ირაკლი მინაშვილი

ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა

თბილისი 2019

მთავარი რედაქტორი: ირაკლი გაბისონია

რედაქტორები: ჯემალ გაბელია
თეიმურაზ დარსანია

რეცენზენტები: ჯემალ გახოკიძე
შოთა რიჟამაძე

ტექნიკური
რედაქტორი: ელენე ჩალაძე

ტექნიკური
უზრუნველყოფა: თამარ ბარამია

გამომცემლობა „მერიდიანი“,
თბილისი, ალ. ყაზბეგის გამზ., №47.
☎ 239-15-22
E-mail: meridiani777@gmail.com

ISBN 978-9941-25-700-1

ნაშრომი **„ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა“ სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის სამეცნიერო–კვლევითი პროექტის „მტკიცების (მტკიცებულებათა შეგროვების, საპროცესო დამაგრების შემოწმებისა და შეფასების) აქტუალური პრობლემების“ ფარგლებში მომზადდა.**

საქართველოს ტექნიკური უნივერსიტეტის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტი აქტიურად ცდილობს, რომ ხელი შეუწყოს სხვადასხვა დარგების ახალი მიმართულებების შექმნას და განვითარებას, სწორედ ამ მიზანს ემსახურება ფაკულტეტზე მიმდინარე სხვადასხვა სამეცნიერო–კვლევითი პროექტები.

აღსანიშნავია, რომ ნაშრომი არის ინოვაციური, ვინაიდან წარმოდგენილია ორი — იურიდიული და კომპიუტერული მეცნიერებების მოკლე ანალიზი და აღნიშნული დარგების პრაქტიკული ცოდნის მოცულობითი განხილვა. იგი უდავოდ პასუხობს დროის მოთხოვნებს და მას არამხოლოდ დიდი პრაქტიკული მნიშვნელობა აქვს არამედ სავსებით შესაძლებელია სახელმძღვანელოდ იქნეს გამოყენებული საერთაშორისო და ეროვნული უსაფრთხოების, კერძოდ, კიბერტერორიზმისა და ციფრულ დანაშაულთან დაკავშირებული სასწავლო პროგრამების განხილვისა და შედგენისათვის.

ნაშრომი რეკომენდირებულია სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის ბაკალავრების, მაგისტრებისა და დოქტორანტებისათვის. მისი გამოყენება ასევე სასარგებლო იქნება ოპერატიული და საგამოძიებო–სამსახურის მუშაკებისათვის, რომლებიც იძიებენ ციფრული დანაშაულს.

სარჩევი

შესავალი

ნაშრომი „ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა“ არის არასტანდარტული სტილის, ვინაიდან თქვენს წინაშე წარმოდგენილია ორი სხვადასხვა დარგის – სამართალის და კომპიუტერული მეცნიერების ერთობლივი ნაზავი, რომლებიც ქმნიან ერთ მნიშვნელოვან მიმართულებას–ციფრული დანაშაულის გამოძიების მეთოდიკას.

ნაშრომის პირველ ნაწილში წარმოდგენილი არის თეორიული საკითხები – რომლებიც შეეხება ციფრული დანაშაულის ცნების და არსის განმარტებას. აღსანიშნავია ისიც, რომ „ციფრული დანაშაული“ ქართულ კანონმდებლობაში როგორც დანაშაულის ცალკე ცნება არ გვხვდება, მაგრამ იმ შემთხვევაში, როდესაც დანაშაული ჩადენილია ციფრული საგნის საშუალებით სახეზეა სწორედ ციფრული დანაშაული.

ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკაში, თქვენ ვერ ნახავთ სხვადასხვა სახის ნიმუშების აღებას, ვერ ნახავთ სტანდარტულ ექსპერტიზებს, სამაგიეროდ წარმოდგენილი იქნება კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა, კომპიუტერული პროგრამები და მათთან მუშაობის სპეციფიკა, რომელიც აუცილებელია იმ გამომძიებლებისათვის, ვინც იძიებს მსგავსი ტიპის დანაშაულს.

რაც შეეხება ნაშრომის მეთოდოლოგიას, იგი ახლოს არის არსებულ პრაქტიკასთან და თანხვედრაშია ამ მიმართულებით არსებულ თეორიულ კვლევებთან.

ნაშრომში შეხვდებით სააპელაციო და საკონსტიტუციო სასამართლოს გადაწყვეტილებებს და მათ ანალიზს, ვინაიდან საკითხს – რომელიც თეორიულად რეგულირებული არ არის – სამართლებრივ ჭრილში არეგულირებს სწორედ სააპელაციო სასამართლოს განჩინებები თუ საკონსტიტუციო სასამართლოს გადაწყვეტილებები.

არასტანდარტულია თავად ნაშრომის სტრუქტურა, რაც გამოწვეულია იმით, რომ არის ფოტოილუსტრაცია, რაც გაცილებით ამარტივებს და თვალსაჩინოს ხდის საგამოძიებო მოქმედებების წარმოებას. ასევე, მნიშვნელოვანია სამართლებრივი ტერმინოლოგიის განმარტება, რაც ეხება ციფრულ დანაშაულებს, რის შემდეგაც წარმოდგენილი არის საერთაშორისო, ევროპის, აშშ–ს და რუსეთის პრაქტიკული გამოცდილება ციფრულ დანაშაულთან ბრძოლის კუთხით.

ასევე დამუშავებულია ქართულ სისხლის სამართალში არსებული მუხლები და მათი შესაბამისობა საერთაშორისო დანაშაულის კლასიფიკაციასთან, განხილულია დანაშაულის გამოძიების მეთოდიკა; კომპიუტერის ამოღების სამართლებრივი და ტექნიკური პროცედურები, კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვის სამართლებრივი და ტექნიკური პროცედურები და კომპიუტერული სისტემის დათვალიერების სამართლებრივი ტექნიკური პროცედურები. ასევე მნიშვნელოვანი ადგილი უჭირავს IP მისამართის დადგენას და ექსპერტიზის დანიშვნის თავისებურებებს. ნაშრომის ბოლოს კი წარმოდგენილია ის მნიშვნელოვანი კომპიუტერის კლავიშთა კომბინაციები, რომლებიც აუცილებელია იცოდეს თითოეული საგამოძიებო მოქმედების ჩამტარებელმა.

აქვე გვინდა აღვნიშნოთ, რომ ამ კუთხით მუშაობა გრძელდება, მომავალში შემოგთავაზებთ ნაშრომის მეორე ნაწილს, სადაც საუბარი იქნება პლასტიკური ბარათების საშუალებით და ციფრული ხელმოწერის გამოყენებით ჩადენილი დანაშაულების გამოძიების მეთოდიკაზე და ფარული საგამოძიებო მოქმედებების შედეგად მოპოვებულ აუდიო–ვიდეო მასალაზე–როგორც ციფრულ მტკიცებულებებზე.

ავტორი

გამომცემლობის მიერ, ავტორისა და რედაქტორებისათვის შემოთავაზებული იქნა სქოლიოს შედგენა თანამედროვე QR კოდური ფუნქციით, რაც გულისხმობს იმას, რომ სქოლიოში მითითებული ყველა ელექტრონული გვერდი მასზე განთავსებული შესაბამისი ინფორმაციით, სქოლიოში აღრიცხული იქნება QR კოდის საშუალებით.

ავტორის მიერ მიწოდებული სქოლიოში ასახული ტექსტობრივი ინფორმაციის თანხვედრაზე სქოლიოში მითითებულ QR კოდებთან, პასუხისმგებლობას იღებს გამომცემლობა.

QR კოდი „Quick Response" — „სწრაფი პასუხი" არის ორგანზომილებიანი კოდი, რომელიც შეიქმნა იაპონიაში 1994 წელს, კოდი ინახავს დაშიფრულ მონაცემებს/ინფორმაციას ამა თუ იმ პროდუქტის შესახებ. QR კოდი შეიძლება შეიცავდეს ტექსტებს, ვებ-გვერდის მისამართს, SMS ან E-mail შეტყობინებასა და სხვადასხვა სახის ინფორმაციას. QR კოდის საშუალებით ინფორმაციის გაცვლის მრავალი გზა არსებობს, თუმცა მსოფლიოში ყველაზე პოპულარულია Mobile Tagging-ი, მობილური ტელეფონის საშუალებით კომპიუტერის მონიტორიდან ან ნაბეჭდი მასალიდან QR კოდის სწრაფი წაკითხვა და მასში შენახული ინფორმაციის მყისიერი მიღება. QR კოდის სკანერი (სპეციალური პროგრამა) ავტომატურად ამოიცნობს დაშიფრულ ინფორმაციას ნებისმიერ ბრაუზერში ან ფურცელზე.[1]

როდესაც ნაშრომის სქოლიოში იხილავთ QR კოდს, შეგიძლიათ შესაბამისი მოწყობილობის კამერით დააფიქსიროთ ის და მალევე ავტომატურად გაგიხსნით შესაბამის ვებ-გვერდს.

QR კოდის წამკითხველი პროგრამები;

ინტერნეტის საძიებო სისტემაში აკრიბეთ QR Scanner ან QR Reader, კომპიუტერი მოგცემთ რამდენიმე შესაბამის ვერსიას, საიდანაც შეგიძლიათ აირჩიოთ და გადმოწეროთ თქვენთვის მისაღები ნებისმიერი პროგრამა, რომლის გააქტიურების შემდეგაც პროგრამა დაიწყებს ფუნქციონირებას.

მაგალითად;

ანდროიდის სისტემის მქონე ტელეფონებში და სმარტფონებში შესაბამისი პროგრამის გადმოსაწერად ეწვიეთ ვებ-გვერდს – https://play.google.com/store/search?q=qr სადაც არის არჩევანი შესაბამისი QR პროგრამების.

ანდროიდის სისტემის მქონე ტელეფონებში და სმარტფონებში შესაბამისი პროგრამის გადმოსაწერად შედით ფუქციონალში – Play Market სადაც ძებნა ფუნქციონალში აკრიბეთ QR Scanner ან QR Reader, ჩემოთვლილი პროგრამებიდან აირჩიეთ გადმოწერეთ თქვენთვის მისაღები პროგრამა.

iPhone, iPad, or iPod – ში შესაბამისი პროგრამის გადმოსაწერად ეწვიეთ ვებ-გვერდს – https://apps.apple.com/us/app/qr-reader-for-iphone/id368494609 და გადმოწერეთ პროგრამა.

iPhone, iPad, or iPod – ში შესაბამისი პროგრამის გადმოსაწერად შედით ფუქციონალში – App Store სადაც ძებნა ფუნქციონალში აკრიბეთ QR Scanner ან QR Reader და ჩემოთვლილი პროგრამებიდან გადმოწერეთ თქვენთვის მისაღები პროგრამა.

1 ელ. გვერდი. https://biblioni.wordpress.com/2012/10/24/qr/ ნანახია 06.09.2019

კარი I

ციფრული დანაშაულის ცნება, არსი და კლასიფიკაცია

თავი I
ციფრული დანაშაული

1. 1.1. ციფრული დანაშაულის ცნება და არსი

მსოფლიოს მასშტაბით დღითი-დღე ვითარდება კომპიუტერული მოწყობილობები და უფრო სრულყოფილი და მრავალფუნქციური ხდება კომპიუტერული სისტემები, ხოლო მთავარი საგანი, რის საფუზველზეც ყოველივე აღნიშნულის სწრაფი განვითარება ხდება არის შესაბამისი ციფრული პროგრამები.

დღეის მდგომარეობით მსოფლიოში და მათ შორის საქართველოშიც გვაქვს სამართლებრივი ცნებები „კიბერდანაშაული", „კომპიუტერული დანაშაული" და ასე შემდეგ, მაგრამ როდესაც უკვე გამოძიება იწყება, პრაქტიკაში საქმე გვაქვს სხვა რეალობასთან, გამოძიება ეძებს არა კომპიუტერულ მოწყობილობას — როგორც მტკიცებულებას, არამედ კომპიუტერულ სისტემაში დაცულ ინფორმაციას, რომელიც თანამედროვეობაში არის ციფრული ბუნების.

ამდენად, გამომძიებელი იძიებს ციფრულ და არა კომპიუტერულ დანაშაულს, მაგალითისათვის შესაძლოა მოვიყვანოთ შემთხვევა, როდესაც დამნაშავე ციფრული ვიდეოკამერის გამოყენებით გადაიღებს პიროვნების პირადი ცხოვრების ამსახველ ჩანაწერს, შემდგომ გადაიწერს მას მობილურ ტელეფონში და შესაბამისი დანაშაულებრივი განზრახვით და მიზნით ავრცელებს სოციალური ქსელის საშუალებით, ასეთ შემთხვევაში სახეზეა საქართველოს სისხლის სამართლის კოდექსით გათვალისწინებული (შემდგომში სსკ) დანაშაული, მაგრამ – რა არის დანაშაულის საგანი – ვიდეოკამერა – ? მობილური ტელეფონი – ? თუ სოციალური ქსელი – ? დანაშაულის საგნის ბუნებიდან გამომდინარე აშკარაა, რომ არცერთი ზემოაღნიშნული, აღნიშნულ და მსგავს შემთხვევებში დანაშაულის საგანი არის გადაღებული ვიდეოჩანაწერი, მაგრამ რა სახის ინფორმაციაა აღნიშნული ჩანაწერი? – ეს არის ციფრული ინფორმაცია, ხოლო რაც შეეხება ვიდეოკამერას და შემდგომ მობილურ ტელეფონს – აღნიშნული ნივთები გვევლინებიან დანაშაულის ხერხად და საშუალებად.

წარმოდგენილი ნაშრომის შექმნა, განაპირობა სწორედ სისხლის სამართლის პროცესის წარმოების ეტაპზე — ციფრული დანაშაულის გამოძიებისას თეორიული და პრაქტიკული ცოდნის არათანმიმდევრულობამ და პრაქტიკაში არსებულმა იმ პრობლემებმა, რომელთა რეგულირების მიზნითაც სააპელაციო სასამართლო აკეთებს განმარტებებს და აღნიშნული განმარტებები არაპრეცედენტული სამართლის სისტემის ქვეყნის – საქართველოს სისხლის სამართალში, ხდება პრეცედენტული ხასიათის მატარებელი იმიტომ, რომ ცალკე დანაშაულად არ გვაქვს ციფრული დანაშაული და არ არსებობს აღნიშნულის თუნდაც ნაშრომის დონეზე წარმოდგენილი განმარტება.

როდესაც ვმსჯელობთ ციფრულ დანაშაულზე, უპირველეს ყოვლისა აღსანიშნავია, რომ ციფრული დანაშაულის მთავარ ბირთვს წარმოადგენს ციფრული საგანი, რადგან მის შემთხვევაში, მონაცემთა კომპიუტერული სისტემების და კომპიუტერული მოწყობილობების საშუალებით დამუშავება, არსებითი მნიშვნელობის მქონეა, მიუხედავად იმისა, რომ ბევრ დანაშაულს შემადგენლობაში სიტყვა ციფრული არ უწერია, ხშირად არის ხოლმე შემთხვევები – როდესაც დანაშაულები, ელექტრონული გზით ჩადენის შემთხვევაში ანაცვლებენ ტრადიციული დანაშაულის

შემადგენლობებს, მაგალითად ქურდობა – როდესაც იგი ჩადენილია ციფრული საგნის გამოყენებით – გადადის ციფრულ დანაშულში.

ციფრული დანაშაულის ობიექტზე მსჯელობისას დავეთანხმებით ალ. კაცმანს, იმ კონტექსტში, რომ ვინაიდან ინფორმაციის არამართლზომიერი გამოყენების შედეგი სხვადასხვაგვარია, მან შეიძლება დაარღვიოს, როგორც ინტელექტუალური საკუთრების ხელშეუხებლობა, ასევე გამოიწვიოს მოქალაქეთა პირადი ცხოვრების შესახებ ცნობების გახმაურება, ქონებრივი ზიანი, რეპუტაციის შელახვა, წარმოების, დარგის ნორმალური საქმიანობის დარღვევა და სხვა.

რაც შეეხება აღნიშნული დანაშაულის გვარეობით ობიექტს; მასში უნდა მოვიაზროთ სისხლის სამართლის კანონით დაცული ის ერთგვაროვანი ან იგივეობითი საზოგადოებრივი ურთიერთობები, რომელთა წინააღმდეგაც მიმართულია დანაშაულებრივი ხელყოფა[1], აქვე გასათვალისწინებელია, რომ მიუხედავად იმისა, რომ ქართულ კანონმდებლობაში არ გვაქვს ციფრული დანაშაულის ცნება, ვხვდებით კომპიუტერულ დანაშაულებს, შესაბამისად გარკვეული პარალელის გავლება მის შემადგენლობასთან შესაძლებელია, მაგრამ არა ზედმიწევნით ანალოგიური პარალელის, მაგალითისათვის – სისხლის სამართლის კოდექსში 35–ე თავი რომელიც ეხება კიბერდანაშაულს, მოცული აქვს სისხლის სამართლის კოდექსის მე–9 კარს რომლის სათაურიც არის „დანაშაული საზოგადოებრივი უშიშროებისა და წესრიგის წინააღმდეგ“, შესაბამისად კიბერდანაშაულის გვარეობითი ობიექტი იმპერატიულად არის საზოგადოებრივი უშიშროება და წესრიგი, მაგრამ ციფრული დანაშაულის შემთხვევებს შესაძლოა შევხვდეთ სხვადასხვა კარში, მაგალითად – როდესაც საავტორო უფლების დარღვევით ხდება ინტერნეტიდან სხვადასხვა ინფორმაციის გადმოწერა. ვინაიდან საქართველოს სისხლის სამართლის კოდექსში კომპიუტერის საშუალებით საავტორო უფლების დარღვევის სპეციალური მუხლი არ არის გათვალისწინებული, პირის ქმედება კვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284–ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 189–ე (საავტორო, მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა) მუხლებით – ასეთ შემთხვევაში ქმედების გვარეობით ობიექტად ვერ იქნება მოაზრებული მხოლოდ საზოგადოებრივი უშიშროება და წესრიგი, ვინაიდან საკუთრების წინააღმდეგ მიმართული დანაშაულის გვარეობით ობიექტს წარმოადგენს საკუთრების ურთიერთობა მთლიანად, ამ შემთხვევაში უკვე გადავდივართ ძირითად და დამატებით ობიექტიან დანაშაულზე და სახეზე იქნება სამართლებრივი სიკეთე საკუთრების სახით და საზოგადოებრივი უშიშროების და წესრიგის სახით.

რაც შეეხება სახეობითი ობიექტის განსაზღვრას, აღნიშნულის კონკრეტიზაცია ციფრული დანაშაულის კონტექსტში ამ მოცემულობის სისხლის სამართლის კოდექსის საფუძველზე შეუძლებელია, მაგრამ უნდა აღინიშნოს, რომ უმეტესწილად სახეზე გვექნება ორ ან მეტ ობიექტიანი დანაშაულები.

ციფრული დანაშაული, უნდა მივაკუთვნოთ დანაშაულთა იმ ჯგუფს, რომელშიც ყოველთვის არსებობს დანაშაულის საგანი, ამგვარი დანაშაული გამოხატულებას პოულობს არამატერიალური სამყაროს საგანზე – ანუ ციფრულ საგანზე მართლსაწინააღმდეგო ზემოქმედების შედეგად, უფრო კონკრეტულად რომ განვიხილოთ, ციფრული დანაშაულის საგანი არის ციფრული ინფორმაცია; რომლის დამუშავებაც ხდება ციფრული სისტემის საშუალებით, რომელიც „[...] არის ციფრული ფორმით (კოდებით) წარმოდგენილი ინფორმაციის დამუშავების სისტემა. ინფორმაციის ციფრული ფორმით წარმოდგენა ფართოდ გამოიყენება ინფორმაციის დამუშავების სისტემებში, მართვის ავტომატიკის და ავტომატიზებულ სისტემებში, ციფრულ საკომუნიკაციო სისტემებში და ა.შ. ამდენად, ციფრული ფორმით წარმოდგენილი ინფორმაციის გამოყენების არეალი დღეისათვის მეტად ფართოა და ციფრული სისტემების განვითარების თავბრუდამხვევი ტემპების გამო, გამოყენების სფეროების მარტო ჩამოთვლაც კი რთული საქმეა. ციფრული სისტემა, როგორც ნებისმიერი სხვა

[1] თ.წერეთელი, გ. ტყეშელიაძე, “მოძღვრება დანაშაულზე”, თბ. 1969წ. გვ. 150

სისტემა, ხასიათდება სტრუქტურით, იერარქიულობით და ფუნქციით.“ [2]

თავად „ტერმინი «ციფრული სისტემა» (ცს) სამეცნიერო-ტექნიკურ ლიტერატურაში ხშირად გამოიყენება, მაგრამ უმეტეს შემთხვევაში არ მოიცემა მისი ცხადი განმარტება. ხშირად იხმარება «ციფრული სისტემის» სინონიმები: «კომპიუტერული სისტემა», «ციფრული ელექტრონიკა» და სხვა.“[3]

„ციფრული სისტემის სტრუქტურა არის მისი ელემენტების და მათ შორის კავშირების სივრცეში და დროში მყარი მოწესრიგებულობა. ციფრული სისტემებისათვის დამახასიათებელია სხვადასხვა ელემენტების და მათ შორის კავშირების არსებობა, რაც განაპირობებს ციფრული სისტემების სხვადასხვა სტრუქტურებს. ამრიგად, ელემენტების ქვესისტემებში შესვლის წესი, ხოლო შემდგომ ქვესისტემების თანმიმდევრობითი გაერთიანება ერთიან სისტემაში წარმოქმნის სისტემის დანაწევრების სტრუქტურას. აქედან გამომდინარე ასეთი სტრუქტურა მუდამ იერარქიულია და გააჩნია არანაკლებ ორი დონისა: მაღალი დონე — სისტემა და დაბალი დონე — ელემენტი“.[4]

„ციფრული სისტემების ანალიზის შედეგად შეიძლება გამოვყოთ მათი აგების იერაარქიის შემდეგი დონეები:

- სისტემა;
- ფუნქციონალური ქვესისტემა;
- ბლოკი (პროცესორი, მეხსიერების ბლოკი და ა.შ.);
- კვანძი (ციფრული კვანძები, აგებული ლოგიკურ ელემენტებზე);
- ელემენტი (ტრივიალური ლოგიკური ელემენტები).“[5]

მაგალითისა და თვალსაჩინოებისათვის განვმარტოთ;

- **ტექსტური ინფორმაცია;**
- **გრაფიკული ინფორმაცია;**
- **ბგერითი ინფორმაცია;**

„ტექსტური ინფორმაცია; წარმოადგენს ანბანური სიმბოლოების ერთობლიობას. თუ თითოეულ ანბანურ სიმბოლოს რიცხვით კოდს შეუსაბამებთ, მაშინ მივიღებთ ტექსტის რიცხვების საშუალებით გამოსახვის შესაძლებლობას, მაგალითად“:[6]

[7]

---

[2] ლევან იმნაიშვილი, ციფრული სისტემების სინთეზის პრინციპების დამუშავება მრავალფუნქციურობის ბაზაზე. დისერტაცია, სამეცნიერო კონსულტანტი ბ-ნი არჩილ ფრანგიშვილი. 2006 წელი. გვ.17.

[3] იქვე. გვ.3-4

[4] ლევან იმნაიშვილი, ციფრული სისტემების სინთეზის პრინციპების დამუშავება მრავალფუნქციურობის ბაზაზე. დისერტაცია, სამეცნიერო კონსულტანტი ბ-ნი არჩილ ფრანგიშვილი. 2006 წელი. გვ.17.

[5] იქვე. გვ.17.

[6] ვ.ჩხაიძე. ი.სალუქვაძე. ინფორმაციული ტექნოლოგიები ბგეოგრაფიაში. 2016 გვ..7

[7] იქვე.

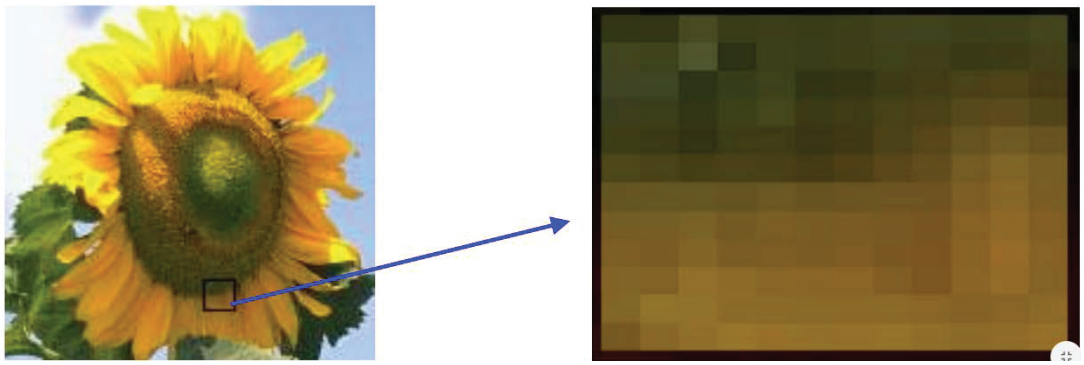
სიტყვა“ინფორმაცია”ციფრულად შემდეგნაირად შეიძლება გამოისახოს შემდეგნაირად:

[8]

ი ნ ფ ო რ მ ა ც ი ა
0231-0235-0243-0236-0239-0234-0224-0249-0231-0224.

„გრაფიკული ინფორმაციის წარმოდგენის შემთხვევაში გამოსახულება პირობითად “იშლება” წერტილოვან ელემენტებად. ბუნებრივია რომ რაც უფრო მეტია წერტილების რაოდენობა, ანუ მცირეა ელემენტარული წერტილის ზომა, მით უფრო ხარისხიანია ციფრული გამოსახულება. თითოეული წერტილი აღიწერება მისი ეკრანზე მდებარეობის კოორდინატთა წყვილით (რიცხვებით) და ფერის კოდით. ამ რიცხვების ერთობლიობა ქმნის ე.წ. რასტრს, რომელიც შეიძლება ასე გამოიყურებოდეს: „[9]

[10]



„ბგერითი ინფორმაციის წარმოდგენისათვის ხმოვანი სიგნალი ანალოგიურად იშლება ერთეულოვან ელემენტებად (მაგ. ნოტებად ან სიხშირეებად) და თითოეულ გამოყოფილ ერთეულს მიენიჭება შესაბამისი რიცხვითი კოდი“.[11]

„გრაფიკულ გამოსახულებათა ერთობლიობა შეიძლება წარმოდგენილ იქნას თანმიმდერული რასტრების მეშვეობით და აღწერილ იქნას როგორც ე.წ. ნაკადი. გამოსახულებათა ნაკადური ცვლილება ქმნის მოძრაობის ეფექტს.[12]

„გრაფიკული და ბგერითი (ხმოვანი) ინფორმაციის გაერთიანებას ნაკადში კიდევ მულტი-მედიურსაც უწოდებენ. მონაცემთა თითოეულ სტრუქტურულ ჯგუფს გააჩნია კლასიფიცირების მახასიათებლები (კრიტერიუმები)“ [13]

ციფრული დანაშაულის საგანი არ შეიძლება იყოს არაციფრული ინფორმაციის მატარებელი ნივთი, მაგალითად; დავუშვათ დანაშაულის ჩამდენმა პირმა დააზიანი კომპიუტერული მოწყობი-ლობის ეკრანი, იმ მიზნით, რომ კომპიუტერში ინახება მისთვის არასასურველი ინფორმაცია — ზიანი

---

[8] ვ. ჩხაიძე. ი.სალუქვაძე. ინფორმაციული ტექნოლოგიები ბგეოგრაფიაში. 2016 გვ.გვ.7

[9] ვ. ჩხაიძე. ი.სალუქვაძე. ინფორმაციული ტექნოლოგიები ბგეოგრაფიაში. 2016 გვ.გვ. 7

[10] იქვე.

[11] იქვე.

[12] იქვე.

[13] ვ. ჩხაიძე. ი.სალუქვაძე. ინფორმაციული ტექნოლოგიები ბგეოგრაფიაში. 2016 გვ.გვ.7

განისაზღვრა 200 ლარით, ასეთ შემთხვევაში, მიუხედავად იმისა, რომ დანაშაულის საგანი – სახეზეა კომპიუტერული მოწყობილობის ეკრანი, ბუნებრივია სახეზე ვერ იქნება ციფრული დანაშაული, რადგან დანაშაულის საგანს არ წარმოადგენს ციფრული ინფორმაცია, მაგრამ იმ შემთხვევაში თუ დამნაშავემ გამოიყენა სხვა პირის პლასტიკური ბარათი და ე.წ. ბანკომატიდან განახორციელა აღნიშნული ბარათის გამოყენებით ფულადი ტრანზაქცია – სახეზე გვექნება ციფრული დანაშაული ვინაიდან, კი მართალია გამოყენებული საგანი ერთი შეხედვით არის მატერიალური ნივთი – პლასტიკური ბარათი, მაგრამ დანაშაულის ჩასადენად გამოყენებულ იქნა არა თავად ბარათი, არამედ მასზე არსებული ციფრული ინფორმაცია შესაბამისი პიროვნების საბანკო რეკვიზიტების და პარამეტრების შესახებ.

ზემოაღნიშნულიდან გამომდინარე, ნივთი – როგორც ციფრული დანაშაულის ჩადენის საგანი, შესაძლოა მოვიაზროთ მხოლოდ იმ შემთხვევაში, თუ აღნიშნულ ნივთში დაცულია ციფრული ინფორმაცია, რომელიც გამოყენებულ იქნა დანაშაულის ჩასადენად.

რაც შეეხება ციფრული დანაშაულის ობიექტურ მხარეს, პირველ რიგში ხასიათდება მართლ-საწინააღმდეგო მოქმედებით. მაგალითად; მოქმედებით ჩადენილ ციფრულ დანაშაულად შე-საძლოა მოვიაზროთ, შესაბამისი მართლსაწინაარმდეგო მოტივით, მიზნით და განზრახვით, ციფრული საგნის გამოყენებით ჩადენილი;

- კიბერტერორიზმი;
- ჰაკერობა;
- კიბერ ქურდობა:
- იდენტიფიკაციის ქურდობა:
- ვირუსული პროგრამები:
- კიბერ გადაკიდება:
- ბავშვთა დაყოლიება;
- პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების ხელყოფა;
- პირადი ცხოვრების საიდუმლოს ხელყოფა;
- კერძო კომუნიკაციის საიდუმლოების დარღვევა;
- პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა;
- და სხვა.

როგორც უკვე აღინიშნა, თითოეულ დანაშაულს შესაძლოა ჰქონდეს ინდივიდუალური შემადგენლობის ნიშნები, მაგრამ როდესაც ვსაუბრობთ ციფრულ დანაშაულზე აუცილებელია განისაზღვროს, რომ ყველა აღნიშნული დანაშაულის ჩადენის ხერხი/საშუალება არის – კომპიუტერული სისტემა, ხოლო დანაშაულის საგანი – კომპიუტერული სისტემის გამოყენებით შექმნილი ციფრული ინფორმაცია – ტექსტური ინფორმაცია (მაგ. დოკუმენტი), გრაფიკული ინფორმაცია (მაგ. ფოტო, ვიდეო), ბგერითი ინფორმაცია (მაგ. აუდიოჩანაწერი, მუსიკა), ტექსტურ – გრაფიკული ინფორმაცია (მაგ. ელექტრონული ფული), გრაფიკულ–ბგერითი ინფორმაცია და ასე შემდეგ. ასევე კომპიუტერულ მოწყობილობაში ან მის გარეთ – შესაბამის ელექტრონულ მეხსიერების მოწყობილობაში დაცული ციფრული მასალა – მაგ (ID ბარათზე, პლასტიკურ ბარათზე, სიმ ბარათზე) და ა.შ.

განვიხილოთ ციფრული დანაშაულის ჩადენის ხერხი/საშუალება, რომელიც რათქმაუნდა არის კომპიუტერული სისტემა, იმიტომ, რომ ციფრული მასალის შექმნა ხდება კომპიუტერული სისტემის საშუალებით, კერძოდ;

„კლასიკური სტრუქტურის მიხედვით აგებული მანქანა მუშაობს შემდეგნაირად. მანქანის ავტომატური მუშაობის დაწყებემდე მართვის პულტიდან გაიცემა ბრძანებები, რომელთა მიხედვითაც გარე მოწყობილობებიდან ხდება მანქანის მახსოვრობაში კონკრეტული ამოცანის შესრულებისათვის საჭირო მონაცემების და შესასრულებელი პროგრამის ჩატვირთვა. შემდეგ მართვის პულტიდან ოპერატორი ჩაწერს მართვის მოწყობილობის ბრძანების მისამართის რეგისტრში იმ უჯრედის მისამართს, რომელშიც ინახება პროგრამის პირველი ბრძანება. ამის შემდეგ ხდება მართვის მოწყობილობის ჩართვა. მართვის მოწყობილობიდან მახსოვრობის მოწყობილობაში იგზავნება მმართველი სიგნალი, რომლის საშუალებითაც ხდება მახსოვრობის მოწყობილობაში მითითებული უჯრედის წაკითხვა და მისი შგთავსი გადაიწერება მართვის მოწყობილობის რეგისტრში. ეს ინფორმაცია წარმოადგენს ბრძანებას — ინსტრუქციას. ხდება ინსტრუქციის გაშიფვრა და შესაბამისი მმართველი სიგნალების გამომუშავება მახსოვრობის მოწყობილობისათვის, რის საფუძველზეც ხდება ოპერანდების წაკითხვა და არითმეტიკულ მოწყობილობაში გადაწერა. მმართველი სიგნალები გაიცემა აგრეთვე არითმეტიკული მოწყობილობისთვისაც, რათა მან შეასრულოს ინსტრუქციით (ბრძანებით) მოთხოვნილი ოპერაცია. ამის შენდეგ მმართველი სიგნალების მიხედვით უნდა მოხდეს შედეგის არითმეტიკული მოწყობილობიდან მითითებული მისამართით მახსოვრობის მოწყობილობაში გადაწერა. ამასთანავე, მმართველ მოწყობილობაში ბრძანების მისამართის რეგისტრში უნდა მოხდეს ახალი ბრძანების მისამართის ფორმირება. ეს შეიძლება მოხდეს რეგისტრის შიგთავსისათვის ერთის დამატებით.“[14]

„პირველი ბრძანების შესრულების შემდეგ მართვის მოწყობილობა გასცემს ახალ სიგნალს შემდეგი ბრძანების წასაკითხად და ანალოგიურად იწყებს ახალი ბრძანების შესრულებას. ზოგიერთი ბრძანების კოდი, რომელიც მითითებულია ინცტრუქციაში, შეიძლება აღნიშნავდეს არა არითმეტიკულ ოპერაციას, არამედ ოპერაციას თვით მართვის მოწყობილობისათვის.“[15]

„კიდევ ერთხელ გავუსვათ ხაზი კომპიუტერის აგების კლასიკურ სტრუქტურაში ჩადებულ ორ ფუნდამენტურ იდეს, რომლებმაც დიდად შეუწყო ხელი გამოთვლითი ტექნიკის განვითარებას [...].“[16]

„პირველი, კომპიუტერში პროგრამები და საწყისი მონაცემები შეიტანება ერთი და იგივე გარე მოწყობილობებიდან და ინახება ერთი და იგივე დამხსომებელ მოწყობილობაში. ეს უზრუნველყოფს კომპიუტერის ოპერატიულ გადასვლას ერთი ამოცანიდან მეორეზე და აქცევს მას უნივერსალურ გამომთვლელ მოწყობილობად.“[17]

„მეორე, ინსტრუქციები, რომლებიც ქმნის პროგრამებს, კოდირებულია რიცხვების მსგავსად. ეს საშუალებას იძლევა პროგრამების შესრულების დროს ინსტრუქციებიც გადაგზავნილ იქნას არითმეტიკულ მოწყობილობაში მათზე გარკვეული მოქმედებების ჩასატარებლად და შემდეგ დაბრუნებული იქნას დამხსომებელ მოწყობილობაში. ამრიგად, პროგრამის შესრულებასთან ერთად შეიძლება მისი გარდაქმნაც ან ახალი პროგრამის შექმნაც.“[18]

რაც შეეხება ციფრული ტექნოლოგიებით რაიმე სახის დანაშაულის ჩადენას უპირველეს ყოვლისა უნდა დავადგინოთ და გამოვიძიოთ ვინ შეიძლება შექნას, დაამზადოს და შემდგომ გამოიყენოს ციფრული ტექნოლოგიები დანაშაულის ჩასადენად.

---

14 თეიმურაზ კივილაძე, ინფორმატიკის ისტორია. 2018. გვ. 24.

15 იქვე.

16 იქვე.

17 იქვე.

18 იქვე.

ქმედების სუბიექტი შესაძლოა იყოს; ნებისმიერ ფიზიკური პირი, იურიდიული პირი და სახელმწიფო.

„კომპიუტერული დანაშაულის შესახებ“ კონვენციის თანახმად (ბუდაპეშტი 23.11.2001) მომსახურების მიმწოდებელი არის; „ნებისმიერი საჯარო ან კერძო პირი, რომელიც მისი სერვისის მომხმარებლებს უზრუნველყოფს კომპიუტერული სისტემის საშუალებით ურთიერთობის შესაძლებლობით, და ნებისმიერი სხვა პირი, რომელიც გადაამუშავებს ან ინახავს კომპიუტერულ მონაცემებს ამგვარი საკომუნიკაციო მომსახურების ან ამგვარი მომსახურების მომხმარებელთა სახელით.“

სუბიექტზე მსჯელობისას გამოვყოთ რამდენიმე სპეციალური სუბიექტი და ასევე სუბიექტები, რომლებსაც გააჩნიათ სპეციპიური მახასიათებლები;

სპეციალური სუბიექტად შესაძლოა შეგვხვდეს;

„სახელმწიფო – უცხოეთის ქვეყნების სადაზვერვო სამსახურები კომპიუტერულ ტექნოლოგიებს იყენებენ ინფორმაციის შეგროვებისა და ჯაშუშობისთვის. მსგავსი ქმედებები სადაზვერვო სამსახურების მხრიდან შეიძლება მიმართული იყოს როგორც მეგობარი, ისე მოწინააღმდეგე ქვეყნების მიმართ, ან არასახელმწიფო სუბიექტების წინააღმდეგ. სახელმწიფო თავისი სადაზვერვო სამსახურების გამოყენებით, ახორციელებს კიბერშეტევებს პოტენციური მოწინააღმდეგე სახელმწიფოების მიმართ დეზინფორმაციის, დესტაბილიზაციის, დაშინების ან ფართომასშტაბიანი კიბერომის წარმოების მიზნით. ასევე საყურადღებოა ის გარემოება, რომ ხშირად ხდება პიროვნების უსაფრთხოებისა და უფლებების დარღვევა. კერძოდ, სახელმწიფოს სპეციალურმა სამსახურებმა შეიძლება მიმართონ ისეთ ქმედებებს, რომელთა გამოყენებითაც ხდება მოქალაქეთა პერსონალური მონაცემების გადაჭერა, მოპარვა და გამოყენება. მსგავსი ქმედებები ხშირ შემთხვევაში ხდება სასამართლოს შესაბამისი ორგანოების სანქციისა და სწორი დემოკრატიული კონტროლის გარეშე.“ [19]

„კორპორაციები, კომპანიები — დაკავებულნი არიან სამრეწველო/კორპორაციული ჯაშუშობითა და/ან დივერსიული საქმიანობით, რაშიც ისინი ხშირად იყენებენ ჰაკერებსა და ორგანიზებულ დამნაშავეთა ჯგუფებს. კომპანიების, კორპორაციებისა და კერძო სექტორის სხვა წარმომადგენლებს ასევე შეუძლიათ დაარღვიონ ადამიანის უფლებები პიროვნების პერსონალური მონაცემების შეგროვებისა და ანალიზის გზით, ან ზოგ შემთხვევაში მოცემული მონაცემების სახელმწიფო ორგანოებთან ან სხვა დაინტერესებულ პირებთან გაცვლით.“ [20]

„კიბერ დივერსანტები – ქსელის უკმაყოფილო მომხმარებელთა რიცხვიდან – ზოგადად, უკმაყოფილო მომხმარებლები წარმოადგენენ სერიოზულ საფრთხეს, ვინაიდან ისინი კარგად იცნობენ სისტემის მუშაობის პრინციპებს და შეუძლიათ თავიანთი ეს ცოდნა გამოიყენონ დესტრუქციული მიზნებისთვის. მაგალითად, სისტემის დასაზიანებლად ან კონფიდენციალური ინფორმაციის მოსაპარად. შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) მონაცემებით, სისტემის მომხმარებლებისა და გარე წყაროების მხრიდან კიბერშეტევის ორგანიზების შესაძლებლობის ერთმანეთთან შეფარდება შეადგენს 2:1.“ [21]

---

19 ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131–75/131 ელ. გვერდი; . ნანახია 06.06.2019.

20 იქვე.

21 ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131–75/131 ელ. გვერდი; . ნანახია 06.06.2019.

„კიბერ ტერორისტები – ცდილობენ ინფრასტრუქტურის მნიშვნელოვანი ობიექტები გამოიყვანონ მწყობრიდან, საერთოდ გაანადგურონ ან გამოიყენონ თავიანთი მიზნებისთვის. მათი ქმედება სერიოზული საფრთხის ქვეშ აყენებს ქვეყნების ეროვნულ უსაფრთხოებას, იწვევს ადამიანთა მასიურ მსხვერპლს, ასუსტებს ეკონომიკას, ასევე ზიანს აყენებს საზოგადოების მორალურ მდგომარეობასა და ამცირებს მათ სანდოობას ხელისუფლების მიმართ. ყველა ტერორისტული ორგანიზაცია და დაჯგუფება არ ფლობს საკმარის ცოდნასა და ტექნიკურ საშუალებებს ეფექტური კიბერშეტევის განხორციელებისთვის, თუმცა არსებობს თეორიული დაშვება, რომ მათ მიიღონ მსგავსი ცოდნა და შესაძლებლობა, ან დახმარებისთვის მიმართონ ორგანიზებული დანაშაულის წარმომადგენლების მომსახურებას.“ [22]

სუბიექტებად, რომლებსაც გააჩნიათ სპეციპიური მახასიათებლები შესაძლოა განვიხილოთ;

„ჰაკერები – იყო დრო როცა ჰაკერების მხრიდან ქსელებში არასანქცირებული შეღწევა ან პროგრამების გატეხვა დაკავშირებული იყო ჰაკერთა საზოგადოებაში ავტორიტეტის მოპოვებასთან ან წვრილმან ჰულიგნობასთან. დღესდღეისობით სურათი კარდინალურად არის შეცვლილი, კერძოდ ჰაკერთა უმრავლესობის ქმედება ატარებს კრიმინალურ ხასიათს. ადრე თუ ჰაკერებისთვის ქსელის გატეხვისათვის საჭირო იყო კომპიუტერული ტექნოლოგიების სფეროში სპეციალური უნარჩვევების ცოდნა, როცა ამჟამად საკმარისია ინტერნეტიდან შესაბამისი ინსტრუქციებისა და პროტოკოლების გადმოქაჩვა და მათი გამოყენება შერჩეულ საიტზე კიბერშეტევის ორგანიზებისთვის. ამის გამო, კიბერშეტევის განხორციელება მომხმარებლისთვის გახდა უფრო ადვილად ხელმისაწვდომი. ჰაკერთა მომსახურეობით სარგებლობენ არამარტო კორპორაციები და კომპანიები, არამედ სადაზვერვო ან სხვა სახის სპეციალური სამსახურებიც.“ [23]

„ჰაკტივისტები – ტერმინი „ჰაკტივიზმი“(hacktivism) წარმოიშვა ორი სიტყვის „Hack“ და “Activism” შეერთებით და ის აღნიშნავს სოციალური პროტესტის გამოხატვის ახალ მოვლენას, რომელიც წარმოადგენს თავისებურ სინთეზს რაღაცის მიმართ გამოხატული პროტესტის სოციალური აქტიურობისა და ჰაკერობის, რომელიც მიმართულია გარკვეული ვებ-გვერდების ან საფოსტო სერვისების წინააღმდეგ. თავიანთი პოლიტიკური მიზნების მისაღწევად, ჰაკტივისტები მიისწრაფვიან დააზიანონ ან საერთოდ მწყობრიდან გამოიყვანონ ზოგიერთი ვებ – გვერდი.“ [24]

,ბოტნეტი — ინტერნეტ – ბოტის შემქნელი ფიზიკური ან/და იურიდიული პირი, „ბოტნეტი წარმოადგენს პროგრამას, რომელიც ფარულად არის დაყენებული მსხვერპლის/ობიექტის კომპიუტერულ მოწყობილობაში, რაც დამნაშავეს/ბოროტმოქმედს საშუალებას აძლევს “დავირუსებული” კომპიუტერის რესურსების გამოყენებით, შეასრულოს გარკვეული ქმედებები. ჰაკერების ეს სახეობა თავისი პროგრამებით “ავირუსებენ” კომპიუტერების დიდ რაოდენობას, რომელთა რესურსებსაც შემდეგ იყენებენ კიბერშეტევის კოორდინირებისთვის, ასევე „სპამის“

---

22 ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი; . ნანახია 06.06.2019.

.

23 ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი ; ნანახია 06.06.2019.

24 ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი ; ნანახია 06.06.2019

გასაგზავნად, "ფიშინგისთვის" და სხვა მავნე ქმედებისთვის. მსგავსი სახის ქსელები წარმოადგენენ არალეგალური ვაჭრობის ობიექტს." [25]

„ფიშერები – ეს არის ფიზიკური პირები ან პატარა დაჯგუფებები, რომლებიც იყენებენ "ფიშინგის" ტექნოლოგიებს პერსონალური რეკვიზიტების მოპარვისა და ფასიანი ინფორმაციების გადაყიდვის მიზნით. თავიანთი მიზნების მისაღწევად ფიშერები ხშირად იყენებენ „სპამებს" და ჯაშუშურ პროგრამებს." [26]

„სპამერები – ფიზიკური ან იურიდიული პირები, რომლებიც მასიურად აგზავნიან არამოთხოვნილ ელექტრონულ ფოსტას დაფარული ან მცდარი ინფორმაციით, რომლის მიზანია ფიშინგითა და ჯაშუშური პროგრამების გამოყენებით კონკრეტულ ორგანიზაციებზე კიბერშეტევის განხორციელება; ჯაშუშური და მავნე პროგრამების შემქმნელები — ფიზიკური ან იურიდიული პირები, რომლებსაც გააჩნიათ დანაშაულებრივი ზრახვები კომპიუტერების მომხმარებლებზე კიბერშეტევის განსახორციელებლად." [27]

„პედოფილები – ეს კატეგორია სულ უფრო აქტიურად იყენებს ინტერნეტს საბავშვო პორნოგრაფიის გასავრცელებლად, ასევე სოციალური ქსელებისა და ინტერნეტ ჩათების გამოყენებით, პოტენციური მსხვერპლების გასაცნობად." [28]

ასევე აღსანიშნავია, რომ დროთა განმავლობაში, დამნაშავეებმა, რომლებიც იყენებენ მაღალ ტექნოლოგიებს, ე.წ. ჰაკერებმა[29], „დანაშაულის ახალი ფორმები და მიმართულებები შექმნეს. მათ უკვე არ იზიდავთ დანაშაულის ჩადენის ძველი მეთოდები. კომპიუტერული საშუალებები ჰაკერებს შესაძლებლობას აძლევს, მიზნის მიღწევისთვის სრულიად ახალი სქემები გამოიყენონ. თავიანთ ანგარებით მიზნებს ისინი კომპიუტერის მეშვეობით ახორციელებენ, კერძოდ, ქმნიან და გამოიყენებენ ე.წ. ვირუსებს ან ჩადიან სხვა სახის კიბერდანაშაულს. არსებობს კომპიუტერული დანაშაულის სამი კატეგორია;'' [30]

ზემოაღნიშნული სუბიექტების მიერ;

„1. კომპიუტერი გამოიყენება, როგორც ელექტრონული ინფორმაციის შექმნის, შენახვის, მისით მანიპულაციის და ელექტრონული კომუნიკაციის საშუალება. ამ შემთხვევაში

---

25 ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები". 2015 წ. გვ. 71/131–75/131 ელ. გვერდი ; ნანახია 06.06.2019 .

26 იქვე.

27 იქვე.

28 იქვე.

29 ჰაკერები (ინგლ. hacker, ტერმინის ფუძეა to hack — ჭრილობა, ჭრილი, კვეთილი; გაპობა, გაჭრა, გაცეხვა, კიწვა, ნაკუწ-ნაკუწად ქცევა, დაკბილვა, გათლა (ქვისა)) ეწოდება კომპიუტერული პროგრამისტების განსაკუთრებულ ჯგუფს. პირველად ეს ტერმინი 1960-იან წლებში გაჩნდა და ამის შემდეგ მას მრავალი მნიშვნელობა გაუჩნდა. ჰაკერი აუცილებლად, სულ ცოტა, 2 პროგრამირების ენას უნდა ფლობდეს, ერკვეოდეს ქსელში და იყენებდეს ძლიერ ოპერაციულ სისტემებს (*nix — UNIX, BSD, Linux და ა.შ.) . ელ. გვერდი;ნანახია 03.05.2019

30 ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები". 2015 წ. გვ. 71/131–75/131 ელ. გვერდი; .ნანახია 06.06.2019.

კომპიუტერი არ არის დანაშაულის იარაღი, თუმცა, მისი მეშვეობით შესაძლებელია განხორციელდეს კრიმინალურ აქტივობასთან დაკავშირებული ქმედებები, მაგალითად, ამოღებულ იქნას (გადმოიქაჩოს) ნარკოდილერის შავი ბუღალტერია;

2. კომპიუტერი შეიძლება გამოყენებულ იქნას, როგორც დანაშაულის ინსტრუმენტი. ასე მაგალითად, მისი მეშვეობით შესაძლებელია დაიბეჭდოს ყალბი ფული, გაყალბდეს საბუთები, ინტერნეტში გავრცელდეს არასრულწლოვანთა პორნოგრაფია, ჩაიტვირთოს თაღლითური ვებ-გვერდები და ა.შ;
3. „კომპიუტერი ასევე შეიძლება იქცეს დანაშაულის იარაღად. ამ შემთხვევაში თავდასხმა ხორციელდება ინფორმაციის მოპოვების შესაძლებლობაზე, მის მთლიანობასა და დაცულობაზე (ასეთია, მაგალითად, ინფორმაციისა და სერვისების მითვისება, კომპიუტერული ტექნიკის დაზიანება). ამ სახეობის დანაშაული უკავშირდება ვირუსების უკანონო გავრცელებას, სერვისებისა და ქსელების არა ავტორიზებულ დაბლოკვას. ასეთ დანაშაულს ხშირად ჩადიან ე.წ. „კიბერ-ვანდალები". ბოლო წლებში მთელ მსოფლიოში საგრძნობლად გაიზარდა სხვადასხვა ორგანიზაციების წინააღმდეგ მიმართული კიბერთავდასხმების რაოდენობა." [31]

1.2 ციფრულ დანაშაულის კლასიფიკაცია ქართულ სისხლის სამართალში

საქართველოს სისხლის სამართლის კოდექსი ახდენს მასში მოთავსებული 415 მუხლის კლასიფიცირებას სხვადასხვა კარების და თავების მიხედვით, მაგრამ არცერთ მუხლში არ გვაქვს მოცემული სიტყვა ციფრული დანაშაული, ან დანაშაული ჩადენილი ციფრული საგნის გამოყენებით, შესაბამისად როდესაც ციფრული დანაშაული მოხდება, მისი დაკვალიფიცირება ხდება სხვადასხვა მუხლებით, ამასთან საქართველოს სისხლის სამართლის კოდექსი ფეხს ვერ უბამს საერთაშორისო კლასიფიკაციით გათვალისწინებული თუნდაც კიბერდანაშაულის ტიპებს, აღნიშნულიდან გამომდინარე, მიზანშეწონილად ვთვლით წარმოგიდგინოთ დანაშაულთა ციფრული დანაშაულის ტიპები, რომელთა კვალიფიკაციისათვის უნდა მოვძებნოთ საქართველოს სისხლის სამართლის კოდექსში არსებული შესაბამისი მუხლები და შევუსაბამოთ ქმედების სამართლებრივ ბუნებას და შემადგენლობას.

ჰაკერობა: ნიშნავს სხვისი კომპიუტერული უსაფრთხოების მექანიზმის დარღვევას, სხვის კომპიუტერში არსებული პირადი ინფორმაციის ხელმისაწვდომობას. არსებობს როგორც დანაშაულებრივი, ასევე ე.წ. „ეთიკური ჰაკერობა" რომელსაც ორგანიზაციები იყენებენ მათი ინტერნეტ უსაფრთხოებისათვის, შესაბამისად ბუნებრივია „ეთიკურ ჰაკერობას" როგორც დანაშაულს ვერ მოვიაზრებთ თუ მისი გამოყენების მიზანია სისტემის დაცვა, ხოლო რაც შეეხება სხვა სახის ჰაკერობას – აღნიშნული არის დანაშაული, ჰაკერობა დანაშაულად გვევლინება ამერიკის შეერთებულ შტატებში. რაც შეეხება საქართველოს, სისხლის სამართლის კოდექსში ასეთი დანაშაული არ გვაქვს, მაგრამ ქმედების ობიექტური შემადგენლობის ნიშნებიდან გამომდინარე შესაძლოა ვიმსჯელოთ, რომ აღნიშნული დანაშაული საქართველოს სისხლის სამართლის

[31] იხ. ალექსანდრე ღლონტი, კიბერდანაშაულის პრობლემა საქართველოსა და უცხოეთის ქვეყნებში. ელ.გვერდი ; ნანახია 03.05.2019

კანონმდებლობის მიხედვით შესაძლოა დავაკვალიფიციროთ საქართველოს სისხლის სამართლის კოდექსის **284–ე** მუხლით, რომლის თანახმად დანაშაულია;

„1. კომპიუტერულ სისტემაში უნებართვო შეღწევა;

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

2. იგივე ქმედება:

ა) წინასწარი შეთანხმებით ჯგუფის მიერ;

ბ) სამსახურებრივი მდგომარეობის გამოყენებით;

გ) არაერთგზის;

დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია, — ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე.“[32]

კიბერტერორიზმი: მიუხედავად იმისა, რომ საქართველოს სისხლის სამართლის კოდექსის 323ე მუხლი ითვალისწინებს პასუხისმგებლობას ტერორისტული აქტისთვის, საქართველოს კანონმდებელმა ამ კუთხით ფეხი აუბა საერთაშორისო სტანდარტებს და სისხლის სამართლის კოდექსში გვხვდება 324–ე მუხლი - კიბერტერორიზმი, „ესე იგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას, ჩადენილი მოსახლეობის დაშინების ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით“. აღნიშნული განმარტება სისხლის სამართლის კოდექსში გვხვდება 2012 წლის 2 მარტის ცვლილების შემდეგ.

„კიბერ ქურდობა: აღნიშნული სახეზეა, როდესაც საავტორო უფლების დარღვევით ხდება ინტერნეტიდან სხვადასხვა ინფორმაციის გადმოწერა. უმეტეს შემთხვევაში ვებ–გვერდები თავად სთავაზობენ მომხმარებელს პირატულ მასალას. საქართველოს სისხლის სამართლის კოდექსში კომპიუტერის საშუალებით საავტორო უფლების დარღვევის სპეციალური მუხლი არ არის გათვალისწინებული. ასეთი დანაშაულის ჩადენის შემთხვევაში პირის ქმედება კვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284–ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 189–ე (საავტორო, მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა) მუხლებით. ეს უკანასკნელი (189–ე მუხლი), საავტორო, მომიჯნავე უფლების მფლობელის ან მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა, ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ორ წლამდე. იგივე ქმედება ჩადენილი განსაკუთრებით დიდი ოდენობით შემოსავლის მიღების მიზნით ან წინასწარი შეთანხმებით ჯგუფის მიერ, ისჯება თავისუფლების შეზღუდვით ვადით სამ წლამდე ან თავისუფლების აღკვეთით იმავე ვადით.“ [33]

„იდენტიფიკაციის ქურდობა: ბოლო რამდენიმე წლის განმავლობაში სწორედ ასეთი ქმედება

---

[32] საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით. მუხლი 284.

[33] საქართველოს მთავარი პროკურატურის ანალიტიკური სამმართველო, ინფორმაცია კიბერდანაშაულის შესახებ. ელ.გვერდი; ნანახია 03.05.2019

წარმოადგენს კიბერდანაშაულებში მთავარ პრობლემას. დამნაშავე ნახულობს ბაზას პირის საბანკო ანგარიშის, საკრედიტო ინფორმაციის, დაზღვევის და სხვა მნიშვნელოვანი ინფორმაციის შესახებ, ხოლო შემდგომ იყენებს ამ ინფორმაციას მისი ნების გარეშე სხვადასხვა ფულადი ტრანზაქციებისა და საბანკო კრედიტებისათვის. აღნიშნულმა შესაძლოა გამოიწვიოს არა მხოლოდ მნიშვნელოვანი მატერიალური ზიანი, არამედ გააფუჭოს დაზარალებულის საბანკო ისტორიაც. საქართველოს სისხლის სამართლის კოდექსში იდენტიფიკაციის ქურდობის სპეციალური მუხლი არ არის გათვალისწინებული. ასეთი დანაშაულის ჩადენის შემთხვევაში პირის ქმედება კვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 177-ე (ქურდობა) მუხლებით. თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა არ აღემ ატება 150 ლარს ქურდობა ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ერთიდან სამ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით. თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა აღემატება 150 ლარს, მაგრამ არ აღემატება 10 000 ლარს, იგი ისჯება თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე, ხოლო თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა აღემატება 10 000 ლარს ქურდობა ისჯება თავისუფლების აღკვეთით ვადით ექვსიდან ათ წლამდე.“ [34]

„ვირუსული პროგრამები: ეს გულისხმობს სპეციალური პროგრამების შექმნას, რომლებიც მიზნად ისახავს ქსელიდან კომპიუტერის გამოთიშვას. ამგვარი პროგრამების საშუალებით დამნაშავეს ეძლევა საშუალება უპრობლემოდ ჰქონდეს წვდომა სხვა პირთა პირად ინფორმაციაზე. საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლის თანახმად, დანაშაულია კომპიუტერული მონაცემის უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვა და ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით იმავე ვადით. თუ ქმედებამ გამოიწვია მნიშვნელოვანი ზიანი ან თუ იგი ჩადენილია წინასწარი შეთანხმებით ჯგუფის მიერ, სამსახურებრივი მდგომარეობის გამოყენებით ან ამგვარი ქმედებისათვის ნასამართლევი პირის მიერ ისჯება ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე.“ [35]

„კიბერ გადაკიდება: კიბერ გადაკიდების დროს დამნაშავის მიზანია მსხვერპლის საჯარო ან პირადი შეურაცხყოფა, რაც დაზარალებულის პირად ცხოვრებაზე ახდენს ძლიერ ფსიქოლოგიურ გავლენას. აღნიშნული ქმედება მას შემდეგ მოექცა ყურადღების ქვეშ, რაც მკვეთრად გაიზარდა ინტერნეტ შეურაცხყოფისა და აბუჩად აგდების საფუძველზე თვითმკვლელობისა შემთხვევები. კიბერ-გადაკიდებას, როგორც დანაშაულის ცალკე სახეს, არ იცნობს საქართველოს კანონმდებლობა, თუმცა საქართველოს სისხლის სამართლის კოდექსი ითვალისწინებს სისხლისსამართლებრივ პასუხისმგებლობას თვითმკვლელობამდე მიყვანისათვის, რომელიც გამოიწვია მსხვერპლისადმი განხორციელებულმა მუქარამ, მისი პატივის ან ღირსების სისტემატურმა დამცირებამ.“ [36]

ბავშვთა დაყოლიება: ბავშვთა დაყოლიების დროს, სოციალური ქსელების და კომპიუტერული

---

[34] საქართველოს მთავარი პროკურატურის ანალიტიკური სამმართველო, ინფორმაცია კიბერ-დანაშაულის შესახებ. ელ.გვერდი; ნანახია 03.05.2019

[35] საქართველოს მთავარი პროკურატურის ანალიტიკური სამმართველო, ინფორმაცია კიბერ-დანაშაულის შესახებ. ელ.გვერდი ; ნანახია 03.05.2019

[36] იქვე.

სისტემების გამოყენებით ცდილობენ არასრულწლოვნები დაითანხმონ საბავშვო პორნოგრაფიაზე ან სხვა დანაშაულებრივ ქმედებაზე. საქართველოს სისხლის სამართლის კოდექსი კომპიუტერული სისტემებისა და სოციალური ქსელის გამოყენებით არასრულწლოვნის პორნოგრაფიაზე დათანხმების სპეციალურ მუხლს არ ითვალისწინებს. ასეთი დანაშაულის ჩადენის შემთხვევაში შესაძლებელია ქმედებას მოერგოს საქართველოს სსკ-ის 255 პრიმა მუხლის შემადგენლობა, რომლის მიხედვითაც;

„1. პორნოგრაფიული ნაწარმოების, ნაბეჭდი გამოცემის, გამოსახულების ან პორნოგრაფიული ხასიათის სხვა საგნის უკანონოდ დამზადება, გავრცელება ან რეკლამირება, აგრეთვე ასეთი საგნით ვაჭრობა ანდა მისი შენახვა გაყიდვის ან გავრცელების მიზნით, — ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

2. წინასწარი შეცნობით არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოების შეძენა, შენახვა, ჩვენებაზე დასწრება, შეთავაზება, გავრცელება, გადაცემა, რეკლამირება, ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ან ასეთი ნაწარმოებით სარგებლობა, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით სამ წლამდე.

3. წინასწარი შეცნობით არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოების დამზადება ან გასაღება, — ისჯება ჯარიმით ან თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე.

4. ამ მუხლის პირველი, მე-2 ან მე-3 ნაწილით გათვალისწინებული ქმედება, ჩადენილი არაერთგზის, — ისჯება თავისუფლების აღკვეთით ვადით ოთხიდან ექვს წლამდე.“[37]

აღნიშნული მუხლის ციფრულ დანაშაულად მიჩნევისათვის მნიშვნელოვანია ყურადღება გავამახვილოდ მუხლის შენიშვნაზე, რომლის მიხედვითაც „არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოები არის ნებისმიერი მეთოდით შექმნილი ვიზუალური ან აუდიოვიზუალური მასალა, აგრეთვე დადგმული წარმოდგენა, რომელშიც სხვადასხვა საშუალებით წარმოდგენილია არასრულწლოვნის ან არასრულწლოვნის გამოსახულების მქონე პირის მონაწილეობა ნამდვილ, სიმულირებულ ან კომპიუტერული ტექნოლოგიის მეშვეობით გენერირებულ სექსუალურ სცენებში ან ნაჩვენებია არასრულწლოვნის გენიტალური ორგანოები მომხმარებლის სექსუალური მოთხოვნილების დაკმაყოფილების მიზნით. პორნოგრაფიულად არ ჩაითვლება ნაწარმოები, რომელსაც აქვს სამედიცინო, სამეცნიერო, საგანმანათლებლო ან სახელოვნებო ღირებულება“, თუ ასეთი მასალა მოპოვებულია ან/და გავრცელებულია ციფრული ინფორმაციის სახით, ასეთ შემთხვევაში სახეზე გვექნება ბავშვთა დაყოლიება, როგორც ციფრული დანაშაულის განშტოება, ხოლო იმ შემთხვევაში თუ არასრულწლოვნის გადაბირება მიზნად ისახავს არასრულწლოვნის ექსპლოატაციას, სახეზე გვაქვს საქართველოს სსკ-ის 143 სეკუნდა მუხლით გათვალისწინებული დანაშაული - არასრულწლოვნით ვაჭრობა (ტრეფიკინგი), ანუ „არასრულწლოვნის ყიდვა ან გაყიდვა, ან მის მიმართ სხვა უკანონო გარიგების განხორციელება, აგრეთვე მისი გადაბირება, გადაყვანა, გადამალვა, დაქირავება, ტრანსპორტირება, გადაცემა, შეფარება ანდა მიღება ექსპლუატაციის მიზნით“.

[37] საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით. მუხლი 255.

პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების ხელყოფა;

საქართველოს სისხლის სამართლის კოდექსის 157-ე მუხლის თანახმად, დასჯად ქმედებას წარმოადგენს - „პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ მოპოვება, შენახვა, გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფან [...]"[38] და „პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ გამოყენება ან/და გავრცელება ამა თუ იმ ხერხით გავრცელებული ნაწარმოების, ინტერნეტის, მათ შორის, სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით, რამაც მნიშვნელოვანი ზიანი გამოიწვია"[39] იმ შემთხვევაში თუ ასეთი ქმედება ჩადენილია ციფრული ტექნიკის გამოყენებით - მაგალითად ნაწარმოებია ფოტო - ვიდეოგადაღება ან აუდიოჩაწერა, ან სხვადასხვა სახით ელექტრონული ინფორმაციის მოპოვება პირადი ცხოვრების შესახებ - სახეზე გვაქვს ციფრული დანაშაული, ხოლო რაც შეეხება არნიშნული მუხლის მე-2 ნაწილს - თავად მუხლის შინაარსი გვაძლევს მოცემულობას რომ ეს დაკავშირებულია ციფრულ დანაშაულთან, როდესაც ინფორმაციის „გავრცელება ამა თუ იმ ხერხით გავრცელებული ნაწარმოების, ინტერნეტის, მათ შორის, სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით"[40].

პირადი ცხოვრების საიდუმლოს ხელყოფა;

საქართველოს სისხლის სამართლის კოდექსის 157[1]-ე მუხლის თანახმად, დასჯად ქმედებას წარმოადგენს „პირადი ცხოვრების საიდუმლოს უკანონოდ მოპოვება, შენახვა, გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა"[41] შესაბამისად, იმ შემთხვევაში თუ ასეთი ქმედება ჩადენილია ციფრული ტექნიკის გამოყენებით - მაგალითად ნაწარმოებია ფოტო - ვიდეოგადაღება ან აუდიოჩაწერა, ან სხვადასხვა სახისლ ელექტრონული ინფორმაციის მოპოვება პირადი ცხოვრების შესახებ - სახეზე გვაქვს ციფრული დანაშაული, ხოლო რაც შეეხება არნიშნული მუხლის მე-2 ნაწილს - თავად მუხლის შინაარსი გვაძლევს მოცემულობას რომ ეს დაკავშირებულია ციფრულ დანაშაულთან იმ შემთხვევაში, თუ პირადი ცხოვრების საიდუმლოს უკანონოდ გამოყენება ან/და გავრცელება ხორციელდება „ინტერნეტის, მათ შორის, სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით"[42].

კერძო კომუნიკაციის საიდუმლოების დარღვევა;

საქართველოს სისხლის სამართლის კოდექსის 158-ე მუხლის თანახმად, დასჯად ქმედებას წარმოადგენს „კერძო საუბრის უნებართვო ჩაწერა ან მიყურადება, აგრეთვე კომპიუტერულ სისტემაში ან სისტემიდან კერძო კომუნიკაციისას გადაცემული კომპიუტერული მონაცემის ან ამგვარი მონაცემის მატარებელი ელექტრომაგნიტური ტალღების უნებართვო მოპოვება ტექნიკური საშუალების გამოყენებით ან კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ შენახვა, აღნიშნული დანაშაული მიეკუთვნება"[43] ხოლო ამავე მუხლის მე-2 ნაწილის თანახმად „კერძო კომუნიკაციის

---

38 საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით. მუხლი 157 ნაწილი 1-ლი.

39 იქვე. ნაწილი მე - 2;

40 იქვე.

41 იქვე. მუხლი 1571 მუხლის 1-ლი ნაწილი.

42 იქვე. მე-2 ნაწილი

43 საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით. მუხლი 158 მუხლის ნაწილი 1-ლი

ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა,“[44] შესაბამისად აღნიშნული მუხლით სანქცირებული ქმედება მიეკუთვნება ციფრულ დანაშაულთან კატეგორიას.

პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა;

საქართველოს სისხლის სამართლის კოდექსის 159-ე მუხლის თანახმად, დასჯად ქმედებას წარმოადგენს „პირადი მიმოწერის ან საფოსტო გზავნილის, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ჩანაწერის ან ტელეგრაფით, კომპიუტერული სისტემით, ფაქსით ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების უკანონოდ მოპოვება, გახსნა, შინაარსის გაცნობა ან შენახვა“[45] ხოლო ამავე მუხლის მე-2 ნაწილით დასჯადია; „პირადი მიმოწერის ან საფოსტო გზავნილის, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ჩანაწერის ან ტელეგრაფით, კომპიუტერული სისტემით, ფაქსით ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების უკანონოდ გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა“[46]. შესაბამისად აღნიშნული დანაშაული მიეკუთვნება ციფრულ დანაშაულთა კატეგორიას.

---

44 იქვე. ნაწილი მე-2

45 იქვე. მუხლი 159 მუხლის 1-ლი ნაწილი;

46 იქვე. მე-2 ნაწილი;

თავი II
ციფრულ დანაშაულთან დაკავშირებული ტერმინოლოგია

2.1. საერთაშორისო სამართლებრივი ტერმინოლოგია ციფრული დანაშაულის შესახებ

აღნიშნულ პარაგრაფში წარმოდგენილია ყველა ის საერთაშორისო სამართლებრივი ტერმინი და მათი განმარტება, რაც ციფრული დანაშაულის სფეროში დღეის მდგომარეობით საერთაშორისო აქტების დონეზე არსებობს, აღნიშნული ტერმინოლოგიის და მათი განმარტებების ცოდნა უცილებელია ყველა იმ სამართალდამცავი ორგანოს თანამშრომლისათვის და ექსპერტისათვის, ვინც აწარმოებს ან ვისაც შესაძლოა შემხებლობა ჰქონდეს ციფრული დანაშაულის გამოძიებასთან.

როდესაც ნაშრომზე ვმუშაობდით მივხვდით, რომ ვიყენებდით ძალიან ბევრ არაქართულენოვანი ტერმინს, დავინტერესდით და დავიწყეთ შესაბამისი ტერმინების ძიება ქართულ ენაზე, მაგრამ ვერ მოვიძიეთ, ამიტომ იმისათვის, რათა მკითხველმა არ იფიქროს, რომ ნაშრომის ავტორმა ძალღონე დავაკელი შესაბამისი ტერმინოლოგიის ქართულ ენაზე თარგმნას, გვინდა შემოგთავაზოთ აღნიშნული თავი, სადაც განმარტებული იქნება თუ რა არის კომპიუტერული ტერმინოლოგია და რატომ ვერ ხდება მისი ქართულ ენაზე თარგმნა.

„ვინაიდან კომპიუტერის ენა ინგლისურია, არც არის გასაკვირი, რომ მსოფლიოს სხვადასხვა ენის ლექსიკა მდიდარია ინგლისურენოვანი სიტყვებით. სხვადასხვა ენაში, უპირველეს ყოვლისა, ხდება მათი პროტოტიპისა თუ სინონიმის მოძიება, რაც ხშირ შემთხევაში არ ხერხდება. ორიგინალური ტერმინებისა თუ ცნებების შემუშავების მაგივრად, ინგლისურენოვანი სიტყვები პირდაპირ შედის სხვადასხვა ენის ლექსიკაში და რა თქმა უნდა, ხანგრძლივი დროით მკვიდრდება. ამ ენობრივი მოვლენის განვითარება და გავრცელება უდაოდ მეტყველებს კომპიუტერული ტექნიკის ღრმა დანერგვაზე თანამედროვე საზოგადოების ცხოვრებაში. ამ ტერმინოლოგიამ დროთა განმავლობაში ისევე, როგორც ზოგიერთი სფეროს სპეციფიკურმა ლექსიკამ, შეაღწია სალიტერატურო ენაში და მალე იქაც დაიმკვიდრებს ადგილს.“ [47]

„კომპიუტერული ენის ლექსიკის ანალიზის საფუძველზე შეიძლება დავასკვნათ, რომ მეცნიერების ეს სფერო მოიცავს აბრევიატურების ყველაზე დიდ რაოდენობას. უმეტესწილად, შემოკლებულ ერთეულებს ვხვდებით ისეთ კომპიუტერულ ენებში, როგორებიცაა: Hardware, Operating Systems, Editors and Shells, Programming Languages. “ [48]

„რაც შეეხება კომპიუტერულ შემოკლებებს, როგორც ვხედავთ, მათ ბოლომდე ვერ მივაკუთვნებთ ვერც სალიტერატუროს, ვერც არასალიტერატურო ლექსიკას. შეგვიძლია უბრალოდ განვიხილოთ, როგორც მოვლენა, რომელსაც თითოეულისთვის დამახასიათებელი ნიშნები აქვს. ეს კი გვაძლევს უფლებას, კომპიუტერული შემოკლება-ტერმინები ჩავთვალოთ სიტყვებად, რომელსაც იყენებს საზოგადოების ის ჯგუფი, ვისაც მუდმივი შეხება აქვს ინტერნეტთან. ამ სიტყვების უმეტესობა, როგორც ვიცით, გამოირჩევა სასაუბრო-სალაპარაკო, ხშირად უხეში ფამილარული ელფერით, მაგრამ არც იმის დავიწყება შეიძლება, რომ კომპიუტერული და ინტერნეტის შემოკლებები ძირითადად პროფესიული ტერმინებიდან ნაწარმოები სიტყვებია.“ [49]

---

47 ეკატერინე ბაკარაძე ინგლისური ენის ლექსიკის განვითარების თანამედროვე ტენდენციები, დ ი ს ე რ ტ ა ც ი ა 2009. ნანახია ელ. გვერდი ;

48 იხ. იქვე.

49 ეკატერინე ბაკარაძე ინგლისური ენის ლექსიკის განვითარების თანამედროვე ტენდენციები, დ ი ს ე რ ტ ა ც ი ა 2009. ნანახია ელ. გვერდი ;

„ციფრული მტკიცებულება“ – ნებისმიერი ელექტრონული ფორმის დოკუმენტი ან მონაცემი, რომელიც შენახულია, გაგზავნილია ან მიღებულია კომპიუტერული სისტემის მიერ და შეიცავს სისხლის სამართლის საქმის ფაქტობრივი ან სამართლებრივი გარემოების დასადგენად საჭირო ინფორმაციას.[50]

კომპიუტერული დანაშაულის შესახებ ბუდაპეშტის 2001 წლის 23 ნოემბრის კონვენცია გვთავაზობს შემდეგ ტერმინთა განმარტებას;

„კომპიუტერული სისტემა — ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ ან ურთიერთდაკავშირებულ მექანიზმთა ჯგუფი, რომელთაგან ერთი ან მეტი, პროგრამის მეშვეობით, ასრულებს მონაცემთა ავტომატურ დამუშავებას;

კომპიუტერული მონაცემები – კონცეფციათა ნებისმიერი გამოსახვა ფაქტების, ინფორმაციის ან კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ფორმით, მათ შორის პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას;

მომსახურების მომწოდებელი – ნებისმიერი საჯარო ან კერძო პირი, რომელიც მისი სერვისის მომხმარებლებს უზრუნველყოფს კომპიუტერული სისტემის საშუალებით ურთიერთობის შესაძლებლობით, და ნებისმიერი სხვა პირი, რომელიც გადაამუშავებს ან ინახავს კომპიუტერულ მონაცემებს ამგვარი საკომუნიკაციო მომსახურების ან ამგვარი მომსახურების მომხმარებელთა სახელით;

ინტერნეტ-ტრაფიკის მონაცემები – კომუნიკაციებთან დაკავშირებული და კომპიუტერული სისტემის მიერ გენერირებული ნებისმიერი კომპიუტერული მონაცემები, რომელიც წარმოადგენს კომუნიკაციათა ჯაჭვის ნაწილს, მიუთითებს კომუნიკაციის წყაროს, დანიშნულების ადგილს, მიმართულებას, დროს, თარიღს, ზომას, ხანგრძლივობას, ძირითადი მომსახურების ტიპს. “ [51]

ევროპის საბჭოს 2005 წლის 24 თებევრლის ჩარჩო გადაწყვეტილება ინფორმაციულ სისტემებზე თავდასხმის შესახებ გვთავაზობს რამდენიმე ტერმინის საერთაშორისო დეფინიციას;

„კომპიუტერული მონაცემები – ფაქტების, ინფორმაციის ან პროგრამების გამოსახვა, ინ–ფორმაციულ სისტემაში გადამუშავებისთვის განკუთვნილი ფორმით, ისეთი პროგრამის ჩათვლით, რომელსაც ინფორმაციული სისტემის მეშვეობით ფუნქციების შესრულების მოქმედებაში მოყვანა შეუძლია.“ [52]

„არაუფლებამოსილი მოქმედება – ისეთი შეღწევა ან თავდასხმა, რომელიც სისტემის ან სისტემის ნაწილის მესაკუთრის ან სხვა კანონიერად მფლობელის მიერ არ არის ნებადართული, ან ცალკეული სახელმწიფოებრივი სამართლებრივი ნორმების მიხედვით დაუშვებელია.“ [53]

რაც შეეხება კიბერდანაშაულს — არსებობს „კიბერდანაშაული“–ს ტერმინის სხვადასხვა განმარტება, ამ ტერმინთან დაკავშირებით არ არსებობს რაიმე სახის ერთიანი მიდგომა და მსოფლიოს სხვადასხვა ქვეყნის კანონმდებლობაში ხშირად განსხვავებული მნიშვნელობა აქვს. არსებობს კიბერდანაშაულის შინაარსობრივად მსგავსი ტერმინები.

კიბერდანაშაული — წარმოადგენს ორი სიტყვის „კიბერ“ და „დანაშაულის“ ერთობლიობას.

სიტყვა „კიბერ“ — კომპიუტერული ქსელი, ვირტუალური რეალობა.

---

50 Eoghan Casey. „ციფრული მტკიცებულება და კომპიუტერული დანაშაული; სასამართლო მეცნიერება, კომპიუტერები და ინტერნეტი“ (ინგლისურად), მესამე გამოცემა. ელ. გვერდი ;

51 ოთხივე ტერმინი; კომპიუტერული დანაშაულის შესახებ კონვენცია 2001 წლის 23 ნოემბერი ბუდაპეშტი.

52 იქვე. მუხლი 1–ლი ქვეპუნქტი “ბ”;

53 იქვე. მუხლი 1–ლი ქვეპუნქტი “დ”;

სიტყვა „დანაშაული“ — სისხლის სამართლის კოდექსით გათვალისწინებული მართლსაწინააღმდეგო, ბრალეული ქმედება.

კიბერვიქტიმიზაცია — კიბერდანაშაულის მსხვერპლად გახდომის პროცესების შესწავლა.

„სართლებრივი ინფორმატიკა – გამოყენებითი მეცნიერებაა, რომელიც შეისწავლის სამართლის სფეროში ინფორმაციის (ნორმატიული, საცნობარო და სხვა) შეგროვების, შენახვის, დამუშავების და გამოყენების პრობლემებს, გადაწყვეტის მეთოდებსა და საშუალებებს. ანუ, სამართლებრივი ინფორმატიკა ინფორმატიკაა, რომელიც შეისწავლის სამართლებრივი ინფორმაციის ფორმირების, ინტერპრეტაციის და კომუნიკაციის პროცესებს.“ [54]

2.2. ციფრული დანაშაულის შესახებ სამართლებრივი ტერმინოლოგია ქართულ კანონმდებლობაში

პარაგრაფში, წარმოდგენილია ქართულ საკანონმდებლო სივრცეში არსებული სამართლებრივი ტერმინოლოგია და მათი განმარტებები, აღნიშნული ტერმინოლოგია აუცილებელია ციფრული დანაშაულის გამოსაძიებლად და ციფრული მტკიცებულებების ძიების პროცესში.

„კომპიუტერული სისტემა — ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის, პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, აგრეთვე მობილური ტელეფონი).“ [55]

„კომპიუტერული მონაცემი — კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას.“ [56]

„უნებართვო შეღწევა — უნებართვო გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისათვის.“ [57]

„მომსახურების მომწოდებელი – ნებისმიერი ფიზიკური ან იურიდიული პირი, რომელიც მომხმარებლებს უზრუნველყოფს შესაძლებლობით, ურთიერთობა განახორციელონ კომპიუტერული სისტემის საშუალებით, ასევე ნებისმიერი სხვა პირი, რომელიც ამუშავებს ან ინახავს კომპიუტერულ მონაცემებს ამგვარი საკომუნიკაციო მომსახურების ან ასეთი მომსახურების მომხმარებელთა სახელით.“ [58]

---

[54] ციური ნოზაძე, სამართლებრივი ინფორმატიკა, ლექციების კურსი. გვ. 2. ელ. გვერდი. . ნანახია 24.6.2019.

[55] საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით. მუხლი 284, შენიშვნა, ნაწილი 1;

[56] საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით. მუხლი 284, შენიშვნა, ნაწილი 1;

[57] იქვე, ნაწილი 3;

[58] საქართველოს სისხლის სამართლის საპროცესო კოდექსი (09/10/2009 რედ) 29.05.2019 წლის მგდომარეობით.. მუხლი 3. ნაწილი 29.

“ინტერნეტტრაფიკის მონაცემი – კომუნიკაციებთან დაკავშირებული და კომპიუტერული სისტემის მიერ გენერირებული ნებისმიერი კომპიუტერული მონაცემი, რომელიც კომუნიკაციათა ჯაჭვის ნაწილია, მიუთითებს კომუნიკაციის წყაროს, დანიშნულების ადგილს, მიმართულებას, დროს, თარიღს, ზომას, ხანგრძლივობას, ძირითადი მომსახურების ტიპს.“ [59]

„ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან — შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს მიერ ელექტრონული კავშირიდან (ელექტრონული ფოსტა), კავშირგაბმულობის ქსელიდან, სატელეკომუნიკაციო ან საინფორმაციო სისტემიდან მიმდინარე, გადაცემული, მიღებული, შეკრებილი, დამუშავებული ან დაგროვებული ინფორმაციის მოხსნა და ფიქსაცია ტექნიკურ ან/და პროგრამულ საშუალებათა გამოყენებით.“ [60]

„ინფორმაციის მოხსნა და ფიქსაცია კომპიუტერული სისტემიდან — შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს მიერ კომპიუტერული სისტემიდან გადაცემული, მიღებული, აგრეთვე კომპიუტერულ სისტემაში მიმდინარე, შეკრებილი, დამუშავებული ან დაგროვებული ინფორმაციის მოხსნა და ფიქსაცია ტექნიკურ ან/და პროგრამულ საშუალებათა გამოყენებით.“ [61]

„ინფორმაციული უსაფრთხოება —საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას.“ [62]

„ინფორმაციული უსაფრთხოების პოლიტიკა — ამ კანონით, საქართველოს სხვა ნორმატიული აქტებითა და საერთაშორისო შეთანხმებებით გათვალისწინებული ნორმებისა და პრინციპების, აგრეთვე პრაქტიკის ერთობლიობა, რომელიც ემსახურება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს.“ [63]

„კიბერსივრცე — სივრცე, რომლის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვისათვის, შეცვლისათვის ან გაცვლისათვის.“ [64]

„კიბერშეტევა — ქმედება, როდესაც ელექტრონული მოწყობილობა ან/და მასთან დაკავშირებული ქსელი ან სისტემა გამოიყენება კრიტიკულ ინფორმაციულ სისტემაში შემავალი სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით.“ [65]

„კომპიუტერული ინციდენტი — ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით

---

59 იქვე. ნაწილი 30.

60 იქვე. ნაწილი 33.

61 იქვე. მუხლი 3. ნაწილი 34.

62 საქართველოს კანონი ინფორმაციული უსაფრთხობის შესახებ. (5.06.2016 წლის რედაქციით. კონოლიდირებული 08.07.2017) მუხლი 2. ქვეპუნქტი “ა”.

63 საქართველოს კანონი ინფორმაციული უსაფრთხობის შესახებ. (5.06.2016 წლის რედაქციით. კონოლიდირებული 08.07.2017) მუხლი 2 ქვეპუნქტი “ბ”.

64 იქვე. ქვეპუნქტი “გ”.

65 იქვე. ქვეპუნქტი “დ”.

და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინ-ფორმაციული რესურსის მიტაცებას. “ [66]

„ინფორმაციული სისტემა — ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას. “ [67]

„ქსელური სენსორი — მოწყობილობა, რომელიც სპეციალურად გამიზნულია ქსელის სეგმენ-ტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციუ-ლი სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე.“ [68]

„მონაცემთა გაცვლის სააგენტო — საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი (შემდგომ — მონაცემთა გაცვლის სააგენტო). “ [69]

„კიბერუსაფრთხოების ბიურო — საქართველოს თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი (შემდგომ — კიბერუსაფრთხოების ბიურო).“ [70]

„ინტერფეისი — ელექტრონული საკომუნიკაციო ქსელის ელემენტების, ტექნიკური საშუა-ლებების, საოპერაციო პროგრამული რესურსებისა და სისტემების ურთიერთმოქმედების ფიზიკური ან ლოგიკური ფორმატი, რომელიც განსაზღვრულია საერთო ფუნქციონალური, ელექტრული, ოპტიკური, კონსტრუქციული და სხვა თავსებადობის მახასიათებლებით, პროტოკოლის მიმართ ერთგვაროვანი მოთხოვნებით.“ [71]

„აბონენტი – ბოლო მომხმარებელი, რომელსაც ელექტრონული საკომუნიკაციო მომსახურე-ბის მიმწოდებელთან წინასწარ გაფორმებული წერილობითი ხელშეკრულების საფუძველზე მიეწოდება საერთო სარგებლობის ელექტრონული საკომუნიკაციო მომსახურება.“ [72]

„აბონენტის ინდივიდუალური დაშვების სისტემა – ტექნოლოგიური სისტემა, ტექნიკური საშუალებები და მათთან დაკავშირებული საოპერაციო მართვის პროგრამული უზრუნველყოფის რესურსები, რომლებიც უზრუნველყოფს აბონენტის მიერ ინდივიდუალური, კოდირებული ციფრუ-ლი მაუწყებლობის მომსახურების მიღებას.“ [73]

„ელექტრონული საკომუნიკაციო ქსელის ელემენტები – ელექტრონული საკომუნიკაციო ქსელის შემადგენელი, ფუნქციონალურად განცალკევებული (ან განცალკევებადი) ტექნიკური ან ტექნოლოგიური საშუალებები, მათი საოპერაციო ფუნქციონალური რესურსები და სიმძლავრეები, რომლებიც თავიანთი მახასიათებლებით უზრუნველყოფს: გამოძახებებისა და საინფორმაციო სიგნალების გატარებას, გადაცემას, დამისამართებას (კომუტაციას); ბილინგის ინფორმაციის

---

66 საქართველოს კანონი ინფორმაციული უსაფრთხობის შესახებ. (5.06.2016 წლის რედაქციით. კონოლიდირებული 08.07.2017) მუხლი 2 ქვეპუნქტი “ე”.

67 იქვე. ქვეპუნქტი “ლ”.

68 იქვე. ქვეპუნქტი “მ”.

69 საქართველოს კანონი ინფორმაციული უსაფრთხობის შესახებ. (5.06.2016 წლის რედაქციით. კონოლიდირებული 08.07.2017) მუხლი 2 ქვეპუნქტი “ნ”.

70 იქვე. ქვეპუნქტი “ო”.

71 საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2-“ჰ”;

72 იქვე. ქვეპუნქტი “ა”;

73 იქვე. ქვეპუნქტი “ბ”;

შეგროვებას; ბოლო მომხმარებლისათვის მიწოდებული მომსახურების პირობების მართვას და ურთიერთოპერაბელურობას; სააბონენტო ნომრების პორტაბელურობას; ოპერატორის საოპერაციო, საცნობარო, დამხმარე და საგანგებო მომსახურებას; ქსელების სინქრონიზაციასა და სიგნალიზაციას; გამოძახებებთან დაკავშირებულ მონაცემთა ბაზებში შეღწევას; მულტიმედიას; ციფრული მაუწყებლობის მომსახურების მიწოდებას; კონვერსიას, კოდირებას, უსაფრთხოების დაცვას; პეიჯინგს; ციფრული მონაცემების ტელედამუშავებას და ინტერნეტის ან სხვა პროტოკოლის გამოყენებით გადაცემას და სხვა.“ [74]

„ადგილობრივი დაშვების ქსელი — ადგილობრივი მომსახურების ზონაში ოპერატორის სადენიანი (ელექტროსადენიანი ან ოპტიკურ-ბოჭკოვანი) საკაბელოსახაზო მეურნეობა ან უსადენო (ფიქსირებული რადიოსიხშირული ან ღია ოპტიკური) დაშვების ტექნიკური საშუალებები ელექტრონული საკომუნიკაციო მომსახურების მიწოდების მიზნით, ბოლო მომხმარებლის ფიქსირებულ ტერმინალურ მოწყობილობასა და საკომუტაციო ან გადამცემ სადგურს შორის გამოძახებების ან საინფორმაციო სიგნალების გასატარებლად, ციფრული მაუწყებლობის სიგნალების გადასაცემად.“[75]

„ადგილობრივი მომსახურების ზონა — მომსახურების ბაზრის გეოგრაფიული (ტერიტორიული) სეგმენტი, სადაც ავტორიზებული პირი ახორციელებს ბოლო მომხმარებლისთვის საერთო სარგებლობის ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას.“[76]

„ავტორიზაცია — საქართველოს კომუნიკაციების ეროვნული კომისიის მიერ საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებითა და საშუალებებით უზრუნველყოფის ან/და ელექტრონული საკომუნიკაციო მომსახურების მიწოდების განმახორციელებელი ფიზიკური ან იურიდიული პირის საქმიანობის რეგისტრაცია ამ კანონით დადგენილი ერთიანი წესით.“[77]

„ავტორიზებული პირი — საქართველოს კომუნიკაციების ეროვნული კომისიის მიერ რეგისტრირებული ნებისმიერი სამეწარმეო პირი, აგრეთვე ნებისმიერი არასამეწარმეო იურიდიული პირი, რომელიც ახორციელებს ელექტრონული საკომუნიკაციო ქსელებით უზრუნველყოფას (ელექტრონული საკომუნიკაციო ქსელის ოპერატორი) ან/და ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას (ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელი).“ [78]

„ავტორიზებული პირების ერთობლივი მნიშვნელოვანი საბაზრო ძალაუფლება — მომსახურების ბაზრის შესაბამის სეგმენტზე ორი ან მეტი ავტორიზებული პირის ერთობლივი მნიშვნელოვანი საბაზრო ძალაუფლება, ანუ ისეთი მდგომარეობა, როცა საქართველოს კომუნიკაციების ეროვნული კომისიის მიერ ჩატარებული ანალიზი ადასტურებს, რომ ბაზრის ამ სეგმენტზე ჩამოყალიბებული კონიუნქტურა და კონკურენციის მახასიათებლები მათი შეთანხმებულად მოქმედებისა და ბაზარზე არაკონკურენტული უპირატესობის ერთობლივად მოპოვების შესაძლებლობას იძლევა, მაშინაც კი, თუ მათ შორის არ არსებობს სტრუქტურული ან სხვა სახის, მათ შორის, სახელშეკრულებო ურთიერთობები.“ [79]

---

74 საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2-“ჰ37”;

75 იქვე. ქვეპუნქტი “გ”;

76 იქვე. ქვეპუნქტი “დ”;

77 იქვე. ქვეპუნქტი “ე”;

78 საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი “ვ”;

79 იქვე. ქვეპუნქტი “ზ”;

„ამოწურვადი რესურსი - რადიოსიხშირული სპექტრი ან/და ნუმერაციის რესურსი.''[80]

„არაპირდაპირი დაშვება — ელექტრონული საკომუნიკაციო ქსელის ოპერატორის მიერ საკუთარი ქსელის ელემენტებთან, მათ ფუნქციონალურ რესურსებთან და თავისუფალ სიმძლავრეებთან, ან მათი გამოყენებით განხორციელებულ (ან განხორციელებად) ელექტრონული საკომუნიკაციო მომსახურების სახეებთან მომხმარებლის ან მსურველი ავტორიზებული პირის დაშვება სხვა ტრანზიტული კავშირის (მომსახურების) ოპერატორის ქსელების გავლით.“ [81]

„ბილინგის ინფორმაცია — მომხმარებლისთვის მიწოდებული მომსახურების ან ოპერატორის ქსელის შესაბამისი ელემენტების დატვირთვის (ტრაფიკის) და მათი საოპერაციო რესურსების გარკვეულ პერიოდში გამოყენებული მოცულობის შესახებ მონაცემები, რომელთაც ოპერატორები აწვდიან ერთმანეთს ან ბოლო მომხმარებელს ანგარიშსწორების ჩატარების მიზნით.“ [82]

„ბოლო მომხმარებელი — მომხმარებელი, რომელიც საკუთარი მოხმარებისათვის იყენებს ან განზრახული აქვს გამოიყენოს საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებითა და საშუალებებით განხორციელებული მომსახურება და მიზნად არ ისახავს მის შემდგომ მიყიდვას სხვა მომხმარებლისათვის.“ [83]

„გამოყენებითი პროგრამული ინტერფეისი — ციფრული მაუწყებლობის ან ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის მომსახურების სახეების სამომხმარებლო რესურსებისა და ციფრული მაუწყებლობის ტექნიკური საშუალებების ფუნქციონალური რესურსების დამაკავშირებელი პროგრამული ინტერფეისი.“ [84]

„დაშვება — ელექტრონული საკომუნიკაციო ქსელის ოპერატორის მიერ განსაზღვრული პირობებით (მათ შორის, ტარიფებით) საკუთარი ქსელის შესაბამისი ელემენტებით, ტექნიკური საშუალებებით, მათი თავისუფალი ფუნქციონალური რესურსებითა და სიმძლავრეებით, ან მათი გამოყენებით განხორციელებული (ან განხორციელებადი) ელექტრონული საკომუნიკაციო მომსახურების სახეებით სარგებლობის უზრუნველყოფა, რომელიც მოიცავს:

ელექტრონული საკომუნიკაციო ქსელის ოპერატორის საკუთარი ქსელის ფიზიკური ინფრასტრუქტურის შესაბამისი ელემენტებითა და ტექნიკური საშუალებებით სარგებლობის უზრუნველყოფას; ადგილობრივი დაშვების ქსელის ელემენტებითა და მათი თავისუფალი რესურსებით, მათ შორის, საკანალიზაციო არხებითა და ჭებით, სააბონენტო წყვილებით, ანძებით და ბოძებით სარგებლობის უზრუნველყოფას; თანალოკაციის ფართობით სარგებლობის უზრუნველყოფას; ფიქსირებული და მობილური საკომუნიკაციო ქსელის ოპერატორების ქსელის შესაბამისი ელემენტებით, მათი თავისუფალი საოპერაციო ფუნქციონალური რესურსებითა და სიმძლავრეებით (მათ შორის, როუმინგის მიწოდებასთან დაკავშირებული რესურსებით) სარგებლობის უზრუნველყოფას; აბონენტის ინდივიდუალური დაშვების სისტემისა და პროგრამების (მომსახურების) ელექტრონული სარჩევის (მეგზურის) რესურსებით სარგებლობის უზრუნველყოფას; ელექტრონული საკომუნიკაციო ქსელების საოპერაციო პროგრამული მართვისა და მომხმარებელთა საინფორმაციო ბაზების,

[80] საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი “თ”;

[81] იქვე. ქვეპუნქტი “კ”;

[82] საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი “ნ”;

[83] იქვე ქვეპუნქტი “ო”;

[84] იქვე ქვეპუნქტი “ჟ”;

სააბონენტო ნომრების პორტაბელურობასთან (ტრანსლირებასთან) დაკავშირებული რესურსებით სარგებლობის უზრუნველყოფას; ვირტუალური ქსელების მომსახურების სახეებით სარგებლობის უზრუნველყოფას; ელექტრონული საკომუნიკაციო ქსელის სხვა შესაბამისი ელემენტების ფუნქციონალური რესურსებითა და სიმძლავრეებით ან საკომუნიკაციო მომსახურების სახეებით სარგებლობის უზრუნველყოფას.“ [85]

„დაშვების (ურთიერთჩართვის) წერტილი — თანალოკაციის ფართობზე განთავსებული წერტილი, სადაც მთავრდება ერთი ოპერატორის და იწყება მეორე ოპერატორის დაშვებასთან ან/და ურთიერთჩართვასთან დაკავშირებული პასუხისმგებლობა.“ [86]

„ელექტრონული საკომუნიკაციო მომსახურება — საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებითა და საშუალებებით განხორციელებული მომსახურება, რომელსაც მომსახურების მიმწოდებელი ავტორიზებული პირი განსაზღვრული საფასურის სანაცვლოდ სთავაზობს მსურველ ოპერატორს ან მომხმარებელს.“ [87]

‘’ელექტრონული საკომუნიკაციო ქსელები (ელექტრო-კავშირგაბმულობის ქსელები) — გამოძახებებისა და სხვადასხვა საინფორმაციო სიგნალების ელექტრონული დამუშავების, დამისამართების (კომუტაციის), გატარების და გადაცემის ტექნოლოგიური სისტემა, რომელიც მოიცავს სადენიან (მათ შორის, ოპტიკურბოჭკოვან), თანამგზავრულ, რადიოსიხშირულ ან ოპტიკურ აღჭურვილობას, სხვა ტექნოლოგიურ საშუალებებს და საოპერაციო ტექნიკურ რესურსებს, მათ შორის, ფიქსირებული (არხული და პაკეტური კომუტაციის, მათ შორის, ინტერნეტის) და მობილური კომუნიკაციების, ციფრული მაუწყებლობის, საეთერო და საკაბელო ქსელებს. სახელმწიფო თავდაცვის, უშიშროებისა და მართლწესრიგის დაცვის ორგანოების ელექტრონული საკომუნიკაციო ქსელებით უზრუნველყოფა ითვალისწინებს ელექტრონული საკომუნიკაციო სპეციალური ქსელების არსებობასაც.“ [88]

„ელექტრონული საკომუნიკაციო ქსელებით უზრუნველყოფა — ქსელების, ტექნიკური საშუალებების ან ქსელის შესაბამისი ელემენტების მონტაჟი, საოპერაციო მართვა, ექსპლუატაცია და მათი გამოყენებით ეკონომიკური საქმიანობა, აგრეთვე ქსელის ამ ელემენტებთან, მათ რესურსებთან და სიმძლავრეებთან მსურველი ავტორიზებული პირების დაშვება.“ [89]

„ელექტრონული საკომუნიკაციო უწყებრივი ქსელი — ქსელი, რომელიც შექმნილია არაკომერციული მიზნით, ფუნქციონირებს შიდასაწარმოო საჭიროებისათვის და ჩართულია საერთო სარგებლობის ელექტრონულ საკომუნიკაციო ქსელში.“ [90]

„ელექტრონული საკომუნიკაციო ქსელის ოპერატორი — ავტორიზებული პირი, რომელსაც განზრახული აქვს ან ახორციელებს საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებით ან ქსელის შესაბამისი ელემენტებით უზრუნველყოფას და განსაზღვრული საფასურის სანაცვლოდ მსურველი ავტორიზებული პირის ამ ელემენტებთან, მათ რესურსებთან და

---

[85] საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2-“რ-რზ”;

[86] იქვე ქვეპუნქტი “უ”;

[87] იქვე. ქვეპუნქტი “ღ”;

[88] იქვე.ქვეპუნქტი“ყ”;

[89] საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი “შ”;

[90] იქვე ქვეპუნქტი “ჩ”;

სიმძლავრეებთან დაშვებას, ასევე მათი გამოყენებით მომხმარებლებისათვის ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას.“ [91]

„ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელი — ელექტრონული საკომუნიკაციო ქსელის ოპერატორი ან მისი ქსელის შესაბამის ელემენტებთან ან რესურსებთან დაშვებული ავტორიზებული პირი, რომელსაც განზრახული აქვს ან ახორციელებს ქსელის ამ ელემენტებით ან რესურსებით ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას.“ [92]

„მომხმარებელი — იურიდიული ან ფიზიკური პირი, რომელიც იყენებს ან განზრახული აქვს გამოიყენოს ელექტრონული საკომუნიკაციო მომსახურება.“ [93]

„მომხმარებლის ტერმინალური მოწყობილობა — აბონენტის ან ბოლო მომხმარებლის მიერ ელექტრონული საკომუნიკაციო მომსახურების მისაღებად განკუთვნილი, მობილური ან ფიქსირებულ მისამართზე განთავსებული ტექნიკური აღჭურვილობა, რომელიც არ არის ოპერატორის ქსელის ნაწილი, თუმცა დაკავშირებულია მასთან.“ [94]

„ნუმერაციის სისტემა — სიმბოლოების განსაზღვრული კომბინაცია, რომელიც გამოიყენება ელექტრონული საკომუნიკაციო მომსახურების მიწოდების პროცესში ელექტრონული საკომუნიკაციო ოპერატორის ქსელის ან მომხმარებლის ტერმინალური მოწყობილობის იდენტიფიცირებისათვის.“[95]

„სააბონენტო ნუმერაცია — ნუმერაციის სისტემის საფუძველზე არსებული ციფრული სისტემა აბონენტის ტერმინალური მოწყობილობის იდენტიფიცირებისათვის.“ [96]

„საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელი — ელექტრონული საკომუნიკაციო ქსელების ერთიანი სისტემა, რომელიც განკუთვნილია მომხმარებლებლისთვის საზოგადოებისათვის შეუზღუდავად ხელმისაწვდომი, საერთო სარგებლობის ელექტრონული საკომუნიკაციო მომსახურების მისაწოდებლად.“ [97]

„ელექტრონული საკომუნიკაციო სპეციალური ქსელები — საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელისგან ფიზიკურად განცალკევებული ქსელები, რომლებიც შექმნილია არაკომერციული მიზნით, სახელმწიფო თავდაცვის, უშიშროებისა და მართლწესრიგის დაცვის ღონისძიებათა ჩასატარებლად.“ [98]

„ტექნიკური საშუალებები — ელექტრონული საკომუნიკაციო გამოძახებებისა და საინფორმაციო

---

[91] საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი “ც”;

[92] იქვე. ქვეპუნქტი“ძ”;

[93] იქვე. ქვეპუნქტი“ჰ9”;

[94] იქვე ქვეპუნქტი “ჰ10”;

[95] საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი “ჰ13”;

[96] იქვე ქვეპუნქტი “ჰ17”;

[97] იქვე. ქვეპუნქტი“ჰ18”;

[98] იქვე.ქვეპუნქტი“ჰ22”;

სიგნალების ფორმირების, დამუშავების, გატარების, გადაცემის ან მიღების მიზნით გამოყენებული ელექტრონული საკომუნიკაციო ქსელის აღჭურვილობა და საშუალებები. “ [99]

„ტრაფიკი – ოპერატორის ქსელის ელემენტებისა და ტექნიკური საშუალებების ჯამური დატვირთვა დროის ინტერვალში. “ [100]

„ელექტრონული საკომუნიკაციო ქსელების სახაზო საშუალებები და ნაგებობები – ელექტრონული საკომუნიკაციო ქსელების საკაბელო, საჰაერო, რადიოსარელეო, თანამგზავრული ხაზების ფიზიკური წრედები და სახაზო ტრაქტები ან/და მათი ტექნოლოგიური სისტემის შემადგენელი დანადგარების, მოწყობილობებისა და ნაგებობების ერთიანი კომპლექსები, რომლებიც გამოიყენება ელექტრონული საკომუნიკაციო გამოძახებისა და საინფორმაციო სიგნალების გატარებისათვის ან/და გადაცემისათვის.“ [101]

„ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემები — მომხმარებლის მაიდენტიფიცირებელი მონაცემები; კომუნიკაციის წყაროს კვალის დადგენისა და იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის ადრესატის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის თარიღის, დროისა და ხანგრძლივობის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის სახის იდენტიფიცირებისათვის საჭირო მონაცემები; მომხმარებლის კომუნიკაციის აღჭურვილობის ან შესაძლო აღჭურვილობის იდენტიფიცირებისათვის საჭირო მონაცემები; მობილური კომუნიკაციის აღჭურვილობის ადგილმდებარეობის იდენტიფიცირებისათვის საჭირო მონაცემები.“ [102]

„ობიექტის ტექნიკური იდენტიფიკატორი – საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის 37-ე ნაწილით განსაზღვრული იდენტიფიკატორი, აგრეთვე „კონტრდაზვერვითი საქმიანობის შესახებ“ საქართველოს კანონის მე-2 მუხლის „რ“ ქვეპუნქტით გათვალისწინებული იდენტიფიკატორი.“ [103]

„კომუნიკაციის რეალურ დროში მოპოვების ნახევრად სტაციონარული ტექნიკური შესაძლებლობა – ელექტრონული საკომუნიკაციო ქსელით გადაცემული კომუნიკაციის და მისი მაიდენტიფიცირებელი მონაცემების გადაჭერა უფლებამოსილი ორგანოს მიერ კომუნიკაციის მიმდინარეობისას ან მისი დასრულებისთანავე, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურე ინფრასტრუქტურაზე შესაბამისი აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების დროებითი ან მუდმივი განთავსებით/მონტაჟით.“ [104]

---

99 იქვე. ქვეპუნქტი“ჰ25”;

100 იქვე ქვეპუნქტი “ჰ28”;

101 საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2-“ჰ44”;

102 იქვე ქვეპუნქტი -“ჰ62”;

103 იქვე.ქვეპუნქტი“ჰ65”

104 იქვე. ქვეპუნქტი “ჰ66”;

თავი III
ციფრულ დანაშაულთან ბრძოლის სამართლებრივი რეგულაციები

3.1 ციფრულ დანაშაულთან ბრძოლის საერთაშორისო სამართლებრივი რეგულაციები

აღსანიშნავია, რომ მსოფლიოს მასშტაბით ძალზედ ინტენსიურად წარმოებს ციფრულ მტკიცებულებების საფუძველზე ჩადენილ დანაშაულებთან ბრძოლა, რასთან დაკავშირებითაც შექმნილ იქნა რამდენიმე საერთაშორისო ძალის მქონე დოკუმენტი, მათ შორის საერთაშორისო და საქართველოსთვის მნიშვნელოვანი ძალის მქონე დოკუმენტს წარმოადგენს ევროსაბჭოს კონვენცია «კიბერდანაშაულის შესახებ», რომელიც მიღებულა 2001 წლის 23 ნოემბერს ქ. ბუდაპეშტში, დოკუმენტი მიღებულია ევროსაბჭოს 41 წევრი სახელმწიფოს მიერ.

გარდა სხვა დებულებებისა, კონვენციის 35–ე მუხლის თანახმად, ყველა წევრ სახელმწიფოს ეკისრება ვალდებულება, რომ დანიშნოს საკონტაქტო პირი, რომელსაც დაუკავშირდებიან კვირაში 7 დღის მანძილზე, 24 საათის განმავლობაში რათა უზრუნველყოფილ იქნეს კომოპიუტერულ სისტემებთან და მონაცემებთან დაკავშირებულ დანაშაულების გამოძიება და დევნა – ბუნებრივია ასეთი საჭიროების არსებობის შემთხვევაში, ხოლო ამგვარი დახმარება უნდა უზრუნველყოფდეს ტექნიკური რჩევებით, მტკიცებულებათა მოპოვებისათვის და დაცვისათვის მიცემული რჩევებისა და დანაშაულის ჩამდენ შესაძლო პირთა ადგილმდებარეობის დადგენის მიზნებისათვის რჩევების გაცემას. გასათვალისწინებელია, რომ საქართველოს შინაგან საქმეთა სამინისტროს გააჩნია უფასო ცხელი ხაზი – 112 და შესაბამისი ელექტრონული ფოსტა cybercrime@mia.gov.ge.

მსგავსი ცხელი ხაზის შექმნასთან დაკავშირებით „ეუთო“–მაც მოუწოდა მისი გადაწყვეტილებით სახელმწიფოებს, რომ შეუერთდნენ ევროსაბჭოს მიღებულ კონვენციას «კიბერდანაშაულის შესახებ» და «დიდი რვიანის» ქვეყნების მიერ კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლისთვის შექმნილ მუდმივმოქმედ ქსელს, რომლის მიზანია კვირაში შვიდი დღე ოცდა ოთხი საათი მოკავშირე სახელმწიფოებისთვის ინფორმაციის მიწოდება და კომპეტენციის ფარგლებში სათანადო დახმარების აღმოჩენა., მსგავსი ქსელი ასევე შექმნილია „ინტერპოლის“ ფარგლებშიც. იგი მთელი მსოფლიოს მასშტაბით აერთიანებს ასამდე მუდმივმოქმედ დაწესებულებას, რომელიც ინტერპოლის წევრსახელმწიფოებს ეხმარება მოძებნონ საჭირო სპეციალისტი სხვადასხვა ქვეყანაში, დროულად მიიღონ მათი დახმარება კომპიუტერული დანაშაულის გამოძიების და მასზე მტკიცებულების შეგროვებასთან დაკავშირებით. [105]

,,უნდა აღინიშნოს ასევე საბჭოს 2005 წლის 24 თებევრლის ჩარჩო გადაწყვეტილება ინფორმაციის სისტემებზე თავდასხმის შესახებ, რომლის მიზანია ცალკეული სახელმწიფოების სისხლისსამართლებრივი ნორმების ჰარმონიაციის გზით ინფორმაციულ სისტემებზე თავდასხმების აღსაკვეთად წევრი სახელმწიფოების იუსტიციურ და სხვა უფლებამოსილ ორგანოებს შორის თანამშრომლობის გაუმჯობესება. აღსანიშნავია, რომ უკანასკნელ პერიოდში, განსაკუთრებით ორგანიზებული დანაშაულის ფარგლებში, ხშირად ხორციელდება ინფორმაციულ სისტემებზე თავდასხმები და იზრდება ამგვარ სისტემებზე ტერორისტული თავდასხმების რისკი. ამით კი, საფრთხე ემუქრება საზოგადოების ინფორმაციულ უსაფრთხოებასა და თავისუფლების, უსაფრთხოებისა და სამართლოს სივრცის აშენების მიზანს. აღნიშნული საშიშროებების გადასალახად, 2001 წლის 5 სექტემბერს, ევროპულმა პარლამენტმა თავის გადაწყვეტილებაში მიუთითა ამ პრობლემისათვის

[105] იხ. უჩა ზაქაშვილი. ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2014 წელი. გვ. 24

პრაქტიკული დახმარების მხარდაჭერის აუცილებლობაზე, ამ მიზით კი 2005 წლის 24 თბერვალს, ევროკავშირის საბჭომ, ევროპის კავშირის ხელშეკრულების, განსაკუთრებით 29–ე, 30–ე მუხლის 1–ლი ნაწილის "ა", 31–ე მუხლის 1–ლი ნაწილის "ე" და 34–ე მუხლის მე–2 ნაწილის "ბ" პუნქტებზე დაყრდნობით, კომისიის ინიციატივით, ევროპარლამენტის მიერ პოზიციის გამოხატვის შემდეგ, მიიღო წარმოდგენილი ჩარჩო — გადაწყვეტილება. ჩარჩო გადაწყვეტილება იცავს ძირითად უფლებებსა და თავისუფლებებს და პატივს სცემს იმ პრინციპებს, რომლებიც ევროპის კავშირის ხელშეკრულების მე–6 მუხლითა და ევროპის კავშირის ძირითად უფლებათა ქარტიით, უპირველეს ყოვლისა მე–2 და მე–4 თავებით არის აღიარებული." [106] აღნიშნული გადაწყვეტილება შედგება პრეამბულისა და 13 ძირითადი დებულებისაგან.

როდესაც ვსაუბრობთ ციფრულ დანაშაულზე, მნიშვნელოვანია განვიხილოთ ევროპის ქვეყნებში აღნიშნულ დანაშაულთან ბრძოლის სამართლებრივი მექანიზმები, რომელთა საფუძველზეც საქართველომ უნდა აიღოს მაგალითი და გაატაროს ისეთი ღონისძიებები, როგორც ევროპაში. განვიხლოთ რამდენიმე მნიშვნელოვანი მიღწევების მქონე სახელმწოფო;

„გერმანია — გერმანიაში კომპიუტერული ინფორმაციის სფეროში ჩადენილ დანაშაულებზე სისხლისსამართლებრივი პასუხისმგებლობის საკითხი 1986 წლიდან დადგა. 1987 წლის აგვისტოდან განხორციელდა შესაბამისი ცვლილებები გერმანიის სისხლის სამართლის კოდექსში, რითიც დადგინდა პასუხისმგებლობა კომპიუტერული დანაშაულისთვის.''[107]

„გერმანიამ საკანონმდებლო ცვლილებაზე მსჯელობა 2007 წლიდან დაიწყო. ევროსაბჭოს ექსპერტი მარკო გერკე, რომელიც მიწვეული იყო გერმანიის საკანონმდებლო ორგანოში ცვლილებების პროექტის მომზადების პროცესში, ჯერ კიდევ 2007 წლის ივლისში, აცხადებდა, რომ გერ–მანიის კანონმდებლობა განსხვავებით ბევრი სხვა ქვეყნისგან არ აწესებდა სისხლისსამართლებრივ პასუხისმგებლობას კომპიუტერში ან მის ქსელში უნებართვო შეღწევისთვის. ეს ქმედება დასჯადი იყო მხოლოდ მაშინ, თუ იგი ინფორმაციის მოპოვებას გამოიწვევდა. მ.გერკეს დასაბუთებულად მიაჩნდა, რომ აღნიშნული ხარვეზი საჭიროებდა აღმოფხვრას და კომპიუტერულ სისტემაში უნებართვო შეღწევა უნდა ყოფილიყო დასჯადი, მიუხედავად იმისა დადგა თუ არა რაიმე შედეგი. მ. გერკეს აუცილებლად მიაჩნდა „კიბერდანაშაულის შესახებ" კონვენციის მე–6 მუხლით გათვალისწინებული ქმედების კრიმინალიზაცია. მისი აზრით, ცვლილება უნდა შეხებოდა გერ–მანიის სისხლის სამართლის 303–ბ მუხლსაც, რომლის ძველი რედაქციით დასჯადი იყო იმ ინფორმაციის დამუშავების პროცესის ხელყოფა, რომელიც განსაკუთრებული მნიშვნელობის იყო ბიზნესის, საწარმოს ან ადმინისტრაციული ორგანოსთვის. მ. გერკეს აზრით, ცვლილების შედეგად ქმედება დასჯადი უნდა ყოფილიყო იმ შემთხვევაშიც თუ მოხდებოდა იმ ინფორმაციის დამუშავების პროცესის ხელყოფა, რომელიც ინახებოდა კერძო პირის კოპიუტერში. მ. გერკეს პოზიციას ყველა ნაწილში ვიზიარებ. იგი კიბერდანაშაულის სფეროში ერთ–ერთი საუკეთესო ექსპერტია, თუმცა მისი პოზიცია 2007 წელს გაზიარებული არ იქნა, მაგრამ გერმანიამ «კიბერდანაშაულის შესახებ» კონვენციის რატიფიცირება 2009 წლის მარტში მაინც მოახდინა. ამჟამად, გერმანულ სისხლის სამართლის კოდექსში გათვალისწინებულია, მ. გერკეს პოზიცია[...] " [108].

---

[106] მერაბ ტურავა, "ევროპული სისხლის სამართალი" 2010 წ. გვ. 472.

[107] იხ. უჩა ზაქაშვილი. ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში". 2014 წელი. გვ.18

[108] უჩა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში". 2013 წ. გვ. 120. ელ. გვერდი ნანახია 06.06.2019 წელი.

მნიშვნელოვანია, გერმანიის სისხლის სამართლის კოდექსის მიმოხილვაში გავითვალისწინოთ კიოლნის უნივერსიტეტის პროფესორის პაულ მარტინ ვასმერი მსჯელობა, რომელიც 2017 წლის 24 ოქტომბერს, საქართველოს უნივერსიტეტში გაკეთებული მოხსენების დროს იქნა გაჟღერებული, სადაც იგი კომენტარს უკეთებს გერმანიის სისხლის სამართლის კოდექსის მუხლებს ციფრულ დანაშაულთან დაკავშირებით, და აღნიშნავს, რომ გერმანიის სისხლის სამართლის კოდექსის 303–ე მუხლის შემადგენლობაში მოიაზრებს რა ქონების ელექტრონულ დაზიანებას, თავის შემადგენლობაში აერთიანებს სხვადასხვა ფორმებსა თუ გზებს კომპიუტერულ სისტემაზე თავდასხმისა და ინფორმაციის მოპოვების მიმართულებით, მაგალითად – 303–ე მუხლის „ა“ პუნქტით, ისჯება პირი, რომელიც მართლსაწინააღმდეგო წაშლის ან დამალავს მონაცემებს ან შეუძლებელს გახდის მათ გამოყენებას, ამავე მუხლის „ბ“ პუნქტით კი ისჯება პირი, რომელიც ხელს უშლის სხვისთვის მნიშვნელოვანი მონაცემის დამუშავების პროცესს, იმით, რომ იგი მონაცემებში შედის იმ მიზნით, რომ ზიანი გამოიწვიოს ან მათ გადამისამართებას ახდენს ან მონაცემების დამუშავების სისტემას ან მონაცემთა მატარებელს აზიანებს, ანადგურებს, მის გამოყენებას შეუძლებელს ხდის, შლის ან ცვლის. თუკი მონაცემთა დამუშავება უცხო საწარმოსთვის, უცხო კომპანიისათვის ან სახელმწიფო

ორგანოსათვის არსებითი მნიშვნელობის მქონეა, აქვე აუცილებლად ყურადღება უნდა გამახვილდეს.

ასევე გერმანიის სსკ–ის 202b (მონაცემების ხელში ჩაგდება) მიხედვით, ისჯება პირი, რომელიც უფლებამოსილების გარეშე თავისთვის ან სხვა პირისთვის ტექნიკური საშუალებების გამოყენებით მონაცემთა არასაჯარო გაცვლის პროცესში ჩარევით ან მონაცემთა დამუშავების სისტემის ელექტრომაგნიტური გამოსხივების საფუძველზე მოიპოვებს მონაცემებს, რომლებიც მისთვის არაა განკუთვნილი – აღნიშნულ მუხლს პაულ მარტინ ვასმერი განმარტავს, რომ; ამ შემთხვევაში მოიაზრება მონაცემთა გადაცემის ნებისმიერი ფორმა (მაგალითად, უკაბელო ინტერნეტის, ელექტრონული შეტყობინების, ტელეფონის, ხმოვანი შეტყობინების, ფაქსის მეშვეობით). დანაშაულის შემადგენლობა მოითხოვს „არასაჯაროობის” ელემენტის არსებობას, რისთვისაც გადამწყვეტია არა მონაცემების სახეობა და შინაარსი, არამედ მონაცემების გადაცემის პროცესი. მონაცემთა მოპოვებისათვის არ აქვს მნიშვნელობა მონაცემთა კოდირების ფაქტის არსებობას. ამ შემთხვევაში არ მოიაზრება მაგალითად, ე. წ. Phishing, რომლის დროსაც, მსხვერპლი წვდომის მონაცემებს თავისი სურვილით უგზავნის დამნაშავეს.

,,დღეის მდგომარეობით გერმანიაში ინფორმაციული უსაფრთხოების პოლიტიკის განვითარების, იმპლემენტაციის და კრიტიკული ინფრასტრუქტურის დაცვის საქმეში განსაკუთრებული პასუხისმგებლობა ეკისრება შინაგან საქმეთა სამინისტროს. 2011 წელს მზარდი კიბერ–საფრთხეების საპასუხოდ სამინისტროს გადაწყვეტილებით შეიქმნა ეროვნული კიბერ–თავდაცვის ცენტრი («Nationale Cyber–Abwehrzehntrum» (NCAZ). ცენტრი კოორდინაციას უწევს ინფორმაციული უსაფრთხოების სფეროში სამთავრობო უწყებების, მათ შორის, თავდაცვის სა–მინისტროს, ფედერალური პოლიციის და საგარეო დაზვერვის სააგენტოს საქმიანობას. ცენტრის მისიას წარმოადგენს კიბერ–უსაფრთხოების ინციდენტების სწრაფი და დეტალური შეფასება და კოორდინირებული რეაგირებისთვის რეკომენდაციების შემუშავება. შინაგან საქმეთა სამინისტრო ზედამხედველობს სხვა უწყებებსაც (კერძოდ, სამოქალაქო თავდაცვის ფედერალურ ოფისს, ინფორმაციის უსაფრთხოების ფედერალურ ოფისს, კრიმინალური პოლიციის ფედერალურ სამსახურს), რომლებიც ასევე მუშაობენ კიბერ–საფრთხეების შეფასების, ანალიზის და თავდაცვითი კონცეფციების განვითარების საკითხებზე.“ [109]

[109] იხ. ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07–3/255, 19.09.13) ელ. გევრდი ; ნანახია 06.06.2019

„გერმანიაში ფუნქციონირებს ცალკე სამთავრობო სააგენტო – ინფორმაციული უსაფრთხოების ფედერალური ოფისი, რომლის ძირითადი მოვალეობაა გერმანიის მთავრობისთვის კომპიუტერული და კომუნიკაციური უსაფრთხოების უზრუნველყოფა. ოფისი განთავსებულია ბონში და ჰყავს 400-ზე მეტი თანამშრომელი. ოფისის ძირითად ფუნქციებს შეადგენს: ინფორმაციული უსაფრთხოების მართვა, ინტერნეტის უსაფრთხოება, ქსელური უსაფრთხოება, ფედერალური ინფორმაციის ტექნოლოგიებისადმი არსებული საფრთხეების პრევენცია, ფედერალური კომუნიკაციური სისტემების დაცვა და ა.შ. გერმანიაში მოქმედებს კომპიუტერულ ინციდენტებზე დახმარების 20 ჯგუფი. აქედან ერთი ჯგუფი (Computer Emergency Response Team BundeswehrCERTBw) იმყოფება უშუალოდ თავდაცვის უწყების დაქვემდებარების ქვეშ და პასუხისმგებელია თავდაცვის სფეროში წარმოშობილი კომპიუტერული ინციდენტების მართვაზე.“ [110]

ლატვია — ლატვიაში კიბერუსაფრთხოების პოლიტიკის განსაზღვრასა და პრაქტიკულ განხორციელებაზე პასუხისმგებელობა ეკისრება ლატვიის რესპუბლიკის ინფორმაციული უსაფრთხოების ინციდენტებზე რეაგირების ინსტიტუტს ე.წ. CERT.LV (ინფორმაციააღებულია მათივე ელ. გვერდიდან – https://cert.lv/en/about-us), როგორც მათ ელექტრონულ გვერდზე არის მითითებული აღნიშნული ინსტიტუტი ექვემდებარება ლატვიის თავდაცვის სამინისტროს, ხოლო მისი საქმიანობა რეგულირდება ინფორმაციული ტექნოლოგიების უსაფრთხოების შესახებ კანონით. ინსტიტუტს გააჩნია 24/7 – ზე ცხელი ხაზი, რომლის მიზანია ინციდენტების მოგვარება და სხვადასხვა სახის დახმარების გაწევა, ასევე IT უსაფრთხოებასთან დაკავშირებული ღონისძიებები და ინფორმირებულობა საქმიანობის ამაღლება. აღსანიშნავია, რომ თავის მხრივ აღნიშნული ინსტიტუტი არის FIRST -ს სრული წევრი.

FIRST — არის გლობალურ სივრცეში აღიარებული უმაღლესი ორგანიზაცია ინციდენტებზე რეაგირებისთვის და მისი წევრობა საშუალებას აძლევს ინციდენტების რეაგირების გუნდებს უფრო ეფექტურად რეაგირდნენ უსაფრთხოების ინციდენტებზე, როგორც რეაქტიული, ასევე პროაქტიული მიმართულებებით, FIRST აერთიანებს სხვადასხვა სახის კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების გუნდებს სამთავრობო, კომერციული და საგანმანათლებლო ორგანიზაციებისგან. FIRST მიზნად ისახავს ინციდენტების პრევენციის სფეროში თანამშრომლობისა და კოორდინაციის გაღრმავებას, ინციდენტებზე სწრაფი რეაგირების სტიმულირებას და წევრებისა და საზოგადოების ფართო საზოგადოებაში ინფორმაციის გაზიარებას. ნდობის ქსელის გარდა, რომელიც FIRST ქმნის გლობალურ ინციდენტებზე რეაგირების საზოგადოებაში, აღნიშნული ორგანიზაციის ელექტრონული გვერდი არის (https://www.first.org/).

დიდი ბრიტანეთი — დიდ ბრიტანეთში კანონი «კომპიუტერული ტექნოლოგიის არასანქცირებული გამოყენების შესახებ», ფუნქციონირებს 1990 წლიდან, დიდი ბრიტანეთის რეგულაციები მსგავსებაშია გერმანიაში არსებულ რეგულაციებთან ციფრული დანაშაულის კუთხით, ვინაიდან ისევე როგორც გერმანიაში, დიდ ბრიტანეთშიც დასჯად ქმედებად ითვლება კომპიუტერში, მასში დაცულ ინფორმაციაში ან/და პროგრამაში უკანონო შეღწევა, ინფორმაციის ბლოკირება, მოდიფიცირება, განადგურება ან კოპირება რომლის შემადგენლობის მთავარი ნაწილი არის წინასწარ განზრახვა.

„დღევანდელი მდგომარეობით დიდ ბრიტანეთში ინფორმაციული უსაფრთხოების პოლიტიკის მიმართულებებს განსაზღვრავს „კიბერუსაფრთხოების და ინფორმაციული უზრუნველყოფის“ სამსახური, რომელიც თანამშრომლობს სხვადასხვა უწყებებთან, მათ შორის, თავდაცვის სამინისტროსთან, ბრიტანეთის თავდაცვის სამინისტროს წამყვანი ადგილი უკავია იმ სტრატეგიების

[110] იქვე.

შემუშავების პროცესში, რომლებიც კიბერუსაფრთხოების რისკების მართვის ეფექტურობის ამაღლებას ისახავს მიზნად. სამინისტროს სადაზვერვო სააგენტოები მნიშვნელოვან როლს ასრულებენ ინფორმაციული უსაფრთხოების სფეროში არსებული გამოწვევების შემცირების პროცესში. ამ კუთხით განსაკუთრებით აღსანიშნავია „სამთავრობო კომუნიკაციების შტაბის“ საქმიანობა, რომელიც პასუხისმგებელია მთავრობის ინფორმაციული სისტემების, კომუნიკაციებისა და კრიტიკული ინფრასტრუქტურის უსაფრთხოების დაცვაზე. დიდ ბრიტანეთში 2012 წლის აპრილიდან თავდაცვის სამინისტროს დაქვემდებარებაშია „კიბერ-ოპერაციებისგან თავდაცვის ჯგუფი“ (Defence Cyber Operations Group), რომელსაც პასუხისმგებლობა ეკისრება თავდაცვის სექტორში კიბერშესაძლებლობების განვითარებაზე, ოპერაციების ეფექტურობის ამაღლებასა და კიბერსივრცეში უსაფრთხოების დონის ზრდაზე.“ [111]

ისევე როგორც სხვა სახელმწიფოებმა ბრიტანეთის თავდაცვის სამინისტრომაც „დააფუძნა გლობალური ოპერაციების და უსაფრთხოების კონტროლის ცენტრი“. ცენტრის საქმიანობა ორიენტირებულია შეიარაღებული ძალებისთვის ინფორმაციული თავდაცვის უზრუნველყოფაზე; მის დაქვემდებარებაში მყოფი სტრუქტურული ერთეული (Joint Cyber Unit) შეიმუშავებს ტექნიკურ საშუალებებს და იღებს პროაქტიულ ზომებს იმ საფრთხეების აღმოსაფხვრელად, რომელიც ემუქრება თავდაცვის სექტორის კიბერსივრცეს. ბრიტანეთში მოქმედი კომპიუტერულ ინციდენტზე დახმარების 17 ჯგუფიდან - 1 უშუალოდ ექვემდებარება თავდაცვის უწყებას (MODCERT — Ministry of Defence Computer Emergency Response Team). აღნიშნული ჯგუფი, თავის მხრივ, აერთიანებს შემდეგ სტრუქტურულ ქვედანაყოფებს: უსაფრთხოების კოორდინაციის ცენტრს, მონიტორინგისა და ანგარიშგების ცენტრებს, რჩევის და გაფრთხილების ერთეულებს და უსაფრთხოების ინციდენტზე პასუხის მცირე ჯგუფებს.“ [112]

„შვეიცარია - შვეიცარიის ფედერალურმა ადმინისტრაციამ ბოლო წლებში აქტიური ზომები გაატარა კიბერშეტევების საწინააღმდეგო საშუალებების და ინფორმაციული ინფრასტრუქტურის დაცვის გაძლიერების მიზნით. სხვადასხვა ორგანოები ფედერალურ დონეზე ჩართული არიან კიბერ-უსაფრთხოებასთან დაკავშირებული პრევენციული და რეაქტიული ამოცანების გადაწყვეტაში.“ [113]

თავდაცვის სფეროში ინფორმაციული უსაფრთხოების პოლიტიკის განსაზღვრასა და იმპლემენტაციაში მონაწილეობს შვეიცარიის თავდაცვის სამინისტროს დაქვემდებარებაში მყოფი 3 ორგანო:

1. „ინფორმაციული უსაფრთხოების და ობიექტთა დაცვის ინსტიტუტი“ (Information Security and Facility Protection Institute (ISFP). იმისათვის, რომ უზრუნველყოს ინფორმაციის და ინფორმაციული სისტემების კონფიდენციალურობის, ხელმისაწვდომობის, ერთიანობის და განგრძობადობის დაცულობა, აღნიშნული ინსტიტუტი შეიმუშავებს ინფორმაციული უსაფრთხოების რეგულაციებს. ზოგადად, ინსტიტუტი წარმოადგენს კიბერ-უსაფრთხოებასთან დაკავშირებული საკითხების გადაწყვეტის მთავარ ეროვნულ ორგანოს და წამყვან როლს ასრულებს შვეიცარიის ფედერაციული ადმინისტრაციის ინფორმაციული უსაფრთხოების შესახებ კანონმდებლობის დახვეწაში.“ [114]
2. „შეიარაღებული ძალების სარდლობის მხარდაჭერის ორგანიზაცია Armed Forces Command Support

[111] იხ. ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07-3/255, 19.09.13) ელ. გევრდი ნანახია 06.06.2019

[112] იქვე.

[113] იქვე.

[114] იქვე.

Organisation (CSO). ორგანიზაციასთან ფუნქციონირებს კომპიუტერული ქსელური ოპერაციების მართვაზე პასუხისმგებელი ორგანო – ელექტრონული ოპერაციების ცენტრი; ცენტრი აანალიზებს საფრთხეებსა და ინციდენტებს, რის შემდეგაც ახდენს შესაბამის რეაგირებას. აღნიშნული ორგანიზაცია (CSO) ასევე მართავს სამხედრო სფეროში კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს (Military Computer Emergency Response Team (milCERT), რომელიც მონიტორინგს უწევს შეიარაღებული ძალების ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის დაცულობას.“ [115]

3. „სამხედრო სადაზვერვო სამსახური (Military Intelligence Service (MIS) – პასუხისმგებელია სამხედრო ინფორმაციის მოპოვებაზე, თანამშრომლობს გაერთიანებულ შტაბთან და ქმნის ოპერაციებისთვის საჭირო სადაზვერვო ბაზას. ორგანიზაცია უზრუნველყოფს ფედერალურ სადაზვერვო სამსახურს კიბერ-რისკებთან დაკავშირებული ინფორმაციისა და სამხედრო კვლევების მიწოდებით.“ [116]

იტალია – იტალიელი მეცნიერის ჯუზეპე კორასანიტის აზრით, „ევროპის საბჭოს კონვენცია აბსტრაქტულ კანონმდებლობას არ წარმოადგენს, ის კიდევ უფრო ეფექტური გახდება მას შემდეგ, როცა წაიშლება საზღვარი და ყველა ქვეყანა მოახდენს მის რატიფიცირებას.“

უნდა აღინიშნოს, რომ იტალიური კანონმდებლობა ჯერ კიდევ 1993 წლიდან ითვალისწინებდა სასჯელს კომპიუტერულ სისტემაში უნებართვო შეღწევისთვის, კომპიუტერული თაღლითობისთვის, კომპიუტერული მონაცემის გადაცემის ხელყოფისთვის და ა.შ. იტალია კონვენციას სრულად კი მართალია შეუერთდა, ანუ საკუთარ კანონმდებლობაში გადაიტანა ყველა ის პრინციპი და ტერმინი, რომელიც კონვენციამ განსაზღვრა,[117] მაგრამ – იტალიაში კიბერდანაშაულის შესახებ კონვენცია ძალაში შევიდა 2008 წლის 1 ოქტომბრიდან.

იტალიური სისხლის სამართლის კოდექსში გვაქვს რეგულაცია, რომლითაც იტალიური სისხლის სამართლის კოდექსი ჰგავს გერმანულ სისხლის სამართალს ციფრული დანაშაულის სფეროში, კერძოდ, იტალიის სისხლის სამართლის კოდექსით სანქცირებულია კომპიუტერული თაღლითობა, კერძოდ; აღნიშნული გულისხმობს ელექტრონული ხელმოწერის უკანონო გამოყენებას, რომლის საშუალებითაც დამნაშავე საკუთარი ან სხვა პირისათვის იღებს შემოსავალს არალეგალური გზებით, აღნიშნული მუხლი მსგავსებაშია გერმანიის სსკ-ის 263ა მუხლთან, რომლის მიხედვითაც 5 წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით ისჯება პირი, რომელიც საკუთარი თავისათვის ან მესამე პირისათვის მართლსაწინააღმდეგო გზით ქონებრივი სარგებლის მიღების განზრახვით, სხვა პირის ქონებას იმით აზიანებს, რომ მონაცემთა დამუშავებით მიღებულ შედეგს მოიპოვებს რამდენიმე გზით; პროგრამის არასწორად აწყობის საფუძველზე, არასწორი ან არასრულყოფილი მონაცემების გამოყენების საფუძველზე, მონაცემების არაავტორიზებული გამოყენებით ან არასანქცირებული ზეგავლენით პროგრამის მოქმედების პროცესში.

იტალიის სისხლის სამართლის კოდექსის 640-IV მუხლით (თაღლითობის) გათვალისწინებული ქმედების სუბიექტი შეიძლება იყოს მხოლოდ ელექტრონული ხელმოწერის გამოყენებაზე უფლებამოსილი პირი. ეს განსაკუთრებული სიახლეა, რადგან მსოფლიოში ელექტრონული ხელ-

---

115 ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07-3/255, 19.09.13) ელ. გევრდი ; ნანახია 06.06.2019

116 იქვე.

117 უჩა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2013 წ. გვ. 122-123. ელ. გვერდი ; ნანახია 06.06.2019 წელი.

მოწერის გამოყენება აქტიურად ხდება. შესაბამისად, გაზრდილია მისი გაყალბების საფრთხეც და სწორედ ამიტომ იტალიელმა კანონმდებელმა გადაწყვიტა ქმედების კრიმინალიზაცია. უნდა აღინიშნოს, რომ მსგავსი დანაშაულის გავრცელების საფრთხე საქართველოს ჯერ არ ემუქრება, რადგან ელექტრონული ხელმოწერა, როგორც ოფიციალური იურიდიული მოქმედება, ჯერაც არაა ფართოდ გავრცელებული. იტალიის სისხლის სამართლის კოდექსის 635-ბის მუხლით დასჯადია კომპიუტერის ან კომპიუტერული სისტემის მუშაობის შეფერხება. სისხლისსამართლებრივი პასუხისმგებლობა განსაზღვრულია იმ პირისთვის, რომელმაც დაამზადა ან გაავრცელა ისეთი მოწყობილობა ან კომპიუტერული პროგრამა რომელიც უზრუნველყოფს კომპიუტერულ სისტემაში უნებართვო შეღწევას. იტალიელი კანონმდებლის მიერ კომპიუტერის, კომპიუტერული სისტემის და კომპიუტერული მონაცემის დაზიანებისთვის დამამძიმებელ გარემოებად გათვალისწინებულია დაშინება და შანტაჟი, ან თუ ქმედება კომპიუტერული ქსელის ოპერატორის მიერ ანგარებითაა ჩადენილი.“ [118]

„ჩეხეთის რესპუბლიკა — აღნიშნულ სახელმწიფოში ინფორმაციული უსაფრთხოების უზრუნველყოფის პოლიტიკაში ჩართული არიან შემდეგი სახელმწიფო ორგანოები: კიბერ-უსაფრთხოების დეპარტამენტი (ექვემდებარება შინაგან საქმეთა სამინისტროს), ეროვნული უშიშროების საბჭო, ვაჭრობისა და ინდუსტრიის სამინისტრო, ჩეხეთის ინფორმაციული უსაფრთხოების სამსახური და სხვ. კრიტიკული ინფრასტრუქტურის და ინფორმაციული სისტემების დაცვის კუთხით, ჩეხეთში მთავარ უწყებას წარმოადგენს შინაგან საქმეთა სამინისტრო, რომელიც ამავე დროს პასუხისმგებელია ინფორმაციული უსაფრთხოების პოლიტიკის კოორდინაციაზე. 2010 წელს ჩეხეთის მთავრობის გადაწყვეტილებით შინაგან საქმეთა სამინისტროსთან შეიქმნა უწყებათაშორისო ორგანო „კიბერუსაფრთხოების საკოორდინაციო საბჭო“. საბჭოს თავმჯდომარეობს შინაგან საქმეთა მინისტრი, წევრებს შეადგენენ ჩეხეთის პოლიციის, თავდაცვის სამინისტროს, ტელეკომუნიკაციების ოფისის, ეროვნული უსაფრთხოების ორგანოს, ინფორმაციული სამსახურის, სამხედრო დაზვერვის და სხვა უწყებების წარმომადგენლები. საბჭოს მიზანია კიბერუსაფრთხოების სფეროში შინაგან საქმეთა სამინისტროს კომპეტენციის გამყარება და მისი, როგორც მაკოორდინირებელი ორგანოს, როლის მხარდაჭერა.“ [119]

„შვედეთში ფუნქციონირებს „ეროვნული თავდაცვის რადიო-დაწესებულება“ (National Defence Radio Establishment), რომლის საქმიანობას ორგანიზებას უწევს შვედეთის თავდაცვის სამინისტრო. აღნიშნული დაწესებულება სამთავრობო ორგანოებს აწვდის როგორც მიმდინარე კიბერ-საფრთხეების შესახებ ინფორმაციას, ასევე ზოგად რჩევებს უსაფრთხოების გარემოს გაუმჯობესების მიმართულებით. შვედეთში აგრეთვე მოქმედებს თავდაცვის სამინისტროსადმი ანგარიშვალდებული ორგანო „თავდაცვის საკითხების კვლევის სააგენტო“, რომლის ერთ-ერთი ფუნქციაა კიბერ-საფრთხეების შესახებ კვლევების წარმოება და შედეგების თაობაზე შვედეთის თავდაცვის სამინისტროს ინფორმირება.“ [120]

„საფრანგეთი – საფრანგეთში თითოეული სამინისტრო მისი კომპეტენციის სფეროში ახდენს

---

[118] უჩა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2013 წ. გვ.122-123. ელ. გვერდი ; ნანახია 06.06.2019 წელი.

[119] იხ. ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07-3/255, 19.09.13) ელ. გევრდი ; ნანახია 06.06.2019

[120] იქვე.

ინფორმაციულ უსაფრთხოებასთან დაკავშირებული რისკების ანალიზს. 2009 წელს საფრანგეთის მთავრობის გადაწყვეტილებით შეიქმნა „ქსელური და ინფორმაციული უსაფრთხოების სააგენტო“ (The French Network and Information Security Agency), რომელიც ინფორმაციული სისტემების დაცვის უზრუნველყოფაზე პასუხისმგებელ მთავარ ეროვნულ ორგანოს წარმოადგენს. სააგენტოს ფუნქციებია: კიბერ-შეტევების დაფიქსირება და სწრაფი რეაგირება, სამთავრობო ქსელებზე მუდმივი მეთვალყურეობა, საფრთხეების პრევენცია, მთავრობის ორგანოებისთვის და კრიტიკული ინფრასტრუქტურის ოპერატორებისთვის მხარდაჭერის აღმოჩენა და რჩევების მიცემა, კომპანიების და საზოგადოების ინფორმირება ინფორმაციული უსაფრთხოების გამოწვევების შესახებ. აღნიშნული სააგენტოს დაქვემდებარებაშია ინფორმაციული სისტემების უსაფრთხოების ოპერატიული ცენტრი (Operational Centre for Information Systems Security — COSSI), რომელიც ახდენს სამთავრობო უწყებების წინაშე მდგარი კიბერ-საფრთხეების პრევენციას, გამოვლენას და აღმოფხვრას, ასევე კრიზისული სიტუაციების მართვის კოორდინირებას.“[121]

„საფრანგეთში აგრეთვე ფუნქციონირებს ინფორმაციულ ტექნოლოგიებთან და კომუნიკაციებთან დაკავშირებული დანაშაულის წინააღმდეგ ბრძოლის ცენტრალური ოფისი. მისი ფუნქციაა ლოკალურ და რეგიონულ დონეზე პოლიციის დახმარება, რაც გამოიხატება კიბერსივრცეში არსებული გამოძიებების წარმოებაში, ინფორმაციული უსაფრთხოების შესახებ საკითხების ანალიზში, მონაცემთა შეგროვებაში და კიბერ-დანაშაულთან დაკავშირებული სხვა საჭიროებების უზრუნველყოფაში.“ [122]

„ესტონეთი — თერთმეტი წლის წინ, ესტონეთი გახდა პირველი ქვეყანა მსოფლიოში, სადაც თანამედროვე ტიპის კიბერ-შეტევები ვიხილეთ. კიბერ-თავდამსხმა რუსეთიდან განხორციელდა. ამ შემთხვევამ ესტონეთი სამუდამოდ შეცვალა. ესტონეთმა თავდასხმის შემდეგ ციფრული რევოლუცია განიცადა. დღეისათვის, ყოფილი საბჭოთა რესპუბლიკა მსოფლიოში ტექნოლოგიურად ერთერთი ყველაზე განვითარებულია. ესტონეთის ციფრული გარდაქმნების ერთ-ერთი ცენტრალური რეფორმა „X-Road-ის» პლატფორმაა, რომელიც სხვადასხვა მომსახურებას აერთიანებს, და მთავრობას მოქალაქეებთან აკავშირებს. პლატფორმას იყენებენ წამყვანი კერძო კომპანიებიც. პლატფორმის გამოყენებით მოქალაქეებს შეუძლიათ ისეთი მომსახურების მიღება როგორიცაა ჯანდაცვა, საბანკო ოპერაციები, გადასახადების გადახდა, სამართალდაცვა, და განათლება. ბოჭკოვანი ქსელი მთელს ქვეყანას აკავშირებს. კანონდებლებს შეუძლიათ ელექტრო-კაბინეტის პროგრამის გამოყენებით, ციფრულად მიიღონ კანონები. ხოლო მოქალაქეებს აქვთ საშუალება ონლაინ ხმის მიცემის მეშვეობით აირჩიონ პოლიტიკოსები და იყვნენ მათთან კავშირზე.“ [123]

„ციფრული ტექნოლოგიების გამოყენების ერთ-ერთი სარგებელი თანხების დაზოგვაა. ჩვენ ყოველ წელს მთლიანი შიდა პროდუქტის 2 პროცენტს ვზოგავთ ხარჯების ნაწილში, მათ შორის ხელფასებზე. ჩვენ ბიუროკრატია შევზღუდეთ. ბიუროკრატია თითქმის აღარ არსებობს. ეს დეცენტრალიზებული ინფორმაციული სისტემაა, რომელიც 1200 დაცულ და უსაფრთხო სისტემას აკავშირებს ერთმანეთთან“, – ამბობს მარტენ კაევატსი, პრემიერ-მინისტრის მრჩეველი ციფრულ საკითხებში. ლინარ ვიიკი ელექტრონული მთავრობის სააგენტოს დამფუძნებელია, ის 2007

---

121 იხ. ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07-3/255, 19.09.13) ელ. გევრდი ; ნანახია 06.06.2019

122 იქვე.

123 სტატია ესტონეთის ციფრული რევოლუცია ელ გვერდი ნანახია 06.06.2019.

წელ ესტონეთზე კიბერ თავდასხმის დროს მთავრობის ციფრული მრჩეველი იყო. მისი თქმით, თავდასხმა დიდხანს არ გაგრძელებულა და მისი სამიზნე ძირითადად უცხოურ პარტნიორებთან კრიტიკული კომუნიკაცია იყო.“ [124]

3.2 ციფრულ დანაშაულთან ბრძოლის სამართლებრივი რეგულაციები ამერიკის შეერთებული შტატებში

ამერიკის შეერთებული შტატები არის ერთ–ერთი მოწინავე ციფრული დანაშაულის გამოძიების და აღნიშნული დანაშაულის ბრძოლის წინააღმდეგ განხორციელებულ რეგულაციებში, ასევე აშშ არის ერთ–ერთი მოწინავე, რომელმაც კომპიუტერის შექმნის საწყისი წლებიდანვე დაიწყო ბრძოლა რათა აღნიშნული გამოყენებული არ ყოფილიყო დანაშაულის ჩასადენად, კერძო; „კომპიუტერული დანაშაული ყურადღების ცენტრში პირველად აშშ–ში XX საუკუნის 70იან წლებში მოექცა. ნაციონალურ და საერთაშორისო დონეზე დაიწყო ამ ფენომენის გამოკვლევა. მიღებულ იქნა სპეციალური ნორმები კიბერდანაშაულის მოსაწესრიგებლად. აშშში ჯერ კიდევ 1977 წელს შეიმუშავეს კანონპროექტი “ფედერალური კომპიუტერული სისტემების დაცვის შესახებ”, რომელიც ითვალისწინებდა სისხლისსამართლებრივ პასუხისმგებლობას ისეთი ქმედებისთვის, როგორიცაა: კომპიუტერულ სისტემაში ცრუ მონაცემების შეყვანა, კომპიუტერული მოწყობილობის უკანონო გამოყენება, ფულადი სახსრების მითვისება კომპიუტერული ტექნოლოგიების და კომპიუტერული ინფორმაციის მეშვეობით და სხვ. ამ კანონპროექტის საფუძველზე 1984 წლის ოქტომბერში მიღებულ იქნა „კომპიუტერული თაღლითობის და კომპიუტერის ბოროტად გამოყენების შესახებ“ კანონი. კომპიუტერული დანაშაულის წინააღმდეგ აქტიური ბრძოლის დასაწყებად კი ამერიკის შეერთებულ შტატებში ექსპერტები გამოყოფენ სამ შემთხვევას, რომლებმაც ცხადი გახადა, რომ ახალი კომპიუტერული და სატელეკომუნიკაციო ტექნოლიგიები დიდ პრო ბლემებს შეუქმნიდა სამართალდამცავ ორგანოებს. საყოველთაო „კომპიუტინგი“[125] მარტო ცხოვრების წესის შეცვლას კი არ ნიშნავდა, არამედ შეიცვლებოდა კრიმინალების მიერ დანაშაულებრივი საქმიანობის წარმართვის სპეციფიკაც.“ [126]

„მაგალითისთვის მოვიყვანოთ ზემოაღნიშნული სამი შემთხვევა:

1. 1986 წელს კალიფორნიის უნივერსიტეტის ასტრონომს დაევალა არასასიამოვნო, მაგრამ აშკარად მცირე მნიშვნელობის პრობლემის გადაჭრა უნივერსიტეტის კომპიუტერულ ლაბორატორიაში. უნივერსიტეტი ამუშავებდა ორ საბუღალტრო პროგრამას, რომლიც აღრიცხავდა კომპიუტერების გამოყენებას და არეგისტრირებდა მათ მომხმარებლებს. ვინაიდან, ამ პროგრამით ხდებოდა თანხებთან დაკავშირებით ერთი და იმავე ინფორმაციის დაფიქსირება, მათი შედეგიც ერთნაირი უნდა ყოფილიყო. თუმცა, გაურკვეველი მიზეზით სხვაობამ 75 აშშ დოლარი შეადგინა. გამოძიების ფედერალურმა ორგანოებმა უარი განაცხადეს საქმის გამოძიებაზე იმ მოტივით, რომ 75 დოლარიანი დანაკარგი უმნიშვნელო იყო, მაგრამ ასტრონომმა კლიფორდ სტოლმა თავად დაიწყო გამოძიება. ის იწერდა ჰაკერის მოქმედებებს და მუშაობდა როგორც ადგილობრივ ასევე უცხოურ სატელეფონო კომპანიებთან, რათა

[124] სტატია ესტონეთის ციფრული რევოლუცია ელ გვერდი ნანახია 06.06.2019.

[125] „კომპიუტინგი“ ტერმინი — კომპიუტერების მასშტაბური ინტეგრაცია ყოველდღიურ ცხოვრებაში.

[126] უჩა ზაქაშვილი. ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2014 წელი. გვ.15–16

დაედგინა თავდასხმის წყარო. აღმოჩნდა, რომ გერმანელ ჰაკერს მარკუს ჰესს აფინანსებდა რუსეთის სახელმწიფო უსაფრთხოების კომიტეტი, რათა გაემჟღავნებინა აშშს სამხედრო საიდუმლოება. ამრიგად, ეს იყო მნიშვნელოვანი გაკვეთილი როგორც სამართალდამცავი ორგანოების, ასევე დაზვერვის სამსახურისთვის. პირველ რიგში, ცხადი გახდა, რომ ქსელური ინფორმაცია არ იყო დაცული მასში უნებართვო შეღწევისგან და მეორე — ფინანსური ზარალი ყოველთვის არ განსაზღვრავს ხელყოფის სერიოზულობას და ინფორმაცია კიბერდანაშაულის შესახებ არ უნდა შემოწმდეს მხოლოდ ფინანსური ზარალის მიხედვით;

2. ეორე შემთხვევა დაკავშირებული იყო კომპიუტერულ ვირუსთან ე.წ. მორისის მატლთან. 1988 წელს ქორნელის უნივერსიტეტის სტუდენტმა რობერტ მორისმა შექმნა პროგრამა ინტერნეტის მეშვეობით კომპიუტერში შესაღწევად. მას შემდეგ რაც კომპიუტერული ვირუსი შეაღწევდა სამიზნე კომპიუტერში იგი დაიკავებდა კომპიუტერის მეხსიერებას, რაც გამოიწვევდა კომპიუტერის გამორთვას. სანამ კომპიუტერული ვირუსი გაუვნებელყოფილ იქნა, მან დააზიანა დაახლოებით 6200 კომპიუტერი და გამოიწვია 98 მილიონ დოლარზე მეტი ზარალი;

3. მესამე მაგალითი ეხება 1989 წლის თავდასხმას კომპანია „ბელსაუსზე“, რომელიც განხორციელდა „სიკვდილის ლეგიონის“ სახელით ცნობილი ჰაკერთა ჯგუფის მიერ. მათთვის შესაძლებელი გახდა ადგილობრივ სატელეფონო სისტემაში ცვლილებების შეტანა და მონაცემების განადგურება.“ [127]

„ასევე აღსანიშნავია, რომ, კიბერუსაფრთხოების პირველი სტრატეგია შემუშავებულ იქნა ამერიკის შეერთებულ შტატებში 2000 წლების დასაწყისში. შეერთებული შტატები გახდა ის ქვეყანა, რომელმაც დაიწყო კიბერუსაფრთხოების აღქმა, როგორც სახელმწიფო მნიშვნელობის საკითხი. 2003 წელს შეერთებულ შტატებში გამოქვეყნდა კიბერსივრცის უსაფრთხოების ეროვნული სტრატეგია (National Strategy to Secure Cyberspace). მოცემული დოკუმენტი წარმოადგენს უფრო ფართო ეროვნული უსაფრთხოების უზრუნველყოფის სტრატეგიის ნაწილს (National Strategy for Homeland Security), რომელიც შეიქმნა 2001 წლის 11 სექტემბრის ტერორისტული შეტევის პასუხად.“ [128]

„ამავე აქტის 814-ე მუხლით ცვლილება შევიდა კანონთა კრებულის მე18 ტიტულის 1030-ე მუხლში, რომელიც ეხება ცალკეულ კომპიუტერულ დანაშაულს. ამ ცვლილების შედეგად კომპიუტერული დანაშაულისთვის დადგენილი სასჯელის მაქსიმალური ზღვარი გაიზარდა და პირველად ჩადენილი დანაშაულისთვის გახდა თავისუფლების აღკვეთა 10, განმეორებითისთვის კი 20 წლამდე.“ „[..] ცვლილების შემდეგ ამერიკაში ქმედების დანაშაულად კვალიფიკაციისთვის აუცილებელი გახდა დამნაშავის მიზნის დადგენა, მასში განისაზღვრა ზიანის ცნება და იგი ჩამოყალიბდა, როგორც «მონაცემთა, სისტემის, პროგრამის ან ინფორმაციის მთლიანობის ნებისმიერი დაზიანება». ამერიკელი კანონმდებელი დასჯადად აცხადებს კომპიუტერულ სისტემაში არასანქცირებულ შეღწევას, მასში უნდა ვიგულისხმოთ, სანქცირებული შესვლის ფარგლების გადამეტებაც. კანონმდებელმა განსაზღვრა კომპიუტერული ჯაშუშობის ცნება, რომელიც გულისხმობს პირის მიერ კომპიუტერულ სისტემაში არასანქცირებული შეღწევას ან სანქცირებულ შესვლის ფარგლების გადამეტებას, ასევე ისეთი ინფორმაციის მოპოვებას, რომელსაც კავშირი აქვს სახელმწიფო უსაფრთხოების, საერთაშორისო ურთიერთობის და ატომური ენერგიის საკითხთან.,“ „[...] გარდა ზემოაღნიშნულისა, დასჯადია კომპიუტერული თაღლითობა, ესე იგი თაღლითური განზრახვით

[127] სამივე შემთხვევა — უჩა ზაქაშვილი. ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2014 წელი. გვ.15-16

[128] ვლადიმერ ცერცვაძე, “კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“ გვ. 42/131 ელ. გვერდი https://gipa.ge/uploads/files/Cyber_Protection.pdf ნანახია 06.06.2019

და უკანონო სარგებლის მიღების მიზნით კომპიუტერულ სისტემაში შეღწევა.“ „[...] აღსანიშნავია, რომ აშშ-ს ყველა შტატს გააჩნია საკუთარი ნორმატიული აქტი კომპიუტერული დანაშაულის რეგულირებასთან დაკავშირებით და ხშირად მათი შინაარსი განსხვავდება ფედერალური კანონმდებლობით დადგენილი დანაშაულებრივი შემადგენლობებისგან. მაგალითად, თუ ზოგიერთ შტატში სისხლისსამართლებრივი პასუხისმგებლობა უკავშირდება დამნაშავის მიზანს, ზოგიერთ შტატში მას განაპირობებს ის გარემოება, არასანქცირებული შეღწევის შედეგად დაკარგულ ინფორმაცია ექვემდებარება თუ არა აღდგენას. იმ შემთხვევაში, თუ განადგურებული ინფორმაციის აღდგენა შესაძლებელია, დამნაშავე თავისუფლდება სისხლისსამართლებრივი პასუხისმგებლობისგან. ასევე საინტერესოა, რომ იუტას შტატში დასაშვებია ორგანიზაციის მიერ კომპიუტერული თავდასხმა იმ კომპიუტერულ ქსელზე ან სისტემაზე, რომლიდანაც ცდილობდნენ არასანქცირებული შეღწევის განხორციელებას მათ კომპიუტერში ან სისტემაში[129].“

3.3 ციფრულ დანაშაულთან ბრძოლის სამართლებრივი რეგუ ლაციები რუსეთის ფედერაციაში

რუსეთის ფედერაცია იყო ერთ-ერთი ყველაზე ბოლო სახელმწიფო, რომელმაც მისი სისხლის სამართლის კანონმდებლობით გახადა დასჯადი ციფრული დანაშაული, „რუსეთის სისხლის სამართლის კოდექსში ამ მიმართულებით მნიშვნელოვანი ცვლილებები შევიდა 2011 წელს.

ცვლილებების შედეგად შეიცვალა და 272-ე, 273-ე და 274-ე მუხლები. 272-ე მუხლებით დასჯადი გახდა „კანონით დაცულ კომპიუტერულ ინფორმაციაში არამართლზომიერი შეღწევა, თუ ამ ქმედებამ გამოიწვია კომპიუტერული ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან კოპირება. მუხლის მე-2 ნაწილში დამამძიმებელ გარემოებად განსაზღვრულია 1-ლი ნაწილით გათვალისწინებული ქმედების ჩადენა ანგარებით ან თუ ამ ქმედებამ გამოიწვია მნიშვნელოვან ზიანი. მუხლის შენიშვნაში მნიშვნელოვანი ზიანი განიმარტება, როგორც ზიანი, რომელიც აღემატება ერთ მილიონ რუბლს. 272-ე მუხლის მე-3 ნაწილი კიდევ უფრო ამძიმებს პასუხისმგებლობას მუხლის პირველი და მეორე ნაწილით გათვალისწინებული ქმედებისათვის, რომელიც ჩადენილია ჯგუფურად, ორგანიზებული ჯგუფის მიერ ან სამსახურებრივი მდგომარეობის გამოყენებით. მე-4 ნაწილი კი ადგენს პასუხისმგებლობას 272-ე მუხლის 1-ლი, მე-2 და მე-3 ნაწილით გათვალისწინებული დანაშაულისთვის თუ დადგა მძიმე შედეგი ან არსებობდა მისი დადგომის საფრთხე. ამავე მუხლის შენიშვნაში განსაზღვრულია კომპიუტერული ინფორმაციის ცნება: „კომპიუტერული ინფორმაცია“ არის მონაცემი რომელიც წარმოდგენილია ელექტრო სიგნალის ფორმით. მისი შენახვის, დამუშავების და გადაცემის ფორმას მნიშვნელობა არ აქვს. სავარაუდოდ რუს კანონმდებელს სურდა ტერმინი „კომპიუტერული მონაცემის ორიგინალური რეპროდუქცია''. კონვენციის მიხედვით კომპიუტერული მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით ინფორმაციის გამოსახვა, მათ შორის პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას. კომპიუტერული ინფორმაცია თავისთავად იგულისხმება ამ დეფინიციაში. გარდა ამისა, კომპიუტერული მონაცემის ქვეშ უნდა

[129] უჩა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2013 წ. გვ. 118-119. ელ. გვერდი ნანახია 06.06.2019 წელი.

ვიგულისხმოთ ნებისმიერი კომპიუტერული პროგრამაც. რუსული კანონმდებლის ვიწრო მიდგომა არასრულყოფილია, რადგან დანაშაული იწყება კომპიუტერულ სისტემაში უნებართვო შეღწევიდან და მხოლოდ ამის შემდეგ ხდება კომპიუტერული ინფორმაციის ხელყოფა. თუმცა, როგორც ჩანს, ეს გარემოება რუსეთში ყურადღების მიღმა დარჩა.“ [130]

„რუსი მეცნიერი პაველ დომკინი განმარტავს თუ რა უნდა ვიგულისხმოთ რუსეთის სისხლის სამართლის კოდექსის 272-ე მუხლის I ნაწილში მითითებულ ტერმინ «არამართლზომიერში»: არამართლზომიერი — ესე იგი კომპიუტერული ინფორმაციის ძებნის და მიღების დადგენილი წესის დარღვევით განხორციელებული ქმედება. კანონით დაცულ კომპიუტერულ ინფორმაციაში შეღწევა არამართლზომიერია, როდესაც ხდება ჩამოთვლილთაგან ერთ-ერთი წესის დარღვევა: ა) ინფორმაციის მოძებნა არაა ხელმისაწვდომი ყველასთვის; ბ) ინფორმაციაში შესვლას გააჩნია ტექნიკური შეზღუდვა, მაგალითად, პაროლი. გ) ინფორმაციის მიღების უფლებამოსილება ყველას არ გააჩნია; დ) კომპიუტერულ ინფორმაციაში შეღწევა შეუძლებელია ტექნიკური დაცვის საშუალების გადალახვის გარეშე. პ. დომკინი განმარტავს, რომ გარდა ზემოაღნიშნულისა, რუსული სასამართლო პრაქტიკა “არამართლზომიერ” შეღწევაში გულისხმობს შემდეგს: ვთქვათ, პირი არის კომპიუტერული სისტემის ადმინისტრატორი და გააჩნია კომპიუტერული ინფორმაციის მოძებნის და მიღების უფლება, მაგრამ სამსახურის შინაგანაწესით, გარკვეულ ინფორმაციაში შესვლა აკრძალული აქვს. იმ შემთხვევაში, თუ ის მაინც განახორციელებს ამ ტიპის ინფორმაციის კოპირებას, ის არამართლზომიერად შეაღწევს კომპიუტერულ ინფორმაციაში. ასევე, “არამართლზომიერ” შეღწევასთან გვექნება საქმე, როდესაც კომპიუტერული ინფორმაცია დაცულია რუსეთის კანონმდებლობით, ანუ იგი არის სახელმწიფო საიდუმლოება და კონფიდენციური ინფორმაცია. სახელმწიფო საიდუმლო განსაზღვრულია კანონით „სახელმწიფო საიდუმლოების შესახებ“ და მასში შედის სამხედრო, ეკონომიკური, სამეცნიერო, შიდა პოლიტიკასთან დაკავშირებული, კონტრდაზვერვის, ოპერატიულ-სამძებრო და სხვა ინფორმაცია. კონფიდენციური მონაცემებია: პერსონალური, საგამოძიებო და სამართალწარმოების მონაცემი, ასევე სამსახურებრივი საიდუმლო (განსაზღვრულია რუსეთის სამოქალაქო კოდექსით), საადვოკატო, საექიმო საიდუმლო, სატელეკომუნიაკციო კავშირის, პირადი მიმოწერის საიდუმლო, კომერციული საიდუმლო და ა.შ.“[131]

---

130 უჩა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2013 წ. გვ. 124-125. ელ. გვერდი [QR], ნანახია 06.06.2019 წელი.

131 იქვე.

კარი II
ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა

თავი IV
ციფრული მტკიცებულება

4.1. ციფრული მტკიცებულების რაობა და ადგილი მტკიცებულებათა კლასიფიკაციაში

წინა თავებში განმარტებულ იქნა ციფრული დანაშაულის არსი და მნიშვნელობა, მისი ობიექტური და სუბიექტური შემადგენლობა და ციფრული დანაშაულის ადგილი საქართველოს სისხლის სამართლის მატერიალური კანონმდებლობაში, მაგრამ იმისათვის, რომ სისხლის სამართლის კანონმდებლობა იყოს სამართლებრივ ჰარმონიაში, აუცილებელია, რომ სისხლის სამართლის პროცესმა მოგვცეს საშუალება — გამოიძიო სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაული და მიხვიდე შედეგამდე.

სწორედ აღნიშნული მიზნებიდან გამომდინარე, წარმოდგენილი თავი შეეხება ციფრული მტკიცებულების ადგილის განსაზღვრას სისხლის სამართლის პროცესში, მაინც სად არის აღნიშნულის ადგილი — რომელიმე მტკიცებულებათა ჯგუფში, თუ დამოუკიდებელი სახით?

მოქმედი საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის თანახმად, მტკიცებულება ეს არის — „კანონით დადგენილი წესით სასამართლოში წარდგენილი ინფორმაცია, ამ ინფორმაციის შემცველი საგანი, დოკუმენტი, ნივთიერება ან სხვა ობიექტი, რომლის საფუძველზედაც მხარეები სასამართლოში ადასტურებენ ან უარყოფენ ფაქტებს, სამართლებრივად აფასებენ მათ, ასრულებენ მოვალეობებს, იცავენ თავიანთ უფლებებსა და კანონიერ ინტერესებს, ხოლო სასამართლო ადგენს, არსებობს თუ არა ფაქტი ან ქმედება, რომლის გამოც ხორციელდება სისხლის სამართლის პროცესი, ჩაიდინა თუ არა ეს ქმედება გარკვეულმა პირმა, დამნაშავეა თუ არა იგი, აგრეთვე გარემოებებს, რომლებიც გავლენას ახდენს ბრალდებულის პასუხისმგებლობის ხასიათსა და ხარისხზე, ახასიათებს მის პიროვნებას. დოკუმენტი მტკიცებულებაა, თუ ის შეიცავს სისხლის სამართლის საქმის ფაქტობრივი და სამართლებრივი გარემოებების დასადგენად საჭირო ცნობას. დოკუმენტად ითვლება ნებისმიერი წყარო, რომელშიც ინფორმაცია აღბეჭდილია სიტყვიერ-ნიშნობრივი ფორმით ან/და ფოტო-, კინო-, ვიდეო-, ბგერისა თუ სხვა ჩანაწერის სახით ან სხვა ტექნიკური საშუალების გამოყენებით.“ [132]

ზემოაღნიშნული მუხლიდან გამომდინარე გვაქვს რამდენიმე სახის მტკიცებულება, ესენია ინფორმაცია, ამ ინფორმაციის შემცველი საგანი, დოკუმენტი, ნივთიერება ან სხვა ობიექტი.

„ინფორმაცია — მისი შინაარსით მრავლის მომცველი ტერმინია, მაგალითისათვის ინფორმაციის შემცველი მტკიცებულებაა მოწმის მიერ სასამართლოსთვის მიცემული ჩვენება. აღსანიშნავია, რომ ნებისმიერი ინფორმაცია მტკიცებით ძალას იძენს სასამართლოში მტკიცებულებებით მისი დადასტურების შემდეგ;

ინფორმაციის შემცველი საგანი — მართალია კანონმდებელმა ნივთისგან განასხვავა საგანი რომელიც შეიცავს გარკვეულ ინფორმაციას, მაგრამ აღნიშნულის გამიჯვნა ნივთისგან მაინც რთულია, მაგალითისათვის ინფორმაციის შემცველ საგნად შესაძლოა განვიხილოთ ელექტრონული დისკი,

[132] საქართველოს სისხლის სამართლის საპროცესო კოდექსი 29.05.2019 წლის რედ.

რომელიც არის საგანი და შეიცავს ინფორმაციას მასში განთავსებული ვიდეო ჩანაწერის გამო, ასევე საგანი შესაძლოა გვაძლევდეს ნივთიერი მტკიცებულების იგივეობას;

ნივთიერი მტკიცებულება — ჩამონათვალი სანიმუშოა და მას შესაძლებელია ეწოდებოდეს ნებისმიერი საგანი/ნივთიერება/კვალი, რომელსაც მნიშვნელობა აქვს საქმისათვის. ამასთან, ნივთიერ მტკიცებულებას აღნიშნული საგნები წარმოადგენს იმ შემთხვევაში თუ მათი არსი და დანიშნულება გასაგებია ყოფითი აღქმისათვის, რაც შესაძლებელია გამოყენებულ იქნეს სასამართლოში საკუთარი პოზიციის დასადასტურებლად და რომელთა გადაცემა შესაძლებელია ხელიდან ხელში (რომელთა ფიზიკური დათვალიერებაა შესაძლებელი. მაგალითად, თითის ანაბეჭდი, რომელიც გადატანილია შესაბამის ლენტზე, დანაშაულის ჩასადენად გამოყენებული სამზარეულოს დანა, დაზარალებულის სისხლიანი პერანგი, აუდიო/ვიდეო ჩანაწერი და სხვა)." [133]

„ნივთიერ მტკიცებულებას წარმოადგენს ასევე სულიერი ცხოველი/არსება, რომელიც წარმოადგენდა დანაშაულის ჩადენის საგანს ან გამოყენებული იყო დანაშაულის ჩასადენად (მაგალითად, შინაური პირუტყვის ქურდობის შემთხვევაში, სხვისი ქონების (მსხვილფეხა პირუტყვის) განზრახ განადგურებისას და სხვა), თუმცა აღნიშნულის სხდომის დარბაზში წარდგენა დათვალიერებისათვის არ დაიშვება, ნივთიერ მტკიცებულებას არ წარმოადგენს მატერიალური სამყაროს ნივთები/საგნები, რომელთა აღქმა პროცესის მონაწილეების გრძნობის ორგანოების მიერ შეუძლებელია. მაგალითად, ნანონაწილაკები/ მიკრონაწილაკები, რომელთა დათვალიერება შესაძლებელია მხოლოდ მიკროსკოპის მეშვეობით და საჭიროებს სპეციალურ ცოდნას. მაგრამ ნივთიერ მტკიცებულებას წარმოადგენს შემთხვევის ადგილიდან ამოღებული შალითა, რომელზეც საექსპერტო კვლევის შედეგად აღმოჩენილი იქნება აღნიშნული ნანონაწილაკები, თუ ეს მიუთითებს საქმისათვის მნიშვნელოვან გარემოებაზე (მაგალითად, რომ ბრალდებული იქ იყო)." [134]

„დოკუმენტი — დოკუმენტს მტკიცებულებითი ძალა ენიჭება კუმულაციურად სამი სპეციალური წინაპირობის არსებობისას: 1. ცნობილია მისი წარმომავლობა; 2. ავთენტიკურია; 3. შესაძლებელია დაიკითხოს პირი რომელმაც შექმნა/მოიპოვა ან ვისთანაც ინახებოდა დოკუმენტი სასამართლოში წარდგენამდე, იგი შესაძლებელია არსებობდეს როგორც წერილობითი, ასევე ნებისმიერი სხვა ფორმით (აუდიო-ვიდეოჩანაწერი, კომპიუტერული ფაილების, სმს-ს, მმს-ის, მეხსიერების ბარათების სახით და ა.შ.), ოფიციალური/საქმიანი ქაღალდის, ასევე არაოფიციალური სახით, მაგალითად, საჯარო/ სამოქალაქო რეესტრიდან ამონაწერი, სანოტარო წესით დამოწმებული ნასყიდობის ხელშეკრულება, ცნობა ხელფასის შესახებ, ცნობა ნასამართლეობის შესახებ, ჯანმრთელობის ცნობა, ამონაწერი მობილური კავშირგაბმულობის ოპერატორისგან განხორციელებული სატელეფონო კომუნიკაციის (შემავალი-გამავალი ზარების ხანგრძლივობის, რაოდენობის, ლოკაციის, სიხშირის და ა.შ.), ინტერნეტ სერვის პროვაიდერის მიერ მიწოდებული ინფორმაცია ინტერნეტაქტივობის შესახებ, ე.წ. შინაურული ხელწერილი, მესიჯი, ელექტრონული წერილი, ფოტოსურათი, და ა.შ. (დოკუმენტის განმარტება, სსსკ მე-3 მუხლის 23-ე ნაწილი). ოფიციალური დოკუმენტები პირობითად შეიძლება დაიყოს თავის მხრივ ორ სახედ; 1. პროცესის მწარმოებელი ორგანოს მიერ შექმნილი (მაგალითად, საგამოძიებო მოქმედების ოქმები); 2. სხვა დაწესებულების

133 სამივე ტერმინი — ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციტივის მხარდაჭერით. 2015 წელი.გვ. 38-39

134 ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციტივის მხარდაჭერით. 2015 წელი.გვ. 38-39

ოფიციალური დოკუმენტაცია, რომელსაც გააჩნია საქმისათვის მნიშვნელოვანი ინფორმაცია პროცესში მისი არსებობა უკავშირდება პროცესის მონაწილის მიერ მის მოპოვებას გარეშე წყაროებიდან, ან პროცესის მონაწილის მიერ მის ნებაყოფლობით წარმოდგენას. მაგალითად, სსკ 177-ე მუხლით გათვალისწინებული დანაშაულით დაზარალებული პირის მიერ სალაროს აპარატის ჩეკის/ საგარანტიო ტალონის წარმოდგენა, რომლითაც დასტურდება მოპარული ნივთის მის საკუთრებაში არსებობა, ღირებულება, სერიული ნომერი, მარკა და ა.შ.“ [135]

ხოლო თავად „ციფრული მტკიცებულების რაობაზე როდესაც ვსაუბრობთ, პირველ რიგში განვიხილოთ მისი ზოგადი განმარტება; ციფრული მტკიცებულებები ან ელექტრონული მტკიცებულებები არის ციფრული ფორმით შენახული ან გადაცემული ნებისმიერი სავარაუდო ინფორმაცია, რომელიც სასამართლოში საქმის განხილვისას შეიძლება იქნეს გამოყენებული. ციფრული მტკიცებულებების მიღებამდე სასამართლო განსაზღვრავს, არის თუ არა მტკიცებულება შესაბამისი, ავთენტიკური, არის თუ არა ორიგინალი.“ [136]

„მტკიცებულებათა ჩამონათვალის საფუძველზე იბადება კითხვა – შედის თუარა ციფრული მტკიცებულება მისი ბუნებიდან გამომდინარე რომელიმე მტკიცებულებათა სამართლებრივ შემადგენლობაში, შესაძლოა ვივარაუდოთ, რომ ზემოაღნიშნულს მოიცავს დოკუმენტი, რადგანაც დოკუმენტი თავის თავში გარკვეულწილად მოიცავს ინტერნეტ სერვის პროვაიდერის მიერ მიწოდებული ინფორმაციას ინტერნეტ აქტივობის შესახებ, მესიჯებს, ელექტრონული წერილებს, ფოტოსურათებს, და ა. შ. აღნიშნულ ვარაუდს გვიმყარებს საფრანგეთის სამოქალაქო კოდექსი, რომელიც წერილობით მტკიცებულებებს აკუთვნებს ყველა სახის წერილებს, სიმბოლოებს, ციფრებს ან სხვა ნიშნებს, რომლებსაც აქვთ შინაარსი, მნიშვნელობა და მათი გაგება შესაძლებელია, მიუხედავად იმისა თუ რა ფორმით არიან ისინი გადმოცემული. როგორც ვხედავთ, ფრანგულმა კანონმდებელმა ფართოდ განმარტა წერილობითი მტკიცებულებები და მოიცვა როგორც კონკრეტული ისე აბსტრაქტული მონაცემები.“ [137]

მაგრამ, მივიჩნევთ, რომ ციფრული მტკიცებულება, როგორც მტკიცებულების სახე, მკაფიო დეფინიციასთან ერთად აუცილებლად უნდა იქნეს შეტანილი საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში, ვინაიდან 21-ე საუკუნე ციფრული ეპოქაა და როგორც ბიზნეს ასევე სხვა სახის კომუნიკაცია და ურთიერთობები ინტერნეტ სივრცეში და კომპიუტერულ ტექნიკაში წარმოებული დოკუმენტაციის საფუძველზე წარმოებს, უფრო მეტიც, ბრუნვაშია ელექტრონული ფული, შეიქმნა ხელოვნური ინტელექტი დ ა.შ.

როდესაც განვიხილავთ ციფრულ მტკიცებულებებს, უნდა ვაღიაროთ, რომ „ელექტრონული წერილობითი დოკუმენტაციის წარმოება [...] ამცირებს რისკებს, როგორიცაა: წერილობითი მტკიცებულებების ფალსიფიკაცია, გათეთრება, თაღლითობა და ა.შ. ამ ყველაფრის აღმოფხვრას ხელს უწყობს და აიოლებს მართლმსაჯულებაში ახალი ტექნოლოგიების დანერგვა. დღეს ყველაფერი უფრო უსაფრთხოდ და სანდოდ შეგვიძლია მივიჩნიოთ ვიდრე წლების წინ...

---

[135] ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციტივის მხარდაჭერით. 2015 წელი.გვ. 275

[136] ელ.გვერდი  ; ნანახია. 21.07.2019

[137] Fabien Kerbouci სტატია ელექტრონული მტკიცებულება — ახალი გამოწვევა ფრანგულ მართლმსაჯულებაში თარგმანი: თამთა მიქაია (თბილისის სააპელაციო სასამართლის თავმჯდომარის ბიუროს სტაჟიორი) ელ. გვერდი  ;

ელექტრონულად წარმოდგენილ მტკიცებულებების სუსტ მხარედ შეიძლება ჩაითვალოს, ასეთი სახით წარმოდგენილი ესა თუ ის ტექსტი, ტექსტური შეტყობინება (SMS) და ტელეფონის ზარი. ყველა ეს საშუალება ძალიან დაუცველი და არასანდოა, რაც ზრდის შეცდომის დაშვების რისკს და შესაძლებელია მოსამართლეს მასზე დაყრდნობით არასწორი წარმოდგენაც კი შეექმნას, რაც დღესდღეობით სერიოზულ პრობლემას წარმოადგენს და რასაც ხშირად მოსდევს უსამართლო გადაწყვეტილებები. თანამედროვე ტექნოლოგიები არ უნდა აძლევდეს მხარეებს მანიპულირების საშუალებას. შეჯიბრითობის პრინციპიდან გამომდინარე მხარეებს აქვთ სრული თავისუფლება თავად გადაწყვიტონ: რა სახის მტკიცებულებები წარმოადგინონ სასამართლოში და როგორც დაიცვან თავი, თუმცა აღსანიშნავია ის გარემოებაც რომ, არცერთ მტკიცებულებას არ აქვს წინასწარ დადგენილი ძალა და მხოლოდ მოსამართლეზეა დამოკიდებული, როგორ შეაფასებს მას.“ [138]

„საფრანგეთის სამოქალაქო კოდექსის 1316-ე მუხლის 1-ელი ნაწილი მიუთითებს რომ, ელექტრონული ფორმით დასაშვებია ისეთი მტკიცებულებები, რომლის გამომგზავნი პირი, გამცემი ორგანო ცნობილია და ინახება ისეთ პირობებში, რომელიც წარმოადგენს გარანტს მისი მთლიანობის. მისი ნამდვილობისთვის, ის დამოწმებული უნდა იყოს გამომგზავნის ელექტრონული ხელმოწერით, რომელიც უნდა აკმაყოფილებდეს კანონიერი უსაფრთხოების მოთხოვნებს (1316-ე მუხლის მე-4 ნაწილი). კომპიუტერული პროგრამების გამოყენებით კრიპტოგრაფიული ალგორითმები უზრუნველყოფენ დოკუმენტების მთლიანობასა და ნამდვილობას. ელექტრონული ხელმოწერის მიმართ მოქმედებს პრეზუმცია, იგი ითვლება სარწმუნოდ იქამდე, სანამ საწინააღმდეგო არ დამტკიცდება. მტკიცებულების გამოკვლევისას მოსამართლეს უფლება აქვს უხმოს ექსპერტს. ელექტრონული სახით შეიძლება წარმოდგენილი იყოს აუდიო, ვიდეო ფაილები, ფოტოები.“ [139]

ამდენად, ვფიქრობთ, რომ ციფრული მტკიცებულების ადგილი სამართლებრივ კლასიფიკაციაში უნდა იყოს დამოუკიდებელი და განსაზღვრული უნდა იყოს მტკიცებულების ერთ ერთ დამოუკიდებელ სახეობად.

---

[138] Fabien Kerbouci სტატია ელექტრონული მტკიცებულება — ახალი გამოწვევა ფრანგულ მართლმსაჯულებაში თარგმანი: თამთა მიქაია (თბილისის სააპელაციო სასამართლის თავმჯდომარის ბიუროს სტაჟიორი) ელ. გვერდი

[139] იქვე.

თავი V
ციფრული ინფორმაციის შემცველი მოწყობილობის ამოღების მეთოდიკა და ტექნიკა

5.1. ციფრული ინფორმაციის შემნახველი კომპიუტერული მოწყობილობის ამოღების სამართლებრივი საფუძვლები

არის შემთხვევები, როდესაც გამოძიების ინტერესებიდან გამომდინარე აუცილებელია არა კომპიუტერული სისტემიდან ინცორმაციის გამოთხოვა, არამედ თავად კომპიუტერის ამოღება, იმისათვის, რომ გამომძიებლის მიერ ჩატარებულ იქნეს აღნიშნული საგამოძიებო მოქმედება, აუცილებელია გამომძიებელი კარგად ფლობდეს საგამოძიებო მოქმედების სამართლებრივი საფუძვლებს და კომპიუტერის აგებულების იმ მნიშვნელოვან კომპონენტებს, რომელიც საჭიროა მსგავსი ხასიათის საგამოძიებო მოქმედების ჩასატარებლად.

არსებობს საგამოძიებო მოქმედების ჩატარების 3 სამართლებრივი შემთხვევა;

1. მესაკუთრის/მფლობელის წერილობითი თანხმობა;
2. პროკურორის დადგენილება – გადაუდებელი აუცილებლობის შემთხვევში;
3. სასამართლოს განჩინება;

განვიხილოთ თითოეული მათგანი;

მესაკუთრის/მფლობელის წერილობითი თანხმობა;

„მესაკუთრის, მფლობელის ან კომუნიკაციის ერთი მხარის თანხმობის შეფასებისას, ყოველ კონკრეტულ შემთხვევაში, ყურადღება უნდა მიექცეს იმას, თუ რა ტიპის საგამოძიებო მოქმედება ტარდება და რა არის საგამოძიებო მოქმედების ჩატარების მიზანი – საგამოძიებო მოქმედება დაკავშირებულია მხოლოდ საკუთრებაში ან მფლობელობაში შესვლასთან თუ საკუთრებიდან, მფლობელობიდან ან პირისგან იმავდროულად რაიმე ნივთის ამოღებასთან. ამოღების და ჩხრეკის ჩატარების დროს თანხმობის შეფასებისას აუცილებელია პირის თანხმობა არა მხოლოდ საგამოძიებო მოქმედების ჩატარებაზე, არამედ საგამოძიებო მოქმედების შედეგად ნივთის/ნივთების ამოღებაზე, ვინაიდან აღნიშნული საგამოძიებო მოქმედებების მიზანი დასაწყისშივე ნივთის ამოღებაა. უფრო კონკრეტულად, გამომძიებელმა, საგამოძიებო მოქმედების დაწყებამდე, პირს, ვისთანაც ატარებს საგამოძიებო მოქმედებას, უნდა განუმარტოს საგამოძიებო მოქმედების ჩატარების მიზნები, საფუძვლები, და მისი შედეგები. კერძოდ, გამომძიებელმა პირს უნდა აუხსნას, რომ საგამოძიებო მოქმედების მიზანია არა მხოლოდ ბინაში შესვლა, არამედ ბინიდან მტკიცებულების ამოღება. შესაბამისად, ბინის მესაკუთრემ თანხმობა უნდა განაცხადოს როგორც ბინაში გამომძიებლის შესვლაზე, ისე ბინიდან მტკიცებულების ამოღებაზე. წინააღმდეგ შემთხვევაში, სახეზე იქნება პირის თანხმობის გარეშე გადაუდებელი აუცილებლობით ჩატარებული საგამოძიებო მოქმედება, რომელსაც საერთო წესით სჭირდება დაკანონება.“ [140]

გადაუდებელი აუცილეობლობით ჩატარებული საგამოძიებო მოქმედება;

საქართველოს სისხლის სამართლის საპროცესო კოდექსის 112–ე მუხლის თანახმად; ‘’როდესაც დაყოვნებამ შეიძლება გამოიწვიოს გამოძიებისათვის მნიშვნელოვანი ფაქტობრივი მონაცემების

[140] ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციტივის მხარდაჭერით. 2015 წელი. გვ. 369-370

განადგურება ან როცა დაყოვნება შეუძლებელს გახდის აღნიშნული მონაცემების მოპოვებას, ან როცა საქმისათვის საჭირო საგანი, დოკუმენტი, ნივთიერება ან ინფორმაციის შემცველი სხვა ობიექტი აღმოჩენილია სხვა საგამოძიებო მოქმედების ჩატარებისას (თუ აღმოჩენილია მხოლოდ ზედაპირული დათვალიერების შედეგად), ან როცა არსებობს სიცოცხლის ან ჯანმრთელობის ხელყოფის რეალური საფრთხე, საგამოძიებო მოქმედება შეიძლება ჩატარდეს სასამართლოს განჩინების გარეშეც, რის შესახებაც მოსამართლეს, რომლის სამოქმედო ტერიტორიაზედაც ჩატარდა აღნიშნული საგამოძიებო მოქმედება, ან გამოძიების ადგილის მიხედვით მოსამართლეს პროკურორმა უნდა აცნობოს საგამოძიებო მოქმედების დაწყებიდან 24 საათის განმავლობაში და უნდა გადასცეს სისხლის სამართლის საქმის მასალები (ან მათი ასლები), რომლებიც ასაბუთებს საგამოძიებო მოქმედების გადაუდებლად ჩატარების აუცილებლობას. მოსამართლე მასალების შესვლიდან არა უგვიანეს 24 საათისა ზეპირი მოსმენის გარეშე წყვეტს შუამდგომლობას. მოსამართლე უფლებამოსილია შუამდგომლობა განიხილოს მხარეთა (თუ სისხლისსამართლებრივი დევნა დაწყებულია) და იმ პირის მონაწილეობით, რომლის მიმართაც ჩატარდა საგამოძიებო მოქმედება. შუამდგომლობის განხილვისას მოსამართლე ამოწმებს სასამართლო გადაწყვეტილების გარეშე ჩატარებული საგამოძიებო მოქმედების კანონიერებას. მოსამართლე უფლებამოსილია განმარტების მისაცემად გამოიძახოს ის პირი, რომელმაც საგამოძიებო მოქმედება სასამართლოს განჩინების გარეშე ჩაატარა. ამ შემთხვევაში შუამდგომლობის განხილვისას გამოიყენება ამ კოდექსის 206–ე მუხლით გათვალისწინებული წესი.“ [141]

სასამართლოს მიერ განჩინების გამოტანა;

„მასალების განხილვის შემდეგ სასამართლოს გამოაქვს განჩინება:

ა) ჩატარებული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ;

ბ) ჩატარებული საგამოძიებო მოქმედების უკანონოდ ცნობისა და მიღებული ინფორმაციის დაუშვებელ მტკიცებულებად ცნობის შესახებ.“ [142]

სასამართლოს განჩინებით ჩატარებული საგამოძიებო მოქმედება;

„მოსამართლის განჩინების გამოთხოვა ხორციელდება მხარის (ბრალდების და დაცვის) წერილობითი შუამდგომლობის საფუძველზე. შუამდგომლობა უნდა იყოს დასაბუთებული, მასში დეტალურად უნდა იყოს ჩამოყალიბებული მხარის მოთხოვნა, საგამოძიებო მოქმედების ჩატარების მიზანი და საფუძველი, ფაქტები და მათი დამადასტურებელი მტკიცებულებები, მსჯელობა და არგუმენტაცია ფაქტებსა და მტკიცებულებებზე, კანონი, რომელიც არგუმენტებს და მსჯელობას ამყარებს. მხარე ვალდებულია შუამდგომლობაში დაასაბუთოს მტკიცებულებათა იმ სტანდარტის (დასაბუთებული ვარაუდის) არსებობა, რომელსაც საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელ წინაპირობად მიიჩნევს საქართველოს სსსკ–ის მე–3 მუხლის მე–11 ნაწილი;“ [143]

მხარის შუამდგომლობა სტრუქტურულად სამი ნაწილისაგან უნდა შედგებოდეს: შესავალი, აღწერილობითი (სამოტივაციო) და სარეზოლუციო ნაწილებისგან.

„შუამდგომლობის შესავალ ნაწილში უნდა მიეთითოს:

- სასამართლოს დასახელება, რომელსაც მხარე მიმართავს შუამდგომლობით;
- შუამდგომლობის შედგენის ადგილი და თარიღი;

---

141 საქართველოს სისხლის სამართლის საპროცესო კოდექსი (09/10/2009 რედ) 29.05.2019 წლის მგდომარეობით.. მუხლი 112

142 იქვე.

143 ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციტივის მხარდაჭერით. 2015 წელი. გვ.369

- შუამდგომლობის ავტორთა ვინაობა;
- სისხლის სამართლის საქმის ნომერი;
- დანაშაულის კვალიფიკაცია;
- მხარის მოთხოვნა.“ [144]

„შუამდგომლობის აღწერილობით ნაწილში უნდა მიეთითოს:

- საქმის ფაქტობრივი გარემოებები;
- მტკიცებულებები, რომლებიც ადასტურებენ ფაქტობრივ გარემოებებს;
- შუამდგომლობის ავტორის მოსაზრებები და არგუმენტაცია გადასაწყვეტ საკითხებზე (შუამდგომლობის დასაბუთება);
- შესაბამისი კანონმდებლობა, მუხლის, ნაწილისა და ქვეპუნქტის მითითებით, რომლებიც ადასტურებენ მითითებულ მოსაზრებებსა და არგუმენტებს.“ [145]

„შუამდგომლობის დასკვნით ნაწილში უნდა მიეთითოს:

- მხარის მოთხოვნა ამა თუ იმ საგამოძიებო მოქმედების ჩატარების თაობაზე ნებართვის გაცემის შესახებ;
- საგამოძიებო მოქმედების ჩატარების ადგილი, ჩამტარებელი პირის და იმ პირისვინაობა, რომელთანაც ტარდება საგამოძიებო მოქმედება.“ [146]

ამოღების და ჩხრეკის წესი;

„საგამოძიებო მოქმედების დაწყებამდე გამომძიებელი, პირველ რიგში, არკვევს აცხადებს თუ არა მესაკუთრე, მფლობელი ან კომუნიკაციის ერთი მხარე თანხმობას საგამოძიებო მოქმედების ჩატარებაზე. თანხმობის შემთხვევაში, გამომძიებელი ატარებს საგამოძიებო მოქმედებას და ადგენს შესაბამისი საგამოძიებო მოქმედების ოქმს. ის შემთხვევაში, გამომძიებელი იღებს გადაწყვეტილებას საგამოძიებო მოქმედება ჩაატაროს მოსამართლის განჩინებით თუ განჩინების გარეშე გადაუდებელი აუცილებლობით. ამ უკანასკნელ შემთხვევაში გამომძიებელს გამოაქვს დადგენილება. დადგენილების გამოტანის აუცილებლობა, როგორც უკვე აღინიშნა, შესაბამისი მუხლების კომენტირებისას, ყველა სახის საგამოძიებო მოქმედების ჩატარებისას არ არსებობს. ამოღება და ჩხრეკა საგამოძიებო მოქმედებათა იმ კატეგორიას განეკუთვნება, რომელთა ჩატარებამდეც გამომძიებელმა უნდა გამოიტანოს დადგენილება.“ [147]

„ორივე შემთხვევაში (საგამოძიებო მოქმედების განჩინებით და განჩინების გარეშე ჩატარებისას), საგამოძიებო მოქმედების დაწყებამდე, გამომძიებელს ეკისრება იმ დოკუმენტის (განჩინების, დადგენილების) წარდგენის ვალდებულება, რაც საფუძვლად უდევს საგამოძიებო მოქმედების ჩატარებას. კერძოდ, გამომძიებელმა მოსამართლის განჩინება ან საკუთარი დადგენილება უნდა წარუდგინოს და ხელმოწერით გააცნოს იმ პირს, ვისთანაც ტარდება საგამოძიებო მოქმედება, ვინაიდან სწორედ აღნიშნული განჩინების (დადგენილების) საფუძველზე მოიპოვებს გამომძიებელი საცავში, სადგომში სათავსში ან სხვა მფლობელობაში საგნის, დოკუმენტის, ნივ-

---

144 ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციტივის მხარდაჭერით. 2015 წელი. გვ.369.

145 იქვე.

146 იქვე.

147 იქვე. გვ.390-392.

თიერების თუ ინფორმაციის შემცველი სხვა ობიექტის აღმოსაჩენად და ამოსაღებად შესვლის უფლებამოსილებას და შემდგომში პირის თანხმობას.“[148]

„განჩინების (დადგენილების) გაცნობაზე ან/და ხელმოწერაზე უარის შემთხვევაში, გამომძიებელი განჩინებაზე (დადგენილებაზე) აკეთებს შესაბამის მინაწერს. განჩინების, ხოლო გადაუდებელი აუცილებლობის შემთხვევაში — დადგენილების წარდგენის შემდეგ გამომძიებელი პირს, რომელთანაც ტარდება ამოღება ან ჩხრეკა, სთავაზობს ამოსაღები საგნის, დოკუმენტის, ნივთიერების თუ ინფორმაციის შემცველი სხვა ობიექტის ნებაყოფლობით გადაცემას.“ [149]

„აღსანიშნავია, რომ 1998 წლის 20 თებერვლის სსსკ-ი ამოღებასა და ჩხრეკას ნებაყოფლობითობის ნიშნით განასხვავებდა ერთმანეთისგან. კერძოდ, საქმისთვის მნიშვნელობის მქონე ნივთის ნებაყოფლობით გადაცემის შემთხვევაში, გამომძიებელს უნდა ჩაეტარებინა ამოღება, ხოლო ნივთის ნებაყოფლობით გადაცემაზე უარის შემთხვევაში — ჩხრეკა. შესაბამისად, აღნიშნული კოდექსი უშვებდა ამოღების ჩხრეკაში გადაზრდის შესაძლებლობას მაშინ, როცა ნივთის ამოსაღებად მისულ გამომძიებელს მის ნებაყოფლობით გადაცემაზე უარს ეტყოდნენ. მსგავს შემთხვევაში გამომძიებელი ვალდებული იყო შეედგინა ჩხრეკის ოქმი. მოქმედი საპროცესო კოდექსი კი როგორც ჩხრეკის, ისე ამოღების შემთხვევაში, უშვებს იძულების პროპორციული ზომების გამოყენების შესაძლებლობას. კერძოდ, ამოსაღები ობიექტის ნებაყოფლობით გადაცემის შემთხვევაში, აღნიშნული ფაქტი ფიქსირდება ოქმში, ხოლო მის ნებაყოფლობით გადაცემაზე უარის თქმის ან მისი არასრულად გადაცემის შემთხვევაში, ამოღება ხდება იძულებით.“ [150]

„ამასთან, გამომძიებელი უფლებამოსილია, გააღოს დაკეტილი საცავი, სადგომი და სათავსი, თუ გასაჩხრეკი პირი უარს ამბობს მათ ნებაყოფლობით გაღებაზე. ამოღებისა და ჩხრეკის განჩინებაში (დადგენილებაში) მიეთითება იმ საგნის, დოკუმენტის, ნივთიერების თუ ინფორმაციის შემცველი სხვა ობიექტის შესახებ, რომლის ამოღებაც უნდა განხორციელდეს. შესაბამისად, გამომძიებელი, საგამოძიებო მოქმედების ჩატარების ადგილზე ეძებს და იღებს იმ საგანს, დოკუმენტს, ნივთიერებას თუ ინფორმაციის შემცველ სხვა ობიექტს, რომელიც აღნიშნულია განჩინებაში ან დადგენილებაში. სსსკ-ი ადგენს საგანის, დოკუმენტის, ნივთიერების, თუ ინფორმაციის შემცველი სხვა ობიექტის ამოღების და შენახვის სპეციალურ წესებს, რომელთა დაუცველობამ შესაძლოა მტკიცებულებათა დაუშვებლად ცნობა გამოიწვიოს.“ [151]

„როგორც წესი, ჩხრეკის ან ამოღების დროს აღმოჩენილი საგანი, დოკუმენტი, ნივთიერება თუ ინფორმაციის შემცველი სხვა ობიექტი ამოღებამდე უნდა წარედგინოს ამ საგამოძიებო მოქმედებაში მონაწილე პირებს, შემდეგ ამოღებულ იქნეს, დაწვრილებით აღიწეროს, დაილუქოს და შეიფუთოს, შეფუთულ ნივთზე, ლუქის გარდა, აღინიშნება თარიღი და იმ პირთა ხელმოწერები, რომლებიც საგამოძიებო მოქმედებაში მონაწილეობდნენ, ამ წესიდან სსსკ-ის 120-ე მუხლი გამონაკლისს ითვალისწინებს. კერძოდ, ამოსაღები ობიექტი მხოლოდ მაშინ წარედგინება საგამოძიებო მოქმედების მონაწილეებს და ამოღების შემდეგ მხოლოდ მაშინ დაილუქება, თუ ამ საპროცესო მოქმედებების შესრულება შესაძლებელია, ანუ თუ ამოსაღები ობიექტი მისი გაბარიტების და ნიშან-თვისებების გათვალისწინებით იძლევა საგამოძიებო მოქმედების მონაწილეთათვის წარდგენისა და ამოღების შემდეგ დალუქვის შესაძლებლობას.“ [152]

---

148 ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციტივის მხარდაჭერით. 2015 წელი. გვ.390

149 იქვე.

150 იქვე. გვ.391.

151 იქვე. გვ.391-392

152 იქვე. გვ.392

5.2. დეტალიზაციის მეთოდური პრობლემა კომპიუტერული მოწყობილობის ამოღების დროს

როდესაც გამომძიებელი იწყებს საგამოძიებო მოქმედება – ამოღებას, დგება საკითხი, ხომარ ხდება ზედმეტი კომპიუტერის ნაწილების ამოღება და ხომარ ჰყოფს აღნიშნული რაიმე სხვა კონსტიტუციით გათვალისწინებულ უფლებას.

ხშირად არის ხოლმე შემთხვევები, როდესაც საგამოძიებო მოქმედების – ჩხრეკის ან ამოღების დროს, გამომძიებელი მიდის საგამოზიებო მოქმედების ადგილზე და იღებს კომპიუტერის ყველა მოწყობილობას, მათ შორის მაუსს, ე.წ. პრინტერს, სკანერს და ა.შ. ან შესაძლოა გამომძიებელმა ამოიღოს კომპიუტერის პროცესორი – მაგრამ მასში არ იყოს კომპიუტერის შემნახველი შესაბამისი მოწყობილობა – რაზეც ქვემოთ იქნება საუბარი, როგორ უნდა მოიქცეს ასეთ დროს გამომძიებელი –? მან უნდა ამოიღოს მხოლოდ ის ნივთი რომელიც არის ინფორმაციის მატარებელი, უფრო კონკრეტულად კი რომელშიც დაცულია ციფრული ინფორმაცია.

ამ საკითხის გადასაწყვეტად ძალზედ მნიშვნელოვანი კვლევა აქვს ჩატარებული ქალბატონ ლალი ფაფიაშვილს, რომელიც მიიჩნევს, რომ „ბრალდების მხარის მიერ სასამართლოს წინაშე დაყენებული შუამდგომლობის და შესაბამისად, სასამართლოს განჩინების დეტალიზაცია განსაკუთრებულ მნიშვნელობას იძენს, როდესაც ჩხრეკის ფარგლებში იგეგმება კომპიუტერულ მონაცემთა შესანახი საშუალებების ამოღება, რაც განპირობებულია მათზე არსებული ინფორმაციის მოცულობით და ხასიათის მრავალფეროვნებით. შესაბამისად, შუამდგომლობაში და სასამართლოს განჩინებაშიც, როგორც მინიმუმ, აღნიშნული უნდა იყოს ამოსაღები კომპიუტერული მონაცემების შესანახი საშუალებები, ამ საშუალებების საოპერაციო სისტემა, მყარი დისკის მახასიათებლები და ა.შ.“ [153]

ზემოაღნიშნულიდან გამომდინარე ძალზედ მნიშვნელოვანია რომ;
პროკურორმა სწორად მიუთითოს შუამდგომლობაში ის თუ რისი ამოღება სურს და დაასაბუთოს საქმისათვის რა მნიშვნელობის მატარებელია აღნიშნული, ან – დადგენილებაში გადაუდებლად ჩხრეკის ჩატარების დროს დეტალიზება მოხდეს რა ნივთი და რატომ უნდა იქნეს ამოღებული.

როდესაც მოსამართლე განჩინებას გასცემს – „თუ განჩინება დეტალურად განსაზღვრავს, კომპიუტერის რომელი მყარი დისკები უნდა იქნეს ამოღებული, მაგრამ არაფერს უთითებს ჩხრეკის მე–2 სტადიასთან მიმართებით, კერძოდ, არ იძლევა მითითებას იმის შესახებ, თუ რა მტკიცებულებას შეიძლება შეიცავდეს კომპიუტერი, ან, მაგალითად, განჩინება დეტალურად ასახელებს კომპიუტერის ფაილებს, რომლებიც უნდა გადამოწმდეს მე–2 ეტაპზე წარმოებული ჩხრეკის ფარგლებში, მაგრამ არაფერს აღნიშნავს იმის შესახებ, თუ რომელი კომპიუტერები უნდა იქნეს ამოღებული ჩხრეკის ადგილიდან, ასეთ შემთხვევებში რომელიმე ამ განჩინებებიდან არის საკმარისად დეტალიზებული? იმის განსაზღვრისათვის, ჩხრეკაზე განჩინება არის თუ არა საკმარისად დეტალიზებული, მხედველობაში მიიღება შემდეგი გარემოებები:

1. არსებობს თუ არა დასაბუთებული ვარაუდი განჩინებაში მითითებული კონკრეტული ტიპის ყველა საგნის ამოღებისათვის?

[153] ლალი ფაფიაშვილი. სტატია; ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი. 2014. გვ. 146

2. განჩინება ადგენს ობიექტურ კრიტერიუმს, რომლის მეშვეობით აღმასრულებელ პირს შეეძლება, გამოყოს ამოღებას დაქვემდებარებული საგნები იმ საგნებიდან, რომელთა ამოღებაც არ უნდა განხორციელდეს?

3. შეეძლო თუ არ პროცესის მწარმოებელ ორგანოს, უფრო დეტალურად აღეწერა ამოსაღები საგნები იმ ინფორმაციის გათვალისწინებით, რომელიც მის ხელთ იყო განჩინების გაცემის მომენტისათვის?“ [154]

„საქმეზე — აშშ რიკარდის წინააღმდეგ (UNITED STATES V. RICCARDI) — პორნოგრაფიული მასალის გავრცელებასთან დაკავშირებით წარმოებული ჩხრეკის ორდერში მითითებული იყო, რომ ჩხრეკის მწარმოებელ სუბიექტებს კომპიუტერის ამოღებასთან ერთად, ასევე უნდა ამოეღოთ: „კომპიუტერში ჩაწერილი ნებისმიერი სახის ელექტრონული ინფორმაცია, ასევე ყველა ჩამწერი მოწყობილობა (კომპიუტერში/კომპიუტერულ სისტემაში ინტეგრირებული და გარემეხსიერება), მათ შორის, და არამხოლოდ: დისკები, დისკეტები, მყარი დისკები, მაგნიტური ლენტები, გამოცალკევებადი მედიადრაივერები, ფლეშბარათები, მეხსიერების ბარათები, პრინტერები, მოდემები და ნებისმიერი სხვა ელექტრონული ან მაგნიტური მოწყობილობა, გამოყენებული კომპიუტერის ან კომპიუტერული სისტემის დამხმარე მოწყობილობა და მათზე ჩაწერილი ელექტრონული ინფორმაცია“.[155]

აღნიშნულ საქმეში მოთხოვნა და შემდეგ დაკმაყოფილება აღნიშნული მოთხოვნის იყო ძალიან მსუყე და რაც მთავარია დაუსაბუთებელი, ან უ საგამოძიებო მოქმედების განჩინების გაცემა მოხდა ზოგადი დასაბუთებიდან გამომდინარე, არ არის ინფორმაცია რა საქმისათვის მნიშვნელოვანი მასალა შესაძლოა ყოფილიყო მაგალითად მეხსიერების ბარათებში, ან რაში იყო საჭირო ისეთი მოწყობილობა როგორიც არის პრინტერი, მოდემი და ასე შემდეგ, შესაბამისად არც ბრალდების მხარის მიერ ყოფილა დასაბუთებული არნიშნული, სასამართლომ კი გამოიტანა შემდეგი გადაწყვეტილება;

„სასამართლომ აღნიშნა, რომ განჩინება (აშშ-ის შემთხვევაში — ორდერი) არ აკმაყოფილებდა დეტალიზაციის მოთხოვნას და იყო ზედმეტად ფართო შინაარსის მატარებელი. კომპიუტერის ჩხრეკის განჩინებამ/ორდერმა უნდა შეზღუდოს ჩხრეკა კონკრეტული დანაშაულის ჩადენის მამხილებელი მტკიცებულების ან კონკრეტული ტიპის მასალის აღმოჩენით. ამ შემთხვევაში ორდერი არ იყო შემოფარგლული რომელიმე კონკრეტული დანაშაულით ან კონკრეტული ფაილებით. ამდენად, ორდერი უფლებას აძლევდა ჩხრეკის მწარმოებელ პირებს, განეხორციელებინათ ჩხრეკა ნებისმიერი საგნის აღმოსაჩენად — ბავშვთა პორნოგრაფიიდან საგადასახადო კანონმდებლობის დარღვევამდე.“ [156]

„ითვლება, რომ დეტალიზაციის მოთხოვნას აკმაყოფილებს სასამართლოს განჩინებები, რომლებშიც ამოსაღები საგნების ნუსხაში ერთდროულად მითითებულია ზუსტად განსაზღვრული ნივთები და ნივთები, რომელთა განსაზღვრისათვის სასამართლო იყენებს ე.წ. „ყოვლისმომცველ ცნებებს“, როგორებიცაა, მაგალითად: ელექტრონული მატარებლები ან ელექტრონული მოწყობილობები, რაც მოიცავს ნებისმიერი სახის ელექტრონულ მატარებელს, მათ შორის ჩხრეკის ადგილას არსებულ ყველა კომპიუტერს, გარემეხსიერებას, დისკებს, მეხსიერების ბარათებს და

---

154 იქვე. 146

155 ლალი ფაფიაშვილი. სტატია; ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი. 2014. გვ. 147

156 იქვე.

ა.შ. ამ შემთხვევაში განჩინების დეტალიზაციას განაპირობებს განჩინების კონტექსტი, მასში მითითებული სხვა ამოსაღები საგნები. შედეგად, განჩინება წაკითხული უნდა იქნეს როგორც ჩხრეკის მწარმოებელი პირებისათვის ამოღებულ კომპიუტერებსა და ელექტრონულ მოწყობილობებში მხოლოდ განსაზღვრული საკითხების წრესთან დაკავშირებული ინფორმაციის შემცველი მასალის ჩხრეკაზე უფლების მიმნიჭებელი. განჩინების ამგვარი განმარტებისას სასამართლო მას თვლის საკმარისად დეტალიზებულად. წინააღმდეგ შემთხვევაში, თუ განჩინება ითვალისწინებს კომპიუტერში არსებული ყველა ჩანაწერის ჩხრეკის უფლებას აღწერის ან შეზღუდვის გარეშე, ის ვერ აკმაყოფილებს მე-4 შესწორებით განსაზღვრულ სტანდარტს (იხ. აშშ რიკარდის წინააღმდეგ (United States v. Riccardi), 405 F.3d 852,862,10th Cir. 2005)." [157]

ამდენად, ზემოაღნიშნული გადაწყვეტილება და განმარტებები, რომ მოვარგოთ საქართველოში არსებულ რეალობას, აუცილებელია რომ;

გამომძიებლის მიერ დადგენილებაში საგამოძიებო მოქმედების ჩატარების შესახებ და შემდგომ პროკურორის შუამდგომლობაში საგამოძიებო მოქმედების კანონიერების შემოწმების შესახებ დეტალურად უნდა იყოს დასაბუთებული;

2. რა საგანი (საგნები) უნდა იქნეს დაძებნილი და ამოღებული საგამოძიებო მოქმედების შედეგად;
3. რატომ უნდა მოხდეს აღნიშნული საგნის (საგნების) დაძებნა და შემდგომ ამოღება;
4. რა შემხებლობაშია ამოსაღები საგანი საქმესთან და რა ინფორმაცია ინახება ან შესაძლოა ინახებოდეს მასზე;
5. რა საპროცესო საფუძველი არსებობს საგამოძიებო მოქმედების გადაუდებლად ჩატარებისათვის;

ხოლო თუ მხარე შუამდგომლობით მიმართავს სასამართლოს და სთხოვს მას, რომ გასცეს განჩინება – ჩატარებულ იქნეს საგამოძიებო მქომედება ჩხრეკა – ან/და ამოღება, პროკურორი ვალდებულია დაასაბუთოს

1. რა საგანი (საგნები) უნდა იქნეს დაძებნილი და ამოღებული საგამოძიებო მოქმედების შედეგად;
2. რატომ უნდა მოხდეს აღნიშნული საგნის (საგნების) დაძებნა და შემდგომ ამოღება;
3. რა შემხებლობაშია ამოსაღები საგანი საქმესთან და რა ინფორმაცია ინახება ან შესაძლოა ინახებოდეს მასზე;
4. რა საპროცესო საფუძველი არსებობს საგამოძიებო მოქმედებისათვის განჩინების გასაცემად;

---

[157] ლალი ფაფიაშვილი. სტატია; ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი. 2014. გვ. 147-148

5.3. ციფრული ინფორმაციის შემნახველი კომპიუტერული მოწყობილობების სახეები

ციფრული ინფორმაციის ამოღება როდესაც ხორციელდება, მთავარია გამომძიებელმა, რომელიც აწარმოებს საგამოძიებო მოქმედებას იცოდეს თუ რა საგანი უნდა ამოიღოს და რატომ, ამისათვის აუცილებელია გამომძიებელმა იცოდეს რა სახის კომპიუტერული სისტემები არსებობს, რაშიც შეიძლება საქმისთვის მნიშვნელოვანი ინფორმაცია იყოს განთავსებული.

აუცილებელია გაიმიჯნოს რა სახის ინფორმაციას უნდა ფლობდეს გამომძიებელი და რას არა, მნიშვნელოვანია რომ გამომძიებელმა იცოდეს კომპიუტერის აგებულება არაპროფესიანალურ არამედ იმ დონეზე, რაც ხელს შეუწყობს მის მიერ საგამოძიებო მოქმედების წარმოებას, ასევე იცოდეს რა ნაწილებისგან შედგება კომპიუტერი და სად არის დაცული მისთვის საჭირო ინფორმაცია აღნიშნულ კომპიუტერში.

აღნიშნული საკითხის დეტალიზება დავიწყოთ პერსონალური კომპიუტერით, რისთვისაც საწყის ეტაპზე მოლკედ მიმოვიხილოთ კომპიუტერის კლასიფიკაცია;

„კომპიუტერი არის ტექნიკურ საშუალებათა კომპლექსი, რომლის დანიშნულებაა ინფორ-მაციული და გამოთვლითი ამოცანების გადაწყვეტის პროცესში, ინფორმაციის ავტომატური და-მუშავება. გამოთვლების შესაძლებლობისა და ზომის მიხედვით კომპიუტერები შეიძლება დაიყოს (იხილეთ სურათი N1):

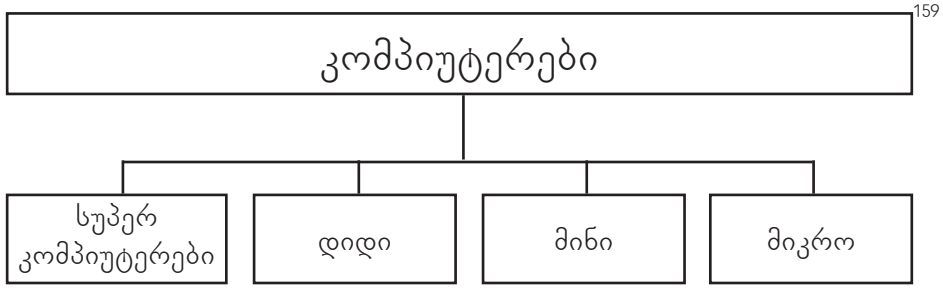
ზედიდი (სუპერ-კომპიუტერები);

დიდი;

მცირე;

ზემცირე (მიკროკომპიუტერები);“ [158] **(იხილეთ სურათი №1)**

(კომპიუტერების დაყოფა – სურათი N1);



[159]

„სუპერკომპიუტერებს მიეკუთვნება მძლავრი მრავალპროცესორიანი გამომთვლელი მანქანები, რომელთა სისწრაფე ასეულ მილიონობით მილიარდ ოპერაციას შეადგენს წამში. დიდ კომპიუტერებს საზღვარგარეთ უწოდებენ ეინფრეიმებს; მათ მიეკუთვნება კომპიუტერები, რომელთაც აქვთ: წარმადობა არანაკლებ 100 MIPS; ძირითადი მეხსიერების მოცულობა 512-დან 10000 მბაიტამდე; გარე მეხსიერება არანაკლებ 100 გბაიტი; მუშაობის მრავალ-მომხმარებლიანი რეჟიმით.“ [160]

---

[158] ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი

[159] სურათი; ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი

[160] იქვე.

„მეინფრეიმის ეფექტური მოხმარების მიმართულებაა სამეცნიერო-ტექნიკური ამოცანების გადაწყვეტა, ინფორმაციის პაკეტური დამუშავებით, მუშაობა დიდი მოცულობის მონაცემთა ბაზებთან, გამოთვლითი ქსელებისა და მათი რესურსების მართვით. უკანასკნელ პერიოდში მეინფრეიმებს გამოიყენებენ გამოთვლით ქსელებში დიდ სერვერებად.“ [161]

„მცირე კომპიუტერები (მინი-კომპიუტერები) არის საიმედო, იაფი და მოსახერხებელი ექსპლუატაციაში, რომლებიც ფლობენ შედარებით მცირე შესაძლებლობებს.“ [162]

„მინი-კომპიუტერების მიღწევად შეიძლება აღინიშნოს: სპეციფიკური არქიტექტურა მოდულურობის პრინციპით; საუკეთესო შეფარდება წარმადობა/ფასი; გამოთვლების დიდი სიზუსტე. მინი-კომპიუტერები ორიენტირებულები არიან მმართველ-გამომთვლელ კომპლექსებში გამოსაყენებლად. აგრეთვე წარმატებით გამოიყენებიან მრავალი მოხმარების გამოთვლით სისტემებში, ავტომატიზებული დაპროექტების სისტემებში, მამოდელირებელ სისტემებში, ხელოვნური ინტელექტის სისტემებში.“ [163]

„მიკროკომპიუტერების კლასს განეკუთვნებიან პერსონალური კომპიუტერები (pk), რომლებიც მათი მასობრივი გავრცელების გამო იმსახურებენ განსაკუთრებულ ყურა-დღებას. [...][164] ამჟამად კომპიუტერების მსოფლიო პარკი შეადგენს მილიარდის მეოთხედ ცალს, მათგან 90% პერსონალური კომპიუტერებია (IBM PC ტიპის კომპიუტერები შეადგენს მთელი რაოდენობის 80%).“ [165]

მნიშვნელოვანი საკითხია, რას ინახავს კომპიუტერული მოწყობილობა და რატომ უნდა ამოვიღოთ ის, კომპიუტერში ინახება ინფორმაცია, ინფორმაცია კი არის ყველაფერი ის რასაც ადამიანი აღიქვამს გრძნობათა ორგანოების მეშვეობით. ინფორმაცია ლათინური სიტყვაა და ქართულად — ცნობას ნიშნავს;

კომპიუტერი ინახავს სამი სახის ინფორმაციას. ესენია:

1. ტექსტური;
2. გრაფიკული;
3. აუდიო;

ტექსტური ინფორმაცია შედგება ციფრების, ასოების, სასვენი ნიშნებისა და სპეციალური სიმბოლოებისაგან.

გრაფიკული ინფორმაცია წარმოადგენს – ნახაზებს, ნახაზებს, ფოტო სურათებს, მოძრავ სურათებს და სხვა.

აუდიო (ანუ ხმოვანი) ინფორმაცია – არის მუსიკა, საუბარი, და სხვადასხვა ხმოვანი ეფექტები.

„ინფორმაციას, ისევე როგორც ნებისმიერ სხვა ფიზიკურ სიდიდეს გააჩნია საზომი ერთეულები. ინფორმაციის ყველაზე მცირე საზომ ერთეულს ბიტი (bit) ეწოდება. მას შეიძლება ჰქონდეს მხოლოდ ორი მნიშვნელობა. ის შეიძლება უდრიდეს 0 ან 1-ს. ორობითი თვლის სისტემის ერთ-ერთ ციფრს.“ [166]

„პრაქტიკაში ასევე გამოიყენება ბაიტი (Byte) რომელიც უდრის 8 ბიტს და ერთ ტექსტურ სიმბოლოს.“ [167]

---

161 ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი

162 იქვე.

163 იქვე.

164 იქვე.

165 იქვე.

166 იქვე.

167 იქვე.

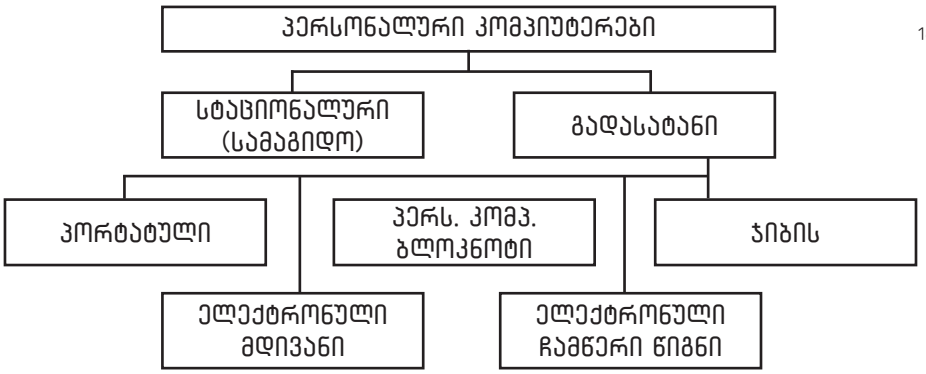
რადგანაც ბიტი და ბაიტი მცირე ზომის საზომი ერთეულებია უფრო სირად გამოიყება მათგან წარმოებული ერთეულები:[168]

კილობაიტი (KB);	მეგაბაიტი (MB);	გიგაბაიტი (GB);
ტერაბაიტი (TB);	კილობიტი (Kb);	მეგაბიტი (Mb);
გიგაბიტი (Gb);	თერაბიტი (Tb);	

დაახლოებით:	ზუსტად:
1KB = 1 000B	(1024B)
1MB = 1 000 000B	(1024KB)
1GB = 1 000 000 000B	(1024MB)
1TB = 1 000 000 000 000B	(1024GB)

ხოლო, როდესაც გამომძიებელი შედის საგამოძიებო მოქმედების ჩასატარებლად და უნდა ამოიღოს რაიმე სახის კომპიუტერული მოწყობილობა, მნიშვნელოვანია კარგად იცოდეს რა უნდა ეძებოს მან და რა მოწყობილობა უნდა ამოიღოს რომელიც შესაძლოა იყოს ინფორმაციის მატარებელი. მიუხედავად იმისა, რომ ასეთი მოწყობილობები უამრავი შეიძლება იყოს, წარმოგიდგენთ პრაქტიკაში ხშირად გავრცელებულ სახეობებს (იხილეთ სურათი N2);

(პერსონალური კომპიუტერის ნაირსახეობები სურათი N2);



169

პორტატიული კომპიუტერი;

„ეს არის კომპიუტერი, რომელიც არის პერსონალური კომპიუტერების სწრაფად განვითარება–დი ქვეკლასი. ვიდეომონიტორად გამოიყენება ბრტყელი თხევად კრისტალური დისპლეი.“ [170]

კომპიუტერი ბლოკნოტი;

„კომპიუტერი — ბლოკნოტი ანუ ნოუთბუქი ასრულებს პერსონალური კომპიუტერის ყველა ფუნქციას, მასში შე–იძლება გამოყენებული იქნას იგივე ოპერაციული სისტემები და პროგრამები.

---

168 ელ. გვერდი ; ნანახია 15.07.2019

169 ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი

170 იქვე.

კომპიუტერი-ბლოკნოტები იყოფიან კლასებად მათი გა-ბარიტების შესაბამისად (სქელი და თხელი), ეკრანის ზომებით, ხშირად მასში გამოყენებული მიკროპროცესო-რების მიხედვით. პრაქტიკულად ყველა ნოუთბუქი მუშაობს OC WINDOWS XP მართვით.“ [171]

ჯიბის კომპიუტერები;

„ჯიბის კომპიუტერები არის ყველაზე სწრაფად განვითარებადი პორტატიული კომპიუტერების კლასი. ჟიბის კომპიუტერებში გამოიყენება თავისი ოპერაციული სისტემა, პერსონალური კომ-პიუტერისაგან განსხვავებით. ჯიბის კომპიუტერები არის სრულფასოვანი კომპიუტერები, რო-მელთაც აქვთ მიკროპროცესორები, ოპერატიული მეხსიერება, ფერადი თხევადკრისტალური დისპლეი, პორტატიული ფიზიკური ან ვირტუალური კლავიატურა, პორტები (ხშირად უსადენო) გარე მოწყობილობასთან მისაერთებლად.“ [172]

ელექტრონული მდივანი;

„ელექტრონულ მდივანს ხშირად უწოდებენ (ხელით დამხმარეს), რომელსაც აქვს ჯიბის კომპიუტერის ფორმატი. მოწყობილობას გააჩნია ფართო ფუნქციონალური შესაძლებლობა. ის აღჭურვილია აპარატურულ და ჩადგმული პროგრამული უზრუნველყოფით, ორიენტირებულია ელექტრონული ცნობარის ორიენტაციაზე, რომელიც ინახავს სახელს, მისამართს და ტელეფონების ნომრებს, დღის განრიგისა და შეხვედრების ინფორმაციას, მიმდინარე საქმეების სიას, დანახარჯების შესახებ ჩანაწერებს და სხვ. უმთავრესად ასეთ მოწყობილობებს აქვთ მოდემები სხვა კომპიუტერებთან ინფორმაციის გასაცვლელად, თუ მიერთებული იქნება გამოთვლით ცენტრთან შესაძლე-ბელი ხდება ელექტრონული ფოსტისა და ფაქსის გაგზავნა. ზოგიერთ მათგანს აქვს ავტომატური ნომრის ამკრები. უსადენო, დინსტანციური ინფორმაციის გასაცვლელად გამოიყენება რადიომოდემები და ინფრაწითელი პორტები. ძოგიერთ მოდელს აქვს სენსორული ეკრანი მაჩვენებელით.“ [173]

ელექტრონული ჩამწერი წიგნაკი;

„ელექტრონული ჩამწერი წიგნაკი – ორგანაიზერი მიეკუთვნება პორტატიულ კომპიუტერებს (ამ კატეგორიას ამის გარდა ეკუთვნის კალკულატორები, ელექტრონული მთარგმნელები და ა. შ.). ორგანაიზერი მომხმარებლის მიერ არ პროგრამირდება, მაგრამ აქვს მეხსიერება 2-256 კბაიტი, რომელშიდაც შეიძლება ჩაიწეროს აუცილე-ბელი ინფორმაცია და მოხდეს მისი რედაქტირება, (აქვს ჩადგმული ტექსტური რედაქტორი); მეხსიერებაში შეიძ-ლება შენახული იქნას სატელეფონო და სამისამართო წიგნები, საქმიანი წერილები, შეთანხმების ტექსტი, კონტრაქტი, დღის განრიგი და საქმიანი შეხვედრების განრიგი. ორგანაიზერში არის შიდა ტაიმერი და შესაძლებლობა ხმოვანი სიგნალით მოგვცეს შეტყობინება საქმის შესახებ მოცემულ დროში. შესაძლებელია ინფორმაციის დაცვა არასანქცირებული ქმედებისაგან, ჩვეულებრივი პაროლის მეშვეობით.“ [174]

მობილური მოწყობილობები (mobile intelligent devices – მობილური ტელეფონები, კომუნიკატორები);

„წარმოადგენენ მოწყობილობებს, რომლებიც გამოიყენებიან ხმოვანი კავშირებისთვის, იშვიათად რაიმე ინფორმაციის დასამუშავებლად ან ინტერნეტში შესასვლელად. მობილური მოწყობილობებისთვის მნიშვნელოვანი პარამეტრია ხმოვანი სიგნალის ხარისხი და ბატარეიის ავტონომიური მუშაობის დრო. მათში ასევე მნიშვნელოვანია ციფრული ფოტო და ვიდეოკამერები. მობილური მოწყობილობებისთვის ოპერაციული სისტემა ხასიათდება დიდი კომპაქტურობით, მეხსიერებასთან უფრო მკაცრი შეზღუდვებით. მობილური ტელეფონების ბაზარზე დომინირებდა

---

171 ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი.

172 იქვე.

173 იქვე.

174 იქვე.