

Др Небојша М. Петковић*

Прегледни научни чланак

УДК: 004:336

DOI: <https://doi.org/10.46793/GP.1701.063P>

**ДИГИТАЛНИ ИДЕНТИТЕТ, ДИГИТАЛНИ НОВЧАНИК,
ДИГИТАЛНА ВАЛУТА ЦЕНТРАЛНЕ БАНКЕ И СИСТЕМИ
ПРАЋЕЊА КАРБОНСКОГ ОТИСКА – КОРИСНА
ТЕХНОЛОГИЈА ИЛИ ИНФРАСТРУКТУРА
ЗА КОНТРОЛУ И НАДЗОР?**

Рад примљен: 11. 08. 2026.

Рад исправљен: 24. 08. 2026.

Рад прихваћен за објављивање: 25. 09. 2026.

Технологије дигиталног идентитета, дигиталног новчаника, дигиталне валуте централне банке и системи праћења карбонског отиска представљају кључне стубове дигиталне инфраструктуре која мења, до сада људској цивилизацији познате, финансијске, социјалне и еколошке односе. Циљ рада је да се, на бази систематизације и анализе нормативне регулативе и релевантних извора литературе, испита да ли ова четири стуба дигиталне инфраструктуре представљају корисну технологију која промовише укључивање грађана у дигитални финансијски систем, повећава ефикасност јавне управе и подстиче еколошку одрживост или инфраструктуру која омогућава државну и корпоративну контролу, масовни надзор и ограничавање понашања. Рад тежи да, уз компаративну анализу националних студија случаја и нормативних оквира, понуди уравнотежену процену користи и ризика примене умрежених дигиталних технологија, укаже на правне и етичке дилеме и идентификује моделе заштите грађана у технолошки интегрисаним системима.

Кључне речи: дигитални идентитет (DI), дигитални новчаник (DW), дигитална валута централне банке (CBDC), системи праћења карбонског отиска (CFTS), систем социјалног кредита (SCS), дигитални надзор (DS).¹

* Наставник у Економској школи у Нишу, судски вештак за економско-финансијску област, pesapet@mail.ru

¹ Напомена: У раду ће кључне речи бити коришћене као скраћенице енглеских назива: Digital Identity (DI); Digital Wallet (DW); Central Bank Digital Currency (CBDC); Carbon Footprint Tracking Systems (CFTS); Social Credit System (SCS); Digital Surveillance (DS).

I УВОД

Убрзани развој дигиталних технологија последњих деценија поставља пред савремена друштва комплексна питања у области економије, идентитета, безбедности и слободе избора. Четири концепта: *DI*, *DW*, *CBDC* и *CFTS*, у све већој мери се преплићу и интегришу у дигиталну инфраструктуру која мења начин на који грађани учествују у друштвеним процесима. Успон умреженог друштва представља прекретницу у начину на који се производе, складиште и размењују информације, а самим тим и у начину на који функционишу институције и грађани.²

Развој дигиталне инфраструктуре представља део ширег процеса технолошке интеграције јавне управе, финансијског система и свакодневног живота грађана и, иако је пројектована да омогући већу ефикасност, транспарентност и еколошку одрживост, отвара и нове могућности за надзор, биополитичко управљање и концентрацију моћи.³ У еколошком домену, дигиталне технологије су првобитно развијане као алат за мерење емисија индустријских загађења и оптимизацију производних процеса. Са еволуцијом оквира Еколошког, друштвеног и корпоративног управљања (*Environmental, Social and Governance – ESG*)⁴ и глобалних климатских политика, системи праћења карбонског отиска шире се, не само на корпоративне и урбанистичке нивое, већ и на индивидуалне.

Предмет овог рада је анализа односа између *DI*, *DW*, *CBDC* и *CFTS*, као кључних компоненти савремене дигиталне инфраструктуре, и њихове конвергенције у јединствен дигитални екосистем. Циљ рада је да се, кроз компаративну анализу националних студија случаја и релевантних нормативних оквира, критички испита равнотежа између корисних ефеката и потенцијалних опасности ових технологија, као и да се укаже на правне и етичке дилеме и идентификују модели заштите грађана од злоупотребе. Анализа укључује искуства на развоју дигиталних система у Кини, Индији и ЕУ, са освртом на потенцијал технологија за минимизацију ризика и обезбеђивање већег степена контроле над личним подацима и финансијским ресурсима, као што су: децентрализовани идентификатор (*Decentralized Identifier – DID*), самостални дигитални идентитет (*Self-Sovereign Identity – SSI*),

² М. Castells, *The Rise of the Network Society*, Chichester, 2010, 501.

³ Ш. Зубофф, *Эпоха надзорного капитализма: Битва за человеческое будущее на новых рубежах власти*, Москва, 2022, 22.

⁴ UN, *The Global Compact, Who Cares Wins: Connecting the Financial Markets to a Changing World*, Swiss Federal Department/United Nations, 2004. *ESG* представља инвестициони принцип који даје приоритет еколошким и друштвеним питањима, као и корпоративном управљању, а инвестирање уз поштовање *ESG* фактора одговорно инвестирање.

децентрализоване финансије (*Decentralized Finance – DeFi*), технологије доказа без откривања података (*Zero-Knowledge Proofs – ZKP*).⁵

Методолошки, рад се заснива на компаративној, нормативној и дескриптивно-аналитичкој методи и полази од претпоставке да интеграција *DI*, *DW*, *CBDC* и *CFTS* значајно повећава потенцијал за институционални надзор и централизовано управљање друштвеним понашањем, уколико није праћена снажним правним ограничењима, транспарентним механизмима управљања и независним институцијама контроле. Истовремено, рад полази и од става да наведене технологије могу имати значајне позитивне ефекте у области финансијске инклузије, административне ефикасности и одрживог развоја, уколико се примењују у оквиру система који гарантује заштиту основних права и слобода грађана. Рад је структурно конципиран тако да се након уводних разматрања анализира утицај дигиталне технологије на друштво, наставља анализом четири стуба дигиталне инфраструктуре, компаративном анализом националних студија случаја, правним и етичким дилемама, моделима заштите грађана и на крају формулишу закључци рада.

II ДИГИТАЛНА ТЕХНОЛОГИЈА И ДРУШТВО

Стратешке основе економске и политичке моћи у индустријској ери чинили су природни ресурси и енергетски извори, капитал, радна снага и индустријски производни капацитети, док су предузетништво, технологија и организационе способности омогућавали њихово ефикасно комбиновање и претварање у економску вредност. Са убрзаном дигитализацијом друштва, подаци постају нови ресурс економске и политичке моћи. Дигитални свет, који настаје и развија се незамисливом брзином, удаљава нас од света који познајемо. Савремени облици моћи све више зависе од прикупљања, обраде и анализе великих количина података. Контрола података, дигиталне инфраструктуре и информационих токова постаје централно питање суверенитета новог доба. Модел територијалних граница и тоталитарне моћи се кроз дигиталну технологију трансформише у модел алгоритамске моћи. Мултинационалне технолошке корпорације незаустављиво расту и одузимају суверенитет не само појединцу, већ и традиционалној држави.⁶ Иако држава ствара институционалну климу за развој дигиталног друштва, по природи развоја моћи дигиталних платформи, препушта контролу података приватним

⁵ *DID* креира и контролише сама особа или ентитет, без потребе за централним регистром или ауторитетом; *SSI* даје кориснику потпуну контролу над сопственим личним подацима и доказима, чувајући их у личном дигиталном новчанику; *DeFi* су финансијске услуге засноване на паметним уговорима без посредника попут банака; *ZKP* су криптографска техника која омогућава једној страни да докаже истинитост одређене тврдње другој страни, а да притом не открива никакве додатне информације.

⁶ S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019, 376.

корпорацијама, чиме постепено губи дигитални суверенитет и *de facto* и политички суверенитет.⁷ Технолошке корпорације престају да буду само економски актери и све више преузимају функције које су традиционално припадале државама – управљају идентитетом корисника, посредују у финансијским трансакцијама, контролишу проток информација и обликују јавни простор. У том контексту, дигитални суверенитет не подразумева само контролу државе над подацима, већ и способност друштва да спречи прекомерну концентрацију моћи у приватним технолошким платформама.⁸ За разлику од традиционалних правних система, који се ослањају на законодавне и судске институције, ове платформе регулишу понашање корисника путем алгоритама, често кроз приватна правила и аутоматизоване механизме одлучивања, стварајући нови облик регулације у коме технолошка инфраструктура постаје средство управљања друштвеним понашањем.⁹

Дигитална технологија постаје фактор који активно учествује у обликовању институција, процедура и друштвених односа. Она мења природу институционалног притиска на појединца. Традиционални надзор је био повремен, упадљив и захтевао људску присутност.¹⁰ Нови облици дигиталног надзора (*DS*) се не користе за кажњавање друштвено непожељног понашања, већ за социјално сортирање где се систематским и рутинским прикупљањем података становништво класификује у категорије ризичних и подобних.¹¹ Алгоритми су уграђени у саму техничку архитектуру свакодневног живота¹² где техничка немогућност да заобиђе дигитални систем приморава појединца на конформност. Кроз императив ефикасности, транспарентности и практичности, појединац сам добровољно учествује у сопственом надзору, модификујући сопствено понашање како би остао у пожељној категорији и тиме задржао приступ друштвеним и економским привилегијама.¹²

По питању односа технологије и друштва постоје два супротстављена приступа – технолошки детерминизам и приступ демократског управљања технологијом. Први полази од претпоставке да технолошке иновације представљају главни покретач друштвених промена и да њихов развој следи сопствену унутрашњу логику, независно од политичких и друштвених

⁷ E. Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism*, New York, 2013, 115.

⁸ B. H. Bratton, *The Stack: On Software and Sovereignty*, Cambridge, 2015, 109.

⁹ N. Couldry, U. A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Stanford, 2019, 13-14.

¹⁰ М. Фуко, *Надзирати и кажњавати: Настанак затвора*, Сремски Карловци, 1997, 210.

¹¹ G. T. Marx, *Windows Into the Soul: Surveillance and Society in an Age of High Technology*, Chicago, 2016, 61.

¹² B.-C. Han, *Psychopolitics: Neoliberalism and New Technologies of Power*, London, 2017, 5-6, 8-9.

околности.¹³ Присталице другог приступа полазе од претпоставке да технолошки системи нису неутрални, већ да одражавају вредности, интересе и односе моћи присутне у друштву и да технологија није независна од политике, већ управо супротно – њу дизајнирају, финансирају и обликују конкретне друштвене групе, класе и институције, како би заштитиле своје интересе, учврстиле моћ или репродуковале владајуће вредности.¹⁴

III ЧЕТИРИ СТУБА ДИГИТАЛНЕ ИНФРАСТРУКТУРЕ

А. Дигитални идентитет

Традиционални облици идентификације се ослањају на физичка документа и непосредну проверу идентитета. Као скуп података и дигиталних атрибута, *DI* омогућава идентификацију појединца у електронском окружењу. Он представља први конститутивни стуб у дигиталној архитектури кроз који аналогни појединац постаје видљив за систем.¹⁵ За Светску банку (*World Bank – WB*)¹⁶ и Уједињене нације (*United Nations – UN*),¹⁷ *DI* је важан инструмент за повећање финансијске инклузије, приступ јавним услугама и ефикасније функционисање институција. *WB* посматра *DI* као базу финансијске и друштвене интеграције, фундаментални јавни интерес и први стуб за изградњу модерних државних апарата. Без универзалног *DI* немогуће је изградити други стуб – дигитална плаћања, нити ефикасно пратити дистрибуцију ресурса.¹⁸ Светски економски форум (*World Economic Forum – WEF*) описује како *DI* прожима сваки аспект људског живота и позиционира га, у контексту Четврте индустријске револуције, као први и најважнији стуб,¹⁹ а Банка за међународна поравнања (*Bank for International Settlements – BIS*) у својим студијама о

¹³ Вид. L. Winner, *Do Artifacts Have Politics?*, *Daedalus* Vol. 109 No. 1, 1980, 121–136; M. McLuhan, *Understanding Media: The Extensions of Man*, Cambridge, 1994, 7–11; T. Veblen, *The Engineers and the Price System*, New York, 1921, 52–58; J. Ellul, *The Technological Society*, New York, 1964, 133–140.

¹⁴ Вид. E. Morozov, *op. cit.*, 5–9; A. Feenberg, *Transforming Technology: A Critical Theory Revisited*, Oxford, 2002, 169; R. Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*, Cambridge, 2019, 40; M. Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*, Cheltenham, 2015.

¹⁵ A. Greenfield, *Radical Technologies: The Design of Everyday Life*, London, 2017, 23.

¹⁶ WB, *Principles on Identification for Sustainable Development: Toward the Digital Age*, Washington, D.C.: World Bank Group, 2021.

¹⁷ UN, *Transforming our world: The 2030 Agenda for Sustainable Development*, A/RES/70/1, UN General Assembly, 2015. Подциљ 16.9 Агенде 2030 предвиђа да се до 2030. године обезбеди законски идентитет за све, укључујући и регистрацију рођења.

¹⁸ WB, *Identification for Development (ID4D) Annual Report: Better Data and Evidence for Digital ID Systems*, Washington, D.C.: World Bank Group, 2021.

¹⁹ WEF, *A Blueprint for Digital Identity: The Role of Financial Institutions in Shaping the Digital Identity Landscape*, Geneva: WEF, 2016.

увођењу дигиталног новца наводи да успешна имплементација *CBDC* захтева унапред постављену инфраструктуру *DI*²⁰ јер он представља основни архитектонски стуб сигурности, спречавања анонимности и праћења токова капитала.

Развој националних система *DI* у великој мери се ослања на употребу биометријских података – јединствених физичких или физиолошких карактеристика појединца ради његове идентификације. Најчешће коришћени биометријски параметри су отисци прстију, скенирање очију, препознавање лица и гласа, ДНК идентификација. Биометријски системи се карактеришу високим степеном поузданости и смањењем могућности злоупотребе идентитета, али су истовремено биометријски подаци веома осетљива категорија информација трајно повезана са физичким идентитетом појединца.

Системи за управљање идентитетом могу да буду засновани на централизованим и децентрализованим моделима. У централизованом моделу држава управља јединственом базом података која садржи идентитетске информације свих грађана. Овај модел омогућава висок степен административне ефикасности и лакшу интеграцију јавних услуга, али истовремено повећава ризик од злоупотребе података и сајбер напада. У децентрализованом моделу подаци се чувају у више међусобно повезаних система. Такав приступ може допринети већој заштити приватности, али често подразумева сложенију техничку инфраструктуру и већу цену имплементације.²¹ Без обзира на архитектуру система, заједничка карактеристика савремених дигиталних идентификационих модела је тежња ка интеграцији различитих јавних и приватних услуга у оквиру јединственог дигиталног екосистема.

Осим бројних предности, системи дигиталне идентификације носе и низ значајних ризика: масовно прикупљање података – интеграција различитих институционалних база података омогућава стварање детаљних профила грађана који могу обухватати финансијске, здравствене, образовне и друге информације²²; алгоритамска категоризација становништва – повезивањем података из различитих извора могуће је креирати сложене профиле који утичу на приступ услугама, кредитима, осигурању или другим ресурсима,²³ неовлашћени приступ подацима – што је већа концентрација података у оквиру једног система, то су потенцијалне последице успешног сајбер напада

²⁰ BIS, *Annual Economic Report: Blueprint for the Future Monetary System: III The tech architecture of digital finance*, Basel: BIS, 2023.

²¹ A. Goel, Y. Rahulamathavan, *A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility*, Future Internet MDPI Vol. 17 No. 1, 2024, 25-26.

²² S. Zuboff, *Big other: surveillance capitalism and the prospects of an information civilization*, Journal of Information Technology Vol. 30 Issue 1, 2015, 78.

²³ D. Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, London-New York, 2003, 14-15.

озбиљније;²⁴ могућност дигиталног искључења – грађани који немају приступ интернету, адекватну дигиталну писменост или се суочавају са техничким проблемима могу бити ограничени у приступу услугама које постају доступне искључиво кроз дигиталне канале.²⁵

Б. Дигитални новчаник

DW представља финалну материјализацију дигиталне јавне инфраструктуре (*Digital Public Infrastructure – DPI*) у свакодневном животу грађана, софтверско окружење²⁶ које омогућава безбедно складиштење, управљање и коришћење различитих дигиталних акредитива, докумената и инструмената плаћања. Савремени универзални DW није само апликација за плаћање, већ централно корисничко чвориште у којем се, кроз паметне уговоре, на заједничкој дигиталној платформи, спајају новац, имовина и информације.²⁷ Ова конвергенција чини DW најосетљивијом компонентом интегрисане дигиталне инфраструктуре. У њему се чувају идентитет, службена документа, дипломе и сертификати, професионалне лиценце, здравствено осигурање, инструменти плаћања, електронски потписи. DW омогућава грађанину да остварује своја права у реалном времену било где унутар јединственог економског простора, елиминишући бирократско кашњење, корупцију и папирологију. Уместо коришћења више физичких докумената и различитих дигиталних налога, корисник добија централизовану приступну тачку за велики број услуга.

Повезујући идентитетске, финансијске и административне функције у јединствен систем,²⁸ DW постаје контролни стуб дигиталне инфраструктуре. Подаци више нису раздвојени по местима евидентирања – они се секундарно укрштају кроз метаподатке трансакција. То омогућава увођење система социјалног кредита, где се приступ одређеним функцијама DW аутоматски условљава усклађеношћу грађанина са тренутним критеријумима које

²⁴ B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York, 2015, 164-165.

²⁵ V. Eubanks, *Automating Inequality: How High Tech Tools Profile, Police, and Punish the Poor*, New York, 2018, 12.

²⁶ European Commission, *EU Digital Identity Wallet*, <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home>, датум посете: 28. 06. 2026.

²⁷ BIS, *Annual Economic Report 2025, Promoting global monetary and financial stability*, Basel, 2025, 102.

²⁸ European Commission, *European Digital Identity: Digital Identity for all Europeans - A personal digital wallet for EU citizens, businesses and residents*, 2026. https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en, датум посете: 28. 06. 2026.

дефинишу власти.²⁹ Управо због тога значај *DW* превазилази домен плаћања и постаје релевантан за питања приватности, суверенитета података и друштвеног управљања. Посебна карактеристика европског приступа је наглашавање принципа контроле корисника над подацима, а регулаторни оквир настоји да обезбеди да грађани сами одлучују које податке деле и са ким их деле.³⁰

Европска комисија, *WEF* и водећи технолошки институти као аргументе увођења *DW* наводе: повећање ефикасности јавне администрације, омогућавање прекограничних плаћања, интероперабилност, корисничку сувереност, унапређење приватности и минимализацију података. Међународне организације за дигитална права: Фондација за електронске границе (*Electronic Frontier Foundation – EFF*)³¹ и Европска дигитална права (*European Digital Rights – EDRi*)³² предводе критичку струју која у *DW* види крај личне приватности и стварање савшеног алата за административно искључење појединца. Као аргументе наводе архитектуру јединствене тачке прекида, тоталну видљивост и пасивну присилу. Истичу да *DW* представља елиминацију аналогног уточишта и претварање права у условљени приступ и синхронизацију података у реалном времену. Иако се *DW* формално уводи као опциони инструмент, кроз елиминацију физичких алтернатива, *de facto* постаје пасивна присила. Када се сва права грађана лоцирају унутар једне софтверске апликације, држава и корпорације добијају моћ дигиталне екскомуникације. Техничка архитектура у којој иста апликација управља монетарним трансакцијама и државним акредитивима, омогућава држави, кроз јединствену књигу, тоталну видљивост грађанина у реалном времену.

Најутицајнији модели *DW*: *Apple Wallet* и *Google Wallet* представљају пример платформске интеграције у којој приватне технолошке мултинационалне корпорације постају посредници између корисника, финансијских институција и државних органа. Оне доприносе ширењу дигиталних услуга и иновација, али и концентришу значајну количину података у руке ограниченог броја корпорација, што отвара питања

²⁹ E. Prasad, *China's New Digital Currency: Function and Motives*, in: *Digital Currencies* (eds., D. Duffie and E. Economy), Stanford, 2022, 39-40.

³⁰ Европски модел представља покушај успостављања равнотеже између дигиталне ефикасности и заштите приватности, ослањајући се на принципе из Опште уредбе о заштити података – *General Data Protection Regulation (GDPR)*: *GDPR.EU, Document 32016R0679: Regulation (EU) 2016/679 of the European Parliament and of the Council*, Official Journal of the European Union L 119/1, 2016.

³¹ EFF, *Digital ID Isn't for Everybody, and That's Okay*, https://www.eff.org/hi/deeplinks/2024/09/digital-id-isnt-everybody-and-thats-okay?language=hi&utm_source=chatgpt.com, датум посете: 28. 06. 2026.

³² EDRi, *Digital ID – civil society demands protection of Users*, https://edri.org/our-work/digital-id-civil-society-demands-protection-of-users/?utm_source=chatgpt.com, датум посете: 28. 06. 2026.

конкуренције, суверенитета и заштите приватности.³³ Пример најразвијенијег *super-app* екосистема имамо у Кини где су развијене платформе *WeChat* и *Alipay*. Ове платформе интегришу комуникацију, плаћања, електронску трговину, јавне услуге, здравствене сертификате, свакодневне услуге, различите облике идентификације, пословни сектор и функционишу као свеобухватна дигитална инфраструктура свакодневног живота, неупоредиво измењеног.

В. Дигитална валута централне банке

Као неки од разлога за појачани државни интерес увођења *CBDC*, као дигиталног облика новца централне банке,³⁴ и тиме успостављања контроле над осетљивом облашћу дигиталних финансија која се убрзано развија, наводе се спонтани развој приватних дигиталних финансијских инструмената,³⁵ растућа капитализација криптовалута³⁶ и све већа деглобализација међународних односа.³⁷ Централне банке, Међународни монетарни фонд (*International Monetary Fund – IMF*) и *BIS*, као водећи заговорници увођења *CBDC*, посматрају дигитални новац као суверени одговор на успон нерегулисаних криптовалута и као алат за модернизацију монетарног система, а као примарни аргумент наводе очување монетарног суверенитета и сузбијање финансијског криминала.³⁸ Будући да је свака јединица *CBDC* дигитално потписана од стране централне банке, систем драматично смањује могућност прања новца, утаје пореза и финансирања нелегалних активности. Трансакције су брже, јефтиније и отпорније на системске ризике приватних платформских монопола *Visa* или *Mastercard*. Други аргумент је постизање ефикасности прекограничних плаћања и финансијска инклузија.³⁹ Постојећи међународни банкарски систем *SWIFT* постаје спор и скуп за прекогранична плаћања због мноштва посредничких банака. *CBDC* омогућава инстант поравнања између различитих држава по (тренутно) занемарљивим надокнадама и омогућава

³³ N. Couldry, U. A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Stanford, 2019, 21-24.

³⁴ Bank for International Settlements, *Central Bank Digital Currencies: Foundational Principles and Core Features*, Basel: BIS, 2020, 3.

³⁵ С.Ю. Глазьев, Р.С. Глазьев, *Криптовалюты как новый тип денег*, Евразийская интеграция: экономика, право, политика №1, 2018, 22.

³⁶ Н.Ю. Лебедева, Г.В. Назаренко, Л.К. Седракан, *Цифровая валюта центрального банка: перспективы и риски эмиссии*, Проблемы экономики, Государственное и муниципальное управление, Ученые записки № 2, 2020, 147.

³⁷ А. А. Недров, *Правовая природа цифрового рубля*, Вестник Московского университета, Серия 21, Управление (государство и общество) Т. 22 № 1, 2025, 237.

³⁸ R. Auer et al., *Central Bank Digital Currencies: Motive, Economic Implications and the Research Frontier*, BIS Working Papers No 976, Basel, 2021.

³⁹ G. Soderberg et al., *Behind the Scenes of Central Bank Digital Currency: Emerging Trends and Insight*, IMF Fintech Notes No. 2022/004, Washington D.C., 2022.

грађанима, који немају традиционалне банкарске рачуне, директан приступ сувереном дигиталном новцу преко паметних телефона.

Критичари виде увођење *CBDC* као најмоћнији алат за укидање економске аутономије појединца, а као примарни аргумент наводе кризу финансијске приватности и државни надзор у реалном времену.⁴⁰ За разлику од физичког новца који обезбеђује природну анонимност у трансакцијама, *CBDC* укида приватни простор размене. Свака трансакција постаје трајно забележена у централном државном регистру. Ово омогућава потпуну видљивост трансакција грађана, стварајући ризик од политички мотивисаног замрзавања средстава⁴¹ без традиционалних судских налога. Други аргумент истиче програмабилност новца као средства социјалног инжењеринга⁴² која је опаснија димензија *CBDC* од самог надзора. Ако новац има намену коју одређује држава, може бити деактивиран, временски ограничен и условљен понашањем по *ESG* протоколима, чиме престаје да буде пуна својина, већ условно, реверзибилно, административно право коришћења.⁴³

У великом броју земаља, како развијених, тако и земљама у развоју, покренут је или је у припреми пројекат на развоју *CBDC*. Бахами су прва држава на свету која је у потпуности и званично лансирала своју дигиталну валуту *Sand Dollar* октобра 2020. године,⁴⁴ с циљем унапређења финансијских

⁴⁰ E. S. Prasad, *The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance*, Cambridge, 2021, 22.

⁴¹ Н. Планојевић, *Престанак права својине*, у: Зборник радова Правног факултета Универзитета у Крагујевцу, књ. 1 (ур. Д. Вујисић), Правни факултет Универзитета у Крагујевцу, Институт за правне и друштвене науке, Крагујевац 2024, 331. Политички мотивисано замрзавање средстава без традиционалних судских налога доводи у питање право својине које је трајно и незастариво право, које неће престати зато што га власник не врши и које би могло трајати онолико дуго колико траје и његов предмет, односно ствар на којој је засновано.

⁴² N. Anthony, *Digital Currency or Digital Control? Decoding CBDC and the Future of Money*, Washington D.C., 2024, 87.

⁴³ Право на коришћење новца је непотпуно, условно и потенцијално поништиво, за разлику од класичног права својине које је уставно заштићено и стабилно. Пуна својина подразумева право коришћења новца, уживања плодова, располагања имовином, оно је стабилно и трајно докле год је законито, док условно и реверзибилно право коришћења значи да држава или надлежни орган могу, у било ком тренутку, ограничити или блокирати приступ средствима, а услови могу бити непоштовање *ESG* стандарда, прекорачење лимита потрошње или други административни критеријуми. Ако се услови промене или наруше, право коришћења се повлачи или реверзибилно враћа држави.

⁴⁴ Central Bank of The Bahamas, *Project Sand Dollar: The Central Bank Identifies Preferred Technology Solutions Provider for Bahamas Digital Currency*, <https://www.centralbankbahamas.com/news/press-releases/project-sand-dollar-the-central-bank-identifies-preferred-technology-solutions-provider-for-bahamas-digital-currency>, датум посете: 28. 06. 2026.

услуга за недовољно услужене заједнице и социо-економске групе, смањења трошкова и повећања трансакционе ефикасности, широм Бахама. Пројекат *e-krona* у Шведској, која је глобални предводник у елиминацији физичког новца из оптицаја,⁴⁵ од 2017. године води *Sveriges Riksbank*,⁴⁶ као технократски одговор на чињеницу да приватне компаније и комерцијалне банке преузимају потпуну контролу над платним прометом. Примарни циљ је осигурати широј јавности директан приступ државном новцу у све више безготовинском друштву. Служила би као безбедна, ликвидна и универзално доступна алтернатива депозитима комерцијалних банака. Покренута 2021. године и подржана суверенитетом државе, *eNaira*⁴⁷ је прва државна дигитална валута у Африци коју, као законско средство плаћања, емитује *Central Bank of Nigeria*. Чува се у *eNaira* новчанику, користи као готовина и представља дигитални облик званичне валуте *Naira* – обрачунску јединицу, средство чувања вредности и средство размене.

Европска централна банка (*European Central Bank – ECB*) промовише дигитални евро⁴⁸ као: конвертибилну дигиталну валуту чије издавање контролише Евросистем; широко доступну под једнаким условима у свим земљама еврозоне; тржишно неутралну, поуздану и од поверења крајњих корисника. У саопштењу за јавност од 30. октобра 2025. године *ECB* наводи: припремна фаза започета у новембру 2023. године је успешно завршена; циљ нове фазе је техничка спремност за прво издавање; ако током 2026. године буде обезбеђена потребна законодавна основа, пробне активности би могле почети 2027. године, а прво издавање дигиталног евра могуће током 2029. године.⁴⁹ Систем федералних резерви (*Federal Reserve System – FRS*) опрезно приступа питању дигиталне валуте коју генерално дефинише као обавезу *FRS*, најбезбеднију дигиталну имовину доступну широј јавности без повезаног кредитног или ликвидног ризика. Документ Одбора *FRS*⁵⁰ испитује предности

⁴⁵ B. Segendorf, *How many e-krona are needed for payments?*, *Sveriges Riksbank Economic Review* No. 3, 2018, 66-78.

⁴⁶ *Sveriges Riksbank*, *E-krona*, <https://www.riksbank.se/en-gb/payments--cash/e-krona/>, датум посете: 28. 06. 2026.

⁴⁷ *Central Bank of Nigeria*, *eNaira*, <https://www.cbn.gov.ng/currency/eNaira.html>, датум посете: 28. 06. 2026.

⁴⁸ *ECB*, *Report on a digital euro*, October, 2020, https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf, датум посете: 13. 11. 2025.

⁴⁹ *ECB*, *Press Release, Eurosystem moving to next phase of digital euro project*, <https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr251030~8c5b5beef0.en.html>, датум посете: 18. 11. 2025.

⁵⁰ *FRS*, *Research & Analysis, Board of Governors of The Federal Reserve System, Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, January 2022, <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>, датум посете: 13. 11. 2025.

и недостатке потенцијалне *U.S. CBDC* и наводи потенцијалне користи, али истовремено идентификује и потенцијалне ризике⁵¹ увођења *CBDC*.

Г. Системи праћења карбонског отиска

CFTS представљају оперативне алгоритме који кроз *DW*, као интегрисан систем са *DI* и *CBDC*, омогућавају квантификацију еколошког утицаја сваке појединачне економске одлуке у реалном времену. У прилог имплементацији микро праћења емисија угљен диоксида, заговорници тврде да без прецизне фискалне и потрошачке алгоритамске метрике није могуће спречити климатски колапс. Један од најважнијих пилот пројеката, који користе као доказ ефикасности, спровео је *The Carbon Trust* у сарадњи са глобалним корпорацијама.⁵² У њему је показано како личне дозволе за угљеник могу помоћи потрошачима да разумеју како се карбонски отисак одређених производа и услуга односи на укупну дневну дозволу и како се подиже свест о одрживости.⁵³

Напредак у области свеprisутне алгоритамске инфраструктуре чини личне карбонске квоте (*Personal Carbon Allowances – PCA*)⁵⁴ технички остваривим механизмом за контролу друштвене потрошње. Процењује се да би примарни модел ових квота обухватио око 40% емисија угљеника повезаних са потрошњом енергије у земљама са високим дохотком, и то кроз директну контролу појединачног транспорта, кућног грејања и потрошње електричне енергије, чиме би се појединац позиционирао као незаобилазна карика за постизање циљева нето нулте емисије угљеника. Сматра се да је систем *PCA* далеко социјално праведнији од карбонских пореза (*Carbon Taxes – CT*). Код *PCA* система сви грађани добијају исту почетну бесплатну квоту па сиромашнији слојеви, који по правилу троше знатно мање енергије, могу

⁵¹ *Ibid.* Потенцијалне користи увођења *CBDC*, *FRS* види у: безбедном задовољавању будућих потреба и потражње за услугама плаћања; побољшању прекограничних плаћања; подршци међународној улози долара; финансијској инклузији; проширењу јавног приступа безбедном новцу централне банке, а потенцијалне ризике у: променама у структури тржишта финансијског сектора; безбедности и стабилности финансијског система; ефикасности спровођења монетарне политике; приватности и заштити података и спречавању финансијског криминала; оперативној отпорности и сајбер безбедности.

⁵² *The Carbon Trust, Personal carbon allowances white paper: How to help consumers make informed choices - exploring the concept of Personal Carbon Allowances*, <https://www.carbontrust.com/our-work-and-impact/guides-reports-and-tools/personal-carbon-allowances-white-paper>, датум посете: 28. 06. 2026.

⁵³ K. Kumar, WEF, *My Carbon: An approach for inclusive and sustainable cities*, <https://www.weforum.org/stories/2022/09/my-carbon-an-approach-for-inclusive-and-sustainable-cities/>, датум посете: 28. 06. 2026.

⁵⁴ F. Nerini et al., *Personal carbon allowances revisited*, *Nature Sustainability* No. 4, 2021, 1025–1031, <https://doi.org/10.1038/s41893-021-00756-w>, датум посете: 28. 06. 2026.

вишак карбонских јединица продати богатима.⁵⁵ Код *СТ* богати могу да плате вишу цену и наставе да загађују, док сиромашни упадају у енергетско сиромаштво.

Критичари виде *CFTS* као инфраструктуру за, до сада, најинтензивнији облик социјалног инжењеринга и потпуну промену људског понашања преласком са дисциплине на контролу и надзор. Спој *CFTS* са *DW* представља врхунац моћи државе да управља свакодневним навикама грађана. У овом концепту држава више не контролише грађане ретроактивним казнама, већ алгоритмима превентивно усмерава њихове виталне потребе, па тако карбонски отисак постаје валута преживљавања.⁵⁶ Основна грађанска права, попут слободе кретања или приватност, бивају деградирана на ниво алгоритамски условљеног приступа, чиме се успоставља нови облик социјалне стратификације у друштву техно феудализма.⁵⁷ Захваљујући технократским моделима, који предвиђају могућност трговине карбонским квотама, стварају се нови карбонски феудализам и социјална стратификација, где економски супериорни појединци могу купити карбонске кредите од сиромашних. Тиме *CFTS* у пракси репродукује и продубљује класну неједнакост – елита задржава неограничену физичку слободу и конзумеристички стил живота плаћањем еколошких пенала, док нижи друштвени слојеви бивају закључани унутар дигитално контролисаног материјалног минимализма.⁵⁸

IV КОМПАРАТИВНА АНАЛИЗА НАЦИОНАЛНИХ СТУДИЈА СЛУЧАЈА

Анализа националних студија случаја обухвата три модела: кинески, индијски и модел ЕУ. Кинески *SCS* модел инфраструктуре државног надзора⁵⁹ дизајниран је тако да функционише кроз укрштање велике количине података из приватне и јавне сфере – од историје трансакција у *DW* до свакодневног понашања у дигиталном простору. То је веома компликован систем, првенствено фокусиран на финансијске и комерцијалне активности. Даљим развојем систем отвара могућности за иновације у области велике количине

⁵⁵ W. Xu et al., *Low-carbon lifestyle revolution: China's recent progress toward a personal carbon market*, PLOS Sustain Transform Vol. 2 No. 10, 2023., e0000079, <https://doi.org/10.1371/journal.pstr.0000079>, датум посете: 28. 06. 2026.

⁵⁶ Ако софтвер усклади дигитални новчаник тако да се након прекорачења месечне карбонске квоте аутоматски блокира куповина одређеног добра, право на слободу кретања престаје да буде уставна категорија и постаје алгоритамска привилегија.

⁵⁷ J. Варуфакис, *Технофеудализам*, Земун, 2025, 82-85.

⁵⁸ R. Starkey, *Personal carbon trading: A critical survey: Part 1: Equity*, Ecological Economics Vol. 73, 2012, 7-18, <https://www.sciencedirect.com/science/article/abs/pii/S0921800911003983>, датум посете: 28. 06. 2026.

⁵⁹ F. Liang et al., *Constructing a Data - Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, Policy & Internet Vol. 10 No. 4, 2018, 434-435.

података који постају нови драгоцен ресурс. Циљ изградње SCS је централизовање платформе велике количине података у инфраструктуру надзора, како би се пратило, предвиђало и управљало понашање грађана, корпорација, организација и државне администрације у Кини. Систем кажњавања/награђивања, заснован на кредитним резултатима, одређује да ли грађани и организације могу да приступе јавним услугама и системској инфраструктури. Тиме је успостављена дигитална архитектура у којој право на физичку мобилност и потрошњу више није подразумеван грађански избор, већ државно условљена привилегија која се аутоматски администрира кроз систем технократске контроле. Иако би било за очекивати да друштвено напреднији и информисанији грађани буду највише забринуте због последица SCS по приватност, они лакше прихватају SCS дајући им предност, кроз оквире стварања користи и промовисања поштењег пословања у друштву и економији, у односу на кршење приватности.⁶⁰

Модел централизоване технократске ефикасности кроз биометријски систем *Aadhaar*, путем отисака прстију и скенирања зенице, покренут је у Индији 2009. године под прогресивним технократским наративом стварања инклузивнијег и ефикаснијег система социјалне помоћи (посебно за становништво које није поседовало формалне идентификационе документе), модернизације јавне управе и административне транспарентности. Међутим, у пракси је демонстрирао другу димензију алгоритама контроле – транзицију са државног дисциплиновања на егзистенцијално условљавање.⁶¹ Иако се, са становишта јавне политике, *Aadhaar* често наводи као пример успешне примене дигиталног идентитета у циљу укључивања великог броја грађана у формалне економске токове, систем је истовремено постао предмет бројних критика. Указивало се на ризике повезане са централизацијом биометријских података, потенцијалним нарушавањем приватности и могућим искључењима корисника услед инфраструктурних дефеката у процесу идентификације.⁶² Изван ове дигиталне архитектуре нема социјалне сигурности нити економске егзистенције. Системска грешка у алгоритму или читавању података не представља само привремену техничку сметњу, већ производи реално изопштење из друштвеног и биолошког живота.⁶³

⁶⁰ G. Kostka, *China's social credit systems and public opinion: Explaining high levels of approval*, New Media & Society Vol. 21 No. 7, 2019, <https://doi.org/10.1177/1461444819826402>, датум посете: 28. 06. 2026.

⁶¹ R. Khera, *Dissent on Aadhaar: Big Data Meets Big Brother*, Hyderabad, 2018, 13-14.

⁶² J. Drèze et al., *Aadhaar and Food Security in Jharkhand: Pain Without Gain?* Economic & Political Weekly Vol. 52 No. 50, 2017, 59.

⁶³ R. Khera, *Aadhaar: Uniquely Indian Dystopia?*, Economic sociology the european electronic newsletter Vol. 21 No. 1, 2019, 4-12. У раду се истиче да је *Aadhaar* временом постао *de facto* обавезан за приступ социјалним давањима. Званичници, задужени за спровођење пројекта открили су да су користили три стратегије: урадити брзо не остављајући људима време да схвате последице; урадити неприметно и створити

За разлику од претходна два модела – отвореног државног дисциплиновања у Кини или сировог егзистенцијалног условљавања у Индији, модел ЕУ карактерише специфична технократска софистицирана архитектура добровољне конвергенције засноване на јавно–приватном партнерству. Европски новчаник за *DI – EUDI Wallet* се не представља као отворена државна директива, већ као прогресивна платформа за административно олакшавање живота грађана кроз наратив о практичности, модернизацији, безбедности и неутралним еколошким циљевима.⁶⁴ Критичка анализа дигиталне архитектуре уочава како се кроз њу ствара префињени амбијент у којем се неприхватање *DW* или неодговорно еколошко понашање појединца не кажњава физички, већ га води у постепено економско и функционално искључење из друштвених токова. Истовремено, елита, кроз тржишне механизме, задржава своју конзументичку слободу. Спајањем званичних државних докумената, финансијских трансакција и приватних технолошких чворишта ствара се структура суптилног условљавања. Проблем заштите приватности се може решити у процесу дизајнирања система – као што се технологија може користити за нарушавање приватности појединца, може се користити и за његову заштиту.⁶⁵

Упоредни преглед кинеског, индијског и модела ЕУ открива да, упркос фундаменталним разликама у политичким идеологијама и институционалним наративима, сва три система деле заједничку функционалну суштину – употребу дигиталне архитектуре за управљање становништвом. Ова три модела не представљају изоловане феномене, већ три различита технократска одговора на комплексне изазове безбедности, економије и управљање ресурсима у XXI веку. У сва три система присутна је трансформација легитимитета и моћи кроз различите механизме: кинески модел отворено користи државни суверенитет и легитимизује се кроз наратив о друштвеној хармонији, индијски модел свој легитимитет црпи из обећања о социјалној инклузији и ефикасности, модел ЕУ наступа под наративом заштите грађанских права и заштите приватности. Оно што их повезује је сужавање простора за избор појединца. Без обзира да ли је механизам изражен кроз експлицитне државне декрете, законску обавезу биометријске идентификације или кроз правно–техничке стандарде, резултат на институционалном нивоу је

коалицију за *Aadhaar* како би брзо постигли велики успех тако да повраћај на старо изгледа немогућ. За реализацију стратегије коришћени су огласи, брендирање, етикетирање, контрола штете, подметање прича, манипулисање насловима, спонзорисана истраживања.

⁶⁴ European Commission, *European Digital Identity Wallet*, <https://digital-strategy.ec.europa.eu/en/factpages/european-digital-identity-wallet>, датум посете: 28. 06. 2026.

⁶⁵ J.-H. Hoepman, *Privacy Is Hard and Seven Other Myths: Achieving Privacy through Careful Design*, Cambridge, 2023, 213-215.

исти – успостављање централизованих или децентрализованих дигиталних система који посредују између човека и његових права.

У ПРАВНИ И ЕТИЧКИ ОКВИР ДИГИТАЛНЕ ИНФРАСТРУКТУРЕ

Савремени правни и етички оквир дигиталног друштва развија се као одговор на изазов: Како омогућити технолошке иновације без стварања инфраструктуре која би могла угрозити основна људска права и слободе? Право на приватност представља једно од основних људских права⁶⁶ признатих у бројним међународним документима. Право на приватност је традиционално било повезано са заштитом приватног живота од неовлашћеног мешања државе. У дигиталном окружењу његов значај је проширен на питања прикупљања, обраде, складиштења и дељења података. Савремени системи *DI*, *DW* и *CBDC* инфраструктуре генеришу велике количине података о понашању грађана, због чега право на приватност постаје један од централних механизма заштите грађана у дигиталном друштву.⁶⁷ Општа уредба о заштити података (*General Data Protection Regulation – GDPR*)⁶⁸ представља најзначајнији нормативни оквир за заштиту личних података у ЕУ. Заснива се на неколико кључних принципа: законитост обраде, ограничење сврхе, минимизација података, тачност података, ограничење периода чувања, интегритет и поверљивост, одговорност руковаоца подацима.

Посебан значај за анализу дигиталне инфраструктуре има принцип минимизације података. Он полази од претпоставке да се ризици надзора повећавају сразмерно количини и разноврсности прикупљених података, те се могу прикупљати само они подаци који су неопходни за остваривање конкретне и легитимне сврхе. У контексту *DI* и *CBDC* система то значи да техничка могућност прикупљања великог броја података не представља сама по себи правни основ за њихову обраду, чиме *GDPR* поставља важну границу између технолошке способности и правне дозвољености. У пракси то подразумева прикупљање најмање могуће количине података, орочавање

⁶⁶ М. Рапajiћ, D. Logarušić, *The Concept of Human Rights and the Rights of National Minorities in the Serbian Constitution*, Kultura polisa Vol. 22 No. 2, 2025, 82–93, 83. Аутори истичу да су људска права независна од воље државе или било које друге власти, да их људима не даје милосрдна државна власт, нити их немилосрдна власт може одузети и да је појединачно људско биће господар својих права, чак и када она нису предвиђена уставом или другим законским актима.

⁶⁷ European Court of Human Rights - Council of Europe, *European Convention on Human Rights*, https://www.echr.coe.int/documents/d/echr/convention_ENG, датум посете: 28. 06. 2026.

⁶⁸ GDPR.EU, *General Data Protection Regulation (GDPR)*, (EU) 2016/679, <https://gdpr.eu/tag/gdpr/>, датум посете: 28. 06. 2026.

периода чувања, децентрализовано складиштење, селективно дељење информација, анонимизацију и псеудонимизацију података.⁶⁹

Поред традиционалних права, последњих година све више се говори о концепту дигиталних права под којима се најчешће подразумевају право на заштиту података, право на дигиталну приватност, право на транспарентност алгоритама, право на објашњење аутоматизованих одлука, право на дигиталну инклузију, право на сајбер безбедност, право на дигиталну аутономију – право грађана да задрже контролу над сопственим подацима и дигиталним идентитетом.⁷⁰ Развој система вештачке интелигенције (*Artificial Intelligence – AI*) отворио је нова питања у области дигиталних права, из којих разлога је ЕУ усвојила *AI Act*⁷¹, као први свеобухватни регулаторни оквир за употребу система *AI*. Основна логика овог акта заснива се на процени ризика. Системи се класификују као минимално ризични, ограничено ризични, високо ризични и неприхватљиво ризични. Посебно су значајне одредбе које се односе на биометријску идентификацију, профилисање грађана, аутоматизовано доношење одлука, системе социјалног бодовања. *AI Act* представља покушај спречавања развоја алгоритамских система који би могли довести до дискриминације или прекомерне контроле грађана.

Иако се савремени дигитални системи у великој мери ослањају на концепт пристанка корисника, формални пристанак често не представља стварни израз слободног избора. Корисници се у пракси суочавају са сложеним условима коришћења, недостатком разумљивих информација, несразмером моћи између грађана и институција, немогућношћу коришћења услуге без прихватања услова. Због тога се све више пажње посвећује концепту сагласности који се односи на начин дизајнирања механизма пристанка.⁷² Циљ овог приступа није само формално прибављање сагласности, већ обезбеђивање стварног разумевања и контроле над подацима. Најсложеније питање савремене дигиталне трансформације односи се на границу између легитимног управљања и прекомерне контроле. Иако државе имају легитиман интерес да осигурају безбедност, спрече финансијски криминал и побољшају јавне услуге, истовремено исти технички механизми могу бити употребљени за масовно праћење, профилисање, дискриминацију и политичку злоупотребу података.

⁶⁹ *Ibid.*

⁷⁰ J. E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford, 2019, 238-268.

⁷¹ EU Artificial Intelligence Act, *The EU Artificial Intelligence Act: Up-to-date developments and analyses of the EU AI Act*, <https://artificialintelligenceact.eu/>, датум посете: 28. 06. 2026.

⁷² H. Nissenbaum, *Privacy in Context, Technology, Policy, and the Integrity of Social Life*, Stanford, 2009, 129-139.

VI МОДЕЛИ ЗАШТИТЕ ГРАЂАНА У ДИГИТАЛНОЈ ИНФРАСТРУКТУРИ

Док правни оквири *GDPR* и *AI Act* дефинишу норме понашања, савремена дебата о дигиталним системима све више се помера ка питању архитектуре самих система јер заштита грађана се не може заснивати на накнадној правној контроли, већ мора бити уграђена у дизајн дигиталне инфраструктуре. Најзначајнији модели заштите су децентрализовани идентификатор (*DID*) и самостални дигитални идентитет (*SSI*). У овим моделима корисник контролише своје акредитиве, подаци нису централизовано складиштени, верификација се врши криптографским путем, минимизује се размена личних података, омогућава се селективно откривање података. Овај приступ значајно смањује ризик од масовног профилисања јер не захтева централизоване базе података као у класичним моделима *DI*.⁷³ У контексту интегрисане дигиталне инфраструктуре *DI-DW-CBDC-CFTS*, *DID* и *SSI* модели представљају кључни механизам раздвајања идентитета од трансакционих података. Основни принцип архитектуре система у концепту дизајниране приватности укључује минимизацију прикупљања података, енкрипцију по подразумеваној поставци, децентрализовано складиштење, аутоматску анонимизацију, ограничење приступа подацима. Тиме дизајнирана приватност помера одговорност са корисника на дизајнере система и институције које их имплементирају.⁷⁴

Системи децентрализованих финансија (*DeFi*) заснивају се на *blockchain* архитектури и паметним уговорима, при чему безбедност не произилази из поверења у централизованог посредника већ из криптографских механизма, дистрибуираног консензуса и транспарентности извршавања програмског кода. Основни механизми заштите обухватају криптографско потписивање трансакција, непроменљивост записа у *blockchain* архитектури, децентрализовану валидацију, формалну верификацију паметних уговора и њихову независну безбедносну ревизију.⁷⁵ Пракса показује да највећи ризик не представља сама инфраструктура, већ пропусти у имплементацији паметних уговора, грешке у дизајну протокола и експлоатација економских слабости, због чега се безбедност *DeFi* система све више посматра као комбинација криптографске сигурности и поузданог софтверског инжењеринга.⁷⁶

⁷³ C. Allen, *The Path to Self-Sovereign Identity*, 2016, <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>, датум посете: 28. 06. 2026.

⁷⁴ A. Cavoukian, *Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*, Information & Privacy Commissioner, Ontario, 2011, 2.

⁷⁵ R. Auer et al., *The Technology of Decentralized Finance (DeFi)*, BIS Working Papers No. 1066, Basel, 19 January 2023, 3-7.

⁷⁶ Y. Wang et al., *A Survey of DeFi Security: Challenges and Opportunities*, Journal of King Saud University – Computer and Information Sciences Vol. 34 No. 10, 2022, 10378–10404, <https://doi.org/10.1016/j.jksuci.2022.10.028>, датум посете: 28. 06. 2026.

У савременим *DeFi* системима, један од најзначајнијих механизма заштите приватности представља доказивање без откривања података (*ZKP*).⁷⁷ Најзаступљенији протоколи заштите приватности су *zk-SNARK* и *zk-STARK*.⁷⁸ Протокол *zk-SNARK* захтева дугу иницијалну процедуру успостављања поверења уз веома мале доказе и брзу верификацију, док *zk-STARK* елиминише потребу за оваквом почетном фазом и нуди већу отпорност на нападе по цену већих доказа и већих рачунарских захтева. Избор конкретног механизма зависи од односа између нивоа приватности, скалабилности и рачунарске ефикасности који се жели постићи у одређеном систему.

Када се ради о техничким механизмима очувања приватности, један од најзначајнијих је *off-line* функционалност *CBDC* система. Његове основне функције су да омогућава трансакције без сталне конекције, смањује тренутну видљивост трансакција централном систему, симулира функционалност готовине и повећава отпорност система у кризним ситуацијама.⁷⁹ Иако *off-line CBDC* систем не обезбеђује потпуну анонимност нити трајно онемогућава анализу трансакција, његова архитектура уводи временски и технички слој раздвајања између извршења трансакције и њене регистрације у централном систему.⁸⁰ Пошто се трансакције синхронизују тек након поновног успостављања мрежне везе, надзор у реалном времену није могућ, већ се контрола и аналитичка обрада података спроводе накнадно. Такав модел значајно умањује могућност непосредног праћења понашања корисника, иако не искључује *ex post* анализу ради испуњавања безбедносних и регулаторних захтева.⁸¹

За спречавање злоупотребе дигиталне инфраструктуре изузетно важан услов је и постојање независних регулаторних тела са надлежностима у области заштите података, надзора алгоритама, ревизије *CBDC* система, контроле интероперабилности података, санкционисања злоупотреба. Посебно је важно да ове институције буду институционално независне, финансијски стабилне, технички оспособљене и транспарентне у раду. Европски модел, кроз

⁷⁷ R. Shashidhara, R. Nair Chirakarotu, P. Panakalapati, *Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions*, Security and Privacy Vol 8 Issue 1, 2025, e461, <https://doi.org/10.1002/spy2.461>, датум посете: 28. 06. 2026.

⁷⁸ B. O. Roelink, M. El-Hajj, D. Sarmah, *Systematic Review: Comparing zk-SNARK, zk-STARK, and Bulletproof Protocols for Privacy-Preserving Authentication*, Security and Privacy Vol. 7 Issue 5, 2024, 12-13.

⁷⁹ R. Auer et al., *Project Polaris: Handbook for Offline Payments with CBDC*, Basel, 2023, 19-20.

⁸⁰ Bank for International Settlements, *Project Polaris Part 1: A handbook for offline payments with CBDC*, Basel, 2023.

⁸¹ Ова карактеристика је кључна за очување минималног нивоа финансијске анонимности у дигиталним системима.

тела попут *Data Protection Authorities*, представља један од најразвијенијих примера оваквог приступа.⁸²

Питање програмабилности новца⁸³ је једна од најконтроверзнијих тема везана за *CBDC*. Иако програмабилност може имати легитимне примене попут циљаних социјалних трансфера, постоји ризик да се користи за ограничење врсте потрошње, временска ограничења приступа средствима, географска ограничења, условљавање понашања. Због тога се намеће потреба нормативне забране дискреционог ограничења потрошње од стране државе или приватних оператера. То би подразумевало да новац мора задржати заменљивост, да средства не могу бити условљена понашањем корисника, да сва ограничења морају бити експлицитно законски дефинисана и судски контролисана.

Са ширењем алгоритамског одлучивања у финансијским и јавним системима, транспарентност постаје кључни заштитни механизам. Основни елементи укључују право корисника да зна да ли се користи алгоритам, право на објашњење одлуке, могућност оспоравања аутоматизованих одлука, реверзибилност алгоритама. Овај принцип је директно повезан са одредбама *GDPR* о аутоматизованом одлучивању, као и са *AI Act* регулативом. У контексту интегрисане дигиталне инфраструктуре, алгоритамска транспарентност је кључна да спречи црне кутије управљања понашањем.

Право на недигитални приступ услугама је један од најважнијих, али често занемарених аспеката дигиталне трансформације. Ово право подразумева да грађани морају имати могућност да приступе основним јавним услугама без дигиталног идентитета, користе алтернативне механизме плаћања, избегну искључење из система због технолошких баријера, задрже физичке или аналогне форме комуникације са институцијама. Овај принцип је кључан за спречавање дигиталне дискриминације и принудне дигитализације друштва. У теоријском смислу, право на аналогну алтернативу представља један од последњих механизма очувања стварне слободе избора у дигиталном друштву.⁸⁴

⁸² European Data Protection Board, *Guidelines on Data Protection by Design and by Default*, Guidelines 4/2019 on Article 25, 2020.

⁸³ Програмабилност новца представља функционалну способност дигиталне новчане инфраструктуре да у правила преноса или употребе новчане вредности угради унапред дефинисане услове чије се испуњење може аутоматски проверавати и извршавати посредством софтверског кода или паметних уговора. Потребно је направити разлику између програмабилних плаћања, (аутоматски пренос средства на основу унапред одређених услова) и програмабилног новца (ограничење коришћења): О. Freiman, *CBDC Governance: Programmability, Privacy and Policies*, Centre for International Governance Innovations, Digital Policy Hub – Working Paper, Waterloo, 2024, 8-10.

⁸⁴ Н. Dubois, С. Peroni, *Digitalisation of social protection*, Luxembourg, Publications Office of the European Union, 2025, 3.

VII ЗАКЉУЧАК

Анализа четири стуба дигиталне инфраструктуре – *DI*, *DW*, *CBDC* и *CFTS* и њихове интеграције у јединствен дигитални инфраструктурни систем показује да се одвија трансформација незамисливих размера, која не представља само технолошку иновацију и корак напред у развоју друштва, већ постаје платформа за дубоке промене у свим сферама људске егзистенције.

DI постаје инструмент дефинисања грађанских права, а не само средство идентификације. Као предуслов за приступ јавним сервисима, *DI* ствара нову форму зависности грађанина који постаје везан за технолошку инфраструктуру, опредељујућу за статус унутар друштвене заједнице. У драстично промењеном концепту суверенитета, грађанин престаје да буде носилац права и постаје корисник система чија се егзистенција непрестано одобрава и/или условљава. Када се централизује, *DI* се повезује са осетљивим базама података, а ако изостану јасни правни оквири заштите приватности, постаје инструмент надзора.

DW није само апликација за плаћање, већ централно корисничко чвориште у којем се преплићу идентитет, новац, јавна администрација, регулаторни оквири и надзорне могућности. Кроз паметне уговоре, *DW* на заједничкој дигиталној платформи спаја новац, имовину и информације. Повезујући идентитетске, финансијске и административне функције у јединствен систем, *DW* постаје контролни али и најосетљивији стуб интегрисане дигиталне инфраструктуре.

CBDC, као најзначајнији структурни елемент дигиталне трансформације финансијских система, представља истовремено највећу иновацију и највећи изазов јер добија димензије моћи коју ниједан постојећи облик новца није омогућавао. Јавности се *CBDC* представљају као валуте које доносе ефикасније системе плаћања, већу монетарну стабилност, сузбијање нелегалних финансијских трансакција и лакша међународна плаћања. Међутим, *CBDC* доносе и могућност превеликог државног увида у финансијски живот грађана. Присутна је реална опасност да новац постане програмабилан по времену, намени, условима исплате, аутоматским радњама, локацији или индивидуалном профилу корисника.

Подстакнути глобалним *ESG* трендовима и климатском политиком, *CFTS* у почетку делују као инструмент одговорне еколошке политике. Међутим, дубље посматрање проблема доводи до закључка да могу постати основа за увођење персонализованих еколошких квота, климатских кредита и профилисање грађана. Еколошка политика, која би требало да буде транспарентна и контролисана, прелази на ниво технократског управљања у којем, уместо човека, алгоритми процењују и санкционишу понашање.

Ако се *DI*, *DW*, *CBDC* и *CFTS* интегришу у јединствену дигиталну инфраструктуру, могуће је формирање алгоритамског екосистема који повезује лични идентитет, финансијске токове и еколошке норме у једну свеобухватну

архитектуру управљања. Опасност настаје када се технологија развија без надзора, транспарентности и јасних механизма заштите права грађана. Уколико не постоје чврсти правни оквири који ће обезбедити да дигиталне технологије остану у служби друштва, а не његова надзорна инструментализација, не буду успостављене независне институције које могу контролисати како државу тако и корпорације, и не буду изграђени модели заштите приватности грађана, дигитална инфраструктура се лако може претворити у инструмент моћи и доминације.

Nebojša M. Petković, PhD*

**DIGITAL IDENTITY, DIGITAL WALLET, CENTRAL BANK
DIGITAL CURRENCY AND CARBON FOOTPRINT TRACKING
SYSTEMS – USEFUL TECHNOLOGY OR INFRASTRUCTURE
FOR CONTROL AND SURVEILLANCE?**

Summary

The subject of this paper is the analysis of the relationship between digital identity, digital wallet, central bank digital currency and carbon footprint tracking systems, as key components of a modern digital infrastructure and their convergence into a single digital infrastructure. Although these technologies are most often presented as a means of modernizing public administration, increasing financial inclusion and supporting sustainable development goals, their increasing integration raises significant questions related to privacy protection, concentration of power and the possibility of institutional oversight. Through a comparative analysis of national case studies and relevant normative frameworks, the author seeks to critically examine the balance between the beneficial effects and potential dangers of these four pillars of digital architecture, to point out legal and ethical dilemmas and to identify models for protecting citizens from abuse.

Digital identity, as a set of data and digital attributes that enable the identification of an individual in an electronic environment, constitutes the first constitutive pillar in the digital architecture through which the analog individual becomes visible to the system. As a prerequisite for access to public services, digital identity creates a new form of citizen dependence, which

* Teacher at the School of Economics in Niš, court expert for the economic and financial field.

becomes tied to the technological infrastructure, determining the status within the social community. In a drastically changed concept of sovereignty, the citizen ceases to be a holder of rights and becomes a user of a system whose existence is constantly approved and/or conditioned. The digital wallet represents a central user hub that connects identity, financial and administrative functions into a single system. It is the most sensitive pillar of the integrated digital infrastructure and its control component. It enables access to public services and system infrastructure, and at the same time represents a potential source of risk due to data collection and the possibility of monitoring financial activities.

The central bank digital currency, as the most important structural element of the digital transformation of financial systems, represents both the greatest innovation and the greatest challenge, as it gains dimensions of power that no existing form of money has ever enabled. A common feature of all digital currency models, developed by central banks around the world, is the possibility of increasing surveillance over the individual, centralization of economic power, and potential manipulation of payment systems. Although initially carbon footprint tracking systems, driven by global trends and climate policy, act as an instrument of responsible environmental policy, they can become the basis for the introduction of personalized environmental quotas, climate credits, and citizen profiling.

If digital identity, digital wallet, central bank digital currency, and carbon footprint tracking systems are integrated into a single digital infrastructure, it is possible to form an algorithmic ecosystem that connects personal identity, financial flows, and environmental norms into a single comprehensive governance architecture. The danger arises when technology develops without oversight, transparency, and clear mechanisms to protect citizens' rights. Unless there are solid legal frameworks in place to ensure that digital technologies remain at the service of society, rather than its surveillance instrumentalization, unless independent institutions are established that can control both the state and corporations, and unless models for protecting citizens' privacy are built, then digital infrastructure can easily be turned into an instrument of power and domination.

Key words: Digital Identity, Digital Wallet, Central Bank Digital Currency, Carbon Footprint Tracking Systems, Social Credit System, Digital Surveillance.