Немања ЈАНКОВИЋ[*]
Правни факултет
Универзитет у Крагујевцу

УДК 342.7(4-67 EU)
DOI: 10.5937/adpn2601067J
Прегледни рад

ПАМЕТНИ УГОВОРИ У ПРАВУ ЕВРОПСКЕ УНИЈЕ[**]

Сажетак

Паметни уговори представљају својеврсни спој технологије и права. Реч је о уговорима који се аутоматски извршавају и који су, захваљујући блокчејн технологији, релативно непроменљиви. Због аутоматизације и непроменљивости, паметни уговори су користан инструмент савременог дигиталног промета. На нивоу Европске уније, паметни уговори су детаљно уређени Уредбом бр. 2023/2854 о фер приступу и употреби података. У првом делу рада, аутор анализира појам паметних уговора, уз кратко објашњење блокчејн технологије која је у основи паметних уговора. У другом делу рада, аутор анализира законодавства држава чланица Европске уније у вези паметних уговора пре усвајања поменуте Уредбе. Централни део рада посвећен је анализи одредаба Уредбе бр. 2023/2854 које се тичу паметних уговора, а нарочито битних услова у погледу паметних уговора за извршавање споразума о дељењу података и поступка оцењивања усклађености паметног уговора са наведеним битним условима. У закључку, аутор разрађује тезу да ново законодавство Европске уније које се односи и на паметне уговоре, представља квалитативни скок у односу на дотадашња решења, јер детаљно уређује нека од најзначајнијих питања која се тичу функционисања паметних уговора и пружа одговарајуће правне и техничке гаранције успешне примене паметних уговора.

---

[*] Аутор је асистент Правног факултета Универзитета у Крагујевцу. Електронска адреса аутора: njankovic@jura.kg.ac.rs, ORCID: https://orcid.org/0009-0008-5083-9513.

[**] Рад је резултат научноистраживачког рада аутора у оквиру Програма истраживања Правног факултета Универзитета у Крагујевцу за 2026. годину, који се финансира из средстава Министарства науке, технолошког развоја и иновација Републике Србије.

Кључне речи: паметни уговори, блокчејн технологија, право Европске уније, Уредба о подацима ЕУ, споразум о дељењу података

1. УВОД – ПОЈАМ И ЗНАЧАЈ ПАМЕТНИХ УГОВОРА

Идејни творац паметних уговора је информациони научник и правник Ник Сабо (*Nick Szabo*), који је у свом чланку из 1996. године изложио основне поставке паметних уговора. Сабо полази од претпоставке да ће будући развој технологије довести до аутоматизације уговорних односа. Ове идеје су биле напредније од стања технике тог времена. Сабо паметне уговоре дефинише као скуп обећања одређених у дигиталној форми, укључујући протоколе које стране извршавају на тим обећањима (Szabo 1996, 50). Основна идеја која стоји иза паметних уговора је да велики број уговорних одредаба може бити уграђен у хардверске и софтверске системе, на такав начин да се тиме кршење уговора учини прохибитивно скупим за ону уговорну страну која жели да прекрши своју уговорну обавезу (Szabo 1996, 50). Сабо нуди још једну дефиницију паметних уговора, као компјутерског протокола за реализацију трансакције у складу са условима уговора, при чему је основни циљ паметних уговора: да се обезбеди извршење одредби уговора, минимализује потреба за непристрасним посредницима и смање губици због превара, трошкова извршења и решавања спорова, као и други трансакциони трошкови (Цветковић, 2021, 64). Паметни уговори су новина у свету технологије и права који омогућавају брже и ефикасније закључење и извршење уговора. Основни начин остваривања ових циљева је аутоматизација свих фаза уговорног односа. Наиме, код паметних уговора, поступак од закључења до извршења одвија се аутоматизовано, без потребе за додатном интервенцијом уговорних страна.

У основи паметних уговора је блокчејн (*blockchain*) технологија. Реч је о технологији која се заснива на коришћењу криптографски заштићеног ланца трансакционих блокова. Те трансакције се групишу у блокове, који се даље везују у ланац, и то криптографски кроз хеш функцију (*hash function*). Након тога, садржај блокова више се не може променити, а да се не промени садржај свих других блокова који му претходе (Цветковић 2020, 128). Ланци даље граде

још сложенију целину – мрежу. Мрежа се састоји од чворова. Сваки чвор садржи целовити запис о свим подацима који су икада забележени у том блокчејну (Глушац 2022, 431). Не постоји територијална веза чвора и неког подручја – чвор се може налазити апсолутно било где на свету. Две важне особине блокчејн технологије су непроменљивост и непосредност.

Повезаност информација у блокове, који даље граде ланац, омогућила је непроменљивост блокчејна. Наиме, нове информације се уносе у блок у који су већ смештене старије и раније верификоване информације које заједно граде један блок, а цео један блок садржи податке о претходном блоку у ланцу. То значи да је, приликом уношења нове информације у блок, неопходно да нова информација буде верификована од стране мреже, кроз тзв. консензус механизам. Свака промена садржаја једног блока у ланцу аутоматски узрокује промену на сваком наредном блоку у ланцу. Блокови су међусобно криптографски повезани. Верификација информације у ланцу се врши коришћењем криптоване сигнатуре. Дакле, непроменљивост блокчејна треба схватити у релатвном смислу. Блокчејн је немогуће променити без верификације од стране мреже, што значи да је неовлашћена промена информација практично немогућа.

Непосредност се огледа у чињеници да блокчејн функционише као *peer-to-peer* мрежа. То је још једна револуционарна новина коју блокчејн доноси са собом. Већина других мрежа, заснованих на класичним технологијама, су централизоване. То значи да постоји главни рачунар на серверу (администратор) који контролише и бележи активности свих осталих учесника и посредује у њиховој комуникацији. У контексту блокчејна, ситуација је знатно другачија, управо захваљујући *peer-to-peer* мрежи, којом се обезбеђује комуникација без било каквих посредника. Притом, ово не значи да је сваки учесник директно повезан са сваким другим учесником, већ директна веза постоји са свега неколико њих, а са свима осталима веза је посредна (Матановић 2022, 5).

Кључне предности паметних уговора у односу на класичне уговоре су: умањење ризика (због непроменљивости блокчејн ланца), смањење административних и услужних трошкова (нема потребе за посредником) и већа ефикасност пословања (peer-to-peer трансакције) (Zheng et al. 2020, 476). Паметни уговори се могу користити у банкарском пословању, осигурању, здравству, регули-

сању јавних набавки и другим областима.[1] Ипак, примена паметних уговора носи и ризике: проблем је утврдити идентитет уговорних страна, што може имати утицај на пуноважност уговора; заштита личних података на мрежи; немогућност измене уговорних одредаба; проблем кодирања правничких термина (нарочито правних стандарда); проблем неизвршења или неуредног извршења уговорних престација, које су аутоматизоване.

2. ПРЕГЛЕД СТАЊА У ЕВРОПСКОЈ УНИЈИ ПРЕ УРЕДБЕ О ПОДАЦИМА ЕУ

Прва држава која је правно препознала паметне уговоре је Малта. Наиме, на Малти је Законом о дигиталној имовини (*Virtual Financial Assets Act*) од 1. новембра 2018. године паметни уговор нормиран као облик технолошког споразума који се састоји од:

а) компјутерског протокола;

б) споразума закљученог, делимично или у целости, у електронској форми, који је аутоматизован и извршив преко компјутерског кода, иако неки делови могу захтевати људску активност и контролу и који могу бити извршиви уобичајеним правним средствима или комбинацијом оба метода.

Путем Малте је убрзо кренула и Италија. Наиме, у Италији је 14. децембра 2018. године, председник Републике Италије, потписао Уредбу број 135/18 о хитној подршци поједностављивању система пословања и јавне управе (*Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione*). Овом уредбом су паметни уговори дефинисани као компјутерски програми који раде на основу дистрибуиране базе података чије извршење аутоматски обавезује две или више страна сходно ефектима које су странке раније уговориле. Посебан значај ове уредбе је у томе што садржи одредбу којом је установљено правило да паметни уговор испуњава услов постојања писане форме у ситуацији када је законом таква форма предвиђена као обавезна (Durovic & Lech 2019, 82). Овакво решење италијанског законодавца је значајно, јер је на једноставан начин решен проблем форме који је у теорији паметних уговора више пута постављан и који ће се сигурно јављати

[1] За конкретне начине примене паметних уговора у овим областима, видети: Jan et al. 2026; Borselli 2019; Vargas & Mira da Silva 2023; Sava & Dragos 2022.

у судској пракси. Свест о томе да паметни уговор испуњава услов форме, онде где се тај услов поставља, ће само додатно појачати пажњу уговорних страна приликом закључења паметног уговора.

Овакво правно уређење паметних уговора у националним законодавствима појединих држава чланица ЕУ показује тенденцију ка правном препознавању паметних уговора, али се своди на сумарно одређивање појма паметних уговора, без детаљнијег уређења појединих проблема који се у пракси могу јавити. Те празнине су попуњене у законодавству Европске уније.

3. ПАМЕТНИ УГОВОРИ У УРЕДБИ О ПОДАЦИМА ЕУ

Потреба за правним уређењем паметних уговора на нивоу Европске уније је настала услед пораста броја прекограничних трансакција у државама чланицама (Volos 2020, 567). Европски парламент и Европски савет су 13. децембра 2023. године усвојили Уредбу бр. 2023/2854 о фер приступу и употреби података (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828). Ова Уредба је познатија под називом Уредба о подацима Европске уније (*EU Data Act*). Ступила је на снагу 11. јануара 2024. године, али се већина одредаба примењује од 12. септембра 2025. године. Циљ Уредбе о подацима је да утврди усклађеност правила о: доступности података о производу и повезаних услуга кориснику повезаног производа или повезане услуге; доступности података од стране власника података примаоцима података; доступности података од стране власника података јавним институцијама, Комисији, Европској централној банци и телима Уније, када постоји изузетна потреба за тим подацима ради обављања одређеног задатка у јавном интересу. Додатни циљеви уредбе су и: олакшавање преласка између услуга обраде података; увођење заштитних мера против незаконитог приступа подацима који нису лични подаци од стране трећих страна; и развој стандарда интероперабилности за приступ, пренос и коришћење података (став 5 преамбуле Уредбе о подацима).

Када је о паметним уговорима реч, један од главних циљева Уредбе о подацима је утврђивање усклађених правила, између ос-

талог, и о развоју стандарда интероперабилности за приступ подацима, пренос података и употребу података, при чему је интероперабилност дефинисана као способност два или више простора података или комуникацијских мрежа, система, повезаних производа, апликација или компоненти да размењују и користе податке ради обављања својих функција (чл. 2 ст. 1 тач. 40 Уредбе). С тим у вези, паметни уговори су уређени поменутом Уредбом као један од начина за постизање интероперабилности алата за аутоматизовано извршавање споразума о дељењу података (*data sharing agreement*). Осим тога, паметни уговори су препознати и као једна од мера техничке заштите које држалац података (*data holder*) може применити како би спречио неовлашћен приступ подацима, укључујући метаподатке (чл. 11 Уредбе). Паметни уговори имају потенцијал да обезбеде да се услови за дељење података поштују. Стога су они од посебног значаја за трансфер података и удруживање података, јер могу да улију поверење држаоцима података и примаоцима података како би споразуми о дељењу података били успешно извршавани (Forum 2022, 20).

Уредбом о подацима је паметни уговор је дефинисан као рачунарски програм који се употребљава за аутоматско извршење споразума или дела споразума, при чему се употребљава низ електронских записа података и осигурава њихова целовитост и тачност хронолошког редоследа (чл. 2 ст. 1 тач. 39 Уредбе). Оваква дефиниција паметних уговора је технолошки неутрална, али делује и да јој недостаје правна компонента. Наиме, у контексту блокчејна, само они паметни уговори који подразумевају претходни договор између страна могу бити у складу са дефиницијом из Уредбе (Olivieri et al. 2024, 7). Из овакве дефиниције паметног уговора, може се закључити да, у Европској унији, пуноважан паметни уговор не може да постоји без претходно сачињеног класичног уговора. Заправо је смисао постојања паметног уговора аутоматско извршење, у целини и делимично, раније закљученог уговора. Овакво правно уређење паметних уговора наводи нас на закључак да је европски законодавац паметни уговор приближио технолошком инструменту за извршење ранијег уговора, који је потребно извршити на блокчејн мрежи.

Кључна одредба која се тиче паметних уговора, налази се у Глави VIII Уредбе о подацима. Наиме, одредбом чл. 36 ст. 1 поменуте Уредбе, установљени су битни услови у погледу паметних

уговора за извршавање споразума о дељењу података. Продавац апликације у којој се користе паметни уговори или, ако продавац не постоји, особа чија трговачка, пословна или професионална делатност укључује увођење паметних уговора за друге у контексту извршавања споразума о дељењу података или дела тог споразума, у обавези је да осигура да ти паметни уговори испуњавају следеће битне услове:

1. поузданост и контролу приступа ради осигуравања да је паметни уговор осмишљен тако да омогућује механизме контроле приступа и врло висок ниво стабилности, како би се избегле функционалне грешке и постигла отпорност на манипулацију трећих страна;
2. сигурно окончање и прекид ради осигуравања постојања механизма за окончање континуираног извршавања трансакција и да паметни уговор садржи интерне функције којима се уговор може вратити на почетне поставке или му се може наредити да заустави или прекине извршавање операције, а посебно како би се избегла будућа случајна извршења;
3. архивирање и континуитет података ради осигуравања, у околностима у којима се паметни уговор мора раскинути или обуставити, да постоји могућност за архивирање података о трансакцијама, логике паметног уговора и кода ради вођења евиденције о претходним операцијама извршеним на подацима (могућност ревизије);
4. контрола приступа ради осигуравања да је паметни уговор заштићен строгим механизмом контроле приступа на нивоу управљања и на нивоу паметних уговора; и
5. доследност ради осигуравања усклађености с условима споразума о дељењу података који се извршава паметним уговором.

Важно је указати да су ови услови техничке, а не правне природе. Циљ постављања ових услова је у томе да се паметни уговори учине сигурнијим за коришћење. Њиховим испуњењем би требало да буду отклоњени неки од недостатака паметних уговора. Ту се пре свега мисли на следеће недостатке: заштита података који се уносе у паметни уговор, немогућност измене уговорних одредаба и аутоматско извршење уговора, које представља проблем у случају грешке приликом кодирања уговора или непотпуног извршења уговора.

3.1. Услов поузданости и контроле приступа

Поузданост је једна од основних особина паметних уговора, имајући у виду чињеницу да су паметни уговори готово непроменљиви након постављања на мрежу. Кроз услов поузданости се спречавају недозвољене интервенције трећих лица на садржину паметног уговора. Међутим, људски фактор у настанку и функционисању паметних уговора не може се занемарити. Имајући у виду да паметне уговоре креирају људи, постоји могућност грешке приликом кодирања садржаја паметног уговора. Једном постављен на блокчејн мрежу, тако манљив паметни уговор је тешко изменити и отклонити грешку. Као један од практичних начина за решавање овог проблема, предлаже се статичка анализа која може помоћи у откривању грешака у раној фази развијања кода, пре него што постане непроменљив (Olivieri & Passeto 2023, 9).

Значај контроле приступа у контексту паметних уговора лежи у чињеници да се, кроз контролу приступа, уређује круг субјеката који могу да извршавају одређене команде у оквиру паметног уговора. Један од главних проблема који је примећен у функционисању паметних уговора је неуспех да се на адекватан начин ограничи приступ осетљивим функцијама или подацима, што омогућава неовлашћеним корисницима да изводе спорне операције (Kuppa & Madisetti 2025, 201). Иако складиштење података засновано на блокчејну нуди већи степен безбедности и децентрализацију, обезбеђење ефикасне и безбедне контроле приступа подацима остаје крупан изазов. Тренутне методе или поново уводе централизацију или немају неопходну флексибилност за управљање дозволама у реалном времену. Без поузданих механизама контроле приступа, осетљиви подаци који се складиште у децентрализованим системима могу бити изложени неовлашћеном приступу, цурењу података или злоупотреби.

3.2. Сигурно окончање и прекид

Овај захтев је успостављен ради неутралисања ризика од сајбер напада. Наиме, у случају напада на паметни уговор, потребно је обезбедити механизам за прекид рада паметног уговора, како би се спречиле штетне последице које могу бити далекосежне и погодити велики број субјеката. Међутим, када је реч о сигурном окончању и

прекиду као услову који треба да испуне паметни уговори, постоји суштински проблем. Једна од особина паметних уговора је фиксираност у погледу садржине и начина функционисања: немогуће их је раскинути, а то је неспојиво са захтевом за безбедним прекидом и обуставом (Casolari et al. 2023, 2). С друге стране, „нетерминација“[2] паметних уговора се сматра „грешком у погледу живости“ (*liveness bug*), јер би случајно омогућавање извршавања паметног уговора које се никада не завршава, неизоставно довело до колапса целог система. Такав нетерминирајући паметни уговор би се извршавао на сваком чвору у децентрализованом систему заувек. Сваки појединачни покушај да се прекине његово извршавање довео би до нарушавања консензуса у мрежи (Le et al. 2018, 57). Додатно, услед проблема у области сајбер-безбедности, функције сигурног окончања и прекида нису оптимално решење за имплементацију унутар паметног уговора, јер подаци, средства и операције повезане са паметним уговором могу лако бити изложени ризику (EU Crypto Initiative 2023, 8).

У технолошком смислу, сигурно окончање и прекид паметног уговора је могуће обезбедити кроз *kill switch* функцију. Ради се о механизму који омогућава моментално и принудно искључење софтвера, у случају опасности. Конкретна опасност се унапред предвиђа као услов услед чијег наступања систем престаје са радом, без обзира на све остале околности. Проблем са *kill switch* функцијом у контексту паметних уговора тиче се чињенице да је, због блокчејн технологије, потребно постизање консензуса у мрежи како би дошло до прекида извршавања паметног уговора. Оваква процедура нужно доводи до смањења ефикасности и знатно успорава функционисање паметног уговора. Уколико би било усвојено другачије решење и била прихваћена „класична“ верзија *kill switch* функције, настаје другачија опасност. У случају додељивања једном лицу или ограниченом кругу лица могућност да активирају *kill switch* функцију, то би довело у опасност истинску децентрализацију, као још једну од особина паметних уговора. Тиме би настало једно непожељно стање – да један субјект контролише и управља свим операцијама паметног уговора. Увођење *kill switch* механизама

[2] У рачунарству, нетерминација означава ситуацију у којој рачунарски програм не достиже своју крајњу тачку, тј. никада се не завршава (нити враћа резултат, нити прекида извршавање) и доводи до тзв. „бесконачне петље“.

у паметне уговоре представља парадокс: овај механизам доприноси сигурности и безбедности корисника паметних уговора, а истовремено доводи до ризика од централизоване контроле паметног уговора (Seneviratne 2024, 479). Данас већина блокчејн система прекид извршења паметног уговора обавља или кроз механизме који захтевају централизовано одлучивање или кроз механизме засноване на координисаном консензусу међу субјектима на мрежи.[3]

Што се тиче захтева за прекид трансакције, постоје решења која омогућавају да се у код паметног уговора угради изузеци који регулишу његово извршавање (Olivieri & Passeto 2023, 9). На *Ethereum* мрежи постоји *selfdestruct* функција, која омогућава уништавање већ постављених уговора и уједно је једини начин да се паметни уговор уклони са *Ethereum* блокчејна. Активирање функције *selfdestruct* када уговор више није потребан, доприноси „чишћењу" *Ethereum* окружења, због чега се овакво понашање и стимулише (Chen et al. 2021, 6).

3.3. Архивирање и континуитет података

Овај услов има за циљ да обезбеди очување података и могућност њихове накнадне ревизије у случају обуставе или прес-

[3] Тако, *Bitcoin* функцинише на основу *Turing* некомплетног система, а *Ethereum* функционише на основу gas механизма. *Bitcoin* блокчејн је свесно изграђен као *Turing* некомплетни систем, управо ради повећања безбедности и предвидивости при извршавању трансакција. Заснива се на једноставном коду, јер не садржи фунцкије понављања (петље). Функционалност оваквог кода је ограничена, јер је могуће извршавати само ограничен скуп, унапред дефинисаних функција. Због тога је реализација трансакција веома предвидива, тако да се све трансакције окончавају у ограниченом броју корака. Додатно, овакав код значајно доприноси безбедности, јер је овако једноставан систем, без петљи и компликованих функција, мање рањив и подложан хакерским нападима. Детаљно у: Antonopoulos 2017.
Сигурно окончање помоћу механизма гаса, који се користи на Ethereum мрежи, функционише на следећи начин: када се уговор извршава, одређује се количина гаса која се троши током извршавања инструкција. Ако се гас потроши пре завршетка извршавања, одређује се количина гаса која се троши током извршавања инструкција. Ако се гас потроши пре завршетка извршавања, извршавање се аутоматски прекида, што доводи до грешке „неуспеха". Применом формалне верификације може се доказати исправно функционисање механизма гаса и открити неочекивана понашања, као што је рањивост услед „несташице" гаса.

танка паметног уговора.[4] Чињеница да су подаци који пролазе кроз блокчејн видљиви на сваком чвору и да се не могу брисати са блокчејна су две карактеристике блокчејна које су у супротности са два основна начела Опште уредбе – начелом минимизације података и начелом ограничења чувања података (Maxwell & Salmon 2018, 14). У контексту архивирања података, паметни уговори представљају алат за извршавање кодираних одредаба над подацима који се уносе у ланац. Блокчејн се заснива на мрежи у којој сваки чвор чува делимичну или пуну копију ланца. Пошто је структура дистрибуирана и децентрализована, те копије се обично налазе на различитим географским тачкама. На тај начин блокчејн чува евиденцију о претходним операцијама са подацима (Olivieri & Passeto 2023, 9).

Кроз овај захтев је могуће извршити усклађивање паметних уговора са Уредбом 2016/679 о заштити појединца у вези са обрадом лучних података (Општа уредба о заштити података) (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Према одредби чл. 5 ст. 1 тач. б Опште уредбе, подаци, који су прикупљени у одређене, изричите и легитимне сврхе, не могу се даље обрађивати на начин који није у складу са тим сврхама, осим у сврхе архивирања у јавном интересу, научног или историјског истраживања или истраживања у статистичке сврхе.

Посебну пажњу треба посветити подацима о личности. Општом уредбом су подаци о личности дефинисани као сви они подаци који се односе на појединца чији је идентитет утврђен или се може утврдити. Појединац чији се идентитет може утврдити је особа која се може директно или индиректно лично идентификовати уз помоћ идентификатора, као што су име, идентификациони број, подаци о локацији, мрежни идентификатор или уз помоћ једног или више чинилаца својствених за физички, физиолошки, генетски, ментални, економски, културни или социјални идентитет тог појединца (чл. 4 ст. 1 тач. 2 Опште уредбе). У контексту паметних

[4] Колико су подаци значајни за паметне уговоре, говори и чињеница да је у оквиру програмског језика *Solidity*, паметни уговор дефинисан као збир кода (функција паметног уговора) и збир података (стања паметног уговора) који се налази на одређеној адреси на *Ethereum* блокчејну.

уговора, важно је указати да трансакциони подаци који се чувају у блоковима могу бити квалификовани као лични подаци, чак и када су шифровани и прошли процес хеширања, као технике псеудонимизације (Voss 2021, 85). Општом уредбом су предвиђена посебна правила у случају да је сврха обраде података различита од сврхе у коју су подаци прикупљени, а која се не темељи на сагласности испитаника, праву Европске уније или праву државе чланице који представља разумну и сразмерну меру у демократском друштву ради заштите циљева из чл. 23 ст. 1 Опште уредбе. У том случају, обрађивач података о личности, како би утврдио да ли је обрада у другу сврху у складу са сврхом у коју су подаци прикупљени, узима, између осталог, у обзир и постојање одговарајућих заштитних мера, које могу укључивати енкрипцију или псеудонимизацију (чл. 6 ст. 4 тач. е Опште уредбе). Овај критеријум је од значаја за паметне уговоре.

С једне стране, приступ паметном уговору који се налази на затвореном блокчејну је могућ само за оне субјекте који имају шифру на основу које им је могућ приступ блокчејну. И у том случају је, за извршење било које трансакције у паметном уговору, потребно постизање консензуса на мрежи. С друге стране, уколико се ради о јавном (отвореном) блокчејну, приступ је дозвољен свим субјектима и они могу слободно учествовати у трансакцијама, али им је и у том случају потребна потврда осталих учесника на ланцу. Блокчејн мрежа се састоји од више чворова који дају одобрење (*endorsing peers*), а који функционишу као валидатори. Ови чворови извршавају паметне уговоре ради провере достављених података и обезбеђивања њиховог интегритета пре него што буду додати у књигу евиденције (*ledger*) (Parab et al. 2025, 238).

3.4. Контрола приступа

Суштина овог услова је осигуравање да је паметни уговор заштићен строгим механизмом контроле приступа на нивоу управљања и на нивоу паметних уговора. Контрола приступа на нивоу управљања је посебно значајна за контролисање приступа подацима, јер обезбеђује да се размена података и извршавање трансакција одвијају само између оних субјеката који су овлашћени да приступе паметном уговору. Ризици за податке у паметном уговору се састоје у могућности неовлашћеног приступа подацима, што

може довести до крађе података, финансијских губитака и нарушавања угледа оног привредног субјекта који паметни уговор користи. Слаба заштита података током њиховог преноса или складиштења их може учинити нарочито рањивим и погодним за хакерске нападе. Осим тога, постоји и унутрашњи ризик, који се огледа у могућности да запослени могу, намерно или случајно, злоупотребити податке са којима раде (Chougule & Cantisani 2024, 140). Технички, овај услов је могуће остварити кроз енкрипцију и токенизацију.[5]

3.5. Доследност

Захтев доследности код паметних уговора је успостављен ради осигуравања усклађености с условима уговора о дељењу података који се извршава паметним уговором. Уговор о дељењу података (*data sharing agreement*) представља уговор којим се дефинишу детаљи процеса по којем подаци треба да буду дељени између две стране и којим се прецизирају: услови закључења уговора, обавезе уговорних страна, спецификација података који су предмет размене, износ накнаде, однос према трећим лицима, заштитне мере и остала правна питања (ADAPTAC 2025, 2). Сврха уговора о дељењу података је да обезбеди следеће: да се подаци деле у складу са важећим правом и да субјекти који размењују податке поступају у складу са стандардима управљања информацијама и прате организационе политике управљања подацима (Krebs & Bennett Moses 2024, 129). У контексту законодавства Европске уније, нарочито је значајно ускладити садржину уговора о дељењу података са одредбама Опште

[5] Енкрипција је шифровање информација ради спречавања неовлашћеног приступа. За разлику од класичног шифровања, енкрипција осигурава додатни ниво заштите, јер и у случају да неовлашћеном лицу постану доступни подаци, читање тих информација је немогуће без информације о одговарајућем кључу за дешифровање. Дакле, да би једно лице могло самостално да користи податке са блокчејна, неопходно је да има барем два кључа: један који ће му омогућити приступ подацима и други који ће му омогућити да податке дешифрује.

Још један од начина за практично остваривање овог захтева је токенизација. Токенизација је процес у коме се поверљиви подаци замењују токенима, који представљају јединствене идентификаторе, који су насумично одређени и сами по себи не садрже корисне информације. Токенизацијом се смањује изложеност осетљивих података трећим лицима, те се ти подаци додатно штите од неовлашћеног приступа. Вид: Chougule & Cantisani 2024, 140.

уредбе о подацима. Ради законитог ангажовања обрађивача или подобрађивача, руковалац, односно обрађивач података, мора имати закључен уговор о дељењу података у коме је јасно назначено које врсте података се могу обрађивати, што значи да уговор треба да спречи обраду и размену података на нетранспарентан или непознат начин (GDPR Summary 2022).

Што се тиче података који се обрађују на блокчејн мрежи, важно је знати да блокчејн мреже, а самим тим и паметни уговори, по правилу за предмет обраде имају посебну врсту података, која је данас позната као *big data*. Ради се о масивним скуповима података, који се одликују великим обимом, разноврсношћу и сложеношћу, што ствара потешкоће у њиховом складиштењу, анализи и визуализацији ради даљих процеса или добијања резултата.[6] Ове податке је немогуће обрађивати коришћењем традиционалних софтвера за обраду података. Појавом блокчејн технологије и дистрибуираних база података, анализа оваквих података је знатно олакшана. Кроз досадашњу праксу обраде података успостављена су два значајна принципа успешне обраде, који су формулисани кроз тзв. *CAP* принципе[7] и кроз тзв. *ACID* принципе.[8] Код обе постоји услов доследности, али му је значење различито.[9] У контексту паметних

---

[6] Истраживање ових података се назива аналитика великих података *(big data analytics*) и омогућава откривање скривљених образаца и тајних корелација међу подацима. Ови подаци су изузетно значајни за компаније и велике организације јер им омогућава стицање богатијих и дубљих увида и остваривање конкуретнске предности. Вид: Sagiroglu & Sinanc 2013, 42–47.

[7] CAP теорема, или Бруерова теорема, названа по свом творцу Ерику Бруеру (*Eric Brewer*) који га је изложио на једном свом предавању 2000. године. Сам израз CAP је акроним и значи: *Consistency* (доследност), *Availability* (доступност) и *Partitions Tolerance* (отпорност на прекид). Заснована је на идеји да сваки систем за размену података може истовремено задовољавати само два од три критеријума. Детаљније у: Brewer 2000**.**

[8] ACID принципе су, још 1983. године, формулисали Тео Хердер (*Theo Hearder*) и Андрес Ројтер (*Andreas Reuter*). Име ACID је акроним за *Atomicity* (својство да се свака трансакција извршава одједном или да се не извршава уопште), *Consistency* (доследност), *Isolation* (изолација) и *Durability* (трајност). Више у: Haerder & Reuter 1983, 287–317.

[9] Доследност код CAP принципа значи да сваки сервер враћа исправан одговор на сваки захтев, односно одговор који је тачан у складу са жељеном спецификацијом услуге и представља класично безбедносно својство: сваки податак послат клијенту је тачан. Детаљније у: Gilbert & Lynch 2012, 30–36. Речју, доследност према CAP принципу значи идентичност података међу

уговора, доследност је нарочито значајна у случају када постоји неусклађеност између кода паметног уговора и раније закљученог уговора. Последица такве неусклађености је аутоматско извршење које доводи до нежељених последица.

3.6. Поступак оцењивања усклађености паметног уговора са захтевима из чл. 36 ст. 1 Уредбе о подацима

Уредбом о подацима је утврђен круг правних субјеката овлашћених на спровођење поступка усклађености паметног уговора са захтевима из чл. 36 ст. 1 Уредбе. Правни субјекти који спроводе овај поступак могу бити:

1. продавац паметног уговора;

2. лице чија трговачка, пословна или професионална делатност обухвата увођење паметних уговора за друге у контексту извршавања споразума о стављању података на располагање или његовог дела, али само под условом да продавац паметног уговора не постоји.

Након што се у поступку утврди усклађеност паметног уговора са захтевима из чл. 36 ст. 1 Уредбе о подацима, издаје се ЕУ

серверима, без обзира на њихову тачност, јер се тачност претпоставља уколико је податак послат. Доследност као саставни део ACID принципа се односи на следеће: трансакција која досегне свој нормални завршетак, чиме се њени резултати потврђују, очувава конзистентност базе података. Другим речима, свака успешно извршена трансакција по самој дефиницији потврђује искључиво правно и логички ваљане резултате. Вид: Haerder & Reuter 1983, 289. У оквиру ACID модела, доследност гарантује интегритет података који се размењују. Заправо, овде је могућа само размена тачних података. У контексту паметних уговора, под доследношћу података подразумевамо логичка ограничења повезаности између променљивих стања паметног уговора које непосредно подржавају пословну логику апликације. Када је реч о услову доследности као услова из Уредбе о подацима, можемо извести закључак да европски законодавац определио за концепт доследности из CAP модела. Наиме, захтев доследности се у Уредби поставља у циљу осигуравања усклађености с условима уговора о дељењу података који се извршава паметним уговором. Захтева се да постоји идентичност информација које се налазе у уговору о дељењу података и информација које се паметним уговором деле, при чему се не улази у садржину самих информација. Међутим, логично је да ће писци оба ова уговора настојати да обезбеде да предмет уговора буде дељење истинитих података.

изјава о усаглашености (*EU declaration of conformity*). Састављањем ове изјаве, правни субјект који спроводи поступак преузима одговорност за усклађеност паметног уговора са битним захтевима из чл. 36 ст.1 Уредбе о подацима. ЕУ изјава о усаглашености представља обавезни документ који састављају произвођачи који намеравају да своју робу пласирају на тржиште Европске уније. Изјава о усаглашености се захтева, између осталог, и за медицинске производе и за софтвере засноване на вештачкој интелигенцији. И на овај начин се повећава правна сигурност и расте поверење уговорних страна приликом закључења паметног уговора.

Важно је приметити да изјаву о усаглашености издаје продавац паметног уговора или лице које у оквиру своје делатности уводи паметне уговоре за друге у контексту извршавања споразума о стављању података на располагање. Дакле, гаранти да је постигнута усаглашеност са захтевима из чл. 36 ст. 1 Уредбе нису уговорне стране паметног уговора, него креатори паметног уговора или они субјекти који паметни уговор пуштају у промет и стављају га на располагање крајњим корисницима. У конкретном случају, то би биле или софтверске компаније које се баве развојем софтвера у које су имплементирани паметни уговори или компаније које се баве продајом таквих софтвера.

За разлику од захтева из чл. 36 ст. 1 Уредбе, који обезбеђује висок степен технолошке поузданости, процедура која се односи на обавезу издавања изјаве о усаглашености, усмерена је пре свега на повећање нивоа правне сигурности и поверења субјеката који ће касније користити паметни уговор.

4. ЗАКЉУЧАК

Паметни уговори се већ увелико примењују у различитим областима пословног живота. Предност паметних уговора је аутоматизација извршења престација, искључење посредника из трансакција и директна комуникација уговорних страна. Ове предности нарочито долазе до изражаја у прекограничним трансакцијама које су честе у савременом привредном окружењу. Речју, паметни уговори се у значајној мери уклапају у потребе савременог дигиталног промета који омогућава висок степен аутоматизације и у коме се велики број радњи одвија електронским путем.

Примена паметних уговора носи са собом и читав сет ризика: потпуна анонимизација уговорних страна при закључењу и извршењу уговора, што може имати утицај на пуноважност уговора; опасност по личне податке који се нађу на мрежи; непроменљивост уговорних одредаба и немогућност ревизије уговора; потешкоће у кодирању правничких израза и друге грешке у кодирању; проблем у случају неизвршења, а нарочито неуредног извршења уговорних обавеза, које се аутоматски извршавају.

Због проблема који могу настати у примени паметних уговора, било је потребно правно уредити нека значајна питања. У Европској унији је то учињено Уредбом о подацима. За разлику од решења која су до тада постојала у упоредним законодавствима, где су углавном постојале само дефиниције паметних уговора, у Уредби о подацима се отишло корак даље. Наиме, постављени су јасни услови које паметни уговори морају испуњавати пре него што буду употребљени: поузданост и контрола приступа, сигурно окончање и прекид, архивирање и континуитет података, контрола приступа и доследност. С једне стране, ови услови ће повећати правну сигурност у примени паметних уговора и додатно подстаћи њихово коришћење. С друге стране, они могу довести у питање основне концептуалне поставке на којима су паметни уговори засновани, а нарочито непроменљивост паметног уговора и аутоматско извршење уговорних одредаба. Наведени утицај не доводи у питање опстанак паметних уговора. Наиме, код паметних уговора који су на правилан начин кодирани, а потом и извршени, чињеница да су мењање уговора и прекид уговора могући, неће доћи до изражаја, јер ће такав уговор бити аутоматски извршен. Заправо, до одступања од особина непроменљивости и аутоматског извршења паметних уговора ће долазити само у случајевима када паметни уговор садржи недостатке.

Уредбом је уређен и круг субјеката који спроводе поступак оцењивања усклађености паметног уговора са овим условима, чиме се установљава њихова одговорност за исправно функционисање уговора.

Овакво правно нормирање паметних уговора у Европској унији представља квалитативни скок у односу на тренутно стање у упоредном законодавству. Отишло се даље од давања просте дефиниције паметних уговора. Детаљно су уређени услови које сваки паметни уговор мора да испуњава да би био употребљаван и уређен

је поступак испитивања усклађености паметног уговора са тим условима. Због тога се може оправдано очекивати све шира примена паметних уговора на јединственом ЕУ тржишту у будућности.

ЛИТЕРАТУРА

Apprenticeship Data Alignment & Performance Technical Assistance Center [ADAPTAC]. 2025. *Understanding Data Sharing Agreements*. Lexington: The Council of State Governments.

Casolari, Federico, Taddeo, Mariarosaria, Turillazzi, Aina & Floridi, Luciano. 2023. "How to Improve Smart Contracts in the European Union Data Act". *Digital Society*, 2 (9), pp. 1–6. doi: https://doi.org/10.1007/s44206-023-00038-2

Chen, Jiachi, Xia, Xin, Lo, David & Grundy, John. 2021. "Why Do Smart Contracts Self-Destruct? Investigating the Selfdestruct Function on Ethereum". *ACM Transactions on Software Engineering and Methodology*, 31 (2), pp. 1–37. doi: https://doi.org/10.1145/3488245

Chougule, Sharmin & Cantisani, Luigi. 2024. "The Oracle Problem in Smart Contracts: Data Privacy, Security, and Solutions". *Rivista di Diritto dei Media*, 2/2024, pp. 122–143.

Đurović, Mateja & Lech, Franciszek. 2019. "The Enforceability of Smart Contracts". *Revija kopaoničke škole prirodnog prava*, 1/2019, pp. 73–94. doi: https://doi.org/10.5937/rkspp1901073d

EU Crypto Initiative. 2023. T*he Data Act Smart Contracts: Implications for the Future of Innovation in Europe*. Brussels.

Forum, EU Blockchain and Observatory. 2022. *Smart Contracts.* Brussels: European Commission.

Gilbert, Seth & Lynch, Nancy. 2012. Perspectives on the CAP Theorem. *Computer, vol. 45, no. 2*, pp. 30–36.

Haeder, Theo, & Reuter, Andreas. 1983. "Principles of Transaction-Oriented Database Recovery". *Computing Surveys,* Vol. 15, No. 4, pp. 287–317.

Krebs, Shiri, & Bennett Moses, Lyria. 2024. "Data Sharing Agreements: Contracting Personal Information in the Digital Age". *Melbourne University Law Review,* 48(1), pp. 96–149.

Kuppa, Nishank & Madisetti, Vijay. 2025. "Robust Detection and Analysis of Smart Contract Vulnerabilities with Large Language Model Agents". *Journal of Information Security,* 16(1), pp. 197–226.

Le, Ton Chanh, Xu, Lei, Chen, Lin & Shi, Weidong. 2018. "Proving Conditional Termination for Smart Contracts". *BCC '18: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts.* Incheon Republic of Korea: Association for Computing Machinery, New York, United States, pp. 57–59.

Maxwel, Winston & Salmon, John. 2018. *A guide to blockchain and data protection.* London: Hogan Lovells.

Olivieri, Luca & Pasetto, Luca. 2023. "Towards Compliance of Smart Contracts with the European Union Data Act". In Andrea Brunello, Alessandro Gianola и Fabio Mogavero (ed.), *Short Paper Proceedings of the 5th Workshop on Artificial Intelligence and Formal Verification, Logic, Automata, and Synthesis (OVERLAY 2023)* (pp. 61–66). Rome: CEUR Workshop Proceedings.

Olivieri, Luca, Pasetto, Luca, Negrini, Luca & Ferrara, Pietro. 2024. "European Union Data Act and Blockchain Technology: Challenges and New Directions". In Massimo Bartoletti, Claudio Schifanella и Andrea Vitaletti (ed.), *Proceedings of the Sixth Distributed Ledger Technology Workshop (DLT 2024)* (стр. 321–334). Turin: CEUR Workshop Proceedings

Parab, Aishwarya, Pradhan, Prakhar, Simmhan, Yogesh & Paul, Arnab K. 2025. "A Blockchain-Enabled Framework for Storage and Retrieval of Social Data". In Kyle Chard, Suren Byna, David Donofrio и Giulia Guidi (ed.), *2025 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)* (pp. 237–240). Milan: Institute of Electrical and Electronics Engineers doi: https://doi.org/10.1109/IPDPSW66978.2025.00046

Savin, Andrej. 2022. *Digitalna pravda.* Beograd: Clio.

Seneviratne, Oshani. 2024. "The Feasibility of a Smart Contract 'Kill Switch'." *2024 6th International Conference on Blockchain Computing and Applications (BCCA),* pp. 473–480.

Szabo, Nick. 1996. Smart Contracts: Building Blocks for Digital Markets. *Extropy Journal of Transhuman Thought*, pp. 50–53.

Volos, Aleksei. 2020. "The Technology of Blockchain and Smart Contract and Their Regulation Under the Conflict of Laws of the European Union". *2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020) - Advances in Economics, Business and Management Research.* Yekaterinburg: Institute of Digital Economics, pp. 563–568.

Voss, W. Gregory. 2021. "Data Protection Issues for Smart Contracts". In Marcelo Corrales Compagnucci, Mark Fenwick & Stefan Wrbka (eds), *Smart Contracts - Technological, Business and Legal Perspectives* (pp. 79–100). London: Bloomsbury Publishing.

Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning, Chen, Weili, Chen, Xiangping, Weng, Jian, Imran, Muhammad. 2020. "An overview on smart contracts: Challenges, advances and platforms". *Future Generation Computer Systems*, Vol. 105, pp. 475–791. doi: https://doi.org/10.1016/j.future.2019.12.019

Глушац, Данијела. 2022. „Правни оквир регулисања паметних уговора". У Драган Вујисић (ур.), *Садашњост и будућност услужног права* (стр. 429–440). Крагујевац: Правни факултет Универзитета у Крагујевцу. doi: https://doi.org/10.46793/xviiimajsko.429g

Матановић, Александар.2022. *Увод у блокчејн.* Београд: Иницијатива Дигитална Србија.

Цветковић, Предраг. 2020. „Блокчејн као правни феномен: уводна разматрања". *Зборник радова Правног факултета у Нишу*, Vol. 59, стр. 127–144. doi: 1 https://doi.org/0.5937/zrpfn0-24414

Цветковић, Предраг. 2021. „Синтеза правног текста и програмског кода: случај Рикардијанског уговора". *Зборник радова Правног факултета у Нишу*, Vol. 60, стр. 61–76. doi: https://doi.org/10.5937/zrpfn0-29556

ИЗВОРИ ПРАВА

Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione, Gazzetta Ufficiale Serie Generale n. 290, 14 December 2018, https://www.gazzettaufficiale.it/eli/id/2018/12/14/18G00163/SG (04.05.2026).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119, 4.5.2016, pp. 1–88, https://eur-lex.europa.eu/eli/reg/2016/679/oj (04.05.2026).

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), Official Journal of the European Union L, 2023/2854, 22.12.2023, https://eur-lex.europa.eu/eli/reg/2023/2854/oj (04.05.2026).

Virtual Financial Assets Act, 1st November 2018, https://legislation.mt/eli/cap/590/eng/pdf (04.05.2026).

ИНТЕРНЕТ И ДРУГИ ИЗВОРИ

GDPR Summary. 2022. “Data Sharing Agreement.” GDPR Summary. https://www.gdprsummary.com/gdpr-definitions/data-sharing-agreement/ (15.01.2026).

Securr Web3 Security. 2025. “Access Control in Smart Contracts: Why It’s Non-Negotiable.” Securr (Medium). https://securrtech.medium.com/access-control-in-smart-contracts-why-its-non-negotiable-79af14523f28 (01.01.2026).

Solidity. n.d. “Introduction to Smart Contracts.” Solidity Documentation. https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html (12.01.2026).

Nemanja JANKOVIĆ

SMART CONTRACTS IN EUROPEAN UNION LAW

Resume

Smart contracts represent a specific synthesis of technology and law. They are agreements that are automatically executed and, owing to blockchain technology, relatively immutable. Due to their automation and immutability, smart contracts constitute a useful instrument of contemporary digital transactions. At the level of the European Union, smart contracts are comprehensively regulated by Regulation (EU) 2023/2854 on fair access to and use of data. In the first part of the paper, the author analyzes the concept of smart contracts, along with a brief explanation of blockchain technology as their underlying basis. In the second part, the author examines the legislation of the Member States of the European Union concerning smart contracts prior to the adoption of the aforementioned Regulation. The central part of the paper is devoted to an analysis of the provisions of Regulation (EU) 2023/2854 relating to smart contracts, with particular emphasis on the essential requirements for smart contracts used in the performance of data sharing agreements, as well as on the procedure for assessing the compliance of smart contracts with those essential requirements. In the conclusion, the author elaborates the thesis that the new European Union legislation, including that relating to smart contracts, represents a qualitative leap compared to previous solutions, as it provides a detailed regulation of some of the most significant issues concerning the functioning of smart contracts and offers appropriate legal and technical guarantees for their successful application.

Keywords: smart contracts, blockchain technology, European Union law, EU Data Act, data sharing agreement

Достављено: 8.5.2026. године
Прихваћено: 17.6.2026. године