

დაბლოკილ ციფრულ სივრცეზე წვდომის მოპოვების შესაძლებლობა და თვითინკრიმინაციისგან დაცვის პრივილეგია აშშ-ის სამართალში

გია მარკოიძე

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის მონვეული ლექტორი და დოქტორანტი; ალტე უნივერსიტეტის ასისტენტი; შინაგან საქმეთა სამინისტროს საზღვრის მართვის პოლიტიკის დაგეგმვისა და რისკების შეფასების განყოფილების უფროსი

შესავალი

თანამედროვე ტექნოლოგიურ განვითარებასთან ერთად, უფრო და უფრო რთული ხდება კანონმდებლობისა და პრაქტიკის კომპლექსურ ციფრულ სამყაროზე მორგება. მსგავსი პრობლემატიკა არსებობს, მათ შორის, თვითინკრიმინაციისგან დაცვის პრივილეგიასთან მიმართებითაც. კერძოდ, დოქტრინასა და პრაქტიკაში სადავოა სახელმწიფოს იძულების მექანიზმების გამოყენება იმ მიზნობრივობით, რომ ბრალდებულმა გახსნას/განბლოკოს დაშიფრული მონაცემები.¹ ამ მხრივ, იურიდიული ლიტერატურა არ არის მდიდარი, თუმცა საკითხი უფრო მეტად დამუშავებულია აშშ-ის დოქტრინაში. შესაბამისად, სტატია, საკითხს სწორედ აშშ-ის მაგალითზე განიხილავს.

მითითებული პრობლემა უფრო და უფრო აქტუალური ხდება, ვინაიდან ყოველდღიურ ცხოვრებაში ტექნოლოგიები კიდევ უფრო მეტი მოცულობით იჭრება და ეს სფერო განუწყვეტლივ ვითარდება. მაგალითად, 2018 წლის მონაცემებით, აშშ-ის 18-29 წლის მოქალაქეთა 94% იყენებს სმარტფონს და მათ უმეტესობას დაბლო-

კილ მდგომარეობაში აქვს იმ პერიოდში, როდესაც მისით არ სარგებლობს.² ბოლო პერიოდში განსაკუთრებით განვითარდა კრიპტო სფეროც, რაც გამოძიებისთვის ერთგვარ გამოწვევად იქცა. როდესაც გამოძიებას კრიპტოვალუტით განხორციელებული ტრანზაქციები აინტერესებს, ზოგიერთ შემთხვევაში, ტრანზაქციაში მონაწილე სუბიექტის ანგარიშზე წვდომის გარეშე, შეუძლებელი ხდება ინფორმაციის მოპოვება, რაც საკვლევ საკითხს კიდევ უფრო აქტუალურს ხდის. მსგავსი სისტემების განვითარებასთან ერთად, სავარაუდოა, რომ საქართველოში საგამოძიებო ორგანოების ეფექტიანობის შენარჩუნებისა თუ ზრდისთვის, აუცილებელი გახდება საკანონმდებლო ცვლილებები, რათა შესაბამისი ინფორმაციების მოპოვება შესაძლებელი გახდეს. ამ კუთხით აშშ-ში უკვე ჩამოყალიბებული დოქტრინა და პრაქტიკა ამ პროცესს მნიშვნელოვნად გაამარტივებს.

პრაქტიკაში, როგორც წესი, სამართალდამცავი ორგანოების მიერ მონაცემების გაშიფვრა შესაძლებელია კომპიუტერული ექსპერტიზების დანიშვნით, თუმცა შეიძლება გამოვლინდეს შემთხვევები, როდესაც გაშიფვრა ვერ ხერხდება.³ არსებობს უამრავი პროგრამული

¹ მაგ., In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012) (აკრძალა იძულებითი გაშიფვრა); United States v. Apple MacPro Computer, 851 F.3d 238, 248 & n.7 (3d Cir. 2017) (დაუშვა იძულებითი გაშიფვრა);

² Kerr, O. S., Compelled Decryption and the Privilege against Self-Incrimination, Texas Law Review, Vol. 97, no. 4, 2019, 768.

³ Morrison, C. M., Passwords, Profiles, and the Privilege against Self-Incrimination: Facebook and the Fifth

უზრუნველყოფა, რომლითაც სახელმწიფოს ეზღუდება წვდომა. მაგალითად, არსებობს ე.წ. „უარყოფა“ - მოდელი, რომლითაც ერთი პაროლი გამიფრავს მონყობილობას სრულად, ხოლო მეორე პაროლი - ნაწილობრივ და გარკვეულ ფაილებს დაშიფრულს ტოვებს. ამ დროს სახელმწიფოს ჰგონია, რომ ყველა ფაილი მოიპოვა, თუმცა ეს ასე არ არის.⁴ შესაბამისად, აუცილებელია ბრალდებულის მიერ მონყობილობის გახსნა, რათა სახელმწიფომ მასში არსებული ინფორმაცია სრულად მოიპოვოს.

სახელმწიფო ფიზიკურად ვერ აიძულებს პირს, შეიყვანოს პაროლი ან სხვა მეთოდით გახსნას მონყობილობა - მსგავსი ქცევა ჩათვლება არასათანადო მოპყრობად, რაც აბსოლუტური დაცვით სარგებლობს.⁵ ყველაზე გავრცელებული იძულების მექანიზმია პასუხისმგებლობის დაკისრება, თუ პირი არ გახსნის/განბლოკავს მონყობილობას.⁶

ციფრულ სივრცეზე წვდომის მოპოვებასთან დაკავშირებით სწორი დასკვნების გასაკეთებლად, აუცილებელია ერთმანეთისგან გაიმიჯნოს სახელმწიფოს მიერ იძულების შესაძლო სახეები. როგორც აღინიშნა, იძულების მეთოდი, როგორც წესი, პასუხისმგებლობის დაკისრების მუქარაა, თუმცა მუქარის საგანი შეიძლება სხვადასხვა იყოს.

პირველი, სახელმწიფო აიძულებს ბრალდებულს, რომ ვერბალურად ან წერილობით გადასცეს პაროლი. მეორე, სახელმწიფო აიძულებს ბრალდებულს, გადასცეს ისეთი დოკუმენტი, რომელზეც წერია პაროლი. მესამე, სახელმწიფო აიძულებს მონყობილობაში პაროლის შეყვანას, თუმცა ამ პროცესს არავინ აკვირდება და პაროლიც არსად ინახება. მეოთხე, სახელმწიფო პირს აიძულებს თითის ანაბეჭდით, სახის

ამომცნობით ან სხვა ბიომეტრიული მონაცემით მონყობილობის გახსნას.⁷ სტატიაში თითოეული მეთოდი თვითინკრიმინაციისგან დაცვის პრივილეგიასთან შესაბამისობის ქრილში ცალ-ცალკე არის განხილული.

1. პაროლის გადაცემის იძულების მიმართება თვითინკრიმინაციისგან დაცვის პრივილეგიასთან

აშშ-ის კონსტიტუციის მე-5 შესწორების მიხედვით, დაუშვებელია პირის იძულება, სისხლის სამართლის პროცესის ფარგლებში მისცეს ჩვენება საკუთარი თავის წინააღმდეგ. აღნიშნული შესწორების მიზანია ბრალდებულის დაცვა მართლმსაჯულების სისტემის წინაშე **ბოროტი ტრილემისგან**⁸ - 1. პირმა თქვას სიმართლე და სახელმწიფომ მოიპოვოს მაინკრიმინირებელი ინფორმაცია, 2. მოიტყუოს და თავი გაიმართლოს ან 3. უარი თქვას პასუხის გაცემაზე და დაეკისროს პასუხისმგებლობა.⁹

პაროლის მოთხოვნა სახელმწიფოს შეუძლია სხვადასხვა ფორმით, მაგალითად, გამოკითხვის ან დაკითხვის ფარგლებში. დაკითხვის დროს, მათ შორის, ქართულ რეალობაში, კითხვებზე პასუხის გაცემა სავალდებულოა (გარდა გამოწვევისა), წინააღმდეგ შემთხვევაში, მონეს დაეკისრება სისხლისსამართლებრივი პასუხისმგებლობა. შესაფასებელია იძულების მსგავსი ფორმით ინფორმაციის მოპოვებაზე ვრცელდება თუ არა მე-5 შესწორებით გათვალისწინებული გარანტია.

პაროლის გადაცემის იძულება, არ აქვს მნიშვნელობა, ის გამოსახულია ასოებით, ციფრებით თუ სიმბოლოებით, პირდაპირ მოიცავს ჩვენე-

Amendment, Arkansas Law Review, Vol. 65, no. 1, 2012, 158.

⁴ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 220.

⁵ Gafgen v. Germany [ECHR] #22978/05, 2010 წლის 1-ელი ივნისი, § 107.

⁶ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 221.

⁷ Wiseman, T., A., Encryption, Forced Decryption and the Constitution, A Journal of Law and Policy for the Information Society, 2015, 530-534.

⁸ აშშ-ის დოქტრინისა და პრაქტიკის შესახებ იხ. მარკოიძე, გ., თვითინკრიმინაციისგან დაცვის პრივილეგია ადამიანის უფლებათა ევროპული სასამართლოსა და აშშ-ის უზენაესი სასამართლოს პრაქტიკაში, ადამიანის უფლებების დაცვა, პანდემია და სამართლის უზენაესობა, კონსტანტინე კორკელიას რედაქტორობით, 2021, 173-179.

⁹ Pennsylvania v. Muniz, 496 U.S. 582, 596 (1990).

ბის ელემენტებს, შესაბამისად, უნდა სარგებლობდეს მე-5 შესწორების დაცვით.¹⁰ აშშ-ის უზენაეს სასამართლოს არაერთხელ განუმარტავს, რომ ვერბალური გამოხატვა უნდა მიიჩნეოდეს ჩვენებად¹¹ და ამ წესიდან, ფაქტობრივად, არ არსებობს გამონაკლისი,¹² ვინაიდან ვერბალური გამოხატვა ან გადმოსცემს ინფორმაციას, ან ამტკიცებს ფაქტებს.¹³ მსგავს შემთხვევებში სახელმწიფომ პირს თავიდან უნდა აარიდოს უკვე ნახსენები ე.წ. „ბოროტი ტრილემა“.

მე-5 შესწორება იცავს როგორც სწორი, ისე - ცრუ ინფორმაციის მიწოდებას, შესაბამისად, პაროლის გადაცემაც მსგავს კლასიფიკაციაში ექცევა.¹⁴ ამასთან, პაროლის გამჟღავნება არ მოიხრება შემთხვევათა იმ კატეგორიაში, რომლებსაც სასამართლო პრაქტიკა არ მიიჩნევს ჩვენებად.¹⁵ მაგალითად, *Pennsylvania v. Muniz* საქმეში გამოძიებელმა მთვრალ ადამიანს ჰკითხა სახელი, გვარი, ასაკი და სხვა ფაქტები, თუმცა ის სიმთვრალის გამო პასუხებს კარგად ვერ სცემდა, რის გამოც მიწოდებული ინფორმაცია არ იქნა მიჩნეული ჩვენებად.¹⁶ პაროლთან მიმართებით არ მოქმედებს მსგავსი გამონაკლისი, ვინაიდან ამ ინფორმაციას შემდგომში სახელმწიფო არ იყენებს ბრალდებისთვის, შესაბამისად, მისი სარწმუნოება სიმთვრალის გამო ეჭვქვეშ ვერ დადგება, არამედ - იმ მომენტში მონყობილობის გაშიფვრისას შემონმდება მისი სისწორე. მითითებულიდან გამომდინარე, მიწოდებული ინფორმაცია არის თუ არა ჩვენება, დამოკიდებულია ინფორმაციის მიწოდების ფორმასა და კონტექსტზე.¹⁷

ზემოაღნიშნულიდან გამომდინარე, პაროლის წერილობით ან სიტყვიერად გადაცემა არის ჩვენება, შესაბამისად, მას სრული მოცულობით იცავს მე-5 შესწორება - სახელმწიფოს არ შეუძლია, აიძულოს პირი, რომ გადასცეს მონყობილობის პაროლი, რომელშიც შეიძლება მისი მამხილებელი ინფორმაცია იყოს.

2. პაროლის ჩანაწერების გადაცემის იძულების მიმართება თვითინკრიმინაციისგან დაცვის პრივილეგიასთან

დოკუმენტებზე ან სხვა მყარ მატარებელზე პაროლის თაობაზე ჩანაწერის არსებობის შემთხვევაში, სახელმწიფოს შეუძლია ამოიღოს დოკუმენტები ან, სხვადასხვა სამართლებრივი სისტემის გათვალისწინებით, სხვაგვარად მოიპოვოს ის. მაგალითად, აშშ-ში შესაძლებელია სახელმწიფომ პირს მოსთხოვოს ჩანაწერების გადაცემა და გადაცემაზე უარის თქმის შემთხვევაში, შეუძლია პირს დააკისროს პასუხისმგებლობა.¹⁸ მითითებულ შემთხვევაში არ ამოქმედდება თვითინკრიმინაციისგან დაცვის პრივილეგია, ვინაიდან ჩანაწერი არის **მატერიალური მტკიცებულება**,¹⁹ ხოლო მე-5 შესწორების მიხედვით, პრივილეგია მხოლოდ **ჩვენებაზე** (არამატერიალური მტკიცებულება) ვრცელდება.

აშშ-ის უზენაეს სასამართლოს არაერთ საქმეში აღუნიშნავს, რომ დოკუმენტების შინაარსი არ არის დაცული მე-5 შესწორებით.²⁰ კონკრეტული პირი სახელმწიფოს მოთხოვნის გამო არ

¹⁰ Villasenor, J., Mohan, V., Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era, *Journal of Constitutional Law Heightened Scrutiny*, 2012, 12.

¹¹ მაგალითად, *Pennsylvania v. Muniz*, 496 U.S. 582, 589 (1990).

¹² Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 *Fordham L. Rev.* 2018, 221.

¹³ *Doe v. United States*, 487 U.S. 201, 213 (1988).

¹⁴ *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012); *United States v. Kirschner*, 823 F. Supp. 2d 669 (E.D. Mich. 2010).

¹⁵ Regan, E. K., *United States v. Balsys: Denying a Suspected War Criminal the Privilege against Self-Incrimination*, *St. John's Law Review*, Vol. 73, no. 2, 1999, 595-596.

¹⁶ *Pennsylvania v. Muniz*, 496 U.S. 582-590 (1990).

¹⁷ Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 *J. CRIM. L. & CRIMINOLOGY* 243, 273-74 (2004). ციტირება იხ. Sacharoff, L. *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 *Fordham L. Rev.* 2018, 224.

¹⁸ Skarlatos, B. C., *The Fifth Amendment Privilege against Self-Incrimination and Tax Returns: Oil and Water or Peanut Butter and Jelly*, *Journal of Tax Practice & Procedure*, Vol. 18, no. 1, 2016, 53.

¹⁹ შეად. Bisset, A., *The Privilege Against Self-Incrimination in Truth Commission-Administered Accountability Initiatives*, *Leiden Journal of International Law*, Vol. 30, no. 1, 2017, 169-170.

²⁰ მაგ., *Fisher v. United States*, 425 U.S. 410 (1976).

წერს დოკუმენტზე პაროლს, არამედ - გადასცემს უკვე არსებულს. ამასთან, სახელმწიფო იღებს დოკუმენტს შინაარსის გამო, თუმცა პირის მიერ ამ დოკუმენტის გადაცემა არცერთ შემთხვევაში არ მიუთითებს, რომ ეს არის მონყობილობის პაროლი. შესაბამისად, წარმოების აქტის დოქტრინა²¹ ვერ იმოქმედებს, ანუ ფიზიკური ქცევა - დოკუმენტების გადაცემა - ვერ მიიჩნევა ჩვენებად და მასზე ვერ გავრცელდება მე-5 შესწორება.

ზემოაღნიშნულიდან გამომდინარე, სახელმწიფოს შეუძლია მოიპოვოს დასახელებული მასალები, თუმცა ეს არ არის პაროლის მოპოვების ეფექტიანი გზა, ვინაიდან სახელმწიფოსთვის არც თუ ისე ხშირადაა ხელმისაწვდომი მონყობილობის პაროლის ჩანაწერები.

3. პაროლის შეყვანის იძულების მიმართება თვითინკრიმინაციისგან დაცვის პრივილეგიასთან

განსახილველ შემთხვევაში სახელმწიფოს შეუძლია პასუხისმგებლობის დაკისრების მექანიზმით აიძულოს პირი, შეიყვანოს პაროლი იმგვარად, რომ სახელმწიფო არ აკვირდებოდეს პაროლის შეყვანის პროცესს. აქ სამართალდამცავებისთვის მნიშვნელოვანია შედეგი - მონყობილობის გახსნა. მსგავს შემთხვევებში პარადიგმული მნიშვნელობის საკითხია იმის განსაზღვრა, თუ რა არის პაროლის შეყვანა. უფრო კონკრეტულად, შესაფასებელია, სახელმწიფოს მიერ პაროლის შეყვანის იძულებით მოპოვებული მტკიცებულება ჩვენ მიერ ზემოთ განხილულ მტკიცებულებათა რომელ კლასიფიკაციაში ექცევა.

იურიდიულ დოქტრინაში მიმდინარეობს დავა, პაროლის შეყვანის იძულებით მოპოვებული

მტკიცებულება 1. არის არამატერიალური ან მატერიალური მტკიცებულება თუ 2. საერთოდ სხვა კატეგორია, რომელსაც დოქტრინაში **კვაზი ჩვენებას** უწოდებენ.²²

სანამ უშუალოდ მითითებულ საკითხს განვიხილავდეთ, თავიდანვე უნდა აღვნიშნოთ, რომ იმ შემთხვევაში, თუ სახელმწიფოს წარმომადგენელი აკვირდება პაროლის შეყვანის პროცესს, აქ კითხვები არ ისმება და აქტი ცალსახად ჩვენებად უნდა იქნეს მიჩნეული, ვინაიდან ის გაიგებს პაროლს.²³ საკითხი რთულდება, როდესაც სახელმწიფოს წარმომადგენელი არ აკვირდება ამ პროცესს.

3.1. პაროლის შეყვანის იძულებით მოპოვებული ინფორმაციის არამატერიალურ მტკიცებულებად (ჩვენებად) მიჩნევის შესაძლებლობა

პაროლის კონკრეტულ მონყობილობაში შეყვანა შეიძლება განვიხილოთ სამართალდამცავი ორგანოებისთვის ინფორმაციის სიტყვიერად გადაცემად. თუ ეს ასე მოხდება, სახელმწიფოს აღარ ექნება უფლება, პირს მოსთხოვოს პაროლის შეყვანა, ვინაიდან მასზე სრული მოცულობით გავრცელდება თვითინკრიმინაციისგან დაცვის პრივილეგიის გარანტიები.²⁴ მითითებულადან გამომდინარე, შესაფასებელია, რამდენად სწორია მსგავსი მსჯელობა.

თავიდანვე ხაზი უნდა გაესვას იმ ფაქტს, რომ გადამწყვეტი მნიშვნელობა აქვს სახელმწიფოს წარმომადგენლის მიერ პაროლის შეყვანის პროცესზე კონტროლის არარსებობას. ის არ უყურებს პაროლის შეყვანის პროცესს, შესაბამისად, ვერ იმახსოვრებს პაროლს და ის არც სხვა ფორმით ფიქსირდება სადმე. დოქტრინაში

²¹ დოქტრინის შესახებ დეტალურად იხ. მარკოიძე, გ., თვითინკრიმინაციისგან დაცვის პრივილეგია ადამიანის უფლებათა ევროპული სასამართლოსა და აშშ-ის უზენაესი სასამართლოს პრაქტიკაში, ადამიანის უფლებების დაცვა, პანდემია და სამართლის უზენაესობა, კონსტანტინე კორკელიას რედაქტორობით, 2021, 174-176.

²² იხ. მაგ., Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 225.

²³ Kerr, O. S., Compelled Decryption and the Privilege against Self-Incrimination, Texas Law Review, Vol. 97, no. 4, 2019, 785.

²⁴ Theophilopoulos, C., Electronic Documents, Encryption, Cloud Storage and the Privilege against Self-Incrimination, South African Law Journal, Vol. 132, no. 3, 2015, 598.

განსახილველ შემთხვევას ადარებენ ისეთ მოცემულობას, როდესაც, მაგალითად, ბრალდებულს აიძულებენ ოთახში შესვლას და საკუთარი თავისთვის ჩურჩულით რაიმეს თქმას.²⁵

მეორე მხრივ, შეიძლება გამოითქვას პოზიცია, რომ პაროლის შეყვანასა და პაროლის გადაცემას ერთი და იგივე შედეგი აქვს - სახელმწიფო მოიპოვებს წვდომას მოწყობილობაზე. აღნიშნული ფაქტორი გავლენას ვერ მოახდენს პაროლის შეყვანის ჩვენების ტიპის მტკიცებულებად კლასიფიკაციაზე, ვინაიდან ერთნაირი შედეგი ვერ განსაზღვრავს მტკიცებულება მატერიალურია თუ არამატერიალური. მაგალითად, ბრალდებულს სთხოვენ, თქვას სეიფის პაროლი, მაგრამ, პაროლის ნაცვლად, ის გასაღებით გახსნის სეიფს. შედეგი ორივე შემთხვევაში ერთია - გაიხსნა სეიფი, თუმცა გახსნის ფაქტი ვერ შეფასდება ჩვენებად.²⁶

მესამე მხრივ, პაროლის შეყვანის ჩვენების ტიპის მტკიცებულებად მოაზრების მომხრეებმა შეიძლება გამოთქვან პოზიცია, რომ ამ დროს პირი იყენებს მის გონებაში არსებულ ინფორმაციას. მითითებული არგუმენტი საყურადღებოა, ვინაიდან სასამართლო ხშირად იყენებს ამ ვიწრო პერსპექტივაზე გათვლილ მეთოდს იმის შესაფასებლად, აქტი არის თუ არა ჩვენების ტიპის. კერძოდ, სასამართლო აფასებს, იძულება მოითხოვს თუ არა ბრალდებულის გონებაში არსებული ინფორმაციის დამუშავებას.²⁷ ამ ლოგიკას რომ გავყვეთ, პაროლის შეყვანაში გონება მარტივად არის ჩართული და ენერგია იხარჯება პაროლის შექმნაში, შენახვაში, დამახსოვრებასა და შენარჩუნებაში.²⁸ მითითებული არგუმენტის საპასუხოდ შეიძლება ითქვას, რომ ბრალდებული გონებაში დამუშავებულ ინფორმაციას არ ხდის საჯაროს. შესაბამისად, იმ შემთხვევაშიც კი, თუ გავითვალისწინებთ მოსაზრე-

ბას, რომ აღნიშნული აქტი არის ჩვენების ტიპის, ვინაიდან გონება იყო ჩართული, ის მაინც ვერ მოექცევა ჩვენების კლასიკურ გაგებაში. მართლაც, სასამართლო მითითებულ ტესტს იყენებს არა მარტო იმის შესაფასებლად აქტი არის თუ არა კლასიკური ჩვენება, არამედ, მათ შორის, არის თუ არა ე.წ. კვაზი ჩვენება.²⁹

ზემოაღნიშნულიდან გამომდინარე, პაროლის შეყვანის აქტს ვერ განვიხილავთ ჩვენებად კლასიკური გაგებით, თუმცა სამსჯელოა, რამდენად შეიძლება იყოს ე.წ. კვაზი ჩვენება.

3.2. პაროლის შეყვანის იძულებით მოპოვებული ინფორმაციის მატერიალურ მტკიცებულებად მიჩნევის შესაძლებლობა

პაროლის შეყვანის იძულების საფუძველზე მოპოვებული ინფორმაცია საერთო ჯამში არის თუ არა მატერიალური მტკიცებულება, უნდა შეფასდეს რელევანტური სასამართლო პრაქტიკისა და დოქტრინის გამოყენებით. აშშ-ის სამართალში, მათ შორის, ფიზიკური ქცევა შეიძლება ჩაითვალოს ჩვენების ტიპად. ფაქტი, რომ პირმა განახორციელა ქმედება, აღნიშნულის შედეგად მოპოვებულ მტკიცებულებას ავტომატურად მატერიალურად ვერ გადააქცევს.³⁰

აშშ-ის უზენაესი სასამართლოს პრაქტიკაში განხილულა პრეცედენტები, როდესაც ფიზიკური ქმედების საფუძველზე მოპოვებულ მტკიცებულებაზე თვითინკრიმინაციისგან დაცვის პრივილეგია არ გავრცელებულა. მაგალითად, შემთხვევის ადგილზე ნაპოვნი მაისურის ჩაცმის იძულება, ამოცნობის მიზნებისთვის,³¹ ან კალიგრაფიული,³² ხმის³³ ან სხვაგვარი ნიმუშის აღების იძულება. განსახილველ საქმეებში ქცევები მხოლოდ ბრალდებულის ფიზიკურ მახასი-

²⁵ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 226.

²⁶ იქვე, 227.

²⁷ იხ. მაგ., United States v. Hubbell, 530 U.S. 27, 43 (2000); In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1345–46 (11th Cir. 2012).

²⁸ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 227

²⁹ United States v. Hubbell, 530 U.S. 27, 43 (2000).

³⁰ Wiseman, T., A., Encryption, Forced Decryption and the Constitution, A Journal of Law and Policy for the Information Society, 2015, 539.

³¹ Holt v. United States, 218 U.S. 245, 252–53 (1910).

³² Gilbert v. California, 388 U.S. 263, 265–67 (1967).

³³ United States v. Dionisio, 410 U.S. 1, 5–6 (1973).

ათებლებს ეხებოდა, შესაბამისად, არ ვრცელდებოდა კონსტიტუციის მე-5 შესწორება.³⁴ კალიგრაფიული და ხმის ნიმუშებიც კი, რომლებიც მეტწილად ახლოსაა ჩვენებებთან, არ ექცევა მე-5 შესწორების ქვეშ, ვინაიდან ისინი არ მიიჩნევიან ჩვენების ტიპად.³⁵ აღნიშნულის მიზეზია ის, რომ პირს სახელმწიფო აიძულებდა უშუალოდ ქცევას - სახელმწიფოსთვის მნიშვნელობა არ ჰქონდა, მაგალითად, რას წერდა პირი, არამედ - რა ფორმით აკეთებდა ამას.³⁶

პირისთვის პაროლის შეყვანის იძულების სიტუაცია რამდენადმე განსხვავებული შემთხვევაა. მარტივად რომ ვთქვათ, სახელმწიფო არ აიძულებს პირს ისეთი ქმედების განხორციელებას, რისი შედეგიც შემდგომში შემონადემა, შედარდება რაიმეს ან რაზეც ექსპერტიზა ჩატარდება, სხვა ნიმუშთან იდენტობის დასადგენად. პაროლის შეყვანით სასამართლო მოიპოვებს წვდომას მონაცემების ბაზაში არსებულ შინაარსობრივ მასალებზე. შესაბამისად, არ იქნება სწორი, რომ პაროლის იძულებით შეყვანით მოპოვებული მტკიცებულება განგვეხილა კლასიკურ მატერიალურ მტკიცებულებად.³⁷

3.3. პაროლის იძულებით შეყვანის მოპოვებული ინფორმაციის ე.წ. კვაზი ჩვენებად მიჩნევის შესაძლებლობა

პაროლის იძულებით შეყვანით მოპოვებული მტკიცებულებები შეიძლება განვიხილოთ ე.წ. კვაზი ჩვენებად, ანუ ისეთი ტიპის ინფორმაციად, რომელზეც თვითინკრიმინაციისგან დაცვის პრივილეგიის გარანტიები მხოლოდ გარკვეული მოცულობით ვრცელდება. აშშ-ში გავრცელებული წარმოების აქტის დოქტრინის მიხედვით, ფიზიკურ ქცევას შეიძლება მიენიჭოს არამატერიალური მტკიცებულების ხასიათი, თუ პირი მტკიცებულების გადაცემით რაიმეს

„ამბობს“.³⁸ პარალელი რომ გავავლოთ, პირმა რაიმე შეიძლება დაგვიდასტუროს როგორც „კის“ თქმით, ისე „თავის დაქნევით“. ამ შემთხვევაში ქცევა (თავის დაქნევა) არის შინაარსის მატარებელი. ანალოგიურად, დოკუმენტის ან სხვა საგნის წარმოების აქტი ინფორმაციას გამოსცემს სხვადასხვა გზით.³⁹ თუ სახელმწიფო აიძულებს პირს, რომ გადასცეს იარაღი, იარაღის გადაცემით ის ადასტურებს, რომ იარაღს ფლობდა, გაცნობიერებული ჰქონდა თავად ფლობის ფაქტიც და ისიც, რომ ეს საგანი ნამდვილად იარაღია.⁴⁰ დოკუმენტის გადაცემის იძულების ფაქტთან დაკავშირებით ერთ-ერთ ფუნქციონალურ საქმეში სასამართლომ განმარტა, რომ დოკუმენტის გადაცემა „ამბობდა“ შემდეგს:

- დოკუმენტები არსებობდა;
- დოკუმენტები ამ კონკრეტული პირის მფლობელობაში იყო;
- გადაცემული დოკუმენტები იყო სწორედ ის დოკუმენტები, რომლებსაც სახელმწიფო ითხოვდა (ანუ ისინი ავთენტური).⁴¹

მითითებული დოქტრინა რომ განსახილველ საკითხს მოვარგოთ, პირის მიერ მონაცემების ბაზაში პაროლის შეყვანის შემთხვევაში, ის ადასტურებს მონაცემების კონტროლს, შესაბამისად, მასში არსებული დოკუმენტების ფლობის ფაქტს. პირი მიუთითებს, რომ აღნიშნულ დოკუმენტებს ფლობს გააზრებულად და დოკუმენტები სწორედ ის დოკუმენტებია, რომლებიც სახელმწიფომ მოითხოვა. უფრო კონკრეტულად, პაროლის შეყვანითა და მონაცემების გაშიფვრით პირი ადასტურებს, რომ გაშიფრული ფაილები სწორედ ის ფაილებია, რომლებიც დაშიფრული იყო და სახელმწიფოს სურდა მათი მოპოვება.⁴²

³⁴ Gilbert v. California, 388 U.S. 263, 166 (1967); United States v. Wade, 388 U.S. 218, 222-223 (1967).

³⁵ United States v. Dionisio, 410 U.S. 6 (1973).

³⁶ Gilbert v. California, 388 U.S. 266 (1967).

³⁷ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 229.

³⁸ მარკოიძე, გ., თვითინკრიმინაციისგან დაცვის პრივილეგია ადამიანის უფლებათა ევროპული სასამართლოსა და აშშ-ის უზენაესი სასამართლოს

პრაქტიკაში, ადამიანის უფლებების დაცვა, პანდემია და სამართლის უზენაესობა, კონსტანტინე კორკელიას რედაქტორობით, 2021, 174-176.

³⁹ იხ. მაგ., In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1342-46 (11th Cir. 2012).

⁴⁰ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 229.

⁴¹ Fisher v. United States, 410-411, U.S. 410 (1976).

⁴² იქვე.

საბოლოოდ, მტკიცებულების მსგავსი ფორმით მოპოვების შემთხვევაში, სახელმწიფო სამართლოში მიუთითებს სწორედ ზემოაღნიშნულ გარემოებებზე. მაგალითად, თუ ბრალდებული წარადგენს იარაღს, სახელმწიფო გამოიყენებს მას, როგორც იარაღის ფლობის დამადასტურებელ მტკიცებულებას.⁴³ რეალურად, ის შეიძლება იყოს ერთადერთი მტკიცებულება, რომელიც ადასტურებს ფლობის ფაქტს. მსგავსად ამისა, სახელმწიფომ შეიძლება გამოიყენოს ბრალდებულის მიერ პაროლის შეყვანის ფაქტიც, იმის დასადასტურებლად, რომ ფაილების წარდგენამდე ეს მტკიცებულებები სწორედ მის მფლობელობაში იყო, პირს გააზრებული ჰქონდა ფლობის ფაქტი და ისინი ავთენტურია.⁴⁴ **მითითებულიდან გამომდინარე, პაროლის ნებისმიერი ფორმით შეყვანა უნდა იქნეს განხილული ე.წ. კვაზი ჩვენებად და მასთან მიმართებით პრივილეგიის გამოყენება მსგავსი ტიპის ჩვენებებისთვის გათვალისწინებული წინაპირობებით უნდა მოხდეს.**

აშშ-ის სამართალში ე.წ. კვაზი ჩვენებაზე პრივილეგიით დაცვა სრული მოცულობით ვრცელდება, გარდა იმ შემთხვევისა, თუ **წინასწარი დასკვნის დოქტრინით** არ იქნა გამორიცხული მისი მოქმედება. კერძოდ, თუ წარმოების აქტით, ანუ კვაზი ჩვენებით გამჟღავნებული ინფორმაცია სამართალდამცავი ორგანოსთვის ისედაც ცნობილი იყო, წარმოების აქტი აღარ მიიჩნევა ჩვენებად. აღნიშნული დოქტრინის მიხედვით, თუ სახელმწიფომ იცის, რომ ბრალდებული ფლობს კონკრეტულ დოკუმენტებს ან იცის პაროლი (ცხადია, აღნიშნული უნდა დგინდებოდეს გონივრული კონკრეტიზაციით), წარმოების აქტი თითქმის არაფერს სძენს სამართალდამცავი ორგანოების აქამდე არსებულ ცოდნას. შედეგად, ის უკვე აღარ არის ჩვენების ტიპის.⁴⁵

3.3.1. წინასწარი დასკვნის დოქტრინის განმარტების პრობლემატიკა პაროლის შეყვანის იძულებასთან დაკავშირებით

აშშ-ის იურიდიულ დოქტრინასა და სასამართლო პრაქტიკაში სადავოა, რასთან მიმართებით უნდა არსებობდეს **წინასწარი დასკვნა**. აზრთა მსგავსი სხვადასხვაობის ფარგლებში განვითარდა ე.წ. „**კონკრეტულობის წესი**“.⁴⁶ მითითებული წესი გულისხმობს სამართალდამცავების მიერ ფაქტის არსებობის გონივრული კონკრეტიზაციით დამტკიცებას, თუმცა, თუ რა ფაქტის, აღნიშნული ლიტერატურაში აზრთა სხვადასხვაობას იწვევს.⁴⁷ ამასთან, ცალკე შეფასების საგანია, რა იგულისხმება გონივრულ კონკრეტიზაციაში. **მაგალითად**, სამართალდამცავებმა ნარკოტიკულ დანაშაულში ბრალდებული პირი დააკავეს, რა დროსაც მისგან მობილური ამოიღეს. შესაფასებელია, რა უნდა დაადასტუროს სამართალდამცავმა ორგანომ - ის, რომ მასში შეიძლება იყოს დანაშაულთან დაკავშირებული ინფორმაცია, თუ უნდა მიუთითოს **კონკრეტულ** ინფორმაციაზე - ფოტოზე, მიმონერაზე და ა.შ, თუ მხოლოდ იმ ფაქტზე, რომ პირმა პაროლი იცის?⁴⁸

კონკრეტულობის ზოგიერთი მომხრე მიუთითებს, რომ კონკრეტულობის წესის მიხედვით, ზემოაღნიშნულ და სხვა მსგავს მაგალითებში სახელმწიფომ უნდა დაადასტუროს, უშუალოდ რომელი ინფორმაცია არსებობს ელექტრონულ მონაცემთა ბაზაში. ამასთან, თუ დადასტურდება მსგავსი ფაქტი, სამართალდამცავებს არ უნდა მიეცეთ შესაძლებლობა, რომ მობილურიდან მოიპოვონ ამ ინფორმაციის გარდა სხვა ინფორმაცია. სხვა ინფორმაციასთან დაკავშირებით ცალკე უნდა არსებობდეს წინასწარი დასკვნა.⁴⁹

⁴³ იხ. იგივე მსჯელობა, Todd, T. M., The Fifth Amendment and the Conjurer's Circle: Exploring the Privilege against Self-Incrimination in Federal Tax Practice, Charleston Law Review, Vol. 9, no. 1, 2014, 174-177.

⁴⁴ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 230.

⁴⁵ Fisher, 425 U.S. at 411; იხ. ასევე, United States v. Hubbell, 530 U.S. 27, 44 (2000).

⁴⁶ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 230.

⁴⁷ Clemens, A. M., The Pending Reinvigoration of Boyd: Personal Papers are Protected by the Privilege against Self-Incrimination, Northern Illinois University Law Review, Vol. 25, no. 1, 2004, 110-111.

⁴⁸ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 230.

⁴⁹ იქვე, 234.

საქმეში *In re Boucher*, პოლიციელმა დაინახა ფოტოები მანამდე, სანამ ბრალდებული დაბლოკავდა ელექტრონულ მონაცემებს. დაბლოკვის შემდეგ სამართალდამცავებმა ველარ გახსნეს მონაცემები, თუმცა სასამართლომ დააკმაყოფილა მოთხოვნა ფაილების სახელმწიფოსთვის გადაცემასთან დაკავშირებით. ბრალდებული ამტკიცებდა, რომ მოთხოვნა, გადაეცა ფოტოების გაშიფრული ვერსია, იყო წარმოების აქტი, შესაბამისად, ჩვენების ტიპის. სასამართლო არ დაეთანხმა და მიუთითა, რომ სამართალდამცავებს ჰქონდათ სათანადო მტკიცებულება, რომელიც ადასტურებდა მსგავსი ფაილების არსებობას - მათ თავად დაინახეს ფოტოები.⁵⁰

ზემოაღნიშნულის საწინააღმდეგოდ, ზოგიერთი ავტორი მიუთითებს, რომ საკმარისია სახელმწიფომ დაადასტუროს პირის მიერ პაროლის ცოდნა, რათა ჩაითვალოს, რომ არსებობს წინასწარი დასკვნა. ანუ გამოდის, რომ პაროლის ცოდნის დადასტურება ავტომატურად სახელმწიფოს აძლევს შესაძლებლობას, აიძულოს პირი პაროლის შეყვანაზე და მოიპოვოს მისი მაინკრიმინირებული ინფორმაცია.⁵¹

მიუთითებულ პოზიციას იზიარებს არაერთი იურისტი⁵² და ზოგიერთ შემთხვევაში, აშშ-ის სასამართლო პრაქტიკაც, მათ შორის, სააპელაციო სასამართლოს დონეზე.⁵³ მეორე მხრივ, აღნიშნული პოზიცია მნიშვნელოვან კრიტიკას იმსახურებს. მაგალითად, პროფესორი საქაროვი მიუთითებს, **პაროლის შეყვანა არა მარტო იმაზე მეტყველებს, რომ პირმა იცის პაროლი, არამედ - გაშიფრული დოკუმენტების არსებობაზე, ფლობასა და ავტენტირობაზე.** თუ სახელმწიფო ვერ დაადასტურებს, რომ პირს მონაცემების არსებობაში აქვს კონკრეტული ფაილები, პა-

როლის შეყვანის აქტი მიუთითებს, რომ ეს ნამდვილად ასეა - დოკუმენტები არსებობს, ამ პირის მფლობელობაშია და ავტენტიურია. გამოდის, რომ სახელმწიფომ მიიღო ის ინფორმაცია, რაც აქამდე არ იცოდა.⁵⁴ შესაბამისად, იმოქმედებს მე-5 შესწორება.⁵⁵

კონკრეტულობის წესის ზემოთ თქმული განმარტებების შეცდომის საილუსტრაციოდ, პროფესორი საქაროვი პარალელს ავლებს დოკუმენტების გადაცემის ქრესტომათიულ მაგალითთან. პაროლის შეყვანა შეიძლება ჰგავდეს დოკუმენტების გადაცემის შესაძლებლობის მიცემას, მაგალითად, სეიფის გასაღების გადაცემას. მსგავს შემთხვევებში წინასწარი დასკვნის დოქტრინის ძირითადი მოძღვრება წინასწარი დასკვნის არსებობას მოითხოვს დოკუმენტების არსებობასთან და ბრალდებულის მიერ ფლობასთან დაკავშირებით და არა იმ ფაქტთან დაკავშირებით, რომ რაღაც აბსტრაქტული დოკუმენტები მოთავსებულია სეიფში და მისი გასაღები კონკრეტულ პირს აქვს.⁵⁶

კონკრეტულობის წესის საქაროვისეული განმარტების მოწინააღმდეგე მეცნიერები მიუთითებენ, რომ პაროლის შეყვანით ადამიანი ამბობს მხოლოდ ერთ რამეს: „მე ვიცი პაროლი“. იმის გათვალისწინებით, რომ პაროლი არ გადაეცემა სახელმწიფოს, ნებისმიერი კომუნიკაციის მნიშვნელობა, რაც თავად პაროლს შეიძლება ჰქონდეს, მხედველობაში არ მიიღება (მაგალითად, პაროლი - „მეცხადინარკოტიკებს“). მეტიც, აღნიშნული პოზიციის მომხრე მეცნიერები მიუთითებენ, რომ მონაცემების გაშიფვრა არ მიუთითებს მონაცემების არსებობაში ინფორმაციის ცოდნაზე. ერთი საკითხია პაროლის ცოდნა, ხოლო მეორე საკითხია მონაცემების არსებობაში ინფორმაციის ცოდნა.

⁵⁰ No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009), ციტირება იხ. Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 234.

⁵¹ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 234.

⁵² იხ. მაგ., Kerr, O. S., Compelled Decryption and the Privilege against Self-Incrimination, Texas Law Review, Vol. 97, no. 4, 2019, 773.

⁵³ იხ. მაგ., Apple MacPro Comput., 851 F.3d at 241; Spencer, 2018 WL 1964588, at *3; Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615 (Mass. 2014).

⁵⁴ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 237.

⁵⁵ Morrison, C. M., Passwords, Profiles, and the Privilege against Self-Incrimination: Facebook and the Fifth Amendment, Arkansas Law Review, Vol. 65, no. 1, 2012, 153.

⁵⁶ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 237.

არსებული ინფორმაციის ცოდნა. ერთმა ადამიანმა შეიძლება იცოდეს პაროლი, თუმცა არაფერი იცოდეს მონყობილობაში არსებული ინფორმაციის შესახებ.⁵⁷ მაგალითად, პირმა თავისი დის მობილურის პაროლი გაიგო მისივე დაბადების დღეზე, სადაც სთხოვეს ფოტოების გადაღება და პაროლი დასჭირდა, რათა ამ პროცესში დახმარებოდა მათ. მსგავს შემთხვევაში ძმამ იცის მხოლოდ პაროლი და არა ის, თუ რა ინფორმაციაა მონყობილობაში.⁵⁸

როგორც ზემოაღნიშნულიდან ჩანს, აზრთა სხვადასხვაობა ძირითადად დაკავშირებულია იმ ფაქტთან, თუ რას „ამბობს“ პირი პაროლის შეყვანით. ერთნი მიუთითებენ, რომ პაროლის შეყვანით პირი ადასტურებს მონყობილობაში არსებული ინფორმაციის **არსებობას, ფლობასა და ავთენტურობას**, ხოლო მოწინააღმდეგეები - მხოლოდ იმ ფაქტს, რომ **პირმა იცის პაროლი**. მეორე მხრივ, შეიძლება გაჩნდეს აზრი, რომ თუ პირმა პაროლი იცოდა, იქმნება იმის პრეზუმფცია, რომ, როგორც წესი, მან მონყობილობაში არსებული ფაილების შესახებაც უნდა იცოდეს. აღნიშნულზე საპასუხოდ, სამხრეთ კალიფორნიის სამართლის სკოლის პროფესორი კერი პარალელს ავლებს ჩვენებასთან. მაგალითად, პირმა მისცა ჩვენება, რომ ის იყო დანაშაულის ადგილზე. აღნიშნული მხოლოდ იმას ნიშნავს, რომ ის იყო დანაშაულის ადგილზე და არავითარ შემთხვევაში არ ნიშნავს იმას, რომ მან ჩაიდინა დანაშაული. დანაშაულის ადგილზე ყოფნა, ცხადია, შეიძლება გამოყენებულ იქნეს ბრალდების მხარის მიერ სასამართლოში ბრალდების სამტკიცებლად, თუმცა ის არის ერთ-ერთი გარემოება და არა - ცალსახა დასკვნის საფუძველი. **გამოდის, რომ ჩვენებიდან დასკვნის გაკეთების შესაძლებლობა არ წარმოადგენს ჩვენებას ამ დასკვნის შესახებ.**⁵⁹ ამ პოზიციის ავტორი ერთმანეთისგან მიჯნავს მტკიცე-

ბითი სამართლის წესებსა და თვითინკრიმინაციისგან დაცვის პრივილეგიის გარანტიებს. კერძოდ, ის ფაქტი, რომ გარემოება რალაცაზე მიუთითებს, არ ნიშნავს, რომ ეს ასეა. თვითინკრიმინაციისგან დაცვის პრივილეგიის პრინციპებისთვის ეს ასე უნდა იყოს, სხვა შემთხვევაში, წინასწარ დასკვნაზე ვერ ვიმსჯელებთ.

რაც შეეხება პაროლის ცოდნის მტკიცების საკითხს, ის შეიძლება დადასტურდეს სხვადასხვა გარემოებით. მაგალითად, პირი რეგულარულად იყენებს მონყობილობას ან დაკავებისას ჯიბიდან ამოუღეს და მისი თითის ანაბეჭდები იყო მონყობილობაზე ან ოფიციალურ ბაზაში მის სახელზე რეგისტრირებული ნომერი იყო მოთავსებული მასში და ა.შ.⁶⁰ მსგავს შემთხვევებში სახელმწიფოს აქვს უფლება, რომ პირს მოსთხოვოს პაროლის შეყვანა.

ზემოთ მითითებული მსჯელობა ისე არ უნდა გავიგოთ, რომ თუ სახელმწიფო დაადასტურებს, რომ პირმა პაროლი იცის, მან მონყობილობაში არსებულ ყველა ფაილზე წვდომა ავტომატურად უნდა მოიპოვოს. ერთი მხრივ, თუ მონყობილობაში კიდეც არსებობს დაშიფრული ფაილები, ყველა მათგანთან დაკავშირებით უნდა არსებობდეს წინასწარი დასკვნა, რომ პირმა იცის მათი პაროლი. მეორე მხრივ, მონყობილობაში არსებული ფაილების მოსაპოვებლად მოქმედებას იწყებს მე-4 შესწორების (და არა პრივილეგიის), ანუ პირადი ცხოვრების ხელშეუხებლობის დაცვის გარანტიები და თუ არსებობს დასაბუთებული ვარაუდი, მხოლოდ მაშინ შეიძლება მსგავსი მონაცემების მოპოვება.⁶¹ მითითებული პოზიცია მხარდაჭერას იმსახურებს და, მათ შორის, მე-4 და მე-5 შესწორებათა ურთიერთმიმართების ლოგიკურ გააზრებას გვთავაზობს.

⁵⁷ Kerr, O. S., Compelled Decryption and the Privilege against Self-Incrimination, Texas Law Review, Vol. 97, no. 4, 2019, 779.

⁵⁸ იქვე, 780.

⁵⁹ იქვე, შეად. Sacharoff, L., What Am I Really Saying When I Open My Smartphone? Response (to Orin S. Kerr), Texas L. Rev., no. 97, 2019, 105.

⁶⁰ Kerr, O. S., Compelled Decryption and the Privilege against Self-Incrimination, Texas Law Review, Vol. 97, no. 4, 2019, 782.

⁶¹ იქვე.

3.3.1.1. რელევანტური სასამართლო პრაქტიკა და მისი დოქტრინალური ანალიზი

პაროლის შეყვანის იძულების ქრილში წინასწარი დასკვნის ინტერპრეტაციის განსაზღვრის საკითხი დაისვა მე-11 სააპელაციო სასამართლოს ერთ-ერთ რეზონანსულ საქმეში - *Grand Jury Subpoena Duces Tecum*.⁶² ფაქტობრივი გარემოებების მიხედვით, საჩივრის ავტორი გამოიძახეს ნაფიც მსაჯულთა სასამართლოში და სავალდებულოდ მოსთხოვეს ლეპტოპსა და მყარ დისკებზე წვდომის შესაძლებლობის სახელმწიფოსთვის გადაცემა. საჩივრის ავტორი არასრულწლოვანთა პორნოგრაფიის საქმეში სისხლისსამართლებრივ პასუხისგებაში იყო მიცემული. კერძოდ, არასრულწლოვანი გოგონას ამსახველი მასალების სოციალურ ქსელში გაზიარებისთვის. სამართალდამცავმა ორგანომ დაადგინა ბრალდებულის ვინაობა IP მისამართის გამოყენებით, ამოიღეს 2 ლეპტოპი და 5 მყარი დისკი, თუმცა ექსპერტებმა ვერ შეძლეს მათი გაშიფვრა.⁶³

სასამართლოს განმარტებით, საჩივრის ავტორის მიერ მოწყობილობების გახსნის იძულება ექცეოდა მე-5 შესწორების დაცვის ქვეშ. ის მიუთითებდა, რომ მათი გაშიფვრით სახელმწიფოს მიაწოდა ინფორმაცია მოწყობილობებში მოთავსებული ფაილების ფლობის, კონტროლის, გამოყენებისა და სხვა საკითხების შესახებ. გარდა ამისა, სასამართლომ აღნიშნა, რომ საჩივრის ავტორის იძულება, გაეშიფრა პაროლი, „გონების გამოყენების“ იდენტური იყო, შედეგად, გაშიფრული შინაარსი მყარ დისკზე - ჩვენების ხარისხის. წინასწარი დასკვნის დოქტრინა აქ ვერ გამოიყენებოდა, ვინაიდან წინასწარი დასკვნა არ არსებობდა.⁶⁴ მოსამართლე ჯოფლათის მოსაზრებით, დოქტრინა მხოლოდ მაშინ იმოქმედებდა, თუ სახელმწიფო შეძლებდა

იმის ჩვენებას, რომ მან „გონივრული კონკრეტიზაციით“ იცოდა მოწყობილობებში კონკრეტული ინფორმაციების არსებობის შესახებ. ამ საქმეში ასე არ იყო, შესაბამისად, დაირღვა თვითინკრიმინაციისგან დაცვის პრინციპი.⁶⁵ როგორც მითითებულიდან ჩანს, სასამართლომ არ გაიზიარა პროფესორი კერისა და სხვა ავტორთა პოზიცია და ცოდნის ფაქტი დაუკავშირა არა პაროლს, არამედ - მოწყობილობაში დაცულ ინფორმაციას.

იურიდიულ ლიტერატურაში ზემოაღნიშნული რეზონანსული საქმე აზრთა სხვადასხვაობას იწვევს. ერთი მხრივ, გაჟღერებული პოზიცია დადებითად ფასდება,⁶⁶ ვინაიდან გარკვეულწილად ავითარებს კონკრეტულობის წესის საწყისებს, თუმცა, მეორე მხრივ, კრიტიკასაც იმსახურებს.⁶⁷ ლიტერატურაში მოჰყავთ სეიფის გახსნის მაგალითი. წარმოვიდგინოთ მოცემულობა, როდესაც პირს ევალება მხოლოდ სეიფის გახსნა, ხოლო მეორე შემთხვევაში - როგორც სეიფის გახსნა, ისე მასში არსებული ნივთების გადამოწმება, სახელმწიფოსთვის გადაცემა და ა.შ. პირველი მოცემულობა ემსგავსება პაროლით მოწყობილობის გახსნის შემთხვევას - პირს არ ევალება ფაილების ძებნა. რაც შეეხება სეიფში ან მოწყობილობაში არსებული ინფორმაციის ცოდნას, ის შესაფასებელია არა მე-5 შესწორების, არამედ - მე-4 შესწორების ფარგლებში, რომელიც ეხება პირადი ცხოვრების ხელშეუხებლობის დაცვას. მას შემდეგ, რაც პირი გახსნის მოწყობილობას, მისი როლი ამოწურულია და სახელმწიფომ თავად უნდა მოიპოვოს მასში არსებული ინფორმაციები.⁶⁸

ზემოაღნიშნულთან ერთად, ზოგიერთი მეცნიერი პრობლემურად მიიჩნევს, თუ მტკიცების რა სტანდარტი უნდა არსებობდეს წინასწარი დასკვნის დოქტრინის გამოსაყენებლად. კერძოდ, რას ნიშნავს „გონივრული კონკრეტიზაციის“ სტანდარტი, ანუ რამდენად ცხადად უნდა

⁶² *In re Grand Jury Subpoena Duces Tecum* Dated March 25, 2011, 670 F.3d (11th Cir. 2012).

⁶³ იქვე, 1338-1339.

⁶⁴ იქვე, 1341, 1344-45, 1349.

⁶⁵ იქვე, 1347.

⁶⁶ მაგ., Goldman, K. Biometric passwords and the privilege against self-incrimination. *Cardozo Arts & Entertainment Law Journal*, 33(1), 2015, 234

⁶⁷ მაგ., Kerr, O. S., *Compelled Decryption and the Privilege against Self-Incrimination*, *Texas Law Review*, Vol. 97, no. 4, 2019, 787-788.

⁶⁸ იქვე, 788-789.

დაამტკიცოს სახელმწიფომ, რომ სხვა პირმა იცის პაროლი? არაერთ საქმეშია მითითებული, რომ წინასწარი დასკვნის მტკიცების ტვირთი სახელმწიფოზეა,⁶⁹ თუმცა რა დონის მტკიცებაზეა საუბარი, არ განმარტებულა.⁷⁰ აღნიშნული საკითხი აშშ-ის სამართალში კვლავ ვითარდება და ტექნოლოგიურ მიღწევებთან ერთად, რაციონალური უფრო და უფრო მეტი დეტალიზაციით ჩამოყალიბდება.

4. ბიომეტრიული პაროლის შეყვანის იძულება პრივილეგიის ქრილში

საერთაშორისოდ აღიარებული განმარტების მიხედვით,⁷¹ ბიომეტრიულ მონაცემში მოიაზრება ფიზიკური, ფსიქიკური ან ქცევითი მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი, სახის მახასიათებელი და სხვა). ბიომეტრიული მონაცემების საშუალებით ელექტრონული მოწყობილობების დაშიფვრა დროთა განმავლობაში უფრო და უფრო აქტუალური ხდება, შემდგომში მარტივი გაშიფვრის შესაძლებლობის გამო. მაგალითად, წამის მეასედებში შესაძლებელია მობილურის გაშიფვრა თითის ანაბეჭდით, სახის ამომცნობითა და ა.შ.⁷²

ბიომეტრიული პაროლი ნელ-ნელა ანაცვლებს ტრადიციულ ციფრობრივ, ალფაბიტურ ან სხვაგვარი სიმბოლოებით გამოსახულ პაროლებს. ამასთან, ორივე მათგანი გამოიყენება სხვადასხვა ტიპის, მათ შორის, პერსონალური ინფორმაციის დასაცავად.⁷³ სწორედ აღნიშნულის

გათვალისწინებით, შესაფასებელია, შესაძლებელია თუ არა ბრალდებულის იძულება, ბიომეტრიული მონაცემის გამოყენებით გახსნას მოწყობილობა. შეფასებისას ყურადღება უნდა გამახვილდეს, ვრცელდება თუ არა თანაბარი სტანდარტები ტრადიციულ და ბიომეტრიულ პაროლებზე. იძულების ფორმას რაც შეეხება, კვლავ აქტუალური იქნება პასუხისმგებლობის დაკისრების მუქარით მოწყობილობის გაშიფვრა, ვინაიდან ფიზიკური ან სხვაგვარი იძულება მსგავს შემთხვევებში ნაკლებად გამოიყენება.

კითხვა, რომელსაც პირველ რიგში უნდა გაეცეს პასუხი, არის ის, თუ რა ტიპის მტკიცებულებას მიეკუთვნება მოწყობილობის ბიომეტრიული მონაცემით გახსნის იძულებით მოპოვებული ინფორმაცია.⁷⁴ ლიტერატურასა და სასამართლო პრაქტიკაში აღნიშნული საკითხი განსხვავებულად ფასდება, თუმცა თავიდანვე გამოირიცხება მსგავსი ინფორმაციის კლასიკური ტიპის ჩვენებად მიჩნევა, ვინაიდან შეუძლებელია მისი სიტყვიერად ან წერილობით გადმოცემა.⁷⁵ შესაბამისად, მსჯელობა მიდის იმის შესახებ, აღნიშნული არის მატერიალური მტკიცებულება თუ კვაზი ჩვენება.

იურიდიულ ლიტერატურაში გავრცელებულია პოზიცია, რომლის მიხედვითაც, ყველა ინფორმაცია არის მატერიალური მტკიცებულება, თუ პირი „არ იყენებს გონებას“⁷⁶ და „არ გადმოცემს მის გამოცდილებას კონკრეტულ საკითხზე“⁷⁷. თითის ანაბეჭდს, მეორე მხრივ, არ აქვს მსგავსი ხასიათი. ის არის ხილული, ფიზიკური

⁶⁹ United States v. Bright, 596 F.3d 683, 693 (9th Cir. 2010); United States v. Rue, 819 F.2d 1488, 1493 n.4 (8th Cir. 1987).

⁷⁰ შეად. Reitz, K. R., Clients, Lawyers and the Fifth Amendment: The Need for a Projected Privilege, 41 DUKE L.J. 572, 1991, 631. ციტირება იხ. მაგ., Kerr, O. S., Compelled Decryption and the Privilege against Self-Incrimination, Texas Law Review, Vol. 97, no. 4, 2019, 787-789

⁷¹ ზოგადი მონაცემების დაცვის რეგულაციის (GDPR) მე-4 მუხლის მე-14 პუნქტი

⁷² Goldman, K. Biometric passwords and the privilege against self-incrimination. Cardozo Arts & Entertainment Law Journal, 33(1), 2015, 211

⁷³ იქვე, 212.

⁷⁴ Lemus, E. When fingerprints are key: Reinstating privacy to the privilege against self-incrimination in light of fingerprint encryption in smartphones, 70(2) S.M.U. L. Rev., 2017, 555-556

⁷⁵ იქვე, 553

⁷⁶ United States v. Hubbell, 530 U.S. 43, (2000).

⁷⁷ United States v. Wade, 388 U.S. 218, 222 (1967).

მტკიცებულება და არ არსებობს „ბრალდებულის გონებაში“.⁷⁸ ის არის იდენტიფიკაციის საშუალების მქონე ფიზიკური მონაცემი,⁷⁹ რომელიც ძალიან ემსგავსება ხმისა⁸⁰ და კალიგრაფიულ ნიმუშებს⁸¹. ის უფრო ჰგავს სეიფის გასაღებს, ვიდრე სეიფის კომბინაციას, ვინაიდან ის მოწყობილობას ხსნის ფიზიკური საშუალებით და არა - გონების ჩართულობით.⁸² როგორც მითითებულიდან ჩანს, აღნიშნული პოზიციის მომხრეები ბიომეტრიულ პაროლს განიხილავენ იდენტიფიკაციის საშუალებად და არა - ალფაბეტური ან სხვაგვარი სიმბოლოების პაროლის ანალოგად.

ზემოაღნიშნული მიდგომის საწინააღმდეგოდ, მეცნიერთა სხვა ჯგუფი აპელირებს ტექნოლოგიის განვითარების ტენდენციებსა და ძველი ან არსებული მიდგომების გადასინჯვის საჭიროებაზე.⁸³ საწყის ეტაპზე ბიომეტრიული მონაცემები, მათ შორის, თითის ანაბეჭდი გამოიყენებოდა იდენტიფიკაციისთვის, თუმცა ტექნოლოგიურ განვითარებასთან ერთად, მან შეიძინა მონაცემთა დაცვის ფუნქცია. მსგავსი მონაცემის გამოყენებით შესაძლებელია მობილურის ან სხვა ნებისმიერი მოწყობილობის დაბლოკვა/გახსნა, შესაბამისად, ის ისეთივე ფუნქციის მატარებელია, როგორც - სტანდარტული პაროლი.⁸⁴ აღნიშნული პოზიციის მიხედვით, ერთმანეთისგან უნდა გაიმიჯნოს **ბიომეტრიული მონაცემი, როდესაც ის იდენტიფიკაციისთვის გამოიყენება და ბიომეტრიული მონაცემი, როდესაც ის იმავე ფუნქციას ასრულებს, როგორსაც ჩვეულებრივი პაროლი**. საკითხი მე-5 შესწორების კონტექსტში სწორედ ამ დიფერენცირების ფარგლებში უნდა შეფასდეს.⁸⁵

სენსორზე თითის დაჭერა, ან სახის ჩვენება, ან სხვაგვარად ბიომეტრიული მონაცემის შეყვანა არ მოითხოვს ბრალდებულისგან „გონებაში არსებული ინფორმაციის გამჟღავნებას“. მიუხედავად ამისა, სწორია პოზიცია, რომელიც თვლის, რომ ბიომეტრიულ პაროლზეც იმავე სტანდარტი უნდა გავრცელდეს, როგორც სტანდარტულ პაროლზე. სხვა შემთხვევაში **სამართალი დასჯიდა ბრალდებულს იმ ფაქტის გამო, რომ მან გამოიყენა თანამედროვე ტექნოლოგიური განვითარება და არ აირჩია ისევ მოძველებული სისტემები**. სამართალი ცოცხალი, დინამიკაში მოქმედი მიმართულებაა, რომელიც ხშირად საჭიროებს მსგავს ლოგიკურ ინტერპრეტაციებს.⁸⁶

ზემოაღნიშნული არგუმენტების გარდა, ბუნდოვანია „გონებაში არსებული“ ინფორმაციის კრიტერიუმიც. კერძოდ, Fisher-ისა და სხვა საქმეებში მითითებულია, რომ კონსტიტუციის მე-5 შესწორებამ შეიძლება დაიცვას დოკუმენტის გადაცემის ფაქტი, ვინაიდან თავად გადაცემა „ამბობს“ რაღაც ინფორმაციას. ანალოგიურად, პაროლის შეყვანაც შეიძლება „ამბობდეს“ რაღაცას. თუ რას „ამბობს“, მეცნიერებაში აზრთა სხვადასხვაობას შეიძლება იწვევდეს ისე, როგორც პაროლის შეყვანა. ერთნი შეიძლება ფიქრობდნენ, რომ ამ მოწყობილობას ეს ადამიანი ფლობს და აკონტროლებს,⁸⁷ ხოლო მეორენი - რომ ამ პირს მხოლოდ მოწყობილობის გახსნა

⁷⁸ შეად. Lemus, E. When fingerprints are key: Reinstating privacy to the privilege against self-incrimination in light of fingerprint encryption in smartphones, 70(2) S.M.U. L. Rev., 2017, 553.

⁷⁹ United States v. Wade, 388 U.S. 218, 222 (1967).

⁸⁰ იხ. United States v. Dionisio, 410 U.S. 1, 7 (1973).

⁸¹ იხ., Gilbert v. California, 388 U.S. 222-223 (1967).

⁸² Lemus, E. When fingerprints are key: Reinstating privacy to the privilege against self-incrimination in light of fingerprint encryption in smartphones, 70(2) S.M.U. L. Rev., 2017, 554.

⁸³ Vivek Mohan & John Villasenor, Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital

Era, 15 U. PA. J. CONST. L. HEIGHTENED SCRUTINY 11, 2012, 11. ციტირება იხ. იქვე.

⁸⁴ Goldman, K. Biometric passwords and the privilege against self-incrimination. Cardozo Arts & Entertainment Law Journal, 33(1), 2015, 224.

⁸⁵ Lemus, E. When fingerprints are key: Reinstating privacy to the privilege against self-incrimination in light of fingerprint encryption in smartphones, 70(2) S.M.U. L. Rev., 2017, 555.

⁸⁶ Goldman, K. Biometric passwords and the privilege against self-incrimination. Cardozo Arts & Entertainment Law Journal, 33(1), 2015, 236.

⁸⁷ Sacharoff, L. Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 2018, 237.

შეუძლია.⁸⁸ შესაბამისად, მე-5 შესწორებით დაცვა ზუსტად ისეთივე უნდა იყოს, როგორიც პაროლის შეყვანის იძულების შემთხვევაში.

დასკვნა

ციფრული სივრცის განვითარებასთან ერთად, დანაშაულები ნელ-ნელა ციფრულ სივრცეში ინაცვლებს. მეორე მხრივ, ციფრული სივრციდან ინფორმაციის მოპოვება საგამოძიებო ორგანოებისთვის ერთ-ერთ მნიშვნელოვან გამოწვევად იქცა. აღნიშნული განპირობებულია იმ ფაქტით, რომ იქმნება სხვადასხვა ტიპის შიფრები, დაბლოკვის მექანიზმები თუ სხვა საშუალებები, რომლებიც მონაცემის მესაკუთრის ჩართულობის გარეშე, კომპიუტერულ სისტემაზე წვდომას კრიტიკულად ართულებს. აღნიშნულის ნათელი გამოვლინებაა კრიპტოვალუტა და მისი საშუალებით განხორციელებული ტრანზაქციები.

კომპიუტერული სისტემის განბლოკვისთვის შესაძლო დანაშაულის ჩამდენი პირისგან პაროლის გადაცემის მოთხოვნა თვითინკრიმინაციისგან დაცვის პრივილეგიის შესაძლო დარღვე-

ვის რისკებს წარმოშობს. როგორც აშშ-ის პრაქტიკისა და დოქტრინის განხილვა ცხადყოფს, პაროლის გადაცემა არის ე.წ. კვაზი ჩვენება. შესაბამისად, მასთან მიმართებით უნდა გამოვიყენოთ უკვე კარგად განვითარებული წარმოების აქტისა და წინასწარი დასკვნის დოქტრინები. გასათვალისწინებელია, რომ წინასწარ დასკვნასთან მიმართებით უნდა არსებობდეს გონივრული კონკრეტიზაცია. ამასთან, კონკრეტიზებული ინფორმაციის არსებობა, მხარდაჭერილი პოზიციით, პაროლის ცოდნასთან მიმართებით მოითხოვება.

ზემოთ განხილული პრობლემატიკა ქართული საპროცესო პრაქტიკისთვის ძალზე რელევანტურია, თუმცა ცალსახად უნდა ითქვას, რომ დღეს სსსკ-ში არ არსებობს მასთან გამკლავების საკანონმდებლო შესაძლებლობები. ამასთან, მომავალში პრობლემა უფრო და უფრო აქტუალური გახდება, რადგან ტექნოლოგიები იხვეწება. შესაბამისად, აშშ-ის ზემოთ განხილული დოქტრინისა და პრაქტიკის საკანონმდებლო და პრაქტიკულ სივრცეში ასახვა პროცესს მნიშვნელოვნად გაამარტივებს.

⁸⁸ Kerr, O. S., Compelled Decryption and the Privilege against Self-Incrimination, Texas Law Review, Vol. 97, no. 4, 2019, 779.