Varstvo osebnih podatkov in regulativna harmonizacija enotnega digitalnega trga EU

Zlatko Marinič

POVZETEK

Prispevek obravnava izbrane pravne in tehnološko informacijske vidike varstva osebnih podatkov na področju enotnega digitalnega trga EU in analizira novejše tendence aktualnih pristopov k pravni regulaciji tega zahtevnega področja, ki je tesno povezano s hitrim tehnološkim napredkom. V skladu z GDPR je potreba po upoštevanju varstva osebnih podatkov pri načrtovanju tehnoloških rešitev sedaj zakonska obveznost. To vključuje vgraditev ukrepov v nove tehnologije, da bi bile temeljne pravice posameznikov ob obdelavi njihovih osebnih podatkov ustrezno zaščitene. Nova pravila EU o varstvu podatkov nam nudijo orodja za opolnomočenje družbe in zaščito posameznikov pri uporabi informacijske tehnologije. Vendar se uspeh teh orodij v veliki meri opira na izvajanje načel vgrajenega in privzetega varstva s strani tehnoloških oblikovalcev in upravljavcev podatkov, ter njihovo uveljavljanje s strani regulatorjev. Skupno razumevanje tega kar se na tem področju šteje za najsodobnejše je bistveno in prispeva k zagotavljanju novega in pametnega oblikovanja v procesih, tehnologijah, kot tudi poslovnih modelih, ki bodo zagotovili učinkovito zakonsko zaščito posameznikov in njihovega dostojanstva. Temeljna teza prispevka je, da je GDPR in povezana zakonodaja okrepila varstvo pravic posameznikovih osebnih podatkov, vendar je istočasno informiranje in ozaveščanje o pomenu politik zasebnosti in pravicah posameznika ob uporabi digitalnih storitev nezadovoljivo. Ohranjanje varstva in varnosti podatkov je tudi pomembno politično vprašanje, če želi Evropa izkoristiti vse prednosti enotnega digitalnega trga. Spletne interakcije namreč niso razumljene kot varne. Pomemben in naraščajoč problem pri tem so predvsem negotove navade uporabnikov spleta.

Ključne besede: varstvo osebnih podatkov, GDPR, informacijska zasebnost, obdelava osebnih podatkov, enotni digitalni trg EU.

Personal data protection and regulatory harmonization of the EU digital single market

ABSTRACT

The paper deals with selected legal and technological information aspects of personal data protection in the field of the EU digital single market and analyzes the recent tendencies of current approaches to the legal regulation of this demanding field, which is closely linked to the rapid technological progress. According to the GDPR, the need to consider the protection of personal data when designing technological solutions is now a legal obligation. This involves incorporating measures into new technologies to ensure that the fundamental rights of individuals are properly protected when processing their data. The new EU data protection rules provide us with tools to empower society and protect individuals in the use of information technology. However, the success of these tools relies heavily on the implementation of embedded and default protection principles by technology designers and data controllers, and their enforcement by regulators. A shared understanding of what is considered state-of-the-art in this field is essential and contributes to providing new and smart design in processes, technologies, as well as business models that will ensure effective legal protection of individuals and their dignity. The underlying thesis of the paper is that GDPR and related legislation have strengthened the protection of the rights of individuals‘ data, but at the same time information and awareness of the importance of individual privacy policies and rights when using digital services is unsatisfactory. Maintaining data protection and security is also an important political issue if Europe is to reap the full benefits of the Digital Single Market. Indeed, online interactions are not seen as safe. An important and growing problem is the unsafe habits of web users.

Keywords: personal data protection, GDPR, information privacy, processing of personal data, EU single digital market.

1. Uvod

Razvoj sodobnih informacijskih tehnologij je prinesel veliko pozitivnih pojavov, povzročil pa tudi neverjetno rast zbirk osebnih podatkov o skoraj vseh posameznikih širom sveta. V vsakem trenutku se v virtualnem svetu zbirajo milijarde podatkov, ki se prodajajo kot komercialno blago (t.i. nafta 21 stoletja) ter se zlorabljajo na številne načine. Vsak posameznik je soočen z dejstvom, da razne državne ustanove, privatna podjetja in posamezniki zbirajo, obdelujejo in uporabljajo njegove osebne podatke. Zaradi neverjetne lahkotnosti dostopa in hitrosti, s katero se lahko osebni podatki zbirajo, obdelujejo in zlorabljajo, kot tudi zaradi velikega števila posameznikov, ki so s tem prizadeti, je zaščita osebnih podatkov eno od najpomembnejših vprašanj 21. stoletja. Uporaba umetne inteligence in sofisticirane programske opreme pri zbiranju in obdelavi podatkov samo povečujejo število novih vprašanj, ki se neposredno reflektirajo na vsakega posameznika in njegovo zasebnost.

Države, ki so zavezane varovanju človekovih pravic, morajo zagotoviti, da so prav tisti odgovorni za svoja tveganja in posledice, ki imajo največje koristi od razvoja ter uporabe digitalnih tehnologij in umetne inteligence. Potrebni so učinkoviti in legitimni mehanizmi za obvarovanje in preprečevanje kršitev človekovih pravic in temeljnih svoboščin, kot tudi za spodbujanje socialno-ekonomskega okolja, v katerem so uveljavljene človekove osebnostne pravice in pravna država. Le legitimni mehanizmi zagotavljajo, da lahko ustrezno, trajnostno in skupno izkoristimo številne koristi sodobne digitalne informacijske tehnologije.

Kadar zasebno podjetje (tehnološki velikani) s pomočjo interneta poseduje milijarde podatkov in informacij o posamezniku, med katerimi so lahko tudi politično prepričanje, spolna orientacija, geolokacija, gibanje po digitalnem okolju, premoženjsko stanje, finančne transakcije, izobrazba, zdravstveno stanje, poklicna angažiranost, se mnogi pričnejo spraševati, kako se lahko posameznik ubrani nadzora in kontrole, ki se vrši ves čas nad njegovo zasebnostjo. Danes je pravna regulativa na tem področju vse bolj usmerjena k temu, da zaščiti posameznika pred nezaželeno upo-

rabo osebnih podatkov, oziroma, da zaščiti vse interese posameznika na področju zbiranja, obdelave, shranjevanja, posredovanja in izbrisa osebnih podatkov. Posameznik se lahko zavaruje pred nevarnostmi, ki jih s seboj prinašajo nove digitalne tehnologije, če se mu pravno prizna in zaščiti pravica seznanjenosti z informacijskimi tokovi podatkov, ki se nanašajo na njega, ter, da ima možnost vpliva in nadzora nad osebnimi podatki.

Splošna uredba o varstvu podatkov je ključna za uresničevanje in izvajanje Strategije Evropske komisije za enotni digitalni trg EU, s katero se bo zagotovil prost pretok osebnih podatkov med državami članicami EU in se bo istočasno krepilo zaupanje in varnost potrošnikov, kar je temelj resnično enotnega digitalnega trga. V okviru strategije za enotni digitalni trg bo nova Uredba o prostem pretoku neosebnih podatkov, ki se je začela uporabljati v državah članicah, omogočila shranjevanje in obdelavo podatkov povsod v EU, brez neupravičenih omejitev. Nova uredba o prostem pretoku neosebnih podatkov skupaj s Splošno uredbo o varstvu podatkov, ki se je začela uporabljati 2018, zagotavlja stabilno pravno in poslovno okolje za obdelavo podatkov.[1] Ob pravni ureditvi harmonizacije enotnega digitalnega trga pa se je pričel tudi proces vzpostavljanja sistemov varovanja podatkov s čimer bi se morale vzpostaviti ustrezne ravni varnosti, ki upoštevajo predvsem tveganja obdelav, zlasti nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so bili poslani, shranjeni ali kako drugače obdelani.

2. Pregled evropskega prava varstva osebnih podatkov

Mnogi izzivi (in težave) na relaciji med pravom in tehnologijo, ki se odražajo tudi na področju informacijske zasebnosti, so posledica opustitve vsakršne regulacije interneta, ki je eden pomembnih generatorjev spreminjanja družbenega okolja na nacionalni in globalni ravni. Pri tem je bistveno, da interneta in globalnega digitalnega trga, ki sta pomembna vira velikega podatkovja (Big data) in dostopnosti do podatkov, zaradi njihove narave preprosto ni mogoče regulirati na nacionalni ravni oziroma z nacionalnim pravom, temveč je potrebna intervencija na področju

[1] Komisija objavila smernice o prostem pretoku neosebnih podatkov, Evropska komisija, 2019, e-vir.

mednarodnega oziroma nadnacionalnega prava.

Pri pregledu evropskega prava varstva osebnih podatkov je potrebno prvenstveno predstaviti, kako področje človekovih pravic in temeljnih svoboščin, kamor spada tudi varstvo osebnih podatkov, urejajo predpisi Sveta Evrope in Evropske unije (EU). Z začetkom veljavnosti Lizbonske pogodbe, decembra 2009, je Listina Evropske unije o temeljnih pravicah postala pravno zavezujoča, pravica do varstva osebnih podatkov pa je tako dobila status samostojne temeljne pravice. Za varstvo te temeljne pravice je ključnega pomena boljše razumevanje Konvencije Sveta Evrope št. 108 in instrumentov Evropske unije, ki so utrli pot varstvu podatkov v Evropi, ter sodne prakse Sodišča Evropske unije in Evropskega sodišča za človekove pravice.[2]

Opozoriti je treba, da so reforme in posodobitve pravil o varstvu podatkov v Evropi, ki so bile izvedene v okviru Sveta Evrope (posodobljena konvencija 108, spremenjena s Protokolom CETS št. 223) in EU (sprejetje Splošne uredbe o varstvu podatkov in Direktive 2016/680 / EU) so potekale vzporedno. Regulatorji v obeh pravnih sistemih so si zelo prizadevali, da bi zagotovili skladnost in združljivost obeh pravnih okvirov. Reforme so tako prinesle večjo usklajenost med zakonodajo Sveta Evrope in zakonodajo EU o varstvu podatkov.[3]

2.1. Konvencija sveta evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov

Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (v nadaljnjem besedilu: Konvencija št. 108) je edini pravno zavezujoč večstranski sporazum na področju varstva osebnih podatkov. Cilj Konvencije je varovati pravico do zasebnosti, priznano v 8. členu Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin. Pravica do zasebnosti in pravica do varstva podatkov sta zapisani tudi v 7. členu in 8. členu Listine EU o temeljnih pravicah ter 16. členu PDEU. Konvencija št. 108 od pogodbenic zahteva, da v svojo nacionalno zakonodajo vključijo ukrepe, ki so potrebni za zagotovitev spoštovanja človekovih pravic vseh posameznikov v zvezi z obdelavo osebnih podatkov. Konvencija je bila eden

[2] Priročnik o evropskem pravu varstva osebnih podatkov, 2014, str. 3.
[3] Explanatory Report to the Protocol amending the Convention, 2018, str. 1.

glavnih virov navdiha za razvoj pravnega reda EU na področju varstva podatkov. Glede na 11. uvodno izjavo Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995, o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov je bil eden od ciljev navedene direktive dati vsebino in razširiti načela in pravice, ki jih vsebuje Konvencija št. 108.[4]

V 35 letih od sprejetja Konvencije o varstvu posameznikov v zvezi z avtomatizirano obdelavo osebnih podatkov, je Konvencija služila kot temelj mednarodne zakonodaje o varstvu podatkov v več kot 40 evropskih državah. Močno je tudi vplivala na politiko in zakonodajo izven meja Evrope. Z novimi izzivi človekovih pravic in temeljnih svoboščin, ki se pojavljajo vsak dan, zlasti pravice do zasebnega življenja je postalo jasno, da bi bilo treba Konvencijo posodobiti. Posodobitve so potekale v širšem kontekstu različnih vzporednih reform mednarodnih instrumentov varstva podatkov in ob ustreznem upoštevanju smernic iz leta 1980 (revidiranih leta 2013) o varstvu zasebnosti in čezmejnih pretokov osebnih podatkov Organizacije za gospodarsko sodelovanje in razvoj (OECD), smernic Združenih narodov iz leta 1990 za urejanje računalniških datotek z osebnimi podatki, zakonodajnega okvirja Evropske unije od leta 1995 dalje, znotraj zasebnosti za Azijsko-Pacifiško gospodarsko sodelovanje (2004) in mednarodnih Standardov o varstvu zasebnosti v zvezi z obdelavo osebnih podatkov iz leta 2009 (Madridska resolucija). Odbor ministrov je protokol sprejel 18. maja 2018 in je bil odprt za podpis v Strasbourgu 10. oktobra 2018.[5]

Protokol o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov št. 223, je bil sprejet zaradi novih izzivov s področja varstva zasebnosti, ki so posledica naraščajoče uporabe novih informacijskih in komunikacijskih tehnologij, globalizacije postopkov obdelave in vedno večjega pretoka osebnih podatkov, obenem pa tudi zaradi boljšega vrednotenja konvencije in njenega mehanizma spremljanja. /..../ Glavni cilj Protokola je, da se posameznik lahko seznani s tem, kako drugi obdelujejo njegove osebne podatke, da lahko razume in tudi nadzoruje takšno obdelavo. Protokol s svojimi načeli in vrednotami, ki jih zagovarja, na eni strani varuje posameznika, na

[4] Predlog Sklep sveta o pooblastitvi držav članic ..., 2018, str. 1.
[5] Explanatory Report to the Protocol amending the Convention, 2018, str. 1.

drugi strani pa zagotavlja okvir za mednarodni pretok podatkov. Protokol je popolnoma skladen s pravnim redom EU, še posebej s Splošno uredbo o varstvu podatkov (Uredba 2016/679) o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES,[6] ter Direktivo 2016/680 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov (direktiva o varstvu podatkov za policijo), s čimer se izključi, da za države članice veljajo različne ali celo nasprotujoče si obveznosti po pravu Unije in pravu Sveta Evrope. Sprejetje trdne konvencije, ki temelji na enakem pristopu in enakih načelih kot (novi) pravni red Unije, je zlasti pomembno za mednarodno strategijo Unije na področju varstva podatkov.[7]

Pomembne novosti posodobljene konvencije so naslednje:

Glavni cilj protokola je, da se posameznik lahko seznani s tem, kako drugi obdelujejo njegove osebne podatke, ter da lahko razume in tudi nadzoruje takšno obdelavo. Preambula konvencije je dopolnjena tako, da poudarja pravico do osebne avtonomije in pravico do nadzora nad osebnimi podatki, ki izvira predvsem iz pravice posameznika do zasebnosti in do človekovega dostojanstva. Slednje narekuje, da morajo biti med obdelavo osebnih podatkov vzpostavljena ustrezna varovala, ki preprečujejo, da bi bil posameznik obravnavan zgolj kot objekt.[8]

Predmet in namen konvencije je v skladu s 1. členom jasno poudarjen in sicer zagotoviti vsakemu posamezniku, ki je v pristojnosti ene od držav pogodbenic, ne glede na njegovo državljanstvo ali kraj stalnega prebivališča, da lahko razume in tudi nadzoruje obdelavo svojih osebnih podatkov. S tem se prispeva k spoštovanju pravic in temeljnih svoboščin ter zlasti posameznikove pravice do zasebnosti. Z uporabo tega besedila Konvencija poudarja dejstvo, da lahko obdelava osebnih podatkov omogoči pozitivno uresničevanje drugih temeljnih pravic in svoboščin, kar se lahko olajšuje z zagotavljanjem pravice do varstva podatkov.[9]

[6] Podpis protokola o spremembi Konvencije o varstvu posameznikov, Ministrstvo za pravosodje, 2019, e-vir.
[7] Predlog Sklep sveta o pooblastitvi držav članic, 2018, str. 2-3.
[8] Pobuda za sklenitev Protokola o spremembi Konvencije, 2019, str. 12.
[9] Prav tam, str. 4.

Uvedena je nova določba s katero se jasno določa pravna podlaga za obdelavo in kakovost podatkov. To je ozaveščena, posebna, nedvoumna, prostovoljno izražena privolitev posameznika, na katerega se osebni podatki nanašajo (ali na drugi upravičeni podlagi, določeni v zakonodaji). Katalog občutljivih podatkov je bil razširjen tako, da vključuje genetske in biometrične podatke, kakor tudi podatke, obdelane v povezavi s članstvom v sindikatu ali etničnim poreklom. Ti dve zadnji kategoriji sta dodani obstoječi prepovedi obdelave osebnih podatkov, ki razkrivajo rasni izvor, politična mnenja, verska ali druga prepričanja, zdravstveno stanje, spolno življenje in osebne podatke v zvezi s kaznivimi dejanji, kazenskimi postopki in obsodbami. [10]

Jamstva, ki so opredeljena v konvenciji, se razširjajo na vsakega posameznika, ne glede na njegovo narodnost ali prebivališče. Pri uporabi teh jamstev je vsakršna diskriminacija med državljani EU in državljani tretjih držav nedopustna. Člani, ki razlikujejo varstvo osebnih podatkov na lastne in tuje državljane z zakonitim prebivališčem, so popolnoma v neskladju s protokolom.[11] Upoštevaje pomen pravice do varstva osebnih podatkov v družbi, spremenjena preambula konvencije podkrepi načelo, da se morajo interesi, pravice in temeljne svoboščine posameznikov medsebojno uskladiti, kjer je to potrebno. Da bi se lahko vzdrževalo ravnovesje med različnimi interesi, pravicami in temeljnimi svoboščinami, protokol določa nekatere pogoje in omejitve glede obdelave informacij in varstva osebnih podatkov. Tako je npr. pravico do varstva podatkov treba obravnavati v povezavi s pravico do »svobode izražanja«, kot je določena v 10. členu Evropske konvencije o človekovih pravicah, ki vključuje pravico do lastnega mnenja in do sprejemanja ter širjenja informacij. Protokol potrjuje, da se uresničevanje pravice do varstva osebnih podatkov, ki ni absolutna, nikakor ne sme uporabljati kot splošno sredstvo za preprečevanje javnega dostopa do uradnih dokumentov (informacije javnega značaja).[12]

Prav tako je pomemben prvi odstavek 14. člena konvencije, ki omogoča, da nadzorni organi držav pogodbenic zaustavijo prenose osebnih podatkov v tretje države ali mednarodne organizacije ali celo države Sveta Evrope ali Evropske unije, če obstaja de-

[10] The modernised Convention 108: novelties in a nutshell, 2019, str. 2.
[11] Pobuda za sklenitev Protokola o spremembi Konvencije, 2019, str. 4.
[12] Prav tam, str. 5.

jansko in resno tveganje (kumulativna pogoja) obhoda določb o varstvu osebnih podatkov iz konvencije in protokola.[13]

2.2. Uredba o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov)

V preteklosti je imela EU ključno vlogo pri spodbujanju razvoja in uvedbe nacionalnega prava o varstvu podatkov v številnih pravnih sistemih, kjer taka zakonodaja še ni bila vzpostavljena. Direktiva EU iz leta 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takšnih podatkov je bila v tem pogledu bistven instrument, saj ta zagotavlja učinkovito varstvo temeljne pravice do varstva podatkov. Vendar so obstajale razlike v načinu in metodah kako je vsaka država članica implementirala Direktivo v nacionalno zakonodajo. Te različne nedoslednosti so povzročale nepotrebno kompleksnost, pravno negotovost in upravna bremena, kar je vplivalo na zaupanje posameznikov in konkurenčnost gospodarstva EU. Ta pravila so morala biti posodobljena, saj so bila uvedena v času ko številne današnje spletne storitve, tehnologije in izzivi kibernetske varnosti, ki se nanašajo na varstvo osebnih podatkov, še niso obstajali.

Tako je Uredba 2016/679 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov - v nadaljevanju GDPR), okrepila varstvo posameznikovih pravic do varstva osebnih podatkov in je namenjena kot novi vseevropski instrument varstva podatkov in tudi posledično informacijske zasebnosti v digitalnem okolju.[14] Uredba še naprej uporablja pristop in načela iz Direktive o varstvu podatkov (95/46/ES), vendar na podlagi 20-letnih izkušenj z izvajanjem zakonodaje EU o varstvu podatkov in ustrezne sodne prakse pojasnjuje in posodablja predpise o varstvu podatkov.[15]

Uredba GDPR uvaja številne nove elemente, načela in predvsem pravice, ki močno krepijo varstvo pravic posameznikov in odpirajo priložnosti za podjetja in družbe, zlasti:

[13] Prav tam, str. 6.
[14] Dogovor o reformi varstva podatkov v EU, Evropska komisija, 2015, e-vir.
[15] Navodila Komisije o neposredni uporabi splošne uredbe o varstvu podatkov, 2018, str. 2.

Harmoniziran pravni okvir, ki bo omogočal enotno uporabo pravil v korist enotnega digitalnega trga EU. To pomeni en sam sklop pravil za državljane in podjetja. To bo odpravilo današnje stanje, ki je nastalo zaradi tega, ker so države članice EU različno prenesle pravila Direktive. Za zagotovitev enotne in dosledne uporabe v vseh državah članicah je uveden mehanizem »vse na enem mestu« ter enaki konkurenčni pogoji za vsa podjetja, ki delujejo na trgu EU. Uredba določa, da morajo družbe s sedežem zunaj EU, spoštovati ista pravila kot podjetja s sedežem v EU, če ponujajo blago in storitve v zvezi z osebnimi podatki ali spremljajo vedenje posameznikov v Uniji. Podjetja, ki poslujejo zunaj EU in so dejavna na enotnem trgu EU, morajo v nekaterih okoliščinah imenovati zastopnika v EU, na katerega se lahko poleg podjetja, ki ima sedež v tujini, ali namesto tega podjetja, obrnejo državljani in organi.[16]

Načeli vgrajenega (Privacy by design) in privzetega varstva (Privacy by default) podatkov proizvajata spodbude za inovativna izboljšanja z namenom obravnave vprašanj varstva podatkov od samega začetka. Zaščita podatkov po načelu vgrajenega varstva je namenjena vzpostavitvi varstva podatkov in zasebnosti že v razvojni stopnji oblikovanja postopkov obdelave, kreiranja, integracije informacijskih sistemov z namenom, da se zagotovi skladnost načel varstva podatkov. Organizacije morajo upoštevati zaščito pravic posameznikov pred in med postopki obdelave z izvajanjem ustreznih tehničnih in organizacijskih ukrepov za zagotovitev varstva podatkov. Načelo privzetega varstva pomeni, da je treba ob izdaji izdelka ali storitve v uporabo že imeti aktivirane najstrožje nastavitve zasebnosti brez ročnega vnosa s strani končnega uporabnika. Ob tem je treba vse osebne podatke, ki jih zagotovi uporabnik za omogočanje optimalne uporabe izdelka hraniti le toliko časa, kolikor je nujno potrebno za zagotovitev izdelka ali storitve. Če se razkrije več informacij, kot je potrebno za zagotavljanje storitve, potem je bila kršena »privzeta zasebnost«. Zaščita podatkov je sedaj sestavni del tehnološkega razvoja in tudi način, kako se izdelek ali storitev dobavlja končnemu uporabniku.[17]

Večje pravice posameznikov z uvajanjem nove zahteve glede preglednosti, okrepljene pravice do informacij, dostopa in do izbrisa (pravica do pozabe), molk ali nedejavnost se ne bosta več

[16] Prav tam, str. 2.
[17] Prav tam, str. 1.

štela kot veljavna privolitev, kot znak soglasja bo potrebno jasno pritrdilno dejanje. Omogočen bo večji nadzor nad osebnimi podatki za posameznike, saj uredba določa novo pravico do prenosljivosti podatkov, ki bo državljanom omogočila, da od podjetja ali organizacije zahtevajo, da jim osebne podatke, ki so jih posredovali na podlagi privolitve ali pogodbe, vrnejo nazaj. Omogočila bo tudi, da se taki osebni podatki posredujejo neposredno drugemu podjetju ali organizaciji, če je to tehnično izvedljivo. Ker uredba omogoča neposreden prenos osebnih podatkov od enega do drugega podjetja ali organizacije, bo ta pravica podpirala tudi prost pretok osebnih podatkov v EU, s čimer bi preprečili vezanost osebnih podatkov, ter spodbujala konkurenco med podjetji. Ker bo prehod med različnimi ponudniki storitev za državljane lažji, bo uredba spodbujala tudi razvoj novih storitev v okviru strategije za enotni digitalni trg.[18]

Večje varstvo pred kršitvami varnosti podatkov. Uredba določa celovit sklop pravil o kršitvah varnosti osebnih podatkov. Jasno opredeljuje kaj je »kršitev varnosti osebnih podatkov« in določa obveznost uradnega obveščanja nadzornega organa najpozneje v 72 urah, če je verjetno, da bi kršitev varnosti pomenila tveganje za pravice in svoboščine posameznika. V nekaterih okoliščinah uredba določa obveznost obveščanja osebe, ki jo zadeva kršitev. To močno krepi varstvo glede na dosedanje stanje v EU, ko so bili le ponudniki elektronskih komunikacijskih storitev, izvajalci osnovnih storitev in ponudniki digitalnih storitev dolžni obveščati o kršitvah varstva podatkov v skladu z direktivo o zasebnosti in elektronskih komunikacijah (direktiva o e-Zasebnosti) in direktivo o varnosti omrežij in informacijskih sistemov (direktiva NIS).[19]

Omogočeno je več prožnosti za upravljavce in obdelovalce podatkov, ki obdelujejo osebne podatke, zaradi nedvoumne določbe o pristojnosti (načelo odgovornosti). Uredba odpravlja sistem obveščanja in ga nadomešča z načelom odgovornosti. To načelo se izvaja prek obsežnih obveznosti, ki so odvisne od tveganja (npr. prisotnost uradne osebe za varstvo podatkov ali obveznost izvedbe ocene učinka v zvezi z varstvom podatkov).[20]

Uvaja se novo orodje, ki bo pomagalo oceniti tveganje pred začetkom obdelave: ocena učinka v zvezi z varstvom osebnih po-

[18] Prav tam, str. 2 -3.
[19] Prav tam, str. 4.
[20] Prav tam, str. 2.

datkov. Takšna ocena je obvezna, kadar bi obdelava lahko povzročila veliko tveganje za pravice in svoboščine posameznikov. Uredba izrecno določa tri primere, ki bi lahko povzročili omenjeno tveganje: ko podjetje sistematično in obsežno ocenjuje osebne vidike posameznika (vključno z oblikovanjem profilov), kadar v velikem obsegu obdeluje občutljive podatke ali kadar v velikem obsegu sistematično spremlja javne površine. Nacionalni organi za varstvo podatkov bodo morali objaviti sezname primerov, pri katerih je potrebna ocena učinka o varstvu podatkov.[21]

Z GDPR se vzpostavlja sodoben sistem upravljanja za zagotovitev, da se pravila izvajajo bolj dosledno in odločno. To vključuje usklajena pooblastila organov za varstvo podatkov, vključno z možnostjo izrekanja visokih glob, in nove mehanizme za sodelovanje navedenih organov v mreži EDPB. Evropski odbor za varstvo podatkov (EDPB) je neodvisno evropsko telo, ki prispeva k dosledni uporabi pravil o varstvu podatkov po vsej Evropski uniji in spodbuja sodelovanje med organi EU za varstvo podatkov. EDPB sestavljajo predstavniki nacionalnih organov za varstvo podatkov in Evropski nadzornik za varstvo podatkov (EDPS).[22]

Varstvo osebnih podatkov, ki ga zagotavlja ta uredba, skupaj s podatki potuje tudi zunaj EU, kar zagotavlja visoko raven varstva. Čeprav struktura pravil o mednarodnih prenosih v uredbi ostaja v bistvu enaka tisti iz direktive iz leta 1995, reforma pojasnjuje in poenostavlja uporabo teh pravil ter uvaja nova orodja za prenos. Kar zadeva sklepe o ustreznosti, uredba uvaja natančen in podroben seznam elementov, ki jih mora Komisija upoštevati pri presojanju, ali tuji sistem ustrezno varuje osebne podatke. Uredba tudi formalizira in razširja področje uporabe na več alternativnih instrumentih za prenos, kot so standardne pogodbene klavzule in zavezujoča poslovna pravila.[23]

Z željo zagotoviti, da bodo posamezniki ostali zaščiteni v mednarodnem podatkovnem gospodarstvu so zakonodajalci EU ustvarili dva zaščitna ukrepa:

1) *lex loci solutionis* (zakon kraja, kjer se izvajajo dejavnosti) zahteva, po kateri mora obdelovalec podatkov upoštevati GDPR kadarkoli se obdelujejo podatki evropskih strank.[24]

[21] Uredba 2016/679, 35. člen.
[22] Prav tam, 65. člen.
[23] Navodila Komisije o neposredni uporabi splošne uredbe o varstvu podatkov, 2018, str. 2-4.
[24] Uredba 2016/679, 3. člen.

2) Da bi zagotovili dodatno zaščito podatkov, ki se prenašajo v tujino, so načela GDPR vključena v mednarodne trgovinske sporazume. Najpomembnejši primeri slednjega so zaščita informacijske zasebnosti med EU in ZDA (EU-US Privacy Shield) [25] ali ustrezni deli nedavno podpisanega sporazuma med EU in Japonsko o gospodarskem partnerstvu (Jefta). Vsi ti sporazumi so neposredno podvrženi GDPR.

Kljub temu, da sta oba mehanizma zasnovana predvsem za zaščito evropskih kupcev, večina svetovno delujočih ponudnikov digitalnih storitev trdi, da se bodo globalno držali standardov uredbe in vsem svojim strankam zagotovili enako raven varstva podatkov. Zato se dozdeva, da je doseg določb uredbe presegel okvire evropskega digitalnega trga in njegovih uporabnikov, saj se z določitvijo standardov za največji potrošniški trg na svetu posredno pritiska na podjetja, ki delujejo po vsem svetu, da sprejmejo svoja načela za vse svoje kupce in uporabnike.[26]

GDPR predvsem ureja obdelavo osebnih podatkov in je bistveni del harmoniziranega okvira EU za varstvo podatkov, ter pomaga razumeti medsebojni vpliv med regulatornimi okvirji sprejetimi na področju varovanja osebnih podatkov, zlasti na relacijah med:

– Uredbo (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji;

– Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES;

– Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (Policijska direktiva);

[25] Okvir za urejanje čezatlantske izmenjave osebnih podatkov v komercialne namene med Evropsko unijo in ZDA. Eden od njegovih namenov je omogočiti ameriškim podjetjem, da lažje prejemajo osebne podatke od subjektov EU v skladu z zakonodajo EU o informacijski zasebnosti, ki je namenjena zaščiti državljanov Evropske unije. EU-US Privacy Shield je nadomestek mednarodnih načel Safe Harbor Privacy, ki jih je Sodišče EU oktobra 2015 razglasilo za neveljavne.

[26] What is GDPR? Everything you need to know, ITPro, 2019, e-vir.

– Direktivo 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah, ali e-Zasebnost), trenutno je v reviziji kot uredba.

3. Enotni digitalni trg EU

Enotni digitalni trg označuje strategijo Evropske komisije za najboljši možni dostop do spletnega sveta za posameznike in podjetja. Evropska komisija si prizadeva za odpravo tistih spletnih ovir, ki ljudem preprečujejo, da bi uživali popoln dostop do blaga in storitev, ki jih ponujajo podjetja v EU. Prenehanje geoblokiranja, neupravičenih čezmejnih ovir, olajšanje cenejših čezmejnih paketnih pošiljk, zaščita pravic spletnih strank in spodbujanje čezmejnega dostopa do spletnih vsebin so nekateri načini za uresničevanje strategije enotnega digitalnega trga. Strategija enotnega digitalnega trga temelji na treh stebrih.

3.1. PRvi steber: dostop

Namen prvega stebra je predvsem močnejši dostop za potrošnike in podjetja do digitalnega blaga in enotnih storitev po vsej Evropi. E-trgovina je eden od temeljev strategije enotnega digitalnega trga, EU pa je sprejela več ukrepov na tem področju, da bi evropskim potrošnikom olajšala in zagotovila varnejšo spletno nakupovanje po celotni EU. Uresničitev vsega potenciala e-trgovanja v EU omogočajo:[27]

- Direktiva o nekaterih vidikih pogodb o dobavi digitalne vsebine in digitalnih storitev (Direktiva (EU) 2019/770 - DCD), ki je že v veljavi in spada na področje zasebnega prava. Namenjena je urejanju pogodbenih pravic in dolžnosti podjetij, ki dobavljajo digitalno vsebino in zagotavljajo digitalne storitve na eni strani, ter potrošnikov takšnih digitalnih vsebin in digitalnih storitev na drugi strani. Direktiva je zasnovana tako, da zagotavlja čim večje usklajevanje ključnih vidikov pogodbenega razmerja, vključno s skladnostjo digitalnih vsebin in storitev, odpovedjo pogodbe s strani potrošnika in odgovornostjo dobavitelja za škodo, povzročeno potrošnikovim digitalnim okoljem. Pomembna novost

[27] The European Digital Single Market, Evropska komisija, 2017, e-vir.

direktive je, da prvič v zakonodaji EU, zajema pogodbena razmerja, pri katerih se digitalne vsebine ali storitve dobavljajo ne samo ob upoštevanju denarne cene (vrednosti), ampak se lahko izvajajo tudi v zameno za zagotavljanje osebnih podatkov ali drugih podatkov s strani potrošnika. Naveden razlog za vključitev pogodb, v katerih potrošniki dajejo na razpolago osebne podatke, namesto da bi plačali denarno ceno, je potreba, da bi se izognili diskriminaciji med različnimi poslovnimi modeli. Direktiva se uporabljala za vsako pogodbo, kjer dobavitelj potrošniku dobavi digitalno vsebino ali se zaveže, da bo to storil v zameno za ceno, pa tudi, ko potrošnik aktivno zagotavlja nasprotne učinke v obliki osebnih podatkov oz. kateri koli drugih podatkov. Vendar pa je že sama zamisel, da bi osebni podatki postali predmet transakcije, sprožila ugovore, vključno s tistimi evropskega nadzornika za varstvo podatkov, na podlagi pomislekov v zvezi s temeljnimi pravicami potrošnikov. Zdaj se zakonodajalci soočajo s kočljivo nalogo uskladitve pristopa k temeljnim pravicam, z zahtevami gospodarske resničnosti enotnega digitalnega trga, vključno s potrebo po pravnem varstvu potrošnikov, ki zagotavljajo svoje osebne podatke, da bi dostopali do digitalnih vsebin ali storitev. Ob tem morajo končna besedila obravnavati zapletena vprašanja medsebojnega razmerja med pravili o digitalni pogodbi na eni strani in pravili o varstvu osebnih podatkov na drugi strani, da se zagotovi pregledno, skladno in uporabno pravno okolje za podjetja in potrošnike v enotnem digitalnem trgu;[28]

- revidirana direktiva o plačilnih storitvah (Direktiva (EU) 2015/2366), ki je že v veljavi;

- nova pravila o storitvah čezmejne dostave paketov (Uredba (EU) 2018/644) in so že v veljavi;

- nova pravila za ustavitev neupravičenega geoblokiranja (Uredba (EU) 2018/302), ki je že v veljavi. Uredba obravnava neupravičeno diskriminacijo kupcev pri spletni prodaji na podlagi njihovega državljanstva, prebivališča ali sedeža podjetja na notranjem trgu. Trgovcem ne nalaga obveznosti, da dovolijo dostop do svojih vsebin, jih prodajajo ali dobavljajo po vsej EU, temveč jim prepoveduje diskriminacijo kupcev na podlagi njihovega državljanstva, prebivališča ali sedeža podjetja, če trgovec že dostavlja blago v njihovo državo članico[29];

[28] Direktiva (EU) 2019/770, uvodne določbe 8-11.
[29] Evropejci in Evropejke po podatkih raziskave dobro poznajo pravila, Evropska komisija, 2019, e-vir.

- spremenjena pravila o varstvu potrošnikov, ki bodo začela veljati leta 2020;
- nova pravila o DDV za spletno prodajo blaga in storitev, ki bodo začela veljati leta 2021.

3.2. Drugi steber: okolje

Namen drugega stebra je ustvarjanje ustreznih pogojev in enakih konkurenčnih pogojev za razcvet digitalnih omrežij in inovativnih storitev, katere zahtevajo ustrezno okolje za uspeh. Komisija si je zadala nalogo, da ustvari pogoje za napredne infrastrukture, ustrezne regulativne pogoje za naložbe v digitalna omrežja in enake konkurenčne pogoje za akterje na trgu. V okviru tega stebra je Komisija predlagala posodobitve in revizije na več področjih: prenovo pravil telekomunikacij, pregled okvirja za avdiovizualne medije, analizo vloge spletnih platform, krepitev zaupanja in varnosti v digitalnih storitvah in pri ravnanju z osebnimi podatki, ter partnerstvo z industrijo na področju kibernetskih varnosti.[30]

3.2.1. Prenova pravil telekomunikacij

Prenova pravil telekomunikacij se nanaša na vrsto ukrepov za zagotovitev, da bodo imeli vsi v EU najboljšo možno internetno povezavo za sodelovanje v digitalni družbi in gospodarstvu. Ti predlogi spodbujajo naložbe v zelo zmogljiva omrežja in pospešujejo uvajanje nove brezžične tehnologije 5G in brezplačne dostopne točk Wi-Fi-ja v javnih prostorih. Tako imenovani povezovalni paket vključuje: Kodeks evropskih elektronskih komunikacij (European Electronic Communications Code), ki je enoten pravilnik za komunikacijske storitve, revidirana Uredba BEREC (Uredba (EU) 2018/1971), skupne širokopasovne cilje za sodobno Gigabitno družbo, načrt za spodbujanje evropskega vodstva na področju pete generacije (5G) brezžične tehnologije, ter načrt podpore javnim organom, da svojim državljanom omogočijo in spodbudijo razvoj brezplačnega dostopa do brezžičnega interneta predvsem v lokalnih, manj razvitih okoljih.[31]

[30] Right environment for digital networks and services, European Commission, 2019, e-vir.
[31] Prav tam.

3.2.2. Pregled okvira za avdiovizualne medije

Pravila o avdiovizualnih medijih v Evropi morajo biti primerna za 21. stoletje. Pregled se bo osredotočil na vlogo različnih akterjev na trgu pri spodbujanju evropskih avtorskih del. Komisija je sprejela revidirano Direktivo 2010/13/EU o avdiovizualnih medijskih storitvah (Direktiva AVMSD), ki omogoča pravičnejšo zakonodajo za celoten avdiovizualni sektor, da bi bili spletni mediji glede regulacije izenačeni s tradicionalnimi. V praksi to pomeni boljšo zaščito Evropejcev pred škodljivimi vsebinami ter okrepljeno zaščito na televiziji in videu na zahtevo proti spodbujanju nasilja ali sovraštva, javnih provokacij, možnosti terorističnih dejanj. Platforme za izmenjavo videov morajo prav tako sprejeti ustrezne ukrepe za zaščito ljudi pred spodbujanjem nasilja, sovraštva in pred vsebinami, ki predstavljajo kazniva dejanja.[32]

3.2.3. Analiza vloge spletnih platform

Evropska komisija s svojimi predlogi želi spodbuditi okolje, v katerem se bodo razvili sodobni ekosistemi spletnih platform, ki igrajo vedno bolj osrednjo vlogo na trgu. To vključuje zagotovitev, da platforme pošteno obravnavajo svoje uporabnike in sprejemajo aktivne ukrepe za omejitev širjenja nezakonitih spletnih vsebin. Komisija bo ocenila njihovo vlogo zlasti glede vprašanj preglednosti, uporabe informacij (vključno s pravico do pozabe), odnosov med platformami in dobavitelji, ter kako se spopasti z nezakonitimi vsebinami na internetu.

3.2.4. Krepitev zaupanja in varnosti v digitalnih storitvah pri ravnanju z osebnimi podatki

Komisija je 10. januarja 2017 sprejela osnutek Uredbe o zasebnosti in elektronskih komunikacijah (e-Zasebnost) in predlagala razveljavitev ter nadomestitev direktive z namenom uskladitve zakonodaje o zasebnosti in elektronskih komunikacijah z novimi pravili EU o varstvu osebnih podatkov. To bi pomenilo, da se državljani EU lahko na zakonodajo EU sklicujejo neposredno, kar pomeni, da države članice EU nimajo več vloge pri razlagi njene vloge v skladu s svojim nacionalnim pravnim redom. Predlog uredbe o visoki ravni pravil o zasebnosti za vse elektronske ko-

[32] Revision of the Audiovisual Media Services Directive, European Commission, 2019, e-vir.

munikacije vključuje pravila o zasebnosti, ki bodo v prihodnosti veljala tudi za nove igralce, ki zagotavljajo elektronske komunikacijske storitve, kot so WhatsApp, Facebook, Messenger, Gmail, Netflix in Skype. To bo zagotovilo, da bodo te priljubljene storitve zagotavljale enako raven zaupnosti komunikacij kot tradicionalni telekomunikacijski operaterji. Vsi ljudje in podjetja v EU bodo uživali enako raven zaščite svojih elektronskih komunikacij s to neposredno veljavno uredbo. Podjetja bodo prav tako imela koristi od enotnega sklopa pravil v EU.[33]

Predlagana uredba bi brskalnikom in drugi programski opremi prav tako zagotovila možnost aktivnega preprečevanja zbiranja osebnih podatkov preko piškotkov in drugih komunikacijskih podatkov, ter uporabnike prisilila, da se med nastavitvijo odločijo kakšne bodo njihove želje v zvezi z zasebnostjo. To ne velja samo za spletne brskalnike, ampak za vse aplikacije in naprave, ki se lahko povežejo z internetom. Zasebnost mora biti zagotovljena za komunikacijske vsebine in metapodatke, npr. čas, dolžina klica in lokacija. Metapodatki imajo visoko komponento zasebnosti in jih je treba anonimizirati ali izbrisati, če uporabniki ne podajo soglasja. Izjema so podatki, potrebni za obračunavanje storitve in še to le najkrajši možni čas.[34]

Zagotavljanje piškotkov, ki je povzročilo preobremenjenost zahtev za soglasje uporabnikov interneta, bo tako racionalizirano. Nova pravila bodo uporabniku prijaznejša, saj bodo nastavitve brskalnika omogočile enostaven način za sprejem ali zavrnitev sledilnih piškotkov in drugih identifikatorjev. Predlog tudi pojasnjuje, da ni potrebno soglasje za vsiljive piškotke, ki ne ščitijo zasebnosti in samo izboljšujejo internetno izkušnjo (npr. spomin za zgodovino nakupovalne košarice) ali piškotke, ki jih spletno mesto uporablja za preštevanje števila obiskovalcev.[35]

Predlog v e-Zasebnosti vsebuje tudi ureditev zaščite pred neželeno pošto in prepoveduje neželene elektronske komunikacije po elektronski pošti, SMS-ih in avtomatiziranih klicnih napravah. Glede na nacionalno zakonodajo bodo ljudje privzeto zaščiteni, lahko pa bodo uporabljali seznam ne-kliči v primeru tržnih telefonskih klicev. Tržni klicatelji bodo morali prikazati svojo telefonsko številko ali uporabiti posebno predpono številki, ki bo ozna-

[33] Proposal for an ePrivacy Regulation, European Commission, 2019, e-vir.
[34] Prav tam, str. 2.
[35] Prav tam, str. 2.

čevala tržni klic. Za izvrševanje pravil o zaupnosti v uredbi bodo pristojni organi za varstvo podatkov, ki so že pristojni za pravila v skladu z GDPR.[36]

3.2.5. Partnerstvo z industrijo na področju kibernetski varnosti

Po raziskavah naj bi se zaradi kibernetske kriminalitete izgubilo več milijard evrov na leto, kar povzroča vse večjo potrebo po sposobnosti takojšnega odzivanja na področju kazenskega pregona. Z naraščajočo uporabo interneta, s širjenjem različnih vrst internetnih naprav in vse večjo količino osebnih podatkov, ki se prenašajo preko spleta se bo vprašanje kibernetske kriminalitete verjetno eksponentno povečalo, če pristojni organi ne sprejmejo usklajenih ukrepov za njeno učinkovito izkoreninjenje. Kot odgovor na to naraščajočo težavo je Evropska komisija zasnovala usklajeno politiko v tesnem sodelovanju z državami članicami Evropske unije in drugimi institucijami EU. Zakonodajni ukrepi EU, ki prispevajo k boju proti kibernetski kriminaliteti obravnavajo vprašanja, kot so napadi na informacijske sisteme, spletna zasebnost, spletno žaljivo gradivo in otroška pornografija, ter spletne goljufije in ponarejanje.[37]

V okviru strategije EU za kibernetsko varnost je Evropska komisija predlagala direktivo EU o varnosti omrežij in informacij. Direktiva o NIS, sprejeta 6. julija 2016 predstavlja prva pravila o kibernetski varnosti na ravni celotne EU. Cilj direktive je doseči visoko skupno raven varnosti omrežij in informacijskih sistemov v EU z istočasnimi izboljšanimi zmogljivostmi kibernetske varnosti na nacionalni ravni, povečanim sodelovanjem na ravni EU in obvladovanjem tveganj, kot tudi obveznostmi poročanja o nezgodah za operaterje osnovnih storitev in ponudnikih digitalnih storitev. Direktiva NIS je pomemben mejnik pri krepitvi odpornosti na kibernetsko varnost na enotni evropski ravni.[38]

Direktiva NIS je razdeljena na tri področne dele:

– nacionalne zmogljivosti: države članice EU morajo imeti določene zmogljivosti nacionalne kibernetske varnosti v vsaki posa-

[36] Prav tam, str. 3.
[37] Kibernetska kriminaliteta, 2012, str. 2-3.
[38] Direktiva (EU) 2016/1148, uvodna izjava 29-33.

mezni državi EU, npr. imeti morajo nacionalni CSIRT (Computer Security Incident Response Team – pri nas CERT.SI), in izvajati kibernetske vaje ipd.;[39]

– čezmejno sodelovanje: čezmejno sodelovanje med državami EU, npr. delujočo mrežo EU CSIRT, strateško skupino za sodelovanje NIS itd;[40]

– nacionalni nadzor kritičnih sektorjev: države članice EU morajo nadzorovati kibernetsko varnost kritičnih tržnih operaterjev v svoji državi, predhodni nadzor v kritičnih sektorjih kot so energetika, promet, voda, zdravstvo in finančni sektor, ter naknadni nadzor nad kritičnimi sektorji ponudnikov digitalnih storitev (internetne izmenjalne točke, sistemi domen itd.).[41]

Direktiva NIS daje državam EU določeno stopnjo prilagodljivosti za upoštevanje nacionalnih okoliščin, na primer za ponovno uporabo obstoječih organizacijskih struktur ali za uskladitev z obstoječo nacionalno zakonodajo. Zaradi navedenega je Komisija napovedala tudi začetek pogodbenega javno-zasebnega partnerstva o kibernetski varnosti. Cilj partnerstva je spodbujanje sodelovanja v zgodnjih fazah raziskovalnega in inovacijskega procesa ter oblikovanje rešitev za kibernetsko varnost za različne sektorje kot so energetika, zdravje, promet in finance.[42]

3.3. Tretji steber: gospodarstvo in družba

Digitalna preobrazba podjetij in družbe EU predstavlja velik potencial rasti za Evropo. Evropska industrija lahko nadgradi svoje prednosti na naprednih digitalnih tehnologijah ter obdrži svojo močno prisotnost v tradicionalnih sektorjih samo tako, da izkoristi številne priložnosti, ki jih ponujajo tehnologije kot so internet stvari, veliko podatkovje, napredna proizvodnja, robotika, 3D tiskanje, blockchain tehnologije in umetna inteligenca. To bo evropski industriji omogočilo zavzeti delež na nastajajočih svetovnih trgih za izdelke in storitve prihodnosti. Za digitalno preobrazbo je predvsem značilno zlivanje naprednih tehnologij in povezovanje fizičnih in digitalnih sistemov, prevlada inovativnih poslovnih modelov in novih procesov, ter ustvarjanje »pametnih izdelkov« in storitev.

[39] Prav tam, 1. člen.
[40] Prav tam, 8. člen.
[41] Prav tam, uvodna izjava 28.
[42] Contractual arrangement setting up a public-private partnership, 2016, str. 8.

Trenutno podjetja v EU ne izkoriščajo v celoti prednosti teh naprednih tehnologij ali inovativnih poslovnih modelov, ki jih ponuja sodelovalno gospodarstvo. Stanje digitalizacije industrije se razlikuje med sektorji, zlasti med visokotehnološkimi in bolj tradicionalnimi območji, pa tudi med državami in regijami EU. Prav tako obstajajo precejšne razlike med velikimi podjetji in malimi ter srednjimi podjetji (MSP).

Uvajanje vrhunskega evropskega računalništva v oblaku za znanstvenike, javni sektor in podjetja, kot je napovedano v sporočilu o evropski pobudi za računalništvo v oblaku[43], bo izboljšalo zmožnost podjetij, zlasti MSP in netehnološke industrije, da so inovativna in ustvarjajo digitalizirane proizvode z višjo vrednostjo. Do leta 2020 bo evropski oblak za odprto znanost ponudil virtualno okolje, v katerem se lahko shranjujejo, izmenjujejo in ponovno uporabljajo podatki čezmejno in iz različnih panog. Zagotovil bo tudi povezave z drugimi pobudami, kot je storitev dostopanja do podatkov in informacij programa Copernicus za neposredno opazovanje Zemlje.[44]

Visokozmogljivo računalništvo je ključno za digitalizacijo industrije in podatkovno gospodarstvo. Omogoča prehod na proizvode in storitve z višjo vrednostjo. Določeni evropski sektorji kot so proizvodnja, energetika, naftni in plinski sektor, prevozništvo, so uspešno uvedli aplikacije, ki jih podpira visokozmogljivo računalništvo. Vendar Evropa na splošno drsi z najvišjih mest lestvic dejavnosti visokozmogljivega računalništva, saj so jo prehitele Kitajska, ZDA in Japonska. Brez vrhunskih zmogljivosti visokozmogljivega računalništva Evropa ne bo izpolnila cilja, da postane dinamično podatkovno gospodarstvo.[45]

Evropa ne sodeluje v tekmi visoko zmogljivega računalništva na ravni svojega gospodarskega potenciala in potenciala znanja, zaostaja za drugimi regijami, saj ne vlaga v svoj ekosistem visoko zmogljivega računalništva in ne izkorišča koristi intelektualne lastnine na tem področju. Na strani ponudbe industrija EU zagotavlja približno 5 % virov visoko zmogljivega računalništva na svetu, medtem ko jih porabi tretjino. Z vedno večjo odvisnostjo od drugih regij, kar zadeva pomembno tehnologijo, se Evropa izpostavlja tveganju

[43] Več v European Cloud Initiative, v: Communication from the Commission to The European Parliament ..., 2016.
[44] Mnenje Evropskega ekonomsko-socialnega odbora ..., 2017, str. 21.
[45] Prav tam, str. 22.

tehnološke blokade, zamude ali prikrajšanosti za strateško strokovno znanje. Evropa zaostaja tudi pri goli skupni računalniški moči, le desetina vodilnih infrastruktur visoko zmogljivega računalništva se nahaja v EU, nemški Höchstleistungrechenzentrum Stuttgart je na osmem mestu. ZDA jih imajo pet, Kitajska pa ima že od leta 2013 najhitrejši super računalnik na svetu.[46]

Zaradi navedenega je bilo ustanovljeno Skupno podjetje za evropsko visokozmogljivostno računalništvo (EuroHPC), ki je izbralo osem lokacij za centre za superračunalništvo v osmih državah članicah, s čimer bo Evropa postala vodilna svetovna regija na področju superračunalništva. Te lokacije bodo v Sofiji (Bolgarija), Ostravi (Češka), Kaajaniju (Finska), Bologni (Italija), Bissnu (Luksemburg), Minhu (Portugalska), Mariboru (Slovenija) in Barceloni (Španija). Centri bodo podpirali razvoj pomembnih aplikacij na področjih kot so personalizirana medicina, načrtovanje novih zdravil in materialov, bioinženiring, napovedovanje vremena in podnebne spremembe. Superračunalniki bodo predvidoma začeli delovati v drugi polovici leta 2020, uporabljali pa jih bodo lahko evropski uporabniki iz akademskih krogov, industrije in javnega sektorja. Vsi novi superračunalniki bodo, tako kot obstoječi superračunalniki, ki so del PRACE (Partnership for Advanced Computing in Europe), povezani z visokohitrostnim vseevropskim omrežjem GEANT.[47]

3.3.1. Odpravljanje ovir v evropskem podatkovnem gospodarstvu

Strategija enotnega digitalnega trga naj bi povečala potencial rasti evropskega digitalnega gospodarstva in njegove družbe, tako da bo lahko vsak prebivalec Evrope v celoti izkoriščal te dobrobiti. V ta namen je bila sprejeta Uredba (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji, katera želi odstraniti ovire za prosti pretok neosebnih podatkov po državah članicah in informacijsko tehnoloških (IT) sistemih v Evropi.[48]

Uredba o prostem pretoku neosebnih podatkov podjetjem zagotavlja pravno varnost z namenom, da lahko svoje podatke v EU

[46] Communication from the Commission to The European Parliament ..., 2016, str. 5.
[47] Evropa razglasila osem lokacij za vrhunske superračunalnike, Evropska komisija, 2019, e-vir.
[48] Uredba (EU) 2018/1807, uvodna izjava 11.

obdelujejo kjerkoli želijo, kar povečuje zaupanje v storitve obdelave podatkov in preprečuje prakse, ki povzročajo vezanost na enega ponudnika. S tem se bo povečala možnost izbire za potrošnike, izboljšala učinkovitost in spodbudilo uvajanje tehnologij v oblaku, kar bo podjetjem v EU omogočilo velike prihranke. Študije kažejo, da lahko podjetja v EU s prehodom na računalništvo v oblaku prihranijo 20-50% stroškov za informacijsko tehnologijo. Zato je sedaj vzpostavljen celovit okvir za skupni evropski podatkovni prostor in prosti pretok vseh podatkov v Evropski uniji.[49]

GDPR že predvideva prosti pretok osebnih podatkov v Uniji, zraven svojega primarnega cilja varovanja osebnih podatkov. Ta uredba o prostem pretoku neosebnih podatkov naj bi skupaj s GDPR zagotovila celovit in skladen pristop k prostemu pretoku vseh podatkov v EU. Da bi podjetjem zagotovili večjo jasnost glede čezmejnega ravnanja s podatki, je Komisija objavila informativne smernice o medsebojnem vplivu med to uredbo in GDPR, zlasti kar zadeva podatkovne nize, ki vsebujejo osebne in neosebne podatke.[50]

Podjetje, ki bo obdelovalo mešane nabore podatkov ga Uredba o prostem pretoku neosebnih podatkov kot tudi GDPR ne zavezuje k ločevanju ali shranjevanju osebnih in neosebnih podatkov. Če se takšno podjetje odloči, da jih ne bo ločevalo ter jih bo obdelovalo kot mešane nabore podatkov bodo pravila o varstvu podatkov veljala za celoten mešani nabor podatkov. Uredba o prostem pretoku neosebnih podatkov in GDPR bosta tako skupaj ustvarjali pravno varnost za podjetja in zagotavljali, da se lahko osebni in neosebni podatki (tudi kadar so vključeni v mešani nabor podatkov) prosto gibljejo v EU. Zato se podjetja in organi lahko odločijo, da bodo mešani nabor podatkov shranili, prenesli ali obdelali kjer koli v EU.[51]

Javni organi bodo obdržali dostop do podatkov in regulativni nadzor tudi v primeru, kadar se le ti nahajajo v drugi državi članici ter so shranjeni ali obdelani v oblaku. Z uredbo bo tako tudi omogočena lažja menjava ponudnikov storitev v oblaku za profesionalne uporabnike. Komisija je želela olajšati samoregulacijo na tem področju in spodbuditi ponudnike k oblikovanju kodeksov

[49] Sporočilo Komisije Evropskemu parlamentu in Svetu - Smernice k uredbi o okviru za prosti pretok neosebnih podatkov v EU, 2019, str. 2.
[50] Prav tam, str. 3.
[51] Mnenje Evropski ekonomsko-socialni odbor, 2019, str. 3.

ravnanja glede pogojev, pod katerimi lahko uporabniki prenašajo podatke med ponudnike storitev v oblaku in nazaj v svoje IT-okolje.[52]

Uredba o prostem pretoku neosebnih podatkov ima tri pomembne značilnosti:

– državam članicam praviloma prepoveduje uvedbo zahtev glede lokalizacije podatkov. Izjeme od tega pravila so lahko utemeljene le na podlagi javne varnosti ob upoštevanju načela sorazmernosti;

– vzpostavlja mehanizem sodelovanja, da bodo lahko pristojni organi še naprej uveljavljali vse pravice dostopa do podatkov, ki se obdelujejo v drugi državi članici;

– industriji daje spodbude, da ob podpori Komisije oblikuje samoregulativne kodekse ravnanja glede zamenjave ponudnikov storitev in prenosa podatkov.[53]

3.3.2 Določitev prednostnih nalog za standarde in interoperabilnost

Komisija si je zadala tudi prednostne naloge na področju standardizacije (tudi kibernetske varnosti) in na kritičnem področju interoperabilnosti enotnega digitalnega trga, kot so zdravje, promet, načrtovanja in energije. Standardizacija je bistvena sestavina industrijske konkurenčnosti na vseh področjih. Uredba 1025/2012 o evropski standardizaciji določa pravni okvir, v katerem delujejo akterji v standardizaciji (Evropska komisija, evropske organizacije za standardizacijo, industrija in družbene interesne skupine). V tej uredbi je bil poudarjen hiter razvoj IKT in kako novi proizvodi in storitve, kot so »pametne« ali povezane naprave (pod imenom internet stvari oz. IoT) ali oblak, preoblikujejo trge.[54]

V zadnjih desetletjih številne najpogosteje uporabljene tehnične specifikacije IKT izdelujejo strokovni forumi in konzorciji proizvajalcev, ki so postali vodilni organi za razvoj standardov IKT. 13. člen Uredbe 1025/2012 o evropski standardizaciji Komisiji omogoča, da opredeli tehnične specifikacije IKT, na katere se lahko naročnik kasneje sklicuje v javnih naročilih, predvsem z namenom zagotovitve interoperabilnosti. To javnim organom omo-

[52] Prav tam, str. 8-9.
[53] Sporočilo Komisije Evropskemu parlamentu in Svetu - Smernice k uredbi o okviru za prosti pretok neosebnih podatkov v EU, 2019, str. 1.
[54] Prednostne naloge na področju standardizacije IKT, 2016, str. 1.

goča, da pri nakupu IT strojne opreme, programske opreme in storitev uporabijo celoten obseg specifikacij, kar omogoča večjo konkurenco na terenu in zmanjšuje tveganje za kasnejšo zavezanost samo enemu dobavitelju opreme.[55]

Skupni standardi zagotavljajo interoperabilnost digitalnih tehnologij in so temelj učinkovitega digitalnega enotnega trga. Zagotavljajo nemoteno in zanesljivo skupno delovanje tehnologij, omogočajo ekonomijo obsega, spodbujajo raziskave in inovacije ter trge ohranjajo odprte. Dejanska interoperabilnost zagotavlja, da povezane naprave kot so avtomobili, telefoni, naprave in industrijska oprema lahko med seboj nemoteno komunicirajo ne glede na proizvajalca, operacijski sistem ali druge tehnične sestavne dele. Odprti standardi takšno interoperabilnost zagotavljajo in spodbujajo inovacije ter znižujejo ovire za vstop na enotni digitalni trg, vključno z dostopom do medijskih, kulturnih in izobraževalnih vsebin. Razlike med nacionalnimi standardi lahko znatno upočasnijo inovacije in evropska podjetja glede na ostali svet postavijo v slabši položaj.[56]

S sporočilom o prednostnih nalogah standardizacije IKT Komisija predlaga, da se viri in skupnosti za določanje standardov osredotočijo na 5 prednostnih področij: 5G, internet stvari, računalništvo v oblaku, kibernetska varnost in podatkovne tehnologije katere so bistvene za širšo konkurenčnost EU. Ukrepi na teh področjih lahko pospešijo digitalizacijo in imajo takojšen vpliv na konkurenčnost informacijskih in komunikacijskih tehnologij, povezanih z zakonodajo in politikami EU, kot so zdravstveno varstvo (e-Zdravstvo), računalništvo v oblaku, inteligentni prometni sistemi, varnost, dostopnost, internet stvari, e-Uprava, pametne mreže ter še mnoge razvijajoče se tehnologije. Ključno pri standardizaciji in interoperabilnosti je razjasniti povezavo med evropsko zakonodajo in razvojnimi politikami, saj IKT standardi vsebujejo pomembne tehnološke zahteve za zasebnost, varnost in dostopnost.[57]

3.3.3. Podpora za vključujočo digitalno družbo

Digitalna družba v Evropi se razvija z razvidom vseh koristi, ki jih ponuja strategija enotnega digitalnega trga. Evropska komisi-

[55] Uredba 1025/2012, 13. člen.
[56] Prednostne naloge na področju standardizacije IKT, 2016, str. 2.
[57] Rolling plan for ICT standardisation, 2019, str. 62.

ja aktivno izvaja konkretne ukrepe za razvoj čezmejnih digitalnih javnih storitev in zagotavlja uporabo digitalnih orodij in sistemov za boljšo in modernejšo e-upravo za vse državljane in podjetja. Na tem področju se razvija in izvaja politika za usposabljanje evropskih državljanov v digitalnih spretnostih, s pobudami kot je Program veščin za Evropo.[58]

Nagle tehnološke spremembe spreminjajo industrijske potrebe v svetovnem merilu, zato je nujno potrebno povečati ključna znanja naše delovne sile, saj je to predpogoj, da bi evropska podjetja globalno ostala konkurenčna. Medtem ko naložbe v nove tehnologije ponujajo priložnost za obnovo proizvodnje v Evropi, bo pomanjkanje spretnosti ustvarilo ozko grlo v tem procesu. Vse več je vrzeli in neskladja v znanju, povezanem z digitalnimi in ključnimi visokotehnološkimi tehnologijami. Podjetja poročajo o težavah pri iskanju zaposlenih s temi znanji. Potrebno bo bolje predvideti potrebe po spretnostih za obvladovanje sprememb, negovanje novih vrst dela in krepitev socialne kohezije. Zato so pomembna prizadevanja za povečanje baze talentov v EU, ki bi iskalcem zaposlitve omogočala pridobiti nova znanja s poudarkom na novih tehnologijah. Digitalne spretnosti so sedaj v središču industrijske politike, saj inovativnost izvira iz ustvarjalnosti in spretnosti posameznikov. Zaradi obstajajoče dirke za talente si bo morala naša delovna sila pridobiti znanja na visoki ravni in jih nenehno izboljševati, da bi se povečala zaposljivost in spodbudila konkurenčnost, ter posledično večja neodvisnost ter rast gospodarstva EU.[59] Ukrepi EU so usmerjeni v primerjalno politiko, spremljanje trendov in ponudbe ter povpraševanja, povečanje dobrih praks, boljše usmerjanje programov in spodbud za financiranje, spodbujanje večje strokovnosti, smernic o učnih načrtih, specializiranih znanj (vključno z velikim podatkovjem, internetom stvari in kibernetsko varnostjo) in partnerstva z več deležniki, v sinergiji z Načrtom za sektorsko sodelovanje na področju spretnosti in Koalicijo digitalnih spretnosti in delovnih mest.[60]

V skladu z navedenim je torej potrebno podpirati vključujočo digitalno družbo, v kateri imajo državljani ustrezne veščine, da izkoristijo priložnosti informacijske tehnologije in povečajo svoje

[58] Creating a digital society, Evropska komisija, 2019, e-vir.
[59] Sporočilo Komisije Evropskemu parlamentu in Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij - Novi program znanj in spretnosti za Evropo ..., 2016, str. 7.
[60] A concept paper on digitisation, 2017, str. 6-7.

možnosti za zaposlitev. Nov akcijski načrt za e-Upravo bo povezal tudi poslovne registre po vsej Evropi ter zagotovil, da bodo lahko različni nacionalni sistemi medsebojno sodelovali in zagotavljali, da bodo podjetja in državljani svoje podatke lahko posredovali javnim upravam samo enkrat. To pomeni, da administracije ne bodo več pošiljale različnih zahtev za iste informacije, kadar lahko uporabijo informacije, ki jih že posedujejo.[61]

4. Sklep

Strategija enotnega digitalnega trga je začrtala pot EU, da ustvari pravilno digitalno okolje, takšno, v katerem so zagotovljena visoka raven zasebnosti, varstvo osebnih podatkov in pravic potrošnikov, podjetja lahko razvijajo inovacije in konkurenco, kibernetska varnost pa krepi tkanje, ki združuje naše družbeno okolje. Konvencija 108+ in GDPR na ravni Evropske unije je dosežek in napredovanje v pravo smer na področju varstva osebnih podatkov, ker je običajne uporabnike ali pa tiste, ki so bolj družbeno dejavni vsaj delno pripravila k temu, da se zavedajo ne samo svojih osebnih podatkov, pač pa tudi podatkov vseh ostalih s katerimi prihajajo v stik preko svojega dela, predavanj, konferenc, objavljanja slikovnega gradiva svojih družinskih in službenih dogodkov, ipd.

Na vprašanje ali je GDPR okrepila varstvo pravic posameznikovih osebnih podatkov, lahko torej odgovorimo, da GDPR skozi načela, novosti, razširjanja posameznikovih pravic in krepitev njegove samonadzorne vloge močno povečuje varstvo posameznikovih osebnih podatkov. Vendar se GDPR izogne podrobnemu razreševanju ključnih problemov, kot sta recimo načeli privzetega in vgrajenega varstva, področja avtomatiziranega odločanja, metode za preverjanje ali je podjetje dejansko prenehalo uporabljati podatke uporabnikov v primeru prenehanja podlag obdelave, dostop podjetja do potrošnikovega digitalnega okolja, ki lahko vključuje virtualni dostop do potrošnikove strojne opreme - kar pomeni morebitno tveganje dostopa do njegovih osebnih podatkov. Implementacija GDPR v nacionalno zakonodajo bo sicer mogoče začasno vplivala na višjo raven varstva osebnih podatkov že zaradi zagroženih visokih denarnih sankcij, vendar ob tem ni smi-

[61] Enotni digitalni trg za Evropo: 16 pobud Komisije za njegovo uresničitev, Evropska komisija, 2015, e-vir.

selno pričakovati, da se bo obdelava ali zloraba osebnih podatkov na različnih področjih digitalne tehnologije pretirano zmanjšala.

Istočasno pa smo zaenkrat še vedno preveč navezani na privid razumnega in informacijsko podkovanega posameznika, ki se mu prepušča vse preveč odgovornosti in dolžnosti, pravice pa se mu hkrati omejujejo pod pretvezo sprejemanja varnostnih politik ponudnika storitve. GDPR sicer meri v pravo smer, a je pri njej težavno ravno prepuščanje odgovornosti posamezniku od katerega se pričakuje visoko cenjenje podeljenih pravic, skrbno vsakodnevno spremljanje kršitev in tekoče prijavljanje le teh kršitev, kar je popolna utopija. Nove in nove informacijske ter komunikacijske tehnologije redno vključujejo posebne značilnosti, ki vplivajo na varnost in varstvo podatkov. Uporabnik je običajno izpostavljen zapletenim in težavnim podrobnostim o tehnologiji, ki jih ni enostavno razumeti, kot so recimo tehnične nastavitve naprav in storitev, privzete vrednosti, posledice uporabe storitev itd. V svoji želji uporabe nove informacijsko komunikacijske tehnologije, uporabnik pogosto sprejema neinformirane odločitve z istočasnim tveganjem nezavednega žrtvovanja svoje informacijske varnosti. Raziskave javnega mnenja so pokazale, da se ljudje kljub skrbi za svojo zasebnost, ne obnašajo temu ustrezno.[62] Obvestila o politikah zasebnosti ponudnikov digitalnih storitev ter pravicah posameznika ne pomagajo veliko - redko jih beremo in še redkeje razumemo. Preučiti je potrebno stopnjo, do katere lahko pritiski, kot so spremembe v okolju, v katerem se sprejema odločitev, spremenijo vedenje na področju digitalne zasebnosti. Vse kaže na to, da prisotnost antropomorfnega značaja vodi do večjega razkritja osebnih podatkov kot pa bi uporabnik želel, kar pa je tudi odvisno od diferenciacij med državami, starostnimi skupinami in stopnjami izobrazbe.

Na podlagi navedenega ugotavljamo, da je način sprejemanja soglasja uporabnika v tradicionalnem spletu zagotovljen preko pogojev in pravilnikov o zasebnosti, ki so uporabnikom v večini primerov predstavljeni z odstavki dolgega besedila, katerega se v večini primerov zadostno ne dojame. Na področju interneta stvari (IoT) soglasje uporabnika pomeni pridobitev zahtevane stopnje dovoljenja od uporabnikov in istočasno tudi neuporabnikov (npr. družinskih članov) na katere vplivajo naprave ali storitve. V

[62] Special Eurobarometer 487b, 2019, str. 34-37.

zadnjem času so se s pojavom socialnih medijev in mobilnih aplikacij tudi spremenili mehanizmi za pridobivanje soglasij. Trenutni pregledi digitalnih storitev so ugotovili, da metode spraševanja in informiranja uporabnika na platformah družbenih medijev, kot je recimo Facebook, niso učinkovite in istočasno večina uporabnikov podcenjuje dovoljenja, dodeljena aplikacijam tretjih oseb.[63] V nekaterih primerih razvijalci platform uporabnikom morda ne bodo podali natančnih in relevantnih informacij za odločitev o odobritvi. V drugih primerih lahko razvijalci podajo natančne informacije, vendar uporabniki sami ne bi zmogli natančno razumeti, kaj soglasje pomeni v danem trenutku zaradi pomanjkanja tehničnega znanja. Eden glavnih izzivov glede informacijske zasebnosti je razvoj tehnologij, ki od uporabnikov zahtevajo soglasje na učinkovit in zavedanja uspešen način. To je zahtevna naloga, ker ima vsak klasični uporabnik zelo omejen čas in tudi omejeno tehnično znanje za vključitev v postopek. Na tem področju se še bodo morale izvesti raziskave, ki bodo morale združiti načela in tehnike interakcije med človekom, računalnikom in posameznikovo kognitivno spretnostjo.

Vse večja uporaba analitike velikega podatkovja in umetne inteligence v procesih odločanja javnih organov, poudarja pomen proučevanja njihovega potencialnega vpliva na posameznike in družbo na splošno. Posledice obdelave podatkov niso več omejene na znana vprašanja povezana z informacijsko zasebnostjo, temveč tudi vključujejo predsodke do skupin posameznikov in širšo paleto temeljnih pravic. Ob tem nastaja navzkrižje interesov med obsežno uporabo velikega podatkovja in umetne inteligence na eni strani, ter naraščajočim povpraševanjem po uporabi etično in družbeno odgovornih podatkov na drugi strani, kar razkriva pomanjkanje regulativnega okvira, ki bi lahko reševal družbena vprašanja povzročena s podatkovno intenzivnimi tehnologijami.

Nedvomno, so se računalništvo in storitve v oblaku razvile z namenom, da vključujejo čim več uporabnikov v različnih državah, vendar pri istem ponudniku storitve. Zaradi lokacijsko razdrobljene informacijske tehnologije (aplikacije, podatki, serverji, diski, odjemalci, varnostni mehanizmi itd.) se pogosto premikajo osebni podatki po več različnih jurisdikcijah in neizogibno vzbujajo pomisleke glede varstva osebnih podatkov. Ker zakonodajal-

[63] Special Eurobarometer 487a, 2019, str. 15-20.

ci v vsaki jurisdikciji poskušajo sprejeti zakone, ki ščitijo njihove volivce in trenutne politične programe, se pojavljajo vprašanja o pristojnostih, ki ogrožajo stabilnost mednarodnega režima računalništva v oblaku. Tudi če Evropski organ za varstvo podatkov lahko pravilno uveljavlja pristojnost nad spletnimi stranmi in ponudniki spletnih storitev v okviru pristojnosti GDPR, je zelo malo verjetno, da bi recimo kitajsko sodišče izvršilo kakšno odredbo EU.[64] Geografska prekomerna širitev informacijskih tehnologij bo neizogibno povzročila neizvedljivost GDPR na globalnem trgu, saj pristojnost organov EU za varstvo podatkov ne presega meja EU.

Opozoriti je tudi potrebno pred novimi določbami[65], ki uvajajo idejo, da lahko ljudje plačujejo digitalno blago ali storitve s svojimi osebnimi in drugimi podatki (ki še niso natančno definirani). V EU osebnih podatkov ne bi smeli obravnavati zgolj kot digitalno gospodarsko dobrino (lastnino). Pravic do varstva osebnih podatkov pa ne bi smeli omejiti samo ozko na trenutne preproste interese potrošnikov, osebnih podatkov posameznika pa tudi ne bi smeli obravnavati kot trgovsko blago digitalnega gospodarstva. Morda bi lahko obstajal trg osebnih podatkov, vendar to ne pomeni, da lahko takšnemu tržišču podamo tudi blagoslov zakonodaje. Ne moremo gledati samo na ekonomske interese (zaslužek) in temeljne človekove pravice spremeniti v zgolj preproste komercialne posle, četudi je posameznik, ki ga zadevajo podatki, stranka tega sporazuma.

Objektivno gledano je torej jasno, da lahko popolno digitalno (informacijsko) zasebnost s tehnološkega stališča uživa samo posameznik, ki ni aktiven v digitalnem svetu. Z obsegom online aktivnosti oziroma uporabe sodobne tehnologije pa obseg tehnološko razumnega pričakovanja zasebnosti eksponentno upada. Večina strokovnjakov s tega področja se v zvezi s tem sprašuje, ali je realno od ljudi zahtevati, da se odločijo, ali bodo uporabljali internet ali pa uživali pravico do zasebnosti, oziroma ali je prav, da se od ljudi pravzaprav zahtevajo takšne odločitve. Argument, da se lahko posameznik odloči, da ne bo aktiven v digitalnem svetu, če ga zbiranje podatkov o njegovih aktivnostih oziroma vsesplošen nadzor moti (in torej deluje po načelu »vzemi ali pusti«), danes ne more biti več realen, saj se vse več vsakodnevnih vendar

[64] Sang Woo, 2018, str. 291.
[65] Direktiva (EU) 2019/770.

nujnih opravil seli v digitalno oziroma virtualno okolje, zato ima posameznik precej omejene možnosti odločanja, če želi razmeroma normalno življenje. Če se s tem strinjamo (in težko se ne bi), se zdi, da je torej treba pritrditi avtorjem, ki ugotavljajo, da v dobi interneta (vključno z internetom stvari, družbenimi omrežji, pametnimi telefoni in videonadzornimi sistemi) in velikega podatkovja na večini področij pričakovanje zasebnosti ni več razumno, saj je jasno, da z uporabo sodobnih naprav in storitev tako ali drugače dajemo na voljo svoje podatke. Zato odgovornost za postavljanje meja tehnologiji in za zaščito zasebnosti in osebnih podatkov nosi predvsem zakonodajalec.

LITERATURA IN VIRI

A concept paper on digitisation, employability and inclusiveness the role of Europe. (2017). Bruselj: European Commission, Directorate-General for Communication Networks, Content and Technology.

Communication from the Commission to The European Parliament, the Council, the European Economic and Social committee and the Committee of the regions - European Cloud Initiative - Building a competitive data and knowledge economy in Europe, COM(2016) 178 final. (2016). Bruselj: Evropska komisija.

Contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation between the European union and the European cybersecurity organization - Commission Decision C(2016) 4400 final. Bruselj: Evropska komisija, 5. 7. 2016. URL: https://ec.europa.eu/transparency/regdoc/rep/3/2016/EN/C-2016-4400-F1-EN-ANNEX-1-PART-1.PDF.

Creating a digital society. Evropska komisija, 27.9.2019. URL: https://ec.europa.eu/digital-single-market/en/policies/creating-digital-society. 12.1.2020.

Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Uradni list Evropske unije, L 281, 23.11.1995, str. 31–50.

Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (Policijska direktiva), Uradni list Evropske unije, L 119, 4.5.2016, str. 89-131.

Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji, Uradni list Evropske unije, L 194, 19.7.2016, str. 1-30.

Direktiva (EU) 2019/770 Evropskega parlamenta in Sveta z dne 20. maja 2019 o nekaterih vidikih pogodb o dobavi digitalne vsebine in digitalnih storitev (Besedilo velja za EGP.), Uradni list Evropske unije, L 136, 22.5.2019, str. 1–27.

Dogovor o reformi varstva podatkov v EU, ki jo je predlagala Komisija, bo spodbudil enotni digitalni trg. Evropska komisija, 15.12.2015. URL: https://ec.europa.eu/commission/presscorner/detail/sl/IP_15_6321, 10.1.2020.

Enotni digitalni trg za Evropo: 16 pobud Komisije za njegovo uresničitev. Evropska komisija, 6.5.2015. URL: https://ec.europa.eu/commission/presscorner/detail/sl/IP_15_4919. 12.1.2020.

Enotni digitalni trg: Evropejci in Evropejke po podatkih raziskave dobro poznajo pravila proti neupravičenemu geografskemu blokiranju. Evropska komisija - Sporočilo za medije, 27.6.2019. URL: http://europa.eu/rapid/press-release_IP-19-2528_sl.htm. 29.7.2019.

Evropa razglasila osem lokacij za vrhunske superračunalnike. Evropska komisija Sporočilo za medije, 7.6.2019.URL: https://europa.eu/rapid/press-release_IP-19-2868_sl.htm. 11.8.2019.

Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (2018). Strasbourg: Council of Europe.
Kibernetska kriminaliteta: državljane EU skrbi varnost osebnih podatkov in spletnih plačil. (2012). Bruselj: Evropska komisija.
Komisija objavila smernice o prostem pretoku neosebnih podatkov. Evropska komisija Sporočilo za medije, 29.5.2019. URL: http://europa.eu/rapid/press-release_IP-19-2749_sl.htm. 26.7.2019.
Mnenje Evropski ekonomsko-socialni odbor - Smernice glede prostega pretoka neosebnih podatkov, TEN/699-EESC-2019. (2019). Bruselj: Evropski ekonomsko-socialni odbor.
Mnenje Evropskega ekonomsko-socialnega odbora – Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o vmesnem pregledu izvajanja strategije za enotni digitalni trg – Povezani enotni digitalni trg za vse, COM(2017) 228 final. (2017). Bruselj: Evropska komisija.
Pobuda za sklenitev Protokola o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. (16.4.2019). Ljubljana: Vlada Republike Slovenije.
Podpis Protokola o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. Ministrstvo za pravosodje, 17.5.2019. URL: http://www.mp.gov.si/si/medijsko_sredisce/novica/7763/. 27.7.2019.
Predlog Sklep sveta o pooblastitvi držav članic, da v interesu Evropske unije podpišejo Protokol o spremembi Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (ETS št. 108) COM/2018/449 final - 2018/0237 (NLE), Evropski parlament, Bruselj: 5.6.2018. URL: https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=COM%3A2018%3A449%3AFIN.
Priročnik o evropskem pravu varstva osebnih podatkov. (2014). Agencija Evropske unije za temeljne pravice, Svet Evrope. Luxembourg: Urad za publikacije Evropske unije.
Proposal for an ePrivacy Regulation. European Commission, 19.6.2019. URL: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation. 10.1.2020.
Right environment for digital networks and services. European Commission, 2.12.2019. URL: https://ec.europa.eu/digital-single-market/en/right-environment-digital-networks-and-services. 10.1.2020.
Revision of the Audiovisual Media Services Directive. European Commission, 2.12.2019. URL: https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd. 10.1.2020.
Rolling plan for ICT standardisation 2019. (2019). Bruselj: Evropska komisija.
Sang Woo, L. (2018). A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing (doktorska disertacija). Beijing: China University of Political Science and Law.
Special Eurobarometer 487a, The General Data Protection Regulation. (2019). Brussels: Directorate-General for Justice and Consumers and co-ordinated by the Directorate-General for Communication.
Special eurobarometer 487a. General Data Protection Regulation - 487b. Charter of Fundamental Rights. (2019). Brussels: Directorate-General for Justice and Consumers and co-ordinated by the Directorate-General for Communication
Sporočilo Komisije Evropskemu parlamentu in Svetu - Smernice k uredbi o okviru za prosti pretok neosebnih podatkov v Evropski uniji, COM(2019) 250 final. (2019). Bruselj: Evropska komisija.
Sporočilo Komisije Evropskemu parlamentu in Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij - Novi program znanj in spretnosti za Evropo, Z roko v roki za večji človeški kapital, zaposljivost in konkurenčnost COM/2016/0381 final. (2016). Bruselj: Evropska komisija.
Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in odboru regij Prednostne naloge na področju standardizacije IKT za enotni digitalni trg COM/2016/0176 final. Bruselj: Evropska komisija, 19.4.2016. URL: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52016DC0176.
Sporočilo Komisije Evropskemu parlamentu in Svetu Okrepljeno varstvo, nove priložnosti – navodila Komisije o neposredni uporabi splošne uredbe o varstvu podatkov od 25. maja 2018, COM(2018) 43 final. Bruselj: Evropska komisija, 24.1.2018. URL: https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX%3A52018DC0043.
The European Digital Single Market. Eyes on Europe, 16.10.2017. URL: https://www.eyes-on-europe.eu/the-european-digital-single-market/. 10.1.2020.
The modernized Convention 108: novelties in a nutshell. (2019). Strasbourg: Council of Europe.
Uredba (EU) 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega

parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta. Uradni list Evropske unije, L 316, 14.11.2012, str. 12-33.

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). Uradni list Evropske unije, L 119, 4.5.2016, str. 1-88.

Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES. Uradni list Evropske unije, L 295, 21.11.2018, str. 39–98.

Uredba (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji. Uradni list Evropske unije, L 303, 28.11.2018, str. 59-68.

What is GDPR? Everything you need to know, from requirements to fines. ITPro, 23.12.2019. URL: https://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know. 10.1.2020.