ბლოკჩეინის სისტემის მიმართება პერსონალურ მონაცემთა მარეგულირებელ კანონმდებლობასთან

გრიგოლ აბაშიძე

I. შესავალი

ბლოკჩეინი 21-ე საუკუნის ერთ-ერთი ყველაზე აქტუალური ტექნოლოგიაა, რომლის განვითარების პერსპექტივები თუ კრიტიკა აქტიურად განიხილება სხვადასხვა მასშტაბით. რეალურად, არ არსებობს ერთი კონკრეტული ბლოკჩეინ სისტემის მოდელი. პრაქტიკაში შესაძლებელია ბლოკჩეინ ტექნოლოგიის თითქმის უსასრულო ნაირსახეობის კონფიგურაციით გამოყენება[1].

ბლოკჩეინ ტექნოლოგიის გამოყენების მრავალფეროვნებაზე მეტყველებს ის ფაქტი, რომ იგი უკვე აქტიურად გამოიყენება სხვადასხვა სფეროში. მაგალითად, ჯანდაცვის სფეროში სამედიცინო ჩანაწერების შესანახად. საჯარო სექტორში ტექნოლოგიის გამოყენების ყველაზე ნათელი მაგალითია საქართველოს იუსტიციის სამინისტროს მიერ მიწის რეგისტრაციის მონაცემების ბლოკჩეინ სისტემაში შენახვა, ფინტეკ (Fintech) კომპანიების შემთხვევაში კრიპტოვალუტებისა და კრიპტობირჟების შექმნა.

ბლოკჩეინ ტექნოლოგიის აქტიური გამოყენება ქსელში ახდენს საკმაოდ დიდი ოდენობის ინფორმაციის გენერირებას, რაც ავტომატურად წარმოშობს კითხვებს მის პერსონალურ მონაცემთა დაცვის შესახებ კანონთან შესაბამისობაზე.

2018 წლის 25 მაისს ძალაში შევიდა ევროკავშირის მონაცემთა დაცვის რეგულაცია („General Data Protection Regulation“) (შემდგომში GDPR). რეგულაციამ 94-ე პარაგრაფის პირველი აბზაცით ჩაანაცვლა პერსონალურ მონაცემთა დაცვის შესახებ ევროკავშირის დირექტივა (Data Protection Directive) 95/46/EG და წარმოადგენს ევროკავშირის ყველა წევრი სახელმწიფოსათვის სავალდებულოდ გამოსაყენებელ დოკუმენტს.

აღნიშნულიდან გამომდინარე საინტერესოა, ბლოკჩეინ ტექნოლოგიის პერსონალურ მონაცემებთან შესაბამისობის განხილვა GDPR-ის ჭრილში[2].

II. ბლოკჩეინის ზოგადი ტექნოლოგიური აღწერილობა

ბლოკჩეინ ტექნოლოგიის დეტალური აღწერა და მის სრულ ტექნიკურ მახასიათებლებზე საუბარი გაცდება მოცემული სტატიის მიზანს. მაგრამ, ვინაიდან პერსონალური მონაცემების დაცვის საკითხი მჭიდრო კავშირშია ბლოკჩეინ ტექნოლოგიის ფუნქციონირებასთან, გვერდს ვერ ავუვლით ტექნოლოგიის იმ კონკრეტულ ტე-

[1] *W. Maxwell/ J. Salmon*, A Guide to Blockchain and Data Protection, 16, https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf
(წინამდებარე სტატიაში მითითებული ყველა ბმულის ბოლო გამოყენების თარიღია 16.01.2020).

[2] ბლოკჩეინ ტექნოლოგიისა და GDPR-ის მიმართებასთან დაკავშირებით იხ. კვლევა - EPRS | European Parliamentary Research Service, Blockchain and the General Data Protection Regulation, ივლისი 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

ქნიკურ ასპექტებს, რომლებიც მჭიდრო კავშირშია პერსონალურ მონაცემებთან.

1. ინტერაქცია ბლოკჩეინსა და მომხმარებელს შორის

როდესაც პირი კომპიუტერის საშუალებით უკავშირდება ინტერნეტს, დაკავშირება არ ხდება მისი რეალური სახელითა და გვარით, არამედ მომხმარებელს აქვს საკუთარი IP მისამართი, რომლითაც ხდება სუბიექტის იდენტიფიცირება ქსელის მიერ.

ანალოგიური პრინციპით ხდება მომხმარებელსა და ბლოკჩეინ სისტემის ინტერაქცია, მაგრამ ამ დროს დამატებით გამოიყენება „საჯარო გასაღები“ (Public key) (გრძელი, შემთხვევით შერჩეული რიცხვებისა და ლათინური ასოების რიგი) რომელიც მომხმარებლის მისამართია ბლოკჩეინზე. საჯარო გასაღების გამოყენება და მოხმარება შესაძლებელია მხოლოდ პირადი გასაღების მეშვეობით, რომელიც ცნობილია მხოლოდ მომხმარებლისათვის და გამოიყენება ისევე, როგორც ელექტრონული ხელმოწერა, ანუ მისი დანიშნულებაა ბლოკჩეინ სისტემაში ონლაინ ტრანზაქციების ვალიდაცია/დადასტურება[3].

პირადი გასაღები წარმოიქმნება დაცული, შემთხვევითი მათემატიკური ფუნქციების მეშვეობით, რაც განაპირობებს, რომ მისი რეკონსტრუქცია/აღდგენა არის თითქმის შეუძლებელი. იმ შემთხვევაში, თუ მომხმარებელი დაკარგავს მის პირად გასაღებს ან მას მოპარავენ, მისი მონაცემებიც დაკარგულად ჩაითვლება და მას შეეზღუდება აღნიშნულ მონაცემებზე წვდომა.[4]

2. ნოდები

თითოეული კომპიუტერი, რომელიც დაკავშირებულია ბლოკჩეინის ქსელთან, იღებს ბლოკჩეინის ასლს, სადაც მოცემულია ინფორმაცია სხვადასხვა სავაჭრო ოპერაციის შესახებ.

ბლოკჩეინის ქსელთან დაკავშირებული კომპიუტერი, რომელიც ხსნის მათემატიკურ ალგორითმს და ამით უზრუნველყოფს ქსელის მუშაობას, არის ნოდი[5].

ნოდი ქსელს თავისი სურვილით უერთდება, რაც საბოლოო ჯამში ქმნის დეცენტრალიზებულ ქსელს.

დახურულ ბლოკჩეინთან დაკავშირებული ნოდების რაოდენობა არის შეზღუდული და თითოეული ნოდი არის იდენტიფიცირებული. საჯარო ბლოკჩეინში მონაწილე ნოდების ოდენობა კი განუსაზღვრელია და ნებისმიერ სუბიექტს შეუძლია მიუერთდეს საჯარო ბლოკჩეინის ქსელს.

3. დეცენტრალიზაცია

აგებულების მიხედვით ბლოკჩეინ ტექნოლოგიის მთავარი მახასიათებელი სწორედ დეცენტრალიზებული სტრუქტურაა.

ნებისმიერი ქმედება, ტრანზაქცია, რომელიც ბლოკჩეინში ხდება, აისახება მთლიან ქსელზე. შესაბამისად, გადაწყვეტილების მიღებისათვის საჭიროა ქსელის მონაწილე სუბიექტების, ნოდების, კონსენსუსი. რაც უფრო მეტი ნოდია ჩართული ქსელში, მით უფრო დაცულად ითვლება ის კონკრეტული ბლოკჩეინი, რადგან ტექნიკურად

---

[3] *B. Maurenbrecher/U. Meier*, „Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen“, Jusletter, 4.12.2017, 3.

[4] საჯარო და პირადი გასაღებების შესახებ იხ. დეტალურად *Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone,* Blockchain Technology Overview, NISTIR 8202, October 2018, U.S. Department of Commerce, National Institute of Standards and Technology; https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

[5] ნოდების შესახებ დეტალური ინფორმაციისთვის იხ. https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f.

უფრო რთულია მცდარი გადაწყვეტილების მიღება ან ქსელზე ჰაკერული შეტევის განხორციელება.

III. ბლოკჩეინ ტექნოლოგიისა და პერსონალური მონაცემების ურთიერთმიმართება

საჯარო ბლოკჩეინის გამოყენება, მაგალითად, ისეთის, როგორიცაა ბიტკოინის ბლოკჩეინი, ეწინააღმდეგება პერსონალურ მონაცემთა დაცვის კანონმდებლობას: ყველა ტრანზაქცია - მიუხედავად იმისა, რომ ისინი დაშიფრულია - ყოველთვის წარმოადგენს ხილულს[6]. ბლოკჩეინის ფუნქციონირებას საფუძვლად უდევს განაწილებული სააღრიცხვო რეესტრის ტექნოლოგია (distributed ledger technology), რომელიც, პირველ რიგში, ხასიათდება იმით, რომ შესაძლებელია ბლოკჩეინ სისტემაში ინფორმაციის შეტანა ისე, რომ ვერ მოხდეს მისი უკან გამოხმობა. საბოლოოდ კი ნოდების მიერ შეტანილი ინფორმაციის შემოწმების და ვალიდაციის, შემდგომ ეს ინფორმაცია ხდება შეუქცევადი და უცვლელი.

აღნიშნულიდან გამომდინარე, საჭიროა, ყურადღება გავამახვილოთ ბლოკჩეინ ტექნოლოგიის შემდეგ ორ მნიშვნელოვან თვისებაზე[7]:

მონაცემების უცვლელობა (Unabänderbarkeit, immutability) და მონაცემების უტყუარობა მონაცემების შეუქცევადობის საფუძველზე (Unwiderlegbarkeit, irrefutability).

ცალკე აღებული ზემოაღნიშნული ბლოკჩეინის ორივე თვისება მეტად პრობლემურია, რადგან პირდაპირ წინააღმდეგობაში მოდის GDPR-ით ისეთ უფლებებთან, როგორიცაა, მაგალითად, შესწორების (წაშლის) უფლება.

GDPR მონაცემთა სუბიექტს ანიჭებს უფლებას, განკარგოს საკუთარი პერსონალური მონაცემები საკუთარი ნების შესაბამისად. განკარგვაში მოიაზრება პირის უფლება, მოსთხოვოს ინფორმაციის დამმუშავებელს პერსონალური მონაცემების შეცვლა, წაშლა და მართლმსაჯულების დავიწყების უფლება (das Recht auf Vergessenwerden), რომელმაც შემდგომი ასახვა ჰპოვა GDPR-ის მე-17 მუხლში[8]. მონაცემთა სუბიექტზე GDPR-ით მინიჭებული უფლებების დიდი ნაწილი წარმოადგენს დროში შეუზღუდავ უფლებას, რომელზეც რაიმე ხანდაზმულობის ვადა არ ვრცელდება.

შესაბამისად, თუ გავითვალისწინებთ იმ ფაქტს, რომ ბლოკჩეინზე ჩატვირთული ინფორმაცია არის განუსაზღვრელი პერიოდით შენახული და შეუძლებელია მისი შეცვლა, ერთი შეხედვით, ნათელია, რომ აღნიშნული თვისებები არათავსებადს ხდის ბლოკჩეინ ტექნოლოგიას პერსონალური მონაცემების შესახებ კანონმდებლობასთან.

---

[6] *Fasching*, Anwendungsbereiche und ausgewählte Rechtsfragen der Blockchain-Technologie, Wien 2017, 9 http://www.it-law.at/publikation/anwendungsbereiche-und-ausgewaehlte-rechtsfragen-der-blockchain-technologie/; *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 6, https://bitcoin.org/bitcoin.pdf.

[7] *Rainer Böhme / Paulina Pesch*, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-
Technologie, in: Datenschutz und Datensicherheit 2017, 473.

[8] მართლმსაჯულების ევროპული სასამართლოს გადაწყვეტილება C-131/12; 13.05.2014; http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=475998.

IV. პერსონალურ მონაცემთა კანონმდებლობის გავრცელება ბლოკჩეინ სისტემაზე

საკმაოდ გავრცელებული მოსაზრების თანახმად[9], ბლოკჩეინ სისტემის არათავსებადობა პერსონალური მონაცემების კანონმდებლობასთან არ წარმოადგენს პრობლემატურ საკითხს.

მიუხედავად იმისა, რომ ბლოკჩეინში შეტანილი ინფორმაცია წარმოადგენს საჯაროდ ხელმისაწვდომს, შეუძლებელია არსებული ინფორმაცის დაკავშირება კონკრეტულ ფიზიკურ პირთან, რაც იმთავითვე გამორიცხავს მის იდენტიფიცირებას.

მაგალითად, ბიტკოინის ბლოკჩეინის ერთ-ერთი მიზანი სწორედ გადახდის ტრანზაქციების ანონიმურობაა[10]. ტრანზაქციაში მონაწილე მხარის ანონიმურობა სწორედ მისი და დეცენტრალიზებული ქსელის მიერ არის გარანტირებული[11]. ანონიმურობის დროს კი შეუძლებელია ინფორმაციის დაკავშირება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან, რაც თავისთავად გამორიცხავს ზემოაღნიშნული მონაცემების პერსონალურ მონაცემებად დაკვალიფიცირებას. აღნიშნული მოსაზრების თანახმად, შესაძლოა ჩაითვალოს, რომ ბლოკჩეინის ტექნოლოგია, მიუხედავად მისი შეუზღუდავი საჯაროობისა, არ არღვევს პერსონალური მონაცემების შესახებ კანონმდებლობის ნორმებს, რადგან მასზე აღნიშნული არ ვრცელდება.

1. ინფორმაციისა და სუბიექტის კავშირი (Personenbezug)

GDPR-ის მე-4 მუხლის თანახმად, პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. ნებისმიერი ინფორმაცია მოიცავს ინფორმაციის ერთობლიობას, რომელიც ნებისმიერი კუთხით მიუთითებს კონკრეტულ ფიზიკურ პირზე. ინფორმაციისა და ფიზიკური პირის იდენტიფიკაციის კავშირის დასადგენად იურიდიულ ლიტერატურაში გამოყოფენ ორ თეორიას:

აბსოლუტური, იგივე ობიექტური თეორიის, თანახმად, ჰიპოთეტური ვარაუდიც კი, რომ მონაცემთა ბაზაში შენახული ინფორმაცია შესაძლოა მესამე პირმა დაუკავშიროს კონკრეტულ სუბიექტს და ამის შესაბამისად მოახდინოს მისი იდენტიფიცირება, გვაძლევს შესაძლებლობას დავასკვნათ, რომ სახეზე გვაქვს პერსონალური მონაცემი[12]. აღნიშნული თეორია არ განიხილავს, თუ რამდენად შესაძლებელია ტექნიკურად მესამე პირის მიერ სუბიექტის იდენტიფიცირება. შესაბამისად, თუ გავითვალისწინებთ იმ ფაქტს, რომ, მაგალითად, კრიპტო საფულის პროვაიდერი კომპანიები ან კრიპტო ბირჟები ფლობენ დამატებით ინფორმაციას ბლოკჩეინში მონაწილე სუბიექტებზე, შეგვიძლია აბსოლუ-

[9] *Francesco Rampone*, Ciberspazio e diritto, vol. 19, n. 61 (3 - 2018), pp. 457-20
https://poseidon01.ssrn.com/delivery.php?ID=310013021027066030080095031005119123059041038044021064118028087030123015002096030104053039042027114097000125127070086097101074019061023049001005067105092118013097104038043001072125029108091003116022006124001115085086007123101012111030110117086115074115&EXT=pdf.

[10] *Alexander Schmid*, Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, in: Jusletter 4.06.2012, Rz 9.

[11] *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 6: „privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone“

[12] *Pahlen/Brandt*, Datenschutz und Datensicherheit (DuD) 2008, 34.

ტური თეორიის თანახმად მივიდეთ იმ დასკვნამდე, რომ ბლოკჩეინზე შესრულებულ ნებისმიერ ტრანზაქციაში მითითებული თითოეული გამგზავნის და მიმღების მისამართი წარმოადგენს პერსონალურ მონაცემს.

ფარდობითობის თეორიის, იგივე სუბიექტური თეორიის, თანახმად, მნიშვნელოვანია დადგინდეს, შეუძლია თუ არა პირს, რომელსაც წვდომა აქვს მონაცემთა ბაზაზე, კონკრეტული პირის იდენტიფიცირება სხვა დამატებითი ინფორმაციის გარეშე, მხოლოდ მონაცემთა ბაზაში შენახული ინფორმაციის საფუძველზე.[13]

მართლმსაჯულების ევროპულმა სასამართლომ[14] საკუთარ გადაწყვეტილებაში გამოიყენა სწორედ ფარდობითობის თეორია და განსაზღვრა, რომ IP მისამართი მხოლოდ მაშინ შეიძლება ჩაითვალოს პერსონალურ მონაცემად, როდესაც პასუხისმგებელ პირს, მაგალითისათვის, ინტერნეტ პროვაიდერს, აქვს შესაძლებლობა, მის მიერ სამართლებრივი გზით მოპოვებული სხვა დამატებითი ინფორმაციის საფუძველზე (აღნიშნულის ქვეშ შეგვიძლია მოვიაზროთ ის პერსონალური ინფორმაცია, რომელსაც მომხმარებელი გადასცემს ინტერნეტ პროვაიდერს თუნდაც პროვაიდერთან პირველადი რეგისტრაციის დროს) აქვს შესაძლებლობა, მოახდინოს კონკრეტული ფიზიკური პირის იდენტიფიკაცია.

საჯარო ბლოკჩეინზე განხორციელებულ ტრანზაქციებში, ერთი შეხედვით, არ გვხვდება ისეთი პერსონალური მონაცემები, როგორიც არის მაგალითად სახელი, გვარი ან საცხოვრებელი მისამართი.

დეცენტრალიზებულ ქსელში გამგზავნი და მიმღები არ არიან ვალდებულნი საკუთარი ვინაობა გაამხილონ. აღნიშნულიდან გამომდინარე, ბლოკჩეინის საჯარო მისამართი ერთი შეხედვით არ გვაძლევს პირდაპირ წვდომას მის უკან მდგომი პიროვნების შესახებ.

ბლოკჩეინზე განხორციელებული ტრანზაქციების ანონიმურობა, რეალურად, წარმოადგენს მხოლოდ ვარაუდზე დამყარებულ მოსაზრებას. მომხმარებელი, რომელიც მონაწილეობს ტრანზაქციაში იყენებს კრიპტოგრაფიულ საჯარო გასაღებს, რომელიც ფსევდონიმურია (pseudonym)[15].

კორნელის უნივერსიტეტის კვლევით[16] დადასტურებულია, რომ ბიტკოინის მისამართებით შესაძლებელია გადამხდელისა და მიმღების IP მისამართების დადგენა. შესაბამისად, იმ შემთხვევაში, თუ სუბიექტი ერთი და იმავე საჯარო გასაღებით ასრულებს ბლოკჩეინში ტრანზაქციებს და ქსელში მის მიერ განხორციელებულ ტრანზაქციებს კარგად შევისწავლით, შესაძლებელი იქნება ტრანზაქციის განმახორციელებელი სუბიექტის IP მისამართის დადგენა.

მართლმსაჯულების ევროპული სასამართლოს პრაქტიკის[17] გათვალისწინებით, თუ სუბიექტმა იცის ტრანზაქციის განმახორციელებლის IP მისამართი და მას კანონიერი გზით მოპოვებული აქვს აღნიშნული IP მისამართის უკან მდგომი პირის ისეთი დამატებითი ინფორმაცია, რომლის საშუალებითაც მოხდება ამ უკანასკნელის იდენტიფიცირება, თამამად შეგვიძლია დავასკვნათ, რომ ბლოკჩეინში განხორციელე-

[13] *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 3.

[14] ECJ: ECLI:EU:C:2016:779; ბრეიერი გერმანიის წინააღმდეგ 19.10.2016.

[15] *Rainer Böhme / Paulina Pesch,* Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-
Technologie, in: Datenschutz und Datensicherheit 2017, 478.

[16] *Alex Biryukov / Dmitry Khovratovich / Ivan Pustogarov*, Deanonymisation of Clients in Bitcoin P2P Network, 5.07.2014, https://arxiv.org/abs/1405.7418

[17] ECJ: ECLI:EU:C:2016:779; ბრეიერი გერმანიის წინააღმდეგ 19. ოქტომბერი 2016.

ბული ტრანზაქციები წარმოადგენს პერსონალურ მონაცემებს.

პრაქტიკაში გასათვალისწინებელია ის, რომ ბლოკჩეინ სისტემაში საკმაოდ დიდი ოდენობით გვხვდება ისეთი მესამე პირები, როგორებიც არიან, მაგალითად კრიპტო ბირჟები და კრიპტოსაფულის პროვაიდერები, რომლებიც კანონიერი გზით ფლობენ მათი ბენეფიციარების შესახებ პერსონალურ ინფორმაციებს.

შესაბამისად, დასკვნის სახით მიზანშეწონილია ითქვას, რომ ბლოკჩეინ სისტემა ექცევა GDPR-ის რეგულირების არეალში, რადგან სახეზე გვაქვს ისეთი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. შედეგად, აზრს მოკლებული იქნება ბლოკჩეინის სრულ ანონიმურობაზე საუბარი.

2. პასუხისმგებელი პირი

ა) პერსონალურ მონაცემთა დამმუშავებელი სუბიექტი

აა) შვეიცარია

ვინაიდან შვეიცარული პერსონალურ მონაცემთა დაცვის შესახებ კანონი (შემდგომში DSG) GDPR-ისგან განსხვავებულად არეგულირებს მონაცემთა დამმუშავებლის განსაზღვრის საკითხს, საინტერესოა, ყურადღება გამახვილდეს შვეიცარული კანონმდებლობის დანაწესზე. DSG-ს თანახმად, მონაცემთა დამმუშავებელი ვალდებულია მონაცემები კანონმდებლობის ნორმების შესაბამისად დაამუშავოს, უფრო კონკრეტულად კი DSG-ს მე-4 მუხლით გათვალისწინებული მოთხოვნების დაცვით. მონაცემთა დამმუშავებელმა უნდა უზრუნველყოს მის მიერ დამუშავებული მონაცემების უტყუარობა (მუხლი 5 DSG) და უნდა იზრუნოს მონაცემების უსაფრთხოებაზე (მუხლი 7 DSG). შვეიცარიელმა კანონმდებელმა არ განსაზღვრა წინასწარ, რომ ზემოაღნიშნული ვალდებულებები კოლექტიურად დაკისრებოდა რამდენიმე პირს ან რაიმე მექანიზმის მეშვეობით მომხდარიყო ერთი კონკრეტული პირის იდენტიფიცირება, რომელიც, საბოლოო ჯამში, განხილული იქნებოდა როგორც ინფორმაციის დამმუშავებელი.[18] აღნიშნულიდან გამომდინარე შეგვიძლია დავასკვნათ, რომ, შვეიცარიის კანონმდებლობის თანახმად, ყველა სუბიექტი, რომელიც ბლოკჩეინის სისტემაში იღებს მონაწილეობას, შეიძლება მოვიაზროთ როგორც ინფორმაციის დამმუშავებელი და მასზეც გავრცელდეს DSG-ით გათვალისწინებული პასუხისმგებლობები და ვალდებულებები.

აღნიშნული დანაწესი ადგენს იმ პირთა საკმაოდ დიდ წრეს, რომელთაც ეკისრებათ ისეთი ვალდებულებების შესრულება და ამ ვალდებულებების შეუსრულებლობისათვის პასუხისმგებლობა, რომლის განხორციელებაც ბლოკჩეინ სისტემაში ფაქტობრივად შეუძლებელია.

ბბ) GDPR

შვეიცარული კანონმდებლობისგან განსხვავებით GDPR-ი არ მოიაზრებს ყველა სუბიექტს მონაცემთა დამმუშავებლად და არ ახდენს მათზე ერთნაირი ვალდებულებების დაკისრებას. აღნიშნული რეგულაციის თანახმად, შეგვიძლია გამოვყოთ 4 მნიშვნელოვანი სუბიექტი:

- მონაცემთა სუბიექტი - იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირი;
- მონაცემთა დამმუშავებელი - საჯარო დაწესებულება, ფიზიკური ან იურიდი-

[18] *David Rosenthal / Yvonne Jöhri* (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 Bst. j DSG, N 116.

ული პირი, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას;

- უფლებამოსილი პირი – ნებისმიერი ფიზიკური ან იურიდიული პირი, რომელიც ამუშავებს მონაცემებს მონაცემთა დამმუშავებლისათვის ან მისი სახელით;
- მესამე პირი – ნებისმიერი ფიზიკური ან იურიდიული პირი, საჯარო დაწესებულება, გარდა მონაცემთა სუბიექტისა, სახელმწიფო ინსპექტორის სამსახურისა, მონაცემთა დამმუშავებლისა და უფლებამოსილი პირისა;

აღნიშნული ჩამონათვალი ემყარება იმ იდეას, რომ მონაცემების დამუშავება ყოველთვის ხდება იერარქიული თანმიმდევრობით. მონაცემთა დამმუშავებელი თავად განსაზღვრავს მონაცემების დამუშავების მიზანს და საშუალებას. შემდეგ კი ან თავად ახდენს მათ დამუშავებას, ან უფლებამოსილ პირზე ახდენს დელეგირებას. აღნიშნული მიუთითებს იმაზე, რომ GDPR მონაცემების დამუშავებისათვის პასუხისმგებლობის დაკისრებას ან მხოლოდ მონაცემთა დამმუშავებელზე ახდენს (თუ იგი თავად ჩადის აღნიშნულ ქმედებას) ან კიდევ უფლებამოსილ პირზე[19]. შვეიცარიული კანონმდებლისგან განსხვავებით სახეზეა მონაცემების დამმუშავებელი პირების დიფერენცირება, რის საფუძველზეც არ ხდება უფლებამოსილი პირისათვის და მონაცემთა დამმუშავებლისათვის ერთნაირი პასუხისმგებლობის დაკისრება.

GDPR-ის 26-ე მუხლი ითვალისწინებს კოლექტიურ პასუხისმგებლობას, ანუ იძლევა იმის შესაძლებლობას, რომ რამდენიმე სუბიექტს ერთობლივად დაეკისროს ვალდებულება და პასუხისმგებლობა მონაცემთა დამუშავებაზე. აღნიშნული მუხლი მიზნად ისახავს ისეთი ფაქტობრივი გარემოების დარეგულირებას, რომელშიც სხვადასხვა ინფორმაციის დამმუშავებლები ორგანიზებულად მიიღებენ გადაწყვეტილებას, რომ საერთო მიზნის მისაღწევად კოლექტიურად დაამუშაონ ინფორმაცია.

აღნიშნული ნორმა მიზნად ისახავს, ერთი მხრივ, ისეთი კომპლექსური ეკოსისტემების მონაწილე პირების იდენტიფიკაციას, რომლებშიც მრავალი სუბიექტი ფარულად და კანონსაწინააღმდეგოდ მოქმედებს. მეორე მხრივ, თითოეული ასეთი მონაწილე პირისათვის ორგანიზებული/თანმიმდევრული და კონტროლირებადი პასუხისმგებლობის დაკისრებას, მათ მიერ ჩადენილი მკაფიოდ განსაზღვრული ქმედებებისათვის.[20]

აღნიშნული მიდგომა კი შეუძლებელია გამოყენებული იქნას საჯარო ბლოკჩეინთან მიმართებით.[21] საჯარო ბლოკჩეინში მონაწილე პირები კოლექტიურად არ ამუშავებენ მონაცემებს იმ მიზნით, რომ რაიმე ტიპის კანონსაწინააღმდეგო შედეგი მიიღონ. მათი მიზანია ტრანზაქციების დადასტურება და ბლოკჩეინ სისტემის გამართული მუშაობის უზრუნველყოფა, რაც წინააღმდეგობაში არ მოდის GDPR-ის 26-ე მუხლის მიზნებთან.

[19] მონაცემთა დამმუშავებლის და უფლებამოსილი პირის დეფინიციისთვის იხ. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[20] *Jürgen Kühling / Benedikt Buchner* (Hrsg.), DS-GVO Kommentar, München 2017, Art. 26, N 10.

[21] *Rainer Böhme / Paulina Pesch*, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, in: Datenschutz und Datensicherheit 2017, 479.

ბ) პერსონალურ მონაცემთა დამმუშავებელი სუბიექტის განსაზღვრა ბლოკჩეინში

ბლოკჩეინის სისტემაში, რომელიც ერთგვარ კოლაბორაციულ სისტემას წარმოადგენს, მეტად რთული და ბუნდოვანი საკითხია მონაცემთა დამმუშავებლის ანუ პასუხისმგებელი პირის დადგენა. აღნიშნულის მიზეზს წარმოადგენს ზუსტად ის, რომ ტექნოლოგია, კონკრეტულად კი მასში მონაცემების ჩაწერა და დამუშავება ეფუძნება დეცენტრალიზაციის პრინციპს. პოტენციურ პასუხისმგებელ პირად შეგვიძლია მოვიაზროთ პირები რომლებმაც ბლოკჩეინი დააპროგრამირეს; პირი რომელმაც იმპლემენტაცია მოახდინა ბლოკჩეინის პირველად ქსელში; ბლოკჩეინ სისტემის მონაწილე პირი, რომელიც ახორციელებს ან/და ადასტურებს ტრანზაქციებს;

ლიტერატურაში აღნიშნული პრობლემის გადაჭრის სხვადასხვა გზაა შემოთავაზებული. *ფაშლინგი*[22] საკუთარ ნაშრომში მონაცემთა დამუშავებისათვის პასუხისმგებლობას აკისრებს იმ კონკრეტულ ჯგუფს, რომელიც მუშაობს ბლოკჩეინის განვითარებაზე, კონკრეტულად კი იმ პირებს, რომლებიც ახდენენ ცვლილებების ტესტირებას და იმპლემენტაციას ბლოკჩეინში. სამწუხაროდ, აღნიშნული მოსაზრება არ შეესაბამება GDPR-ის მოთხოვნებს, რადგან GDPR-ის გამოყენების სფერო შემოიფარგლება მხოლოდ მონაცემთა დამუშავებით, შესაბამისად, პირებზე, რომლებიც მონაცემებს არ ამუშავებენ, არ შეიძლება გავრცელდეს GDPR-ით გათვალისწინებული პასუხისმგებლობა მონაცემთა დამუშავებისათვის. სისტემის და პროგრამის მწარმოებლები, ამ კონკრეტულ შემთხვევაში ბლოკჩეინ სისტემის განმავითარებლები, არ წამოადგენენ მონაცემთა დამმუშავებელ პირებს[23]. ბლოკჩეინ სისტემის განმავითარებელი თვითონ არ არის ამ სისტემის მომხმარებელი. ის არ იღებს მონაწილეობას ქსელის მიერ გადაწყვეტილების მიღებაში. შესაბამისად, მას არ აქვს არც შესაძლებლობა და არც მიზანი, რომ მიიღოს მონაწილეობა საჯარო ბლოკჩენზე მონაცემების დამუშავებაში.

კიდევ ერთი გავრცელებული მოსაზრების[24] თანახმად, გადაწყვეტილების მიღებაში მონაწილე სუბიექტები, ანუ მაინერები (ნოდები) არიან პერსონალური მონაცემების დამუშავებისთვის პასუხისმგებელი პირები. თუ აღნიშნულ მოსაზრებას გავითვალისწინებთ, მაშინ მაინერები (ნოდები) ვალდებულნი არიან, უზრუნველყონ ყველა იმ ვალდებულების შესრულება, რომლებსაც კანონმდებლობა ავალდებულებს მონაცემების დამმუშავებელს. ასეთ შემთხვევაში მართებული იქნება, თუ საჯარო და დახურული ბლოკჩეინის მაგალითებს ცალცალკე განვიხილავთ. იმ შემთხვევაში, თუ დახურულ ბლოკჩეინში მაინერებს (ნოდებს) დაევალებათ კონკრეტული ინფორმაციის შეცვლა, თეორიულად და ტექნიკურად შესაძლებელია, რომ მათ ეს ინფორმაცია შეცვალონ. საჯარო ბლოკჩეინისგან განსხავებით, დახურული ბლოკჩეინი შედგება მხოლოდ კონკრეტული შეზღუდული ოდენობის მონაწილე იდენტიფიცირებულები პირებისაგან, და არის იმის შესაძლე-

[22] *Joachim Galileo Fasching*, Anwendungsbereiche und ausgewählte Rechtsfragen der Blockchain-Technologie, ვენა, ავსტრია 2017 წელი, 9, http://www.it-law.at/publikation/anwendungsbereiche-und-ausgewaehlte-rechtsfragen-der-blockchain-technologie/, 20.

[23] *Jürgen Hartung, in: Jürgen Kühling / Benedikt Buchner* (Hrsg.), DS-GVO Kommentar, München 2017, Art. 24,

[24] *Jacek Czarnecki*, Blockchains and Personal Data Protection Regulations Explained, in: Coindesk, 26.04.2017, https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/.

ბლობა, რომ ისინი შეთანხმდნენ ინფორმაციის შეცვლაზე. რაც შეეხება საჯარო ბლოკჩეინს, გარდა ფაქტობრივი სირთულეებისა, როგორიცაა, მაგალითად, თითოეული მაინერის (ნოდის) იდენტიფიცირება, სახეზე გვაქვს კიდევ ერთი მნიშვნელოვანი პრობლემა. თუ კანონმდებელი საკუთარ იურისდიქციაში მყოფ მაინერებს დაავალდებულებს, რომ უზრუნველყონ კონკრეტული პერსონალური მონაცემის ცვლილება, აღნიშნული მაინერები (ნოდები) ტექნიკური თვალსაზრისით მოკლებულნი არიან შესაძლებლობას, მარტომ აღასრულონ ეს კონკრეტული ვალდებულება.[25]

უნგრეთის პერსონალურ მონაცემთა დაცვის ინსპექტორმა საკითხზე, თუ ვის უნდა დაეკისროს მონაცემთა დამუშავებისათვის პასუხისმგებლობა ბლოკჩეინში, ასევე გააკეთა განმარტება, რომლის თანახმადაც, ბლოკჩეინ სისტემაში (მიუხედავად იმისა, საჯაროა თუ დახურული იგი) მონაწილე ნებისმიერი სუბიექტი უნდა დაკვალიფიცირდეს, როგორც ინფორმაციის დამმუშავებელი და დაეკისროს პასუხისმგებლობა.[26] აღნიშნული მოსაზრების გათვალისწინება არ არის მიზანშეწონილი, რადგან იგი უფრო აფართოებს პასუხისმგებელ პირთა წრეს, ნაცვლად იმისა, რომ კონკრეტიზაცია მოახდინოს. შესაბამისად უფრო მეტად შეუძლებელია პრაქტიკაში მისი განხორციელება.

საჯარო ბლოკჩეინი, როგორც უკვე აღინიშნა, სრულად ემყარება დეცენტრალიზაციის იდეას. შესაბამისად, წარმოადგენს გაწილებულ სისტემას, რომელსაც არ გააჩნია ერთი ცენტრალური მაკონტროლებელი სუბიექტი. აღნიშნულიდან გამომდინარე GDPR-ის დღევანდელი დანაწესის შესაბამისად, ტექნიკურად შეუძლებელია მონაცემთა დამმუშავებელი პირების იდენტიფიცირება და მათზე გარკვეული ვალდებულებისა თუ პასუხისმგებლობის დაკისრება.

3. მონაცემთა სუბიექტის უფლებები

ბლოკჩეინ სისტემის თვისება, რომელიც უზრუნველყოფს მასში არსებული მონაცემების უცვლელობას, როგორც უკვე ზემოთ აღინიშნა, პირდაპირ წინააღმდეგობაში მოდის GDPR-ით განსაზღვრულ დანაწესებთან, კონკრეტულად კი მონაცემთა სუბიექტის შემდეგ უფლებებთან: მონაცემთა სუბიექტის უფლება ჰქონდეს წვდომა ყველა მის პერსონალურ მონაცემზე, რომლის დამუშავებასაც ახდენს მონაცემთა დამმუშავებელი, მონაცემებთან წვდომის უფლება (მუხლი 15 GDPR), დამუშავების შეწყვეტის მოთხოვნის უფლება (მუხლი 21 GDPR), მონაცემთა წაშლის უფლება (მუხლი 17 I GDPR), დავიწყების უფლება[27] (das Recht auf Vergessenwerden) (მუხლი 17 II GDPR), პერსონალურ მონაცემებში ცვლილების შეტანის უფლება (მუხლი 16. GDPR), მონაცემთა ბლოკირების უფლება (მუხლი 18. GDPR).

მნიშვნელოვანი არის, პასუხი გაეცეს კითხვებს, ერთმევა თუ არა ბლოკჩეინ სისტემაში მონაწილე პირს GDPR-ით მისთვის მინიჭებული უფლებები, შესაძლებელია თუ არა ამ უფლებების განხორციელება ისეთ სისტემაში, რომელიც გამორიცხავს მასში შეტანილი მონაცემების ცვლილებას და

[25] *Rainer Böhme / Paulina Pesch*, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, in: Datenschutz und Datensicherheit 2017, 478.

[26] *Dóra Petrányi / Marton Domokos*, Hungary: Data Protection Aspects of Blockchain, 17.08.2017, http://www.cms-lawnow.com/ealerts/2017/08/hungary-data-protection-aspects-of-blockchain.

[27] დამატებითი ინფორმაციისთვის იხ. *Kubis,* Das „Recht auf Vergessenwerden“, DuD 9/2017, 583.

ასეთი მონაცემები განუსაზღვრელი ვადით არის საჯაროდ შენახული.

ა) პერსონალურ მონაცემებში ცვლილების შეტანის უფლება

პერსონალურ მონაცემებში ცვლილების შეტანის უფლება არ არის თავსებადი ბლოკჩეინ სისტემასთან, თუ გავითვალისწინებთ მის მთავარ თვისებას - შეუცვლელობას (Unveränderbarkeit). პრაქტიკული თვალსაზრისით, ნებისმიერი ცვლილების შეტანა ბლოკჩეინ სისტემაში არის შესაძლებელი მხოლოდ ეგრეთ წოდებული 51% შეტევის (51% attac) განხორციელების გზით[28]. ბლოკჩეინის სისტემაში უნდა მოხდეს ფაქტობრივი ტრანზაქციის ინიცირება, რომელსაც სისტემაში მონაწილე პირების 51 პროცენტი დაეთანხმება და შემდგომ მოხდება ინფორმაციის ბლოკში გენერირება. აღნიშნულის პრაქტიკაში განხორციელება პირად ანუ დახურულ ბლოკჩეინში თეორიულად შესაძლებელია, რადგან მასში მონაწილე პირები იდენტიფიცირებულები არიან და შესაძლებელია თეორიულად მათი დავალდებულება, განახორციელონ შესაბამისი ცვლილება. რაც შეეხება საჯარო ბლოკჩეინს, იმ ფაქტორის გათვალისწინებით რომ სახეზე გვყავს საკმაოდ დიდი ოდენობის ნოდები სხვადასხვა იურისდიქციაში, ფაქტობრივად, შეუძლებელი ხდება ასეთი ფიქტიური ტრანზაქციის განხორციელება. შესაბამისად, პერსონალური მონაცემების სუბიექტი მოკლებულია შესაძლებლობას, გამოიყენოს მისთვის GDPR-ის 21-ე მუხლით მინიჭებული უფლება და მოითხოვოს მის დამუშავებულ პერსონალურ მონაცემებში ცვლილების შეტანა.

ბ) მონაცემთა წაშლის უფლება

პერსონალურ მონაცემებში ცვლილების შეტანის უფლების მსგავსად მონაცემთა სუბიექტი მოკლებულია შესაძლებლობას, გამოიყენოს მონაცემთა წაშლის უფლება ბლოკჩეინ სისტემაში. GDPR-ის მოთხოვნების შესაბამისად, პერსონალური მონაცემები შენახული უნდა იყოს იმ დროის განმავლობაში, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად[29]. ინფორმაციის დამმუშავებლის მიერ აღნიშნული მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს.[30]

აღნიშნული პრობლემის მოგვარების საშუალებად შესაძლოა განხილულ იქნეს მონაცემთა ბლოკირება, ანუ მათი ისეთი მოდიფიკაცია, რომ შეუძლებელი იყოს ინფორმაციის მოპოვება არაპროპორციულად დიდ ძალისხმევისა და ხარჯებსა გაღების გარეშე.

თუ გავითვალისწინებთ ბლოქჩეინის ერთ-ერთ მთავარ პლუსს, რომელიც მდგომარეობს მის საჯაროობაში და სისტემის სანდოობის უზრუნველყოფაში, მარტივი დასადგენია, რომ მასში არსებული ინფორმაციის ბლოკირება პირდაპირ წინააღმდეგობაში მოვა ბლოკჩეინის სანდოობის ფუნქციასთან. გარდა ამისა, ბლოკჩეინზე მონაცემების დაბლოკვა წარმოშობს მრავალ ტექნიკურ პრობლემას, რის გამოც შეიძლება დასკვნის სახით ითქვას, რომ პერსონალური მონაცემების ბლოკირება ვერ განიხილება აღნიშნული პრობლემის გადაჭრის გზად.

[28] 51% შეტევასთან დაკავშირებით იხ. https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474.

[29] GDPR-ის მე-5 მუხლი „მონაცემთა დამუშავების პრინციპები“.

[30] დამატებითი ინფორმაციისთვის იხ. *Hofert,* Zeitschrift für Datenschutz (ZD) 2017, 61.

გ) დავიწყების უფლება

GDPR-ის მე -17 II მუხლის თანახმად, მონაცემთა დამმუშავებელი პირი ვალდებულია, აცნობოს მონაცემთა ყველა მიმღებს მონაცემთა წაშლის საჭიროების თაობაზე, თუ ეს არ მოითხოვს არაპროპორციულად დიდ ძალისხმევას (დავიწყების უფლება). იმ შემთხვევაში როდესაც ინფორმაციის დამმუშავებელს, მონაცემთა სუბიექტის მოთხოვნის საფუძველზე ევალება საჯაროდ (მაგალითად, ინტერნეტში) გამოქვეყნებული მონაცემების წაშლა, მან ამის შესახებ, არსებული ტექნოლოგიებისა და ხარჯების გათვალისწინებით, უნდა აცნობოს სხვა ორგანიზაციებს, რომლებიც ამავე მონაცემებს ამუშავებენ.

აღნიშნული მუხლის მიზნებისათვის საჯაროდ გამოქვეყნებულად მიიჩნევა ისეთი ინფორმაცია, რომელიც ხელმისაწვდომია პირთა განუსაზღვრელი წრისათვის.[31]

ვინაიდან საჯარო ბლოკჩეინში სახეზე გვაქვს სწორედ პირთა განუსაზღვრელი წრე, რომელსაც წვდომა აქვს პერსონალურ ინფორმაციაზე, მონაცემთა სუბიექტის მიერ შესაძლებელია, რომ დაყენებულ იქნას მოთხოვნა GDPR-ის მე-17 II მუხლიდან გამომდინარე. სამწუხაროდ, მონაცემთა სუბიექტის ასეთი მოთხოვნა ზემოაღნიშნული ტექნიკური მიზნებიდან და ბლოკჩეინ ტექნილიგიის სპეციფიკიდან გამომდინარე შეუძლებელია, რომ პრაქტიკაში განხორციელდეს.

V. დასკვნა

ბლოკჩეინ ტექნოლოგია ბევრ ასპექტში მოდის მონაცემთა დაცვის შესახებ კანონმდებლობასთან წინააღმდეგობაში. მიუხედავად იმისა, რომ საჯარო ბლოკჩეინზე არსებული მონაცემები, ერთ შეხედვით, დაშიფრულია, მაინც არის იმის შესაძლებლობა, რომ ეს ინფორმაციები დაკავშირებული იქნეს იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან. შესაბამისად, შესაძლებელია, რომ ასეთი მონაცემები დაკვალიფიცირდეს პერსონალურ მონაცემებად.

ამასთან, საჯარო ბლოკჩეინის დეცენტრალიზებული არქიტექტურა საკმაოდ დიდ პრობლემას უქმნის პერსონალურ მონაცემთა დაცვას. ზემოთ მოყვანილი ანალიზი ცხადყოფს, რომ სწორედ განუსაზღვრელი რაოდენობის ნოდებზე დაფუძნებულ ქსელში შეუძლებელია განისაზღვროს ინფორმაციის დამმუშავებელი პირი, რომელსაც დაეკისრება კანონმდებლობით განსაზღვრული ვალდებულებები და პასუხისმგებლობები.

მიუხედავად ყველა კრიტიკისა თუ ეჭვისა, არ უნდა დაგვავიწყდეს, რომ ბლოკჩეინ ტექნოლოგიას აქვს საკმაოდ ბევრი დადებითი თვისება, მათ შორის პერსონალური მონაცემების დაცვის სფეროშიც. კანონმდებლის მიერ საჭირო რეგულაციების შემოღების შემთხვევაში, შესაძლოა, რომ ბლოკჩეინ ტექნოლოგიამ სწორედ მონაცემთა დაცვის გაუმჯობესებაში შეიტანოს დიდი წვრილი.

[31] *Nolte/Werkmeister* in *Gola,* Art. 17 Rn. 34.