnosi nova AI Uredba Europske Unije?*, 5. rujna 2024., dostupno na: https://www.span.eu/hr/price/na-koga-se-odnosi-nova-ai-uredba-europske-unije/ (2. listopada 2024.).

razdoblju početi primjenjivati dio s kaznenim odredbama koje su strukturirane slično kao i kazne kod GDPR-a. Najveći iznos za kategoriju najtežih prekršaja može iznositi do 6% globalnog godišnjeg prihoda poduzeća ili do 30 milijuna eura, ovisno koji je iznos veći. Bitno je napomenuti da se unutar AI Uredbe izostavlja definiranje individualnih prava pojedinaca kao što to imamo u GDPR-u, ali stavlja naglasak na transparentnost jer zahtjeva da korisnici budu informirani kada komuniciraju sa UI sustavima te da imaju pravo na informacije o tome kako se koriste njihovi podaci. Značaj ove uredbe je iznimno velik jer je to prvi zakonodavni okvir za sveobuhvatnu regulaciju umjetne inteligencije uz osiguranje etičke primjene UI sustava.

3.8. UREDBA br. 910/2014 EUROPSKOG PARLAMENTA I VIJEĆA od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (dalje u tekstu: eIDAS)

Uredba je donesena jos 2014. godine sa ciljem povećanja sigurnosti digitalnih transakcija, interoperabilnosti sustava i poticanja univerzalnog digitalnog tržišta. Ona postavlja uvjete prema kojima države članice međusobno priznaju sredstva elektroničke identifikacije za fizičke i pravne osobe uključene u prijavljeni sustav elektroničke identifikacije drugih država članica. Donosi pravila za usluge povjerenja, posebice elektroničke transakcije te definira pravni okvir za elektroničke potpise, elektroničke pečate, vremenske žigove, elektroničke dokumente, usluge preporučene elektroničke dostave i certifikacijske usluge za autentifikaciju web stranica. Ukoliko je država članica prijavila Europskoj komisiji vlastiti sustav elektroničke identifikacije (dalje u tekstu: eID sustav), ostale članice dužne su ga priznati, kako bi građani Unije mogli koristiti vlastite nacionalne eID sustave za pristup javnim uslugama u drugim državama Unije. EIDAS-ovo područje primjene odnosi se na sustave elektorničke identifikacije prijavljene od strane države članice te na pružatelje usluga povjerenja sa poslovnim nastanom unutar Unije. Ukoliko su ti sustavi zatvoreni i proizlaze iz nacionalnog prava ili iz sporazuma među utvrđenim sudionicima, na njih se neće primjenjivati ova uredba. “Usluge povjerenja” definirala je kao elektroničke usluge najčešće uz naknadu koje se sastoje od “verifikacije i validacije elektroničkih potpisa, elektroničkih pečata ili elektroničkih vremenskih žigova, usluge elektroničke preporučene dostave i certifikata koji se odnose na te usluge, certifikata za autentikaciju mrežnih stranica ili čuvanja elektroničkih potpisa, pečata ili

certifikata tih usluga".[25] Jedan od središnjih elemenata ove uredbe je elektronički potpis koji se razvrstava u tri kategorije: osnovni, napredni i kvalificirani. Kvalificirani elektronički potpis jednake je pravne snage kao vlastoručni potpis što građanima i poduzećima omogućava digitalne transakcije visokih sigurnosnih standarda. Elektronički pečat služi pravnim osobama za potvrđivanje cjelovitosti i autentičnosti dokumenata. Vjerodostojnost dokumenata dodatno je zajamčena predviđenim vremenskim žigom kojim se bilježi trenutak nastanka dokumenta. Ove godine prihvaćena je Uredba 2024/1183 europskog parlamenta i vijeća od 11. travnja 2024. o izmjeni Uredbe br. 910/2014, poznata kao eIDAS 2.0, radi uspostave nadograđenog sustava digitalne identifikacije. Ova nadogradnja fokusira se na razvoj europskog digitalnog identitetnog novčanika koji bi djelovao kao aplikacija koju građani Unije koriste za sigurnu pohranu i dijeljenje podataka s pružateljima usluga, uz osiguran strogi nadzor i visoku razinu zaštite privatnosti sukladno GDPR-u. EIDAS uredbe imaju veliki ekonomski značaj jer pomažu u kreiranju jedinstvenog digitalnog tržišta na razini Unije time što standardiziraju vrste elektroničkih identifikacija kako bi se digitalne transakcije učinile pouzdanijima i ohrabrile građane na korištenje istih. Također značajno smanjuje administrativne zapreke s kojima se poduzeća inače susreću u prekograničnim poslovanjima.

3.9. Uredba o digitalnoj operativnoj otpornosti (dalje u tekstu: DORA)

DORA je stupila na snagu još u siječnju 2023. godine, ali je rok do siječnja 2025. godine dan subjektima na koje se primjenjuje da se usklade sa zahtjevima i obvezama koje iz nje proizlaze. Izravno je primjenjiva na financijske subjekte i na pružatelje usluga informacijskih i komunikacijskih tehnologija financijskim subjektima. Njome se uspostavljaju načela i zahtjevi za upravljanje rizicima, uključujući rizike od trećih strana, povezanih s korištenjem ICT sustava koji bi inače mogli dovesti do prekida financijskih usluga u prekograničnom prometu. Takvi prekidi mogu imati utjecaj na druga poduzeća i ostale sektore te podredno na ostatak gospodarstva i ekonomije. Stoga se posebno naglašava važnost digitalne operativne otpornosti u financijskom sektoru. Ovo je jedan od sektorskih propisa iliti zakonodavnih akata Europske Unije specifičnih za financijski sektor, što znači da je ona lat. *lex specialis* te se njezinom primjenom isključuje primjena NIS2 direktive. Naravno, za područja koja nisu pokrivena odredbama DORA-e, primijenit će se NIS2. DORA specificira ključne ugovorne odredbe bitne

[25] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, SL L 257/73, 28. kolovoza 2014.

kod korištenja ICT usluga trećih strana. Od financijskih subjekata zahtijeva da se provede osnovno i napredno digitalno testiranje operativne otpornosti kako bi mogli osvijestiti slabe točke. U Uredbi je određeno što obuhvaća provedba odgovarajućih osnovnih testova: procjenu i skeniranje ranjivosti, analizu javno dostupnih izvora, procjenu mrežne sigurnosti, analizu odstupanja, preispitivanje fizičke sigurnosti, softverska rješenja za skeniranje, preispitivanje izvornoga koda, testiranje na temelju scenarija, testiranje kompatibilnosti i performansi te integralno testiranje i penetracijsko testiranje. Napredno testiranje u obliku penetracijskog testiranja vođenog prijetnjom određenim je subjektima obavezno provoditi svake tri godine. Predviđena je mogućnost nadležnog tijela da na temelju profila rizičnosti i operativnih okolnosti nekog subjekta naredi provođenje naprednog testiranja u navedenom obliku i češće.[26] Donosi stroge obveze izvješćivanja nadležnim tijelima za velike incidente povezane s ICT-om te dopušta subjektima da razmjenjuju informacije o prijetnjama kibernetičkoj sigurnosti.[27] Primjenu DORA-e će nadzirati Europska Središnja Banka za banke te ENISA za sigurnost ICT sustava, te je dana nadležnost tijelima država članica, što bi u Hrvatskoj trebala biti Hrvatska narodna banka i Hrvatska agencija za nadzor financijskih usluga. Nisu predviđena točna vremenska razdoblja za otvaranje nadzora nad financijskih institucijama te to mogu odrediti države članice nacionalnim propisima. Kazne nisu precizno definirane već je određivanje iznosa novčanih kazni i donošenje mjera prepušteno nacionalnim tijelima u sklopu odredbe kojoj im se daje nadzorna ovlast i mogućnost izricanja administrativnih kazni te obaveznih korektivnih mjera. Moguće je i izreći ograničenje poslovanja ili zabranu korištenja određenih ICT usluga.[28] DORA bi trebala pomoći u osiguravanju sigurnosti financijskog sektora jer se u njemu barata iznimno velikom količinom osobnih podataka te posljedice potencijalnih napada na taj sektor često su značajne. Financijskim institucijama usklađivanje s ovim aktom predstavlja velike napore te podredno i troškove, ali bi u konačnici trebalo poboljšati povjerenje između klijenata i njih s obzirom na pojavu sve češćih napada posljednjih godina.

[26] Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011, SL L 333/1, 27. prosinca 2022.
[27] *op.cit.* u bilj. 17., *Digital Law…*
[28] *op.cit.* u bilj. 26., DOR.A

4. PREGLED PRAVNOG UREĐENJA KIBERNETIČKE SIGURNOSTI U SJEDINJENIM AMERIČKIM DRŽAVAMA

Pravno uređenje kibernetičke sigurnosti Sjedinjenih Američkih Država sastoji se od saveznih zakona, zakona specifičnih za određene sektore, dobrovoljnih smjernica i regulatornih agencija koje su nadležne za nadzor, izricanje mjera i kazni te cjelokupnu provedbu navedenih propisa. SAD nema jedan univerzalni zakon o kibernetičkoj sigurnosti koji bismo mogli primijeniti na sve slučajeve. Ukoliko američka poduzeća imaju zaposlenike ili kupce iz drugih zemalja onda se također moraju pridržavati propisa koji se primjenjuju u tim zemljama.[29] Isto tako, SAD nema jedinstveni nacionalni zakon, koji izričito propisuje specifične standarde sigurnosti podataka za sva područja u kojima može doći do kršenja zaštite podataka, poput europskog GDPR-a. Jedini savezni zakoni o sigurnosti podataka koji su precizno definirani odnose se na poduzeća koja upravljaju određenim vrstama podataka, poput financijskih ili zdravstvenih podataka. Ta nedefiniranost jedinstvenih standarda sigurnosti podataka otežava poduzećima da osiguraju korisnicima zaštitu od potencijalne zlouporabe njihovih podataka. Određena udruženja i grupe za zaštitu privatnosti tvrde kako savezna vlada nije zadovoljila potrebe zaštite sigurnosti podataka. Posljednjih godina bilo je nastojanja Kongresa da se donesu takvi zakoni, ali dosad nisu još usvojeni. Okvir za kibernetičku sigurnost Nacionalnog instituta za standarde i tehnologiju izdvojila bih kao sveobuhvatan akt koji je široko primjenjiv i jednostavno definiran te obuhvaća cjelokupan sustav zaštite podataka, iako nije obvezujuć. U sklopu Zakona o elektorničkoj vladi doneseno je mnogo saveznih zakona koji su utjecali na razvoj kibernetičke sigurnosti u SAD-u te ćemo obraditi jedan od bitnijih pod skraćenim nazivom FISMA. Veoma utjecajnu ulogu u području kibernetičke sigurnosti u Americi imaju regulatorne agencije poput Ministarstva domovinske sigurnosti pod čijim okriljem djeluje Agencija za kibernetičku sigurnost i sigurnost infrastrukture, Savezna trgovinske komisije i Savezna komisija za komunikacije, čije funkcije i djelovanja obrađujemo na kraju ovog poglavlja.

[29] Kosseff, J., *Cybersecurity Law*, treće izdanje, John Wiley & Sons, Inc., Hoboken, 2023., str. 1.-2.

4.1. Savezni zakoni

4.1.1. Zakon o upravljanju informacijskom sigurnošću saveznih agencija (dalje u tekstu: FISMA)

FISMA je prvotno donesen 2002. godine kao dio američkog Zakona o elektorničkoj Vladi (eng. *E-Government Act*) te biva izmijenjen 2014. godine. On regulira sigurnost informacija unutar saveznih agencija te postavlja osnovne sigurnosne standarde za sve savezne agencije i za informacijske sustave kojima se one koriste. Ovaj zakon obvezuje savezne institucije da uspostave i održavaju učinkovite sigurnosne prakse kako bi zaštitile povjerljive informacije, integritet i dostupnost svojih sustava. FISMA naglašava potrebu za redovitim procjenama sigurnosti, izvještavanjem o incidentima te kontinuiranim poboljšanjima sigurnosnih procedura. Zakon također uspostavlja Nacionalni institut za standarde i tehnologiju (dalje u tekstu: NIST) kao ključnu instituciju odgovornu za postavljanje standarda i smjernica za kibernetičku sigurnost u vladinim institucijama. NIST razvija smjernice i standarde za agencije sukladno s FISMA-om. Dokumenti koje donosi daju određene upute o specifičnim mjerama za zaštitu privatnosti i dostupnosti podataka. FISMA postavlja zahtjev za procjenom rizika informacijskih sustava svim saveznim agencijama te da se prema provedenoj procjeni ugrade određene zaštitne mjere. Rizičnost sustava se mora kategorizirati kako bi se osiguralo da je osjetljivim podacima i sustavima visokovrijedne imovine (engl. *High Value Asset System*) pružena najveća razina zaštite. FISMA-om je propisano nužno provođenje godišnje sigurnosne revizije te se izvješća tih revizija podnose američkom Kongresu kako bi mogli procjeniti učinak i nedostatke sigurnosnih politika agencije. Ukoliko dođe do kibernetičkog napada ili kršenja sigurnosti, nalaže se brzo reagiranje te nužno prijavljivanje svih kibernetičkih incidenata. Svaka agencija mora imati plan za postupanje u slučaju incidenata sa procedurom za oporavak podataka i sustava. Agencije mogu dobiti FISMA certifikat i akreditaciju kroz postupak od četiri faze koji se sastoji u inicijaciji i planiranju, certifikaciji, akreditaciji i kontinuiranom praćenju. Naglašava se važnost edukacije zaposlenika redovitim obukama koje pomažu zaposlenicima u prepoznavanju prijetnji i smanjenju izlaganja osjetljivih podataka opasnostima. Privatna poduzeća, ponajviše ona koja surađuju sa saveznim agencijama isto mogu imati koristi od primjene FISMA-inih pravila.[30]

[30] Lord, N., *What is FISMA Compliance? (Definition, Requirements, Penalties, & More)*, Digital Guardian, 6. ožujka 2017., dostupno na: https://www.digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more (5. listopada 2024.).

4.1.2. Zakon o razmjeni informacija o kibernetičkoj sigurnosti (engl. Cybersecurity Information Sharing Act)

Ovaj zakon donesen je 2015. godine kako bi se poboljšala suradnja između savezne vlade i privatnih poduzeća te razmjena informacija o potencijalnim prijetnjama i rizicima vezanim uz kibernetičku sigurnost. Kod razmjene podataka, savezne agencije imaju obvezu uklanjanja osobno prepoznatljivih informacija koje nisu nužne za kibernetičku sigurnost, prije bilo kakvog daljnjeg dijeljenja informacija ostalim agencijama. Agencija za kibernetičku sigurnost i sigurnost infrastrukture (dalje u tekstu: CISA) ima obvezu dijeliti informacije s državnim agencijama i privatnim sektorom o realnim prijetnjama i proboju sigurnosnih mjera u stvarnom vremenu. Agencije moraju uspostaviti sigurne linije za komunikaciju i standardizirane načine razmjene informacija, primjerice platforme za automatsko prosljeđivanje podataka o kibernetičkim prijetnjama. Kada govorimo o uputama koje se u ovom zakonu nameću privatnom sektoru, bitno je napomenuti kako za njih one nisu obvezne, već dobrovoljne. One mogu odabrati dijeljenje podataka o prijetnjama s vladinim agencijama. Moraju ukloniti osjetljive podatke korisnika prije dijeljenja, te mogu zatražiti pomoć od CISA-e kako bi lakše učinili podatke anonimnima. Poduzeća su dužna čuvati i arhivirati određene zapise o dijeljenju informacija te se pridržavati sigurnosnih postupaka pri baratanju podacima o prijetnjama, kako bi se pomoglo u eventualnim kasnijim istragama o sigurnosti. Poduzeća koja odluče sudjelovati u dijeljenju informacija, moraju osigurati istinitost i točnost podataka. Ukoliko se ustanovi da su namjerno podijeljeni netočni podaci, postoji mogućnost gubitka određenih vrsta zaštite, primjerice gubitak imuniteta od tužbi. Ovo je vrlo značajno za poduzeća s obzirom da je jedna od glavnih značajki ovog akta izuzeće od odgovornosti za posljedice koje proizlaze iz dijeljenja ovih podataka ukoliko ta poduzeća dijele podatke prema pravilima CISA-e. Dakle, značaj ovog akta proizlazi iz toga što je promijenio običaj da poduzeća ne dijele vrlo značajne informacije za područje kibernetičke sigurnosti zbog straha od mogućeg kršenja propisa. Pruža različite vrste zaštite, poput imuniteta od progona prema saveznim i državnim zakonima o objavljivanju podataka i izuzeća od saveznog zakona o antitrustu, što potiče poduzeća na svojevoljno dijeljenje informacija.[31]

[31] Osaji, P., *Pros and Cons of the Cybersecurity Information Sharing Act of 2015*, The Alliance for citizen engagement, 14. rujna 2023., dostupno na: https://ace-usa.org/blog/research/research-technology/pros-and-cons-of-the-cybersecurity-information-sharing-act-of-2015/ (8.listopada 2024.).

4.1.3. Zakon o zaštiti privatnosti djece na internetu (engl. Children's Online Privacy Protection Act, dalje u tekstu: COPPA)

Ovaj zakon donesen je još je 1998. godine radi zaštite privatnosti djece ispod 13 godina na internetu. COPPA je među prvim zakonima koji uvodi stroge zahtjeve za zaštitu privatnosti djece vezano uz prikupljanje i obradu podataka. Primjenjuje se na sve internetske stranice, aplikacije i usluge namijenjene djeci mlađoj od 13 godina te one koje svjesno prikupljaju informacije o djeci, iako možda nisu namijenjene djeci. Društvene mreže, igrice i drugi digitalni servisi moraju poštovati pravila COPPA-e ukoliko žele prikupljati ili koristiti podatke djece u SAD-u. Prema COPPA-i, platforme moraju dobiti izričit pristanak roditelja ili skrbnika prije nego što prikupe osobne podatke djece ispod 13 godina. Poduzeća su dužna obavijestiti roditelje o vrstama podataka koje žele prikupljati, načinu njihova korištenja te mogućnosti dijeljenja s trećim stranama. Takva obavijest mora biti dostupna roditeljima, jasna, i lako razumljiva prije samog prikupa podataka.[32] Ograničena je mogućnost prikupljanja podataka samo na nužno prikupljanje za određenu aktivnost ili uslugu koja se pruža. Roditelji imaju pravo pristupa podacima koji se prikupljaju na zahtjev te također mogu zatražiti njihovo brisanje. Poduzeća su dužna poduzeti tehničke, organizacijske i fizičke sigurnosne mjere u skladu sa standardima kako bi zaštitile podatke od neovlaštenog pristupa, njihovog otkrivanja ili zloupotrebe. Novčane kazne za kršenje COPPA-e koje izriče Savezna trgovinska komisija (dalje u tekstu: FTC) mogu doseći vrlo visoke iznose. Možemo reći da Savezna trgovinska komisija zapravo provodi ovaj zakon. Neki od poznatijih slučajeva u kojima su platforme bile kažnjene zbog kršenja ovog zakona su slučaj protiv Youtube-a u vlasništvu Google-a, gdje je navedena platforma morala platiti 170 milijuna američkih dolara zbog prikupljanja podataka o djeci ispod 13 godina bez pristanka roditelja. [33]Također je Youtube morao primijeniti mjere ograničavanja prikupa podataka o djeci i prilagoditi sadržaj prema pravilima ovog zakona. Još jedna poznata platforma bio je Tiktok koji je kažnjen sa 5.7 milijuna dolara zbog prikupljanja osobnih podataka djece poput imena i e-mail adrese isto bez roditeljskog pristanka.[34] Ovaj je

[32] Childrens Online privacy Protection Rule, 16 CFR Part 312, Code of Federal Regulations, 17. siječnja 2013., dostupno na: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312 (10. listopada 2024.).
[33] Federal Trade Comission, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, 4. rujna 2019., dostupno na: https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law (12. listopada 2024.).
[34] Federal Trade Comission, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law*, 27. veljače 2019., dostupno na: https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy (13. listopada 2024.).

zakon značajno utjecao na regulaciju prikupljanja i obrade podataka, ali određeni dio stručnjaka smatra da nije najbolje prilagođen razvijenijim suvremenim tehnologijama. Pri ciljanju sadržaja kod raznih stranica sve se više koriste internetski algoritmi koji dodatno otežavaju praćenje prikupa podataka djece.

4.1.4. Okvir za kibernetičku sigurnost Nacionalnog instituta za standarde i tehnologiju (dalje u tekstu: NIST)

NIST je razvio Okvir za kibernetičku sigurnost te ga objavio 2014. godine. Ovaj okvir pruža poduzećima, organizacijama i tijelima vlade skup industrijskih standarda i preporučenih praksi za upravljanje rizicima koji prijete kibernetičkoj sigurnosti. Jezgra ovog okvira podijeljena je u pet faza razvoja kibernetičke sigurnosti, tj. pet neprekidnih funkcija. Počinje s identificiranjem kritičnih sustava i potencijalnih rizika i prijetnji kroz razumijevanje okruženja organizacije i imovine. Zatim se fokusira na primjenu zaštitnih mjera poput zaštite podataka, kontrole pristupa, tehničke sigurnosne mjere i obuku zaposlenika. Faza detektiranja sastoji se od kontinuiranog nadzora i analiziranja svih povezanih aktivnosti radi identifikacije sumnjivih pojava i potencijalnih incidenata. Ukoliko dođe do sigurnosnih incidenata, iduća je faza odgovor na iste, uz uspostavljanje pripadajućih procedura za smanjenje štete te završna faza oporavka koja se sastoji od vraćanja sustava u normalno stanje i nastavka pružanja usluga uz ponovno uspostavljanje sigurnosti. NIST okvir definira i četiri razine implementacije okvira koji prikazuju kako organizacija upravlja rizicima prema definiranom okviru te na kojem je stupnju razvijenosti u tom području. Profili okvira prikazuju koje je kategorije organizacija odredila kao najvažnije prema procjeni rizika analiziranjem svih kategorija.[35] On može biti korišten kako bi se usporedila trenutna razina sigurnosti sa razinom koja se želi postići te također omogućava prilagodbu okvira ovisno o specifičnostima prijetnje i veličini organizacije. NIST okvir nije obvezujuć te je lako prilagodljiv različitim organizacijama i razinama sigurnosti. Okvir je jasan te se jednostavno implementira, bez obzira imaju li organizacije razvijen sustav i stručnjake za kibernetičku sigurnost. Još jedna od prednosti očitava se u tome što se NIST okvir primjenjuje međunarodno kao referentni model, a ne samo na poduzeća u SAD-u.[36] Posebno je bitna njegova primjena u kritičnim infrastrukturama, kao što su

[35] IBM, *What is the NIST Cybersecurity Framework?*, dostupno na: https://www.ibm.com/topics/nist (15. listopada 2024.).
[36] NIST, *CSF 1.1 Uses and Benefits of the Framework*, 6. veljače 2018., dostupno na: https://www.nist.gov/cyberframework/uses-and-benefits-framework (16. listopada 2024.).

financijske institucije, zdravstveni sustavi i energetika. Možemo zaključiti kako je NIST okvir zbog svoje jednostavnosti i prilagodljivosti široko prihvaćen kao alat u području kibernetičke sigurnosti koji omogućava različitim sektorima i veličinama poduzeća da lakše prepoznaju i odgovore na prijetnje te zaštite svoje podatke.

4.2. Zakoni specifični za sektore

4.2.1. Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja (dalje u tekstu: HIPAA)

HIPAA zakon donesen je 1996. godine u SAD-u. Njegov cilj je zaštita privatnosti pacijenata putem definiranja pravila za regulaciju pristupa, razmjene i pohrane osjetljivih podataka pacijenata. HIPAA također omogućava zaposlenicima da zadrže svoje zdravstveno osiguranje kada promijene posao, ali mi ćemo se za potrebe ovog rada fokusirati na dio o zaštiti podataka pacijenata. Zakon se primjenjuje na pružatelje zdravstvenih usluga, zdravstvene planove kao što su osiguravatelji, zdravstvene klirinške kuće koje obrađuju zdravstvene podatke te se primjenjuje na poslovne suradnike koji pristupaju ili prenose zaštićene zdravstvene podatke u ime obuhvaćenih subjekata. HIPAA je podijeljena u nekoliko naslova koje ćemo razložiti kroz njihove odredbe. Odredba o pravilu o privatnosti štiti zaštićene zdravstvene informacije kroz reguliranje kako zdravstvene ustanove, osiguravajuće kuće i pružatelji usluga smiju koristiti i dijeliti zdravstvene podatke pacijenata. Pod zaštićene zdravstvene informacije pripadaju medicinske informacije, informacije o liječenju, informacije o plaćanju te demografske informacije. Svaki pacijent ima pravo zatražiti uvid u svoje zdravstvene podatke te saznati o načinu na koji se oni koriste, pravo na ispravak, traženje ograničenja i podnošenje pritužbe. Pravilo o sigurnosti propisuje tehničke i administrativne mjere koje zdravstvene i ostale organizacije moraju poduzeti radi zaštite elektroničkih zdravstvenih podataka. Ono definira različite vrste tehničkih kontrola, poput kontrole pristupa i autentifikacije korisnika, enkripcije podataka te obuku zaposlenika i razvoj politika sigurnosti što se smatra administrativnim mjerama. Pravilo o obavještavanju o povredi podataka obvezuje zdravstvene ustanove i pružatelje usluga na obavijest pacijentima i vlastima ukoliko dođe do povrede podataka. Dodatna obveza obavještavanja javnosti nalaže se kod ozbiljnih povreda, primjerice kod povrede koja uključuje minimalno 500 osoba. Iznimno se dopušta otkrivanje zaštićenih podataka bez pristanka, ukoliko je riječ o hitnim slučajevima u zdravstvu ili kaznenim

istragama. Ured za građanska prava unutar Ministarstva zdravstva i društvenih usluga je tijelo koje je zaduženo za provođenje i nadzor usklađenost sa navedenim HIPAA-om. Kazne koje su propisane u slučaju neusklađenosti su složene jer ovise o nekoliko čimbenika: razini krivnje, vrsti i broju prekršaja. Mogu se odnositi na građansku odgovornost koja rezultira visokim novčanim kaznama ili na kaznenu odgovornost sa kaznom zatvora u slučaju namjerne zloupotrebe podataka.[37] Neki od značajnijih primjera kažnjavanja organizacija su slučaj organizacije Anthem 2015.godine koja je morala platiti 16 milijuna dolara zbog povrede podataka 78,8 milijuna ljudi te slučaj New York-Presbyterian Hospital i Columbia University Medical Center koji su 2014. godine platili 4,8 milijuna dolara zbog izlaganja elektroničkih zaštićenih zdravstvenih podataka pacijenata na internetu.[38]

4.2.2. Zakon Gramm-Leach-Bliley (dalje u tekstu: GLBA)

Ovaj zakon zove se još i Zakon o modernizaciji financijskih usluga. Donesen je 1999. godine radi zaštite osobnih podataka korisnika financijskih usluga. GLBA je modernizirao financijski sektor tako što je omogućio financijskim institucijama udruživanje i pružanje zajedničkih usluga te je definirao pravila o načinu prikupljanja, korištenja i dijeljenja podataka klijenata te odgovarajuće zaštitne mjere za osiguranje tih podataka. Ovaj se zakon primjenjuje na financijske institucije što uključuje banke, osiguravajuća društva, investicijska društva, kreditne i zajmodavne udruge te financijska poduzeća koja pružaju usluge savjetovanja za financijske ili investicijske planove. GLBA definira financijsku instituciju s obzirom na djelatnosti kojom se institucija bavi ukoliko je ta djelatnost uključena u financijske aktivnosti kako je opisano u odjeljku samog zakona. U tom odjeljku se nalazi popis od devet čimbenika koji se uzimaju u obzir pri određivanju je li neka aktivnost financijske prirode. Slično kao u prethodnom HIPAA zakonu koji smo obradili, GLBA sastoji se od nekoliko ključnih pravila. Pravilo o privatnosti propisuje dužnost informiranja klijenata o prikupljanju i korištenju osobnih podataka, obvezujuće redovno slanje obavijesti o privatnosti sa jasnim navođenjem načina korištenja tih podataka te mogućnost za klijente da odbiju dijeliti podatke s trećim strana (engl. *opt-out*). Pravilo o zaštiti obvezuje sve financijske institucije na uspostavljanje sigurnosnih mjera za zaštitu podataka te su dužne uspostaviti i kontinuirano pratiti i prilagođavati sigurnosne programe koji se sastoje od tehničkih, administrativnih i fizičkih

[37] Solix, *Hipaa*, dostupno na: https://www.solix.com/hr/kb/hipaa/ (18. listopada 2024.).
[38] Chin, K., *Top 20 Worst HIPAA Violation Cases in History*, Upguard, (31. listopada 2024.), dostupno na: https://www.upguard.com/blog/worst-hipaa-violation-cases (2. studenog 2024.).

elemenata. Pravilo o engl. *pretextingu* kriminalizira lažno predstavljanje radi pristupa podacima. Financijske institucije obvezuje na obuku zaposlenika i donošenje mjera koje sprečavaju neovlašten pristup podacima putem prijevara. S obzirom da savezna regulatorna struktura za financijske institucije nije jedinstvena već podijeljena, GLBA navodi nekoliko saveznih regulatornih agencija koje nadziru primjenu zakona.[39] Savezna komisija za trgovinu nadgleda primjenu zakona na nebankarske institucije poput zajmodavnih udruga i poduzeća za financijsko savjetovanje. Ured za zaštitu financijskih potrošača nadzire primjenu pravila o privatnosti od strane financijskih institucija. Ured za kontrolu valute i Savezni ured za nadzor kreditnih zadruga te slične agencije nadziru primjenu pravila o privatnosti i pravila o zaštiti od strane financijskih institucija. U određenim slučajevima, kao što je to kod osiguravajućih društava, primjenu provode regulatorne agencije na razini saveznih država. Kazne, kao i kod HIPAA-e, mogu biti novčane ili kazne zatvora do 5 ili 10 godina u slučaju namjerne zloupotrebe podataka.[40] Visokim novčanim kaznana i mogućnošću izricanja kazne zatvora ovim se zakonom potiče financijske institucije na važnost pridržavanja zaštitnih mjera i očuvanja sigurnosti i privatnosti podataka klijenata.

4.3. Zakoni specifični za države

4.3.1. Zakon o privatnosti potrošača (dalje u tekstu: CCPA)

CCPA donesen je 2018. godine te predstavlja jedan od najopsežnijih zakona o privatnosti u SAD-u postavljajući standarde za zaštitu osobnih podataka građana Kalifornije. Zbog opsežnosti uređene materije često ga se uspoređuje sa GDPR-om.. Ovaj se zakon primjenjuje na prikupljanje ili prodaju osobnih podataka potrošača koji žive u Kaliforniji, bez obzira gdje je sjedište poduzeća koje te podatke prikuplja. Najveći dio poduzeća koja prikupljaju podatke građana Kalifornije je iz sektora informacijskih komunikacija, te se tako primjenjuje i na europska poduzeća navedenih djelatnosti, ako njihovo poslovanje ili proizvodi uključuju prikupljanje podataka uz ispunjenje ostalih propisanih elemenata. Barem jedan od ovih elemenata, uz uvjet građanstva Kalifornije, mora biti ispunjen da bi se na neko poduzeće

[39] Pepper D., Ross S. L., Diamond E., *Gramm-Leach-Bliley Act(GLBA) Privacy & Data Security*, Norton Rose Fulbright US LLP, kolovoz 2024., dostupno na: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/glba---cybersecurity-governance-materials/gramm-leach-bliley-act-glba-privacy-data-security.pdf (20. listopada 2024.).
[40] Porter, A., *Navigating GLBA Compliance: A Comprehensive Guide*, BigID, 5. listopada 2023., dostupno na: https://bigid.com/blog/glba-compliance/ (22. listopada 2024.).

primijenio ovaj zakon: poduzeće ima godišnji prihod veći od 25 milijuna dolara, procesuira osobne podatke od minimalno 50 tisuća potrošača, uređaja ili kućanstva godišnje, više od 50 posto godišnjeg prihoda stječu prodajom osobnih podataka potrošača. Osobni podaci definirani su kao "sve informacije koje se odnose, opisuju, razumno se mogu povezati s, ili bi se razumno mogle povezati, izravno ili neizravno, s određenim potrošačem ili kućanstvom."[41] Prava potrošača koja proizlaze iz ovog zakona su: pravo na obavijest o podacima koji se prikupljaju, svrhu korištenja i dijele li se s trećim stranama, pravo na pristup podacima na zahtjev, pravo na brisanje podataka te pravo na zabranu prodaje podataka što poduzeća moraju jasno istaknuti na svojim web stranicama. Uvjeti za pristanak potrošača na prikupljanje informacija puno su niži od onih u GDPR-u. Nema izričitog uvjeta da potrošač mora sam potvrditi svoj pristanak (engl. *opt-in* consent) osim kod podataka djece ispod određene dobi. CCPA savjetuje poduzeća da implementiraju određene sigurnosne mjere kako bi uspješno ostvarili zaštitu osobnih podataka na koju su obvezni. Propisane su novčane kazne za nepoštivanje zakona u iznosu od 2500 do 7500 dolara, ovisno o stupnju namjere koji se ovdje gleda pri određivanju kazni. CCPA predviđa i pravo privatne tužbe za potrošače u slučaju povrede podataka zbog neovlaštenog ili nezakonitog procesuiranja podataka od strane poduzeća.[42]

4.4. Regulatorne Agencije

4.4.1. Agencija za kibernetičku sigurnost i sigurnost infrastrukture (dalje u tekstu: CISA)

CISA je osnovana 2018. godine radi zaštite kritične infrastrukture u SAD-u i jačanja kibernetičke sigurnosti te djeluje u sklopu Ministarstva domovinske sigurnosti. CISA je definirala svoj cilj kao stvaranje sigurne i otporne kritične infrastrukture. To znači da agencija predvodi nacionalne napore u otkrivanju i suočavanju s prijetnjama za kibernetičku i fizičku infrastrukturu. Tri glavna područja misije agencije obuhvaćaju kibernetičku sigurnost, sigurnost infrastrukture i komunikaciju u hitnim situacijama. CISA pruža ključnu potporu za ublažavanje posljedica u slučaju kibernetičkog napada na neko američko poduzeće. U tome surađuje s nadležnim agencijama za provedbu zakona , kao što je to Nacionalni centar za kibernetičku sigurnost u ostalim državama. Agencija osim odgvora na incidente, pruža usluge

[41] Civil Code, California Consumer Privacy Act of 2018, [1798.100 - 1798.199.100], 28. lipnja 2018., dostupno na: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140. (23. listopada 2024.).
[42] Security Compass, *Enterprise compliance with the California Consumer Privacy Act*, 8. svibnja 2024., dostupno na: https://www.youtube.com/watch?v=2Hrtxu_c0-8 (25. listopada 2024.).

razmjene informacija kao pomoć poduzećima za kontinuirano praćenje sigurnosnih rizika. Podijeljena je u sedam različitih međusobno povezanih odjela : Odjel za kibernetičku sigurnost, Odjel za infrastrukturu, Odjel za komunikacije u hitnim situacijama i Odjel za angažman dionika, Odjel za integrirane operacije, Nacionalni centar za upravljanje rizicima i Urede za omogućavanje misije. Agencija također pruža usluge upozorenja na kibernetičke prijetnje tako što poduzećima na redovnoj bazi izdaje upozorenja i preporuke o novim prijetnjama, probojima sigurnosti i otkrivenim ranjivostima koje prijavljuju poduzeća te se naziva popisom poznatih iskorištavanih ranjivosti (engl. *KEV list*).[43] CISA redovito izdaje savjete i alate za procjenu rizika te razumijevanje trenutnih prijetnji za poduzeća i organizacije. Organizira radionice za zaposlenike u kritičnim sektorima te razne programe kao što su CDM program za kontinuirani nadzor sigurnosti za otkrivanje i smanjenje prijetnji. CDM program pruža "sigurnosne alate, integracijske usluge i nadzorne ploče koje pomažu agencijama sudionicama da poboljšaju svoju sigurnosnu poziciju kroz smanjenje izloženosti prijetnjama u agencijama, povećanje vidljivosti u saveznom kibernetičkom sigurnosnom okruženju, poboljšanje sposobnosti odgovora na kibernetičke prijetnje na saveznoj razini, pojednostavljenje izvješćivanja prema FISMA-i."[44] Razlika CISA-e naspram FTC-a je u tome da ona ne može izricati kazne jer ne provodi primjenu i nadzor zakona kao i FTC, ali se svejedno smatra ključnom regulatornom agencijom u SAD-u te ima velik utjecaj na područje kibernetičke sigurnosti.

4.4.2. Savezna trgovinska komisija (dalje u tekstu: FTC)

FTC ustanovljena je 1914. godine Zakonom o Saveznoj trgovinskoj komisiji te ima značajnu ulogu u kibernetičkoj sigurnosti u SAD-u na području zaštiti privatnosti podataka potrošača. Ona nije primarna agencija za kibernetičku sigurnost jer primarnu ulogu ima CISA-e, ali FTC ima značajnu regulativnu ovlast nad poduzećima koja prikupljaju, koriste i dijele osobne podatke korisnika. Provodi zakone za zaštitu podataka poput COPPA i GLBA koje smo obradili. FTC ima ovlasti poduzeti pravne mjere protiv poduzeća koja ne implementiraju nužne mjere kibernetičke sigurnosti te ih može optužiti za "nepoštenu praksu" prema članku 5(a) Zakona o FTC-u. FTC obično nalaže poduzećima sa slabim sustavom zaštite podataka da uvedu opsežne sigurnosne programe, provode redovite sigurnosne provjere uz kontinuirano

[43] Kelly, R., *What is the Cybersecurity and Infrastructure Security Agency (CISA) and what does it do?*, ITPro, 19. srpnja 2024., dostupno na:https://www.itpro.com/security/what-is-cisa (26. listopada 2024.).
[44] CISA, *Continuous Diagnostics and Mitigation (CDM) Program*, https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program (27. listopada 2024.).

ažuriranje i prilagodbu mjera. Može naložiti i povrat sredstava potrošačima te brisanje nezakonito pribavljenih podataka. FTC pokrenula je više stotina slučajeva protiv različitih poduzeća. Ukoliko poduzeće prekrši nalog FTC-a, ona može odrediti sankcije u obliku novčane kazne. Meta, tadašnji Facebook je prekršio nalog FTC-a iz 2012. godine zbog obmanjivanja korisnika o mogućnosti kontrole privatnosti njihovih osobnih podataka. Sklopio je nagodbu sa FTC-em u iznosu od 5 milijardi dolara. S obzirom da se autoritet FTC-a može jako široko interpretirati došlo je do nesigurnosti u nekoliko slučajeva oko toga što točno potpada pod članak 5(a) koji FTC koristi za izdavanje naloga i optužnica protiv poduzeća sa nižom razinom zaštite podataka. Značajan je slučaj LabMD iz 2018. godine, kad je jedanaesti okružni prizivni sud utvrdio kako nalog FTC-a da se implementira "razumni sigurnosni program" nije bio dovoljno preciziran.[45] Nakon toga FTC je počela izdavati naloge koji su detaljnije opisani i specificirani kao što su naveli u nalogu za Zoom gdje naređuju testiranje ranjivosti web aplikacija prema OWASP Top 10 i javno poznatim ranjivostima prije stavljanja same aplikacije u produkciju.[46] FTC također izdaje smjernice i preporuke za razumijevanje i bolju zaštitu kibernetičke sigurnosti različitim poduzećima. Izdala je i vodiče za poduzeća o odgovoru na proboj podataka, o sigurnosnim savjetima za razvoj aplikacija, o pravilima o zaštititnim mjerama, sigurnosti interneta stvari i mnoge druge. Osim navedenog, organizira kampanje za edukaciju potrošača i poslovnih subjekata kao što je "OnguardOnline", o zaštiti podataka i kibersigurnosti. FTC u svome radu surađuje s CISA-om i FBI-jem u području kibernetičkog kriminala te s međunarodnim tijelima na usklađivanju reakcije na incidente.

4.4.3. Savezna komisija za komunikacije (dalje u tekstu: FCC) i Odjel za kibernetičku sigurnost i pouzdanost komunikacija (dalje u teksu: CCR)

FCC nadzire telekomunikacije, emitiranje, širokopojasne mreže i ostale komunikacijske kanale. Njezina uloga u kibernetičkoj sigurnosti je ograničena na komunikacijske sustave ali svejedno ima bitan utjecaj jer su komunikacijske mreže temelj digitalne infrastrukture te ovisnost o širokopojasnim i bežičnim mrežama kontinuirano raste. CCR unutar FCC-a,

[45] Denny, W. R., *Cyber Center: Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act*, American Bar Association, 20. lipnja 2016., dostupno na: https://www.americanbar.org/groups/business_law/resources/business-law-today/2016-june/cyber-center-cyber-security-as-an-unfair-practice/ (29. listopada 2024.).

[46] ImmuniWeb, FTC Compliance and Cybersecurity *(GLBA, FCRA, SEC)*, 6. rujna 2023., dostupno na: https://www.immuniweb.com/compliance/ftc-cybersecurity-privacy-compliance-glba-fcra-sec/ (30. listopada 2024.).

osigurava pouzdanost komunikacijskih mreža za građane s naglaskom na komunikaciju u izvanrednim okolnostima. Bitna područja djelovanja CCR-a odnose se na hitne komunikacije i sustave za hitna upozorenja, rad komunikacijskih kanala u vrijeme katastrofa te značajne incidente sigurnosti mreža. On nadzire prijetnje komunikacijskih mreža radi definiranja trendova i procjene koje mjere FCC treba donijeti za sprječavanja napada. CCR prikuplja podatke o operativnom statusu komunikacijske infrastrukture tijekom izvanrednih situacija. Pružatelji komunikacijskih usluga poput bežičnih, žičanih, emitiranih i kabelskih poduzeća mogu dobrovoljno izvješćivati o stanju infrastrukture u Sustavu izvješćivanja o informacijama tijekom katastrofa (dalje u tekstu:DIRS).[47] FCC izdaje preporuke i smjernica za poboljšanje sigurnosti mreža za operatore, pružatelje internetskih usluga i ostale entitete koji djeluju na području komunikacija. Pokušavaju smanjiti mogućnost pojavljivanja napada kao što je distribuirani napad uskraćivanjem resursa poznatiji kao DDoS napad, koji može dovesti do nedostupnosti mreže korisnicima. FCC također radi na sigurnosti mobilnih mreža poput 5G mreže. U tim programima surađuje s DHS-om i drugim agencijama na izradi smjernica za sigurnost 5G infrastrukture i sprječavanju napada.[48]

[47] Federal Communications Commission, *Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau*, 7. svibnja 2024., dostupno na: https://www.fcc.gov/cybersecurity-and-communications-reliability-division-public-safety-and-homeland-security-bureau (2. studenog 2024.).

[48] Homeland Security, *SECURITY IMPLICATIONS OF 5G TECHNOLOGY: Overview and Recommendations*, dostupno na: https://www.dhs.gov/sites/default/files/publications/privacy_and_security_implications_of_5g_technology_0.pdf (5. studenog 2024.).

5. USPOREDBA REGULATORNIH PRISTUPA

5.1. Usporedba s GDPR-om

Nakon detaljne analize pojedinačnih akata koji su značajniji u području kibernetičke sigurnosti obaju pravnih krugova, u ovom poglavlju usporedit ćemo pristupe. Europska unija uvrstila je privatnost među temeljna ljudska prava te su stoga zahtjevi za privatnošću i sigurnošću podataka stroži nego oni u SAD-u. To možemo vidjeti već u postojanju opsežnog i sveobuhvatnog GDPR-a. Može doći do primjene GDPR-a i na određena poduzeća u SAD-u, iako poduzeće nije osnovano u EU, pod već spomenutim uvjetom obrade podataka europskih građana povezanim uz nuđenje robe ili usluga na njihovom teritoriju. U SAD-u i dalje ne postoji takav univerzalan zakon unatoč nastojanjima određenih stručnjaka, ali se značajno približila država Kalifornija donošenjem i provođenjem CCPA zakona. Potencijalan problem kod pravnog okvira SAD-a je u fragmentaciji propisa, sa primjenom različitih pravila na saveznom te na državnom nivou, što može rezultirati poteškoćama i pravnom nesigurnošću za poduzeća u području usklađenosti sa regulativama. CCPA je američki zakon po materiji najsličniji GDPR-u, s time da je ograničene primjene na građane Kalifornije. CCPA i GDPR daju korisnicima pravo pristupa podacima, brisanja podataka i ograničenja prodaje osobnih podataka, ali je GDPR stroži oko postojanja pristanka za obradu podataka. GDPR se primjenjuje na sva poduzeća koja obrađuju podatke građana Europske Unije, a CCPA samo na veća poduzeća koja posluju s građanima Kalifornije ili ostvaruju značajan prihod sa tog područja. U SAD-u vidimo zakone koji se odnose na pojedine sektore te stoga i na pojedine vrste podataka, poput HIPAA zakona. HIPAA regulira zaštitu osobnih zaštićenih zdravstvenih podataka u SAD-u te se primjenjuje na zdravstvene organizacije, a GDPR se odnosi na sve vrste osobnih podataka, uključujući i medicinske. HIPAA nameće obvezu osiguranja povjerljivosti zaštićenih zdravstvenih podataka, ali ne pruža sva prava pojedincima iz GDPR-a, poput prava na brisanje podataka. COPPA zakon nameće internetskim stranicama nužno postojanje pristanka roditelja prije prikupljanja i procesuiranja podataka djece mlađe od 13 godina te tu vidimo sličnost sa GDPR-om, koji također ima posebne odredbe o procesuiranju podataka djece. Propisi koji uređuju materiju na način sličan europskom AI aktu, u SAD-u još nisu doneseni.

5.2. Usporedba sektorskih propisa

Prethodno smo spomenuli da u Europskoj Uniji ne postoje sektorski propisi koji se odnose na zaštićene zdravstvene podatke kao što je to u SAD-u HIPAA, već je područje te vrste podataka također pokriveno GDPR-om. Stoga ćemo uspoređivati propise financijskog sektora, što je u Europskoj Uniji DORA, a u SAD-u njoj najsličniji GLBA. Oba se akta primjenjuju na financijske institucije s time da se DORA primjenjuje i na pružatelje ICT usluga trećih strana, kao što je sustav Cloud-a. GLBA ne obvezuje na određenu kontrolu trećih strana. Nameću im obvezu procjene sigurnosnih rizika i poduzimanja odgovarajućih mjera, ali DORA izričito zahtijeva redovita sigurnosna testiranja, uključujući penetracijska testiranja i planove oporavka. GLBA nema definirane zahtjeve za testiranje otpornosti te ostavlja na izbor insititucijama prema procijenjenim rizicima da odaberu sigurnosne mjere. DORA obvezuje financijske institucije na prijavu značajnih ICT incidenata nadzornim tijelima, a GLBA nema tu obvezu već je prijava eventualno ostavljena saveznim i državnim tijelima da reguliraju njezinu obvezu. U oba akta predviđen je nadzor regulatornih agencija, kod DORA-e je to ENISA i Europska središnja banka te je dana ovlast nadzora nacionalnim tijelima država članica, a primjenu GLBA nadzire nekoliko predviđenih saveznih agencija. Niti u jednom od ova dva akta nisu precizirani iznosi novčanih kazni, a u GLBA je predviđena i kazna zatvora. DORA predviđa mogućnost poduzimanja dodatnih mjera, kao što su ograničenje poslovanja ili zabrana korištenja određenih ICT usluga dok ne postupe po predviđenim sigurnosnim standardima te propisuje obavezne korektivne mjere. GLBA predviđa mjere za dodatnim kontrolama zaštite podataka, ali bez opcije izricanja ograničenja poslovanja ili zabrane korištenja ICT usluga. Korektivne mjere nisu uvijek obavezne i ovise o vrsti povreda i regulatornoj agenciji koja je nadležna izreći kaznu.

5.3. Usporedba regulatornih agencija

U Europskoj Uniji ENISA je glavna agencija za koordinaciju i pomoć u području kibernetičke sigurnosti. Ona u suradnji s Europskom komisijom pruža smjernice te europski okvir za kibersigurnost pod nazivom ENISA okvir, provodi istraživanja i daje podršku državama članicama u razvijanju sustava zaštite kibersigurnosti. Nacionalna tijela za kibernetičku sigurnost, poput nacionalnog CERT-a u sklopu CARNET-a u Hrvatskoj, u svakoj državi članici provode europske direktive i uredbe uz donošenje provedbenih propisa kada je to potrebno. U

određenim slučajevima kao što je to kod DORA-e, nacionalna tijela imaju ovlast nadzora provođenja akta i izricanja mjera. Najčešće se aktima propisuje obveza prijavljivanja značajnih incidenta nadležnih tijelima u relativno kratkom roku, primjerice 72 sata od otkrivanja incidenta prema GDPR-u. U SAD-u imamo drugačiji pristup djelovanja agencija u više slojeva, s obzirom na postojanje sektorskih i saveznih agencija za određene zakone. Primarna agencija za ovo područje je CISA, koja djeluje u sklopu Ministarstva domovinske sigurnosti, te kao glavna pomoć poduzećima u slučaju kibernetičkog napada, odgovorna je za zaštitu kritične infrastrukture i za komunikaciju u hitnim situacijama. CISA nema ulogu nadzora primjene zakona, stoga ne može izricati mjere već je njezina uloga više fokusirana na koordiniranje i potporu privatnom sektoru i državnim organizacijama. CISA potiče privatni sektor na suradnju putem definiranja dobrovoljnih standarda i nekih incijativa. FTC provodi nadzor i primjenu akata kao što su COPPA i GLBA, te može pokretati slučajeve, izdavati naloge poduzećima i izricati mjere. Savezne države često donose svoje propise o zaštiti podataka, kao što smo to vidjeli sa CCPA, što dovodi do toga da agencije ne djeluju usklađeno i koordinirano jer primjenjuju različite propise. Također, različiti sektorski propisi znače da se na financijske institucije primjenjuju različiti propisi od onih koji se primjenjuju na zdravstvene ustanove, stoga ih i drugačije agencije nadziru. U SAD-u, prijava incidenata često je dobrovoljna, a definiranje pravila za prijavu mogu biti regulirana državnim i saveznim tijelima.

6. ZAKLJUČAK

Europska unija i SAD imaju donekle slične pravne okvire, ali uz određene razlike koje se najviše ističu u pogledu pitanja jedinstvenog ili fragmentiranog pristupa uređenja kibernetičke sigurnosti. U EU privatnost je uvrštena u temeljna ljudska prava, što onda dovodi i do potrebe za većom razinom zaštite i regulacije pravnim aktima. Možemo izvesti zaključak da SAD daje veću prednost poslovnim interesima nad pravima privatnosti pojedinaca iz toga što u SAD-u ne postoji univerzalan zakon sa razrađenim mehanizmima provedbe zaštite privatnosti kao što je to u Europskoj Uniji GDPR. Razumljivo je kada to sagledamo u političkom kontekstu vladavine veće razine kapitalizma nego što je to u Europskoj Uniji. Također se može razaznati da SAD pridaje vrlo veliki značaj nacionalnoj sigurnosti, što je posebice vidljivo u saveznim zakonima koje smo obrađivali, poput FISMA-e u sklopu Zakona o elektorničkoj vladi. EU ima centraliziraniji pristup materiji kibersigurnosti putem osnivanja institucija kao ENISA, koja ima zadaću koordinacije sigurnosnih politika država članica, pruža smjernice i nadzire provedbu utvrđenih standarda. Nacionalnim tijelima u EU dana je ovlast provedbe nadzora i primjene standarda na razini države članice te su im poduzeća obvezna prijavljivati značajne incidente. SAD-ov pravni okvir kibernetičke sigurnosti i zaštite podataka je više pojedinačan i fragmentiran po sektorima i saveznim državama. Nije donesen univerzalni zakon kao GDPR, već prevladavaju sektorski propisi koji uređuju određene vrste podataka i primjenjuju se prema tome na određene institucije koje ih prikupljaju. Takve smo primjere vidjeli za zaštićene zdravstvene podatke kod HIPAA-e, COPPA za zaštitu podataka djece ispod 13 godina te GLBA za podatke koje prikupljaju financijske institucije. CISA je u SAD-u primarna agencija za kibernetičku sigurnost, ali ona ne nadzire provedbu te stoga ne može ni izricati kazne. FTC nadzire provedbu samo određenih propisa poput GLBA i može pokretati postupke protiv subjekata koji se njih ne pridržavaju. U SAD-u prijava incidenata najčešće je dobrovoljna jer uglavnom nije propisana obveza prijave u nekome roku. Još jednom možemo istaknuti kako EU koristi centraliziran i sveobuhvatan pristup koji dovodi do ujednačenosti obveznih zahtjeva za sve države članice i sektore. U SAD-u fragmentacija propisa i standardi koji se razlikuju na saveznom i državnom nivou mogu rezultirati pravnom nesigurnošću i problemima za poduzeća koja se trebaju uskladiti sa regulativama. Centralizirani model koji je EU odabrala može dovesti do brže reakcije na prijetnje i rizike te bolju usklađenost standarda sigurnosti. Američki pristup omogućava veću fleksibilnost za privatni sektor što olakšava poslovanje poduzeća i dovodi do slobodnijeg tržišta, ali može značiti pravnu nesigurnost i neusklađenost u primjeni propisa.

7. LITERATURA

1. IBM, *Cost of a Data Breach Report*, 30. srpnja 2024., dostupno na: https://www.ibm.com/reports/data-breach (15. rujna 2024.)

2. NICCS, *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases"*, 18. travnja 2024., dostupno na: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c (16. rujna 2024.)

3. CISA, *What is cybersecurity?*, 1. veljače 2021., dostupno na: https://www.cisa.gov/news-events/news/what-cybersecurity (16. rujna 2024.)

4. ISC2, *CISSP Certification Exam Outline Summary* , 15. travnja 2024., dostupno na: https://www.isc2.org/Certifications/cissp/Certification-Exam-Outline (17. rujna 2024.)

5. Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), SL L 151, 7.6.2019.

6. Središnji državni ured za razvoj digitalnog društva, *Kibernetička sigurnost*, https://rdd.gov.hr/kiberneticka-sigurnost/1436 (19. rujna 2024.)

7. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Document 52013JC0001, 7. veljače 2013., dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

8. Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, L 119/1, 4. svibnja 2016.

9. National Cyber Security Centre, *General Data Protection Regulation (GDPR)*, 18. svibnja 2018., dostupno na: https://www.ncsc.gov.uk/information/gdpr (20. rujna 2024.)

10. Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2), SL L 333/80, 27. prosinca 2022.

11. Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, SL L 194/1, 19. srpnja 2016.

12. Koelemij, S., *Securing Process Automation Systems in the European Union: An Overview of the NIS1 Directive and NIS2 Directive*, Industrial Cyber, 25. travnja 2024., dostupno na: https://industrialcyber.co/expert/securing-process-automation-systems-in-the-european-union-an-overview-of-the-nis1-directive-and-nis2-directive/ (25. rujna 2024.)
13. Ured za publikacije Europske unije, *Mala i srednja poduzeća*, 22. veljače 2022., dostupno na: https://eur-lex.europa.eu/HR/legal-content/glossary/small-and-medium-sized-enterprises.html (26. rujna 2024.)
14. Wolf Theiss Rechtsanwälte, *Digital Law: EU's comprehensive cybersecurity framework*, 4. srpnja 2024., dostupno na: https://www.youtube.com/watch?v=-eiGfa4BcAA (26. rujna 2024.)
15. Canonical Ubuntu, *What is the Cyber Resilience Act?*, 3. rujna 2024., dostupno na: https://www.youtube.com/watch?v=ltBtIDvav6c (28. rujna 2024.).
16. Prijedlog uredbe europskog parlamenta i vijeća o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020, COM/2022/454 final, 15. rujna 2022.
17. Europska komisija, *Okvir EU-a za kibersigurnosnu certifikaciju*, 7. veljače 2024., dostupno na: https://digital-strategy.ec.europa.eu/hr/policies/cybersecurity-certification-framework (1. listopada 2024.).
18. Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji), SL L 2024/1689, 12. srpnja 2024.
19. Span, *Na koga se odnosi nova AI Uredba Europske Unije?*, 5. rujna 2024., dostupno na: https://www.span.eu/hr/price/na-koga-se-odnosi-nova-ai-uredba-europske-unije/ (2. listopada 2024.).
20. Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, SL L 257/73, 28. kolovoza 2014.
21. Kosseff, J., *Cybersecurity Law*, treće izdanje, John Wiley & Sons, Inc., Hoboken, 2023.
22. Lord, N., *What is FISMA Compliance? (Definition, Requirements, Penalties, & More)*, Digital Guardian, 6. ožujka 2017., dostupno na: https://www.digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more (5. listopada 2024.).

23. Osaji, P., *Pros and Cons of the Cybersecurity Information Sharing Act of 2015*, The Alliance for citizen engagement, 14. rujna 2023., dostupno na: https://ace-usa.org/blog/research/research-technology/pros-and-cons-of-the-cybersecurity-information-sharing-act-of-2015/(8.10.2024.)
24. Childrens Online privacy Protection Rule, 16 CFR Part 312, Code of Federal Regulations, 17. siječnja 2013., dostupno na: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312 (10. listopada 2024.).
25. Federal Trade Comission, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, 4. rujna 2019., dostupno na: https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law (12. listopada 2024.).
26. Federal Trade Comission, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law*, 27. veljače 2019., dostupno na: https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy (13. listopada 2024.).
27. IBM, *What is the NIST Cybersecurity Framework?*, dostupno na: https://www.ibm.com/topics/nist (15. listopada 2024.).
28. NIST, *CSF 1.1 Uses and Benefits of the Framework*, 6. veljače 2018., dostupno na: https://www.nist.gov/cyberframework/uses-and-benefits-framework (16. listopada 2024.).
29. Solix, *Hipaa*, dostupno na: https://www.solix.com/hr/kb/hipaa/ (18. listopada 2024.).
30. Chin, K., *Top 20 Worst HIPAA Violation Cases in History*, Upguard, (31. listopada 2024.), dostupno na: https://www.upguard.com/blog/worst-hipaa-violation-cases (2. studenog 2024.).
31. Pepper D., Ross S. L., Diamond E., *Gramm-Leach-Bliley Act(GLBA) Privacy & Data Security*, Norton Rose Fulbright US LLP, kolovoz 2024., dostupno na: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/glba---cybersecurity-governance-materials/gramm-leach-bliley-act-glba-privacy-data-security.pdf (20. listopada 2024.).
32. Porter, A., *Navigating GLBA Compliance: A Comprehensive Guide*, BigID, 5. listopada 2023., dostupno na: https://bigid.com/blog/glba-compliance/ (22. listopada 2024.).
33. Civil Code, California Consumer Privacy Act of 2018, [1798.100 - 1798.199.100], 28. lipnja 2018., dostupno na: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140. (23. listopada 2024.).

34. Security Compass, *Enterprise compliance with the California Consumer Privacy Act*, 8. svibnja 2024., dostupno na: https://www.youtube.com/watch?v=2Hrtxu_c0-8 (25. listopada 2024.).
35. CISA, *Continuous Diagnostics and Mitigation (CDM) Program*, https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program (27. listopada 2024.).
36. Denny, W. R., *Cyber Center: Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act*, American Bar Association, 20. lipnja 2016., dostupno na: https://www.americanbar.org/groups/business_law/resources/business-law-today/2016-june/cyber-center-cyber-security-as-an-unfair-practice/ (29. listopada 2024.).
37. ImmuniWeb, FTC Compliance and Cybersecurity *(GLBA, FCRA, SEC)*, 6. rujna 2023., dostupno na: https://www.immuniweb.com/compliance/ftc-cybersecurity-privacy-compliance-glba-fcra-sec/ (30. listopada 2024.).
38. Federal Communications Commission, *Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau*, 7. svibnja 2024., dostupno na: https://www.fcc.gov/cybersecurity-and-communications-reliability-division-public-safety-and-homeland-security-bureau (2. studenog 2024.).
39. Homeland Security, *SECURITY IMPLICATIONS OF 5G TECHNOLOGY: Overview and Recommendations*, dostupno na: https://www.dhs.gov/sites/default/files/publications/privacy_and_security_implications_of_5g_technology_0.pdf (5. studenog 2024.).