ივანე ჯავახიშვილის სახელობის
თბილისის სახელმწიფო უნივერსიტეტი
იურიდიული ფაკულტეტი

სამართლის ჟურნალი

№1, 2021

უნივერსიტეტის გამომცემლობა

თორნიკე ხიდეშელი*

კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის

ნაშრომი ეხება ისეთ აქტუალურ საკითხს, როგორიცაა კომპიუტერული მონაცემი და მისი გამოყენება სისხლის სამართლის პროცესში. მოცემულობას, რომელიც სრულებით განსხვავდება ტრადიციული მტკიცებულებისგან და მისი სპეციფიკური და ტექნიკური მახასიათებლებიდან გამომდინარე, მნიშვნელოვან გამოწვევად იქცა იურიდიული საზოგადოებისათვის. რთული აღმოჩნდა მისი შინაარსობრივი მხარის გაგება, მატერიალურ და ელექტრონულ დოკუმენტს შორის არსებული სხვაობის წარმოჩენა და ელექტრონული სახით არსებული ინფორმაციის ავთენტურობის განსაზღვრა. შესაბამისად, ნაშრომის მიზანს კომპიუტერული მონაცემის შინაარსობრივი მხარის კვლევა, მისთვის დამახასიათებელი ნიშან-თვისებების წარმოჩენა და მისი ავთენტურობის დადგენისთვის აუცილებელი წინაპირობების განსაზღვრა წარმოადგენს.

საკვანძო სიტყვები: *კომპიუტერული მონაცემი, კომპიუტერული სისტემა, ციფრული მტკიცებულება, ელექტრონული მტკიცებულება, კომპიუტერული მონაცემის ავთენტურობა.*

1. შესავალი

ტექნოლოგიების მუდმივი ზრდა და მათი საზოგადოებაში დამკვიდრება ხშირად წინ უსწრებს მათ სამართლებრივ ჩარჩოში მოქცევას. ამის ნათელ მაგალითს, კომპიუტერული მონაცემი წარმოადგენს. მიუხედავად იმისა, რომ კომპიუტერული მოწყობილობები დიდი ხანია არსებობს, სულ რაღაც 20-30 წლის უკან მისი გამოძიების ინტერესებისთვის გამოყენება განსაკუთრებულ მოვლენად განიხილებოდა. დროდადრო მისი მნიშვნელობა გაიზარდა და დღეს უკვე იგი გამოძიების განუყოფელ ნაწილად იქცა.[1] შედეგად სხვადასხვა ქვეყნის კანონმდებლობაში გაჩნდა კომპიუტერულ მოწყობილობასთან დაკავშირებული სიტყვები, როგორებიცაა კომპიუტერული მონაცემი, ელექტრონული და ციფრული მტკიცებულება თუ სხვა. აღსანიშნავია, რომ ამ სიტყვებმა არაერთი საერთაშორისო ორგანიზაციის ყურადღება მიიპყრო და მათი ზუსტი და ამომწურავი შინაარსის განსაზღვრას საკმაოდ დიდი დრო დასჭირდა. სხვა ქვეყნებთან შედარებით, ქართული საპროცესო კანონმდებლობისთვის კომპიუტერული მონაცემი და მასთან დაკავშირებული საგამოძიებო მოქმედებები სიახლეს წარმოადგენს. შეიძლება ითქვას, რომ იგი სწორედ ახლა გადის განვითარების გზას და შესაბამისად, მწირია ინფორმაციაც ქართულ იურიდიულ ლიტერატურაში.[2] ეს ნაკლოვანება კი გარკვეულ პრობლემებს ქმნის როგორც გამოძიების, ისე სასამართლო პრაქტიკის თვალსაზრისით.

---

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, მოწვეული ლექტორი.

1 *Kerr S. O.,* Searches and Seizures in a Digital World, Harvard Law Review, Vol. 119, 2006, 1.

2 *მეურმიშვილი ბ.,* საქართველოს სისხლის საპროცესო სამართალი, კერძო ნაწილი, *ფაფიაშვილი ლ. (რედ.),* თბ., 2017, 534-539. იხ. *თოლორაია ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, *გიორგაძე გ. (რედ.),* თბ., 2015, 422-425.

მსჯელობის საგნად იქცა კომპიუტერული მონაცემის ავთენტურობის საკითხიც. აღნიშნულს საფუძვლად მისთვის დამახასიათებელი ნიშან-თვისებები უდევს. მეცნიერთა გარკვეული ნაწილის ხედვით, კომპიუტერული მონაცემის მახასიათებლებიდან გამომდინარე, ახალი, ტრადიციული მტკიცებულებისგან განსხვავებული საკანონმდებლო მოწესრიგებაა საჭირო.[3] მეორე ნაწილის აზრით კი, მიუხედავად ელექტრონული ინფორმაციის ბუნებისა, ტრადიციული მტკიცებულებისთვის დადგენილი წესების მათზე გავრცელება სავსებით შესაძლებელია.[4] საკანონმდებლო თვალსაზრისით, საქართველოს სისხლის საპროცესო სამართალი განსხვავებულად აწესრიგებს კომპიუტერული მონაცემის მოპოვების საკითხს, ითვალისწინებს არაერთ პროცესუალურ შეზღუდვას, რაც საერთაშორისო სამართალთან ერთად, კომპიუტერული მონაცემის შინაარსისა და მისი მახასიათებლების არასიღრმისეულ გაგებასთან მჭიდროდ არის დაკავშირებული.

ამრიგად, საკითხის აქტუალობიდან გამომდინარე, წერილის მიზანს საკითხთან დაკავშირებული ინფორმაციული სიმწირის შევსება, კომპიუტერული მონაცემის ცნების განსაზღვრა, ელექტრონული მტკიცებულებისთვის დამახასიათებელი ნიშან-თვისებებისა და იურიდიული ლიტერატურისა და სხვადასხვა ქვეყნის გამოცდილების გათვალისწინებით მის ავთენტურობასთან დაკავშირებული აქტუალური საკითხების წარმოჩენა წარმოადგენს.

2. კომპიუტერული მონაცემის არსი

ინფორმაციული და საკომუნიკაციო ტექნოლოგიების ინტენსიურმა განვითარებამ, საქართველოს სისხლის სამართლის საპროცესო კოდექსში ელექტრონული მტკიცებულების მოპოვებასთან დაკავშირებული საგამოძიებო მოქმედებების შემოღება განაპირობა. ვინაიდან ამგვარი პროცესუალური ინსტრუმენტის გარეშე ფაქტობრივად შეუძლებელი იქნებოდა საქმისათვის მნიშვნელობის მქონე ინფორმაციის მოპოვება და მტკიცების პროცესში მისი გამოყენება, „კიბერდანაშაულის შესახებ“ კონვენციის საფუძველზე, მოქმედ საპროცესო კანონმდებლობაში XVI თავის სახით გათვალისწინებულ იქნა კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებები.[5]

შესაბამისად, სისხლის სამართლის საპროცესო კანონმდებლობაში გაჩნდა ახალი სიტყვები, როგორებიცაა: კომპიუტერული სისტემა, კომპიუტერული მონაცემი, მომსახურების მიმწოდებელი, ინტერნეტტრაფიკის მონაცემი და ა. შ. ხოლო მათი ტექნიკური და სპეციფიური ნიშან-თვისებებიდან გამომდინარე, მათი შინაარსობრივი მხარის ზუსტი და სიღრმისეული გაგება არა მხოლოდ დაინტერესებული პირებისათვის, არამედ იურისტებისთვისაც კი რთული აღმოჩნდა. ამრიგად, სტატიის მიზანია იურიდიული ლიტერატურისა და სხვა ქვეყნების გამოცდილების შესწავლით, მკითხველისთვის მეტად ნათელი გახდეს კომპიუტერული სისტემისა და მონაცემის შინაარსი.

საგულისხმოა, რომ კომპიუტერული მონაცემის განმარტება მოცემულია როგორც კიბერდანაშაულის შესახებ კონვენციაში, ისე საქართველოს სისხლის სამართლის საპროცესო

---

[3] *Brenner W. S., Frederiksen A. B.,* Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 1, 2002, 60-63, 80-82.

[4] *Clancy K. T.,* The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and A Primer, Mississippi Law Journal, Vol. 75, 2005, 193.

[5] *მეურმიშვილი ბ.,* საქართველოს სისხლის საპროცესო სამართალი, კერძო ნაწილი, *ფაფიაშვილი ლ. (რედ.)*, თბ., 2017, 534.

კოდექსში. შეიძლება ითქვას, რომ ორივე წყაროში გადმოცემული კომპიუტერული მონაცემის განმარტება იდენტური შინაარსის მატარებელია და შემდეგნაირად გამოიყურება: „კომპიუტერული მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის პროგრამა, რომელიც კომპიუტერული სისტემის ფუნქციონირებას უზრუნველყოფს".[6]

კომპიუტერული მონაცემის არსის უკეთ გასაგებად, უმჯობესია, მისი დეტალური განხილვა. უპირველესად, აღსანიშნავია კომპიუტერული სისტემის დეფინიცია, რომლის ცნება ორივე, ზემოთდასახელებულ დოკუმენტში იდენტურად არის ჩამოყალიბებული: „კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით ავტომატურად ამუშავებს მონაცემებს". შიდასახელმწიფოებრივ კანონმდებლობაში არსებული განმარტების მსგავსად, კიბერდანაშაულის შესახებ კონვენციაშიც, ყურადღება მონაცემების ავტომატურ დამუშავებაზეა გამახვილებული, რაც აღნიშნული პროცესის პროგრამის მეშვეობით წარმართვაზე მიუთითებს.[7] თავის მხრივ კი, კომპიუტერული მონაცემის განმარტებისას გამოყენებულია ტერმინი „დამუშავებისთვის ხელსაყრელი ფორმით", რაც კომპიუტერულ სისტემაში ინფორმაციის იმგვარი ფორმით მოთავსებას გულისხმობს, რომლის ელექტრონულად დამუშავებაც შესაძლებელია.[8]

კომპიუტერული სისტემა უნდა განვიხილოთ, როგორც კომპიუტერული მოწყობილობისა და პროგრამული უზრუნველყოფის ერთიანობა.[9] კომპიუტერული სისტემა სხვადასხვა მოწყობილობებისგან შედგება, თუმცა ძირითად ნაწილებს ცენტრალური პროცესორი, ინფორმაციის შემნახველი მოწყობილობები და პროგრამული უზრუნველყოფა წარმოადგენს.[10]

ცენტრალური პროცესორი – ნებისმიერი ელექტრონული მოწყობილობის ფუნქციონალურ, ძირითად მოწყობილობას წარმოადგენს. იგი იღებს[11] მონაცემებს, რომელთაც ლოგიკურ-არითმეტიკული ოპერაციების მეშვეობით ამუშავებს, ხოლო მიღებული შედეგი გამოაქვს მონიტორზე[12], ინახავს მონაცემთა შემნახველ მოწყობილობაში ან ინტერნეტ ქსელის დახმარებით უკავშირებს სხვა მოწყობილობას.[13]

პროგრამული უზრუნველყოფა – ეს არის პროგრამათა ერთობლიობა, რომლებიც ელექტრონული მოწყობილობების ფუნქციონირებისათვის გასცემენ შესაბამის ინსტრუქციებს. იგი

---

[6] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 03/11/2009. კიბერდანაშაულის შესახებ კონვენცია, 23/11/2001.

[7] Explanatory Report to the Convention on Cybercrime, European Treaty Series – № 185, Budapest, 23.11.2001, 5.

[8] იქვე.

[9] *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 61.

[10] *Mason S., Weir R. S. G.,* The Sources of Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 1-5. *იხ. ოთხოზორია ვ., ცირამუა ზ., სვანიშვილი შ.,* ინფორმაციული ტექნოლოგიების მხარდამჭერი სპეციალისტი, თბ., 2015, 8.

[11] კომპიუტერში შესატანი ინფორმაცია შედგება სიტყვებისგან, რიცხვებისგან, გამოსახულებე ბისგან, ხმებისაგან ან ზემოთჩამოთვლილის კომბინაციით. ყველაზე ხშირად ინფორმაციის შეტანისთვის გამოიყენება კლავიატურა, დისკები, მაუსი, სკანერი, ციფრული კამერა, ინტერნეტ-ქსელი და სხვა.

[12] გავრცელებული მოწყობილობა, რომელიც გამოიყენება ინფორმაციის გამოტანისათვის არის პრინტერი (საბეჭდი მოწყობილობა), ხმოვანი ადაპტორი, რომლის დახმარებითაც კომპიუტერი გასცემს ხმოვან ინფორმაციას. აგრეთვე, დისკეტები, მაგროვებელი ფირი, დისკური მოწყობილობა და სხვა. იმ შემთხვევაში თუ კომპიუტერი ჩართულია ქსელში, ეს მოწყობილობაც შეიძლება ჩაითვალოს განკუთვნილი ინფორმაციის გამოტანისათვის.

[13] *Mason S., Weir R. S. G.,* The Sources of Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 1.

იყოფა ორ ძირითად კატეგორიად, ერთი როგორც სისტემური (ოპერაციული) და მეორე, როგორც აპლიკაციური (გამოყენებითი) უზრუნველყოფა.[14] სისტემური უზრუნველყოფა, როგორც თავად სიტყვა გვკარნახობს წარმოადგენს კომპიუტერული მოწყობილობის ფუნქციონირების საფუძველს. იგი საბაზისო ფუნქციას ასრულებს და ამყარებს კავშირს მოწყობილობებთან, საქაღალდეებთან და მართავს გამოყენებით პროგრამებს.[15] ხოლო აპლიკაციური (გამოყენებითი) – ეს არის „სპეციალური დანიშნულების" პროგრამა, რომელიც საშუალებას აძლევს მომხმარებელს განსაკუთრებული სახის დავალებები შეასრულოს კომპიუტერზე. აღნიშნულს განეკუთვნება ინტერნეტ ბრაუზერი, ელექტრონული ფოსტა, სოციალური ქსელები და სხვა.

ინფორმაციის შემნახველი მოწყობილობები – ინფორმაციის შესანახ საშუალებებს ძირითადად მყარი დისკი და ოპერატიული მეხსიერება წარმოადგენენ. ნებისმიერი პროგრამა, რომელიც უზრუნველყოფს კომპიუტერის ფუნქციონირებას ოპერატიულ მეხსიერებაში ეშვება. ოპერატიულ მეხსიერებაში კი ინახება ის ინფორმაცია, რომელიც უშუალოდ დამუშავების პროცესშია, ხოლო კომპიუტერისთვის ელექტროკვების მოხსნის შემდეგ ძირითად შემთხვევაში იგი იკარგება. სწორედ ამიტომ, მას დროებით მეხსიერებას უწოდებენ. ამრიგად, სამართალდამცავი ორგანოები მონაცემების დროებითი მეხსიერებიდან ამოღებას მოწყობილობის დენის წყაროდან გამორთვამდე ცდილობენ, რასაც „მონაცემების ექსპერტიზა ეთერში/ლაივში ეწოდება".[16]

განსხვავებით ოპერატიული მეხსიერებისგან მყარი დისკი მუდმივ მეხსიერებას წარმოადგენს და მოწყობილობის დენის წყაროდან გამოერთების შემთხვევაში მასზე არსებული ინფორმაცია არ იკარგება.[17] ვინაიდან აღნიშნული არ არის ცვალებადი, ხშირ შემთხვევაში, იგი კომპიუტერული მონაცემის (შემდგომში ელექტრონული მტკიცებულების) მნიშვნელოვან წყაროს წარმოადგენს.

კომპიუტერული მონაცემის მატარებელი შეიძლება იყოს მონაცემთა დამგროვებლები, როგორებიცაა: კომპაქტური დისკი, მეხსიერების ბარათები და სხვა. აგრეთვე, მონაცემთა შენახვა შესაძლებელია დისტანციურად, ონლაინ საცავში.[18]

მოცემული ინფორმაციის შეჯერების შედეგად იკვეთება, რომ კომპიუტერული სისტემა არის მოწყობილობა, რომელიც, თავის მხრივ, ერთ ან რამდენიმე აქტიურ ნაწილს აერთიანებს და მათგან ერთი მაინც ავტომატურად, პროგრამის მეშვეობით იღებს, ამუშავებს და გადასცემს ინფორმაციას.

კომპიუტერული სისტემის მნიშვნელობასთან ერთად, ინტერესის საგანს წარმოადგენს კომპიუტერული მონაცემის შინაარსი. სისხლის სამართლის საპროცესო კოდექსსა და „კიბერდანაშაულის შესახებ" კონვენციაში არსებული განმარტების მიხედვით კომპიუტერულ მონაცემად კომპიუტერული სისტემის ფუნქციონირებისათვის აუცილებელი პროგრამა და ამ მოწყობილობაში დამუშავებისთვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია/ფაქტები მიიჩნევა.[19]

---

[14] იქვე, 2.

[15] *ოთხოზორია ვ., ცირამუა ზ.,* ინფორმაციული ტექნოლოგიები, თბ., 2015, 226.

[16] *ევროპის საბჭო,* მოსამართლეთა ტრენინგი ქსელურ დანაშაულში, 2010, 35, <https://rm.coe.int/16802fa028> [23.02.2021].

[17] *Mason S., Weir R. S. G.,* The Sources of Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 4.

[18] იქვე, 5.

[19] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 03/11/2009. კიბერდანაშაულის შესახებ კონვენცია, 23/11/2001.

მნიშვნელოვანია დადგინდეს, შესაძლებელია თუ არა კომპიუტერული მონაცემის დოკუმენტად მოხსენიება. სისხლის სამართლის პროცესის მიზნებისთვის დოკუმენტად იწოდება ნებისმიერი წყარო, სადაც ინფორმაცია სიტყვიერ-ნიშნობრივი ფორმით ან/და ფოტო-, კინო-, ვიდეო-, ბგერისა თუ სხვა ჩანაწერის სახით ან სხვა ტექნიკური საშუალების გამოყენებით არის აღბეჭდილი.[20] ორი დამოუკიდებელი ტერმინის ურთიერთმიმართების დასადგენად და საკითხზე სიღრმისეული მსჯელობისთვის უმჯობესი იქნება თუ სხვა ქვეყნების გამოცდილებასაც გადავხედავთ. ამ მხრივ, საინტერესოა თუ როგორ განიმარტება დოკუმენტი სხვადასხვა ქვეყნის იურისდიქციაში. მაგალითისთვის, ავსტრალიური კანონმდებლობის მიხედვით, დოკუმენტად მიჩნეულია ინფორმაციის ნებისმიერი წყარო, სადაც გამოსახულია ნიშნები, ფიგურები, სიმბოლოები, ფოტოები, ნახაზები.[21] აგრეთვე, კომპაქტური დისკი, ხმოვანი ფაილები და სხვა.[22] ამრიგად, დოკუმენტის ამგვარი განმარტება საკმაოდ ფართოა იმისთვის, რომ მასში კომპიუტერული მონაცემი, იგივე ელექტრონული ინფორმაციაც მოვიაზროთ.

რაც შეეხება ამერიკის შეერთებულ შტატებს, სისხლის სამართლის საპროცესო კანონმდებლობა, განსხვავებით სამოქალაქო საპროცესო კანონმდებლობისგან, არ შეიცავს დოკუმენტის განმარტებას.[23] თუმცა ფედერალური კანონი სისხლის სამართლის პროცესის შესახებ, განმარტავს საკუთრების ცნებას, რომელიც მოიცავს ერთის მხრივ მატერიალურ საგნებს, როგორებიცაა დოკუმენტი და ჩანაწერები, ხოლო მეორე მხრივ, აღქმად და გასაგებ ინფორმაციას.[24] ხოლო მტკიცებულების შესახებ კალიფორნიის კოდექსი კი დოკუმენტად ინფორმაციის ნებისმიერ გამოსახულებას მიიჩნევს, მიუხედავად იმისა თუ სად და როგორი ფორმით ინახება იგი. მაგალითისთვის, ხელნაწერი, ფოტო-აუდიო მასალა და სხვა.[25]

ამ მხრივ კანადის კანონმდებლობა უფრო შორს წავიდა და ცალკე გამოყო ელექტრონული დოკუმენტის ცნება. კანადის მტკიცებულებათა აქტის მიხედვით ელექტრონულ დოკუმენტში მოიაზრება მონაცემი, რომელიც ჩაწერილია ან მოთავსებულია კომპიუტერულ სისტემაში ან მსგავსი ტიპის მოწყობილობაში და მისი წაკითხვა ან აღქმა შესაძლებელია ადამიანის ან კომპიუტერული მოწყობილობის მიერ.[26]

ინგლისისა და უელსის კანონმდებლობაში კი ვხვდებით მხოლოდ მონაცემის განმარტებას, რომლის მიხედვითაც მონაცემად იწოდება ინფორმაცია, რომელიც შეყვანილია კომპიუტერულ სისტემაში მისი შემდგომი დამუშავების მიზნით; ინფორმაცია, რომლის დამუშავებაც ხდება ავტომატურად ან მოცემული ინფორმაცია კომპიუტერული სისტემის ნაწილს წარმოადგენს.[27]

სხვადასხვა ქვეყნის კანონმდებლობის ანალიზმა ცხადყო, რომ კომპიუტერული, იგივე ელექტრონული მონაცემის შინაარსი ერთიანია. საქართველოს კანონმდებლობის მსგავსად, სხვადასხვა ქვეყნის იურისდიქციაშიც, დოკუმენტი ფართოდ არის განმარტებული და მასში ელექტრონული ინფორმაციაც მოიაზრება. თუმცა აღსანიშნავია, რომ უცხოურ იურიდიულ ლიტერატურაში კომპიუტერული მონაცემის ან ელექტრონული ინფორმაციის ნაცვლად გა-

[20] იქვე, მუხ. 3(23).
[21] Evidence Act, 23/02/1995; Acts Interpretation Act 1901 (Amendment of 14/01/2019).
[22] Evidence Act, 23/02/1995.
[23] Federal Rules of Civil Procedure, 20/12/1937.
[24] Federal Rules of Criminal Procedure, 26/12/44.
[25] Evidence Code of California, 18/05/1965.
[26] Canada Evidence Act, 1985.
[27] Data Protection Act, 1998.

მოიყენება „ციფრული ან ელექტრონული მტკიცებულების“ ცნება და მის დეფინიციას არაერთი საერთაშორისო ორგანიზაცია გვთავაზობს. მაგალითისთვის, ციფრული მტკიცებულებების სამეცნიერო-სამუშაო ჯგუფის (*SWGDE*) ხედვით ციფრულ მტკიცებულებად ითვლება მტკიცებულებითი ღირებულების მქონე ინფორმაცია, რომელიც შენახული ან გადაცემულია ციფრული, ელექტრონული ფორმით.[28] კომპიუტერული მტკიცებულებების საერთაშორისო ორგანიზაციის (*IOCE*) შეფასებით კი ელექტრონული მტკიცებულებაა ინფორმაცია, რომელიც შენახული ან გადაცემულია ბინარული ფორმით და მისი გამოყენება შესაძლებელია სასამართლოში.[29] აქედან გამომდინარე, მოცემული საერთაშორისო ორგანიზაციები ცნების განმარტებისას ყურადღებას ელექტრონული ინფორმაციის მტკიცებულებით ძალაზე ამახვილებენ და არაფერს ამბობენ გამოძიების პროცესში მის მნიშვნელობაზე.[30] თუმცა უფრო ფართო განმარტებას გვთავაზობს უფროს პოლიციელთა ასოციაცია (*ACPO*), რომელთა შეფასებით ელექტრონულ მტკიცებულებას წარმოადგენს გამოძიებისთვის ღირებული ინფორმაცია ან მონაცემი, რომელიც ინახება ან გადაიცემა კომპიუტერის მიერ.[31] მსგავსი ხედვა აქვს მართლმსაჯულების ეროვნულ ინსტიტუტს (*NIJ*), რომლის თანახმად ელექტრონული მტკიცებულება არის გამოძიებისთვის ღირებული ინფორმაცია და მონაცემი, რომლებიც მოთავსებულია, მიღებულია ან გადაცემულია ელექტრონული მოწყობილობის მიერ.[32]

ვინაიდან მიზანს კომპიუტერული მონაცემის არსის დადგენა წარმოადგენდა, ამისთვის აუცილებელი იყო თავდაპირველად, კომპიუტერული სისტემის ბუნებაში გავრკვეულიყავით. საკითხზე მუშაობისას გამოიკვეთა, იმისათვის, რომ მოწყობილობა კომპიუტერულ სისტემად იქნეს მიჩნეული, აუცილებელია, მას ჰქონდეს: 1. პროცესორი – განუყოფელი მოწყობილობა, რომელიც გამოთვლით ოპერაციებს ასრულებს, ანუ ახდენს ინფორმაციის გადამუშავებას 2. პროგრამული უზრუნველყოფა – რომელიც ელექტრონული მოწყობილობის ფუნქციონირებისთვის შესაბამის ინსტრუქციებს გასცემს და 3. ინფორმაციის შემნახველი მოწყობილობა, სადაც დამუშავებული ინფორმაციის განთავსება ხდება.

ეს არის ის სამი ძირითადი კომპონენტი, რომლებიც ქმნიან კომპიუტერულ სისტემას, ხოლო იმისათვის, რომ კომპიუტერულმა სისტემამ შეძლოს კომპიუტერული მონაცემის შექმნა, შენახვა, დამუშავება, გადაცემა და სხვა, აუცილებელია ადამიანური რესურსი, რომელიც ყოველივე ზემოხსენებულის შემოქმედი და მომხმარებელია. ამრიგად, შესაძლებელია ითქვას, რომ კომპიუტერული მონაცემი არის მომხმარებლის მიერ კომპიუტერულ სისტემაში შეყვანილი, ხოლო შემდგომ კომპიუტერული მოწყობილობის მიერ ავტომატურად დამუშავებული, შენახული ან გადაცემული ნებისმიერი ინფორმაცია. ხოლო ელექტრონული მტკიცებულება – კომპიუტერულ სისტემაში არსებული კომპიუტერული მონაცემი, რომელიც ღირებულია გამოძიებისთვის ან პროცესის მონაწილე მხარისათვის, სასამართლოში მნიშვნელოვანი გარემოებების დასადასტურებლად.

---

[28] Scientific Working Group on Digital Evidence (SWGDE), SWGDE Digital and Multimedia Evidence Glossary, 2016, 7, <https://www.swgde.org/documents/published> [20.02.2021].

[29] *Casey O.*, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 7.

[30] იქვე.

[31] იქვე.

[32] *Goodison E. S., Davis C. R., Jackson A. B.*, Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 3.

3. კომპიუტერული მონაცემის მახასიათებლები

ყურადსაღებია, რომ ელექტრონული მტკიცებულება და თავის მხრივ კომპიუტერულ-ტექნიკური ექსპეტიზა მტკიცებით პროცესში სიახლეს წარმოადგენს. განსხვავებით სხვა საექსპერტო დისციპლინებისგან, ელექტრონულმა მტკიცებულებამ პროფესიონალ იურისტებს შორის აზრთა სხვადასხვაობა გამოიწვია.[33] აგრეთვე, განსხვავებული აღმოჩნდა სამართლებრივი სისტემების მიდგომაც ახალი გამოწვევის მიმართ. ერთი მხრივ, შეიქმნა ახალი კანონმდებლობა კონკრეტულად ელექტრონული მტკიცებულებისათვის, ხოლო მეორე მხრივ – მოხდა არსებულ კანონმდებლობასთან მისი შერწყმა და შეძლებისდაგვარად არსებული ნორმების ელექტრონულ მტკიცებულებებზე გავრცელება.[34]

ახალი კანონმდებლობის მიღება ელექტრონულ და ტრადიციულ მტკიცებულებებს შორის არსებული განსხვავებით იყო განპირობებული, ხოლო ელექტრონულ მტკიცებულებებზე მოქმედი ნორმების ანალოგიური წესით გამოყენება კი მასსა და ტრადიციულ მტკიცებულებებს შორის არსებული საერთო ნიშნებით.[35] წინამდებარე ხედვის გაზიარების შემთხვევაში, საქართველოს სისხლის სამართლის საპროცესო კოდექსში კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებების ცალკე თავად გამოყოფა და მასში გათვალისწინებულ ნორმებზე განსხვავებული, იგულისხმება ფარული საგამოძიებო მოქმედებისათვის დადგენილი წესის გავრცელება, არა მარტო „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირებით აიხსნება, არამედ ქართველი კანონმდებლების მიერ ელექტრონულ და ტრადიციულ მტკიცებულებებს შორის ფუნდამენტური სხვაობის დანახვით.

იურიდიულ ლიტერატურაში ელექტრონული მტკიცებულების მრავალ ნიშან-თვისებაზე ამახვილებენ ყურადღებას. მეცნიერთა აზრით, ელექტრონული მტკიცებულება თითის ანაბეჭდის ან დნმ-ის მსგავსად ლატენტურია, მარტივად და სწრაფად კვეთს ფიზიკურ-გეოგრაფიულ საზღვარს,[36] ადვილად ზიანდება.[37] შესაბამისად, მატერიალურ მტკიცებულებასთან შედარებით განსხვავებულ მოპყრობას საჭიროებს.[38]

თანამედროვე მსოფლიოში მოქმედი სამართლებრივი სისტემებისთვის დოკუმენტი მატერიალური მტკიცებულებების ერთ-ერთ მნიშვნელოვან ფორმას წარმოადგენს. იგივე შეიძლება ითქვას ელექტრონულ დოკუმენტზე.[39] ამასთან წერილობითი დოკუმენტისა და ელექტრონული დოკუმენტის ურთიერთშედარება საუკეთესო საშუალებაა ელექტრონული მტკიცებულების მახასიათებლების წარმოსაჩენად. განსაკუთრებით მაშინ, როდესაც სხვადასხვა პროგრამული საშუალების დახმარებით შექმნილ დოკუმენტს, ფიზიკური დოკუმენტის მსგავსი იერსახე აქვს. შესაძლებელია მისი გადაფურცვლა, საქაღალდეში შენახვა ან თუნდაც ნაგ-

---

33 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 18.

34 იქვე.

35 იქვე.

36 *Mukasey B. M., Sedgwick L. J., Hagy W. D.*, Electronic Crime Scene Investigation: A Guide for First Responders, National Institute of Justice, USA, 2008, 9.

37 *Gonzales R. A., Schofield B. R., Hagy W. D.*, Investigations Involving the Internet and Computer Networks, National Institute of Justice, USA, 2007, 2. იხ., *Casey E.*, Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 26.

38 *Goodison E. S., Davis C. R., Jackson A.B.*, Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 3.

39 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 20.

ვის ყუთში ჩაგდება. ხოლო ამგვარი მოჩვენებითი მსგავსება კი ქმნის შთაბეჭდილებას, რომ ელექტრონული დოკუმენტი მისი დახურვისას ან კომპიუტერის გათიშვისას ინარჩუნებს სტრუქტურულ ერთიანობას, ისე როგორც მატერიალური დოკუმენტი საქაღალდეში შენახვისას.[40] ეს სულაც არ მიუთითებს, რომ ელექტრონული დოკუმენტი გარდაუვლად ყალბი ან არასანდოა, თუმცა მისი მახასიათებლებიდან გამომდინარე, მისი ნამდვილობის დადასტურება ზუსტ და თანმიმდევრულ შემოწმებას საჭიროებს.[41]

ელექტრონული დოკუმენტის/მტკიცებულების ძირითად მახასიათებლებზე მსჯელობისას, ყურადღების მიღმა არ უნდა დარჩეს სედონას საკონფერენციო სამუშაო ჯგუფის[42] ძალისხმევა მისი მახასიათებლების განსაზღვრის პროცესში.მათი ხედვით, ელექტრონულ და წერილობით დოკუმენტებს შორის არსებული ძირითადი სხვაობის დაყოფა ექვს კატეგორიად არის შესაძლებელი. კერძოდ: მეტამონაცემები; მოცულობა და გამრავლების შესაძლებლობა; ხანგრძლივუნარიანობა; დინამიური და ცვალებადი შინაარსი; გარემოზე დამოკიდებულება; და დისპერსია.[43]

3.1. მეტამონაცემები

მეტამონაცემები წარმოადგენს მონაცემებს მონაცემების შესახებ.[44] შეიძლება ითქვას, რომ ეს არის ინფორმაციის დამატებითი წყარო, რომელიც მიუთითებს დოკუმენტის შინაარსის, კატეგორიის, კუთვნილების, ფორმატის, მონაცემთა შექმნისა და მეთოდების, ადგილმდებარეობის, მისი გამოყენების პირობების შესახებ და ა. შ. საგულისხმოა, რომ აღნიშნული ჩამონათვალი არ არის ამომწურავი, ვინაიდან მეტამონაცემი იქმნება, როგორც კომპიუტერული მოწყობილობის მომხმარებლის, ისე ავტომატურად, პროგრამული საშუალების მიერ და ეს ინფორმაცია შეიძლება იყოს მრავალგვარი.[45] პროგრამული საშუალების მიერ შექმნილი მეტამონაცემის დაზიანება, გაყალბება ან თუნდაც წაშლა ხშირ შემთხვევაში სირთულეს წარმოადგენს. აღნიშნულის მიზეზი კი მისი ფარული ბუნებაა. მაგალითისთვის, წარმოვიდგინოთ მომხმარებელი, რომელიც ელექტრონულ დოკუმენტს ქმნის, მუშაობის პროცესში პროგრამული საშუალება ავტომატურად განსაზღვრავს ინფორმაციას (მეტამონაცემს) დოკუმენტის შექმნის დროის, ავტორისა და მისი ადგილმდებარეობის შესახებ. ვინაიდან აღნიშნული მონაცემები არ არის ხილული მომხმარებლისათვის, არსებობს ალბათობა იმისა, რომ მას წარმოდ-

---

40 იქვე.

41 იქვე, 21.

42 *The Sedona Conference* – „სედონას კონფერენცია“, როგორც არაკომერციული, კვლევითი და საგანმანათლებლო ინსტიტუტი დაარსდა 1997 წელს *რიჩარდ ბრეიმანის* მიერ. სედონას კონფერენცია აერთიანებს რამდენიმე სამუშაო ჯგუფს, მათ შორის, სამუშაო ჯგუფს ელექტრონული დოკუმენტების შენახვისა და წარმოების შესახებ, რომლის მიზანს ელექტრონული დოკუმენტის მართვისა და ელექტრონული აღმოჩენის შესახებ სახელმძღვანელო პრინციპებისა და რეკომენდაციების შემუშავება წარმოადგენს. იხ.: <https://thesedonaconference.org/> [20.02.2021].

43 *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 207.

44 *Riley J.,* Understanding Metadata, National Information Standards Organization, Baltimore, MD, 2017, 1.

45 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 27.

გენა არ ჰქონდეს არამც თუ მისი შეცვლის ან განადგურების შესაძლებლობის, არამედ მისი არსებობის შესახებ.[46]

საინტერესოა ის ფაქტიც, რომ შესაძლებელია მეტამონაცემი არ იყოს უტყუარი.[47] მისი ნამდვილობა დამოკიდებულია, როგორც კომპიუტერული სისტემის გამართულად ფუნქციონირებაზე, ისე სხვა გარე ფაქტორებზე.[48] მეტი სიცხადისთვის, წარმოვიდგინოთ კომპიუტერული მოწყობილობა, რომლის დროის სარტყელი არასწორია. შესაბამისად, ამგვარი მოწყობილობის მიერ შექმნილი მეტამონაცემი დოკუმენტის შექმნის თარიღთან მიმართებით არაზუსტია.[49] იგივე შეიძლება ითქვას, დოკუმენტის ავტორთან დაკავშირებითაც, თუ კომპიუტერული მოწყობილობა სარგებლობისთვის გადაცემული აქვს მესამე პირს და ეს უკანასკნელი მფლობელის მიერ რეგისტრირებული ანგარიშით სარგებლობს, მაშინ მის მიერ განხორციელებული ნებისმიერი ქმედება და მასთან დაკავშირებული მეტამონაცემი არა მოწყობილობის მფლობელს ეკუთვნის, არამედ მესამე პირს, რომელიც რეალურად სარგებლობს მოწყობილობით.

აღნიშნულიდან გამომდინარე, შესაძლებელია ითქვას, რომ მაიდენტიფიცირებელი მონაცემი (მეტამონაცემი) ელექტრონული დოკუმენტის განუყოფელი ნაწილია[50] და წერილობითი დოკუმენტისგან განსხვავებით, იგი მხოლოდ მას ახასიათებს. ამასთან, ვინაიდან მისი შექმნა დამოუკიდებლად, ავტომატურად პროგრამის მეშვეობით ხდება, სირთულეს წარმოადგენს როგორც მისი წაშლა, ისე მისი დაუზიანებლად მოპოვებაც. ამავდროულად, მისი ნამდვილობა კომპიუტერული სისტემის გამართულ ფუნქციონირებასთან ერთად სხვა ფაქტორებზეც მნიშვნელოვნად არის დამოკიდებული.

3.2. მოცულობა და გამრავლების შესაძლებლობა

ფიზიკურ-გეოგრაფიული საზღვრების არსებობის მიუხედავად კომპიუტერული ტექნოლოგიებისა და ელექტრონული კომუნიკაციის საშუალებების განვითარებამ ინფორმაციის სწრაფ გაცვლა-გამოცვლას დაუდო დასაბამი. ერთმანეთთან დაკავშირებული კომპიუტერული სისტემებით, დროის უმოკლეს მონაკვეთში დედამიწის ნებისმიერი წერტილიდან დიდ მანძილზე დიდი მოცულობის ინფორმაციის გადაცემაა შესაძლებელი.

ელექტრონული კომუნიკაციის საშუალებებით ინფორმაციის გავრცელების თვალსაჩინო მაგალითს ინტერნეტი, სოციალური ქსელი და ელექტრონული ფოსტა წარმოადგენენ. ზემოთჩამოთვლილი არა მარტო ინფორმაციის სწრაფად გადაცემას უწყობს ხელს, არამედ მის განუსაზღვრელი რაოდენობით გამრავლებასაც. მეტი სიცხადისთვის, ელექტრონული ფოსტის მომხმარებლები ერთი და იმავე შეტყობინებას ერთდროულად მრავალ ადრესატს უგზავნიან, ხოლო მიმღებნი თავის მხრივ პასუხს უბრუნებენ წერილის ავტორს ან თავის მხრივ მე-

---

46 იქვე.

47 *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 211.

48 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 28.

49 იქვე.

50 *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 64.

სამე პირებს უგზავნიან მას. ამ დროს კი ხდება ელექტრონული წერილის მრავალი ეგზემპლარის შექმნა.[51]

ელექტრონული დოკუმენტის ადვილად გავრცელებისა და გამრავლების საკითხს ეხება საქმე „ამპ უცნობთა წინააღმდეგ“.[52] დაზარალებულის განცხადებით, მან კუთვნილი მობილური ტელეფონი დაკარგა, რომელშიც მისი სექსუალური ხასიათის ფოტომასალა იყო განთავსებული. ტელეფონის დაკარგვიდან, მცირე დროის შემდეგ, აღნიშნული ფოტოები ინტერნეტ-სივრცეში განთავსდა, რაც მომხმარებლებს საშუალებას აძლევდა გადმოეწერათ ან სხვებისთვის გაეზიარებინათ იგი. შედეგად კი ფოტომასალამ შვედეთის მთლიანი ინტერნეტ სივრცე მოიცვა.

ელექტრონული ინფორმაციის მარტივად დუბლირების თვალსაჩინო მაგალითს კომპიუტერული სისტემის მიერ კომპიუტერული მონაცემის სარეზერვო ასლის (*Backup*) შექმნა წარმოადგენს. მოცემული სისტემის მიზანი კი მონაცემთა დაკარგვის შემთხვევაში ორიგინალი დოკუმენტის აღდგენაა.[53]

ელექტრონული დოკუმენტის დუბლირებასთან ერთად, არანაკლებ საინტერესოა მისი მოცულობის საკითხი. საყურადღებოა, რომ თუ უწინ გარკვეული ოდენობის წერილობით მასალას დიდი ფართობის დაკავება შეეძლო, ახლა იმავე ან უფრო დიდი მოცულობის მასალის ელექტრონული ფორმით შენახვა მცირე ზომის მოწყობილობებშია შესაძლებელი. აღნიშნულს ხელი, კომპიუტერული ტექნოლოგიების განვითარებასთან ერთად, ინფორმაციის შემნახველი მოწყობილობების ხელმისაწვდომობამაც შეუწყო, რაც მომხმარებელს საშუალებას აძლევს მისთვის სასურველი რაოდენობის ელექტრონული მასალა განუსაზღვრელი ვადით შეინახოს.

ინფორმაციის შენახვის გავრცელებულ ფორმას ელექტრონული დოკუმენტების ქვეყნის ფარგლებს გარეთ, მესამე პირთა საკუთრებაში არსებულ სერვერებზე განთავსება წარმოადგენს. ინფორმაციის დეცენტრალიზებული შენახვის შესაძლებლობა ბევრ სიკეთესთან ერთად, გარკვეულ სამართლებრივ პრობლემებსაც ქმნის. აღსანიშნავია იურისდიქციასთან დაკავშირებული საკითხი და ამ ინფორმაციაზე კონტროლის დაკარგვის საშიშროება.[54] ამ მხრივ, საინტერესოა, თუ სად და როგორ ინახება იგი, რამდენად დაცულია კონფიდენციალურობის პრინციპი, ვინ არის პასუხისმგებელი მის დაცვაზე და ა.შ. როდესაც ინფორმაციის განთავსება მსოფლიოს სხვა წერტილში, მესამე პირის საკუთრებაში არსებულ ობიექტზე ხდება, ჩნდება საფრთხე, რომ ინფორმაციის შემქმნელი, გარკვეულწილად, კარგავს მასზე მფლობელობასა და განკარგვის შესაძლებლობას. მაგალითისთვის, თუ მომხმარებელი გადაწყვეტს აღნიშნული ფორმით შენახული ინფორმაციის წაშლას ან განადგურებას, იგი რთული გამოწვევის წინაშე დადგება. შესაძლებელია, მან მოითხოვოს მისი წაშლა, თუმცა გასათვალისწინებელია, რომ ელექტრონულ სივრცეში წაშლა არ ნიშნავს მის განადგურებას.[55] შესაბამისად, მომსახურების მიმწოდებლის მხრიდან კვლავ არსებობს მომხმარებლის კუთვნილი

---

[51] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 208.

[52] *AMP v. Persons Unknown*, [2011] EWHC 3454 (TCC).

[53] Back up Data, Nonprofit Technology Collaboration, 2013, 1, <https://www.baylor.edu/content/services/document.php/192120.pdf> [23.02.2021].

[54] *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 26.

[55] იქვე, 25.

დოკუმენტის არამიზნობრივი და უკანონო გამოყენებით მისი პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლების ხელყოფის საფრთხე.

ამრიგად, დარწმუნებით შეიძლება ითქვას, რომ ელექტრონული დოკუმენტის დუბლირებისა და მოცულობის საკითხი კვლავ მიუთითებს მასსა და წერილობით დოკუმენტს შორის არსებულ მნიშვნელოვან სხვაობაზე. ყოველივე კი საგამოძიებო ორგანოებისა და სასამართლო ხელისუფლების მხრიდან ელექტრონული მტკიცებულებისადმი განსხვავებული და ფრთხილი მოპყრობის აშკარა საფუძველს ქმნის.

3.3. ხანგრძლივუნარიანობა

მართალია, კომპიუტერული მონაცემის/ელექტრონული დოკუმენტის რამდენიმე მახასიათებელზე ვისაუბრეთ, თუმცა კიდევ ერთი, ძირითადი განმასხვავებელი ნიშანი წერილობით და ელექტრონულ დოკუმენტს შორის, ამ უკანასკნელის ხანგრძლივუნარიანობას უკავშირდება.

ელექტრონული დოკუმენტისა და წერილობითი დოკუმენტის ურთიერთშედარებით ნათელი ხდება, რომ ელექტრონული დოკუმენტის წაშლა ან განადგურება სირთულეს წარმოადგენს. წერილობითი დოკუმენტის გასანადგურებლად მისი დაქუცმაცება ან დაწვაც სრულიად საკმარისია, რასაც ელექტრონულ დოკუმენტზე ვერ ვიტყვით.[56]

ელექტრონული ფორმით შენახულ ინფორმაციაზე საუბრისას, სიტყვამ „წაშლა“ შესაძლებელია, საკითხით დაინტერესებული პირი შეცდომაში შეიყვანოს, ვინაიდან იგი სრულებით არ გულისხმობს ინფორმაციის შემნახველი მოწყობილობიდან მის გაქრობას.[57]

საკითხის უკეთ გასაგებად, უმჯობესია კომპიუტერული სისტემის მიერ ელექტრონული ინფორმაციის შენახვის პრინციპი განვიხილოთ. კომპიუტერული მოწყობილობა მასში არსებულ დოკუმენტს ანიჭებს პირობით აღმნიშვნელს, ხოლო როდესაც მომხმარებელი გადაწყვეტს დოკუმენტით სარგებლობას, კომპიუტერული სისტემა ინდექსის მეშვეობით ადგენს იმ სექტორს, სადაც ინფორმაციაა განთავსებული. ხოლო მომხმარებლის მიერ ინფორმაციის „წაშლის“ დროს კი კომპიუტერული სისტემა არა თუ ანადგურებს ინფორმაციას, არამედ ათავისუფლებს კონკრეტულ სექტორს სხვა ინფორმაციის ჩასაწერად. შესაბამისად, იმ შემთხვევაში თუ კონკრეტულ სექტორზე არ მოხდება ძველი ინფორმაციის ახლით გადაწერა, მანამდე „წაშლილი“ ინფორმაციის აღდგენა კომპიუტერული ექსპერტიზის შედეგად სრულებით შესაძლებელია.[58]

ელექტრონული დოკუმენტის/მტკიცებულების განადგურების ეფექტიან საშუალებას ძველი მონაცემების ახლით შეცვლასთან ერთად, სითბოს გამოყენება ან მისი ფიზიკური, ან მაგნიტური დაზიანება წარმოადგენს.[59]

---

[56] *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 65.

[57] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 209.

[58] *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 65-66.

[59] იქვე.

ამრიგად, ნათელია, რომ ელექტრონული დოკუმენტი ხანგრძლივუნარიანია და წერილობითი დოკუმენტისგან განსხვავებით მისი განადგურება გარკვეულ სირთულეებთან არის დაკავშირებული, რაც კიდევ ერთხელ ხაზს უსვამს სამართალდამცავი უწყებების მხრიდან მისდამი განსხვავებული მოპყრობის აუცილებლობას.

3.4. დინამიურობა და ცვალებადობა

დინამიურობა და ცვალებოდა ელექტრონული ინფორმაციის ერთ-ერთი ფუნდამენტური მახასიათებელია. წერილობითი დოკუმენტისგან განსხვავებით, ადამიანური რესურსის ჩარევის მიუხედავად შესაძლებელია ელექტრონული დოკუმენტის შინაარსის ავტომატურად შეცვლა.[60] ნათელ დადასტურებას კომპიუტერული სისტემის მიერ მონაცემთა ავტომატური განახლება წარმოადგენს, რაც, ძირითად შემთხვევაში, დოკუმენტის ადგილმდებარეობის შეცვლას იწვევს. აგრეთვე, ელექტრონული ფოსტა, რომელიც ავტომატურად და პერიოდულად ანახლებს ინფორმაციას მიღებული და გაგზავნილი შეტყობინებების შესახებ და ძველ მონაცემებს ანადგურებს.[61]

ასევე გასათვალისწინებელია, რომ ელექტრონული ფორმით შენახული ინფორმაციის შეცვლა მრავალი ხერხით არის შესაძლებელი, რაც, ძირითად შემთხვევებში, შეუმჩნეველი რჩება მომხმარებლისათვის და მისი დადგენა შეუძლებელია კომპიუტერულ-ტექნიკური ექსპეტიზის გარეშე. მაგალითისთვის, რომელიმე დოკუმენტის ადგილმდებარეობის შეცვლამ, შესაძლოა მისი შექმნისა და მასში განხორციელებული ცვლილებების თარიღის ცვლილება გამოიწვიოს, რომლის დაზუსტებაც მეტამონაცემების გამოკვლევის გარეშე შეუძლებელია.[62]

ყოველივედან გამომდინარე კი კვლავ დარწმუნებით შესაძლებელია ითქვას, რომ კომპიუტერული მონაცემის გამოკვლევა განსაკუთრებულ სიფრთხილეს მოითხოვს და მისი სანდოობის დადგენისთვის კომპიუტერულ-ტექნიკური ექსპეტიზის ჩატარება გარდაუვალია. ამასთან, მისი დინამიური და ცვალებადი ხასიათის საპასუხოდ „კიბერდანაშაულის შესახებ“ კონვენციაში საპროცესო ინსტრუმენტის სახით გათვალისწინებულია როგორც შენახული კომპიუტერული მონაცემის დაჩქარებული დაცვა, ისე ინტერნეტ-ტრაფიკის მონაცემთა დაჩქარებული დაცვა და ნაწილობრივ გადმოცემა, რომლებიც დამოუკიდებელი საგამოძიებო მოქმედებების სახით საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში ამ დროისთვის ასახული არ არის.[63] ხოლო მოცემული საგამოძიებო მოქმედებები მნიშვნელოვან ბერკეტს წარმოადგენენ გამოძიების პროცესში იმგვარი ელექტრონული ინფორმაციის მოპოვებისათვის, რომელთა დაკარგვის ან სახეცვლილების საფრთხეც არსებობს.

3.5. გარემოზე დამოკიდებულება

თუ წერილობითი დოკუმენტის წასაკითხად კარგი მხედველობა და ენის ცოდნა სრულიად საკმარისია, ელექტრონული დოკუმენტის შემთხვევაში ეს არ კმარა. ეს ნაკლოვანება კი

---

[60] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 209.

[61] იქვე.

[62] იქვე.

[63] Convention on Cybercrime, Budapest, 23/11/2001, Art. 16-17.

მისი მოწყობილობისა და პროგრამული უზრუნველყოფისადმი დამოკიდებულებით არის გამოწვეული. მეტიც, მათი დახმარების გარეშე მომხმარებელი არა თუ დოკუმენტის გაცნობას შეძლებს, არამედ ვერ შექმნის მას, მის შეცვლასა და დაზიანებაზე რომ არაფერი ვთქვათ.[64]

ელექტრონული დოკუმენტის გარემოზე დამოკიდებულების ნათელსაყოფად მესამე პირისთვის „ვორდის" დოკუმენტის გაგზავნის მაგალითი შეგვიძლია მოვიყვანოთ. ხშირად ჩვენ მიერ სხვისთვის გაზიარებული დოკუმენტი ადრესატის კომპიუტერულ სისტემაში სათანადოდ ან საერთოდ არ ფუნქციონირებს. აღნიშნულის მიზეზს კი განხვავებული პროგრამული უზრუნველყოფა წარმოადგენს.

ტექნიკური და პროგრამული უზრუნველყოფის განვითარების ტემპმა სამართლებრივი კუთხითაც მრავალი პრობლემა შექმნა. კერძოდ, სირთულეს წარმოადგენს ტექნოლოგიის განვითარების კვალდაკვალ მიყოლა. როგორც იურიდიულ ლიტერატურაში აღნიშნავენ, ელექტრონულ მტკიცებულებებთან მიმართებით იურისტებისა და ექსპერტების პრაქტიკულ გამოცდილებაზე მეტად მათი მუდმივი გადამზადებაა აუცილებელი.[65]

გამოწვევებს ვხვდებით გამოძიების კუთხითაც. მაგალითისთვის, ტექნოლოგიის სწრაფი განვითარების შედეგად რთულია გამოძიებისთვის რელევანტური მტკიცებულების მოპოვება. აღნიშნული შეიძლება გამოწვეული იყოს ორი მიზეზით. ერთი, რომ იმ მომენტისთვის არ შექმნილა შესაბამისი ხელსაწყო კომპიუტერული მონაცემის მოსაპოვებლად და მეორე, მისი შეძენა კოლოსალურ თანხებთან არის დაკავშირებული.[66]

ამრიგად, ცხადია, რომ კომპიუტერული და პროგრამული სისტემები მუდმივად ვითარდება და იმისათვის, რომ კომპიუტერული მონაცემი ადამიანისათვის აღქმადი გახდეს, ამისთვის ტექნოლოგიათა მთელი რიგის გამოყენებაა აუცილებელი. შესაბამისად, შეიძლება ითქვას, რომ ელექტრონული მონაცემის არსებობა კომპიუტერული სისტემისა და პროგრამისგან დამოუკიდებლად გამორიცხულია.

3.6. დისპერსია

ელექტრონული ინფორმაციის ბუნებიდან გამომდინარე, შესაძლებელია მისი მრავალი ეგზემპლარის შექმნა. ამრიგად, თითოეული შესაძლოა, სხვადასხვა ადგილას იყოს განთავსებული – კომპიუტერულ სისტემაში არსებული ოპერატიული მეხსიერებაში ან მყარ დისკზე. აგრეთვე დამოუკიდებელი ინფორმაციის შემნახველები, როგორებიცაა კომპაქტური დისკი, მეხსიერების ბარეთები ან თუნდაც ონლაინ საცავი.

მიუხედავად მათი განსხვავებული ადგილმდებარეობისა, ელექტრონული დოკუმენტები იდენტურად გამოიყურებიან, რაც, გარკვეულწილად, ართულებს მათ შორის პირველწყაროსა და არაორიგინალის გარკვევას. ამას გარდა, შესაძლოა წარმოუდგენლი იყოს დიდი მოცულობის ელექტრონულ ინფორმაციასთან გამკლავება, თუმცა წერილობით დოკუმენტთან შედარებით, ელექტრონული დოკუმენტის მოძიება ნაკლებ ძალისხმევას მოითხოვს. აღნიშნული, კომპიუტერული სისტემის მიერ ავტომატური ძებნის მეთოდით არის განპირობებული.[67]

---

[64] *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 21.

[65] იქვე, 23.

[66] იქვე, 24.

[67] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for

შესაბამისად, ელექტრონული დოკუმენტის დისპერსიულობიდან გამომდინარე, იდენტური შინაარსის მქონე დოკუმენტებს შორის არსებული სხვაობის, ორიგინალობის საკითხის დადგენა მხოლოდ კომპიუტერულ-ტექნიკური ექსპერტიზის მეშვეობით არის შესაძლებელი.

4. კომპიუტერული მონაცემის ავთენტურობა

სისხლის სამართლის საპროცესო სამართლის მიხედვით მტკიცების პროცესი მტკიცებულებათა მოპოვების, მათი საპროცესო დამაგრების, გამოკვლევისა და შეფასებისგან შედგება.[68] მტკიცების პროცესში თითოეული მათგანის მნიშვნელობა განსაკუთრებულია, თუმცა მოცემულ თავში ძირითადად ყურადღება ელექტრონული მტკიცებულების შეფასების საკითხზე გამახვილდება.

საყურადღებოა, რომ მტკიცებულების შეფასება სამართალწარმოების ყველა საფეხურზე მიმდინარეობს, თუმცა საბოლოოდ მისი ფასეულობის განსაზღვრა მხოლოდ სასამართლოს ძალუძს.[69] ამრიგად, გარკვეულწილად მხარეებმა, ხოლო სრული მოცულობით კი სასამართლომ მტკიცებულება კუმულაციურად, რელევანტურობის, დასაშვებობისა და უტყუარობის თვალსაზრისით უნდა შეაფასონ.[70] მტკიცებულება რელევანტურად მიიჩნევა, თუ მას კავშირი აქვს საქმისათვის მნიშვნელოვან გარემოებებთან.[71] ნეგატიური ენუმერაციის პრინციპიდან გამომდინარე, კი სისხლის სამართლის პროცესში მტკიცებულება დასაშვებია, თუ მისი დაუშვებლად ცნობის საფუძველი არ არსებობს.[72] რაც შეეხება უტყუარობას, იგი მტკიცებულების სანდოობასა და ავთენტურობას მოიცავს.[73] ხოლო თავის მხრივ ავთენტურობა არის მტკიცებულების ფუნქცია, უნარი დაადასტუროს მისი ნამდვილობა, დედანთან შესაბამისობა.[74]

სამეცნიერო ლიტერატურაში კომპიუტერული მონაცემის ავთენტურობის საკითხს წერილობით ინფორმაციასთან/დოკუმენტთან შედარების ჭრილში განიხილავენ. მეცნიერთა ერთი ნაწილი მიიჩნევს, რომ წესები, რომლებიც წერილობითი დოკუმენტის ავთენტურობის დასადგენად გამოიყენება სრულებით ვარგისია ელექტრონულ დოკუმენტთან მიმართებით,[75] მეორე ნაწილის ხედვით კი – ელექტრონული დოკუმენტის/ჩანაწერის ნიშან-თვისებებიდან გამომდინარე არსებული ნორმების გამკაცრება ან საკითხის ახლებურად მოწესრიგებაა საჭირო.[76]

Addressing Electronic Document Production, 3th ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 213.

68 *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი – ზოგადი ნაწილის მიმოხილვა, თბ., 2014, 225-226.

69 *ფაფიაშვილი ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 288.

70 საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 03/11/.2009, მუხ. 82(1).

71 Federal Rules of Evidence, Article IV, Rule 401, 20/11/1972.

72 საქართველოს საკონსტიტუციო სასამართლოს 2015 წლის 31 ივლისის გადაწყვეტილება საქმეზე: „საქართველოს მოქალაქე მაია რობაქიძე საქართველოს პარლამენტის წინააღმდეგ“, № 2/2/579, 12.

73 *Mason S.*, *Stanfield A.,* Authenticating Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 193.

74 *Gonzales R. A., Schofield B. R., Hagy W. D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 28.

75 *Mason S.*, *Stanfield A.,* Authenticating Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 193.

76 *Johnson A. M.,* Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability, Marquette Law Review, Vol. 75, Issue 2, 1992, 445.

საუკეთესო გზა მეცნიერთა შორის ელექტრონული დოკუმენტის ავთენტურობასთან დაკავშირებული აზრთა სხვადასხვაობისა და არსებული გამოწვევების უკეთ გასააზრებლად ეროვნული კანონმდებლობის უცხო ქვეყნის კანონმდებლობასთან შედარება და მისი ანალიზია. აღსანიშნავია, რომ ელექტრონული მტკიცებულების ავთენტურობის მხრივ ამერიკის შეერთებული შტატებისა და კანადის კანონმდებლობა მსგავსია. მტკიცებულების შესახებ ფედერალური კანონისა და კანადის მტკიცებულებათა აქტის მიხედვით მტკიცებულების ავთენტურობის დადგენის საშუალებებს მოწმეთა ჩვენება, არაპირდაპირი (ირიბი) მტკიცებულება და იმგვარი შინაარსის მტკიცებულება წარმოადგენს, რომელიც ინფორმაციის მოპოვების პროცესის უტყუარობაზე მიუთითებს.[77] მხარეს, რომელსაც გადაწყვეტილი აქვს სასამართლოში ელექტრონული დოკუმენტის მტკიცებულებად გამოყენება, როგორც წესი, მისი ავთენტურობის დასამტკიცებლად სამ მნიშვნელოვან კითხვას უნდა გასცეს პასუხი. კერძოდ, სასამართლოს უნდა მიაწოდოს ინფორმაცია ჩანაწერის ბუნების, წყაროსა და მისი ერთიანობის შესახებ.[78] ელექტრონული დოკუმენტის წყარო ავთენტურობის განსაზღვრასთან ერთად ზეგავლენას მის სანდოობაზეც ახდენს. მონაცემის შემნახველი, იქნება ეს მყარი თუ კომპაქტური დისკი ან სხვა ინფორმაციის ნებისმიერი მატარებელი, ბუნებით არამყარია. დროის გარკვეულ მანძილზე, როგორც ადამიანის ზემოქმედებით, ისე მის გარეშე, გარე ფაქტორების ზეგავლენით შესაძლებელია მასში მოთავსებული ინფორმაციის დაკარგვა ან დაზიანება.[79] შესაბამისად, მხარემ უნდა დაარწმუნოს სასამართლო, რომ ელექტრონული მტკიცებულება ნამდვილია და იგი სანდო წყაროდან არის მოპოვებული.[80] სწორედ კომპიუტერული მონაცემის ცვალებადი ბუნებისა და სხვა მისთვის დამახასიათებელი ნიშან-თვისებებზე დაყრდნობით ითხოვს მეცნიერთა ნაწილი ელექტრონულ დოკუმენტთან დაკავშირებული კანონმდებლობის ახლებურად ჩამოყალიბებას.

ციფრული მტკიცებულების ავთენტურობის განსაზღვრისას აგრეთვე მნიშვნელოვანია ინფორმაციის მიღების ფორმის საკითხი. კერძოდ, ელექტრონული ჩანაწერი უშუალოდ კომპიუტერული სისტემის/პროგრამის ფუნქციონირების შედეგია თუ ინფორმაცია კომპიუტერულ სისტემაში ელექტრონული ფორმით მომხმარებელმა განათავსა.

კომპიუტერულ სისტემაში დაცული ინფორმაციის ნამდვილობის დადგენისათვის აუცილებელია ჩანაწერის ავტორის ვინაობის დადგენა და მისი შინაარსობრივი მხარის ერთიანობის განსაზღვრა. ელექტრონული დოკუმენტის შემთხვევაში კი მისი ავტორის დადგენა გარკვეულ სირთულეებთან არის დაკავშირებული. საილუსტრაციოდ გამოვიყენოთ ელექტრონული ფოსტის მაგალითი. მართალია, შეტყობინება კონკრეტული პირის ანგარიშით იგზავნება, თუმცა ეს სრულებით არ ნიშნავს, რომ მისი ავტორი საფოსტო ანგარიშის მესაკუთრეა. შესაძლებელია, ანგარიშზე წვდომა რამდენიმე პირს ჰქონდეს. ასეთ შემთხვევაში, მიზანშეწონილია, მაიდენტიფიცირებელი მონაცემების, იგივე მეტამონაცემების გამოკვლევა, რაც ელექტრონული ჩანაწერის განუყოფელი ნაწილია და შეიცავს ინფორმაციას მისი შექმნის დროის, ადგილმდებარეობისა და მეთოდების შესახებ. ეს კი ერთი მხრივ შესაძლებლობას იძლევა იმ

---

77 Federal Rules of Evidence(USA), Rule 901(b)(1,4,9), 20/11/1972 (Amendment of 1/12/2019). იხ. Canada Evidence Act, 1985, Section 31.1-31.7.

78 *Gregory D. J.,* Authentication Rules and Electronic Evidence, The Canadian Bar Review, Vol. 81, № 3 , 2001, 531.

79 იქვე, 537.

80 *Capra D.,* Authenticating Digital Evidence, Baylor Law Review, № 1, 2017, 3.

მომხმარებელთა განსაზღვრისათვის, რომელთაც წვდომა ჰქონდათ დოკუმენტზე,[81] ხოლო მეორე მხრივ ჩანაწერის უცვლელობის დადგენისათვის. არანაკლებ მნიშვნელოვანია საგამოძიებო ორგანოების მიერ მტკიცებულების მოპოვებიდან მის სასამართლოში წარდგენამდე ინფორმაციის უცვლელობის საკითხიც. ამ მხრივ არსებითად მნიშვნელოვანია სრულყოფილი საგამოძიებო მოქმედების ამსახველი ოქმის არსებობა, სადაც მითითებული იქნება თუ რა სახის კომპიუტერული ინფორმაცია მოიპოვეს, კომპიუტერული მონაცემი ბეჭდური სახით ამოიღეს თუ ციფრულ ფორმატში, ვინ და რა მეთოდების გამოყენებით მოიპოვა იგი, რამდენ ადამიანს ჰქონდა წვდომა ამოღებულ ინფორმაციაზე, იყო თუ არა კომპიუტერულ სისტემაში არსებული ინფორმაცია პაროლით დაცული, როდის მოხდა აღნიშნული საგამოძიები მოქმედების ჩატარება და ა. შ.[82] მოვლენების სრულყოფილი და თანმიმდევრული აღწერა ერთი მხრივ მხარეებს სასამართლოს წინაშე წარდგენილი მტკიცებულების ერთიანობის დადასტურებაში დაეხმარებათ, მეორე მხრივ კი მის დამაჯერებლობასა და სანდოობას მნიშვნელოვნად გაზრდის. შესაბამისად, შეიძლება ითქვას, რომ საგამოძიებო ოქმთან ერთად, სადაც საგამოძიებო მოქმედებები დეტალურად და თანმიმდევრულად არის აღწერილი, ასევე მისი შემდგენისა და ინფორმაციის მოპოვების პროცესში ჩართული პირების ჩვენებებით შესაძლებელია ელექტრონული მტკიცებულების ერთიანობის დადგენა.

როგორც კომპიუტერულ სისტემაში შენახული ინფორმაციის, ისე კომპიუტერული სისტემის მიერ ავტომატურად შექმნილი მონაცემის ავთენტურობის განსასაზღვრად, კომპიუტერული მოწყობილობის გამართულად ფუნქციონირებაა მნიშვნელოვანი. თუმცა ყურადსაღებია ის ფაქტიც, რომ ამ უკანასკნელის გამართულობა ელექტრონული ჩანაწერის ნამდვილობისა და უტყუარობის გარანტს არ წარმოდგენს.[83] ამასთან, შესაძლებელია კომპიუტერული სისტემა აბსოლუტურად გამართულად ვერ ფუნქციონირებდეს, თუმცა ამგვარმა ხარვეზმა ზეგავლენა ვერ მოახდინოს სისხლის სამართლის საქმისთვის მნიშვნელოვანი დოკუმენტის მთლიანობაზე. შესაბამისად, აუცილებელია საქმეში მოიპოვებოდეს მტკიცებულება, რომელიც კომპიუტერული სისტემის ან მისი მსგავსი მოწყობლობის გამართულად მუშაობას დაადასტურებს ან გამორიცხავს სისტემაში არსებული ხარვეზის ზეგავლენას გამოძიებისთვის მნიშვნელოვან ელექტრონულ ჩანაწერზე.[84]

თეორიულ მსჯელობასთან ერთად, საინტერესოა სასამართლოს მიდგომის შესწავლაც განსახილველი საკითხისადმი. მაგალითისთვის, ბრალდებულ *მორგანს,*[85] რომელსაც ბრალად სათევზაო ლიცენზიის პირობების დარღვევა ედებოდა, მის წინააღმდეგ ბრალდების მხარემ სასამართლოში მტკიცებულებად ელექტრონული ნებართვის ასლი წარადგინა. სასამართლომ დოკუმენტის ავთენტურობის დადგენისას მოწმის ჩვენებაზე, დოკუმენტის დამახასიათებელ ნიშნებსა და დაცვის მხარის მხრიდან საპირისპირო არგუმენტების არარსებობაზე გაამახვილა ყურადღება.[86]

---

[81] *Outerbridge D., Siller E.,* The Admissibility of Electronic Evidence, 2015, 11, <https://www.lawinsider.com/documents/1tYTXnzcs2u> [23.02.2021].

[82] *Gonzales R. A., Schofield B. R., Hagy W. D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 28.

[83] *Outerbridge D., Siller E.,* The Admissibility of Electronic Evidence, 2015, 11, <https://www.lawinsider.com/documents/1tYTXnzcs2u> [23.02.2021].

[84] *Gonzales R. A., Schofield B. R., Hagy W. D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 44.

[85] *R. v. Morgan, (*2002), N.J., № 15, (NLPC).

[86] იქვე, §22.

აგრეთვე ყურადსაღებია *ნიკოლსის* საქმე[87], რომელშიც სასამართლომ მოქალაქის მიერ გადაუდებელი დახმარების სამსახურის ცხელ ხაზზე განხორციელებული სატელეფონო ზარი კანადის მტკიცებულებათა აქტზე დაყრდნობით ელექტრონულ დოკუმენტად მიიჩნია, ხოლო მისი ავთენტურობის დადგენისთვის ყურადღება კავშირგაბმულობისა და სატელეფონო სისტემის გამართულობას მიაპყრო. ოპერატორის ჩვენების თანახმად სისტემა ტექნიკურად მწყობრში იყო. ამასთან, დასაქმებულთა მუშაობის ხარისხზე ზედამხედველიც სამსახურში იმყოფებოდა და მისი განცხადებით მუშაობის პროცესში რაიმე გართულებას ადგილი არ ჰქონია. ყოველივედან გამომდინარე კი, სასამართლომ ელექტრონული ჩანაწერი ავთენტურად მიიჩნია.

სასამართლო ორივე შემთხვევაში ექსპერტთა დასკვნების ნაცვლად მოწმეთა ჩვენებებს დაეყრდნო. ერთი მხრივ, შესაძლოა მოწმეთა ჩვენებებით კომპიუტერული სისტემის გამართულად ფუნქციონირების შესახებ ინფორმაცია მივიღოთ, თუმცა არანკლებ მნიშვნელოვანია იმის დადგენა თუ რამდენად სწორი და სანდო მონაცემი წარედგინა სასამართლოს. როდესაც საქმე თავად სისტემის მიერ ავტომატურად დამუშავებულ ინფორმაციასთან გვაქვს, სადაც ადამიანის ხელი არ ურევია, რა თქმა უნდა, ელექტრონული დოკუმენტი, როგორც საბოლოო შედეგი მომხმარებლის მიერ კომპიუტერულ სისტემაში შეყვანილ მონაცემთან შედარებით მეტი სანდოობით გამოირჩევა, თუმცა აღნიშნული ვერ იქნება აბსოლუტურად უტყუარი და რიგ შემთხვევებში, საქმის გარემოებებიდან გამომდინარე მისი ავთენტურობის დასადგენად შესაძლოა ექსპერტთა დასკვნის წარდგენა გახდეს საჭირო. იგივე შეიძლება ითქვას მომხმარებლის მიერ კომპიუტერულ მოწყობილობაში შეყვანილ მონაცემზეც.

ყოველივე ზემოაღნიშნულთან ერთად ინტერესის საგანია ბეჭდური სახით სასამართლოსთვის წარდგენილი ელექტრონული მონაცემის ნამდვილობის საკითხიც. მისი ნამდვილობა და დედანთან შესაბამისობა სხვა სახის კომპიუტერული მონაცემის მსგავსად კომპიუტერული მოწყობილობის გამართულად მუშაობაზეა დამოკიდებული. განსხვავებით სხვა ელექტრონული დოკუმენტებისგან, იგი სასამართლოსა და მხარეებს არა ელექტრონული ფორმით, არამედ მატერიალური სახით მიეწოდება. შესაბამისად, ისინი მოკლებულნი არიან მისი ორიგინალი სახით გაცნობის შესაძლებლობას. შეიძლება ითქვას, რომ ამონაბეჭდის ავთენტურობის კვლევისას სირთულეს არაოფიციალური დოკუმენტის შემთხვევაში ვაწყდებით, ვინაიდან ოფიციალური დოკუმენტის რეკვიზიტების დახმარებით მისი ნამდვილობის განსაზღვრა ნაკლებ ძალისხმევას მოითხოვს, ხოლო ამონაბეჭდს, რომელსაც არ გააჩნია დამახასიათებელი ნიშნები და მხარე მას სასამართლოში წარადგენს, მისი უტყუარობისა და დედანთან შესაბამისობის წარმოსაჩენად შესაძლოა ექსპერტიზის დასკვნის წარდგენაც კი დასჭირდეს, რომელიც სასამართლოს ინფორმაციის წყაროს, შემქმნელი მოწყობილობის გამართულობისა და დედანთან, ელექტრონული ფორმით არსებულ ინფორმაციასთან შესაბამისობას დაუდასტურებს.

ამერიკის შეერთებული შტატებისა და კანადის კანონმდებლობასთან ერთად, არანაკლებ საინტერესოა თუ როგორ არის გადაწყვეტილი დოკუმენტის ავთენტურობის საკითხი საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობით. მართალია საპროცესო კანონმდებლობა არ შეიცავს დოკუმენტის ავთენტურობასთან დაკავშირებულ ნორმებს, თუმცა

[87] *R. v. Nichols,* (2004), № 6186, CarswellOnt 8225, (Ont. C.J.).

განსაზღრავს დოკუმენტის მტკიცებულებითი ძალისა და დასაშვებობის საკითხს. კერძოდ, სსსკ-ის 78-ე მუხლის 1-ლი ნაწილის მიხედვით დოკუმენტს მტკიცებულებითი ძალა აქვს თუ ცნობილია მისი წარმომამვლობა და ის ავთენტიკურია. აგრეთვე, იგი დასაშვები მტკიცებულებაა თუ მხარეს შეუძლია მოწმედ დაკითხოს პირი, რომელმაც მოიპოვა/შექმნა ან/და რომელთანაც სასამართლოსთვის წარდგენამდე ინახებოდა იგი. ამასთან, სსსკ-ის 248-ე მუხლის 1-ლი ნაწილით საქმის არსებით განხილვაზე ის მტკიცებულებაა დასაშვები, რომლის ავთენტიკურობაც დასტურდება.

მტკიცებულებითი ძალის განსაზღვრასთან ერთად დოკუმენტის წარმომავლობას განსაკუთრებული მნიშვნელობა აქვს მისი ავთენტურობის დადგენის პროცესშიც. მოგეხსენებათ დოკუმენტის წარმომავლობით ვიღებთ ინფორმაციას მისი შედგენის დროის, ადგილმდებარეობის, ვითარების, ავტორის, მასში ცვლილების შეტანის საფუძვლისა და სხვა მნიშვნელოვანი გარემოებების შესახებ.[88] ამრიგად, შეიძლება ითქვას, რომ მესაკუთრის ან მფლობელის დაკითხვით, რომელთაც შეუძლიათ გამოძიებასა და სასამართლოს ინფორმაცია მიაწოდონ დოკუმენტის წარმომავლობის შესახებ, გარკვეულწილად შესაძლებელია მისი ნამდვილობისა და უტყუარობის განსაზღვრა. მესაკუთრისა და მფლობელის ჩვენებების გარდა საპროცესო კანონმდებლობა დოკუმენტის მომპოვებელი და შემნახველი პირების ჩვენების მიღების შესაძლებლობასაც უშვებს. რა თქმა უნდა, აღნიშნული ობიექტური გარემოებებით უნდა იყოს განპირობებული.[89]

დოკუმენტთან უშუალო კავშირში მყოფი პირების გარდა, მისი ნამდვილობის დადგენა პირდაპირი მტკიცებულებით, მოწმე-ექსპერტის ჩვენებით, ექსპერტიზის დასკვნითა და სხვა უამრავი ხერხით არის შესაძლებელი, რომელთა ამომწურავად ჩამოთვლა პრაქტიკულად შეუძლებელია.[90]

მიუხედავად განსხვავებული სამართლებრივი სისტემებისა, მნიშვნელოვანი მსგავსება გამოიკვეთა დოკუმენტის ავთენტურობის დადგენის საშუალებებს შორის. სამივე კანონმდებლობის მიხედვით დოკუმენტის ნამდვილობის დასადასტურებლად ძირითადად მოწმის ჩვენებას, ექსპერტიზის დასკვნასა და სხვა პირდაპირ ან არაპირდაპირ მტკიცებულებებს ენიჭება უპირატესობა. ამას გარდა, სასამართლო პრაქტიკამ ცხადყო, რომ წერილობითი დოკუმენტის ავთენტურობის დასადგენად არსებული ნორმების გამოყენება ელექტრონულ დოკუმენტთან მიმართებით მიზანშეწონილია, თუმცა მასთან შედარებით აუცილებელია კომპიუტერული მონაცემისთვის დამახასიათებელ ნიშან-თვისებებსა და მის ერთიანობაზე მოქმედ გარემოებებზე ყურადღების გამახვილება. კერძოდ, ავთენტურობის შეფასებისას მნიშვნელოვანია ავტორის ვინაობის დადგენა, წყაროს სანდოობის განსაზღვრა, ელექტრონული ინფორმაციის მიღებისა და მოპოვების ხერხებისა და საშუალებების შესწავლა, მისი ერთიანობისა და უცვლელობის დადგენა. იმ შემთხვევაში თუ სამართალწარმოების პროცესში ზემოთჩამოთვლილი გარემოებები ზუსტად და ყოველმხრივ იქნება გამოკვლეული, კომპიუტერული მონაცემის ცვალებადი ბუნების მიუხედავად, მათთან მიმართებაში წერილობითი დოკუმენტისთვის არსებული ნორმების გამოყენება სრულებით შესაძლებელი იქნება.

---

[88] *ფაფიაშვილი ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 276.
[89] იქვე, 275.
[90] იქვე, 277.

5. დასკვნა

ციფრული მოწყობილობების ყოვლისმომცველობისა და მათზე ჩვენი თითქმის სრული მოცულობით დამოკიდებულების გათვალისწინებით, თანამედროვე სამყაროში წარმოუდგენელია „დანაშაული“, რომელსაც კავშირი არ აქვს ციფრულ განზომილებასთან.[91] ციფრულმა სამყარომ საქმიანობის სხვადასხვა სფეროს წარმომადგენელთა მსგავსად, იურისტების საქმიანობაზეც იქონია ზეგავლენა. შესაბამისად, ელექტრონულ მტკიცებულებებთან დაკავშირებული რიგი სპეციფიკური საკითხების ცოდნა მათთვის არა სავალდებულო, თუმცა მნიშვნელოვანია.

იმის გათვალისწინებით, რომ კომპიუტერული მონაცემი და ელექტრონული მტკიცებულება მტკიცების პროცესში სიახლეს წარმოადგენს და მისი სპეციფიკური და ტექნიკური მახასიათებლებიდან გამომდინარე, მნიშვნელოვან გამოწვევად იქცა იურიდიული საზოგადოებისათვის, ნაშრომში უპირატესად ყურადღება მათი შინაარსობრივი მხარის კვლევას, მახასიათებელი ნიშნების გამოკვეთასა და კომპიუტერული მონაცემის ავთენტურობასთან დაკავშირებულ საკითხებს დაეთმო.

სხვადასხვა სამეცნიერო ლიტერატურის, ქვეყნის გამოცდილების კვლევამ და შედარებითსამართლებრივმა ანალიზმა ცხადყო, რომ მიუხედავად კომპიუტერული მონაცემისა და ელექტრონული მტკიცებულების ფართო შინაარსისა, მათი დეფინიცია ერთიანია და შესაძლოა შემდეგნაირად ჩამოყალიბდეს – „კომპიუტერული მონაცემი, ეს მომხმარებლის მიერ კომპიუტერულ სისტემაში შეყვანილი, ხოლო შემდგომ კომპიუტერული მოწყობილობის მიერ ავტომატურად დამუშავებული, შენახული ან გადაცემული ნებისმიერი სახის ინფორმაციაა“. რაც შეეხება ელექტრონულ მტკიცებულებას, აღნიშნული, „კომპიუტერულ სისტემაში არსებული კომპიუტერული მონაცემია, რომელიც ღირებულია გამოძიებისთვის ან პროცესის მონაწილე მხარისათვის, სასამართლოში მნიშვნელოვანი გარემოებების დასადასტურებლად“.

კომპიუტერული მონაცემების მახასიათებლების კვლევამ ხელი შეუწყო ელექტრონულ და მატერიალურ მტკიცებულებებს შორის არსებული სხვაობის უკეთ წარმოჩენას და ცხადყო, რომ საპროცესო კანონმდებლობაში ახალი, დამატებითი საპროცესო ინსტრუმენტების გათვალისწინების აუცილებლობა არსებობს. მაგალითისთვის, კომპიუტერული მონაცემის დინამიურობისა და ცვალებადი ბუნების საპასუხოდ „კიბერდანაშაულის შესახებ“ კონვენციით გათვალისწინებული საგამოძიებო მოქმედებების, „მონაცემთა დაჩქარებული დაცვის ბრძანება“.

კომპიუტერული მონაცემის მახასიათებლების მნიშვნელობა მით უფრო იზრდება მისი ავთენტურობის კვლევის პროცესში, თუმცა ყოველივესთან ერთად მნიშვნელოვანია ინფორმაციის მიღების ფორმის საკითხი. კერძოდ, ელექტრონული ჩანაწერი უშუალოდ კომპიუტერული სისტემის/პროგრამის ფუნქციონირების შედეგია თუ ინფორმაცია კომპიუტერულ სისტემაში ელექტრონული ფორმით მომხმარებელმა განათავსა. საყურადღებოა ბეჭდური სახით წარდგენილი ელექტრონული მონაცემის ნამდვილობის საკითხიც. ძირითადად ამონაბეჭდის ავთენტურობის კვლევისას სირთულეს არაოფიციალური დოკუმენტის შემთხვევაში ვაწყდებით, ვინაიდან ოფიციალური დოკუმენტის რეკვიზიტების დახმარებით მისი ნამდვილობის განსაზღვრა ნაკლებ ძალისხმევას მოითხოვს, ხოლო ამონაბეჭდს, რომელსაც არ გააჩნია დამახასიათებელი ნიშნები და მხარე მას სასამართლოში წარადგენს, მისი უტყუარობისა და დე-

[91] *Casey E.*, Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 3.

დანთან შესაბამისობის წარმოსაჩენად შესაძლოა ექსპერტიზის დასკვნის წარდგენაც კი დასჭირდეს, რომელიც სასამართლოს ინფორმაციის წყაროს, შემქმნელი მოწყობილობის გამართულობისა და დედანთან, ელექტრონული ფორმით არსებულ ინფორმაციასთან შესაბამისობას დაუდასტურებს.

საკითხის კომპლექსურობის მიუხედავად, სხვადასხვა ქვეყნის კანონმდებლობისა და სასამართლო პრაქტიკის ანალიზმა ცხადყო, რომ კომპიუტერული მონაცემის ნამდვილობის დასადასტურებლად ტრადიციული მტკიცებულების ავთენტურობის დადგენისთვის გათვალისწინებული ნორმების გამოყენება სავსებით გამართლებულია.

ბიბლიოგრაფია:

1. საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 03/11/2009.
2. „კომპიუტერული დანაშაულის შესახებ“ კონვენცია („ბუდაპეშტის კონვენცია“), 23/11/2001.
3. *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი – ზოგადი ნაწილის მიმოხილვა, თბ., 2014, 225-226.
4. *მეურმიშვილი ბ.,* საქართველოს სისხლის საპროცესო სამართალი, კერძო ნაწილი, *ფაფიაშვილი ლ. (რედ.),* თბ., 2017, 534.
5. *ევროპის საბჭო,* მოსამართლეთა ტრენინგი ქსელურ დანაშაულში, 2010, 35, <https://rm.coe.int/16802fa028> [23.02.2021].
6. *ოთხოზორია ვ., ცირამუა ზ., სვანიშვილი შ.,* ინფორმაციული ტექნოლოგიების მხარდამჭერი სპეციალისტი, თბ., 2015, 8.
7. *ოთხოზორია ვ., ცირამუა ზ.,* ინფორმაციული ტექნოლოგიები, თბ., 2015, 226.
8. *ფაფიაშვილი ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, *გიორგაძე გ. (რედ.),* თბ., 2015, 288.
9. საქართველოს საკონსტიტუციო სასამართლოს 2015 წლის 31 ივლისის გადაწყვეტილება საქმეზე: „საქართველოს მოქალაქე მაია რობაქიძე საქართველოს პარლამენტის წინააღმდეგ“, № 2/2/579, 12.
10. Acts Interpretation Act, 14/01/2019.
11. Canada Evidence Act, 1985.
12. Data Protection Act, 16/07/1998.
13. Evidence Code of California, 18/05/1965.
14. Evidence Act, 23/02/95.
15. Federal Rules of Civil Procedure, 20/12/1937.
16. Federal Rules of Criminal Procedure, 26/12/44.
17. Federal Rules of Evidence (USA), 01/12/2019.
18. Explanatory Report to the Convention on Cybercrime, European Treaty Series – № 185, Budapest, 23.11.2001, 5.
19. Back Up Data, Nonprofit Technology Collaboration, 1, <https://www.baylor.edu/content/services/document.php/192120.pdf> [23.02.2021].
20. *Brenner W. S., Frederiksen A. B.,* Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 1, 2002, 60-63, 80-82.
21. *Capra D.,* Authenticating Digital Evidence*,* Baylor Law Review, № 1, 2017, 3.
22. *Casey E.,* Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 3, 7, 26.
23. *Clancy K. T.,* The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and A Primer, Mississippi Law Journal, Vol. 75, 2005, 193.
24. *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations &

Principles for Addressing Electronic Document Production, 3th ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 207-209, 211, 213.

25. *Gonzales R. A., Schofield B. R., Hagy W. D.*, Investigations Involving the Internet and Computer Networks, National Institute of Justice, USA, 2007, 2.
26. *Gonzales R. A., Schofield B. R., Hagy W. D.*, Investigations Involving the Internet and Computer Networks, National Institute of Justice, USA, 2007, 2.
27. *Goodison E. S., Davis C. R., Jackson A. B.*, Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 3.
28. *Gregory D. J.,* Authentication Rules and Electronic Evidence, The Canadian Bar Review, Vol. 81, № 3, 2001, 531.
29. *Johnson A. M.,* Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability, Marquette Law Review, Vol. 75, Issue 2, 1992, 445.
30. *Kerr S. O.,* Searches and Seizures in a Digital World, Harvard Law Review, Vol. 119, 2006, 1.
31. *Mason S., Weir R. S. G.,* The Sources of Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 1, 4.
32. *Mason S.*, *Stanfield A.,* Authenticating Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 193.
33. *Mukasey B. M., Sedgwick L. J., Hagy W. D.*, Electronic Crime Scene Investigation: A Guide for First Responders, National Institute of Justice, USA, 2008, 9.
34. *Outerbridge D., Siller E.,* The Admissibility of Electronic Evidence, 2015, 11, <https://www.lawinsider.com/documents/1tYTXnzcs2u> [23.02.2021].
35. *Riley J.,* Understanding Metadata, National Information Standards Organization, Baltimore, MD, 2017, 1.
36. *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 18, 20-21, 26-28.
37. Scientific Working Group on Digital Evidence (SWDGE), SWGDE Digital and Multimedia Evidence Glossary, 2016, 7, <https://www.swgde.org/documents/published> [20.02.2021].
38. *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 61, 64-65.
39. *AMP v. Persons Unknown,* [2011] EWHC 3454 (TCC).
40. *R. v. Nichols,* (2004), CarswellOnt 8225, (Ont. C.J.).
41. *R. v. Morgan,* (2002), N.J., № 15, (NLPC).
42. <https://thesedonaconference.org/> [20.02.21].