

ურა ზაქაშვილი

**კიბერდანაშაულის
სისხლისსამართლებრივი
რეგულირების პრობლემები
საქართველოში**

თბილისი
2013

უჩა ზაქაშვილი – კიბერდანაშაულის სისხლისსამართლებრივი
რეგულირების პრობლემები საქართველოში

რედაქტორი: მზია ლეკვეიშვილი
Edited by: Mzia Lekveishvili

გარეკანის დიზაინი: თეა აკობია
Design by: Thea Akobia

დაკაბადონება: ნიკა ხვედელიძე
Page make-up: Nika Khvedelidze

© უჩა ზაქაშვილი – კიბერდანაშაულის სისხლისსამართლებრივი
რეგულირების პრობლემები საქართველოში

© გამომცემლობა „საუნჯე“, ვაჟა წონკოლაური
SAUNJE publishing house, Vazha Tsotskolauri

ISBN 978-9941-451-31-7

წინასიტყვაობა

მოცემული წიგნს საფუძვლად დაედო სადისერტაციო ნაშრომი, რომლის დაცვაც აკადემიური ხარისხის მოსაპოვებლად წარმატებით გაიმართა 2013 წლის 18 ნოემბერს ქ. თბილისის ივ. ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტში.

წიგნი ეფუძვნება ქართულ კანონმდებლობას, ევროსაბჭოს კონვენციას, ქართულ სასამართლო პრაქტიკას და მსოფლიოს სხვადასხვა ქვეყნის გამოცდილებას.

მასში განხილულია არაერთი რეალური კაზუსი საქართველოს საგამოძიებო და სასამართლო პრაქტიკიდან. ნაშრომში ჩაწერულია გამოძიების და სასამართლოს მიერ ქმედების დანაშაულად კვალიფიკაციისას დაშვებული ხარვეზები. ასევე, განხილულია საკანონმდებლო უზუსტობები და შემოთავაზებულია მათი აღმოფხვრის გზები.

ამდენად, აღნიშნული წიგნი პრაქტიკულ დახმარებას გაუწევს იმ ადამიანებს ვისი საქმიანობაც უკავშირდება კიბერდანაშაულის გამოძიებას, სამართალშეფარდებას, ცალკეული კიბერშემთხვევების ანალიზს. ასევე, დააინტერესებს იმ პირებს ვისთვისაც 21-ე საუკუნის მთავარი გამოწვევა – კიბერდანაშაული მიმზიდველი თემაა.

წიგნის ავტორი მადლობას უხდის ქ. თბილისის ივ. ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის სისხლის სამართლის მიმართულებას. ასევე, წიგნის შექმნაში შეტანილი წვლილისათვის განსაკუთრებულ მადლობას უხდის ქალბატონ მზია ლეკვეიშვილს.

სარჩევი

წინასიტყვაობა	3
შესავალი	7

I თავი

კიბერდანაშაულის ცნება და სამართლებრივი კვლევის ისტორია...	13
---	----

II თავი

კომპიუტერული დანაშაულის სამართლებრივი მოწესრიგება საქართველოში	27
1. ახალი საკანონმდებლო რეგულირების წინაპირობები ...	27
2. 284-ე მუხლით გათვალისწინებული დანაშაულის	30
ობიექტური შემადგენლობა	30
3. 285-ე მუხლით გათვალისწინებული დანაშაულის	65
ობიექტური შემადგენლობა	65
4. 286-ე მუხლით გათვალისწინებული დანაშაულის	80
ობიექტური შემადგენლობა	80
5. კიბერდანაშაულის სუბიექტური შემადგენლობა	114
6. კიბერდანაშაულის სუბიექტი	129
7. პასუხისმგებლობის დამამძიმებელი გარემოებები კიბერ-დანაშაულის ჩადენისთვის	131
8. იურიდიული პირის სისხლისსამართლებრივი პასუხის-მგებლობა კიბერდანაშაულის ჩადენისთვის	135

III თავი

საქართველოს სისხლის სამართლის კოდექსში ასახული „კიბერ-დანაშაულის შესახებ“ კონვენციით გათვალისწინებული დანაშაულები, რომლებიც დაკავშირებულია კომპიუტერის გამოყენებასთან	140
1. კერძო კომუნიკაციის საიდუმლოების დარღვევა	140
2. პორნოგრაფიული ნაწარმოების ან სხვა საგნის უკანონოდ დამზადება ან გასაღება	146
3. საავტორო, მომიჯნავე უფლების მფლობელის და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა	151

IV თავი

კიბერტერორიზმი	154
----------------------	-----

V თავი

კიბერდანაშაულის სამართლებრივი რეგულირება მსოფლიოს ზოგიერთ ქვეყანაში	161
დასკვნა	176
ბ ი ბ ლ ი ო გ რ ა ფ ი ა	181
სასამართლო პრაქტიკის მასალები.....	185
ნორმატიული მასალა	186
ინტერნეტ-მასალები.....	187

შესავალი

კვლევის აქტუალობა – უნინ მხოლოდ ფილმებში ვხედავდით პაკერებს და ისინი ზღაპრული გმირები გვეგონა. დღეს ტერმინი „კიბერდანაშაული“ აღარავის უკვირს. საზოგადოებისთვის რთულია გაარკვიოს ვინ არის უბრალო თაღლითი, რომელიც კომპიუტერული ტექნიკის საშუალებით 100 დოლარიანებს ბეჭდავს და ვინ გენიოსი, რომელსაც შეუძლია ნებისმიერი კომპიუტერული დაცვითი სისტემის გადალახვა. მათ ყველას პაკერებს უწოდებენ. ჩნდება კითხვა, რა შეიცვალა XX საუკუნის 70-იანი წლებიდან ანუ კომპიუტერული დანაშაულის ჩასახვის დღიდან „კიბერდანაშაულის შესახებ“ ევროსაბჭოს 2001 წლის 23 ნოემბრის კონვენციის მიღებამდე? პასუხი მარტივია – შეიცვალა კომპიუტერული დანაშაულის შინაარსი, გაფართოვდა მისი საზღვრები და გაიზარდა საფრთხე, უფრო მრავალფეროვანი გახდა მისი ჩადენის ხერხი. კომპიუტერული დანაშაულის ბუნებაში გარკვევა ამ დანაშაულის წინააღმდეგ ბრძოლის სფეროში მოღვაწე ექსპერტებსაც უჭირთ.

კომპიუტერული დანაშაულის წარმოქმნის შემდეგ ხშირი იყო მცდელობა, შემოეღოთ კომპიუტერული დანაშაულის ერთიანი ცნება თუმცა ეს მცდელობა უშედეგოდ სრულდებოდა. ერთ საერთაშორისო ცნებას მეორე ორგანიზაციის მიერ გაკეთებული განმარტება ენაცვლებოდა. საბოლოოდ, მივიღეთ ის, რომ არც ევროპის საბჭოს კონვენცია და არც მსოფლიოს რომელიმე ქვეყნის კანონმდებლობა არ იძლევა ამ ცნების ზოგად განმარტებას. საუბარი არაა ცალკეული დანაშაულის შემადგენლობაზე, რადგან ადვილია განმარტო „კომპიუტერულ სისტემაში უნებართვო შეღწევის“ ცნება. თუმცა იგი მხოლოდ ერთ-ერთი კომპიუტერული დანაშაულის განმარტება იქნება და არა დანაშაულებრივი ფენომენის – კიბერდანაშაულისა.

კომპიუტერული დანაშაულის საკითხის შესწავლის დაწყებამდე ვცადე გამერკვია, რამდენად აქტუალური შეიძლება იყოს ეს პრობლემა საქართველოსთვის. დღეს განვითარებად ქვეყნებში აქტიურად მიმდინარეობს სახელმწიფო და კერძო სექტორის კომპიუტერებით და ინტერნეტით უზრუნველყოფა. უკანასკნელ წლებში აღნიშნულ პროცესში საქართველოც აქტიურად ჩაება. ეს კი პაკერებისთვის ქმნის ნოყიერ ნიადაგს კრიმინალური საქმიანობის დაწყებისთვის.

აღნიშნულს ხელს უწყობს ასეთ სახელმწიფოებში უსაფრთხოების ერთიანი სისტემის არარსებობა, მაღალი ტექნოლოგიების სფეროში სამართალდამცავი ორგანოების ნაკლები კომპეტენტურობა და ზოგადად, კიბერდანაშაულის ლატენტურობის მაღალი ხარისხი. ეს უკანასკნელი სერიოზულ პრობლემას წარმოადგენს განვითარებული ქვეყნების სამართალდამცავი ორგანოებისთვისაც.

საქართველოს მასშტაბით საკითხის აქტუალობის დასაბუთების მიზნით მივმართე შსს-ს ადმინისტრაციას და გამოვითხოვე გამოძიების ოფიციალური სტატისტიკა¹. გაირკვა, რომ 2001-2007 წლებში რეგისტრირებულია მხოლოდ ხუთი შემთხვევა, მათგან გახსნილია ორი. 2008 წელს კიდევ ერთი კიბერდანაშაული გამოვლინდა. საბოლოო ჯამში კი 2010 წლამდე საქართველოში სულ ექვსი კომპიუტერული დანაშაულია დაფიქსირებული². 2012 წლის 22 თებერვალს წერილით მივმართე თბილისის საქალაქო სასამართლოს, რათა გამერკვია რამდენი საქმე განიხილა საქართველოს სისხლის სამართლის ახალი რედაქციით გათვალისწინებულ კიბერდანაშაულზე საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიამ 2010 წლის 24 სექტემბრიდან 2012 წლის 22 თებერვლამდე. მათი პასუხიდან ირკვევა, რომ სულ განხილულია 14 საქმე. მათ შორის 6 საქმე სისხლის სამართლის კოდექსის 284-ე, 1 საქმე 285-ე და 7 საქმე 286-ე მუხლით გათვალისწინებული დანაშაულზე³. მოგვიანებით კვლავ მივმართე სასამართლოს და მათი წერილით ირკვევა, რომ 2012 წლის 22 თებერვლიდან 2013 წლის 18 ოქტომბრამდე სასამართლომ განიხილა 38 საქმე. მათ შორის 31 საქმე 284-ე, 3 საქმე 285-ე და 4 საქმე 286-ე მუხლით გათვალისწინებული დანაშაულის ჩადენისთვის. გამამართლებელი განაჩენი არ დამდგარა.⁴

1 იხ. საქართველოს შინაგან საქმეთა სამინისტროს წერილი №7/2/7-4772, 12.12.2007წ.

2 იხ. თ. კაციტაძე, კომპიუტერული დანაშაულები – მსოფლიოს უდიდეს დანაშაულთა რიცხვში, გაზეთი „24 საათი“ 01.02.2010წ. (<http://24saati.ge/index.php/category/news/justice/2010-02-01/3148.html>).

3 იხ. თბილისის საქალაქო სასამართლოს №31/3738-3739 23.02.2012წ. წერილი.

4 იხ. თბილისის საქალაქო სასამართლოს №1-04114/20807-2, 21.10.2013წ. წერილი.

მოყვანილი სტატისტიკის მიხედვით, გამოდის, რომ კომპიუტერული დანაშაულის პრობლემა საქართველოში პრაქტიკულად არ არსებობს ან თუ არსებობს, ძალიან უმნიშვნელო პრობლემებს ქმნის. თუმცა, განსხვავებული მოსაზრება გამაჩნია. მაგალითისთვის ამერიკული გამოცდილების ანალიზი გამოდგება. კერძოდ, ს. ჩარნის და კ. ალექსანდერის სტატიაში „კომპიუტერული დანაშაულის ტიპები“, რომელშიც განხილულია კომპიუტერული დანაშაულის პრობლემის მასშტაბი, ეკითხულობთ: „იმ ფიონზე, როდესაც ეს გამოკითხვა ასეთ საგანგაშო სურათს ქმნის, უსაფრთხოების ექსპერტები მიიჩნევენ, რომ კომპიუტერული დანაშაულის უმეტესობა არც დაფიქსირებულია და არც გამოვლენილი. ამ დასკვნას აშშ-ს მთავრობის ერთ-ერთი სააგენტოს მიერ გაკეთებული სტატისტიკა ამყარებს. ამ სააგენტოს კომპიუტერების უსაფრთხოების შესამოწმებლად მანქანებზე განხორახ განხორციელდა თავდასხმა. 38000 სამიზნე კომპიუტერიდან დაზარალებულ მანქანებში შეღწევა წარმატებით განხორციელდა 65%-ში. წარმატებით დაზიანებული საიტების სისტემურმა ადმინისტრატორებმა დააფიქსირეს შეღწევების მხოლოდ 4%. ამ 4%-დან მხოლოდ 27%-მა განახორციელა გადაცემა. სხვა სიტყვებით რომ ვთქვათ 38000 დაზარალებული მანქანიდან 24700-ში განხორციელდა შეღწევა, რაც ალიქვა მხოლოდ 988 მათგანმა და თავდასხმის შესახებ ინფორმაციის გადაცემა მოახერხა მხოლოდ 267-მა“⁵

ამდენად, უნდა მივიჩნიოთ, რომ საკითხის აქტუალობა ნაკლებადაა დამოკიდებული ოფიციალური სტატისტიკის შედეგზე, ვინაიდან კომპიუტერული დანაშაულის მაღალი ლატენცთური ხასიათი არ იძლევა სრულ შესაძლებლობას მისი გამოვლენისა და გამოძიებისთვის.

აქვე მოვიყვან აშშ-ს გამოძიების ფედერალური ბიუროსთან არსებული ინტერნეტდანაშაულის შესახებ საჩივრების ცენტრის (Internet Crime Complaint Center) მონაცემებს, რომლის თანახმადაც: 2001 წელს 17 მილიონი დოლარი, 2002 წელს – 57, 2003 წელს – 125, 2004 წელს – 68, 2005 წელს კი ზიანმა – 183 მილიონი დოლარი შეადგინა. 2006 წელს ინტერნეტდანაშაულის შესახებ საჩივრების ცენტრს მიმართა კომპიუტერული დანაშაულისგან დაზარალებულმა

5 იხ. SCOTT CHARNEY, KENT ALEXANDER, Types of computer crime, 25.11.2005 (<http://www.crime-research.org/articles/types-of-computer-crime/2>)

207492 ადამიანმა⁶. ზიანმა კი წინა წლებთან შედარებით სარეკორდო ნიშნულს მიაღწია და 198.4 მილიონი დოლარი შეადგინა⁷.

„კომპიუტერულ დანაშაულს ხშირად XXI საუკუნის კრიმინალურ ფორმას უწოდებენ. ამ ტიპის დანაშაულის მუდმივად მზარდი რიცხვი საერთო კრიმინალურ სტატისტიკაში და ეგმ-ის განუზომელი პოტენციალი მიუთითებს იმაზე, რომ დღევანდელი მდგომარეობა ამ საშიში პრობლემის მხოლოდ დასაწყისია“⁸.

საქართველოში უკანასკნელ წლებში, მსგავსად მსოფლიოს სხვა ქვეყნებისა, შეინიშნება ინფორმაციული, გამოთვლითი და საკომუნიკაციო ტექნოლოგიების, საშუალებების ინტენსიური განვითარება. ეს გარემოება, გარდა დადებითისა (კერძოდ, ოპერატიულად ხელმისაწვდომი ხდება აუცილებელი ინფორმაცია, სხვადასხვა სერვისი, შინიდან გაუსვლელად არის შესაძლებელი გადასახადების გადახდა, ვაჭრობა და სხვა) შეიცავს რიგ უარყოფით ფაქტორებსაც: კერძოდ, დგება კომპიუტერული დანაშაულის პრობლემა.

ზემოაღნიშნულიდან გამომდინარე მიმაჩნია, რომ კომპიუტერული დანაშაულის მწირი ოფიციალური სტატისტიკის მიუხედავად, საქართველოში კომპიუტერული დანაშაულის პრობლემის აქტუალობა ყოველწლიურად იზრდება. პროგრესს განაპირობებს კომპიუტერული დანაშაულის ჩადენისთვის ე.წ. ნოყიერი ნიადაგი. ეს ნიადაგია: კომუნალური გადასახადების გადახდის შესაძლებლობა ინტერნეტით, სხვადასხვა ინტერნეტ-მაღაზია, რომელშიც შინიდან გაუსვლელად შესაძლებელია სასურველი ნივთის შეძენა, სახელმწიფო დაწესებულებების მხრიდან ელექტრონულ დოკუმენტბრუნვაზე გადასვლა, ოფიციალური დოკუმენტების ელექტრონული წესით გაცემის შესაძლებლობა. გარდა ამისა, მთელი რიგი სასიცოცხლო მნიშვნელობის ან/და სახელმწიფო დაწესებულება იმართება სხვადასხვა კომპიუტერული პროგრამით და სისტემით. მაგალითად, აეროპორტები, სავადმყოფოები, სახელმწიფოს თავდაცვითი

6 იხ. The Internet Crime Complaint Center 2006 Internet Fraud Crime Report: January 1, 2006-December 31, 2006, გვ. 3 http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf

7 იხ. იქვე.

8 გ. ლანჩავა, „კომპიუტერული დანაშაული“, ჟურნ. „მართლმსაჯულება“, 2008წ. №2, გვ. 63

ობიექტები და ა.შ მათი ხელყოფა, თავისთავად, დიდი საფრთხის შემცველია ქვეყნის თავდაცვის უნარიანობისთვის, მოსახლეობის უსაფრთხოებისთვის და ა.შ.

მოცემული ნაშრომის აქტუალობას განსაზღვრავს ის გარემოება, რომ იგი წარმოადგენს საქართველოში ერთ-ერთ პირველ მცდელობას შეისწავლოს სისხლის სამართლის კოდექსის 2010 წლის 24 სექტემბრის რედაქცია და მისი გამოყენება სასამართლო პრაქტიკაში.

კომპიუტერულ დანაშაულის წინააღმდეგ ბრძოლაში რამდენიმე მნიშვნელოვანი ნაბიჯი საქართველომ უკვე გადადგა. კერძოდ, საქართველოს კანონით „საქართველოს ზოგიერთ საკანონმდებლო აქტში ცვლილებების და დამატებების შეტანის შესახებ“ 24.09.2010წ. სისხლის სამართლის კოდექსში და სისხლის სამართლის საპროცესო კოდექსში უკვე განხორციელდა „კიბერდანაშაულის შესახებ“ კონვენციის ძირითადი პრინციპების ინტეგრაცია. მოგვიანებით, კერძოდ კი 2012 წლის 1 ივნისს საქართველოს პრეზიდენტმა გამოსცა ბრძანებულება „კიბერდანაშაულის შესახებ“ კონვენციის დამტკიცების თაობაზე. 2012 წლის 6 ივნისს კი საქართველოს მუდმივმა წარმომადგენელმა ევროპის საბჭოში ევროპის საბჭოს გენერალურ მდივანს „კიბერდანაშაულის შესახებ“ კონვენციის დამტკიცების სიგელი გადასცა⁹. საქართველოში ევროპის საბჭოს კონვენცია ოფიციალურად ძალაში 2012 წლის 1 ოქტომბრიდან შევიდა.¹⁰ ასევე, ძალიან მნიშვნელოვანი დოკუმენტია 2013 წლის 17 მაისის საქართველოს პრეზიდენტის №321 ბრძანებულება, რომლითაც დამტკიცდა „საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013-2015წ. სამოქმედო გეგმა“. აღნიშნული დოკუმენტი არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს სამოქმედო გეგმებს და ამოცანებს. მასზე

9 იხ. საქართველოს საგარეო საქმეთა სამინისტროს ოფიციალური ვებ-გვერდის ბმული: http://www.mfa.gov.ge/index.php?lang_id=GEO&sec_id=59&info_id=15216

10 იხ. ევროპის საბჭოს ოფიციალური ვებ-გვერდის ბმული: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>

დაყრდნობით, საქართველოს ხელისუფლება გაატარებს ღონისძიებებს, რომლებიც ხელს შეუწყობს სახელმწიფო ორგანოების, კერძო სექტორის და სამოქალაქო საზოგადოების კიბერსივრცეში დაცულად ფუნქციონირებას, ელექტრონული ოპერაციების უსაფრთხოდ განხორციელებას და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებლად მოქმედებას. ერთია, კიბერუსაფრთხოების სტრატეგიის შემოღებით გამოხატული სახელმწიფო ნება, იბრძოლოს კიბერდანაშაულის წინააღმდეგ, რაც მისასაღმებელი ნაბიჯია, თუმცა მეორეა, რამდენად ეფექტურად განხორციელდება სტრატეგიაში დასახული მიზნები.

კიბერდანაშაულის აქტუალობას და მნიშვნელობას კიდევ ერთხელ გაესვა ხაზი, საქართველოს მთავრობის 2013 წლის 2 ოქტომბრის დადგენილებით, რომელიც ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის ეროვნულ სტრატეგიის შეეხება. სტრატეგიის 1.3 პუნქტად გამოყოფილია კიბერდანაშაულის წინააღმდეგ ბრძოლა. მასში ხაზგასმულია კიბერდანაშაულის მზარდი საფრთხე და მისი აღკვეთის მნიშვნელობა სახელმწიფო და კერძო სექტორის ინტერესის დაცვისთვის. დოკუმენტი მიღწევად მიიჩნეეს ბოლო წლებში განვითარებულ საკანონმდებლო ცვლილებებს, შინაგან საქმეთა სამინისტროს ფარგლებში კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველოს და 24/7 ქსელის შექმნას. სტრატეგიაში აღნიშნულია, რომ საჭიროა მუშაობის გაგრძელება საზოგადოების ცნობიერების ამაღლების, კანონმდებლობის დახვეწის, სახელმწიფო როლის გაძლიერების, კერძო სექტორის იფორმირებულობის გაზრდის და საერთაშორისო თანამშრომლობის გაღრმავების კუთხით.

აღნიშნული დოკუმენტის პათოსს სრულად ვიზიარებ და მიმაჩნია, რომ ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის სტრატეგიაში კომპიუტერული დანაშაულის პრობლემის წარმოჩენა კიდევ ერთხელ ადასტურებს საქართველოს მზაობას, მიიღოს ახალი გამოწვევები და გადადგას სერიოზული ნაბიჯები კიბერდანაშაულის წინააღმდეგ ბრძოლაში.

კიბერდანაშაულის ცნება და სამართლებრივი კვლევის ისტორია

რატომ არის კომპიუტერული დანაშაული ძალიან მნიშვნელოვანი? პირველ რიგში იმიტომ, რომ როგორც ისტორია გვასწავლის კრიმინალები ხშირად ბოროტად იყენებენ ახალ ტექნოლოგიებს სარგებლის მისაღებად ან სხვებისთვის ზიანის მისაყენებლად. ავტომობილი ამის შესანიშნავი მაგალითია. ავტომობილი შეიქმნა კანონმორჩილი ადამიანების ტრანსპორტირებისთვის, მაგრამ მალე ის გადაიქცა სხვადასხვა დანაშაულის საგნად (მაგ. მანქანის ქურდობა, მანქანის გაქურდება), საშუალებად (მაგ. ბანკის ძარცვისას კართან მდგარი მანქანა) და იარაღად (მაგ. ავტოსაგზაო შემთხვევა, როდესაც დამნაშავე მიიმალება). კომპიუტერების შემთხვევაშიც აშკარად იგივე მეორდება¹¹.

კომპიუტერული დანაშაული ყურადღების ცენტრში პირველად აშშ-ში XX საუკუნის 70-იან წლებში მოექცა. ნაციონალურ და საერთაშორისო დონეზე დაიწყო ამ ფენომენის გამოკვლევა. მიღებულ იქნა სპეციალური ნორმები კიბერდანაშაულის მოსაწესრიგებლად. აშშ-ში ჯერ კიდევ 1977 წელს შეიმუშავეს კანონპროექტი „ფედერალური კომპიუტერული სისტემების დაცვის შესახებ“, რომელიც ითვალისწინებდა სისხლისსამართლებრივ პასუხისმგებლობას ისეთი ქმედებისთვის, როგორიცაა: კომპიუტერულ სისტემაში ცრუ მონაცემების შეყვანა, კომპიუტერული მონაცემების 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

11 იხ. SCOTT CHARNEY, KENT ALEXANDER, Types of computer crime, 25.11.2005 <http://www.crime-research.org/articles/types-of-computer-crime/2>

ცხადი გახადა, რომ ახალი კომპიუტერული და სატელეკომუნიკაციო ტექნოლოგიები დიდ პრობლემებს შეუქმნიდა სამართალდამცავ ორგანოებს. საყოველთაო „კომპიუტინგი“ (კომპიუტერების მასშტაბური ინტეგრაცია ყოველდღიურ ცხოვრებაში) მარტო ცხოვრების წესის შეცვლას კი არ ნიშნავდა, არამედ შეიცვლებოდა კრიმინალების მიერ დანაშაულებრივი საქმიანობის წარმართვის სპეციფიკაცია. მაგალითისთვის მოვიყვან სამივე შემთხვევას:

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 ინერდა ჰაკერის მოქმედებებს და პუშაობდა როგორც ადგილობრივ ასევე უცხოურ სატელეფონო კომპანიებთან, რათა დაედგინა თავდასხმის წყარო. აღმოჩნდა, რომ გერმანელ ჰაკერ მარკუს ჰესს აფინანსებდა რუსეთის სახელმწიფო უსაფრთხოების კომიტეტი, რათა გაემჟღავნებინა აშშ-ს სამხედრო საიდუმლოება. ამრიგად, ეს იყო მნიშვნელოვანი გაკვეთილი როგორც სამართალდაცავი 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. მეორე შემთხვევა დაკავშირებული იყო კომპიუტერულ ვირუსთან ე.წ. მორისის მატლთან (Morris worm). 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 გამორთვისას. სანამ კომპიუტერული ვირუსი გაუვნებელყოფილი იქნა, მან დააზიანა დაახლოებით 6200 კომპიუტერი და გამოიწვია 98 მილიონ დოლარზე მეტი ზარალი.

3. მესამე მაგალითი ეხება 1989 წლის თავდასხმას კომპანია „ბელსაუსზე“, რომელიც განხორციელდა „სიკედილის ლეგიონის“ სახელით ცნობილი ჰაკერთა ჯგუფის მიერ. მათთვის შესაძლებელი გახდა ადგილობრივ სატელეფონო სისტემაში ცვლილებების შეტანა და მონაცემების განადგურება¹².

მიუხედავად იმისა, რომ ამერიკელი გამომძიებლები განხილულ დანაშაულს წარმატებით გაუმკლავდნენ, აუცილებელი გახდა კომპიუტერული დანაშაულის შესახებ საკანონმდებლო ინიციატივის მომზადება, რომელსაც მხარი დაუჭირა ამერიკის გენერალური პროკურორის ეკონომიკური დანაშაულის საბჭომ. უკვე 1991 წლის სექტემბერში კი იუსტიციის დეპარტამენტის გენერალურ სასარჩელო განყოფილებაში შეიქმნა კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლის განყოფილება.

ჩემი აზრით, ზემოთმოყვანილი მაგალითი არის სახელმძღვანელო მემთხვევა მსოფლიოს სხვადასხვა სახელმწიფოსთვის კიბერ-დანაშაულის წინააღმდეგ ბრძოლაში და ასევე, ცალსახად მიმაჩნია, რომ საქართველომ ამ საკითხში ყოველთვის განსაკუთრებული ყურადღება უნდა მიაქციოს უცხოურ გამოცდილებას.

დიდი ბრიტანეთი მრავალი წლის მანძილზე უშედეგოდ ცდილობდა კომპიუტერული დანაშაულის წინააღმდეგ გამოეყენებინა სასამართლო წარმოებაში მიღებული მრავალსაუკუნოვანი გამოცდილება, თუმცა უშედეგოდ. 1990 წლის აგვისტოში ძალაში შევიდა კანონი „კომპიუტერული ტექნოლოგიის არასანქცირებული გამოყენების შესახებ“, რომლითაც დასჯადად გამოცხადდა კომპიუტერში ან მასში დაცულ ინფორმაციაში ან/და პროგრამაში წინასწარ

12 იხ. SCOTT CHARNEY, KENT ALEXANDER, Types of computer crime, 25.11.2005 <http://www.crime-research.org/articles/types-of-computer-crime/2> (სამივე კაზუსი განხილულია მოცემული სტატიის საფუძველზე).

განზრახული უკანონო შეღწევა, ასევე ამ ინფორმაციის ბლოკირება, მოდიფიცირება, განადგურება ან კოპირება¹³.

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. 1993 წელს მსგავსი ცვლილებები განიცადა ჰოლანდიის სისხლის სამართლის კოდექსმა და დანაშაულად გამოცხადდა კომპიუტერში არასანქცირებული შეღწევა, კომპიუტერული საბოტაჟი, ვირუსების გავრცელება და სხვ.

ბოლო წლებში კომპიუტერული დანაშაული აღიარებულია საერთაშორისო ხასიათის დანაშაულად და მის წინააღმდეგ ბრძოლა წარმოადგენს მრავალი საერთაშორისო ორგანიზაციისთვის პრიორიტეტულ მიმართულებას.

გაერო-ს მიერ მიღებულ იქნა „ინფორმაციული ტექნოლოგიების გამოყენებით ჩადენილი დანაშაულის წინააღმდეგ ბრძოლის შესახებ“ რეზოლუციები, რომლებშიც ხაზგასმულია ყველა წევრი სახელმწიფოს მხრიდან საკუთარი საკანონმდებლო ბაზის გადახედვის და მისი სრულყოფის აუცილებლობა.

ეკონომიკური განვითარებისა და თანამშრომლობის ორგანიზაცია 1983 წლიდან სწავლობს და ამზადებს შესაბამის რეკომენდაციებს, რათა საერთაშორისო დონეზე მსგავს დანაშაულებრივ შემთხვევებზე განხორციელდეს ანალოგიური სისხლისსამართლებრივი პასუხისმგებლობის დაკისრება.

13 საქართველოს სისხლის სამართლის კოდექსი მასში შეტანილ ცვლილებამდე შეიცავდა მსგავსი შინაარსის დანაშაულებრივ ქმედებას, კერძოდ, სისხლის სამართლის კოდექსის ძველი რედაქციის 284-ე მუხლის მიხედვით დასჯადი იყო: „კანონით დაცულ კომპიუტერულ ინფორმაციასთან, ე.ი. მანქანა მატარებელზე, ელექტრო გამომთვლელ მანქანაზე (ეგმ-ზე), ეგმ-ის სისტემაში ან მათ ქსელში ასაბულო ინფორმაციასთან არაშეშორებლად შეღწევა, რამაც ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან მოპოვება ან და ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მოშლა გამოიწვია, ასევე მობილური მონაცემების საერთაშორისო იდენტიფიკატორის შეცვლა.“

დიდი რვიანის ქვეყნებს შექმნილი აქვთ საკონტროლო პუნ-
ქტების მუდმივმოქმედი ქსელი, რომელსაც კომპიუტერულ დანა-
შაულთან დაკავშირებით წამოჭრილი პრობლემების გამო შეუძლია
მიმართონ საერთაშორისო თანამშრომლობის პროცესის მონაწილე
ყველა წევრმა¹⁴.

მნიშვნელოვან დოკუმენტს წარმოადგენს ეუთო-ს მიერ მიღებული
გადაწყვეტილება: ორგანიზაცია წევრ-სახელმწიფოებს აძლევს რე-
კომენდაციას შეუერთდნენ ევროსაბჭოს მიღებულ კონვენციას „კიბერ-
დანაშაულის შესახებ“ და „დიდი რვიანის“ ქვეყნების მიერ კომპიუტერ-
ული დანაშაულის წინააღმდეგ ბრძოლისთვის შექმნილ მუდმივმოქმედ
ქსელს, რომლის მიზანია კვირაში შვიდი დღე ოცდაათი საათი მოკავ-
შირე სახელმწიფოებისთვის ინფორმაციის მიწოდება და კომპეტენციის
ფარგლებში სათანადო დახმარების აღმოჩენა.¹⁵

საინტერესოა, რომ მსგავსი ქსელი შექმნილია ინტერპოლის
ფარგლებშიც. იგი მთელი მსოფლიოს მასშტაბით აერთიანებს
ასამდე მუდმივმოქმედ დანესებულებას, რომელიც ინტერპოლის
წევრ-სახელმწიფოებს ეხმარება მოძებნონ საჭირო სპეციალისტი
სხვა ქვეყანაში, დროულად მიიღონ მათი დახმარება კომპიუტერული
დანაშაულის გამოძიების და მასზე მტკიცებულების შეგროვებასთან
დაკავშირებით¹⁶.

საერთაშორისო აქტებიდან საქართველოსთვის ყველაზე მნიშ-
ვნელოვან დოკუმენტს წარმოადგენს ევროსაბჭოს კონვენცია
„კიბერდანაშაულის შესახებ“, რომელიც მიღებულ იქნა 2001 წლის

14 იხ. Pedro Verdelho, Cybercrime and Electronic Evidence, E-Newsletter “Electronic Newsletter on the Fight Against Cybercrime” (ENAC) №1, jule, 2009, გვ. 2

15 აღნიშნული ვალდებულება სახელმწიფოებს „კიბერდანაშაულის შესახებ“
ევროსაბჭოს კონვენციის რატიფიცირების შემთხვევაში ისედაც უჩნდებათ,
ხოლო ევროკავშირის საბჭოს №2005/222 ჩარჩო გადაწყვეტილების თანახმად
მუდმივი ქსელის შექმნის ვალდებულება ევროკავშირის ყველა წევრ-ქვეყანას
გააჩნია.

16 იხ. <http://www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf>

23 ნოემბერს ქ. ბუდაპეშტში¹⁷ ევროსაბჭოს 41 წევრი სახელმწიფოს მიერ. აღნიშნული დოკუმენტი წარმოადგენს მსოფლიოს მასშტაბით ერთ-ერთ პირველ სერიოზულ მცდელობას კიბერდანაშაულის წინააღმდეგ ბრძოლაში: ნაციონალური უსაფრთხოების დასაცავად, ერთიანი სტრატეგიის ჩამოყალიბებისთვის და ურთიერთთანამშრომლობისთვის. მას, გარდა ევროპული ქვეყნებისა, ხელი მოაწერეს კანადამ, იაპონიამ, სამხრეთ აფრიკამ, აშშ-მ¹⁸. საინტერესოა, რომ 2008 წლის აპრილში რუსეთის ფედერაციამ უარი თქვა კონვენციის ხელმოწერაზე, ხოლო ამავე წლის ივლისში კონვენციას ხელი მოაწერა აზერბაიჯანმა¹⁹.

კონვენცია განსაზღვრავს ექსტრადიციის და ორმხრივი დახმარების პრინციპებს. ევროსაბჭოს წევრ ქვეყნებიდან კონვენციის რატიფიცირება და შესაბამისად კონვენციაში მოცემული ქმედებების კრიმინალიზაცია და სხვა პრინციპების მოქმედება ეროვნული კანონმდებლობის დონეზე განხორციელდა შემდეგ სახელმწიფოებში: ალბანეთი, სომხეთი, ბოსნია, ბულგარეთი, ხორვატია, კვიპროსი, დანია, ესტონეთი, ფინეთი, საფრანგეთი, გერმანია, უნგრეთი, ისლანდია, იტალია, ლიტვა, ლატვია, მოლდავა, ნიდერლანდები, ნორვეგია, რუმინეთი, სერბეთი, სლოვაკეთი, სლოვენია, მაკედონია, უკრაინა²⁰.

დღეის მდგომარეობით კონვენცია „კიბერდანაშაულის შესახებ“, წარმოადგენს ერთ-ერთ უმთავრეს დოკუმენტს და გარანტიას

17 ევროსაბჭოს კონვენცია საქართველოსთვის მნიშვნელოვანი გახდა მას შემდეგ, რაც 2009 წლის 1 ივნისიდან 2010 წლის 31 მაისამდე, ევროსაბჭოს ორგანიზებით საქართველოში განხორციელდა „კიბერდანაშაულის პროექტი საქართველოში“, რომლის ფარგლებშიც ევროსაბჭოს კონვენციის მოთხოვნების შესაბამისად მომზადდა საკანონმდებლო ცვლილებების პროექტი. იგი მოგვიანებით სრულად იქნა ასახული საქართველოს სისხლის სამართლის კოდექსში და საქართველოს სისხლის სამართლის საპროცესო კოდექსში. (შეგიძლიათ იხილოთ პროგრამის ოფიციალური ვებ-გვერდი: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_en.asp).

18 იხ. http://en.wikipedia.org/wiki/Convention_on_Cybercrime

19 იხ. <http://www.today.az/news/society/46054.html>

20 ნაშრომში გამოყენებულია მონაცემები 2012 წლის მდგომარეობით. უკანასკნელი ცნობები იხ. საიტზე <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>

მსოფლიოს სახელმწიფოთა ნაციონალური უსაფთხოების დასაცავად და ურთიერთთანამშრომლობისთვის კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლაში. თუმცა გამოცდილებამ ცხადყო, რომ მხოლოდ კონვენციის მიღება ზემოაღნიშნული ეფექტის მისაღებად არ აღმოჩნდა საკმარისი, რადგან არც ევროსაბჭოს და არც ევროკავშირის წევრ სახელმწიფოთა უმრავლესობამ არ მოახდინა კონვენციის რატიფიცირება, ნაწილმა კი მხოლოდ მისი ხელმოწერა განახორციელა.

არაოფიციალურად, სწორედ ევროპის საბჭოს კონვენციის მიმართ ევროპის ქვეყნების მხრიდან გამოჩენილი გულგრილობა დაედო საფუძვლად ევროკავშირის საბჭოს 2005 წლის 24 თებერვალის №2005/222 ჩარჩო გადაწყვეტილების მიღებას „კომპიუტერულ სისტემაზე შეტევის წინააღმდეგ“, რომელიც იმეორებდა კონვენციის ძირითად პრინციპებს და ევროკავშირის წევრ-სახელმწიფოებს ავალდებულებდა მოეხდინათ გადაწყვეტილებით განსაზღვრული ქმედების კრიმინალიზაცია ნაციონალურ სისხლის სამართლის კანონმდებლობაში ცვლილებების შეტანის გზით. ევროკავშირის წევრი ქვეყნებისთვის ასევე, სავალდებულო გახდა 24 საათიანი ცხელი ხაზის სამსახურის შექმნა. ამ ვალდებულების შესრულებისთვის წევრ სახელმწიფოებს ვადა განესაზღვრათ 2007 წლის 16 მარტამდე²¹. მანამდე, კონვენციის რატიფიცირება განხორციელებული პქონდა ევროკავშირის მხოლოდ 13 ქვეყანას, რაც რა თქმა უნდა, არ შეიძლება ჩათვლილიყო პოზიტიურ ტენდენციად.

აღნიშნული ჩარჩო გადაწყვეტილების საფუძველზე 2007 წლის 16 მარტამდე კომპიუტერული დანაშაულის წინააღმდეგ ჩამოყალიბებულ ძირითად დებულებს უნდა შეერთებოდა ევროკავშირის დანარჩენი ქვეყნებიც. უფრო კონკრეტულად კი, ჩარჩო გადაწყვეტილების მიხედვით, სისხლისსამართლებრივ პასუხისმგებლობას უნდა დაქვემდებარებოდა საინფორმაციო სისტემაში უნებართვო შეღწევა (გადაწყვეტილების მე-2 მუხლი), სისტემაში უნებართვო

21 იხ. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Article 12. (Official journal of the European Union L69/67, from 16.3.2005)

ჩარევა ანუ კომპიუტერული მონაცემების შეყვანის, გადაცემის, დაზიანების, წაშლის, გაუარესების შეცვლის ან დაფარვის გზით საინფორმაციო სისტემის ფუნქციონირების არსებითი შეფერხება (მე-3 მუხლი) და კომპიუტერული მონაცემების უნებართვო წაშლა, დაზიანება, გაუარესება შეცვლა ან დაფარვა (მე-4 მუხლი).

საინტერესოა ისიც, რომ განსხვავებით „კიბერდანაშაულის შესახებ“ კონვენციისაგან, ევროკავშირის საბჭოს ჩარჩო გადანყვეტილებაში ნაცვლად ტერმინისა „კომპიუტერული სისტემა“, გამოყენებულია ტერმინი „საინფორმაციო სისტემა“. თუკი ვიმსჯელებთ ამ ტერმინთაგან რომელიმეს უპირატესობაზე ან სიზუსტეზე, ცხადია, რომ ევროკავშირის გადანყვეტილებით განსაზღვრული დეფინიცია საინფორმაციო სისტემის შესახებ წარმოადგენს, უფრო სრულყოფილს და ყოვლისმომცველს. კერძოდ, თუ „კომპიუტერული სისტემა“ განიმარტება როგორც ნებისმიერი მექანიზმი ან ურთიერთდაკავშირებულ მექანიზმთა ჯგუფი, რომელიც ერთი ან მეტი პროგრამის მეშვეობით ასრულებს მონაცემთა ავტომატურ დამუშავებას, „საინფორმაციო სისტემის“ დეფინიცია განმარტებულია როგორც ნებისმიერი მექანიზმი ან ურთიერთდაკავშირებულ მექანიზმთა ჯგუფი, რომელიც ერთი ან მეტი პროგრამის მეშვეობით ასრულებს მონაცემთა ავტომატურ დამუშავებას, ასევე მონაცემთა შენახვას, აღდგენას და გადაგზავნას სისტემის გამოყენების, მუშაობის, დაცვისა და ტექნიკური მომსახურების მიზნების შესაბამისად.

გადაწყვეტილების თანახმად, სისხლის სამართლის პასუხისმგებლობა უნდა გავრცელდეს მე-2, მე-3 და მე-4 მუხლით გათვალისწინებული ქმედებების ჩადენის წაქეზება, დახმარება, ნახალისება ან მცდელობა. დამამძიებელ გარემოებად დადგინდა დანაშაულის ჩადენა კრიმინალური დაჯგუფების მიერ.

„კიბერდანაშაულის შესახებ“ კონვენციის მსგავსად, გადანყვეტილება ადგენს იურიდიული პირის სისხლისსამართლებრივ პასუხისმგებლობას, თუმცა განსხვავებით კონვენციისგან ნევრ-სახელმწიფოებს უდგენს სასჯელის კონკრეტულ სახეებსაც, კერძოდ: საზოგადოებრივი სარგებლის ან დახმარების მიღების უფლებამოსილების ჩამორთმევას, დროებით ან მუდმივ დისკვალიფიკაციას

კომერციულ საქმიანობაში, იურიდიული ზედამხედველობის დაწესებულებას, სამართლებრივ ლიკვიდაციას²².

საინტერესოა, რომ 2007 წლის 16 მარტამდე მხოლოდ შედეგთმა შეძლო ჩარჩო გადანყვეტილებით დაკისრებული ვალდებულების შესრულება. დანარჩენმა ქვეყნებმა მის შესრულებაზე ანგარიშის წარდგენა მხოლოდ 2008 წლის ივლისამდე მოახერხეს. მათ რიგებში არ იყვნენ პოლონეთი, ესპანეთი, მალტა, და სლოვაკეთი, ხოლო ირლანდიაში, გაერთიანებულ სამეფოში და საბერძნეთში ქვეყნის მთავრობების მიერ არ იქნა გათვალისწინებული კომისიის მიერ მიღებული შეფასება გადანყვეტილების შესრულების შესახებ²³.

ევროკავშირის საბჭოსადმი წარდგენილ იქნა მოხსენება, რომლის მიზანიც იყო შეეფასებინა, რამდენად სწორად იქნა განხორციელებული ევროკავშირის საბჭოს ჩარჩო გადანყვეტილება. ყურადღებას გაავამახვილებ რამდენიმე ასპექტზე. ისევე როგორც კონვენცია „კიბერდანაშაულის შესახებ“, ჩარჩო გადანყვეტილებითაც დანაშაულებრივ ქმედებას წარმოადგენს კომპიუტერულ სისტემაში უნებართვო შეღწევა და ამ ქმედების დანაშაულად კვალიფიკაცია არ უკავშირდება მის შედეგს. დანაშაული დამთავრებულად ითვლება უნებართვო შეღწევის განხორციელების მომენტიდან და არა ამ სისტემაში არსებული მონაცემების დაზიანების, მოპოვების ან სხვა მავნე შედეგის დადგომიდან. მიუხედავად ამისა, ავსტრიამ, ჩეხეთმა, ლატვიამ და ფინეთმა კომპიუტერულ სისტემაში უნებართვო შეღწევის გამო დასჯადობა დაუკავშირა დანაშაულებრივი შედეგის დადგომას, კერძოდ, დამდგარ ზიანს ან ზიანის საფრთხეს.²⁴

„კიბერდანაშაულის შესახებ“ კონვენციამ მე-5 მუხლის მიხედვით დასჯადად გამოაცხადა კომპიუტერული სისტემის ფუნქციონირებისთვის საფრთხის შექმნა, რომელიც ჩადენილია კომპიუტერულ მონაცემთა შეყვანის, გადაცემის, დაზიანების, ნაშლის და დაფარვის

22 იხ. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Article 8-9. (Official journal of the European Union L69/67, from 16.3.2005)

23 იხ. Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448 (Based on article 12 of the Council Framework Decision of 24.02.2005 on attacks against information systems).

24 იხ. იქვე.

გზით, ხოლო ევროკავშირის ჩარჩო გადანყვეტილების მე-3 მუხლის მიხედვით კი ყველა მონაწილე სახელმწიფო ვალდებულია მიიღოს საჭირო ზომები, რათა უზრუნველყოს იგივე ქმედების კრიმინალიზაცია. თუმცა, ავსტრიაში დასჯადია ასეთი ქმედება მხოლოდ იმ შემთხვევაში, თუ ის ატარებს მძიმე დანაშაულის ნიშნებს; ჩეხეთი, ესტონეთი და ლიტვა აუცილებელ პირობად მიიჩნევენ ასეთი ქმედებით გამონეულ ზიანს. ლატვიელი კანონმდებლების აზრით კი საინფორმაციო სისტემაში ჩარევა დანაშაულია მხოლოდ იმ შემთხვევაში, თუ იგი განხორციელდა დაცვის სისტემის განადგურებით ან გამოიწვია დიდი ოდენობის დანაკარგი.

ჩემი აზრით, კონვენციას და ჩარჩო გადანყვეტილებას შორის არსებული განსხვავებები ფუნდამენტურ ხასიათს არ ატარებს. ასევე, არ იქნება მართებული იმ სახელმწიფოების კანონმდებლების კრიტიკა, რომლებმაც კონვენციის და ჩარჩო გადანყვეტილების რიგი თეზისები განსხვავებულად ჩამოაყალიბეს. მთავარია, რომ ჩარჩო გადანყვეტილების მიღებამ შედეგი მოიტანა. კერძოდ, აღნიშნული გადანყვეტილების გამოცემის შემდეგ, ევროპის საბჭოს კონვენციას მრავალი ისეთი ქვეყანა შეუერთდა, რომელიც მანამდე თავს იკავებდა. მაგალითად, დიდი ბრიტანეთი, იტალია და ა.შ.

მსოფლიოში კომპიუტერული დანაშაულის საკანონმდებლო რეგულირების მცდელობის გარდა, ფართოდ გაიშალა მუშაობა კომპიუტერული დანაშაულის ერთიანი დეფინიციის ჩამოსაყალიბებლად. 1983 წელს პარიზში ექსპერტების ჯგუფმა ჩამოაყალიბა კომპიუტერული დანაშაულის ცნება: „კომპიუტერული დანაშაული არის კანონით აკრძალული, არაეთიკური ქმედება, რომელიც აფერხებს მონაცემთა ბაზების ავტომატიზებულ მუშაობას ან ინფორმაციის გადაცემას.“²⁵

ჩემი აზრით, ეს დეფინიცია არასრულყოფილია: პირველ რიგში, მიუღებელია ტერმინი „არაეთიკური ქმედება“, რადგან ბუნდოვანი და არაერთგვაროვანი შინაარსის მატარებელია. მეორე ნაკლები კი გახლავთ, ის, რომ კომპიუტერული დანაშაული მოქცეულია

25 იხ. Richard W. Aldrich, "CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME", USAF Institute for National Security Studies USAF Academy, Colorado, April 2000, გვ.10

გარკვეულ ჩარჩოში. კერძოდ, დეფინიციის ავტორების აზრით, მან შესაძლებელია ხელყოს მხოლოდ მონაცემთა ბაზების ავტომატიზებული მუშაობა და ინფორმაციის გადაცემა. შესაძლოა, 1983 წელს ექსპერტები კომპიუტერულ დანაშაულში მეტ საფრთხეს ვერ ხედავდნენ, თუმცა მეექვსეა არ სცოდნოდათ, რომ კომპიუტერული დანაშაულის მეშვეობით ხდება არა მარტო ინფორმაციის გადაცემის ხელყოფა, არამედ მისი განადგურება, მეცვლა, კოპირება და ა.შ. ამდენად, 1983 წელს შემუშავებულმა დეფინიციამ სამართლიანად ვერ დაიმკვიდრა ადგილი მსოფლიოში და მალე დავიწყებას მიეცა.

1993 წელს ინტერპოლის მუშაობის ჩარჩოებში ორგანიზებული სემინარის „კრიმინალისტიკა და კომპიუტერული დანაშაულის“ ფარგლებში კი კომპიუტერული დანაშაულის ცნებამ შემდეგნაირი სახე მიიღო: „სისხლის სამართლით გათვალისწინებული საზოგადოებრივად საშიში ქმედება, რომელშიც მანქანური ინფორმაცია წარმოადგენს დანაშაულებრივი ხელყოფის საშუალებას ან ობიექტს.“²⁶

მომავალი არც ამ განმარტებას ჰქონია. აღიარება ვერც მან ჰპოვა, რადგან, ჩემი აზრით, ვერც ის მოიცავდა კიბერდანაშაულის არსს სრულყოფილად.

მოცემული ცნების მთავარი ნაკლი ისაა, რომ ავტორებმა კომპიუტერული ინფორმაცია წარმოადგინეს როგორც დანაშაულის ჩადენის საშუალება და ობიექტი. თუმცა არ აღუნიშნავეთ, რომ ის შეიძლება კომპიუტერული დანაშაულის საგანიც იყოს.

2000 წლის 10-19 აპრილს გაეროს X კონგრესზე კიდევ ერთ მცდელობას ჰქონდა ადგილი, შემოეღოთ ერთიანი კიბერდანაშაულის ცნება. გაერომ განმარტა, რომ კიბერდანაშაულზე უნდა ვიმსჯელოთ ვიწრო და ფართო გაგებით. პირველი მათგანი მოიცავს კომპიუტერულ დანაშაულს, მეორე კი კომპიუტერის გამოყენებასთან დაკავშირებულ დანაშაულს. ვიწრო გაგებით, კიბერდანაშაული ესაა: „ელექტრონული ოპერაციებით ჩადენილი კანონით აკრძალული ქმედება, რომელის მიზანია კომპიუტერული სისტემის და მათი მონაცემების უსაფრთხოების ხელყოფა.“ ფართო გაგებით კი კიბერდანაშაულია: „კანონით აკრძალული ნებისმიერი ქმედება, რომელ-

26 იხ. ა. კაცმანი, „კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება“, ჟურნ. „სამართალი“ 2000წ. №2. გვ. 58.

იც დაკავშირებულია კომპიუტერების, მათი სისტემის და ქსელის გამოყენებასთან, მათ შორის კომპიუტერული სისტემის ან ქსელის გამოყენებით ინფორმაციის უკანონო შენახვა, შეთავაზება და გავრცელებასთან.²⁷

მოცემული დეფინიციის პირველი ნაწილი არსებულ სხვა დეფინიციებთან შედარებით სრულყოფილად მიმაჩნია. თუმცა მის მეორე ნაწილს, რომელიც კიბერდანაშაულის ფართო გაგებით განმარტებას ეხება, ვერ გავიზიარებ. კერძოდ, კომპიუტერის საშუალებით ბავშვთა პორნოგრაფიის გავრცელება, ქსენოფობიური ინტენეტ-გვერდების შემწეა, სოციალურ ქსელში რასისტული ნიშნით ადამიანების შეურაცხყოფა, მხოლოდ იმიტომ რომ მისი ჩადენა კომპიუტერის საშუალებით ხდება, არ უნდა მივიჩნიოთ კიბერდანაშაულად. ამასთან დაკავშირებით უფრო დეტალურად ნაშრომის შესაბამის თავში ვისაუბრებ.

კიბერდანაშაულის სხვა ცნებების გახსენებაც შეიძლება. თუმცა ისინი საერთაშორისო აღიარებას ვერ აღწევდნენ. მაგალითად, 2002 წელს პროფ. დ. შინდერმა გააკრიტიკა აშშ-ს იუსტიციის დეპარტამენტის მიერ შემოთავაზებული კიბერდანაშაულის ცნება, რომლის მიხედვითაც: „კიბერდანაშაულია კანონით აკრძალული ისეთი ქმედება, რომლის ჩადენა და გამოძიება უკავშირდება კომპიუტერული ტექნოლოგიებში გარკვეული ცოდნის ქონას.“ დ. შინდერის აზრით, ამ ლოგიკით, ნებისმიერი დანაშაულის გამოძიების დროს, თუ გამოძიებელი ისარგებლებდა კომპიუტერული ბაზით, უნდა ჩაგვეთვალოს, რომ რადგან ამ დანაშაულის გამოძიება უნებლიედ დაუკავშირდა კომპიუტერულ ტექნოლოგიებში არსებული ცოდნის გამოყენებას გამოსაძიებელი დანაშაული კომპიუტერული დანაშაულია.²⁸ ბუნებრივია, დ. შინდერის კრიტიკა აბსოლუტურად საფუძვლიანია.

იმავე ნაშრომში დ. შინდერი ხაზს უსვამდა, რომ საერთაშორისო დონეზე აღიარებული კიბერდანაშაულის ცნება არ არსებობდა და

27 იხ.

(ix. <http://ebookuniverse.net/aconf18710-pdf-d8490066>) გვ.5

28 იხ. Debra Littlejohn Shinder, "Scene of the Cybercrime: Computer Forensics Handbook", USA, Rockland, Syngress Publishing Inc. 2002. გვ.6

თავის მხრივ აღნიშნავდა, რომ: „კიბერდანაშაული არის კომპიუტერული დანაშაულის ქვეკატეგორია, რომელიც მოიცავს ინტერნეტის ან კომპიუტერული ქსელის გამოყენებით ჩადენილ დანაშაულს.“²⁹ ჩემთვის გაუგებარია, მაშინ როცა, გაერო პირიქით, კიბერდანაშაულის ქვეკატეგორიად გამოყოფს კომპიუტერულ დანაშაულს, რატომ აკეთებს პირიქით დ. შინდერი? პროფ. ტ. ტროპინა, იმონებს პროფ. ს. ბრენერის და მ. გუდმანის შეხედულებას და ამტკიცებს, რომ „კიბერდანაშაული“ ბევრად უფრო ზოგადი და ყოვლისმომცველი ტერმინია, რომელშიც უნდა ვიგულისხმოთ, როგორც ტრადიციული დანაშაული ჩადენილი კომპიუტერული ტექნიკის დახმარებით. ასევე, უშუალოდ ის დანაშაულები, რომლებიც მიმართულია კომპიუტერული სისტემის, პროგრამის და მონაცემების წინააღმდეგ³⁰. როგორც უკვე აღინიშნა ამავე პოზიციაზეა გაერო და ის ზოგადი მნიშვნელობით იყენებს ტერმინს „კიბერდანაშაული“, ვინრო მნიშვნელობით კი „კომპიუტერულ დანაშაულს“. ასევე, ევროპის საბჭოც, რომელმაც კონვენციის სათაურში სწორედ ტერმინი „კიბერდანაშაული“ გამოიყენა. მიუხედავად იმისა, რომ გადამწყვეტად არ მიმაჩნია თუ რომელი ტერმინის გამოყენებას მივანიჭებთ უპირატესობას, ტ. ტროპინას და მის თანამოაზრეებს მაინც არ ვეთანხმები, იმიტომ, რომ „კიბერდანაშაულის“ ფართო გაგების თეორიას ზოგადად არ ვიზიარებ და ჩემი აზრით, მასში ისეთი დანაშაულის გაიგივება, რომლის ჩადენაც კომპიუტერის დახმარებით ხდება, არამართებულია. ჩემი აზრით, კიბერდანაშაულში უნდა ვიგულისხმოთ მხოლოდ ის კანონით აკრძალული ქმედება, რომლის მიზანია კომპიუტერული სისტემის და მონაცემის ხელყოფა. ამ საკითხს, კერძოდ კომპიუტერული ტექნიკის გამოყენებით ჩადენილი დანაშაულის უფრო დაწვრილებით შეფასებას ნაშრომის შესაბამის თავში დავუთმობ ადგილს.

დ. შინდერის ნაშრომის გამოქვეყნებიდან 11 წელი გავიდა და კიბერდანაშაულის ცნების შემოღების საკითხი დღემდე გადაუჭრელ ამოცანად რჩება. ამერიკელი მეცნიერები კ. ფინკლ და კ. თეო-

29 იხ. Debra Littlejohn Shinder, "Scene of the Cybercrime: Computer Forensics Handbook", USA, Rockland, Syngress Publishing Inc. 2002. გვ. 5

30 Татьяна Тропина, «Киберпреступности: понятие, составление, уголовно-правовые меры борьбы» (იხ. <http://www.crime.vl.ru/index.php?p=3626&print=1&more=1>).

პარი 2012 წელს გამოქვეყნებულ ნაშრომში აღნიშნავდნენ, რომ კიბერდანაშაულის ერთიანი ცნების შემოღება დღემდე ვერ ხერხდება. მათ მოჰყავდათ კომპიუტერული უსაფრთხოების საკითხებში მსოფლიოში ყველაზე მსხვილი კორპორაცია „სიმანტეკის“ (Symantec Corporation) მიერ შემოთავაზებული დეფინიცია, რომლის მიხედვითაც: „კიბერდანაშაულია კომპიუტერის ან მისი ქსელის საშუალებით ჩადენილი ნებისმიერი დანაშაული“, თუმცა აღნიშნავდნენ რომ ეს დეფინიცია არ გამოდგებოდა კიბერდანაშაულის ერთიან ცნებად, რადგან კიბერდანაშაული მოიცავს ისეთ საკითხებს, რომელიც განხილულ უნდა იქნეს შესაბამისი ქვეყნის მთავრობის მიერ ორგანიზებულ ფართო დისკუსიის და მსჯელობის რეჟიმში³¹. ვეთანხმები, მათ მოსაზრებას და დავამატებ, რომ კიბერდანაშაულის ცნების შემოღება კონკრეტული სახელმწიფოს და საერთაშორისო ორგანიზაციების საქმეა და არა კომპიუტერული უსაფრთხოების საკითხებში მოღვაწე კორპორაციების და სხვა კერძო ორგანიზაციების.

როგორც უკვე ითქვა, კიბერდანაშაულის ერთიანი ცნების შემოღება ბოლო წლებში არცერთ ქვეყანას თუ საერთაშორისო ორგანიზაციას უცდია, რადგან რთულია ზოგადად, კიბერდანაშაული მოვაქციოთ სამ-ოთხ ნინადადებაში. თან ისე, რომ მასში ასახვა ჰპოვოს კომპიუტერული დანაშაულის ყველა ნიშანმა და თავისებურებამ. ამდენად, კიბერდანაშაულის ცნების იდეალურ განმარტებაზე არც ამ ნაშრომს ექნება პრეტენზია. თუმცა, ჩემი აზრით, აღნიშნული ცნება შეიძლება ჩამოყალიბდეს შემდეგნაირად:

კიბერდანაშაული არის სისხლის სამართლის კოდექსით აკრძალული ქმედება, რომელიც მიმართულია კომპიუტერული სისტემის ან მონაცემის უსაფრთხოების ხელყოფის ან/და ნორმალური ფუნქციონირების შეფერხებისკენ, ასევე, კომპიუტერული მონაცემის უნებართვო დაფარვის, შეცვლის, ნაშლის, კოპირების ან დაზიანებისკენ.

31 იხ. Kristin M. Finklea, Catherine A. Theohary, „Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement“, US Congressional Research Service Reports, 2012, გვ.2

კომპიუტერული დანაშაულის სამართლებრივი მონესრიგება საქართველოში

1. ახალი საკანონმდებლო რეგულირების წინაპირობები

2009 წლის 9 იანვარს ვაშინგტონში, საქართველოს და აშშ-ს მიერ ხელმოწერილ იქნა ქარტია სტრატეგიული პარტნიორობის შესახებ, რომელიც ქვეყნებს შორის თანამშრომლობის ერთ-ერთ პრიორიტეტად გამოყოფს კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლას. კერძოდ, ქარტიის მე-4 ნაწილი „დემოკრატიის გაძლიერება“ შეიცავს მე-3 პუნქტს, რომელშიც წერია: „ჩვენ ვგეგმავთ, ჯეროვანი ძალისხმევა მივმართოთ ისეთი საერთო ტრანსნაციონალური დანაშაულის საფრთხის წინააღმდეგ, როგორიცაა ტერორიზმი, ორგანიზებული დანაშაული, ადამიანებით ვაჭრობა, იარაღით უკანონო ვაჭრობა, ფულის გათეთრება და კომპიუტერული დანაშაული“.³²

2009 წლის აგვისტოში, კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლის შესახებ კომპიუტერულ-საინფორმაციო ბიულეტენის „ENAC“-ის ფურცლებზე ევროპის საბჭოს „კიბერსივრცეში კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლის“ პროგრამის ხელმძღვანელმა კრისტინა შულმანმა განაცხადა, რომ მიმდინარე პროგრამებიდან ერთ-ერთი ყველაზე მნიშვნელოვანი არის „კომპიუტერული დანაშაულის შესახებ“ პროექტი საქართველოში, რომლის მიზანია დაეხმაროს საქართველოს სათანადო პოლიტიკის შემუშავებაში „კიბერდანაშაულის შესახებ“ ევროსაბჭოს კონვენციის რეალიზაციასთან დაკავშირებით³³. აღსანიშნავია, რომ პროექტის ფარგლებში შექმნილმა მუშა-ჯგუფმა საკანონმდებლო ცვლილების პირველადი ვერსია წარადგინა 2010 წლის 13-14 მაისს თბილისში

32 იხ. http://www.freegeorgia.ge/uploads/files_11_1.PDF

33 იხ. Cristina Schulman, Council of Europe measures for fighting against cybercrime, E-Newsletter “Electronic Newsletter on the Fight Against Cybercrime” (ENAC) №2, August, 2009, გვ 35

გამართულ რეგიონულ კონფერენციაზე³⁴. კონფერენციას გარდა ქართველი და უცხოელი ექსპერტებისა ესწრებოდა ქ-ნი ქრისტიანა შულმანი. მან ქართველი კანონმდებლების მუშაობა დადებითად შეაფასა. უნდა აღინიშნოს, რომ ცვლილებების ეს პროექტი შემდგომში კიდევ ერთხელ შეიცვალა და საბოლოო სახე მიიღო საქართველოს კანონში „საქართველოს ზოგიერთ საკანონმდებლო აქტში ცვლილებების და დამატებების შეტანის შესახებ“ (24.09.2010წ.). ამჟამად კანონით, საქართველოს სისხლის სამართლის კოდექსის გარდა, შესწორებები შევიდა საქართველოს სისხლის სამართლის საპროცესო კოდექსში, კანონებში „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ და „ელექტრონული კომუნიკაციების შესახებ“.

საკანონმდებლო ცვლილებებზე მუშაობა არ მიმდინარეობდა დახურულ კარს მიღმა. მასში მონაწილეობას იღებდნენ ევროპის საბჭოს კომპიუტერულ დანაშაულის სფეროში მოღვაწე ყველაზე ცნობილი ექსპერტები, ასევე საქართველოს სხვადასხვა უწყების წარმომადგენლები და მონვეული წევრები.

რთულია დაადგინო, რა დრო დაგვჭირდება ამ ცვლილებების პრაქტიკული ეფექტის შესაფასებლად, თუმცა ფაქტია, რომ მთავარი გამოწვევა, რომელიც იდგა საკანონმდებლო ცვლილებებზე მომუშავე ჯგუფის წინაშე, მიღწეულია. კერძოდ, საქართველოს სისხლისსამართლებრივი კანონმდებლობა მაქსიმალურად დაახლოვებულია ევროპულთან, რაც კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლაში ქმნის საფუძველს, მომავალში მჭიდრო საერთაშორისო თანამშრომლობისა და ურთიერთდახმარებისთვის. ეს, რა თქმა უნდა, არ ნიშნავს, რომ კანონმდებლობა უნაკლოა და დახვეწას არ საჭიროებს. ამ ფაქტს ადასტურებს 2013 წლის 17 მაისს საქართველოს პრეზიდენტის №321 ბრძანებულებით დამტკიცებული „საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013-2015წ. სამოქმედო გეგმა“, რომლის ერთ-ერთ პრიორიტეტულ მიმართულებად განსაზღვრულია საკანონმდებლო ბაზაში ხარვეზების აღმოფხვრა და მისი სრულყოფა.

34 იხ. http://www.justice.gov.ge/index.php?lang_id=GEO&sec_id=23&info_id=2309

თავდაპირველად, საქართველოს სისხლის სამართლის კოდექსში 2000 წლის 5 მაისის და 2000 წლის 30 ივნისის კანონების საფუძველზე შევიდა ცვლილება, რომლის თანახმადაც კოდექსმა განსაზღვრა სისხლისსამართლებრივი პასუხისმგებლობა კომპიუტერული დანაშაულისთვის. კერძოდ, XXXV თავი „კომპიუტერული დანაშაული“ შედგებოდა 284-ე, 285-ე, 286-ე მუხლებისგან. ხოლო 2002 წლის 28 დეკემბრის ცვლილებით კოდექსის XXXVIII თავს (ტერორიზმი) დაემატა 324¹ მუხლი, რომელიც ითვალისწინებდა პასუხისმგებლობას კიბერტერორიზმისთვის.

დღეს ჩამოთვლილი მუხლების პირველადი რედაქციები აღარ არსებობს.

აღსანიშნავია, რომ სისხლის სამართლის კოდექსის ძველ რედაქციაში კომპიუტერული დანაშაულის განსაზღვრისას კანონმდებელი იყენებდა ისეთ ტერმინებს, როგორიცაა მანქანა-მატარებელი, ელექტროგამომთვლელი მანქანა (ეგმ), ელექტროგამომთვლელი მანქანის სისტემა და მისი ქსელი, მაშინ როცა, მსოფლიოს უმრავლეს ქვეყანაში, საკანონმდებლო დონეზე გამოიყენებოდა ტერმინი „კომპიუტერი“. კომპიუტერი ინგლისური სიტყვაა და გამომთვლელს ნიშნავს. შინაარსობრივი განსხვავება კომპიუტერსა და ელექტრონულ გამომთვლელ მანქანას შორის არაა. დღეს მსოფლიოში დამკვიდრებულია ტერმინი კომპიუტერი და არა ეგმ. მარტივად რომ ვთქვათ, 80-იან წლებში გამოსული „უიგულიც“ მანქანაა და 2009 წელს გამოსული „მერსედესიც“, მაგრამ პირველზე არავინ იტყვის, რომ „მერსედესია“ და პირიქით. ეს ქართველმა კანონმდებელმაც გაითვალისწინა და დღეს მოქმედ სისხლის სამართლის კოდექსში მსგავსი მოძველებული ტერმინები აღარ გვხვდება.

საინტერესოა, რომ ქართველმა კანონმდებელმა ტერმინებთან დაკავშირებული სხვა მიდგომაც გაიზიარა: კერძოდ, სისხლის სამართლის კოდექსის XXXV თავს შეეცვალა სათაური და ნაცვლად „კომპიუტერული დანაშაულისა“ ეწოდა „კიბერდანაშაული“.

უნდა აღინიშნოს, რომ გარდა კიბერდანაშაულის თავში შესული მუხლებისა, კომპიუტერის გამოყენებასთანაა დაკავშირებული 324¹-ე მუხლი (კიბერტერორიზმი), 158-ე მუხლი (კერძო კომუნიკაციის საიდუმლოების დარღვევა), 189-ე მუხლი (საავტორო და მომიჯნავე უფლებების დარღვევა), 255-ე მუხლი (ბავშვთა პორნოგრაფია). მათ შესახებ დეტალურად შესაბამის პარაგრაფში ვისაუბრებ.

ახალი რედაქციით სისხლის სამართლის კოდექსის XXXV თავი შეიცავს 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევას), 285-ე (კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება) და 286-ე (კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა) მუხლებს.

2. 284-ე მუხლით გათვალისწინებული დანაშაულის ობიექტური შემადგენლობა

სისხლის სამართლის კოდექსის 284-ე მუხლის დისპოზიცია შემდეგნაირადაა ჩამოყალიბებული:

„კომპიუტერულ სისტემაში უნებართვო შეღწევა“

სანამ 284-ე მუხლის უშუალო ობიექტზე ვისაუბრებ, უნდა აღინიშნოს, რომ კიბერდანაშაულის ზოგადი ობიექტი ყველა იმ საზოგადოებრივ ურთიერთობათა ერთობლიობაა, რომლიც დაცულია სისხლის სამართლის კანონით. ალ. კაცმანი მიუთითებს, 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 სხვ. მართალია, აღნიშნული მოსაზრება გამოითქვა მაშინ, როცა ძველი რედაქცია მოქმედებდა, მაგრამ იგი მისაღებია ახალ რედაქციასთან მიმართებაში, რადგან იგი საერთოა სისხლის სამართლის კოდექსით გათვალისწინებული ყველა დანაშაულის შემადგენლობისთვის.

დანაშაულის გვარეობითი ობიექტია სისხლის სამართლის კანონით დაცული ის ერთგვაროვანი ან იგივეობითი საზოგადოებრივი ურთიერთობები, რომელთა წინააღმდეგაც მიმართულია დანაშაულებრივი ხელყოფა³⁵. დანაშაულის გვარეობითი ობიექტი, ასევე არის სისხლის სამართლის კერძო ნაწილის სისტემის აგების ძირითადი

35 იხ. თ.წერეთელი, გ. ტყეშელიაძე, „მოდერნა და დანაშაულზე“, გამომც. „მეცნიერება“, თბ. 1969წ. გვ. 150

საფუძველი.³⁶ ვინაიდან, კომპიუტერული დანაშაულის შესახებ თავი მოქცეულია საქართველოს სისხლის სამართლის კოდექსის მეცხრე კარში – „დანაშაული საზოგადოებრივი უშიშროებისა და წესრიგის წინააღმდეგ“, იგულისხმება, რომ კანონმდებელმა ამ დანაშაულთა გვარეობით ობიექტად განსაზღვრა საზოგადოებრივი უშიშროება და წესრიგი.

სახეობითი ობიექტია საზოგადოებრივი ურთიერთობების ერთობლიობა, კომპიუტერული სისტემის და კომპიუტერული მონაცემების მართლზომიერი და უსაფრთხო მოხმარებისათვის.

დანაშაულის უშუალო ობიექტს წარმოადგენს სისხლის სამართლის კანონით დაცული კონკრეტული საზოგადოებრივი ურთიერთობა, რომლის წინააღმდეგაც მიმართულია დანაშაულებრივი ხელყოფა³⁷.

კომპიუტერული დანაშაულის უშუალო ობიექტის განსაზღვრას ალ. კაცმანი უკავშირებს კომპიუტერული დანაშაულის შემადგენლობის შემცველ კონკრეტული მუხლების სახელწოდებას³⁸. გ. მამულაშვილი კი 284-ე მუხლის ძველი რედაქციით გათვალისწინებული დანაშაულის უშუალო ობიექტად გამოყოფს კომპიუტერული ინფორმაციის ხელშეუხებლობას ანუ საკუთრების უფლებას კომპიუტერულ ინფორმაციაზე³⁹. 284-ე მუხლის ახალი რედაქციით დაცვის უშუალო ობიექტად გ. მამულაშვილი მიუთითებს: მონაცემის/ინფორმაციის მთლიანობას, ხელმისაწვდომობას და კონფიდენციალურობას, ასევე, კომპიუტერული სისტემის ინტეგრირებულობას.⁴⁰ აღნიშნულ მოსაზრებას სრულად ვიზიარებ და მიმაჩნია, რომ 284-ე მუხლით გათვალისწინებული დანაშაულის ობიექტია იმ კომპიუტერული სის-

36 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის ზოგადი ნაწილი“, გამომც. „მერიდიანი“ თბ. 2007წ. გვ. 111

37 იხ. თ.წერეთელი, გ. ტყეშელიაძე, „მოდერნა და დანაშაულზე“, გამომც. „მეცნიერება“, თბ. 1969წ. გვ. 153

38 იხ. ა. კაცმანი, დისერტაცია თემაზე „კომპიუტერული დანაშაული“, თბილისი 2004წ. გვ. 35

39 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი II, გამომც. „მერიდიანი“, თბ. 2012წ. გვ. 46

40 იხ. იქვე. გვ. 36

ტემის მთლიანობა და უსაფრთხოება, რომელშიც განხორციელდა უნებართვო შეღწევა.

საინტერესოა, პასუხი გაცეთ შეკითხვას: კომპიუტერული ტექნიკა მივაკუთნოთ თუ არა დანაშაულის ობიექტს და საგანს?

ვ.ნ. ჩერკასოვი არ ეთანხმება დანაშაულებრივი ხელყოფის ობიექტად კომპიუტერული ტექნიკის გამოყოფას. მისი აზრით, კომპიუტერული თაღლითობა, საბოტაჟი, ჯაშუშობა და სხვა რჩება ისევ თაღლითობად, საბოტაჟად და ჯაშუშობად, რაც ჩადენილია კომპიუტერის, როგორც ტექნიკური საშუალების დახმარებით.⁴¹ მოცემულ მსჯელობას სრულად ვიზიარებ და მიმაჩნია, რომ აქ, რა თქმა უნდა, იგულისხმება ისეთი დანაშაული, რომლის ჩადენაც ხორციელდება კომპიუტერული ტექნიკის გამოყენებით. მაგალითად, ყალბი საკრედიტო ბარათის დამზადება, ყალბი პირადობის მონმობის დამზადება და სხვ.

იგივე მოსაზრებას ამყარებს ნ.ვ. კარჩევსკი ნაშრომში „კომპიუტერული დანაშაული: განსაზღვრება, ობიექტი და საგანი“. ნ. კარჩევსკი წერს: „როგორც ჩანს, აუცილებელია ისეთი ტერმინების გამიჯვნა, როგორიცაა „კომპიუტერული დანაშაული“ და „კომპიუტერულ ტექნიკასთან დაკავშირებული დანაშაულები“⁴².

ვეთანხმები მოყვანილ მსჯელობას და მიმაჩნია, რომ კომპიუტერული ტექნიკა არ უნდა იქნეს განხილული, როგორც კიბერ-დანაშაულის ობიექტი, რადგან დანაშაულებრივი ხელყოფისას ზემოქმედებას განიცდის არა უშუალოდ კომპიუტერული ტექნიკის რომელიმე დეტალი, არამედ, კომპიუტერული სისტემა, მასში ჩანერგილი მონაცემი, პროგრამა და ა.შ. მაგალითად, განვიხილოთ კაზუსი. ა. ალფაიძემ საკუთარი ლეპტოპის გამოყენებით უნებართვოდ შეაღწია ბ. დუნდუას პერსონალური კომპიუტერის კომპიუტერულ სისტემაში. ასეთ შემთხვევაში რა განიცდის დანაშაულებრივ ხელყოფას? ბ. დუნდუას პერსონალური კომპიუტერი თუ მისი კომპიუტერული სისტემა? რა თქმა უნდა, მეორე! მაშ, რას წარმოადგენს

41 იხ. В.Н. Черкасов О понятии «Компьютерная преступность». // Проблемы компьютерной преступности: Выпуск 2. - Мн.: НИИ ПККСЭ МЮ РБ, 1992. გვ.5.

42 იხ. Н.В.Карчевский, Компьютерные преступления: определение, объект и предмет, Доклад V Международной конференции «Право и Интернет: теория и практика» 2003г. www.ifap.ru/pi/05/karchev.htm

კომპიუტერული ტექნიკა? ის უნდა მივიჩნიოთ დანაშაულის ჩადენის საგნად თუ საშუალებად? ჩემი აზრით, თუ საკითხს ზედპირულად მივუდგებით, კომპიუტერი არის როგორც კიბერდანაშაულის ხელყოფის საგანი, ასევე, შესაძლებელია იყოს ამ ტიპის დანაშაულის ჩადენის საშუალებაც, მაგრამ ეს მიდგომა მცდარია. თუ საკითხს ჩავუღრმავდებით, აღმოვაჩენთ, რომ უშუალო დანაშაულის ფაქტის განხორციელება ხდება კომპიუტერული ტექნიკის კომპიუტერული სისტემის გამოყენებით. დანაშაულის კვალი, ჩადენის დრო, შინაარსი, აისახება სწორედ კომპიუტერულ სისტემაში. კომპიუტერული ტექნიკა კი წარმოადგენს ერთგვარ გამტარს, მონყობილობას, რომლის საშუალებითაც აღქმადი და ხილული ხდება კომპიუტერული სისტემა. კომპიუტერული ტექნიკა მხოლოდ იმ შემთხვევაში უნდა ჩაითვალოს დანაშაულის ჩადენის საშუალებად, როცა მისი გამოყენებით უშუალოდ ხდება დანაშაულის ჩადენა. მაგალითად, ყალბი დოკუმენტის დამზადება, ფულის გაყალბება და ა.შ. ეს დანაშაული კი კიბერდანაშაულს არ განეკუთვნება. ვინაიდან, კიბერდანაშაულის ჩადენა ხორციელდება კომპიუტერული სისტემის და კომპიუტერული მონაცემის გამოყენებით ან/და მათზე ზემოქმედების მოხდენის მიზნით, კომპიუტერული ტექნიკა ვერ განიხილება ვერც დანაშაულის საგნად და ვერც მისი ჩადენის საშუალებად. ჩემი პოზიციის დასაბუთებისთვის მოვიშველიებ, თ. წერეთლის და გ. ტყეშელიაძის განმარტებას, რომლის მიხედვითაც, „დანაშაულის საგნისგან უნდა განვასხვავოთ დანაშაულის ჩადენის საშუალება. დამნაშავემ ნივთი შეიძლება გამოიყენოს დანაშაულის ჩადენის იარაღად. ნივთი დანაშაულის ჩადენის იარაღად მაშინ ჩაითვლება, როდესაც მისი საშუალებით დამნაშავე ცდილობს ხელყოს ობიექტი. დანაშაულის საგანი კი თვითონ განიცდის დანაშაულებრივ ხელყოფას“.⁴³

ზემოაღნიშნულის გათვალისწინებით ცხადი ხდება, რომ ცალკე აღებული კომპიუტერული ტექნიკით, ტექნიკურად კომპიუტერულ სისტემაში შეღწევას ვერ განვახორციელებთ. თვალსაჩინოებისთვის წარმოვიდგინოთ პეროსნალური კომპიუტერის დეტალები: მეხსიერების ბარათი, მონიტორი, პროცესორი, ოპერატიული მეხსიერება და

43 იხ. თ. წერეთლი, გ. ტყეშელიაძე, „მოდერება დანაშაულზე“, გამომც. „მეცნიერება“, თბ. 1969წ. გვ. 160

ა.შ. ანუ კომპიუტერი წარმოადგენს ფიზიკური ელემენტებისგან აგებულ მანქანას უშუალოდ ცალკე აღებული დეტალები ან მთლიანად კომპიუტერი კიბერდანაშაულის ჩადენისას შეუძლებელია გამოვიყენოთ იარაღად, ან პირიქით ზემოქმედება მოვახდინოთ მასზე, რადგან კიბერსივრცეში მოქმედება ხორციელდება მხოლოდ იმ კომპიუტერული სისტემით, რომელიც ადაპტირებულია კომპიუტერულ ტექნიკაში, ინტერნეტში მინიჭებული აქვს საიდენტიფიკაციო მონაცემი, აქვს სახელწოდება და ა.შ. ხაზგასასმელია, რომ როდესაც დამნაშავე უნებართვოდ აღწევს კომპიუტერულ სისტემაში, აღნიშნული ქმედება არანაირ ზემოქმედებას არ ახდენს კომპიუტერულ ტექნიკაზე, ტექნიკა არ განიცდის მისი გამოყენების ჩვეული რეჟიმისგან განსხვავებულ ცვეთას, არ გამოდის მწყობრიდან. ეს შედეგი შესაძლოა გამოიწვიოს მხოლოდ მასზე უშუალო ძალადობის ფაქტმა, რაც კიბერდანაშაული თავისთავად არ იქნება და ჩაითვლება სისხლის სამართლის კოდექსის 187-ე მუხლით გათვალისწინებულ ნივთის დაზიანებად ან განადგურებად.

აღ. კაცმანი მიიჩნევს, რომ კომპიუტერული დანაშაულის ხელყოფის საგანს წარმოადგენს ინფორმაცია, რომლის დამუშავებაც ხდება კომპიუტერულ სისტემაში, ხოლო კომპიუტერი ითვლება ხელყოფის იარაღად.⁴⁴ რთული გასარკვევია, როდესაც დანაშაულის იარაღად კომპიუტერს მიუთითებს, აღ. კაცმანი მასში გულისხმობს კომპიუტერს, როგორც ტექნიკას, თუ კომპიუტერს როგორც სისტემას. როგორც აღვნიშნე მხოლოდ კომპიუტერული ტექნიკით უშუალოდ კიბერდანაშაულის საგანზე ზემოქმედების მოხდენა შეუძლებელია და თუ აღ. კაცმანს იმის თქმა სურდა, რომ კომპიუტერული ტექნიკა კიბერდანაშაულის იარაღი, მაშინ ვერ დავეთანხმებო.

ნ.ვ. კარჩევსკი საკუთარ ნაშრომში სამართლიანად იზიარებს ვ. ვეხოვის მოსაზრებას, რომელიც გვთავაზობს კომპიუტერული დანაშაულის განმარტებას ორგვარი მიდგომით, კერძოდ, სისხლისსამართლებრივი და კრიმინალისტიკური. ეს უკანასკნელი ბევრად ფართოა და მასში შეიძლება განვიხილოთ ქმედება, რომელშიც კომპიუტერი წარმოადგენს დანაშაულის ჩადენის საგანს ან

44 იხ. ა. კაცმანი, დისერტაცია თემაზე „კომპიუტერული დანაშაული“, ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2004 წ. გვ. 30

საშუალებას.“⁴⁵ ეს უკანასკნელი კი, როგორც უკვე აღვნიშნე არ უკავშირდება კიბერდანაშაულს.

თ. წერეთლის და გ. ტყეშელიაძის აზრით, დანაშაულის საგანი არის შესაბამისი დანაშაულის შემადგენლობით გათვალისწინებული მატერიალური ნივთი, რომელზეც მიმართულია დამნაშავეს მოქმედება⁴⁶. აქედან გამომდინარე, ვინაიდან კომპიუტერულ სისტემაში უნებართვო შეღწევა არ გულისხმობს მხოლოდ კომპიუტერულ მონაცემში ან ინფორმაციაში შეღწევას, უნდა ვიგულისხმოთ, რომ ამ დანაშაულის საგანია, როგორც კომპიუტერული სისტემა, ასევე კომპიუტერული მონაცემი. ბუნებრივია, კომპიუტერული სისტემა და მონაცემი ვერ იქნება მატერიალური ნივთი, მაგრამ მაშინ, როდესაც თ. წერეთლის და გ. ტყეშელიაძის მიერ ეს განმარტება გაკეთდა, კომპიუტერული დანაშაული ჩანასახშიც არ იყო. ამდენად, როდესაც ვსაუბრობთ კიბერდანაშაულის საგნის განმარტებაზე, მასში უნდა ვიგულისხმოთ კომპიუტერული სისტემა და კომპიუტერული მონაცემი.

ამერიკელი ექსპერტები, კენტ ალექსანდერი და სკოტ ჩარნი მიიჩნევენ, რომ კომპიუტერი ან მასში შენახული ინფორმაცია შეიძლება იყოს დანაშაულის საგანი. ასეთ შემთხვევაში დამნაშავეს მიზანია კომპიუტერიდან ინფორმაციის მოპარვა ან მისთვის ზიანის მიყენება. მეორე – კომპიუტერი შეიძლება იყოს დანაშაულის იარაღი. ასეთ შემთხვევას ადგილი აქვს მაშინ, როდესაც ადამიანი იყენებს კომპიუტერს რომელიმე ისეთი ტრადიციული დანაშაულის ჩადენის ხელშეწყობისთვის, როგორიცაა თაღლითობა ან ქურდობა (მაგალითად, ბანკის თანამშრომელმა შეიძლება გამოიყენოს კომპიუტერული პროგრამა თანხის მოსახსნელად ამავე ბანკში გახსნილი სხვა მოქალაქეების ანგარიშიდან). მესამე – ზოგჯერ კომპიუტერი მეორეხარისხოვანია დანაშაულის ჩასადენად, მაგრამ მნიშვნელოვანია სამართალდამცავთათვის, რადგან იგი შეიცავს დანაშაულთან დაკავშირებულ მტკიცებულებას. მაგალითად, ნარკოტიკებით მოვაჭ-

45 იხ. ა. კაცმანი, დისერტაცია თემაზე „კომპიუტერული დანაშაული“, ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2004 წ. გვ. 30

46 იხ. თ. წერეთელი, გ. ტყეშელიაძე, „მოდერნული დანაშაულები“, გამომც. „მეცნიერება“, თბ. 1969წ. გვ. 157

რეებმა, ფურცლების და ჟურნალის ნაცვლად შეიძლება გამოიყენონ პერსონალური კომპიუტერი ნარკოტიკებით ვაჭრობასთან დაკავშირებული ჩანაწერის შესანახად⁴⁷. მოცემული მოსაზრება ყველაზე უფრო ახლოსაა ჩემს პოზიციასთან, გარდა იმ ნაწილისა, სადაც დანაშაულის საგნად კომპიუტერს მიუთითებენ. თუმცა, ავტორები არ აზუსტებენ კონკრეტულად კომპიუტერულ ტექნიკაზე აქვთ საუბარი თუ არა და შესაძლოა ისინი მასში გულისხმობენ კომპიუტერულ სისტემასაც.

კიბერდანაშაულის ძირითად მახასიათებლებად ალ. კაცმანი გამოყოფს:

- ა) დანაშაულებრივი ხელყოფის ობიექტის არაერთგვაროვნებას;
- ბ) ერთი და იგივე კომპიუტერული ინფორმაცია შეიძლება იყოს, ერთ შემთხვევაში ხელყოფის საგანი, ხოლო მეორე შემთხვევაში დანაშაულის ჩადენის იარაღი ან საშუალება.
- გ) დანაშაულებრივი ხელყოფის საგნისა და საშუალების მრავალფეროვნებას.⁴⁸

ამ კლასიფიკაციას სრულად ვიზიარებ, იმ განსხვავებით, რომ როგორც ზემოთაც აღვნიშნე, ხელყოფის საგანი, გარდა კომპიუტერული ინფორმაციისა, არის კომპიუტერული სისტემა და კომპიუტერული მონაცემიც.

284-ე მუხლით გათვალისწინებული დანაშაულის საგანი არის ის კომპიუტერული სისტემა და კომპიუტერული მონაცემი, რომელშიც ხორციელდება უნებართვო შეღწევა.

284-ე მუხლით გათვალისწინებული დანაშაულის საგნის უკეთ გაგებისთვის ამავე მუხლის პენიშნის 1-ლ და მე-2 ნაწილში განმარტებულია, როგორც კომპიუტერული სისტემის, ასევე, კომპიუტერული მონაცემის ცნება: კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის პერსონალური კომპიუტერი, ნებისმიერი

47 იხ. SCOTT CHARNEY, KENT ALEXANDER, Types of computer crime, 25.11.2005 <http://www.crime-research.org/articles/types-of-computer-crime/2>

48 იხ. ა. კაცმანი, „კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება“, ჟურნ. „სამართალი“ 2000წ. №2, გვ. 58.

მონყობილობა მიკროპროცესორით, აგრეთვე, მობილური ტელეფონი), ხოლო კომპიუტერული მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით ინფორმაციის გამოსახვა, მათ შორის პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას.

საინტერესოა, რომ ქართული კანონმდებლობისგან მცირე განსხვავებით განმარტავენ კომპიუტერულ სისტემას და კომპიუტერულ მონაცემს ლ. ბოძაშვილი და ნ. კობხრიძე სახელმძღვანელოში „კიბერსივრცის სამართალი“. მათი აზრით, კომპიუტერული სისტემაა „ნებისმიერი მონყობილობა ან ურთიერთდაკავშირებულ ხელსაწყოთა ჯგუფი, რომელთაგან ერთ-ერთი მაინც ასრულებს მონაცემების ავტომატურ გადაცემას პროგრამის საშუალებით“, ხოლო კომპიუტერული მონაცემია „ინფორმაციის, ფაქტების ან საერთო წარმოდგენის გადმოცემა კომპიუტერული სისტემის თუ პროგრამისთვის გასაგებ ფორმაში, რომელმაც შეიძლება შეასრულებინოს კომპიუტერულ სისტემას გარკვეული ქმედება“⁴⁹.

მოცემულ განმარტებაში კომპიუტერულ სისტემასთან დაკავშირებით დაკონკრეტებულია, რომ ურთიერთდაკავშირებულ ხელსაწყოთა შორის საკმარისია, თუნდაც ერთ-ერთი ასრულებდეს მონაცემთა ავტომატურ დამუშავებას. აღნიშნული პოზიცია სავსებით მისაღებია და შეიძლება ითქვას, რომ ეს იმაზე ზუსტია ვიდრე ქართულ კანონმდებლობაში მოცემული განმარტება, რომელიც, თავის მხრივ, ევროპის საბჭოს კონვენციიდანაა გადმოღებული. ეჭვს იწვევს მხოლოდ ტერმინი „ხელსაწყო“. ჩემი აზრით, „მექანიზმი“ ბევრად უკეთ გამოხატავს კომპიუტერული სისტემის შემადგენელ ნაწილს, ვიდრე ხელსაწყო, რადგან ქართულ ენაში ხელსაწყო ძირითადად გამოიყენება სხვადასხვა საყოფაცხოვრებო ან სახელოსნო საქმიანობაში საჭირო ინვენტარის გამოსახატავად. „მექანიზმი“ კი ზოგადი შინაარსისაა და მისი გამოყენება უამრავ კონტექსტში შეგვიძლია. ამდენად, ჩემი აზრით, უმჯობესი იქნებოდა კომპიუტერული სისტემა განგვემარტა, როგორც „ნებისმიერი მონყობილობა ან ურთი-

49 იხ. ლ. ბოძაშვილი, ნ. კობხრიძე, „კიბერსივრცის სამართალი“, 2012წ. (ნაშრომში გამოყენებულია ნიგნის ოფიციალური ელექტრონული ვერსია გამოქვეყნებული საიტზე www.iit.ge, რომელშიც გვერდები მითითებული არაა)

ერთდაკავშირებულ მექანიზმთა ჯგუფი, რომელთაგან ერთ-ერთი მაინც ასრულებს მონაცემების ავტომატურ გადაცემას პროგრამის სამუშაოებით".

როცა ვსაუბრობთ კომპიუტერულ სისტემაზე დამატებით უნდა აღინიშნოს, რომ კომპიუტერულ სისტემაში გარდა ჩვეულებრივი კომპიუტერისა, ლეპტოპისა და ა.შ. უნდა ვიგულისხმოთ ნებისმიერი ნივთი, რომელსაც კავშირი გააჩნია ინფორმაციის ავტომატურ დამუშავებასთან. ესეთია: მიკროპროცესორიანი და მაგნიტურლენტიანი ბარათი (ელექტრონული პირადობის მოწმობა, საშვი, საკრედიტო, ელექტრონული ხელმოწერის და ტელეფონზე სასაუბრო ბარათი).

რაც შეეხება კომპიუტერული მონაცემის ლ. ბოძაშვილის და ნ. კოხრიეიძისეულ განმარტებას, უნდა აღინიშნოს, რომ მასში მითითებული ტერმინები „ფაქტები და საერთო წარმოდგენა“ სრულიად ზედმეტია. ჩემი აზრით, ორივე ამ სიტყვის მნიშვნელობას შეიცავს „ინფორმაცია“. უფრო მეტიც, რა მიზანი აქვს ტერმინს „საერთო წარმოდგენა“ გაუგებარია. ქართული ენაში იგი უნდა გავიგოთ, როგორც საზოგადოდ აღიარებული წარმოდგენა ანუ შეხედულება, ამათუიმ საკითხზე, რაც რბილად რომ ვთქვათ, უადგილოა „კომპიუტერული მონაცემის“ განმარტებისას. ამდენად, ჩემი აზრით, უპირატესობა უნდა მიეანიჭოთ სისხლის სამართლის კოდექსში მოცემულ განმარტებას.

იმ მნიერი გამოცდილებიდან, რაც საქართველომ შეიძინა კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლაში, შესაძლებელია ერთი კაზუსის მოყვანა. მართალია, ეს დანაშაული სისხლის სამართლის კოდექსის ძველი რედაქციის მოქმედების პერიოდში განხორციელდა და შესაბამისად, მისი კვალიფიკაციაც ძველი კანონმდებლობით მოხდა, მაგრამ, როცა ვსაუბრობთ კომპიუტერულ სისტემაში უნებართვო შეღწევის ობიექტზე, შესაძლებელია, განვიხილოთ კანონით დაცულ კომპიუტერულ ინფორმაციაში არამართლზომიერი შეღწევის მაგალითი, რადგან ეს ორი დანაშაული არსებითად მსგავსი შინაარსის მატარებელია.

თბილისის საოლქო სასამართლომ საქმე №1/ა-74-ზე 2004 წლის 19 მაისის გამამტყუნებელი განაჩენით დამნაშავედ ცნო ბ. სალაძე, შ. სიგუა და ზ. მანასიანი სისხლის სამართლის კოდექსის 180-ე, 202-ე, 210-ე, 362-ე და 284-ე მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით და მე-3 ნაწილით გათვალისწინებული დანაშაულის ჩადენაში. განაჩენში ვკითხულობთ:

სააქციო საზოგადოებებს „ინტელექტბანკს“ და „საქართველოს ბანკს“ საქართველოში რეგისტრირებულ და მოქმედ კაზინოებთან „აჭარა“, „ფლამინგო“, „არაგვი“, „ვიქტორია“, „ევროპა,“ ასევე სამეურნეო და სავაჭრო სუბიექტებთან გაფორმებული პქონდათ ხელშეკრულება „მასტერქარდის“ საკრედიტო ბარათებით მომსახურების შესახებ, რომლის თანახმად, საბარათო გარიგებები (ტრანზაქციები) ხორციელდებოდა აღნიშნულ ობიექტებში დამონტაჟებული „პოსტტერმინალების“ მეშვეობით, ხოლო იურიდიულ პირებს თანხებს თავის მხრივ „მასტერქარდისგან“ გადმორიცხული სახსრების მეშვეობით უნაზღაურებდა „ინტელექტბანკი“ და „საქართველოს ბანკი“.

2002 წლის შემოდგომაზე, დაახლოებით სექტემბერ-ოქტომბერში საქართველოს მოქალაქეებმა ბ. სალაძემ და ზ. მანასიანმა, ისრაელის მოქალაქე ლ. ინაევმა და ასევე სხვა დაუდგენელმა პირმა, რომელიც სარგებლობდა ლ. მოსაშვილის ყალბი პირადობის მონაბოთით, წინასწარი შეთანხმებით, სხვისი ქონების მართლსაწინააღმდეგო მისაკუთრების მიზნით, განიზრახეს საქართველოში მოქმედ საბანკო დანესებულებებში გაეხსნათ საბარათე ანგარიშები, მიეღოთ მასტერქარდის სისტემის საკრედიტო ბარათები, არამართლზომიერად შეელწიათ კანონით დაცულ კომპიუტერულ ინფორმაციაში, უკანონოდ მოეპოვებინათ და გამოეყენებინათ საბანკო საიდუმლოების შემცველი ცნობები და კომპიუტერული მანიპულირების – ე.წ. „ჰაკერული ოპერაციების“ განხორციელების გზით მოეხდინათ საკრედიტო ბარათებზე უცხოეთის საბანკო ანგარიშებიდან თანხების მითვისება. ასევე, დაემზადებინათ ყალბი საკრედიტო ბარათები და მათი არასაბანკო ობიექტებში გამოყენებით მიეთვისებინათ მის კანონიერ მფლობელთა კუთვნილი თანხები.

დანაშაულებრივი განზრახვის აღსასრულებლად ბ. სალაძემ ჯგუფის სხვა წევრებთან წინასწარი შეთანხმებით 2002 წლის 7 ნოემბერს „ინტელექტბანკისგან“ ხელშეკრულების საფუძველზე მიიღო მასტერქარდის სისტემის საკრედიტო ბარათი. იმავე დღეს ბ. სალაძემ „საქართველოს ბანკში“ მიიღო მასტერქარდის სისტემის ორი საკრედიტო ბარათი.

პარალელურად, ბ. სალაძემ, ზ. მანასიანმა და ლ. ინაევმა გადანყიციეს შეეძინათ კომპიუტერული ტექნიკა, რომლის საშუა-

ლებითაც მოხდებოდა ინტერნეტში მუშაობა, კანონით დაცულ კომპიუტერულ ინფორმაციასთან არამართლზომიერი შელწევა, საბანკო საიდუმლოების შემცველი ცნობების შეგროვება-გამოყენება და ე.წ. „ჰაკერული ოპერაციების“ განხორციელება. ამ მიზნით ბ. სალაძემ მეგობრის ო. დადიანის მეშვეობით გაიცნო გაზეთ „ახალ დღეში“ დამკაბადონებლად მომუშავე ა. სურმავა, რომელიც კარგად ერკვეოდა კომპიუტერულ ტექნიკაში და ხელენიფებოდა კომპიუტერული ქსელის მოწყობა, დამონტაჟება და ექსპლუატაცია.⁵⁰

ამის შემდეგ ა. სურმავამ შეიძინა ორი ერთეული კომპიუტერული ტექნიკა და იგი განათავსა ჭავჭავაძის ქუჩაზე დაქირავებულ სახლში.

შედეგად, ბ. სალაძემ, ზ. მანასიანმა და ლ. ინაევმა სხვა დაუდგენელი პირების ხელშეწყობით მოახერხეს კანონით დაცულ კომპიუტერულ ინფორმაციაში შელწევა და უცხოეთის რიგი დანესებულებების საბანკო საიდუმლოების შემცველი მონაცემების მოპოვება.

ამის შემდეგ მოპოვებული ინფორმაციის გამოყენებით მათ არაერთგზის 2002 წლის 25 ნოემბრიდან 11 დეკემბრამდე პერიოდში სს „ინტელექტბანკში“ ბ. სალაძის კუთვნილ მასტერქარდის სისტემის საკრედიტო ბარათზე ამერიკის შეერთებული შტატების სხვადასხვა ობიექტიდან ინტერნეტის მეშვეობით გაანაღდეს (არასაბანკო გადარიცხვებით) 98.728.40 აშშ დოლარი...“ ამ თანხიდან 2000 აშშ დოლარი ბ. სალაძემ სს „საქართველოს ბანკის“ ორი ბანკომატიდან მეორე დღესვე (2002 წლის 26 ნოემბერს) გაანაღდა. დარჩენილი თანხის განაღდება ბ. სალაძემ და მისმა თანამოაზრეებმა ველარ შეძლეს, რადგან „ინტელექტბანკმა“ მათ უარი განუცხადა თანხის გაცემაზე და ბ. სალაძის საკრედიტო ბარათი დაიბლოკა იმ მოტივით, რომ თანხის ჩარიცხვის ოპერაციები ნაწარმოები იყო ყალბი ტრანზაქციების შედეგად.⁵¹

ვინაიდან, საბანკო დანესებულებებიდან ვერ ხერხდებოდა ყალბი ტრანზაქციის შედეგად საკრედიტო ბარათებზე დარიცხული თანხის განაღდება, დამნაშავეებმა შეცვალეს დანაშაულებრივი მოქმედების ფორმა და გადანყვიტეს დაემზადებინათ მასტერქარდის სისტემის

50 იხ. თბილისის საოლქო სასამართლოს სისხლის სამართლის საქმეთა სასამართლო კოლეგიის განაჩენი საქმეზე №1/ა-74, 19.05.2004წ. გვ. 4-5

51 იხ. იქვე გვ. 6

ყალბი საკრედიტო ბარათები, რომელთა გამოყენებასაც შეძლებდნენ ისეთ არასაბანკო დაწესებულებებში, როგორიცაა სამორინე, სუპერმარკეტი და სხვა სავაჭრო ობიექტები⁵².

ამის შემდეგ ლ. ინაევმა არალეგალურად შეიძინა და საქართველოში შემოიტანა სპეციალური მონეობილობა, რომლის მეშვეობით შესაძლებელი იყო მასტერქარდის სისტემის საკრედიტო ბარათებისთვის მაგნიტური ველის შეცვლა-გაყალბება. ამავე პერიოდში ბ. სალაძემ განზრახვა გააძლიერა და დანაშაულებრივ საქმიანობაში ჩააბამოქ. შ. სიგუა. დამნაშავეები საკრედიტო ბარათების დამამზადებელი მონეობილობის მეშვეობით, სისტემატურად ამზადებდნენ ყალბ საკრედიტო ბარათებს, მათ შორის კომპიუტერულ ქსელში უკანონოდ შეღწევის გზით აგროვებდნენ საბანკო საიდუმლოების შემცველ ინფორმაციას და მათი გამოყენებით მაგნიტური ველს ჩანანერს უცვლიდნენ. მათ ბ. სალაძის და ლ. მოსაშვილის სახელზე „საქართველოს ბანკიდან“ და „ინტელექტბანკიდან“ გაცემულ საკრედიტო ბარათების მაგნიტურ ველზე შეჰყავდათ უცხოეთის იმ მოქალაქეთა საკრედიტო ბარათების ნომრები, რომლებზეც შესაბამის საბანკო დაწესებულებებში ირიცხებოდა გარკვეული ოდენობის თანხები. დამნაშავეები გაყალბებულ საკრედიტო ბარათებს თაღლითურად იყენებდნენ სხვადასხვა ობიექტებში, რის შედეგადაც ეუფლებოდნენ ამ ბარათების კანონიერ მფლობელთა კუთვნილ დიდი ოდენობის სახსრებს.“

კაზუსიდან ნათლად ჩანს თუ რა სიკეთის ხელყოფა განხორციელდა და რა იყო დანაშაულის საგანი. კერძოდ, დანაშაულის საგანს წარმოადგენდა უცხოეთის რიგი დაწესებულების საბანკო საიდუმლოების შემცველი მონაცემები, ხოლო დანაშაულის უშუალო ობიექტი იყო იმ მოქალაქეთა საკუთრების უფლება კონკრეტულ საბარათე ანგარიშებზე, რომლებიდანაც თვითნებურად განხორციელდა თანხების ჩამოჭრა. ასევე, იმ ქართული ბანკების ფინანსური ინტერესი, რომლებიც ახორციელებდნენ შუამავლის როლს დამნაშავეების მიერ განხორციელებულ ტრანზაქციებში. დამატებითი ობიექტი იყო შუამავალი ბანკების რეპუტაცია.

52 იხ. თბილისის საოლქო სასამართლოს სისხლის სამართლის საკმეთა სასამართლო კოლეგიის განაჩენი საქმეზე №1/ა-74, 19.05.2004წ. გვ.4-5

განხილული კაზუსიდან რთულია დავადგინოთ რა წარმოადგენდა დანაშაულის ჩადენის საშუალებას. თუმცა ლოგიკურად, მასში უნდა ვიგულისხმოთ ის კომპიუტერული სისტემა, რომლის საშუალებითაც განხორციელდა უნებართვო შეღწევა.

რაც შეეხება ქმედების ობიექტურ მხარეს, საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლის 1-ლი ნაწილი გულისხმობს კომპიუტერულ სისტემაში უნებართვო შეღწევას.

ტერმინი „უნებართვო“ კი 284-ე მუხლის შენიშვნის მე-3 ნაწილის მიხედვით გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისთვის.

ტერმინ „შელწევის“ განმარტებას კანონმდებლობა არ იძლევა, თუმცა, ჩემი აზრით, ის უნდა განიმარტოს, როგორც პირის ძალისხმევა გარკვეული მოქმედების განხორციელებით მართლსაწინააღმდეგოდ ჩაერიოს ინფორმაციის დამუშავების პროცესში ან ზემოქმედება მოახდინოს მათზე. სამართლიანად აღნიშნავს გ. მამულაშვილი, რომ „შელწევა“ გულისხმობს კონკრეტულ მოქმედებას, რომლის შედეგიც არის კომპიუტერული სისტემის მთლიანობის დარღვევა. ეს მოქმედება შეიძლება განხორციელდეს როგორც კომპიუტერში უშუალო ფიზიკური შეღწევით, ისე სხვადასხვა პროგრამული საშუალების გამოყენებით.⁵³

აღსანიშნავია, რომ 284-ე მუხლში გათვალისწინებული ქმედება შეესაბამება „კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციის მე-2 მუხლს, სადაც მითითებულია კომპიუტერულ სისტემაში ან მის ნაწილში უნებართვო შეღწევის შესახებ. საინტერესოა, რომ ქართველი კანონმდებელი სისხლის სამართლის კოდექსში შესატანი ცვლილების პირველ ვერსიაში, რომელიც 2010 წლის 13-14 მაისს თბილისის რეგიონულ კონფერენციაზე იქნა წარმოდგენილი, სისხლისსამართლებრივ პასუხსიმგებლობას უკავშირებდა კომპიუტერულ სისტემაში უნებართვო შეღწევას, თუ ამ ქმედებას ჰქონდა კომპიუტერული მონაცემის უკანონო მოპოვების მიზანი, ანუ პასუხსიმგებლობა უკავშირდებოდა კონკრეტულ შედეგის დადგომის

53 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი II, გამომც. „მერიდიანი“, თბ. 2012წ. გვ. 37

მიზანს. მოგვიანებით კანონმდებელი მივიდა დასკვნამდე, რომ კომპიუტერულ სისტემაში უნებართვო შეღწევა არის კიბერდანაშაული და 284-ე მუხლი ჩამოყალიბდა არსებული სახით. ამ პოზიციას სრულად ვიზიარებ და მის დასაბუთებას ქვემოთ შევეცდები.

აღსანიშნავია, რომ „კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციის რატიფიცირებამდე მრავალი ქვეყანა დანაშაულებრივ ქმედებას მართლსაწინააღმდეგო შეღწევის შედეგს უკავშირებდა. ამ დამკვიდრებული საკანონმდებლო პრაქტიკიდან განსხვავებით, ევროპის საბჭოს კონვენციის, ასევე ევროკავშირის საბჭოს 2005 წლის 24 თებერვლის ჩარჩო გადანყეტილების მიხედვით დადგინდა, რომ ხელმომწერმა ქვეყნებმა და ევროკავშირის წევრმა სახელმწიფოებმა უნდა უზრუნველყონ ისეთი კანონმდებლობის მიღება, რომლის საფუძველზე დანაშაულად გამოცხადდება კომპიუტერულ სისტემაში ან მის ნაწილში უნებართვო შეღწევა. ამრიგად აღინიშნა, რომ ამ დანაშაულებრივი ქმედებისთვის სპეციალური მიზნის არსებობა საჭირო არ იყო. მიუხედავად ამისა, ჩეხეთმა საინფორმაციო სისტემაში უნებართვო შეღწევისთვის სისხლისსამართლებრივი პასუხისმგებლობა მხოლოდ ინფორმაციის დაზიანებისთვის განსაზღვრა. უნებართვო შეღწევის გამო დამდგარ მავნე შედეგთანაა დაკავშირებული ქმედების დანაშაულად კვალიფიცირება ლატვიასა და ფინეთშიც. ლატვიაში ქმედება დანაშაულად ითვლება, თუ მას მოჰყვა არსებითი ზიანი, ხოლო ფინეთში დასჯადია მონაცემებისათვის საფრთხის შექმნა⁵⁴. აღენიშნავ, რომ ამ ქვეყნების პოზიციას არ ვიზიარებ.

ამ საკითხზე საინტერესოა გერმანიის გამოცდილების ანალიზიც. ევროსაბჭოს ექსპერტი, დოქტორი მარკო გერკე მინვეული იყო გერმანიის საკანონმდებლო ორგანოში სისხლის სამართლის კოდექსში ცვლილებების პროექტის მომზადებისას. იგი ჯერ კიდევ 2007 წლის ივლისში აცხადებდა, რომ გერმანიის კანონმდებლობა განსხვავებით ბევრი სხვა ქვეყნისგან არ აწესებდა სისხლისსამართ-

54 იხ. Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448, (Based on article 12 of the Council Framework Decision of 24.02.2005 on attacks against information systems), Article 2.3

ლებრივ პასუხისმგებლობას კომპიუტერში ან მის ქსელში მართლსა-
წინააღმდეგო შეღწევისთვის. ეს ქმედება დასჯადი ხდებოდა მხო-
ლოდ მაშინ, თუ გამოიწვევდა ინფორმაციის უნებართვო მოპოვებას
(გერმანიის სისხლის სამართლის კოდექსის 202-ა პარაგრაფი)⁵⁵.
კოდექსის დღეს მოქმედი რედაქციის 202-ა პარაგრაფით დამთა-
ვრებულ დანაშაულად ითვლება დაცულ მონაცემთა ბაზაში შეღწევა
ან სხვისთვის შეღწევის უზრუნველყოფა. 202-ბ პარაგრაფით დას-
ჯადია ისეთ მონაცემთა ბაზაში შეღწევა ან სხვისთვის შეღწევის
უზრუნველყოფა, რომელიც არ არის საჯარო გამოყენებისთვის
განკუთვნილი.⁵⁶ ამდენად, გერმანელი კანონმდებლის მიერ გამოიჯ-
ნულია „დაცულ მონაცემთა ბაზა“ და „არასაჯარო გამოყენებისთ-
ვის განკუთვნილ მონაცემთა ბაზა“. უნდა ვივარაუდოთ, რომ პირ-
ველი მათგანი გულისხმობს ისეთ მონაცემთა ბაზას, რომელიც
აღჭურვილია დაცვის სპეციალური პროგრამით, ხოლო მეორე კი,
მართალია, არაა დაცული, მაგრამ თავისი შინაარსით წარმოად-
გენს არასაჯარო დანიშნულების მონაცემთა ბაზას. ჩემი აზრით,
ამ ტერმინით კანონმდებელს სურდა გაემიჯნა საჯარო და კერძო
მონაცემთა ბაზები.

ბუნებრივია, ჩვეულებრივი ინტერნეტ-საიტი უნდა მივაკუთვ-
ნოთ საჯარო ხასიათის მონაცემთა ბაზას, რომელში შესვლაც ნების-
მიერ მომხმარებელს შეუძლია. მაგრამ წარმოვიდგინოთ ქ. თბილისის
მერიის შიდასამსახურებრივი საიტი, რომელზეც ინფორმაცია მხო-
ლოდ მერიის თანამშრომლებისთვის ვრცელდება. აღნიშნულ საიტ-
ზე ვრცელდება მხოლოდ საჯარო ხასიათის ინფორმაცია, მაგრამ
მის არასაჯარო ხასიათს განაპირობებს არა ინფორმაციის შინაარ-
სი, არამედ მისი ადმინისტრატორის მიერ დანესებული შეზღუდვა,
რომ მოცემული საიტით სარგებლობა შესაძლებელი იყოს მხოლოდ
მერიის კომპიუტერულ ქსელში ჩართული კომპიუტერებისთვის.
აქედან გამომდინარე, არასაჯარო მონაცემთა ბაზის თვალსაჩინო
მაგალითად გამოდგება მსგავსი ტიპის შიდასამსახურებრივი საიტი.

55 იხ. Interview: Germany and new cybercrime law By Federico Biancuzzi 11.07.2007.
(<http://www.crime-research.org/interviews/Interview-Germany-and-new-cyber-crime-law/>)

56 იხ. <http://www.gesetze-im-internet.de/stgh/>

შესაბამისად, გერმანიაში დაცულ მონაცემთა ბაზაში შელწევა ითვლება უფრო მძიმე დანაშაულად, ვიდრე არასაჯარო ხასიათის მონაცემთა ბაზაში.

არ შეიძლება დაეთანხმო გერმანელი კანონმდებლის მიდგომას, დაცულ და არასაჯარო მონაცემთა ბაზასთან დაკავშირებით, რადგან როდესაც საუბარია კომპიუტერულ სისტემაში უნებართვო შელწევაზე, მნიშვნელობა არა აქვს იმას, დამნაშავემ შესვლის პაროლი რა გზით მოიპოვა (დაძლია დაცვის სისტემა, კომპიუტერული ვირუსი შეჰყარა და ა.შ.). საკითხი დგას შემდეგნაირად: უნდა იყოს თუ არა კომპიუტერული სისტემა სისხლის სამართლის კოდექსის დაცვის ობიექტი და მასში უნებართვო შელწევა უნდა იყოს თუ არა სისხლის სამართლის დანაშაული? ჩემი პასუხი მარტივია – რა თქმა უნდა!

უფრო ზუსტი იქნებოდა გერმანელ კანონმდებელს დაცულ მონაცემთა ბაზაში შელწევა გამოეყო, როგორც მონაცემთა ბაზაში უნებართვო შელწევის დამამძიმებელი გარემოება.

ბუნებრივია, სანამ კანონმდებელი შემოიღებს კონკრეტულ ამკრძალავ ნორმას, მან უნდა განიხილოს ყველა შესაძლო კაზუსი. როგორც ზემოთაც აღინიშნა, საკანონმდებლო ცვლილების პირველი ვერსია არ კრძალავდა კომპიუტერულ სისტემაში უნებართვო შელწევას, თუ მას არავითარი საზიანო შედეგი არ მოჰყვებოდა მისი მფლობელისთვის.

საქართველოს სისხლის სამართლის კოდექსის 160-ე მუხლის პირველი ნაწილით, რომელიც ბინის ან სხვა მფლობელობის ხელშეუხებლობის დარღვევად მიიჩნევს ბინაში მფლობელის ნების საწინააღმდეგოდ უკანონო შესვლას. კანონმდებლისთვის სულ ერთია დამნაშავე დაკეტილ კარს ალებს თუ ღიად დარჩენილში შედის. თავად ტერმინი „შესვლა“ გამორიცხავს რაიმე ფიზიკურ ზემოქმედებას და ძალადობას. თუ გვექნებოდა ტერმინი „შელწევა“, ვიფიქრებდით, რომ დამნაშავე ბინაში შესაღწევად გადაძკრა ლობეზე, გატეხა საკეტი და ა.შ.

აქედან გამომდინარე, უნდა დავასკვნათ, რომ კანონმდებელი 160-ე მუხლის შემოღებით იცავს ბინის მფლობელის ხელშეუხებლობას და ეს ქმედება დასრულებულ დანაშაულად ჩაითვლება ბინაში მფლობელის ნების საწინააღმდეგოდ შესვლისთანავე.

თუ კანონმდებელი სისხლის სამართლის კოდექსის 160-ე მუხლით სრულიად სამართლიანად იცავს ბინის მფლობელის ხელ- შეუხებლობას, რატომ არ უნდა იყოს იგივესაგან დაცული კომპიუ- ტერული სისტემის მფლობელი?

ვირტუალურად, კომპიუტერული სისტემა შეგვიძლია შევადა- როთ სახლს:

ა) ორივეს აქვს მისამართი - კომპიუტერისთვის ესაა IP მისამართი;

ბ) ყავს მესაკუთრე ან მფლობელი - ქსელის ადმინისტრატორი ან/და კომპიუტერის მფლობელი;

გ) აქვს ავეჯი და სხვადასხვა ტექნიკური მოწყობილობა რაიმე სამუშაოს შესასრულებლად. სახლისთვის ეს შეიძლება იყოს სამზა- რეულო, აბაზანა და ა.შ. კომპიუტერისთვის - კომპიუტერული პროგრამა, რომლიც უზრუნველყოფს კომპიუტერული სისტემის მუშაობას;

დ) აქვს კარი და სიგნალიზაცია, კომპიუტერისთვის ესაა სისტემაში შესვლის პაროლი, სისტემის დამცავი პროგრამა;

ე) აქვს კონკრეტული ფართი, კომპიუტერისთვის ესაა მყარი დისკი, რომელიც განსაზღვრავს დასამუშავებელი ან დამუშავებული მონაცემების ტევადობას.

კიდევ ბევრი საინტერესო პარალელის გავლება შეიძლება. ჩემს პოზიციას სწორედ ამ არგუმენტით ვასაბუთებ და ამ საკითხზე არსებული აზრთა სხვადასხვაობის მიუხედავად მიმაჩნია, რომ კომპიუტერულ სისტემაში უნებართვო შეღწევა უნდა იყოს დასჯადი ქმედება, რაც აისახა კიდევ ქართულ კანონმდებლობაში და დღეს 284-ე მუხლი ნარმოადგენს ფორმალურ შემადგენლობას, რადგან კანონმდებელი ქმედების დანაშაულად კვალიფიკაციას არ უკავში- რებს კონკრეტულ შედეგს. თუმცა მუხლის მე-2 ნაწილის „დ“ პუნქტი მატერიალური შემადგენლობისაა.

ვიზიარებ პროფ. გ. ნაჭყებიას აზრს, რომ „ქმედების შემადგენ- ლობის ობიექტური მხარის ნიშნების ზუსტად დადგენას ქმედების დანაშაულად კვალიფიკაციისთვის უაღრესად დიდი მნიშვნელობა აქვს. ამ მიმართებით, უპირველეს ყოვლისა, იგულისხმება ქმედების

ე.ნ. მატერიალური შემადგენლობა, რომელიც დანაშაულებრივი ქმედების მატერიალურ შედეგში ვლინდება.⁵⁷

284-ე მუხლის მე-2 ნაწილის „დ“ პუნქტში მითითებული „მნიშვნელოვანი ზიანი“ კი გულისხმობს 2000 ლარზე მეტი ოდენობის ზიანს. ამდენად, მოცემული მუხლის „დ“ პუნქტით ქმედების კვალიფიკაციისთვის, გარდა დისპოზიციით გათვალისწინებული ქმედებისა, სახეზე უნდა გვექონდეს, ქმედების შედეგად დამდგარი კონკრეტული შედეგი – მატერიალური ზიანი 2000 ლარს ზევით.

საინტერესოა, გაეხსენოთ საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლის ძველი რედაქცია, რომელიც ჩამოყალიბებული იყო შემდეგნაირად: „კანონით დაცულ კომპიუტერულ ინფორმაციასთან, ე.ი. მანქანა მატარებელზე, ელექტრო გამომთვლელ მანქანაზე (ეგმ-ზე), ეგმ-ის სისტემაში ან მათ ქსელში ასახულ ინფორმაციასთან არამართლზომიერი შელწევა, რამაც ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან მოპოვება ან და ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მოშლა გამოიწვია, ასევე მობილური მონყობილობის საერთაშორისო იდენტიფიკატორის შეცვლა“.

უნდა აღინიშნოს, რომ სისხლის სამართლის კოდექსის ახალი რედაქცია გაექცა იმ მანკიერ პრაქტიკას, რომელიც დამკვიდრებული იყო ყოფილ საბჭოთა ქვეყნებში. მათი უმრავლესობა სისხლის-სამართლებრივ პასუხისმგებლობას უკავშირებდა „კანონით დაცულ კომპიუტერულ ინფორმაციასთან არამართლზომიერ შელწევას“.

დღეს, როცა ახალი კანონმდებლობა აღარ აკეთებს მსგავს დათქმას, მაინც საინტერესოა, გავცეთ პასუხი კითხვას: რა არის საერთოდ ინფორმაცია და რა იგულისხმება „კომპიუტერულ ინფორმაციაში“, მაშინ როცა ამ ტერმინს, მეტნაკლებად უახლოვდება ტერმინი „კომპიუტერული მონაცემი“. უკვე ითქვა, რომ დღეს მოქმედი 284-ე მუხლის რედაქცია, ევროსაბჭოს კონვენციის გავლენით, პასუხისმგებლობას უკავშირებს არა კანონით დაცულ კომპიუტერულ ინფორმაციაში, არამედ კომპიუტერულ სისტემაში უნებართვო შელწევას. აღსანიშნავია, რომ კომპიუტერულ ინფორ-

57 იხ. გ. ნაჭყებია, „სისხლის სამართალი, ზოგადი ნაწილი“, საგამომცემლო სახლი „ინოვაცია“, თბ. 2011წ. გვ. 251.

მაციაში ვერ ვიგულისხმებდით კომპიუტერულ პროგრამას, რადგან ეს უკანასკნელი არ ექცეოდა სიტყვა „ინფორმაციის“ დეფინიციაში. ინფორმაცია ლათინური სიტყვაა და გაცნობას, გადაცემას ნიშნავს. ეს სიტყვა სამეცნიერო ბრუნვაში XX საუკუნის II ნახევარში შემოვიდა. ამის შემდეგ მისდამი ინტერესს იურისტებიც იჩენდნენ. არსებობს ინფორმაციის განმარტების უამრავი გზა და აღსანიშნავია, რომ იურიდიული განმარტება საკითხის ფილოსოფიური გააზრების გარეშე შეუძლებელია. ძირითადად ფილოსოფიურ ლიტერატურაში ინფორმაციის განსაზღვრისთვის იყენებენ ატრიბუტულ და ფუნქციონალურ კონცეფციებს. პირველის მომხრეები მიიჩნევენ, რომ ინფორმაცია მატერიალური ობიექტის შინაგანი თვისებაა, ხოლო მეორენი არ ეთანხმებიან ასეთი ინფორმაციის არსებობას. სხვა მრავალი საინტერესო მოსაზრებაც არსებობს ამ საკითხზე, მაგრამ ჩვენთვის ყველაზე მთავარი „ინფორმაციის“ იურიდიული განმარტებაა. იურიდიული თვალსაზრისით კი ინფორმაცია არის ცნობა, მონაცემი, რომელიც შეტყობინების პროცესში (მიღება, შენახვა, დამუშავება, გადაცემა) სამართლებრივი ურთიერთობის საგანს წარმოადგენს და შეიძლება გახდეს რაიმე სამართლებრივი ვალდებულების წარმოშობის ან შეწყვეტის საფუძველი⁵⁸.

კომპიუტერული ინფორმაცია ყოველთვის მოიცავს სამ ძირითად მახასიათებელ ნიშანს:

ფიზიკური – კომპიუტერული ინფორმაციის ფიზიკურ ნიშანს განსაზღვრავს მისი მატარებელი (დისკი, ოპტიკური დისკი და სხვა.), რომელიც, როგორც წესი, განიხილება როგორც საგანი, ნივთი, რომელიც გამოიყენება ინფორმაციის დამუშავების, გადაცემის, შენახვისთვის და ა.შ. კომპიუტერული ინფორმაციის მატარებლად ასევე განიხილება სხვადასხვა სიგნალი. მაგ. ელექტრონული სიგნალი სატელეფონო ხაზით დამყარებულ კავშირში შეიძლება იყოს კომპიუტერული ქსელების ინფორმაციის მატარებელი. ასე რომ, კომპიუტერული ინფორმაციის ფიზიკურობის ნიშნის დასადგენად უნდა არსებობდეს ინფორმაციის მატარებელი სიგნალი. ასევე სხვა

58 იხ. მ. ცაცანაშვილი, „ინფორმაციული საზოგადოება და ინფორმაციის სამართლებრივი რეგულირება“, გამომც. „ტექნიფორმი“ თბ. 1999წ. გვ. 26

მონყობილობა, რომელიც გამოიყენება ელექტრონული სახით არსებული ინფორმაციის შენახვა, გადაცემა, დამუშავებისთვის.

ეკონომიკურ ნიშანს განსაზღვრავს ამ ინფორმაციის ღირებულება, ფასი.

იურიდიული ნიშანი – კომპიუტერულ ინფორმაციას ჰყავს მესაკუთრე და მას ამ ინფორმაციის საჯარო ხელმისაწვდომობა შეზღუდული აქვს სხვადასხვა დაცვითი პროგრამით, პაროლით და ა.შ.⁵⁹ თუმცა, აღსანიშნავია, რომ შესაძლებელია ამგვარ ინფორმაციასთან მელწევა არც იყოს შეზღუდული⁶⁰.

გამოდის, რომ კომპიუტერული ინფორმაცია და კომპიუტერული პროგრამა არაფრით უკავშირდება ერთმანეთს, გარდა იმისა, რომ ორივე კომპიუტერული წარმოშობისაა. თუკი მოქმედი კანონმდებლობით დასჯადი იქნებოდა კომპიუტერულ ინფორმაციაში უნებართვო შეღწევისთვის საჭირო პაროლის, კოდის და ა.შ. დამზადება, ღიად დარჩებოდა იგივეს, კომპიუტერულ პროგრამაში შეღწევის მიზნით ჩადენა, რაც პრაქტიკაში შექმნიდა მნიშვნელოვან დაბრკოლებას. მიმაჩნია, რომ ტერმინი „კომპიუტერული მონაცემი“ პასუხობს ევროსაბჭოს კონვენციის მოთხოვნებს და იძლევა შესაძლებლობას სისხლისსამართლებრივ პასუხისგებაში მიეცეს დამნაშავე.

კანონით დაცული ინფორმაციის განმარტებას განსაკუთრებული მნიშვნელობა ენიჭებოდა 284-ე მუხლის ძველი რედაქციის არსებობის პირობებში, თუმცა მისი განხილვა დღევანდელი მდგომარეობითაც არ არის ინტერესს მოკლებული, რადგან ზოგადად ტერმინი „ინფორმაცია“ და „კომპიუტერული ინფორმაცია“ კვლავაც აქტუალურია ქმედების დანაშაულად კვალიფიკაციისთვის. შესაძლებელია, ინფორმაციას შეიცავდნენ დოკუმენტები, მონაცემთა ბაზები, ინფორმაციული რესურსები, ინფორმაციული მასივები. კანონით

59 იხ. Н.В.Карчевский, Компьютерные преступления:определение, объект и предмет, Доклад V Международной конференции «Право и Интернет: теория и практика», www.ifap.ru/pi/05/karchev.htm

60 მაგალითად გამოდგება აშშ, კერძოდ, კანონთა კრებულის მე-18 ტიტულის 1030-ე მუხლი, რომლითაც ამერიკელი კანონმდებელი დასჯადად აცხადებს კომპიუტერულ სისტემაში არასანქცირებულ შეღწევას, ან სანქცირებული შესვლის ფარგლების გადამეტებას (U.S. Code, Title 18, part I, Chapter 47, § 1030, Fraud and related activity in connection with computers).

დაცული ანუ დახურული ინფორმაცია კი მათგან საქართველოში მოქმედი კანონმდებლობის შესაბამისად არის:

ა) სახელმწიფო საიდუმლო - „სახელმწიფო საიდუმლოების შესახებ“ საქართველოს კანონის 1-ლი მუხლის პირველი ქვეპუნქტის მიხედვით, სახელმწიფო საიდუმლოება არის ინფორმაციის სახეობა, რომელიც მოიცავს სახელმწიფო საიდუმლოების შემცველ მონაცემებს თავდაცვის, ეკონომიკის, საგარეო ურთიერთობების, დაზვერვის, სახელმწიფო უსაფრთხოების და მართლწესრიგის დაცვის სფეროებში, რომელთა გამჟღავნებას ან დაკარგვას შეუძლია ზიანი მიაყენოს საქართველოს ან საერთაშორისო ხელშეკრულებებისა და შეთანხმებების მონაწილე მხარის სუვერენიტეტს, კონსტიტუციურ წყობილებას, პოლიტიკურ და ეკონომიკურ ინტერესებს;“ მე-2 მუხლის მე-2 ქვეპუნქტი კი ადგენს, რომ ამ კანონის მოქმედება არ ვრცელდება კომერციული ან საბანკო საიდუმლოებების, საფინანსო, სამეცნიერო-ტექნოლოგიური, საგამომგონებლო და სხვა სახის საიდუმლო ინფორმაციის დაცვასთან დაკავშირებულ ურთიერთობებზე, თუ ეს ინფორმაცია ამავე დროს არ წარმოადგენს სახელმწიფო საიდუმლოს. ამავე კანონის მე-8 მუხლის შესაბამისად სახელმწიფო საიდუმლოს არ შეიძლება მიეკუთვნოს ნორმატიული აქტები, საერთაშორისო ხელშეკრულებები და შეთანხმებები, გარდა საქართველოს თავდაცვის, შინაგან საქმეთა, იუსტიციის, სასჯელაღსრულების, პრობაციის და იურიდიულ დახმარების საკითხთა, ფინანსთა და გარემოს დაცვისა და ბუნებრივი რესურსების სამინისტროების, საქარველოს საგარეო დაზვერვის სპეციალური სამსახურის და საქართველოს სახელმწიფო დაცვის სპეციალური სამსახურის აქტებისა, რომლებიც აწესრიგებს მათ შიდა საქმიანობას თავდაცვის, უშიშროებისა და ოპერატიულ-სამძებრო საქმიანობის თვალსაზრისით. არ შეიძლება სახელმწიფო საიდუმლოებას მიეკუთვნოს რუკები, გარდა სპეციალური რუკებისა. არ შეიძლება სახელმწიფო საიდუმლოებას მიეკუთვნოს ინფორმაცია: სტიქიური უბედურების, კატასტროფების და სხვა განსაკუთრებული მოვლენების შესახებ, რომლებიც უკვე მოხდა, ან შეიძლება მოხდეს და ემუქრება მოქალაქეთა უსაფრთხოებას, აგრეთვე, ინფორმაცია გარემოს მდგომარეობის, მოსახლეობის ჯანმრთელობის, დემოგრაფიული მაჩვენებლის, სამედიცინო მომსახურების, კორუფციის,

კრიმინოგენული სიტუაციის შესახებ, პროვილეგიების, კომპენსაციების და შეღავათების შესახებ, რომლებსაც სახელმწიფო ანიჭებს მოქალაქეებს, თანამდებობის პირებს და ა.შ. ასევე, ინფორმაცია სახელმწიფო სავალუტო ფონდისა და ოქროს საერთო მარაგის შესახებ და სახელმწიფო ხელისუფლების უმაღლეს თანამდებობის პირთა ჯანმრთელობის შესახებ.

ბ) კომერციული საიდუმლოება – ზოგადი ადმინისტრაციული კოდექსის 27²-ე მუხლის მიხედვით კომერციული ინფორმაცია არის – კომერციული ფასეულობის მქონე გეგმის, ფორმულის, პროცესის, საშუალების თაობაზე ან ნებისმიერი სხვა ინფორმაცია, რომელიც გამოიყენება საქონლის სანარმოებლად, მოსამზადებლად, გამოსამუშავებლად ან მომსახურეობის გასანევენად ან/და რომელიც წარმოადგენს სიახლეს ან ტექნიკური შემოქმედების მნიშვნელოვან შედეგს. „საგადასახადო საიდუმლების შემცველი ინფორმაციის შენახვის რეჟიმის და დაშვების წესის შესახებ ინსტრუქციის დამტკიცების თაობაზე“ საქართველოს ფინანსთა მინისტრის ბრძანების მე-5 მუხლის მიხედვით კი კომერციულ საიდუმლოებად ჩაითვლება ნებისმიერი ის ინფორმაცია, რომელსაც გააჩნია კომერციული ღირებულება, ანუ ამ ინფორმაციის საფუძველზე შესაძლებელია მოგების მიღება პირის მიერ. ეს ინფორმაცია შეიძლება წარმოადგენდეს სიახლეს ან ტექნიკური შემოქმედების მნიშვნელოვან შედეგს, მაგალითად, ახალი სამკურნალო პრეპარატის შემადგენლობას. კომერციულ საიდუმლოდ მიიჩნევა აგრეთვე, ინფორმაცია, რომლის გამჟღავნებამ შესაძლოა ზიანი მიაყენოს პირის კონკურენტუნარიანობას ბაზარზე, მაგალითად, სანარმოს ბრუნვა, თანამშრომელთა რაოდენობა, განეული ხარჯები, არსებული ქონება, შეძენილი საქონლის ღირებულება, რა უჯდება ერთი ერთეული პროდუქციის წარმოება და რომელ რეგიონში ყიდის ყველაზე უკეთ ან ყველაზე ცუდად და ა.შ.

გ) პირადი საიდუმლოება – პერსონალური მონაცემების პირად საიდუმლოებად მიჩნევის საკითხს, გარდა კანონით გათვალისწინებული შემთხვევებისა წყვეტს პირი, რომელსაც ეხება ეს ინფორმაცია (ზოგადი ადმინისტრაციული კოდექსის 27-ე მუხლი).

დ) საგადასახადო საიდუმლოება – „საგადასახადო საიდუმლების შემცველი ინფორმაციის შენახვის რეჟიმის და დაშვების წესის

შესახებ ინსტრუქციის დამტკიცების თაობაზე" საქართველოს ფინანსთა მინისტრის ბრძანების საფუძველზე არის ნებისმიერი ინფორმაცია გადასახადის გადამხდელების შესახებ, რომელიც ცნობილი გახდა საგადასახადო ორგანოსთვის კანონმდებლობით განსაზღვრული ფუნქციების შესრულებისას. უფრო კონკრეტულად კი, ცნობები გადასახადის გადამხდელის შესახებ მისი აღრიცხვაზე აყვანის მომენტიდან ითვლება საგადასახადო საიდუმლოებად. ასეთ საიდუმლოებას განეკუთვნება: გადასახადის გადამხდელის მიერ წარდგენილი საგადასახადო დეკლარაციები, გადამხდელისგან შესული წერილები და მათზე გაცემული პასუხები, გადამხდელთა შესამოწმებლად გაცემული ბრძანებები, შემოწმების აქტები, საინკასო დავალებები, გადამხდელთა დაბეგვრის საქმეები, გადასახადის გადამხდელთა რეესტრი და ა.შ.

ლიას ანუ ინფორმაციას, რომელიც არ წარმოადგენს კანონით დაცულს, მიეკუთვნება ნორმატიული აქტები, მასობრივი ინფორმაცია, ოფიციალური დოკუმენტები (მათ შორის ნახაზი, გეგმა, მაკეტი, სქემა, ფოტოსურათი, ელექტრონული ინფორმაცია, ვიდეო და აუდიოჩანაწერები) ანუ საჯარო დანესებულებაში დაცული, აგრეთვე საჯარო დანესებულების ან მოსამსახურის მიერ სამსახურებრივ საქმიანობასთან დაკავშირებით მიღებული, დამუშავებული, შექმნილი ან გაგზავნილი ინფორმაცია, შემოქმედების პროცესში შექმნილი მასალები და ა.შ.

ნებისმიერი ინფორმაცია შეიძლება იყოს ელექტრონული ანუ კომპიუტერული ხასიათის. ჩვეულებრივისგან მისი განსხვავება ისაა, რომ მისი შექმნა, დამუშავება, შენახვა, გადაცემა და სხვა, ხდება ელექტრონული საშუალებებით. ბუნებრივია, ამ სახის ინფორმაციაზეც უნდა გავრცელდეს სახელმწიფოს მიერ დადგენილი ღია და დახურული რეჟიმები. საბოლოოდ გამოდის, რომ სახეზე, კანონით დაცული დახურული ინფორმაცია გვაქვს და მხოლოდ ამ სახის ინფორმაციაში შელწევა, მოდიფიცირება, ბლოკირება და ა.შ. ჩაითვლებოდა დანაშაულად. ვინაიდან, ღია ინფორმაციასთან დაშვება კანონით შესაძლებელი იყო, მასში შელწევა და მისი მოდიფიცირება, ბლოკირება, განადგურება და ა.შ. 284-ე მუხლით დასჯადობას არ ექვემდებარებოდა.

საინტერესო მსგავსებაა სისხლის სამართლის კოდექსის ძველ და ახალ რედაქციებს შორის კიდევ ერთ ნაწილში, კერძოდ, ძველი რედაქციით გათვალისწინებული დანაშაულის ობიექტური მხარე გამოიხატებოდა კანონით დაცულ კომპიუტერულ ინფორმაციაში არამართლზომიერ შეღწევაში, რომელიც იწვევდა ინფორმაციის განადგურებას, ბლოკირებას, მოდიფიცირებას ან მოპოვებას, ანდა ეგმ-ის, ეგე-ის სისტემის ან მათი ქსელის მუშაობის მოშლას. ტერმინში „არამართლზომიერი“ უნდა ვიგულისხმოთ დამნაშავეს მოქმედება კომპიუტერის, მისი სისტემის ან ქსელის მფლობელის ნებართვის და ავტორიზაციის გარეშე.

284-ე მუხლის დისპოზიცია არ განსაზღვრავს კომპიუტერულ სისტემაში შეღწევის კონკრეტულ სახეს, რადგან იგი ახალი ტექნოლოგიების განვითარებისა და აღმოჩენის პარალელურად ხშირად იცვლება. სწორედ ამიტომ დისპოზიციაში ტექნოლოგიებთან მიმართებაში ნეიტრალური ტერმინებია გამოყენებული⁶¹, რაც ქმედების დანაშაულად კვალიფიკაციისას მეტი ინტერპრეტაციის საშუალებას იძლევა. ეს შეიძლება შევაფასოთ დადებითად, რადგან საგამოძიებო ორგანოები და სასამართლო არ იქნება შეზღუდული კომპიუტერულ სისტემაში უნებართვო შეღწევის ხერხის დეტალური გამოკვლევის ვალდებულებით. საკმარისი იქნება დადგინდეს უშუალოდ შეღწევის ფაქტი და ამ ქმედების უნებართვობა. თუმცა, შესაძლებელია გამოვყოთ ის ხერხი, რომლის დახმარებითაც დამნაშავე ახერხებს კომპიუტერულ სისტემაში შეღწევას. კომპიუტერულ სისტემაში შეღწევა შესაძლებელია ფიზიკურად და დისტანციურად. ფიზიკური გულისხმობს კომპიუტერულ ტექნიკასთან უშუალო კონტაქტის გზით კომპიუტერულ სისტემაში შეღწევას, დისტანციურში კი იგულისხმება გლობალური ქსელის საშუალებით (თუნდაც სამიზნე კომპიუტერი მეზობელ ოთახში იდგეს) და სხვადასხვა პროგრამის დახმარებით კომპიუტერულ სისტემაში შეღწევა.

შელწევისთვის დამნაშავე იყენებს სხვადასხვა სახის კომპიუტერულ პროგრამას. მაგალითად, ე.წ. „ტროას ცხენი“. „ფაილების

61 იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ: ტრენინგის სახელმძღვანელო“, ევროსაბჭო, სტრასბურგი, 2010წ. გვ. 47

ხელმისაწვდომობის უზრუნველსაყოფად მის სამიზნე კომპიუტერულ სისტემაში დაინსტალირების (კომპიუტერის ოპერაციულ სისტემაში ინტეგრირების) პროცესს ინფილტრაცია ეწოდება. იგი განსხვავებული მეთოდებს მოიცავს: ერთი მათგანი მოითხოვს მომხმარებლის მიერ მხარდაჭერას (გაუთვითცნობიერებელ), მეორე კი, მომხმარებლის დახმარების გარეშე ხორციელდება.⁶²

„ტროას ცხენის“ მეშვეობით შესაძლებელია უცხო კომპიუტერულ სისტემაზე სრული კონტროლის მოპოვება. მისი ნაირსახეობაა ე.წ. „ლოგიკური ბომბი“ – პროგრამაში ბრძანების შეყვანა, რომელიც მხოლოდ განსაზღვრულ პირობებში ამუშავდება, ან ე.წ. „დროზე დამოკიდებული ბომბი“ – იგი დროის გარკვეულ მომენტში აქტიურდება.

ზემოაღნიშნული კომპიუტერული პროგრამების გამოყენების მიზნით დამნაშავეები ხშირად სარგებლობენ ყალბი ელექტრონული ფოსტით. ყალბი ელექტრონული ფოსტა ძირითადად გამოიყენება შესანიშნავად და კომპიუტერულ სისტემაში შავი ხერხის⁶³ შესაქმნელად. შენიღბვაში იგულისხმება ის, რომ დაზარალებული ელექტრონულ შეტყობინებას იღებს ისეთი მომხმარებლის მისამართიდან, რომლის რეპუტაციაში ეჭვის შეტანის საფუძველიც არ არსებობს⁶⁴ და ამიტომ დაზარალებული შეტყობინების გაცნობის მიზნით ხსნის მას, რაც ინვესს სპეციალური კომპიუტერული პროგრამის გააქტიურებას და შედეგად, სამიზნე კომპიუტერში შესაძლებელი ხდება უნებართვო შეღწევა.

ყალბი ელექტრონული ფოსტის თაობაზე კი ნ. ცომაია წერს, რომ: „იმ მეთოდებს შორის, რომლებშიც გათვალისწინებულია მომხმარებლის ქცევა, ელექტრონული ფოსტის მეშვეობით საინტერესო ფაილების გაგზავნა იგულისხმება. მომხმარებლის მიერ აღნიშნული ელექტრონული გზავნილის გახსნისას ხდება ინფილტრაცია

62 იხ. ნ. ცომაია, „სახელმწიფოს მხრიდან კომპიუტერულ სისტემებში ფარული შეღწევა და ამ ღონისძიების კონსტიტუციურ-სამართლებრივი საზღვრები“, ჟურნ. „მართლმსაჯულება და კანონი“, 2008წ. №2, გვ. 81

63 „შავ ხერხში“ იგულისხმება კომპიუტერულ სისტემაში შეღწევის არალეგალური გზა.

64 იხ. К. Мандиа, К. Просис, «Защита от вторжении: Расследование компьютерных преступлений», Переводчик О.Труфанов, Изд. «Лори», М. 2005 г. გვ. 456

ან იწყება ინფილტრაციის ტექნიკის გააქტიურება.“⁶⁵ ნ. ცომაიას აზრით, ვებ-გვერდების დათვალიერებისას შესაძლოა მომხმარებლის „შეტყუება“ იმ სხვადასხვა ფაილის გასახსნელად, თუ სხვა ოპერაციის შესასრულებლად, რომელიც „ტროას ცხენს“ შეიცავს.“⁶⁶

დამნაშავეები კომპიუტერულ სისტემაში უნებართვოდ შესაღწევად ასევე, იყენებენ პაროლის მოსარგებ (ამომცნობ) პროგრამას. აღნიშნულმა საქართველოშიც ფართო გამოყენება ჰპოვა უკანასკნელ წლებში. მაგალითად, სხვადასხვა ინტერნეტ-საიტზე იოლად მოძებნით ამათუიშ სოციალური ქსელში ან საინფორმაციო პროგრამაში უცხო პირის პირად გვერდზე შეღწევისთვის საჭირო პაროლის ამომცნობი პროგრამის რეკლამას. მათი გადმოწერა და გამოყენება სრულიად უფასოა და შესაძლებელი. ასევე გვხვდება ამათუიშ ტიპის ფაილზე (მაგალითად, ე.წ. „მაიკროსოფტ ვორდი“, ე.წ. „ვინარა“ და ა.შ.) მესაკუთრის მიერ დაცვის მიზნით დადებული პაროლის ამომცნობი პროგრამების ფართო ასორტიმენტი.

სამწუხაროდ, ქართველი სამართალდამცავები იმ ინტერნეტ-საიტების წინააღმდეგ რომლებიც უკანონოდ ავრცელებენ მსგავს პროგრამებს, ქმედით ღონისძიებებს არ ატარებენ, რაც კიბერ-დანაშაულის ჩასადენად კიდევ უფრო „ნოყიერ“ ნიადაგს უქმნის პოტენციურ დამნაშავეებს.

კომპიუტერულ სისტემაში უნებართვო შეღწევისას, ხშირია შემთხვევა, როცა დამნაშავე თანამშრომლობს ჯიბის ქურდებთან, რომელთა საშუალებითაც სამიზნე კომპიუტერის მეპატრონეს ჰპარავენ საფულეს, მობილურ ტელეფონს, ბლოკნოტს, სადაც შესაძლებელია იგი ინახავდეს კომპიუტერულ სისტემაში შესაღწევ პაროლს. ამ დროს დამნაშავე ყოველგვარი ძალისხმევის გარეშე, ისევე როგორც ამავე სისტემის მეპატრონე, შედის კომპიუტერულ სისტემაში. ასევე საინტერესოა, რომ მსოფლიოში ფართოდაა გავრცელებული პაროლით ვაჭრობა. კერძოდ, დამნაშავეთა გარკვეული წრის მიერ ხდება უშუალოდ პაროლის ქურდობა, ხოლო შემ-

65 იხ. ნ. ცომაია, „სახელმწიფოს მხრიდან კომპიუტერულ სისტემებში ფარული შეღწევა და ამ ღონისძიების კონსტიტუციურ-სამართლებრივი საზღვრები“, ურნ. „მართლმსაჯულება და კანონი“, 2008წ. №2, გვ. 81

66 იხ. იქვე.

დეგ მისი მიყიდვა სხვა პირისთვის, რომელიც უნებართვოდ აღწევას კომპიუტერულ სისტემაში.

აღსანიშნავია, რომ ჩემს მიერ სასამართლოდან გამოთხოვილ იქნა 284-ე მუხლით გასამართლებულ პირებთან დაკავშირებული ათამდე საქმე. ხაზგასასმელია, რომ განაჩენების 50 პროცენტში კომპიუტერულ სისტემაში უნებართვო შეღწევის ხერხი განმარტებული არ არის. 50 პროცენტში კი ხერხი ფორმულირებულია დაახლოებით ამგვარად: მოქ. ა. სილაგავა იმყოფებოდა ქ. თბილისში მეტროსადგურ „აელაბარის“ მიმდებარე ტერიტორიაზე არსებულ ინტერნეტ-კაფეში, სადაც მან დაიმხსოვრა იქვე მყოფი მოქ. ნ. ნიკლაურის მიერ ინტერნეტ-ტოტალიზატორ „ფრანჩესკოში“ პირადი გვერდის გახსნისას გამოყენებული სახელი და პაროლი, რითაც უნებართვოდ შეაღწია ამ უკანასკნელის პირად ინტერნეტ-გვერდზე. ან ამგვარად: მოქ. დ. ნებიერიძე მეგობარ ზ. იოსავასთან ერთად იმყოფებოდა ი. ჭავჭავაძის გამზირზე არსებულ მაღაზიაში, სადაც პროდუქტის შეძენის დროს ფარულად ამონერა გ. გოგალაძის კუთვნილი საკრედიტო ბარათის მონაცემები, კერძოდ ბარათის ნომერი და მესაკუთრის სახელი და გვარი, რის შემდეგაც საკუთარი კომპიუტერიდან უნებართვოდ შეაღწია ინტერნეტ-ტოტალიზატორ „ფრანჩესკოს“ საიტზე გახსნილ გ. გოგალაძის პირად გვერდზე და თანხა საკუთარ ანგარიშზე გადარიცხა⁶⁷.

როგორც ვხედავთ, საქართველოში კომპიუტერულ სისტემაში უნებართვო შეღწევისთვის დამნაშავეები ზემოთგანხილულ ხერხებზე ხშირად იყენებენ უფრო იოლ მეთოდებს. კერძოდ, იქნება ეს მომხმარებლის პაროლის გადანერა, დამახსოვრება თუ სხვა.

საგულისხმოა, რომ ისევე როგორც ზოგადად კომპიუტერული დანაშაულის ჩადენის ხერხი, ასევე კომპიუტერულ სისტემაში უნებართვო შეღწევის ხერხი დროთა განმავლობაში სულ უფრო იხვეწება, რაც საბოლოო ჯამში ქმნის დისკომფორტს გამოძიების ორგანოებისთვის, ხოლო მეცნიერისთვის დაბრკოლებას – გადაჭრით ამტკიცონ რაიმე, როგორც ზოგადად კომპიუტერული დანაშაულის, ასევე, უნებართვო შეღწევის კონკრეტულ ხერხთან დაკავშირებით.

67 ორივე კაზუსში დასახელებული ყველა პირის ვინაობა შეცვლილია.

იმისთვის რომ ქმედება მივიჩნიოთ დანაშაულად მნიშვნელოვანია არა ის, თუ რამდენად კანონით დაცულია ინფორმაცია, ან რამდენად დაცულია თავად კომპიუტერი, არამედ ის, რომ უნდა არსებობდეს კომპიუტერულ სისტემაში უნებართვოდ შეღწევის ფაქტი. წარმოვიდგინოთ ავტომობილის კომპიუტერული უზრუნველყოფა, რომელიც განსაზღვრავს სხვადასხვა ტექნიკურ მაჩვენებელს. მაგალითად, ავტომანქანის გარბენის მაჩვენებლი. აღნიშნული ინფორმაცია მნიშვნელოვანია თავად მანქანის ღირებულების განსაზღვრისთვის. განვიხილოთ შემთხვევა, როცა მანქანის მეპატრონე შედის საკუთარი მანქანის კომპიუტერულ სისტემაში (რომლის განხორციელებაც ხშირ შემთხვევაში ქარხნული ლუქის ახსნის გარეშე შეუძლებელია) და ცვლის ამ მონაცემს. ჩნდება კითხვა, გარდა იმისა, რომ ამ მონაცემის შეცვლას სჭირდებოდა თუ არა რაიმე სპეციალური ნებართვა, თავად სისტემაში შეღწევა არის თუ არა უნებართვო?

აღსანიშნავია, რომ თუ მოცემულ კომპიუტერულ სისტემაზე აბსტრაქტულ უფლებას მივანიჭებთ ავტომობილის მწარმოებელს, გამოდის, რომ მესაკუთრეს მისი შეკეთების უფლებაც არ აქვს, რაც არასწორია. მაგალითისთვის, გარკვეული დაზიანების შემთხვევაში, შესაძლებელია საჭირო გახდეს კომპიუტერულ სისტემაში შესვლა და მონაცემების გასწორება. ასეთი ქმედება კი არ უნდა ჩაითვალოს უნებართვო შეღწევად და შესაბამისად, დანაშაულად.

ამ კუთხით აშშ-ში განსხვავებული მიდგომაა დამკვიდრებული, კერძოდ, ქმედების დანაშაულად კვალიფიკაციისთვის აუცილებელია დადგინდეს არა შეღწევის უნებართვობა, არამედ დამნაშავის მიზანი, რომელიც უნდა შეიცავდეს ზოგადად ზიანის მიყენების სურვილს და არაა აუცილებელი რაიმე კონკრეტული ზიანის მიყენების მიზნის დადგენა⁶⁸.

როგორც აღვნიშნეთ, დღევანდელი რედაქციით ტერმინი „არამართლზომიერი“ შეცვლილია ტერმინით „უნებართვო“. ამ სიახლის უპირატესობა არის ის, რომ კოდექსი ახლა თავადვე გვაძლევს განმარტებას, თუ რა უნდა ვიგულისხმოთ „უნებართვოში“, რაც გამო-

68 იხ. Field Guidance New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot act of 2001, Computer Crime and Intellectual Property Section(CCIPS), Перевод М. Буряк (<http://kiev-security.org.ua/box/4/94.shtml>)

რიცხავს მთელ რიგ ბუნდოვან დასკვნას ამა თუ იმ კონკრეტული ქმედების დანაშაულად კვალიფიკაციისას.

საინტერესოა, აშშ-ში დამკვიდრებული პრაქტიკის ანალიზი. კერძოდ, აღსანიშნავია, რომ აშშ-ში სისხლისსამართლებრივ პასუხისმგებლობას განსაზღვრავს არა „კანონით დაცულ ინფორმაციაში“ ან ზოგადად „კომპიუტერულ სისტემაში“ უნებართვო შეღწევა, არამედ ნებისმიერი ქმედება, რომელიც ხელყოფს აშშ-ს კანონთა კრებული მ-18 ტიტულის 1030-ე მუხლით დადგენილ „დაცულ კომპიუტერს“. ამ უკანასკნელში იგულისხმება კომპიუტერი, რომელიც წარმოადგენს სახელმწიფოს საკუთრებას და მის სარგებლობაშია, ან ის წარმოადგენს ფინანსური ორგანიზაციის საკუთრებას და მის სარგებლობაშია, ან კომპიუტერი, რომლის ფუნქციონირების დარღვევა სახელმწიფოს ან ფინანსური ორგანიზაციის ინტერესს ლახავს; ასევე კომპიუტერები, რომლებიც გამოიყენება შტატთაშორის ან საერთაშორისო ურთიერთობაში აშშ-ს მთავრობის მიერ (მიუხედავად მათი ადგილმდებარეობისა) ან კომპიუტერი, რომელიც წარმოადგენს ისეთი სისტემის ან ქსელის ნაწილს, რომლის ელემენტებიც განთავსებულია აშშ-ს ფარგლებს გარეთ.

ამავე საკითხზე ქსელების უსაფრთხოების სპეციალისტის ერიკ მეივოლდის აზრით, აშშ-ს კანონთა კრებული მ-18 ტიტულის 1030-ე მუხლის შესაბამისად „დაცული კომპიუტერის“ ცნებაში ასევე იგულისხმება იმ ორგანიზაციების კომპიუტერები, რომლებიც უკავშირდება ქვეყნის შიდა თუ გარე ვაჭრობას და კომუნიკაციას. აქედან გამომდინარე, ინტერნეტში ჩართული კომპიუტერების კლასიფიკაციისას მათი უმრავლესობა იქნება სწორედ ზემოაღნიშნული „გამოყენებული შიდა თუ გარე ვაჭრობის და კომუნიკაციის“ რიგებში⁶⁹.

კომპიუტერულ სისტემაში უნებართვოდ შეღწევის საილუსტრაციოდ მოვიყვან კაზუსს საქართველოს სასამართლო პრაქტიკიდან.⁷⁰

69 იხ. Интернет-Университет Информационных Технологий, Лекция №5: Юридические вопросы информационной безопасности, автор Ерик Мэйволд (<http://www.intuit.ru/departments/security/netsec/5/>)

70 კაზუსში დასახელებული ყველა თარიღი, ნომერი, დასახელება და პირის ვინაობა შეცვლილია.

მოქალაქე ვასილ თანიაანის მიმართ გამოტანილ იქნა გამამტყუნებელი განაჩენი 2011 წელს საქართველოს სისხლის სამართლის კოდექსის 177-ე მუხლის მე-2 ნაწილის „ა“ პუნქტით და 284-ე მუხლის პირველი ნაწილით გათვალისწინებული დანაშაულის ჩადენისთვის. განაჩენში ვკითხულობთ: „ვ. თანიაანი რეგისტრირებული იყო რა ინტერნეტ-საიტზე „დოლარიბეთის“ ონლაინ-თამაშებზე, პერსონალური და სამსახურებრივი კომპიუტერის გამოყენებით განიზრახა ამავე საიტზე დარეგისტრირებულ სხვა მომხმარებელთა კომპიუტერულ სისტემაში უნებართვოდ შეღწევა. ამის შემდეგ მას სურდა მოეპოვებინა პაროლი და მართლსაწინააღმდეგოდ მიეთვისებინა მათ პირად ანგარიშზე არსებული ფულადი თანხა. განზრახვის სისრულეში მოყვანის მიზნით, ვ. თანიაანმა 2011 წლის 31 მაისს უკანონოდ, რეალური მომხმარებლის პაროლის გამოყენებით შეაღწია ინტერნეტ-საიტ „დოლარიბეთის“ მომხმარებლის ილია სეთურიძის პირად გვერდზე და მისი ანგარიშიდან საკუთარ სახელფასო ბარათზე უკანონოდ გადარიცხა ფულადი თანხა 300 ლარის ოდენობით, რამაც მნიშვნელოვანი ზიანი გამოიწვია.“

განაჩენში მითითებულია, რომ ვ. თანიაანმა ეს ქმედება გაიმეორა რამდენიმე სხვა მომხმარებლის მიმართაც. ვ. თანიაანმა მათი ანგარიშიდანაც გადარიცხა საკუთარ სახელფასო ბარათზე თანხა. აღსანიშნავია, რომ ერთ-ერთი მომხმარებლის ანგარიშიდან მან საკმაოდ დიდი თანხა 2500 ლარი გადარიცხა. ჯამში კი ყველა მომხმარებელს მან მიაყენა დაახლოებით 4000 ლარზე მეტი ოდენობის ზიანი.

სასამართლომ დანაშაული დააკვალიფიცირა საქართველოს სისხლის სამართლის კოდექსის 177-ე მუხლის მე-2 ნაწილის „ა“ პუნქტით, ქურდობა, რამაც მნიშვნელოვანი ზიანი გამოიწვია და 284-ე მუხლის პირველი ნაწილით.

აღსანიშნავია, რომ სასამართლო განაჩენში არ უთითებს კონკრეტულ ხერხს, რის შედეგადაც განხორციელდა უნებართვო შეღწევა. როგორც, ზემოთაც აღვნიშნეთ, მას ეს ვალდებულება არც გააჩნია, რადგან ქმედების 284-ე მუხლით კვალიფიკაციისთვის აუცილებელი არაა ამის დადგენა. თუმცა, საქმის უკეთ შესწავლის მიზნით, 2012 წლის 23 თებერვალს მივმართე სასამართლოს საქმის

გაცნობის თხოვნით, რადგან ვერაუდობდი, რომ საქმეში არსებულ მტკიცებულებაში მივაკვლევდი ისეთ დოკუმენტს, რომელიც ნათელს მოჰყენდა ვ. თანიანის მიერ კომპიუტერულ სისტემაში შეღწევისთვის საჭირო პაროლის მოპოვების და უშუალოდ შეღწევის განხორციელების ხერხს. იმ მასალაში, რომელიც სასამართლოს მიერ იქნა წარმოდგენილი, მსგავსი დოკუმენტი არ აღმოჩნდა.

ამდენად, ამ კაზუსიდან გამომდინარე, რთულია ვისაუბროთ დანაშაულის ჩადენის ხერხზე. თუმცა, გარკვეული ვარაუდის გამოთქმა მაინც შესაძლებელია. განაჩენიდან თვალნათლივ ჩანს, რომ ყველა იმ მომხმარებლის პაროლი, რომელიც მოიპოვა ვ. თანიანმა იყო უმარტივესი. დაახლოებით ესეთი ტიპის: „12345“, ან მაგალითად, თუ მომხმარებლის ინტერნეტ-საიტზე გამოყენებული სახელი (Username) იყო: „რაინდი“, პაროლი შესაბამისად, „რაინდ“ და ა.შ. ეს მაძლევს ვარაუდის საფუძველს, რომ ვ. თანიანი, შესაძლოა არც იყენებდა რაიმე სპეციალურ პროგრამულ უზრუნველყოფას ამ პაროლების მოსაპოვებლად და დამოუკიდებლად, ფანტაზიის დახმარებით, სხვადასხვა ვერსიის მოსინჯვის გზით ადგენდა ამ მონაცემებს. სავარაუდოა, რომ ვ. თანიანმა რაიმე დამხმარე პროგრამაც გამოიყენა. მაგალითად, ზემოთგანხილული პაროლის მოსარგები სპეციალური პროგრამები, რომელიც მარტივ, ანუ არაკომბინირებულ პაროლს მოკლე დროში გამოიცნობს.⁷¹

საინტერესოა, მიზეზშედეგობრივი კავშირის საკითხის განხილვა ზემოთმოყვანილ ორივე კაზუსის მაგალითზე. პირველი ეხებოდა 2004 წლის 19 მაისის განაჩენს. კერძოდ, სასამართლოს განაჩენში ნათქვამი იყო, რომ „საქართველოს მოქალაქეებმა ბ. სალაძემ და ზ. მანასიანმა და ისრაელის მოქალაქე ლ. ინაევმა სხვა დაუდგენელი პირების ხელშეწყობით მოახერხეს კანონით დაცულ კომპიუტერულ ინფორმაციაში შეღწევა და ქსელში ასახული უცხოეთის რიგი დანესებულილებების საბანკო საიდუმლოების შემცველი მონაცემების მოპოვება.“

პირადად ვესწრებოდი სასამართლოში ზემოაღნიშნული საქმის განხილვას, შემდეგ კი სრულად გავეცანი მრავალტომიან საქმეს.

71 კომბინირებული პაროლი შედგება როგორც ლათინური ასოებისგან, ასევე ციფრებისგან და არის 6-7 სიმბოლოზე მეტი, არაკომბინირებულ პაროლში, ანუ მარტივში უნდა მოვიხაზოთ მხოლოდ ციფრებისგან, ან მხოლოდ ასოებისგან შემდგარი კოდები. მათი სიმბოლოების რაოდენობა ექვსს არ აღემატება.

თუმცა საქმის მასალებში კონკრეტული მტკიცებულება, რომელიც დაადასტურებს თუ უშუალოდ ვინ, რა ხერხით და როდის განახორციელა შეღწევა საერთოდ არ მოიპოვება (იხ. საქმე №1/ა-74, 2004 წლის 19 მაისის განაჩენი). ამიტომ ჩემთვის გაუგებარია, რა ლოგიკით იხელმძღვანელა სასამართლომ და მის პოზიციას ვერ გავიზიარებ.

სასამართლომ ჩათვალა, რომ მიზეზშედეგობრივი კავშირი არსებობდა დაზარალებული მოქალაქეების საბანკო ბარათების მონაცემების გამოყენებასა და კანონით დაცულ ინფორმაციაში უნებართვო შეღწევას შორის, რაც უცნაურია, რადგან რთული წარმოსადგენი არ უნდა იყოს, რომ ის ადამიანები ვინც კომპიუტერის სახლში დასამონტაჟებლად ქირობენ კომპიუტერის სპეციალისტს (აღნიშნული საქმის მასალებიდან ირკვევა და ნაშრომში ზემოთაც არის მოხსენიებული), ვერ შეაღწევდნენ ამერიკაში ერთ-ერთი სერიოზული კომპანიის კომპიუტერულ სისტემაში. ყოველ შემთხვევაში, თუ ეს ქმედება ნამდვილად მათ ჩაიდინეს სასამართლო ვალდებული იყო მიეთითებინა თუნდაც ერთ მტკიცებულებაზე. მაშინ, როცა დამნაშავეებს შეეძლოთ, კომპიუტერულ ინფორმაციაში შეღწევის გარეშე, უკვე მოპარული მონაცემების ყიდვა და შემდგომ მათი გამოყენება.

თ. წერეთელი მიიჩნევს, რომ „ადამიანის ქცევა მაშინ უნდა ჩაითვალოს საზოგადოებრივად საშიში შედეგის აუცილებელ პირობად, როდესაც ქმედების გარეშე შედეგი არ განხორციელდებოდა, ხოლო იმის დასადგენად, განხორციელდებოდა თუ არა საზოგადოებრივად საშიში შედეგი მოქმედების გარეშე, შეიძლება გამოვიყენოთ ქმედების აზრობრივი გამორიცხვის მეთოდი, ე.ი. ჩვენს წარმოდგენაში დაეუშვათ, რომ ეს ქმედება ადამიანს არ ჩაუდენია. თუ ასეთი აზრობრივი გამორიცხვისას აღმოჩნდება, რომ შედეგი მაინც დადგებოდა, თანაც დადგებოდა სწორედ ამ დროს და ამ სახით, როგორც იგი სინამდვილეში განხორციელდა, ეს იმას ნიშნავს, რომ ადამიანის ქმედება არ ყოფილა მიზეზშედეგობრივ კავშირში შედეგთან“.⁷²

72 იხ. თ. წერეთელი, „სისხლის სამართლის პრობლემები“, I ტომი, გამომც. „მერიდიანი“, თბ. 2007წ. გვ. 241

მიზეზშედგებორივი კავშირი არსებობს მაშინ, როდესაც ქმედება წარმოადგენდა კოდექსის შესაბამისი მუხლით გათვალისწინებული მართლსაწინააღმდეგო შედეგის ან კონკრეტული საფრთხის აუცილებელ პირობას, ურომლისოდაც ეს შედეგი არ დადგებოდა.

მოცემული მსჯელობიდან გამომდინარე, დამნაშავეების ქმედება, ანუ საბანკო ბარათის მონაცემების გამოყენებით მოქალაქეების თანხების მისაკუთრებისთვის არანაირ აუცილებელ პირობას არ წარმოადგენდა კანონით დაცულ ინფორმაციაში უნებართვო შეღწევა, რადგან დამნაშავეებს უპრობლემოდ შეეძლოთ უკვე მოპოვებული ინფორმაციის შეძენა იმ პირებისგან, ვინც განახორციელა უცხოეთის საბანკო დანესებულების კანონით დაცულ ინფორმაციაში შეღწევა ან თუნდაც ამავე საბანკო დანესებულების იმ თანამშრომლისგან ყიდვა, ვისაც ხელი მიუწვდებოდა ამ ინფორმაციაზე.

საგულისხმოა, ის გარემოებაც, რომ განაჩენის დადგენის დროს მოქმედებდა სისხლის სამართლის კოდექსის ძველი რედაქცია, მაშინდელი 284-ე მუხლი კი მატერიალური შემადგენლობის იყო და კანონმდებელი სისხლისსამართლებრივ პასუხისმგებლობას უკავშირებდა კონკრეტულ შედეგს. განხილული კაზუსის შემთხვევაში კი ეს იქნებოდა „კანონით დაცულ კომპიუტერულ ინფორმაციასთან არამართლზომიერი შეღწევა, რამაც ინფორმაციის მოპოვება გამოინვია.“

ამდენად, იმ ფონზე, რომ საქმეში ერთი მტკიცებულებაც არ იყო იმის შესახებ, თუ უშუალოდ ვინ, სად და როდის განახორციელა კანონით დაცულ ინფორმაციაში შეღწევა, მიმაჩნია, რომ დამნაშავეების ქმედებასა და დამდგარ შედეგს შორის მიზეზშედგებორივი კავშირი არ არსებობდა, ანუ სახეზე არ იყო 284-ე მუხლით გათვალისწინებული კიბერდანაშაული და ქმედება უნდა დაკვალიფიკირებულიყო მხოლოდ 180-ე, 202-ე, 210-ე, 362-ე მუხლებით. აღნიშნული კვალიფიკაციას ვერ შეცვლიდა ვერც ის გარემოება, რომ უცხოეთის საბანკო დანესებულების კანონით დაცული ინფორმაცია დამნაშავეების მიერ შეძენილ იქნა, რადგან სისხლის სამართლის კოდექსის ძველი რედაქციით არც ეს ქმედება წარმოადგენდა კიბერდანაშაულს.

რაც შეეხება მეორე კაზუსს, რომელიც ზემოთ უკვე იქნა განხილული: სასამართლოს განაჩენით დადგინდა, რომ ვ.თანიაშმა შეაღ-

ნია კომპიუტერულ სისტემაში და მიითვისა ინტერნეტ-ტოტალიზატორის მომხმარებლების ფულადი სახსრები. ვინაიდან, ვ. თანიანი ამ ქმედებას, კერძოდ, უცხო პირის პირად ანგარიშზე არსებულ თანხას კომპიუტერულ სისტემაში უნებართვო შეღწევის გარეშე ფიზიკურად ვერ განახორციელებდა, მიზეზმდეგობრივი კავშირის არსებობა ეჭვს არ იწვევს.

სისხლის სამართლის კოდექსის ახალი რედაქციის მიღების შემდეგაც, განსჯის საგნად რჩება საკითხი, რომელიც აქტუალური იყო კოდექსის ძველი რედაქციის არსებობის პერიოდშიც. კერძოდ, თუ უფლებამოსილი პირი შევა კომპიუტერულ სისტემაში მაშინ როგორ უნდა დავაკვალიფიციროთ მისი ქმედება? ასეთ შემთხვევაში, სახეზე საერთოდ არ გვექნება დანაშაული, რადგან ამგვარ ქმედებას სისხლის სამართლის კოდექსის არც ერთი მუხლი ითვალისწინებს!

საინტერესოა, წარმოვიდგინოთ შემდეგი სიტუაცია: „საგადასახადო საიდუმლოების შემცველი ინფორმაციის შენახვის რეჟიმის და დაშვების ნესის შესახებ ინსტრუქციის დამტკიცების თაობაზე“ საქართველოს ფინანსთა მინისტრის 2005 წლის 4 მაისის ბრძანებით, საიდუმლო ინფორმაციის დასამუშავებლად კომპიუტერული ტექნიკის გამოყენებისას იქმნება საიდუმლო ინფორმაციის დაცვის სისტემა და ფინანსთა სამინისტროს სისტემის თანამშრომლებისთვის მასთან დაშვება ხდება სპეციალური ნებართვის საფუძველზე. აღნიშნული ნებართვის მფლობელის მიერ ასეთი ინფორმაციის გაცნობა არ ჩაითვლება არც არამართლზომიერ და არც უნებართვო შეღწევად და შესაბამისად, მის მიერ გადამხდელის შესახებ არსებული მონაცემების განადგურება ან სხვა მოქმედება სისხლის სამართლის კოდექსის არც ძველი და არც ახალი რედაქციით არ დაკვალიფიცირდება, როგორც საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლით გათვალისწინებული დანაშაულებრივი ქმედება. შეგვიძლია ვივარაუდოთ, რომ ასეთ შემთხვევაში თუ სახეზე გვექნება რაიმე ზიანი, რომელიც მიადგა კომპიუტერულ მონაცემს ან შეფერხდა კომპიუტერული სისტემის ფუნქციონირება, პირი დაისჯება საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლის 1-ლი ან მე-2 ნაწილით და არა 284-ე მუხლით.

ჩემი აზრით, უმჯობესი იქნებოდა გაგვეზიარებინა აშშ-ს და უნგრეთის კანონმდებელთა მიდგომა. კომპიუტერულ სისტემაში

მართლზომიერი შესვლის ფარგლების გადამეტების შედეგად დამდგარი უკანონო შედეგისთვის პასუხისმგებლობას ცალკე შემადგენლობად ითვალისწინებს აშშ-ს კანონთა კრებულის მე-18 ტიტულის 1030-ე მუხლი⁷³ და ასევე, უნგრეთის სისხლის სამართლის კოდექსის 300/C-ე მუხლი⁷⁴, რომლის შესაბამისადაც ნებისმიერი პირი, რომელიც კომპიუტერის დამცავი სისტემის ან მოწყობილობის შეცდომაში შეყვანით უკანონოდ შეაღწევს კომპიუტერულ სისტემაში ან ქსელში ან/და გადააჭარბებს თავისი, როგორც მომხმარებლის დაშვების ფარგლებს, პასუხს აგებს სისხლის სამართლის ნესით.

ვიზიარებ აშშ-ს და უნგრეთის მიდგომას ამ საკითხზე და მიმაჩნია, რომ სასურველია, 284-ე მუხლის შენიშვნაში მიეთითოს: „კომპიუტერულ სისტემაში უნებართვო შეღწევად განიხილება, კომპიუტერულ სისტემაში შესვლის უფლებამოსილების ბოროტად გამოყენება“. ამ ჩანაწერის ქართულ სისხლის სამართლის კოდექსში შეტანა, ჩემი აზრით, გამორიცხავს ბუნდოვანებას. კერძოდ, ცალსახა გახდება, რომ კომპიუტერულ სისტემაში შესვლის უფლებამოსილების გადამეტება ისეთივე დანაშაულია, როგორიც კომპიუტერულ სისტემაში უნებართვო შეღწევა.

დასკვნის სახით, შეიძლება ითქვას, რომ კომპიუტერულ სისტემაში უნებართვო შეღწევაა არაკეთილსინდისიერი მიზნით განხორციელებული ისეთ მოქმედება, რომელიც ეწინააღმდეგება კომპიუტერული სისტემის მფლობელის ნებას და იწვევს კომპიუტერული სისტემის ინტეგრირებულობის და კონფიდენციალურობის დარღვევას.

73 იხ. U.S. Code, Title 18, part I, Chapter 47, § 1030, Fraud and related activity in connection with computers (<http://www.law.cornell.edu/uscode/18/1030.html>).

74 იხ. <http://www.cybercrimelaw.net/Hungary.html>

3. 285-ე მუხლით გათვალისწინებული დანაშაულის ობიექტური შემადგენლობა

საქართველოს სისხლის სამართლის კოდექსის 285-ე მუხლის დისპოზიცია შემდეგნაირადაა ჩამოყალიბებული:

„კომპიუტერული პროგრამის ან/და სხვა მონყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეღწევისთვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ამ თავითა და ამ კოდექსის 158-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის მიზნით“.

ვეთანხმები გ. მამულაშვილის პოზიციას, რომლის მიხედვითაც მოცემული ნორმით დაცულ ინტერესს ანუ ხელყოფის ობიექტს წარმოადგენს კომპიუტერული სისტემის ან მისი მონაცემების კონფიდენციალურობა, ინტეგრირებულობა, ხელმისაწვდომობა⁷⁵.

თ. წერეთლის და გ. ტყეშელიაძის აზრით, ზოგიერთი დანაშაულის შემადგენლობა გულისხმობს ხელყოფას ორ ან მეტ უშუალო ობიექტზე. ამასთან ეს ობიექტები შეიძლება სხვადასხვაგვაროვანნი იყვნენ⁷⁶.

საინტერესოა, ასეთი ერთზე მეტ ობიექტიანი დანაშაული ხომ არაა 285-ე მუხლით გათვალისწინებული ქმედება? კომპიუტერული სისტემის, მონყობილობის და მონაცემის უსაფრთხოება, კონფიდენციალურობა და ხელმისაწვდომობა უკვე აღვნიშნეთ. განხილული ქმედებით შესაძლოა მოხდეს იმ კომპიუტერული სისტემის, პროგრამის ან სხვა მონყობილობის მესაკუთრის ინტერესის ხელყოფა, რომლის კომპიუტერულ პროგრამაში, მონყობილობაში ან კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის უზრუნველყოფაც ხორციელდება, რადგან ამ ქმედებით იქმნება რეალური

75 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი II, გამოც. „მერიდიანი“, თბ. 2012წ. გვ.40

76 იხ. თ. წერეთელი, გ. ტყეშელიაძე, „მოძღვრება დანაშაულზე“, გამოც. „მეცნიერება“, თბ. 1969წ. გვ. 156

საფრთხე, რომ განხორციელდება კომპიუტერულ სისტემაში უნებართვო შეღწევა ან კერძო კომუნიკაციის საიდუმლოების დარღვევა და შეილახება ამ მონაცემის მესაკუთრის ინტერესები. ხელყოფის ობიექტი რიგ შემთხვევაში შესაძლოა იყოს რეპუტაცია.

ვინაიდან, 285-ე მუხლში კანონმდებელი აკეთებს დათქმას სისხლის სამართლის კოდექსის 158-ე მუხლზე და ამბობს, რომ თუ დამნაშავის ქმედება, გათვალისწინებული 285-ე მუხლის პირველი ნაწილით მიზნად ისახავს კერძო კომუნიკაციის საიდუმლოების დარღვევას კომპიუტერის გამოყენებით, მაშინ ეს ქმედება ჩაითვლება კომპიუტერული მონაცემის და კომპიუტერული სისტემის უკანონო გამოყენებად. ამ შემთხვევაში, კერძო კომუნიკაციის საიდუმლოებაზე უფლება შეგვიძლია განვიხილოთ როგორც დამატებითი ობიექტი.

ვეცდები, დავასაბუთო ჩემი პოზიცია.

მაგალითად, როცა დამნაშავე დაამზადებს ინტერნეტ-მალაზიის დუბლიკატს, იგი არ ხელყოფს აღნიშნული ინტერნეტ-მალაზიის ორიგინალური ვერსიის კომპიუტერული სისტემის და მონაცემის კონფიდენციალურობას, ინტეგრირებულობას და ხელმისაწვდომობას, მაგრამ საფრთხეს უქმნის მის რეპუტაციას და მესაკუთრის ფინანსურ ინტერესს.

განვიხილოთ უფრო დეტალურად: ინტერნეტ-მალაზიის დუბლიკატის გაკეთებით დამნაშავე ქმნის სრულიად დამოუკიდებელ კომპიუტერულ მონაცემს, რომელიც ადამიანის ვიზუალური აღქმით ძნელად გაირჩევა ორიგინალისგან. სწორედ, ადამიანის აღქმის უნარზე გავლენით ახერხებს დამნაშავე მიიღოს მისი პირადი მონაცემი, რომელიც საჭიროა ამ ინტერნეტ-მალაზიის კომპიუტერულ სისტემაში შესასვლელად. ხაზგასმით უნდა აღინიშნოს, რომ ინტერნეტ-მალაზიაში დამნაშავის შესვლა არ ლახავს ამ უკანასკნელის კონფიდენციალურობას, რადგან ამ მოქმედებით ხდება არა მალაზიის კომპიუტერული სისტემის, არამედ მისი რეგისტრირებული მომხმარებლის საიდუმლო მონაცემში შესვლა, რადგან ინტერნეტ-მალაზია არის ვირტუალური დანესებულება, სადაც შესვლა შეუძლია ნებისმიერს, ვისაც ინტერნეტი აქვს. თუმცა კონკრეტული შესყიდვის ოპერაციას ახორციელებს ის პირი, ვინც რეგისტრირებულია მომხმარებლად და გახსნილი აქვს საკუთარი ანგარიში. პირად

ანგარიშში შესასვლელი პაროლის უსაფრთხოების დაცვა კი პირველ რიგში, მომხმარებლის ვალდებულებაა.

ნარმოვიდგინოთ ასეთი შემთხვევა: შემნახველი საკანი განთავსებულია ცენტრალური ფოსტის შენობაში. მოქ. ა. ნაზლაიძემ დაიქირავა ერთ-ერთი საკანი ფულის და ძვირფასეულობის დროებით შესანახად, თვითონ კი გაეშურა ქალაქის დასათვალიერებლად. გზაში ჯიბის ქურდმა ამოაცალა საკნის გასაღები. მოგვიანებით, ა. ნაზლაიძე დაბრუნდა ფოსტის შენობაში და შემნახველი საკნების ზედამხედველს მოუყვა მომხდარის შესახებ. ზედამხედველმა სარეზერვო გასაღებით გახსნა საკანი და აღმოჩნდა, რომ ის გაექურდათ. თუმცა, არანაირი ძალადობის კვალი არ ჩანდა. მოგვიანებით კრიმინალისტებმა დაასკვნეს, რომ ქურდობა სწორედ იმ გასაღების გამოყენებით მოხდა, რომელიც ა. ნაზლაიძემ დაკარგა.

რა დანაშაულთან გვაქვს საქმე? ესაა ა. ნაზლაიძის გაქურდვა თუ ცენტრალური ფოსტის შენობაში უნებართვო შესვლა? ცენტრალურ ფოსტაში, ისევე, როგორც ინტერნეტ-მალაზიაში შესვლა საჯაროა. ამდენად, სახეზე გვაქვს, ა. ნაზლაიძის გაქურდვის ფაქტი.

უნდა აღინიშნოს კიდევ ერთი გარემოება. ინტერნეტ-მალაზიაში გახსნილი ანგარიშით სარგებლობა აკრძალული არავისთვის არაა. მაგალითად, მის მფლობელს შეუძლია ის დაუთმოს თანამშრომელს, მეგობარს და ა.შ. ინტერნეტ-მალაზია მხოლოდ მომხმარებლის სახელის და პაროლის იდენტიფიკაციას ახდენს. ვინ იყენებს მას, ეს მეორე ხარისხოვანია. მაგალითად, ბ. სურმავეს ანგარიში გახსნილი ჰქონდა ინტერნეტ-მალაზია „სიტი კოლორში“. მას მეგობარმა ა. ლანჩავამ სთხოვა მისი ანგარიშიდან კაბის ყიდვა. ბ. სურმავე დათანხმდა და მისცა საკუთარი ანგარიშის პაროლი. ა. ლანჩავამ ისარგებლა ბ. სურმავეს ანგარიშით და შეიძინა კაბა.

ამის პარალელურად, ბ. სურმავეს ყოფილმა მეუღლე ნ. ნოდიაშვილმა დაამზადა „სიტი კოლორის“ დუბლიკატი, რათა მოეპოვებინა ყოფილი ცოლის პირადი ანგარიშის მონაცემები და შემდეგ მიეყენებინა მისთვის ქონებრივი ზიანი. მართლაც, ნ. ნოდიაშვილმა აღასრულა განზრახვა, მოიპოვა ყოფილი მეუღლის მონაცემი, რომლის გამოყენებითაც დაამზადა ყალბი საკრედიტო ბარათი და მოხსნა მასზე არსებული ფული.

ისმის კითხვა, რომელი ქმედებით მოხდა „სიტი კოლორის“ კონფიდენციალურობის, ინტეგრირებულობის და ხელმისაწვდომობის ხელყოფა? ჩემი აზრით, არც ერთით. თუმცა, სახეზე გვაქვს ბ. სურმავეას კომპიუტერული მონაცემის კონფიდენციალურობის დარღვევა. ამავე დროს ბ. სურმავეას პირადი ანგარიშის მონაცემის მოპარვის ფაქტი საფრთხეს უქმნის „სიტი კოლორის“ რეპუტაციას, რადგან სხვა მომხმარებლები ეჭვს შეიტანენ მის დაცულობაში, რაც საბოლოო ჯამში დააზიანებს ინტერნეტ-მაღაზიის რეპუტაციას და შესაბამისად, ფინანსურ ინტერესსაც.

ჩემს პოზიციას ამყარებს ლ. სურგულაძის მოსაზრება დანაშაულის ობიექტთან დაკავშირებით, რომლის მიხედვითაც: „ყოველ დანაშაულს ვნება მოაქვს ამა თუ იმ სიკეთისთვის. ის, რაც ვნებას განიცდის დანაშაულისგან, ან რასაც ვნების მიყენების საფრთხე ემუქრება, დანაშაულის ობიექტის სახელწოდებით არის ცნობილი“.⁷⁷ ამრიგად, დანაშაულის ობიექტი არის ისიც, რაც ხელყოფის საფრთხეს განიცდის. ჩემს მიერ ზემოთნახსენები დანაშაულის თითოეული ობიექტი 285-ე მუხლით გათვალისწინებული ქმედების ჩადენისას განიცდის როგორც ხელყოფას, ასევე შესაძლებელია შეექმნას ხელყოფის საფრთხე. ამიტომ მიმაჩნია, რომ 285-ე მუხლით გათვალისწინებული ქმედებას შეიძლება ჰქონდეს ერთზე მეტი ხელყოფის ობიექტი ანუ კომპიუტერული სისტემის ან მისი მონაცემების კონფიდენციალურობის, ინტეგრირებულობის, და ხელმისაწვდომობის პარალელურად, დანაშაულმა შესაძლოა ხელყოს ამ კომპიუტერული სისტემის მესაკუთრის რეპუტაცია და ფინანსური ინტერესი.

საქართველოს სისხლის სამართლის კოდექსის 285-ე მუხლის 1-ლი ნაწილით გათვალისწინებული დანაშაულის საგანია ის კომპიუტერული სისტემა და მონაცემი, რომლის ხელყოფის მიზნითაც იქმნება კომპიუტერული პროგრამა, მოწყობილობა და უნებართვო შეღწევისთვის საჭირო პაროლი, დაშვების კოდი ან სხვა მსგავსი მონაცემი.

285-ე მუხლით გათვალისწინებული ქმედების ობიექტური მხარე მრავალფეროვანია.

77 იხ. ლ. სურგულაძე, „სისხლის სამართალი“, გამომც. „ქრონოგრაფი“, თბ. 1997წ. გვ. 81

ევროპის ყველა ქვეყანამ, რომელმაც განახორციელა „კიბერ-დანაშაულის შესახებ“ კონვენციის რატიფიცირება, კანონმდებლობაში მოახდინა კონვენციის მე-6 მუხლის ინტეგრირება. აღნიშნული მუხლის მიხედვით, დანაშაულია იმ მოწყობილობის და კომპიუტერული პროგრამის, კომპიუტერული პაროლის, დაშვების კოდის ან მსგავსი მონაცემის (რომელთა მეშვეობითაც შესაძლებელია მთლიან კომპიუტერულ სისტემაში ან მის ნაწილში შეღწევა) წარმოება, გაციფვა, გამოსაყენებლად შეძენა/მიწოდება, გავრცელება, იმპორტი ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა, რომელთა გამოყენებითაც ხდება კონვენციის მე-2, მე-3, მე-4 და მე-5 მუხლით გათვალისწინებული დანაშაულების ჩადენა-განხორციელება. ამ მუხლებში მითითებულია კომპიუტერულ სისტემაში ან მის ნაწილში უნებართვო შეღწევა, კომპიუტერული სისტემისთვის, სისტემიდან ან მის ფარგლებში მონაცემთა გადაცემის უნებართვოდ ხელში ჩაგდება, კომპიუტერულ მონაცემთა დაზიანება, წაშლა, გაუარესება, შეცვლა ან დაფარვა და ნებართვის გარეშე კომპიუტერული სისტემის ფუნქციონირების არსებითი შეფერხება კომპიუტერულ მონაცემთა შეყვანის, გადაცემის, დაზიანების, წაშლის, დაფარვის გზით.

საინტერესოა, რომ ევროპის საბჭოს კონვენციის მე-6 მუხლით დადგენილი შემადგენლობის სისხლის სამართლის კანონში ასახვა გაერთიანებულმა სამეფომ კონვენციის რატიფიცირებამდე ბევრად ადრე განახორციელა⁷⁸.

აღსანიშნავია, რომ უნგრეთმა გერმანიის, ნიდერლანდების, საფრანგეთის, ხორვატიის და ზოგიერთი სხვა ქვეყნის კანონმდებლობისგან განსხვავებით ამ დანაშაულისთვის პასუხისმგებლობა გაყო ორ ნაწილად. პირველ შემთხვევაში დასჯადად გამოცხადდა ისეთი კომპიუტერული პროგრამის, პაროლის, შესვლის კოდის ან სხვა

78 გაერთიანებულმა სამეფომ ევროპის საბჭოს კონვენციის რატიფიცირება მხოლოდ 2011 წლის 25 მაისს განახორციელა. კონვენციის მე-6 მუხლი დაემატა 2006 წელს „პოლიციისა და მართლსაჯულების შესახებ“ (The Police and Justice Act) კანონის XVIII თავს და ამოქმედდა 2008 წლიდან. უნდა ითქვას, რომ ანდორამ, მონაკომ და ზოგიერთმა სხვა სახელმწიფომ „კიბერდანაშაულის შესახებ“ კონვენციას ხელი არ მოაწერა, თუმცა დაადგინა პასუხისმგებლობა იმ ქმედებისთვის, რომელიც გათვალისწინებულია ევროპის საბჭოს კონვენციის მე-6 მუხლით (იხ. <http://www.cybercrimelaw.net/UK.html>).

მონაცემის დამზადება, მოპოვება, გავრცელება, სავაჭროდ გატანა ან კიდევ სხვაგვარი ხელმისაწვდომობა, რომლის საშუალებითაც სხვა პირი უნებართვოდ შეაღწევს კომპიუტერულ სისტემაში ან ქსელში (უნგრეთის კოდექსის 300/E-ე მუხლი)⁷⁹. მეორე შემთხვევაში კი დასჯადია დანაშაულებრივი ქმედების ჩასადენად სხვა პირისთვის თავისი ეკონომიკური, ტექნიკური ან/და სხვაგვარი ცოდნის გადაცემა იმ კომპიუტერული პროგრამის, პაროლის, შესვლის კოდის ან სხვა ინფორმაციის შესაქმნელად, რომლებიც განკუთვნილია კომპიუტერულ სისტემაში ან ქსელში უნებართვო შეღწევისთვის.

ეს უკანასკნელი თეზისი ძალიან მნიშვნელოვანია და მასში უნდა ვიგულისხმოთ ის ინტერნეტ-საიტები, ბეჭდვითი გამოცემები და სხვა საინფორმაციო საშუალებები, რომლებიც პოპულარიზაციას უწევენ ე.წ. „ჰაკერულ“ პროგრამებს. ხშირია შემთხვევა, როცა ამგვარ საინფორმაციო საშუალების გზით ვრცელდება ინსტრუქცია, როგორ უნდა განხორციელდეს, მაგალითად, ელექტრონულ ფოსტაში უსებართვო შეღწევა. მსგავსი ქმედების მიზანი შესაძლოა არც იყოს რომელიმე კონკრეტულ კომპიუტერულ სისტემაში უნებართვო შეღწევა და ატარებდეს ზოგად ხასიათს. ამდენად, ცალსახად დანაშაულზე საუბარი რთულია, მაგრამ, ჩემი აზრით, სახელმწიფო ვალდებულია გააკონტროლოს მსგავსი ინტერნეტ-საინფორმაციო რესურსები, რადგან მათი მომხმარებლები ძირითადად არიან არასრულწლოვნები და ისინი, ვინაიდან კომპიუტერული დანაშაულის ჩადენასთან დაკავშირებული ინსტრუქცია საჯაროდ ხელმისაწვდომია ვერ აცნობიერებენ საკუთარი ქმედების მართლსაწინააღმდეგო შინაარსს.

285-ე მუხლში კანონმდებელმა კონვენციიდან არ გადმოიტანა რიგი ტერმინები. მაგალითად, კონვენციაში მითითებულია: ნარმოება, გაყიდვა, გამოსაყენებლად შეძენა/მინოდება, გავრცელება, იმპორტი და ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა. ქართველმა კანონმდებელმა კი მუხლში ჩანერა შემდეგნაირად: დამზადება, შენახვა, გაყიდვა, გავრცელება და ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა. თვალსაჩინოა, რომ ქართულ ენაში ტერმინები „მინოდება“ და „იმპორტი“ ექცევიან ტერმინი „გავრცე-

79 იხ. <http://www.cybercrimelaw.net/Hungary.html>

ლების“ განმარტების ქვეშ. გარდა ამისა, ქართველმა კანონმდებელმა 285-ე მუხლის დისპოზიციას დაამატა ტერმინი „შენახვა“, რაც კონვენციაში საერთოდ არ წერია. აღსანიშნავია, რომ ტერმინი „შეძენა“ 285-ე მუხლში არ ჩაიწერა, რასაც არ ვეთანხმები, რადგან არსებული ტერმინები მის შინაარსს არ მოიცავენ. ქართული კახონ-მდებლის მიდგომას დანარჩენ ტერმინებთან დაკავშირებით სრულად ვიზიარებ.

მოცემულ კომპიუტერულ დანაშაულთან დაკავშირებით ძალიან მნიშვნელოვანია ისეთი ტექნიკური და პროგრამული ინსტრუმენტების ხელმისაწვდომობა, რომლებიც გამოიყენება დანაშაულის ჩადენის მიზნით. ასეთი მოწყობილობის უმეტესობა ხელმისაწვდომი, უფასო და ადვილად დასამუშავებელია და მათი გამოყენება შეუძლიათ სპეციალური ცოდნის არმქონე ადამიანებსაც. კომპიუტერული სისტემის სპეციალური პროგრამის გამოყენებით შესაძლოა უკაბელო ქსელით კომუნიკაციის გადაცემის ხელში ჩაგდება, ან ღია უკაბელო ქსელის აღმოჩენა, დაშიფრული ფაილების გაშიფვრა და კიბერშეტევები. ასეთი დანაშაულის ჩადენისთვის, გარდა სპეციალური პროგრამისა, საჭიროა სათანადო მოწყობილობის შეძენაც. ამისთვის არსებობს ე.წ. „შავი ბაზარი“, სადაც ხდება მათი წარმოება და გასაღება. გარდა ამისა, ხშირია კოდური სიტყვების გაცვლაც, რაც საშუალებას აძლევს დამნაშავეს განახორციელოს კომპიუტერულ სისტემაში უნებართვო შეღწევა.⁸⁰

განვიხილოთ უფრო დეტალურად:

კომპიუტერული პროგრამა არის ბრძანებათა თანმიმდევრობა, რომელიც უზრუნველყოფს კომპიუტერში დავალების შესრულებისთვის საჭირო ოპერაციათა განხორციელების რიგს. კომპიუტერული პროგრამის განმარტებას ვხვდებით „საავტორო და მომიჯნავე უფლებების შესახებ“ საქართველოს კანონის მე-4 მუხლის „კ“ ქვეპუნქტში: „კომპიუტერული პროგრამა – ინსტრუქციითა ერთობლიობა, სიტყვების, კოდების ან მანქანით (იგულისხმება კომპიუტერი – ავტ.) ნაკითხვადი სხვა ფორმით, რომელიც საშუალებას იძლევა

80 იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ: ტრენინგის სახელმძღვანელო“, ევროსაბჭო, სტრასბურგი, 2010წ. გვ. 57

აამოქმედოს კომპიუტერი განსაზღვრული შედეგების მისაღწევად."

უნდა აღინიშნოს, რომ თავად კომპიუტერული პროგრამები ერთმანეთისგან განსხვავდებიან დანიშნულებით, ფუნქციით და სპეციფიკური მახასიათებლებით. საინტერესოა, რომ კომპიუტერული პროგრამა უკავშირდება კომპიუტერული მონაცემის განმარტებასაც. ეს უკანასკნელი სწორედ კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით ინფორმაციის გამოსახვას და მათ შორის იმ პროგრამას გულისხმობს, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას.

ყველა პერსონალურ კომპიუტერს აერთიანებს ე.წ. პროგრამა „ბიოსი". იგი ენერგო დამოუკიდებელი მუდმივი მახსოვრობის მონყობილობაა. მასში ჩანერილია მონაცემთა მიღების და გაცემის, კომპიუტერის ელექტრო ქსელში ჩართვის და სხვა პორგრამები, რომელიც შეეხება ინფორმაციას კომპიუტერის აპარატული კონფიგურაციის შესახებ. უნდა აღინიშნოს ოპერაციულ სისტემა, რომელიც ასევე, კომპიუტერული პროგრამაა და მართავს სხვადასხვა სამომხმარებლო პროგრამულ პაკეტებს, ასევე კომპიუტერის სისტემის შემადგენელ მონყობილობებს და ამ სისტემის მომხმარებელს შორის ურთიერთობას. ანუ ოპერაციული სისტემა უნდა განვიხილოთ, როგორც შუამავალი კომპიუტერულ ტექნიკასა და ცალკეულ კომპიუტერულ პროგრამას შორის, რათა მომხმარებლისთვის შესაძლებელი გახდეს მისი ფუნქციონირება. ოპერაციული სისტემის კლასიკური მაგალითია ე.წ. „ვინდოუსი" (Windows). ოპერაციული სისტემაც კომპიუტერული სისტემის შემადგენელი ნაწილია და 285-ე მუხლში მითითებული „კომპიუტერული პროგრამა" მასში არ იგულისხმება. ოპერაციული სისტემა, როგორც აღვნიშნეთ, იძლევა კომპიუტერული სისტემის ფუნქციონირების და სხვა სპეციფიკური გამოყენებითი პროგრამების ადაპტირების საშუალებას. მაგალითად, ანტი-ვირუსული კომპიუტერული პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის და მათ შორის ე.წ. „ვინდოუსის" ოპერაციული სისტემის დაცვას. ამდენად, უნდა განვასხვაოთ სისტემური და გამოყენებითი პროგრამები. პირველი მათგანი საჭიროა ყველა კომპიუტერული სისტემის ფუნქციონირებისათვის, მეორე კი კონკრეტულ კომპიუტერულ სისტემას ანიჭებს დამატებით შესაძლებლობას. 285-ე მუხლში მითითებული კომპიუტერული პრო-

გრაძა უნდა გავიგოთ, როგორც გამოყენებითი კომპიუტერული პროგრამა, რომლითაც შესაძლებელია კოდექსის 35-ე თავით გათვალისწინებული კიბერდანაშაულის ჩადენა.

რაც შეეხება მონყობილობას, მასში უნდა მოვიაზროთ ის დამატებითი დეტალები, რომლებიც თუმცა არაა კომპიუტერული სისტემის შემადგენელ მექანიზმთა განუყოფელი ნაწილი, მაგრამ აღჭურვილია მათში ინტეგრირების უნარით.

სხვა მონყობილობაში უნდა ვიგულისხმოთ ისეთი ტიპის მექანიზმი, რომელიც მონაცემს ელექტრონულად ამუშავებს, გადასცემს, ინახავს, ინერს და ა.შ. ესეთია: ტელეფონის ავტომოპასუხე, ციფრული ვიდეო კამერა, ფაქსის აპარატი, პრინტერი, სკანერი, პეიჯერი, ჯიპიუსი (GPS), სატელიტური მონყობილობა და სხვ.

პაროლი, დაშვების კოდი, სხვა მსგავსი მონაცემი არის ის ინფორმაცია, სხვადასხვა სიმბოლოების, ანბანის ასოების ან ციფრების კომბინაცია, რომელიც გამოიყენება კომპიუტერული სისტემის ან მის ნაწილზე შესვლის უფლების მისაღებად.

რაც შეეხება ობიექტური მხარის ისეთ ნიშნებს, როგორიცაა კომპიუტერული პროგრამის, მონყობილობის, პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარ უზრუნველყოფა უნდა აღინიშნოს, რომ ეს არ გულისხმობს მხოლოდ მათ თავიდან დამზადებას. მასში იგულისხმება უკვე არსებული მონაცემის გაშიფვრაც. მაგალითად, თუ დამნაშავე სპეციალური პაროლის მოსარგები პროგრამის გამოყენებით მიიღებს კომპიუტერულ სისტემაში შეღწევისთვის საჭირო პაროლს, იგი ამ ქმედებით დაამზადებს არა ახალ, არამედ უკვე არსებულ პაროლს. ამის შემდეგ, მას შეუძლია დაამზადოს ახალი პაროლი ძველის შეცვლის გზით.

აღსანიშნავია, რომ ქართულ ენაში „დამზადება“ ცალსახად არ გულისხმობს ახლის შექმნას და ის შეიძლება ვიხმაროთ დუბლიკატის შექმნასთან დაკავშირებითაც. ამდენად, ტერმინში „დამზადება“ უნდა ვიგულისხმოთ, როგორც ახალი პროგრამის, მონყობილობის, პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, ასევე მათი დუბლიკატის დამზადებაც.

პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო შენახვა შეიძლება განხორციელდეს კომპიუტერული პრო-

გრამის საშუალებით, მაგალითად, ჩვეულებრივი ტექსტის შესანახი პროგრამა ე.წ. „მაიკროსოფტ ვორდით“ (Microsoft Word), აღნიშნული ფაილი კი, თავის მხრივ, შესაძლოა ჩანერილ იქნეს დისკზე ან/და შენახულ იქნეს კომპიუტერის მყარ დისკზე, ასევე, ტრადიციული გზით, მაგალითად, ჟურნალში, ბლოკნოტში და ა.შ. ჩანიშნით.

პროგრამის, მონყობილობის, პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო გაყიდვაში უნდა ვიგულისხმოთ გარკვეული თანხის სანაცვლოდ მათი გასხვისება.

პროგრამის, მონყობილობის, პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო გავრცელება არის ამ მონაცემების ნებისმიერი გზით გავრცელება. მაგალითად, სოციალური ქსელით გამოქვეყნება, ელექტრონული ფოსტით გადაცემა და ა.შ.

პაროლის უნებართვო გავრცელების მაგალითს უახლოესი ისტორიიდან მოვიყვან. 2000-2003 წლებში საქართველოში ინტერნეტით სარგებლობის დროის წინასწარი შეძენის სერვისი იყო პოპულარული. ამ დროს მომხმარებელს ინტერნეტით სარგებლობის მიზნით გადაეცემოდა სპეციალური პაროლი. დამნაშავე, რომელიც ახერხებდა პაროლის ხელში ჩაგდებას და მესაკუთრის ნების სანაღმდეგოდ ხარჯავდა მისი ინტერნეტით სარგებლობის დროს, გარკვეული პერიოდის შემდეგ ავრცელებდა ამ პაროლს სოციალური ქსელით და იგი ხელმისაწვდომი ხდებოდა ყველასთვის. ამით ხდებოდა დანაშაულებრივი კვალის დაფარვა. ის მომხმარებელი, რომელიც სოციალური ქსელის საშუალებით იღებდა ინტერნეტით სარგებლობის პაროლს და იყენებდა მას, გაუცნობიერებლად ხდებოდა დანაშაულის თანაამსრულებელი. იმ შემთხვევაში, თუ სამართალდამცავი ორგანო დააკავებდა მას, შესაძლოა ნამდვილ დამნაშავეს თავიდან აეცილებინა სისხლისსამართლებრივი პასუხისმგებლობა, რადგან მის კვალს ველარავინ მიაგნებდა. ამ მონაცემის გავრცელება შესაძლებელია ტრადიციული გზითაც. მაგალითად, ფოსტით გაგზავნით და ა.შ.

რაც შეეხება პროგრამის, მონყობილობის, პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის ხელმისაწვდომობის სხვაგვარი უზრუნველყოფაში უნდა ვიგულისხმოთ ნებისმიერი ის ხერხი, რომელითაც შესაძლებელია მათი კონკრეტული დანაშაულის ჩადენის მიზნით მიწოდება. კონვენცია ამ ტერმინის განმარტებას არ გვთავაზობს, ჩემი აზრით, კი ქართულ ენაში სიტყვა „გავრცელება“

იმდენად ყოვლისმომცველია, „ხელმისაწვდომობის სხვაგვარი უზრუნველყოფის“ მუხლში ჩანერა აუცილებლობას აღარ წარმოადგენდა, რადგან ამ ორ ტერმინს შორის არსებით შინაარსობრივ განსხვავებას ვერ ვხედავ.

285-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის სამუალებათა ის ტექნიკური და პროგრამული უზრუნველყოფა, რომლის დახმარებითაც ხორციელდება პროგრამის, მონაცემების, პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის დამზადება. ამავე დანაშაულის ჩადენის საშუალებათა ის კომპიუტერული პროგრამა, რომელის დახმარებითაც შესაძლებელია სხვადასხვა მონაცემის შენახვა, ასევე, სოციალური ქსელი და საკომუნიკაციო პროგრამა, რომლებიც გამოიყენება ინფორმაციის გადაცემა-გავრცელებისთვის.

285-ე მუხლით გათვალისწინებული დანაშაული, მაგავსად 284-ე მუხლისა. ფორმალური შემადგენლობისაა. ქმედების დანაშაულად კვალიფიკაციისთვის საკმარისია, კომპიუტერული პროგრამის ან/და სხვა მონაცემების, აგრეთვე კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადების, შენახვის, გაყიდვის, გავრცელების ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფის ფაქტის დადგენა. თუმცა, უნდა აღინიშნოს, რომ მსგავსად 284-ე მუხლისა, 285-ე მუხლის მე-2 ნაწილის „დ“ ქვეპუნქტიც მატერიალური შემადგენლობისაა, რადგან ის უკავშირდება კონკრეტულ შედეგს, კერძოდ 2000 ლარზე მეტი ოდენობის ზიანს.

საქართველოს სისხლის სამართლის კოდექსის 285-ე მუხლის ობიექტური შემადგენლობის უკეთ დახასიათებისთვის შესწავლილ იქნა სასამართლო პრაქტიკა. აღსანიშნავია, რომ 2010 წლიდან 2012 წლის 23 თებრვლამდე, სასამართლოს ამ მუხლით განხილული 3ქონდა მხოლოდ ერთადერთი საქმე. ამის მიზეზი ალბათ ისიცაა, რომ 285-ე მუხლით გათვალისწინებული ქმედება გულისხმობს მაღალი ტექნოლოგიების სფეროში ჰაკერების განათლების მაღალ დონეს. აქედან გამომდინარე, ამ ქმედების განხორციელება ყველასთვის შესაძლებელი არ არის. ჩემს მიერ სასამართლო პრაქტიკიდან მოპოვებულ იქნა ერთადერთი საქმე, რომელიც 285-ე მუხლით ჩადენილ დანაშაულს ეხება.

სასამართლოს განაჩენში⁸¹ ვკითხულობთ:

„აღ. მანიას ბრალი ედება მასში, რომ მან ჩაიდინა თაღლითობა ე.ი. მართლსაწინააღმდეგო მისაკუთრების მიზნით სხვისი ნივთის დაუფლება მოტყუებით, რამაც მნიშვნელოვანი ზიანი გამოიწვია;

მანვე ჩაიდინა კომპიუტერულ სისტემაში შეღწევისთვის საჭირო სხვა მსგავსი მონაცემების უნებართვო დამზადება, შენახვა და გავრცელება, ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა, კომპიუტერულ სისტემაში უნებართვოდ შეღწევის მიზნით.“

განაჩენის ეს ნაწილი იმ მიზნით მოვიყვანე, რომ ციტატის მეორე აბზაცი გაუგებარია. კერძოდ, რაში ედება ბრალი აღ. მანიას: კომპიუტერულ სისტემაში შეღწევისთვის საჭირო მონაცემის უნებართვო დამზადებაში, შენახვაში, გავრცელებაში თუ ხელმისაწვდომობის სხვაგვარ უზრუნველყოფაში? თუ ყველაფერში ერთად?

განაჩენი ამაზე პასუხს ბოლომდე არ იძლევა. თუმცა ეს არაა მისი პირველი და უკანასკნელი ბუნდოვანება. მივყვეთ თანმიმდევრულად:

განაჩენით ირკვევა, რომ ალექსანდრე მანიამ, რომელსაც დამთავრებული ჰქონდა ინფორმატიკის ფაკულტეტი და კარგად ფლობდა კომპიუტერს, ინტერნეტში მოიპოვა სათანადო ინფორმაცია და შეისწავლა ყალბი საიტების დამზადების წესი. მან ამ გზით შექმნა ინტერნეტ-საიტი „ფრანჩესკოს“ დუბლიკატი. ის მომხმარებელი, რომელიც შეეცდებოდა საიტზე შესვლას და შეიყვანდა საკუთარ პაროლს შესაბამის ველში, ამ მოქმედებით ინფორმაციას ავტომატურად გადაუგზავნიდა აღ. მანიას, თავად კი საიტზე ვერ შევიდოდა. ინტერნეტ-საიტის ორიგანალური ვერსიის მისამართი იყო www.franchesko.ge, ხოლო ყალბისა კი www.franchecko.ge.

აღ. მანია საიტის ყალბი ვერსიის მისამართს თავადვე ავრცელებდა ინტერნეტ-ფორუმზე და სოციალურ ქსელში. ამის შედეგად მან მოიპოვა ტოტალიზატორ „ფრანჩესკოს“ რეალური მომხმარებლის უამრავი მეტსახელი და კომპიუტერულ სისტემაში შეღწევის პაროლი. აღ. მანიამ შეარჩია მოქალაქე დ. სუტიკინის გვერდი, რომელიც ონლაინ-თამაშზე რეგისტრირებული იყო „სუტიკის“ მეტსახელით და

81 კახუსში დასახელებული ყველა თარიღი, ნომერი, დასახელება და პირის ვინაობა შეცვლილია.

პირად ანგარიშზე ჰქონდა ორიათას ორასი ლარი. ალ. მანიამ გად-
ანყვიტა მისი თანხის მითვისება და ამ მიზნით შეცვალა დ. სუტკი-
ნის გვერდის პაროლი. მოცემული მომენტიდან დ. სუტკინის გვერ-
დით სარგებლობა შეეძლო მხოლოდ მას, რადგან დ. სუტკინისთვის
შეცვლილი პაროლი უცნობი იყო.

შემდეგ ალ. მანია დაუკავშირდა ფართოდ გავრცელებულ საკო-
მუნიკაციო ქსელ „სკაიპით“ მოსარგებლე მეგობარ ელდარ დონაძეს
და სთხოვა დახმარება. მან მოატყუა ე. დონაძე, რომ თითქოს მას ჰქონ-
და ორი ანგარიში, მათ შორის ერთი „სუტკის“ მეტსახელით და სურდა
ამ ანგარიშიდან თანხის „მანიას“ მეტსახელით შექმნილ ანგარიშზე გა-
დატანა. ალ. მანიამ ე. დონაძეს მისცა დ. სუტკინის პაროლი და სთხოვა
თანხა ონლაინ-პოკერში თამაშის გზით მასთან წაეგო. ე. დონაძეს ეჭვი
არ შეჰპარვია ალ. მანიას ნათქვამში და დაეხმარა.

მიუხედავად ამისა, ალ. მანია თანხის განაღდებას მაინც ვერ
მოახერხებდა, რადგან „მანიას“ მეტსახელით ანგარიში ყალბი მონა-
ცემებით ჰქონდა შექმნილი. ამიტომ ის დაუკავშირდა მეგობარ მ.
ქარდავას და სთხოვა თანხის გადატანა მის ანგარიშზე შემდეგი ხერ-
ხით: ალ. მანია საკუთარი გვერდიდან ითამაშებდა ონლაინ-პოკერს მ.
ქარდავასთან და განზრახ წააგებდა. მ. ქარდავა დათანხმდა ალ. მა-
ნიას და შეთანხმებისამებრ, დ. სუტკინის ანგარიშიდან მითვისებული
ორი ათას ორასი ლარი ონლაინ-პოკერის თამაშის შედეგად გადავიდა
მ. ქარდავას ანგარიშზე. ამის შემდეგ ალ. მანია და მ. ქარდავა მიე-
იდნენ ინტერნეტ-ტოტალიზატორ „ფრანჩესკოში“ და მ. ქარდავას ან-
გარიშზე არსებული თანხა გაანაღდეს. ალ. მანიამ მ. ქარდავას განუ-
ული დახმარებისთვის გადასცა სამასი ლარი და დეტალურად მოუყვა
თუ როგორ დაამზადა ყალბი ინტერნეტ-საიტი, ხოლო შემდგომში
როგორ შეძლო ამ თანხის მითვისება.

სასამართლომ მ. ქარდავას ქმედება შეაფასა, როგორც მძიმე
დანაშაულის შესახებ შეუტყობინებლობა (დანაშაულის შეუტყობინებ-
ლობა, გათვალისწინებული სისხლის სამართლის კოდექსის 376-ე
მუხლით) და არა თანამონაწილეობა, რაშიც ეთანხმები, რადგან
მ. ქარდავას არ მიუღია მონაწილეობა ალ. მანიას მიერ განხორ-
ციელებულ დანაშაულში. კერძოდ, მ. ქარდავას არ ჩაუდენია არც
თაღლითობა და არც კომპიუტერულ სისტემაში შეღწევისთვის საჭი-
რო მონაცემის დამზადება, გავრცელება და ა.შ. როგორც საქმის

მასალებიდან ირკვევა, მ. ქარდავამ ალ. მანიას დანაშაულებრივი საქმიანობის შესახებ მხოლოდ უკანასკნელ მომენტში, ანუ თანხის გადაცემის მომენტში გაიგო, შესაბამისად, მისი თანამონაწილედ განხილვა არ იქნებოდა მართებული.

სასამართლოს მიერ გამოტანილ განაჩენში ვკითხულობთ: „ალ. მანიამ თაღლითური დაუფლების განზრახვით შექმნა და გაავრცელა ყალბი საიტი. ცრუ ინფორმაციას გამოეხმაურა დ. სუტკინი და ისე რომ ეჭვი არ შეჰპარვია ამ საიტის რეალურად არსებობაში, შევიდა ვებ-გვერდზე და ავტორიზაციის ველში მიუთითა ის ნიკი (ციტირებულია განაჩენიდან და იგულისხმება მეტსახელი, ინგ. Username) და პაროლი, რომლითაც ეს უკანასკნელი ამ საიტის ორიგინალურ ვერსიაზე შედიოდა ხოლმე. ამ მცდელობის მიუხედავად იგი თავის პირად მონაცემებში ვერ შევიდა. ალ. მანიას კი სპეციალური კომპიუტერული პროგრამის საშუალებით გადაეგზავნა საიტის ნამდვილ ვერსიაზე შესვლისთვის საჭირო დ. სუტკინის პაროლი, რითაც ალ. მანიამ უზრუნველყო კომპიუტერულ სისტემაში შეღწევისთვის საჭირო მონაცემების ხელმისაწვდომობა.“

ჩემი აზრით, ის რომ ალ. მანიამ დ. სუტკინის პაროლი თაღლითური გზით მოიპოვა, სწორია. ამის შემდეგ განაჩენში ვკითხულობთ, რომ „ალ. მანიამ დ. სუტკინის ანგარიშზე არსებული თანხის დაუფლება გადანყვიტა და შეცვალა სუტკინის პაროლი.“ ხოლო მას შემდეგ, რაც ალ. მანია განზრახ აგებს უკვე საკუთარ ანგარიშზე არსებულ თანხას მ. ქარდავასთან, სასამართლო ასკენის, რომ ამ ქმედებით „კომპიუტერულ მონაცემში უნებართვო შეღწევისთვის საჭირო მონაცემის დაშვებისა და გამოყენების გზით, დ. სუტკინის ანგარიშიდან თაღლითურად დაუფლებული ფულადი თანხა ალ. მანიამ განზრახ წააგო.“

ამრიგად, სასამართლომ დაადგინა, რომ ალ. მანიამ ჩაიდინა საქართველოს სისხლის სამართლის კოდექსის 180-ე მუხლის მე-2 ნაწილის „ბ“ პუნქტით და 285-ე მუხლის პირველი ნაწილით გათვალისწინებული დანაშაული, ხოლო მ. ქარდავამ 376-ე მუხლით გათვალისწინებული დანაშაულის შეუტყობინებლობა.

მოცემული კაზუსის კვალიფიკაციასთან დაკავშირებით ჩემი მოსაზრება განსხვავდება საგამოძიებო ორგანოს და სასამართლოს პოზიციისგან. კერძოდ, კი ჩემი აზრით ალ. მანიამ გარდა თაღლითობისა ჩაიდინა:

1. 284-ე მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, ვინაიდან, უნებართვოდ შეაღწია ინტერნეტ-ტოტალიზატორ „ფრანჩესკოს“ კომპიუტერულ სისტემაში.

2. 286-ე მუხლის 1-ლი ნაწილით გათვალისწინებული ქმედება, რადგან მან უნებართვოდ შეცვალა დ. სუტკინის პაროლი.

აღსანიშნავია, სასამართლომ განაჩენში თავადვე მიუთითა, რომ ალ. მანამ კომპიუტერულ სისტემაში უნებართვოდ შეაღწია და ასევე, უნებართვოდ შეცვალა კომპიუტერული მონაცემი. თუმცა განაჩენში ამ გარემოებების სამართლებრივი შეფასება აღარ მოუხდენია.

დაბოლოს, ალ. მანიას საერთოდ არ ჩაუდენია 285-ე მუხლით გათვალისწინებული დანაშაული, რადგან მართალია მას ამოძრავებდა კიბერდანაშაულის თავით გათვალისწინებული დანაშაულის ჩადენის მიზანი, კერძოდ, კომპიუტერულ სისტემაში უნებართვოდ შეღწევის და კომპიუტერული მონაცემის უნებართვოდ შეცვლის მიზანი, მაგრამ ალ. მანიას დ. სუტკინის კერძო კომუნიკაციის საიდუმლოების დარღვევა აზრადაც არ ჰქონია. ჯერ, ერთი დ. სუტკინს არც არავისთან არ ჰქონდა კერძო კომუნიკაცია დამყარებული და მეორეც, სასამართლოს მიერ დადგენილია, რომ გარდა დანარჩენისა, ალ. მანიას მიზანი იყო თაღლითური გზით დ. სუტკინის საკუთრებაში არსებული ფულის მითვისება.

განხილული კაზუსის მაგალითზე შეგვიძლია დავასკვნათ, რომ მოცემულ შემთხვევაში დანაშაულის უშუალო ობიექტი იყო დ. სუტკინის საკუთრებითი ურთიერთობა, პირადი კომპიუტერული მონაცემის კონფიდენციალურობა, ასევე, კომპიუტერული მონაცემის ხელშეუხებლობა და მისი მფლობელის ინტერესები, დამატებითი ობიექტად უნდა განვიხილოთ იმ კომპიუტერული სისტემის უსაფრთხოება, რომელშიც განთავსებული იყო ინტერნეტ-ტოტალიზატორი „ფრანჩესკო“, ასევე მისი რეპუტაცია. რეპუტაციასთან დაკავშირებით უნდა აღინიშნოს, რომ ინტერნეტ-საიტები ყოველთვის ცდილობენ დაფარონ მათ კომპიუტერულ სისტემაში უნებართვო შეღწევის ფაქტები, რადგან მათი გახმაურება პირდაპირ აისახება ინტერნეტ-საიტის მომხმარებლების რიცხვზე. მაშინ როცა ინტერნეტ-საიტი ხშირად ხდება პაკეტების შეტყევის მსხვერპლი მის რეპუტაციას ადგება ზიანი და ის კარგავს მომხმარებელს,

რადგან ეჭვქვეშ დგება კომპიუტერული სისტემის დაცვის საიმედოობის საკითხი. სწორედ ამ გარემოების გამო მნიშვნელოვანია ინტერნეტ-ტოტალიზატორ „ფრანჩესკოს“ რეპუტაცია განვიხილოთ, ალ. მანიას მიერ ჩადენილი დანაშაულის დამატებით ობიექტად. დანაშაულის საგანია ის ფული, რომლის ხელყოფაც განხორციელდა, ასევე, იმ კომპიუტერული სისტემის უსაფრთხოება და კონფიდენციალურობა, რომელშიც განთავსებული იყო დ. სუტკინის პირადი გვერდი. ანუ გამოდის, რომ დანაშაულის საგანია ინტერნეტ-ტოტალიზატორი „ფრანჩესკოს“ კომპიუტერული სისტემა და დ. სუტკინის პირადი გვერდი ამ სისტემაში. ასევე, ის კომპიუტერული მონაცემი, რომელიც შეიცვალა დანაშაულებრივი ხელყოფის შედეგად, ანუ დ. სუტკინის პაროლი.

დანაშაულის ჩადენის ხერხია – ინტერნეტ-ტოტალიზატორის დუბლიკატის შექმნის გზით მოპოვებული პაროლის გამოყენებით კომპიუტერულ სისტემაში შეღწევა, კომპიუტერული მონაცემის შეცვლა და მოტყუებით სხვისი ფულის დაუფლება.

4. 286-ე მუხლით გათვალისწინებული დანაშაულის ობიექტური შემადგენლობა

საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლის I ნაწილის დისპოზიცია ჩამოყალიბებულია შემდეგნაირად:

„კომპიუტერული მონაცემის უნებართვო დაზიანება, ნაშლა, შეცვლა ან დაფარვა“.

მეორე ნაწილში კი ვკითხულობთ:

„ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, აგრეთვე კომპიუტერული მონაცემის უნებართვო ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია.“

აღნიშნული დანაშაულის უშუალო ობიექტია იმ კომპიუტერული მონაცემის მესაკუთრის ინტერესი, რომლის უნებართვო დაზიანება, ნაშლა, შეცვლა ან დაფარვა ხორციელდება. ასევე, ხელყოფის ობიექტი შეიძლება იყოს კომპიუტერული სისტემის მთლიანობა და ნორმალური ფუნქციონირება. გასაზიარებელია, გ. მამულაშვი-

ლის აზრი, რომ დანაშაულის ობიექტია კომპიუტერული სისტემის ინტეგრირებულობა და ნორმალური ფუნქციონირება. ასევე, კომპიუტერული სისტემის მფლობელის ინტერესები და მომხმარებელთა უფლებები⁸².

დანაშაულის საგანია ის კომპიუტერული მონაცემი, რომლის უნებართვო დაზიანება, ნაშლა, შეცვლა ან დაფარვა ხორციელდება. ასევე, ის კომპიუტერული სისტემა, რომლის ფუნქციონირებაც ფერხდება დანაშაულის შედეგად. კომპიუტერული სისტემის ფუნქციონირების შეფერხება არ უნდა გავიგოთ, როგორც კომპიუტერული ტექნიკის მწყობრიდან გამოსვლა. ის გულისხმობს კომპიუტერული სისტემის ფუნქციის მოშლას. იმ შემთხვევაში თუ მოხდება კონკრეტულად კომპიუტერული ტექნიკის დაზიანება და დადგება 150 ლარზე მეტი ოდენობის ზიანი, სახეზე გვექნება არა კიბერდანაშაული, არამედ, სისხლის სამართლის კოდექსის 187-ე მუხლით აკრძალული სხვისი ნივთის დაზიანება ან განადგურება, რამაც მნიშვნელოვანი ზიანი გამოიწვია

საქართველოს სისხლის სამართლის კოდექსის არც ძველი და არც ახალი რედაქცია არ შეიცავს დათქმას სპეციალური ობიექტის შესახებ. მაგალითად, ავსტრალიაში კომპიუტერული დანაშაულის სფეროში მოქმედებს კანონი „კიბერდანაშაულის შესახებ“, რომლის შესაბამისად პირს სასჯელის მაქსიმალური ზომა ეკისრება იმ შემთხვევაში, თუ უნებართვოდ შეაღწევს სახელმწიფო საკუთრებაში არსებულ კომპიუტერში და მოახდენს არსებული ინფორმაციის მოდიფიცირებას. პირი დამნაშავედ ჩაითვლება იმ შემთხვევაშიც, თუ არ დადგება ფაქტობრივი ზიანი⁸³.

როგორც ვხედავთ, ავსტრალიური კანონმდებლობა ცალკე გამოყოფს სახელმწიფოს საკუთრებაში არსებულ კომპიუტერს.

ამ კუთხით საინტერესოა, გერმანიის კანონმდებლობაც. გერმანული სისხლის სამართლის კოდექსის 303-ა მუხლის შესაბამისად იკრძალება მონაცემთა ბაზის ნაშლა, შეზღუდვა, გაუფარგისება და შეცვლა.

82 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი II, გამოცე. „მერიდიანი“, თბ. 2012წ. გვ. 43

83 იხ. <http://www.cybercrimelaw.net/laws/countries/australia.html>

303-ბ^ა მუხლის მიხედვით კი დასჯადია 303-ა მუხლში გათვალისწინებულ ქმედების გზით ან მონაცემთა დამამუშავებელი ხელსაწყო ან მონაცემთა მატარებლის განადგურების გზით მონაცემთა ბაზის დამუშავებისთვის ხელის შეშლა. იმისთვის, რომ დანაშაულის შემადგენლობა გვექონდეს სახეზე, გერმანელი კანონმდებელი დამატებით აღნიშნავს, რომ ამ მონაცემთა ბაზის დამუშავებას განსაკუთრებული მნიშვნელობა უნდა ჰქონდეს რომელიმე სახარმოს, ორგანიზაციის ან დაწესებულებისთვის. ამდენად, 303-ბ მუხლი გამოყოფს ხელყოფის სპეციალურ ობიექტს და ესაა სახარმოს, ორგანიზაციის ან დაწესებულების მონაცემთა ბაზის დამუშავების პროცესის უსაფრთხოება.

ამავე მუხლით დამამძიმებელ გარემოებად არის გამოყოფილი მძიმე შედეგის დადგომა, დიდი ოდენობით ქონებრივი ზიანი, დანაშაულის ჩადენა ორგანიზებული ჯგუფის მიერ. ასევე, თუ ზიანი ადგება მოსახლეობის სასიცოცხლო სიკეთეს ან მომსახურებით უზრუნველყოფას ან/და გერმანიის ფედერაციული რესპუბლიკის უსაფრთხოებას.

სახელმწიფო ინტერესს კიდევ უფრო მეტ ყურადღებას უთმობს სინგაპური. კერძოდ, კანონი „კომპიუტერის ბოროტად გამოყენების შესახებ“ კანონის 50ა თავის, მე-9 მუხლის, მე-2 პუნქტის შესაბამისად.

„კომპიუტერი განიხილება „დაცულ კომპიუტერად“ თუ პირმა, რომელმაც ჩაიდინა დანაშაული იცოდა, ან უნდა სცოდნოდა, რომ კომპიუტერი ან პროგრამა ან ინფორმაცია გამოიყენება ან აუცილებელია:

ა) სინგაპურის უშიშროების, თავდაცვის ან საერთაშორისო ურთიერთობისთვის;

ბ) სისხლის სამართლის კანონის აღსრულებასთან დაკავშირებული კონფიდენციალური ინფორმაციის წყაროს არსებობის ან უტყუარობისთვის;

გ) მომსახურების უზრუნველყოფისთვის, რომელიც პირდაპირ კავშირშია საკომუნიკაციო ინფრასტრუქტურასთან, საბანკო და საფინანსო მომსახურებასთან, კომუნალურ მომსახურებასთან, საზოგადოებრივ ტრანსპორტთან ან ძირითად სახელმწიფო ინფრასტრუქტურასთან;

დ) საზოგადოებრივი უსაფრთხოების დაცვისთვის, მათ შორის სისტემებისთვის, რომლებიც დაკავშირებულია ისეთ მნიშვნელოვან საგანგებო სამსახურებთან, როგორებიცაა პოლიცია, სამოქალაქო თავდაცვა და სამედიცინო სამსახურები.

თუმცა სინგაპურელი კანონმდებლის ფანტაზია ამით არ მთავრდება. განხილული მუხლი შეიცავს ძალიან საინტერესო მე-4 პუნქტს, სადაც ნათქვამია, რომ კანონის მე-9 მუხლის მე-2 პუნქტის საფუძველზე განხორციელებული ნებისმიერი სისხლისსამართლებრივი დევნის მიზნებისთვის ივარაუდება, რომ სანინალმდევოს დამტკიცებამდე ბრალდებული მიიჩნევა დამნაშავედ, თუ ხელყოფილ კომპიუტერთან, პროგრამასთან ან ინფორმაციასთან მიმართებაში არსებობდა ბრალდებულის დასაწახად გამოტანილი ელექტრონული ან სხვა სახის გაფრთხილება იმის შესახებ, რომ არაავტორიზებული პერსონა ამ კომპიუტერში, პროგრამაში ან ინფორმაციაში გამოიწვევდა უფრო მაღალ სასჯელს⁸⁵.

ჩემი აზრით, ზემოთმოყვანილი სახელმწიფოების მიდგომა გასათვალისწინებელია. ქართული სისხლის სამართლის კიბერდანაშაულის მუხლები უნდა შეიცავდნენ დათქმას დანაშაულის ხელყოფის ობიექტთან დაკავშირებით. კერძოდ, განსაკუთრებულად მნიშვნელოვანია დამამძიმებელ გარემოებებში სახელმწიფო ინტერესის და უსაფრთხოების ზაზგასმა.

უმჯობესია, რომ საქართველოს სისხლის სამართლის კოდექსის 284-ე, 285-ე და 286-ე მუხლების დისპოზიციას დაემატოს წინადადება, რომლის მიხედვითაც უფრო მძიმე სასჯელი იქნება გათვალისწინებული იმ კომპიუტერულ სისტემაზე უკანონო ზემოქმედებისთვის რომლის მესაკუთრე სახელმწიფოა და რომელიც ემსახურება ქვეყნის თავდაცვის და უშიშროების ინტერესს.

საინტერესოა, რომ 286-ე მუხლის ძველი რედაქცია შემდეგნაირად იყო ჩამოყალიბებული: „ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის ექსპლუატაციის წესის დარღვევა იმის მიერ, ვისაც ხელი მიუწვდებოდა ეგმ-ზე, ეგმ-ის სისტემაზე ან მათ ქსელზე, რამაც გამოიწვია ეგმ-ის კანონით დაცული ინფორმაციის გაზადგურება, ბლოკირება, მოდიფიცირება ან გადაღება ან/და რამაც მნიშვნელო-

85 იხ. <http://www.cybercrimelaw.net/laws/countries/Singapore.html>

ვანი ზიანი გამოიწვია." უნდა აღინიშნოს, რომ სანამ დადგინდებოდა სისხლისამართლებრივი პასუხისმგებლობა გარკვეული წესის დარღვევაზე, უნდა არსებულიყო შესაბამისი სახელმწიფო უწყების მიერ დადგენილი ზოგადი წესი, რომლის საფუძველზეც სხვადასხვა კომპანია თუ ორგანიზაცია განსაზღვრავდა შიდა კომპიუტერული ქსელის ექსპლუატაციის წესებს. შესაძლებელია თითზე ჩამოსათვლელი შემთხვევის გახსენება, როცა რომელიმე ორგანიზაცია საკუთარი ინიციატივით ადგენდა შიდა კომპიუტერული ქსელით სარგებლობის წესს. მაგალითად, საქართველოს თავდაცვის მინისტრის „საქართველოს შეიარაღებული ძალების გაერთიანებული შტაბის J-6 კავშირგაბმულობის და ინფორმაციული სისტემების (CIS) დეპარტამენტის დებულების დამტკიცების შესახებ“ 2008 წლის 22 მაისის ბრძანების 27-ე მუხლის შესაბამისად დეპარტამენტის კომპიუტერული ქსელების განყოფილების ერთ-ერთი ფუნქციაა კომპიუტერული ქსელების ექსპლუატაციის წესების განსაზღვრა. ბუნებრივია, იმ შემთხვევაში თუ მომავალში ვინმე დაარღვევდა ამ წესებს, დაისჯებოდა სისხლის სამართლის კოდექსის 286-ე მუხლით. თუმცა, როგორც უკვე აღინიშნა ამ წესების დადგენა იშვიათად ხდებოდა. ამ მიზეზით აღნიშნული მუხლი „მკედარი“ ნორმა იყო.

საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლის ახალ რედაქცია ჩამოყალიბებულია შემდეგნაირად:

„1. კომპიუტერული მონაცემის უნებართვო დაზიანება, ნაშლა, შეცვლა ან დაფარვა;

2. ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, აგრეთვე კომპიუტერული მონაცემის უნებართვო ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია“ ქართველი კანონმდებლის მიერ ამ მუხლის პირველ და მეორე ნაწილებში რეალიზებულია ევროპის საბჭოს კონვენციის მე-4 და მე-5 მუხლები.

დანაშაულის ობიექტური მხარე შეიძლება გამოიხატოს უშუალოდ კომპიუტერული მონაცემის უნებართვო დაზიანებაში, ნაშლაში, შეცვლასა ან დაფარვაში.

დანაშაულის ჩადენის საშუალებაა ის კომპიუტერული პროგრამა, რომლის გამოყენებითაც, ხორციელდება კომპიუტერული მონაცემის უნებართვო დაზიანება, ნაშლა, შეცვლა ან დაფარვა. თუმცა,

შეიძლება ამ მოქმედების განხორციელებას არანაირი სპეციალური პროგრამა არ დასჭირდეს. მაგალითისთვის, თუ პირი მოიპოვებს იმ სისტემაში შეღწევის პაროლს, რომელშიც ინახება აღნიშნული მონაცემი, ის ყოველგვარი დამხმარე პროგრამის გარეშე შეძლებს მის განადგურებას, დაზიანებას და ა.შ.

კომპიუტერული სისტემის ან/და მონაცემის დაზიანებაში უნდა იგულისხმოდეს მათი გაუვარგისება, თუმცა ამ შემთხვევაში შესაძლოა დაზიანებული მონაცემი სპეციალური პროგრამის დახმარებით ექვემდებარებოდეს აღდგენას. დაზიანება ცხადია, მოითხოვს კომპიუტერულ სისტემაში ან/და მონაცემთან შეღწევას. კომპიუტერული სისტემის ან/და მონაცემის დაზიანება ზოგ შემთხვევაში შესაძლებელია ინფორმაციის შემნახავ მონყობილობაში შეღწევის გარეშეც. ამ შესაძლებლობას იძლევა ისეთი პროგრამული უზრუნველყოფა, როგორიცაა კომპიუტერული ვირუსი, რომლის უნებართვო ინსტალაცია (კომპიუტერის სისტემაში ინტეგრირება) მონაცემთა ნაშლის ოპერაციის განხორციელების მიზნით, ხორციელდება სამიზნე კომპიუტერში.⁸⁶

კომპიუტერული მონაცემის ნაშლაში იგულისხმება მისი ნებისმიერი ხერხით განადგურება, გამოსაყენებლად გაუვარგისება.

ევროპის საბჭოს კონვენციის მე-4 მუხლი არა მხოლოდ კომპიუტერული მონაცემების დაზიანებას და ნაშლას გამოყოფს დასჯად ქმედებად, არამედ ისეთი ქმედებას, რომელმაც შესაძლოა გამოიწვიოს მსგავსი დაზიანება. ერთ-ერთი ამგვარი ქმედებაა კომპიუტერულ მონაცემებში ცვლილებების შეტანა. თუ კომპიუტერული ვირუსი ცვლის მონაცემების შინაარსს, ეს უთანაბრდება ფაილის ნაშლას⁸⁷. ამდენად, ევროსაბჭოს ექსპერტების აზრით, კომპიუტერული მონაცემის შეცვლაში მოიაზრება მის შინაარსში ცვლილების შეტანა და იგი უნდა გავუთანაბროთ კომპიუტერული მონაცემის ნაშლას. ამ მოსაზრებას არ ეიზიარებ იმ ნაწილში, რომ მონაცემის შეცვლა უთანაბრდება მის ნაშლას. შესაძლოა ვისაუბროთ ამ ორი

86 იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ: ტრენინგის სახელმძღვანელო“, ევროსაბჭო, სტრასბურგი, 2010წ. გვ. 51

87 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი II, გამოშვ. „მერიდიანი“, თბ. 2012წ. გვ. 42

ქმედების გამო დამდგარ მსგავს შედეგზე და ზიანზე, მაგრამ შინა-
არსით ისინი განსხვავდებიან ერთმანეთისგან და ალბათ, სწორედ
ამიტომ, როგორც ევროპის საბჭოს კონვენციამ, ასევე, ქართველმა
კანონმდებელმა კოდექსის 286-ე მუხლში ეს ტერმინები არ გაუი-
გივა ერთმანეთს და ცალცალკე გამოყო. ამდენად, კომპიუტერული
მონაცემის ნაშლაა, როცა ხდება მისი სრული განადგურება, ხოლო
შეცვლაში უნდა ვიგულისხმოთ მის შინაარსში ცვლილების შეტანა.

კომპიუტერული მონაცემის დაფარვაა ამ მონაცემის ისეთი
დამალვა, როცა მისი მფლობელისთვის უცნობია სად ინახება ის.
გარდა ამისა, არსებობს ისეთი კომპიუტერული პროგრამა, რომე-
ლიც ახდენს კომპიუტერული მონაცემის უჩინარად გადაქცევას, ანუ
ასეთ დროს კომპიუტერული მონაცემი ვიზუალურად ვერ აღიქმება,
მაგრამ მყარ დისკზე ინახება. აღნიშნულ ხერხს ხშირად იყენებენ
კომპანიები, როდესაც საგადასახადო სამსახურს უმაღლესენ ე.წ. „შავ
ბულალტერიას“. ამავე ხერხს მიმართავენ პაკერები, როდესაც სა-
მართალდამცავი ორგანოები ამოწმებენ მათ კომპიუტერს. პაკერები
წინასწარ აძლევენ სათანადო ბრძანებას სპეციალურ კომპიუტერულ
პროგრამას, რომელიც ვიზუალური აღქმისგან ფარავს კომპიუ-
ტერულ მონაცემს. ეს მონაცემი მხოლოდ სპეციალური პროგრამის
დახმარების გამოყენებით შეიძლება გახდეს ხილული.

კომპიუტერული მონაცემის დაფარვაში უნდა ვიგულისხმოთ
თუ არა ამ მონაცემის ერთი კომპიუტერიდან მეორეში გადატანა
ისე, რომ პირველში მისი კვალი არ დარჩეს? ჩემი აზრით, მსგავსი
ქმედება უნდა ჩავთვალოთ კომპიუტერული მონაცემის ნაშლად
და არა დაფარვად. წარმოვიდგინოთ ასეთი სიტუაცია: გამოძიე-
ბელმა ა. ამირიძემ შინაგან საქმეთა სამინისტროს კომპიუტერული
მონაცემთა ბაზიდან ამოშალა ძმა – ბ. ამირიძის დანაშაულებრივ
საქმიანობაზე მონაცემები და ის გადაიტანა საკუთარ კომპიუტერში.
გამოდის, რომ ა. ამირიძემ საერთოდ კი არ გაანადგურა მონაცემი,
არამედ მოახდინა მისი კონკრეტულ მონაცემთა ბაზიდან ნაშლა და
სხვაგან გადატანა. როგორ უნდა შეფასდეს მისი ქმედება?

ეს ქმედება განხილულ უნდა იქნეს როგორც კომპიუტერული
მონაცემის ნაშლა და არა დაფარვა, რადგან ძირითადი მოქმედება,
რომლითაც მონაცემზე ზემოქმედება ხორციელდება ნაშლაა, რად-
გან იგი ამ მოქმედების შემდეგ აღარ მოიძებნება იმ კომპიუტერულ

სისტემაში, სადაც ინახებოდა. ის ფაქტი, რომ ა.ამირიძემ მონაცემი საკუთარ კომპიუტერში შეინახა არ ცვლის დამდგარ შედეგს, რადგან სახეზე გვაქვს შინაგან საქმეთა სამინისტროს კომპიუტერული მონაცემთა ბაზიდან კომპიუტერული მონაცემის განადგურება. თუ ა. ამირიძე ამ მონაცემს ერთი მონაცემთა ბაზიდან მეორეში გადატანის ნაცვლად, შეცვლიდა მის შინაარსს, სახეზე გვექნებოდა კომპიუტერული მონაცემის შეცვლა, ხოლო თუ სპეციალური პროგრამის დახმარებით ა. ამირიძე ბ. ამირიძის შესახებ ინფორმაციას მონაცემთა ბაზაში ვიზუალური აღქმისგან დაფარულს გახდიდა, მივიღებდით კომპიუტერული მონაცემის დაფარვას.

მოცემული მსჯელობიდან გამომდინარე, შეიძლება დავასკვნათ, რომ 286-ე მუხლით გათვალისწინებული დანაშაული მატერიალური შემადგენლობისაა, რადგან იგი უკავშირდება კონკრეტული შედეგის დადგომას.

286-ე მუხლის მე-2 ნაწილში მითითებულია:

„286-ე მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, აგრეთვე კომპიუტერული მონაცემის უნებართვო ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია.“

კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვან შეფერხებაში უნდა ვიგულისხმოთ კომპიუტერული სისტემის მუშაობის არსებითი შეფერხება. მაგალითად, თუ კიბერშეტევის ობიექტია ავიაკომპანია, რომელსაც შეტევის შედეგად ხელი შეეშალა ავიარეისების განხორციელებაში, მომხმარებლებს შეეზღუდათ ბილეთის შეძენის საშუალება და ა.შ. ან მაგალითად თუ სამენარეო რეესტრის კომპიუტერულ სისტემაზე იერიშის გამო შეუძლებელი გახდა ახალი სამენარეო სუბიექტების რეგისტრაცია ან უკვე რეგისტრირებულ სუბიექტებზე არსებული საჯარო ინფორმაციაზე შეიზღუდა ხელმისაწვდომობა, რამაც გამოიწვია კონკრეტული ხასიათის ზიანი, იქნება ეს ფინანსური ზარალი, სამენარეო საქმიანობის შეფერხება და ა.შ. აღსანიშნავია, რომ კომპიუტერული სისტემის შეფერხება არის თუ არა მნიშვნელოვანი უნდა შეფასდეს თითოეული საკითხის განხილვისას ინდივიდუალურად, საქმეში არსებული მტკიცებულებების ანალიზის და შეფასების საფუძველზე.

კომპიუტერული მონაცემების უნებართვო ჩასმა უნდა გავიგოთ, როგორც კომპიუტერული მონაცემის არადანიშნულებისამებრ და არამიზნობირვად ჩანერა. მაგალითად, როდესაც დამნაშავე სამიზნე კომპიუტერში უნებართვოდ ჩანერს სპეციალურ პროგრამას, რომლის გააქტიურებაც შეაფერხებს კომპიუტერული სისტემის ფუნქციონირებას.

კომპიუტერული მონაცემის გადაცემის ყველაზე თვალსაჩინო მაგალითია ე.წ. „დოს“ შეტევა, ანუ როდესაც საიტის სერვერის მიმართ გადაიცემა ერთდროულად ათასობით მოთხოვნა (საიტზე შესვლის მცდელობა), რასაც სერვერი ვერ უძლებს და ხდება კომპიუტერული სისტემის ფუნქციონირების შეფერხება.

საინფორმაციო ტექნოლოგიები ბიზნესის წარმოებისა და ბიზნესკომუნიკაციის მნიშვნელოვან ელემენტს წარმოადგენენ. სხვადასხვა ტიპის ინტერნეტ-მომსახურების შეწყვეტა უარყოფით გავლენას ახდენს ამ ურთიერთობაში ჩართული პირების საქმიანობაზე. მაგალითად, თუ მიუწვდომელია სერვერი, რომელიც პასუხისმგებელია მომხმარებელთა შორის კომუნიკაციის უზრუნველყოფაზე, კლიენტი იძულებულია გადაერთოს კომუნიკაციის სხვა საშუალებაზე. ალტერნატიული მომსახურების არსებობა კომპიუტერული უსაფრთხოების სტრატეგიის მნიშვნელოვანი ნაწილია, თუმცა დამატებითი სისტემების შენახვა და ფუნქციონირება მოითხოვს დამატებით ხარჯს, რომლის განევის ფუფუნება ინტერნეტ-მომხმარებლების უმრავლესობას არ გააჩნია. მომსახურების ხელმისაწვდომობაზე ზეგავლენა მრავალი გზით შეიძლება განხორციელდეს. ეს შეიძლება გამოწვეულ იქნეს ჩვეულებრივი ავარიით, მაგალითად, ინტერნეტ-კაბელის დაზიანებით. თუმცა, გარდა ავარიისა არსებობს უამრავი საშუალება, რომელსაც დამნაშავეები იყენებენ ინტერნეტის ხელმისაწვდომობის შეზღუდვისთვის. მაგალითად, ინტერნეტის სერვერის ფიზიკური ხელყოფა აფეთქების, ცეცხლის ნაკიდების და ა.შ. გზით.

საინტერესოა 286-ე მუხლის მე-2 ნაწილით გათვალისწინებული დანაშაულის ჩადენის საშუალების განხილვაც. ამ ნაწილში საუბარია ისეთი ქმედების განხორციელებაზე, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება

გამოიწვია. ბუნებრივია, აღნიშნული შედეგი შესაძლებელია დადგეს სხვადასხვა კომპიუტერული პროგრამის დახმარებით, იქნება ეს კომპიუტერული ვირუსი, თუ სხვა, მაგრამ უნდა აღინიშნოს, რომ მნიშვნელოვანი შეფერხება შესაძლებელია გამოიწვიოს ერთი შეხედვით სრულიად უწყინარმა მოქმედებამ. საუბარია, ე.წ. დოს (DDoS) შეტევებზე. ამ საკითხს უფრო დეტალურად დანაშაულის ობიექტურ მხარესთან მიმართებაში ქვემოთ განვიხილავ, მაგრამ აქ უნდა ითქვას, რომ 286-ე მუხლის მე-2 ნაწილით გათვალისწინებული დანაშაულის ჩადენის საშუალება ე.წ. „დოს“ შეტევების შემთხვევაში არის კომპიუტერი, რომელსაც შესაძლოა სპეციალური კომპიუტერული პროგრამული უზრუნველყოფა არ გააჩნია, მაგრამ ჩართულია გლობალურ ქსელში. კომპიუტერული ვირუსის საშუალებით შეტევის წარმატებული განხორციელებისთვის საჭიროა კომპიუტერული სისტემის დამცავი საშუალების გადალახვა, რაც შეიძლება დამნაშაისთვის შეუძლებელი იყოს. ამიტომ, მსოფლიოში გავრცელება პპოყა ე.წ. „დოს“ (DDoS)⁸⁸ შეტევამ. ასეთ დროს დამნაშავე კომპიუტერული სისტემისკენ მიმართავს იმაზე მეტ მოთხოვნას, რამდენის დამუშავების შესაძლებლობაც აქვს ამ სისტემას⁸⁹.

286-ე მუხლის მე-2 ნაწილით გათვალისწინებული დანაშაულის ობიექტური მხარე გამოიხატება კომპიუტერული მონაცემის ისეთ მიზანმიმართულ გადაცემაში, რომელიც მიმართულია კომპიუტერული სისტემის ნორმალური ფუნქციონირებისთვის ხელის შეშლისკენ.

88 DDoS (Distributed Denial of Service) - საკმაოდ ძველი და პრიმიტიული მეთოდი კომპიუტერულ სერვერზე თავდასხმისთვის. აღნიშნული შეტევა ხორციელდება სპეციალური პროგრამის დახმარებით, რომელიც ერთდროულად, ათასობით კომპიუტერიდან ახორციელებს მოთხოვნას წინსწარ პერჩეული – სამიზნე საფოსტო ან/და ნებისმიერი ვებ-სერვერით სარგებლობაზე. სერვერის რესურსით სარგებლობაზე მიმართული უამრავი მოთხოვნა იწვევს მისი ოპერატიული მექანიზმების და მონაცემთა ბაზასთან ერთდროულად დაკავშირების ლიმიტის გადატვირთვას, რაც საბოლოოდ იწვევს სერვერის ხშირ გამორთვას, ხელახალ ჩართვას და მომხმარებლისთვის ინტერნეტ-რესურსით სარგებლობის ხელმისაწვდომობის შეზღუდვას.

89 იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ: ტრენინგის სახელმძღვანელო“, ევროსაბჭო, სტრასბურგი, 2010წ. გვ. 55

აღსანიშნავია, რომ მოცემული დანაშაული მატერიალური შემაღ-
გენლობისაა, რადგან სისხლისსამართლებრივი პასუხისმგებლობა
უკავშირდება კონკრეტული შედეგის დადგომას, ანუ კომპიუტერული
სისტემის განზრახ მნიშვნელოვან შეფერხებას.

კიბერშეტევების მავნე შედეგებზე საუბარი დაუსრულებლად
შეიძლება, თუმცა ახლა, როცა ეცდილობთ განვმარტოთ, რაში
შეიძლება გამოიხატოს 286-ე მუხლის მეორე ნაწილით გათვალის-
წინებული ქმედების ობიექტური მხარე, ბუნებრივია, პირველი, რაც
შეიძლება გაგვახსენდეს, არის ცოცხალი მაგალითი საქართველოს
უახლესი ისტორიიდან.

2008 წლის ივლის-აგვისტოში საქართველოს სახელმწიფო ორგა-
ნოების და საინფორმაციო რესურსების წინააღმდეგ დაწყებული
კიბერშეტევის განხორციელების მიზნით სხვადასხვა რუსულ ინტერ-
ნეტ-ფორუმზე დაიწყო მოხალისეთა რაზმების შექმნა, რომლებიც
აღჭურვილი იყვნენ სპეციალური პროგრამული უზრუნველყოფით
ე.წ. „დოს“ შეტევის განხორციელების უზრუნველსაყოფად. აღნიშ-
ნულ ფორუმებზე ხდებოდა ჩვეულებრივი მოქალაქეების გათვით-
ცნობიერება შეტევის არსში. კერძოდ, ფორუმზე განთავსებული იყო
საქართველოს სტრატეგიულ ინტერნეტ-რესურსთა სრული ნუსხა
და შემდეგ შერჩევით რომელიმე მათგანზე იწყებოდა იერიში. აღნიშ-
ნული დასკვნის გამოტანის საფუძველს იძლევა ჩემს მიერ რუსული
რესურსის „სტოპჯორჯია.რუს“ (www.stopgeorgia.ru) მუშაობის დეტა-
ლური შესწავლა, ყოველდღიური დაკვირვება და ფორუმის თემებში
აქტიური მონაწილეობა. გარდა ამისა, მოვიშველიებ რუსეთ-საქართ-
ველოს აგვისტოს ომის დროს განხორციელებული კიბერშეტევების
შემსწავლელი ერთ-ერთი ჯგუფის (ე.წ. The grey Goose) წევრთა მიერ
ჩატარებული გამოძიების მონაცემებს. მკვლევართა ჯგუფში 100-ზე
მეტი ექსპერტი იყო ჩართული ისეთი ტექნოლოგიური გიგანტები-
დან, როგორიცაა მაიკროსოფტი (Microsoft), ორაკლი (Oracle) და სხვა
სამთავრობო თუ არასამთავრობო ორგანიზაცია. ჯგუფი გამოძიებას
მაშინვე შეუდგა, როცა საქართველოს სამთავრობო საიტების უმრავ-
ლესობა მწყობრიდან გამოვიდა. გამოძიებლებმა საქმის შესწავლა
დაიწყეს ინტერნეტ-ფორუმიდან – „ჰაკერ.რუ“ (www.xaker.ru). მათ
აღმოაჩინეს გზავნილი მოხალისეებისადმი, რომლებიც იმართებო-

დენ ზემოთხსენებული – „სტოპჯორჯია.რუდან“ (www.stopgeorgia.ru).⁹⁰ ამავე ჯგუფის ექსპერტთა ვარაუდით, ამ კონკრეტული საიტებიდან არა „დოს“ იერიში, არამედ უფრო მარტივი, მაგრამ იგივე ეფექტის მქონე შეტევა განხორციელდა, რომელშიც ერთი კომპიუტერის გამოყენებაც საკმარისი იყო. კერძოდ, თითოეული თავდამსხმელი იყენებს პროგრამების ნაკრებს (ე.წ. მაიესქუელი (MySQL)), რომელიც გამოიყენება ვებ-გვერდზე მონაცემთა ბაზების მართვის დამხმარე სისტემის სამართავად. პაკერებმა ამავე ფორუმებზე გაავრცელეს აღნიშნული ხერხით საიტების მწყობრიდან გამოყვანის შესახებ ინსტრუქციები⁹¹.

2008 წლის 12 აგვისტოს გაზეთი „ნიუ იორკ თაიმსი“ წერდა, რომ ისტორიაში პირველად ორ ქვეყანას შორის შეიარაღებულ კონფლიქტს წინ უძღოდა ინტენსიური კიბერმომზადება. საქართველოზე კიბერშეტევა არ დაწყებულა 8 აგვისტოს. ის კონფლიქტის დაწყებამდე ბევრად ადრე მომზადდა და შედარებით მცირე მასშტაბით ჯერ კიდევ ივლისის ბოლოდან ხორციელდებოდა⁹². 13 აგვისტოს ინტერნეტ-გაზეთში „დნი.რუ“ (dni.ru) გამოქვეყნდა კიბერუსაფრთხოების სფეროში მომუშავე ერთ-ერთი სპეციალისტის ფრაზა, რომელიც საქართველოს პრეზიდენტის საიტის დაცვაზე მუშაობდა: „ახლანდელი სიტუაცია შეიძლება შევადაროთ ჭადრაკის თამაშს. ჩვენ ვიღებთ დარტყმას, საიტი მწყობრიდან გამოდის, ორ საათში აღვადგენთ სისტემას, 30-45 წუთი საიტი მუშაობს, შემდეგ პაკერების თავდასხმა მეორდება და ისინი კვლავ ახერხებენ ინტერნეტ-რესურსის მოშლას.“⁹³ თავის მხრივ, რუსეთის მასობრივი მაუწყებლობის საშუალებები საქართველოს ადანაშაულებდნენ ე.წ. „დოს“ იერიშების განხორციელებაში.⁹⁴

უნდა აღინიშნოს, რომ საომარი მოქმედების დასრულების შემდეგ ქართულ ინტერნეტ-რესურსებზე „აპსნი.ჯი“ (www.apsny.ge) და

90 იხ. რუსეთ-საქართველოს კიბერომს აშშ იძიებს (<http://presa.ge/index.php?text=news&i=4413>)

91 იხ. იქვე.

92 იხ. Before the Gunfire, Cyberattacks, JOHN MARKOFF, 12.08.2008 (http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=2&ref=world&oref=slogin&oref=slogin)

93 იხ. <http://www.crime-research.ru/news/13.08.2008/4727/>

94 იხ. <http://www.crime-research.ru/news/12.08.2008/4722/>

„აფხაზეთი.ნეტ“ (www.abkhazeti.net) იერიში კვლავ განხორციელდა⁹⁵, 2008 წლის 21 სექტემბერს კი უკვე ბლოკირებული იყო „ნიუს.ჯი“ (www.news.ge), „ჯიეიჩენ.ჯი“ (www.ghn.ge) და სხვა ქართული საინფორმაციო ინტერნეტ-საიტები.⁹⁶

აღსანიშნავია, რომ 2007 წლის აპრილში ესტონეთის წინააღმდეგ მსგავსი იერიშის შემდეგ ნატოს შვიდი წევრის: გერმანია, სლოვაკეთი, ლატვია, ლიტვა, იტალია და ესპანეთის ხელშეწყობით ესტონეთში დაარსდა კვლევითი ცენტრი. მან მუშაობა სწორედ რუსეთ-საქართველოს ომის შემდეგ, 2008 წლის აგვისტოში დაიწყო. აღნიშნულთან დაკავშირებით „ამერიკის ხმის“ რუსული სამსახურისთვის მიცემულ ინტერვიუში ნატოს პრეს-მდივანმა ჯეიმს აპატურაიმ აღნიშნა, რომ „კიბერდაცვა ნაციონალური უსაფრთხოების განუყოფელი ნაწილია და ზუსტად ამ ნიშნით ეს საკითხი განხილულ იქნა ნატოში და მიღებულ იქნა გადაწყვეტილება ტალინში კვლევითი ცენტრის დაარსების შესახებ. ცხადია, შეუძლებელია განცალკევებით ერთი რომელიმე ქვეყნის კომპიუტერული სისტემის დაცვა, რადგან კიბერშეტევა ატარებს საერთაშორისო ხასიათს. ესტონეთზე განხორციელებული კიბერსაბოტაჟის დროს სამი კვირის მანძილზე იერიში ხორციელდებოდა ათასობით კომპიუტერიდან, რომელიც სხვადასხვა ქვეყანაში იყო განთავსებული. ამის შემდეგ ნატო მივიდა დასკვნამდე, რომ აუცილებელია საერთაშორისო ჩარევის კოორდინირება, საჭიროა ყველა მოკავშირის ძალისხმევის გაერთიანება“.⁹⁷

ესტონეთის გამოცდილება ცხადყოფს რა საფრთხის წინაშე იდგა საქართველო 2008 წლის აგვისტოში. აქედან გამომდინარე, განსაკუთრებული მნიშვნელობა ენიჭება მომხდარ ფაქტზე ქართველი სამართალდამცავი ორგანოების რეაგირებას. ცნობილია, რომ შესაბამის სტრუქტურებში ამ ფაქტზე სისხლისმართლებრივი დევნა არ დაწყებულა. ეს შეიძლება ორგვარად ავსხნათ:

1. განხილულ ქმედებაში არ არის სისხლის სამართლის კოდექსით გათვალისწინებული არცერთი შემადგენლობის ნიშანი, ანუ

95 იხ. http://www.navigator.ge/index.php?lang_id=GEO&sec_id=27&info_id=3610

96 იხ. <http://www.crime-research.ru/news/21.09.2008/4861/>

97 იხ. В Таллине создается информационно-аналитический Центр кибербезопасности НАТО (<http://www.voanews.com/russian/archive/2008-05/2008-05-16-voa4.cfm>).

არ არსებობს სისხლის სამართლის კანონით გათვალისწინებული მართლსაწინააღმდეგო ქმედება;⁹⁸

2. კიბერდანაშაულის მაღალი ლატენტური ხასიათი, სამართალდამცავი ორგანოების სპეციალური მომზადების არქონა, სისხლის სამართლის კანონის კომენტარების სიმწირე, რაც, თავის მხრივ, ქმნის დანაშაულის კვალიფიკაციის პრობლემას.

შევეცდები, უარყო ჩემს მიერ გამოთქმული ორივე ვარაუდი.

იმ დროს, როდესაც ეს კიბერშეტევა განხორციელდა, საქართველოს სისხლის სამართლის კოდექსი არ შეიცავდა 286-ე მუხლს არსებული რედაქციით, ის კომპიუტერული დანაშაულებები, კი რომელსაც კოდექსი ითვალისწინებდა, არ მოიცავდა მსგავსი შინაარსის ქმედებას. კერძოდ, 284-ე მუხლი ითვალისწინებდა კანონით დაცულ ინფორმაციაში არამართლზომიერ შელწევას, 285-ე მუხლი, ეგმ-ის დამაზიანებელი პროგრამის შექმნას ან არსებულ პროგრამაში ცვლილების შეტანას, რამაც გამოიწვია ინფორმაციის განზრახ განადგურება, ბლოკირება და ა.შ. 286-ე მუხლით აკრძალული იყო ეგმ-ის და მისი ქსელის ექსპლუატაციის წესების დარღვევა. როგორც უკვე აღინიშნა, ე.წ. „დოს“ შეტევა არ მოიცავს არც კომპიუტერულ სისტემაში შელწევის და არც მისი დამაზიანებელი პროგრამის შექმნის, გავრცელების და ა.შ. ფაქტს. აქედან გამომდინარე, 2008 წელს სამართალდამცავი ორგანოები კომპიუტერული დანაშაულის ჩადენის ფაქტებზე გამოძიებას ვერ ჩაატარებდნენ. თუმცა ისევე, როგორც დღეს, მაშინაც არსებობდა კოდექსის 318-ე მუხლი, კერძოდ, საბოტაჟი: „საქართველოს დასუსტების მიზნით სახელმწიფო ან სხვა საწარმოს, დაწესებულების, ორგანიზაციის ან სამსახურის ნორმალური ფუნქციონირებისთვის ხელის შეშლა“. საბოტაჟი ამ

98 აღსანიშნავია, რომ დიდ ბრიტანეთში 2006 წლის 8 ნოემბერს მიღებულ იქნა კანონი (Police and Justice Act) რომლის თანახმადაც ე.წ. „დოს“ (Distributed Denial of Service) შეტევა ცალკე დანაშაულადაა გათვალისწინებული და მასზე-სისხლისსამართლებრივი პასუხისმგებლობა განისაზღვრება თავისუფლების აღკვეთით ვადით 10 წლამდე (იხ. <http://www.berr.gov.uk/whatwedo/sectors/infos-ec/infossecadvice/legislationpolicystandards/legislation/computermisuseact/page33363.html>). მსგავსი პრაქტიკა დაამკვიდრა შვედეთმაც, რომელმაც ანალოგური შინაარსის კანონი 2007 წლის 1 ივნისიდან ამოქმედდა (იხ. <http://www.theinquirer.net/en/inquirer/news/2007/02/20/sweden-hans-dos-attacks>)

ფორმით ფორმალურ დანაშაულს წარმოადგენს და იგი დამთავრებულიად ჩაითვლება საქართველოს დასუსტების მიზნით ხელისმეშველი ნებისმიერი ქმედების ჩადენის მომენტიდან, იმისგან დამოუკიდებლად, მოჰყვა თუ არა მას ქვეყნისთვის საზიანო შედეგი.⁹⁹ 318-ე მუხლის მეორე ნაწილი კი პასუხისმგებლობას უკავშირებს კონკრეტულ შედეგს, კერძოდ, „საქართველოს დასუსტების მიზნით სანარმოს, სატრანსპორტო, კავშირგაბმულობის ან მასობრივი მაუწყებლობის საშუალების, გზის, ნაგებობის, ტექნიკის, დოკუმენტის, დიდი რაოდენობით სტრატეგიული ნედლეულის, მასალის ან პროდუქციის, აგრეთვე მოსახლეობისთვის სასიცოცხლო მნიშვნელობის დაწესებულების ან ორგანიზაციის ნორმალური ფუნქციონირებისთვის აუცილებელი, საზოგადოებრივი უშიშროების ან წესრიგის დაცვისთვის განკუთვნილი ან სხვა განსაკუთრებული დანიშნულების ობიექტის დაზიანებას, მწყობრიდან გამოყვანას ან განადგურებას“.

როგორც ვხედავთ, კანონმდებელი საბოტაჟის საგნის საკმაოდ დიდ ჩამონათვალს აკეთებს და მათ შორის მოიხსენიებს კავშირგაბმულობის ან მასობრივი მაუწყებლობის საშუალებას, ასევე, მოსახლეობისთვის სასიცოცხლო მნიშვნელობის დაწესებულების ან ორგანიზაციის ნორმალური ფუნქციონირებისთვის აუცილებელ ობიექტების დაზიანებას, მწყობრიდან გამოყვანას ან განადგურებას¹⁰⁰.

318-ე მუხლის მე-2 ნაწილი სრულად შეესაბამება საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევის არსს. კერძოდ, „დოს“ შეტევის შინაარსს ზუსტად ამათუიშ საიტის მუშაობისთვის ხელის შეშლა წარმოადგენს და მაშინ, როცა შეტევის მიზანი ხდება სამთავრობო და მასობრივი ინფორმაციის საშუალება, მტკიცება, რომ ესაა საქართველოს წინააღმდეგ განხორციელებული საბოტაჟი, დასაბუთებული ხდება. გარდა ამისა, მოხდა მოსახლეობისთვის სასიცოცხლო მნიშვნელობის დაწესებულების და ორგანიზაციების ნორმალური ფუნქციონირებისთვის აუცილებელი, საზოგადოებრივი უშიშროების და წესრიგის დაცვისთვის განკუთვნილი ობიექტის

99 იხ. მ. ლეკვეიშვილი, გ. მამულაშვილი, „დანაშაული სახელმწიფოსა და სასამართლო ხელისუფლების წინააღმდეგ“, გამომც. „მერიდიანი“, 2002წ. თბ. გვ. 41

100 იხ. იქვე გვ. 42

დაზიანება და მწყობრიდან გამოყვანა, რადგან ყველა სამთავრობო საიტი, მით უფრო შინაგან საქმეთა, თავდაცვის სამინისტროს და პრეზიდენტის საიტები, განსაკუთრებით ომის პირობებში, წარმოადგენენ სასიცოხლო ობიექტებს და ემსახურებიან მოსახლეობის სწორი ინფორმაციით აღჭურვას, რათა არ შეიქმნას პანიკა, შესაძლებელი გახდეს ქვეყნის მასშტაბით გადაადგილება და სხვა.

ჩემი აზრით, 2008 წელს განხორციელებულ კიბერერიშიზე შინაგან საქმეთა ორგანოებს გამოძიება უნდა დაენიშნათ საქართველოს სისხლის სამართლის კოდექსის 318-ე მუხლის მე-2 ნაწილით გათვალისწინებული დანაშაულის ჩადენის ფაქტზე. ცნობილია, რომ მსგავს საქმეებზე მტკიცებულების შეგროვება გართულებულია. როცა ვსაუბრობდი რუსულ ინტერნეტ-რესურსზე „სტოპ-ჯორჯია.რუ“ (www.stopgeorgia.ru) ვგულისხმობდი გამოძიებისთვის საინტერესო თუნდაც ერთ ობიექტს, სადაც მიმდინარე მოვლენები პირდაპირ უკავშირდება საქართველოს წინააღმდეგ განხორციელებულ საბოტაჟს. უშუალოდ „სტოპ-ჯორჯია.რუზე“ რეგისტრირებული იმ მომხმარებლების იდენტიფიკაცია, რომლებიც მონაწილეობდნენ საქართველოს წინააღმდეგ საბოტაჟის განხორციელებაში, ტექნიკური სირთულის გამო შესაძლებელია ვერც მომხდარიყო. მიუხედავად ამისა, არსებობდა შანსი ესტონეთის, აშშ-ს და ნატო-ს მოკავშირე სხვა წევრების სპეციალისტების დახმარებით, რომლებიც ისედაც მონაწილეობდნენ საქართველოს პრეზიდენტის და სხვა სახელმწიფო ინტერნეტ-რესურსების დაცვაში, საქართველოს წინააღმდეგ განხორციელებული კიბერერიშის თუნდაც რიგითი წევრის იდენტიფიკაცია მოგვეხდინა.

სისხლის სამართლის ახალი რედაქციის ამოქმედების შემდეგ რამდენად შეესაბამება 286-ე მუხლის მინარსი ე.წ. „დოს“ შეტყვის არსს? ანუ განხილული კაზუსის შემთხვევაში გვაქვს თუ არა სახეზე კომპიუტერული მონაცემის უნებართვო დაზიანება, წაშლა, შეცვლა, დაფარვა, ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია? ე.წ. „დოს“ შეტევა ხორციელდება სპეციალური პროგრამის საშუალებით, რომელიც, თავის მხრივ, უნდა განვიხილოთ როგორც კომპიუტერული მონაცემი. შეტყვისას კი ხდება ამ მონაცემის გადაცემა, რასაც საბოლოოდ მივყავართ კომპიუტერული სისტემის

ფუნქციონირების შეფერხებამდე, მაგრამ უნდა აღინიშნოს, რომ კომპიუტერული მონაცემის უნებართვო გადაცემა, იმ შემთხვევაში თუ იგი არ იწვევს კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვან შეფერხებას, საერთოდ არ განიხილება დანაშაულად. ისიც აღსანიშნავია, რომ ე.წ. „დოს“ შეტევის შემთხვევაში, მართალია, ხორციელდება კომპიუტერული მონაცემის გადაცემა, თუმცა „უნებართვობა“ სახეზე არ გვაქვს, რადგან ე.წ. „დოს“ შეტევა გულისხმობს საიტზე შესვლის ერთდროულად ათასობით მოთხოვნას, რაშიც უკანონო და მფლობელის ნების საწინააღმდეგო არაფერია. უფრო, მეტიც ინტერნეტ-საიტი არის საჯარო ელექტრონული სივრცე, რომლით სარგებლობა ნებისმიერ ინტერნეტ-მომხმარებელს შეუძლია. გამოდის რომ, სისხლის სამართლის კოდექსი არ არ იძლევა ზუსტ განმარტებას და იმ შემთხვევაშიც კი თუ დამტკიცდება, რომ კიბერშეტევის შედეგად სამიზნე კომპიუტერული სისტემის ფუნქციონირება შეფერხდა განზრახ და მნიშვნელოვნად, ამ ქმედებებს 286-ე მუხლით ვერ დავაკვალიფიცირებთ.

მიზანშეწონილია, რომ ე.წ. „დოს“ შეტევა განხილულ იქნას როგორც დამოუკიდებელი კომპიუტერული დანაშაული და მასში არ მიეთითოს დათქმა „მნიშვნელოვან შეფერხებაზე“, რადგან საკმარისია მივუთითოთ „კომპიუტერული სისტემის ფუნქციონირების შეფერხება“, ხოლო თუ კანონმდებელი აუცილებლად მიიჩნევს ზემოაღნიშნული ტერმინის გამოყენებას, მაშინ შეიტანოს მეტი სიცხადე მის განმარტებაში და მუხლს დაურთოს შესაბამისი შენიშვნა.

ახლა განვიხილოთ, მეორე, მედარებით ლოკალური მნიშვნელობის კაზუსი. საქართველოს შინაგან საქმეთა სამინისტროს ოფიციალურ ვებ-გვერდზე გამოქვეყნდა შემდეგი სახის ინფორმაცია: „2012 წლის 1 სექტემბერს შინაგან საქმეთა სამინისტროში დაიწყო გამოძიება სხვადასხვა ინტერნეტ-პორტალზე კიბერშეტევის განხორციელების ფაქტთან დაკავშირებით. ჩატარებული ოპერატიულ-სამძებრო ღონისძიების შედეგად, პოლიციის მიერ დაკავებულია მოქალაქე შალვა ბენდელიანი, რომელსაც ბრალი ედება კომპიუტერული პროგრამის უკანონოდ დამზადებასა და გავრცელებაში, რამაც გამოიწვია ინტერნეტ-პორტალების ფუნქციონირების განზრახ შეფერხება. შალვა ბენდელიანი ბრალდებულია საქართვე-

ლოს სისხლის სამართლის კოდექსის 285-ე მუხლის პირველი ნაწილით გათვალისწინებული დანაშაულის ჩადენაში¹⁰¹."

ამის პარალელურად ტელევიზიით და სხვა საინფორმაციო საშუალებით გავრცელდა ინფორმაცია, რომ საინფორმაციო პორტალები „პრესა.ჯი“ (presa.ge) და „დრონი.ჯი“ (droni.ge) ე.წ. დოს შეტყვის შედეგად პარალიზებულია. შალვა ბენდელიანს სწორედ ამ საიტების მწყობრიდან გამოყვანაში ედებოდა ბრალი. „კავკასიის ინტერნეტ მედია ჯგუფის“ ხელმძღვანელის განცხადებით, საინფორმაციო პორტალებზე შეტევა 31 მაისს დაიწყო. ეს იყო საკმაოდ კარგად ორგანიზებული, მძლავრი შეტევა, რამაც გამოიწვია ამ საიტების პარალიზება. ტექნიკურმა ჯგუფმა რამდენჯერმე შეძლო საიტების ჩართვა, თუმცა განმეორებითი შეტყვის გამო, ისინი კვლავ მიუწვდომელი გახდა. მისი აზრით, საქმე ე.წ. „დოს“ შეტევასთან გვაქვს.¹⁰² ქართული ვებ-გვერდების რეიტინგის მთელელი საიტის „ტოპ.ჯის“ (top.ge) ადმინისტრატორის განცხადებით: „პრესა.ჯი“ და „დრონი.ჯი“ გათიშული, კი არ არის, მათზე ხორციელდება „დოს“ შეტევა, რაც აფერხებს ამ საიტებზე შესვლას და შეიძლება ათი ცდიდან ერთხელ შეხვიდე. მსგავსი ტიპის შეტევა გულისხმობს, რომ ამ საიტების სერვერზე იგზავნება ერთდროულად ათასობით მოთხოვნა (საიტზე შესვლის მცდელობა), რასაც სერვერი ვერ უძლებს და ჩვეულებრივ მომხმარებელს არ აძლევს საიტზე შესვლის საშუალებას.¹⁰³

აღნიშნული ფაქტზე ჩატარდა გამოძიება და საბოლოოდ, შალვა ბენდელიანის ქმედება სასამართლომ შეაფასა, როგორც 285-ე მუხლის პირველი ნაწილით გათვალისწინებული დანაშაული.

სასამართლოს განაჩენში ვკითხულობთ: „შალვა ბენდელიანმა უნებართვოდ დაამზადა, ინახავდა და 2012 წლის 1 აგვისტოს სოცია-

101 აღნიშნულ დანაშაულიდან დაკავშირებით, არსებობს ძალაში შესული სასამართლოს განაჩენი, რომელსაც ნაშრომში განვიხილავ. ამიტომ ნაშრომში მოყვანილ მსს-ს ოფიციალურ განცხადებაში და კაზუსის განხილვაში ყველა თარიღი, დამნაშავის ვინაობა და სხვა საიდენტიფიკაციო მონაცემი შეცვლილია. ასევე, შეგნებულად არაა მითითებული მსს-ს ოფიციალური განცხადების ნყარო.

102 იხ. <http://netgazeti.ge/GE/105/News/10125/>

103 იხ. იქვე

ლურ ქსელ ფეისბუქის საკუთარ გვერდზე განათავსა კომპიუტერული პროგრამა, რომელიც გააქტიურების შემდეგ კომპიუტერულ სისტემაში ქმნის და თავის მხრივ ააქტიურებს კომპიუტერის დამაზიანებელ სამ დაზიანებით ფაილს.

კიბერნეტიკული ექსპერტიზის დასკვნით, შალვა ბენდელიანის მიერ დამზადებული პროგრამის საშუალებით შესაძლებელი იყო მას მოეხდინა სხვისი კომპიუტერის ინფიცირება და მათი ინტერნეტ-რესურსების გამოყენება (მართვა), აგრეთვე შეეძლო ინტერნეტ-საიტების მუშაობის შეფერხება და დაზიანება.

გარდა ამისა, შალვა ბენდელიანმა მოუწოდა ინტერნეტ-მომხმარებლებს აღნიშნული კომპიუტერული პროგრამით განეხორციელებინათ კიბერშეტევა საინფორმაციო ინტერნეტ-საიტებზე „პრესა.ჯი“, „დრონი.ჯი“ და „ნიუს.ჯი“, რაც მათი მუშაობის შეფერხებას გამოიწვევდა.

ამის შემდეგ სასამართლო ასკვნის, რომ შალვა ბენდელიანმა ჩაიდინა კოდექსის 285-ე მუხლის პირველი ნაწილით გათვალისწინებული დანაშაული, ე.ი. კომპიუტერული პროგრამის უნებართვო დამზადება, შენახვა და გავრცელება კიბერდანაშაულის თავით გათვალისწინებული დანაშაულის ჩადენის მიზნით. ამ შეფასებას სრულიად ვეთანხმები, მაგრამ სად დაიკარგა 286-ე მუხლის მე-2 ნაწილით გათვალისწინებული დანაშაული? ჩამინ, როცა სასამართლო ხაზგასმით მიუთითებს: შალვა ბენდელიანმა მოუწოდა ინტერნეტ-მომხმარებლებს აღნიშნული კომპიუტერული პროგრამით განეხორციელებინათ კიბერშეტევა საინფორმაციო ინტერნეტ-საიტებზე, რაც მათი მუშაობის შეფერხებას გამოიწვევდა. გამოიწვია კიდეც. ამას მონაშობს ზემოთ მოყვანილი ამონარიდები, რომლის ანალიზითაც ჩანს, რომ განხორციელებულმა კიბერშეტევებმა შეაფერხა „პრესა.ჯის“ და „დრონი.ჯის“ მუშაობა.

განხილულ კაზუსში, ერთი შეხედვით, ადვილია აღმოვაჩინოთ 286-ე მუხლის მე-2 ნაწილით გათვალისწინებული დანაშაულის ნიშნები, თუმცა, კვლავ კითხვის ნიშნის ქვეშ დგება ქმედების „უნებართვობა“. მაშინ, როცა საინფორმაციო ინტერნეტ-რესურსებით სარგებლობა არაა კანონით აკრძალული, ნებისმიერ პირს უნებართვის გარეშე შეუძლია შევიდეს და მოინახულოს ის, როგორ ვისაუბროთ „უნებართვობაზე“? ჩემი აზრით, როდესაც საუბარია ე.წ.

„დოს“ შეტევაზე, კანონი ტერმინ „უნებართვოს“ საერთოდ არ უნდა იყენებდეს.

შალვა ბენდელიანი 286-ე მუხლის მე-2 ნაწილით გათვალისწინებული დანაშაული არ შეერაცხა, რადგან საქართველოს მთავარი პროკურატორის შუამდგომლობაში საქმის საპროცესო შეთანხმებით დასრულებასთან დაკავშირებით, სწორად იყო აღწერილი მხოლოდ 285-ე მუხლის 1-ლი ნაწილით გათვალისწინებული დანაშაული. თუმცა, არ უნდა დაევიწყოთ, 285-ე მუხლის დათქმა, რომელიც უკავშირდება დამნაშავეს მიზანს. მართალია, შ. ბენდელიანს განზრახული ჰქონდა კიბერდანაშაულის თავით გათვალისწინებული დანაშაულის ჩადენა, მაგრამ კერძო კომუნიკაციის საიდუმლოების ხელყოფა რა კავშირშია მასთან? აღნიშნულ ხარვეზზე წიგნის შესაბამის ნაწილში უკვე ვისაუბრეთ, ამიტომ მასზე აღარ შევჩერდები.

განვიხილოთ, სხვა სრულიად განსხვავებული ტიპის ორი კაზუსი სასამართლო პრაქტიკიდან, რომელიც უკავშირდება 286-ე მუხლის მე-3 ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული დანაშაულის ჩადენას. 2010 წლის სასამართლოს განაჩენით დამნაშავედ იქნა ცნობილი სამი პიროვნება კომპიუტერული მონაცემის უნებართვო შეცვლის გამო.¹⁰⁴ თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიამ 2010 წლის 17 დეკემბერს განიხილა სისხლის სამართლის საქმე ბრალდებულების ზ. ნოწორიას, დ. იაშვილის და ნ. კაკაბაძის წინასწარი შეთანხმებით ჯგუფის მიერ კომპიუტერული მონაცემის შეცვლასთან დაკავშირებით. განაჩენში ვკითხულობთ: „დ. იაშვილს განზრახული ჰქონდა რა წინასწარი შეთანხმებით ჯგუფის მიერ კომპიუტერული მონაცემის უნებართვო შეცვლა, 2010 წლის 11 ივლისს დაუკავშირდა შპს „ნათიას“ დირექტორ ნათია ნათელაძეს, რომელსაც გარკვეული ანაზღაურების სანაცვლოდ შესთავაზა საკონტროლო-სალარო აპარატის ფისკალური მექანიზმების უკანონო შეცვლა. .ნ. ნათელაძემ შეიტყო რა დ. იაშვილის მხრიდან კანონსაწინააღმდეგო ქმედების შესახებ, 2010

104 კაზუსში დასახელებული ყველა თარიღი, ნომერი, დასახელება და პირის ვინაობა შეცვლილია.

ნლის 17 ივლისს განცხადებით მიმართა ფიხანსთა სამინისტროს საგამოძიებო სამსახურის საგამოძიებო დეპარტამენტის თბილისის მთავარ სამმართველოს, სადაც აღნიშნულ ფაქტთან დაკავშირებით დაიწყო გამოძიება და დამნაშავე პირების გამოვლენის მიზნით დაიგეგმა შესაბამისი ოპერატიული ღონისძიებები, რომელშიც ნებაყოფლობით ჩაერთო ნ. ნათელაძე."

ამის შემდეგ, ნ. ნათელაძე და დ. იაშვილი შეთანხმდნენ, რომ სალარო-აპარატის ფისკალური ქეხიერების შეცვლის და ახალი ე.წ. „Z“ მაჩვენებელი დამზადების შემდეგ დ. იაშვილი მიიღებდა ანაზღაურებას 3000 ლარის ოდენობით.

დ. იაშვილი დაუკავშირდა ზ. წონორიას და ს. კაკაბაძეს, რომლებიც გარკვეული ანაზღაურების სანაცვლოდ დაითანხმა დანაშაულში თანამონაწილეობაზე. კერძოდ, ზ. წონორია და ნ. კაკაბაძე უნდა შეხვედროდნენ ნ. ნათელაძეს, გამოეცხადებინათ საკონტროლო-სალარო აპარატი და მიეტანათ დ. იაშვილთან. როდესაც დ. იაშვილი დაასრულებდა მონაცემების შეცვლას, მათ ისევე უკან ნ. ნათელაძესთან უნდა წაეღოთ იგი.

რამდენიმე დღის შემდეგ ს. ნათელაძეს დაუკავშირდნენ ნ. კაკაბაძე და ზ. წონორია, რომლებმაც გადასცეს საკონტროლო-სალარო აპარატი, სადაც ნაცვლად 201345 ლარისა, ნაეჭრი თანხის სახით დაფიქსირებული იყო 50654 ლარი და ახალი ე.წ. „Z“ მაჩვენებელი.

ვინაიდან ნ. ნათელაძე წინასწარ იყო შეთანხმებული საგამოძიებო ორგანოებთან და თანამშრომლობდა მათთან, მისი დაკავება არ მომხდარა. ზ. წონორია და ნ. კაკაბაძე კი დაკავებული იქნენ. მოგვიანებით, დააკავეს დ. იაშვილიც, რომელმაც უშუალოდ განახორციელა კომპიუტერული მონაცემის, კერძოდ კი ნაეჭრი თანხის მაჩვენებლის შეცვლა. ყველა მათგანმა ჩადენილი დანაშაული სრულად აღიარა. დ. იაშვილს მიესაჯა 4 წლით თავისუფლების აღკვეთა და დამატებითი სასჯელის სახით 10000 ლარიანი ჯარიმა, ხოლო დანარჩენ ორს საპროცესო შეთანხმების საფუძველზე 4 წლით თავისუფლების აღკვეთა შეეცვალათ ერთწლიანი თავისუფლების აღკვეთით და 3 წლიანი პირობითი მსჯავრით. დამატებით სასჯელად განესაზღვრა 10000 ლარიანი ჯარიმა."

აღნიშნული გადანაცვლებები მოგვიანებით სააპელაციო სასამართლომ ძალაში დატოვა.

საინტერესოა, ვიმსჯელოთ ამ კონკრეტული დანაშაულებრივი ქმედების კვალიფიკაციის პრობლემაზე და სისხლის სამართლის 286-ე მუხლის პრაქტიკაში გამოყენების სირთულეზე. თბილისის საქალაქო სასამართლო მოცემულ საქმესთან დაკავშირებით განმარტავდა, რომ სამივე ბრალდებულმა ჩაიდინა საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლის მე-3 ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ქმედება, კერძოდ, წინასწარი შეთანხმებით ჯგუფის მიერ კომპიუტერული მონაცემის უნებართვო შეცვლა. სასამართლო აღნიშნავს, რომ ბრალდებულებმა სრულად ცნეს თავი დამნაშავედ მათთვის ინკრიმინირებულ ქმედებაში. ასევე, უდავოა, რომ დ. იაშვილმა შეცვალა საკონტროლო-სალარო აპარატში არსებული მონაცემი. როგორც ვიცით, კოდექსის 286-ე მუხლით დასჯადია: „კომპიუტერული მონაცემის უნებართვო დაზიანება, ნაშლა, შეცვლა ან დაფარვა“. კოდექსის 284-ე მუხლის შენიშვნის მე-3 ნაწილის შესაბამისად ტერმინი „უნებართვო“ განმარტებულია, რომ უნებართვო გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისთვის.

განაჩენში ვკითხულობთ, რომ ბრალდებულებმა ნ. ნათელაძეს შესთავაზეს და არა აიძულეს სალარო აპარატის მონაცემების შეცვლა გარკვეული ანაზღაურების სანაცვლოდ. საქმის მასალებიდან, კერძოდ, დ. იაშვილის დაკითხვის ოქმიდან ირკვევა, რომ სალარო აპარატის მონაცემების შეცვლა თავდაპირველად თავად ნათელაძემ სთხოვა იაშვილს და არა პირიქით.

როდესაც განაჩენში საუბარია კომპიუტერული მონაცემის უნებართვო შეცვლაზე, სასამართლოს მინიმუმ უნდა აღენიშნა რა იგულისხმა „უნებართვი“ ამ კონკრეტულ კაზუსთან მიმართებაში, რადგან როგორც ვიცით, „უნებართვო“ შეიძლება განიმარტოს, როგორც „უკანონო“ ასევე, როგორც უფლების მფლობელის ნების სანინაალმდეგო, ანუ როცა უფლების მფლობელს პირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისთვის. ეს მნიშვნელოვანი გარემოებაა, რომელზეც გამოძიების ორგანოებს, პირველი ინსტანციის და სააპელაციო სასამართლოს არ უმსჯელია, ამიტომ შევეცდები ეს საკითხი უფრო დეტალურად განვიხილო.

განაჩენში ვკითხულობთ: „2010 წლის 11 ივლისს ქ. თბილისში ახმეტელის თეატრის შესასვლელთან დ. იაშვილი შეხვდა ნ. ნათელაძეს“.

ლაძეს და შესთავაზა, რომ 3000 ლარის სანაცვლოდ შეცვლიდა შპს „ნათიაზე“ რეგისტრირებულ საკონტროლო-სალარო აპარატის ფისკალურ მეხსიერებას და ასევე დაამზადებდა ახალ ე.წ. „Z“ მაჩვენებელს, რაზედაც ნ. ნათელაძემ განუცხადა თანხმობა და გადასცა ხსენებული საკონტროლო-სალარო აპარატი.“

საქმეში არსებული მასალებით დადასტურებულია, რომ შპს „ნათიას“ დირექტორი და 100 პროცენტის ნილის მფლობელი იყო თავად ნ. ნათელაძე.

ვინ შეიძლება ჩაითვალოს სალარო აპარატის მონაცემზე უფლების მფლობელად? კომპიუტერული მონაცემი არის კომპიუტერული სისტემის შემადგენელი ნაწილი, ხოლო მასზე უფლება გააჩნია ამ სისტემის მესაკუთრეს ან კანონიერ მფლობელს, თუმცა გარდა ამისა, მის მფლობელს კანონის წინაშე, კერძოდ კი საგადასახადო ორგანოს მიმართ აქვს კანონისმიერი ვალდებულება გადაიხადოს კანონით დადგენილი გადასახადი, რომლის გამოთვლისთვისაც მნიშვნელოვანია საკონტროლო-სალარო აპარატის მონაცემები. ამდენად, გამოდის, რომ მოცემულ კაზუსში ტერმინ „უნებარსოვში“ სასამართლომ იგულისხმა არა ამ მონაცემის მფლობელის ნების საწინააღმდეგოდ მის მფლობელობაში არსებული კომპიუტერული სისტემის მონაცემის შეცვლა, არამედ, კომპიუტერული მონაცემის უკანონო შეცვლა, რადგან საქმის მასალებიდან ირკვევა, რომ ნ. ნათელაძე, ანუ მფლობელის თანხმობა კომპიუტერული მონაცემის შეცვლაზე არსებობდა. თუ სასამართლომ „უნებარსოვში“ უკანონო იგულისხმა, სახეზე უნდა ჰქონოდა კანონი, რომლის მიხედვითაც აკრძალული იქნებოდა კონკრეტული მინაარსის კომპიუტერული მონაცემის შეცვლა. ჩემი აზრით, სასამართლო ვალდებული იყო დაეზუსტებინა ეს გარემოება, რადგან რთულია დავადგინოთ კონკრეტულად რაში გამოიხატა უკანონობა. მივეყვით თანმიმდევრულად:

სისხლის სამართლის კოდექსის 210-ე მუხლით: „ყალბი საკრედიტო ან საანგარიშსწორებო ბარათის, სხვა საგადასახადო დოკუმენტის ან ქონებრივი უფლებამოსილების დამადასტურებელი ისეთი დოკუმენტის დამზადება ან შეძენა გასაღების ან გამოყენების მიზნით, გასაღება ან გამოყენება, რომელიც არ არის ფასიანი ქაღალდი.“

ბუნებრივია, ამ მუხლს განხილულ შემთხვევაში ვერ გამოვიყენებთ. მართალია, კომპიუტერული მონაცემის შეცვლა შეგვიძლია

გავუიგივოთ მონაცემის გაყალბებას. მაგრამ სახეზე არ გვაქვს მუხლში ჩამოთვლილი საკრედიტო და საანგარიშსწორებო ბარათი, საგადასახადო ან სხვა დოკუმენტი, ვინაიდან, საკონტროლო-სალარო აპარატი ასეთად არ მიიჩნევა. საქართველოს ფინანსთა მინისტრის 2006 წლის 10 მარტის №186 ბრძანებით დამტკიცებული იყო საკონტროლო-სალარო აპარატის ექსპლუატაციის (გამოყენების) წესები, შესაბამისად საკონტროლო-სალარო აპარატი განიმარტებოდა როგორც:

„ფისკალური ჩეხიერების და შესაბამისი პროგრამული უზრუნველყოფის მექანიზმების დამოუკიდებლად მომუშავე, ასევე პროგრამულ-ტექნიკურ კომპლექსში ჩართული ელექტრონული მონაცემების, რომელიც გაჩიზნულია მომხმარებლის მიერ ნაღდი ფულით განხორციელებული გადახდების შესახებ მონაცემების რეგისტრაციისათვის, მათი შენახვისთვის და ამოგეჭდვის გზით შესაბამისი ანგარიშგებითი დოკუმენტების ფორმირებისთვის (მათ შორის სპეციალური მონაცემების საშუალებით)“. დღეის მდგომარეობით, აღნიშნული ბრძანება გაუქმებულია საქართველოს ფინანსთა მინისტრის 2010 წლის 31 დეკემბრის №994 ბრძანებით, რომლითაც დამტკიცდა „საგადასახადო კონტროლის განმარტებული პირის შერჩევისა და საგადასახადო კონტროლის განხორციელების, მიმდინარე კონტროლის პროცედურების ჩატარების, სასაქონლო-მატერიალურ ფასეულობათა ჩამონერის, საგადასახადო დავალიანების გადახდების უზრუნველყოფის ღონისძიებების განხორციელების, სამართალდარღვევათა საქმისწარმოების წესი“.

ახალი წესი სხვა საკითხებთან ერთად არეგულირებს საკონტროლო-სალარო აპარატის ექსპლუატაციის საკითხებს, თუმცა მასში სალარო-აპარატის ცნება განმარტებული არ არის. მიუხედავად ამისა, შეგვიძლია დავასკვნათ, რომ სალარო აპარატში ფორმირებული ინფორმაცია გამოიყენება ანგარიშგებითი დოკუმენტების შექმნისთვის, გადახდების შესახებ მონაცემების რეგისტრაციისთვის და ა.შ. ამდენად, ჩას, როგორც საგადასახადო დოკუმენტს ან საანგარიშსწორებო ბარათს ვერ განვიხილავთ. შესაბამისად, სალარო აპარატის კომპიუტერული მონაცემის შეცვლა სისხლის სამართლის კანონით აკრძალული ქმედება არაა და ამ კუთხით უკანონობაზე ვერ ვისაუბრებთ.

აღსანიშნავია, რომ ფინანსთა მინისტრის 2010 წლის 31 დეკემბრის №994 ბრძანებით დამტკიცებული წესის მე-20 მუხლით განსაზღვრულია საკონტროლო სალარო აპარატის ექსპლუატაციის პირობები. აღსანიშნავია, რომ ამ მუხლში სალარო აპარატში ასახული მონაცემების, მათ შორის „Z“ მაჩვენებლის, მეცვლის აკრძალვაზე პირდაპირ მინიშნება არ გვხვდება. 20-ე მუხლის მე-7 პუნქტით განსაზღვრულია მოლარე ოპერატორის, ანუ იმ პირის ვალდებულება ვინც გადასახადის გადამხდელის მიერ გასაზღვრულია სალარო აპარატთან მუშაობის უფლების მქონე პირად. მე-7 პუნქტის „ვ“ ქვეპუნქტში აღნიშნულია, რომ: „თავისი სამუშაო ცვლის ბოლოს ამობეჭდოს „Z“ ანგარიში და დღის გასამავლობაში შედგენილი აქტები გადასცეს შესაბამისად უფლებამოსილ პირს. ყოველი „Z“ ანგარიშის ამობეჭდვის შემდეგ, შესაბამის ფორმებში უზრუნველყოს ამ საკონტროლო სალარო აპარატის მიხედვით მაჯამებელი მრიცხველის ჩვენების (გაუნაშთავი ჯამის) დაფიქსირება.“ ეს ვალდებულება, ისევე როგორც სალარო აპარატის ექსპლუატაციის წესებთან დაკავშირებული სხვა ვალდებულებების შესრულება, ეკისრება მოლარე ოპერატორს. ეს გარემოება იმითაა მნიშვნელოვანი, რომ თუ სასამართლო უნებართვოში გულისხმობდა უკანონოს, უნდა შეეფასებინა ბრალიც. თუ დ. იაშვილს და მის თანამზრახველებს არ ეკისრებოდათ რაიმე ვალდებულება, განა შესაძლებელია მის შესრულებაზე მოვთხოვოთ პასუხი? აქ საუბარი კანონის არცოდნაზე არ არის. მოქმედი კანონმდებლობით დადგენილია კონკრეტული წესები და ასევე, მათ შესრულებაზე პასუხისმგებელი პირი. ასეთ, პირობებში როგორ შეიძლება ჩაითვალოს უკანონოდ ისეთი ქმედების ჩადენა, რომელიც კანონით აკრძალული არაა? ჩემს პოზიციას ამყარებს საგადასახადო კოდექსიც. კერძოდ, 281-ე მუხლით აკრძალულია საკონტროლო-სალარო აპარატის გამოყენების წესის დარღვევა. ამ წესების დარღვევად განიხილება: მომხმარებელთან ნაღდი ფულით ანგარიშსწორებისას საკონტროლო-სალარო აპარატის გარეშე მუშაობა, მისი გამოყენებლობა, დაკარგვა, ჩეკში ფაქტობრივად გადახდილზე ნაკლები თანხის ჩვენება და ავტოგასამართ სადგურში მადოზირებელი ან/და პრიცხველი მექანიზმის საგადასახადო ორგანოს ლუქის გარეშე ან დაზიანებული ლუქით საქმიანობა. როგორც ვხედავთ, სალარო აპარატში ასახული მონაცე-

მეზის შეცვლის აკრძალვას ვერც ამ მუხლში ვხვდებით. გარდა ამისა, ამ მუხლით გათვალისწინებული დარღვევის სუბიექტი შეიძლება იყოს გადასახადის გადამხდელი ის პირი, ვინც ახორციელებს მომხმარებელთან ნაღდ ანგარიშსწორებას.

მოცემული მსჯელობიდან გამომდინარე მიმაჩნია, რომ კაზუსში დასახელებულ პირებს არ ჩაუდენიათ სისხლის სამართლის კოდექსის 286-ე მუხლით გათვალისწინებული დანაშაული, რადგან მათ არ ჩაუდენიათ კომპიუტერული მონაცემის უნებართვო, კერძოდ, უკანონო შეცვლა და არც სალარო აპარატის მფლობელის ნების საწინააღმდეგო ქმედებას ჰქონია ადგილი, რადგან საქმის მასალებიდან ნათლად ჩანს, რომ ნ. სათელაძე კომპიუტერული მონაცემის შეცვლაზე თანახმა იყო.

ვინაიდან, ნ. სათელაძე კანონით დადგენილი წესით თანამშრომლობდა საგადასახადო ორგანოებთან, ვერც მისი ქმედების დანაშაულებრივ ხასიათზე ვისაუბრებთ. ჩემი აზრით, მსგავს ქმედებაში სისხლის სამართლით გათვალისწინებული დანაშაულის ძიება არამართებულია.

იმ შემთხვევაში თუ კომპიუტერული მონაცემის შეცვლის შედეგად განხორციელდება გადასახადების დაფარვა, საგადასახადო ორგანოში მცდარი მონაცემების წარდგენა და ა.შ. გადამხდელის მიმართ გამოყენებულ უნდა იქნეს საგადასახადო კოდექსით გათვალისწინებული ზომები.

გარდა ამისა, სასამართლომ განაჩენში გამოიყენა 286-ე მუხლის მე-3 ნაწილი, რაც წინასწარი შეთანხმებით ჯგუფის მიერ კომპიუტერული მონაცემის ისეთ უნებართვო შეცვლას გულისხმობს, რამაც კომპიუტერული სისტემის განზრახ მნიშვნელოვანი შეფერხება გამოიწვია. საკითხავია, რაში გამოიხატა ეს მნიშვნელოვანი შეფერხება? ამასთან დაკავშირებით სასამართლო არაფერს მიუთითებს. ჩემი აზრით, საქმის მასალებიდან გამომდინარე კომპიუტერული სისტემის ფუნქციონირების შეფერხების ფაქტი საერთოდ არ დასტურდება. საკონტროლო-სალარო აპარატის კომპიუტერული სისტემის მუშაობის შეფერხებად უნდა ჩაგვეთვალოს ის გარემოება, თუ სალარო აპარატი გამოვიდოდა მწყობრიდან და ვეღარ შეასრულებდა იმ ფუნქციებს, რომლითაც ტექნიკურად და პროგრამულადაა აღჭურვილი. მაგალითად, შეუძლებელი გახდებ-

ბოდა ჩეკის ამობეჭდვა, გადახდების შესახებ ინფორმაციის რეგისტრაცია და სხვა. განხილულ საქმეში ამის დამადასტურებელი მტკიცებულება წარმოდგენილი არ არის და შესაბამისად, თუ არ დასტურდება ზოგადად კომპიუტერული სისტემის ფუნქციონირების შეფერხების ფაქტი, როგორ შეიძლება ვისაუბროთ, მნიშვნელოვანი იყო თუ არა ის?

განაჩენში სხვა ბუნდოვან შეფასებასაც ვხვდებით. ზ. წონორია, დ. იაშვილი და ნ. კაკაბაძე პასუხისგებაში მიეცნენ წინასწარი მეთანხმებით ჯგუფის მიერ კომპიუტერული მონაცემის უნებართვო შეცვლის გამო. განაჩენიდან ნათლად ჩანს, რომ თანამსრულებლობაზე საუბარი რთულია, რადგან უშუალოდ კომპიუტერული მონაცემის შეცვლა დ. იაშვილის მიერ განხორციელდა. კოდექსის 24-ე მუხლში განმარტებულია თანამონაწილეობის სახეები. მუხლის 1-ლი ნაწილის შესაბამისად ორგანიზატორია ის, ვისც მოაწყო დანაშაულის ჩადენა.

ო. გამყრელიძის აზრით, „ეს იმას ნიშნავს, რომ დამნაშავე წინასწარ დაგეგმავს დანაშაულს. ორგანიზატორი შეიმუშავებს დანაშაულის ჩადენის გეგმას და სხვა მონაწილეებს აუხსნის როგორ უნდა იმოქმედონ¹⁰⁵. აქედან გამომდინარე, ჩემი აზრით, დ. იაშვილი უნდა განვიხილოთ დანაშაულის ორგანიზატორად, რადგან მან მიიღო გადაწყვეტილება დანაშაულის ჩასადენად, შემდეგ დაგეგმა დანაშაული და ზ. წონორიას და ნ. კაკაბაძეს აუხსნა, როგორ უნდა ემოქმედათ.

ო. გამყრელიძის აზრით, დახმარება ორი სახისაა ფიზიკური და ფსიქიკური. ფიზიკური დახმარება უნდა განვასხვაოთ ამსრულებლობისგან. ამსრულებელი კოდექსის კერძო ნაწილის მუხლით აღწერილ ქმედების შემადგენლობას ახორციელებს მთლიანად ან ნაწილობრივ, დამხმარე კი შემადგენლობის არც ერთ ნაწილს არ ასრულებს¹⁰⁶.

105 იხ. ო. გამყრელიძე, „საქართველოს სისხლის სამართლის კოდექსის განმარტება“, ზოგადი ნაწილი, I ნიჭი, საქართველოს მსჯენიერებათა აკადემიის თინათონ ნერეთლის სახელობის სახელმწიფოსა დ. სამარილის ინსტიტუტი, თბ 2005წ. გვ. 192

106 იხ. იქვე გვ. 198

განხილული კაზუსიდან ნათლად ჩანს, რომ ზ. ნონორიას და ნ. კაკაბაძეს არ განუხორციელებიათ კერძო ნაწილით გათვალისწინებული ქმედება, მათ მხოლოდ დახმარება აღმოუჩინეს დ. იაშვილს, ამდენად, ისინი უნდა განვიხილოთ, როგორც ფიზიკური დამხმარეები და არა თანამსრულებლები.

კოდექსის 25-ე მუხლის მე-3 ნაწილის მიხედვით, ორგანიზატორის, ნამქეზებლის და დამხმარის სისხლისსამართლებრივი პასუხისმგებლობა განისაზღვრება ამ კოდექსის შესაბამისი მუხლით, ამ მუხლზე მითითებით. გარდა იმ შემთხვევისა, როცა ისინი იმავდროულად დანაშაულის თანამსრულებლები იყვნენ. ვინაიდან, ზ. ნონორია და ნ. კაკაბაძე თანამსრულებლები არ ყოფილან, ბუნებრივია, სასამართლოს განაჩენში მათთვის დადგენილ სასჯელში, გარდა 286-ე მუხლისმე-3 ნაწილის „ა“ ქვეპუნქტისა, უნდა მიეთითებინა 25-ე მუხლიც, თუმცა ეს არ გაუკეთებია. გამოდის, რომ სასამართლომ ზ. ნონორია და ნ. კაკაბაძე თანამსრულებლებად მიიჩნია, რასაც ვერ დავეთანხმები, რადგან საქმის მასალებიდან ირკვევა, რომ ზ. ნონორია და ნ. კაკაბაძე ასრულებდნენ შუამავლის ფუნქციას, მათ გადაქონდათ სალარო აპარატი ერთი მისამართიდან მეორეში, მონაცემებს კი უშუალოდ დ. იაშვილი ცვლიდა.

სასამართლომ სწორად შეაფასა დ. იაშვილის, ზ. ნონორიას და ნ. კაკაბაძის ქმედება, როგორც წინასწარი შეთანხმებით ჯგუფის მიერ ჩადენილი დანაშაული, რადგან კოდექსის 27-ე მუხლის მე-2 ნაწილის მიხედვით, დანაშაული ჯგუფის მიერ წინასწარი შეთანხმებითაა ჩადენილი, თუ მასში მონაწილენი წინასწარ შეკავშირდნენ დანაშაულის ერთობლივად ჩასადენად. ამასთან, ო. გამყრელიძის აზრით, „თუ 27-ე მუხლის მე-2 ნაწილის ტექსტს დაეაკვირდებით, იმ დასკვნამდე უნდა მივიდეთ, რომ აქ თანამსრულებლობა აუცილებელი არ არის და ჯგუფის წევრთა შორის მხოლოდ ერთი შეიძლება იყოს ამსრულებელი.“¹⁰⁷

მართალია, არ ყოფიარებ იმ აზრს, რომ დ. იაშვილმა და მისმა დამხმარეებმა ჩაიდინეს 286-ე მუხლით გათვალისწინებული დანა-

107 იხ. ო. გამყრელიძე, „საქართველოს სისხლის სამართლის კოდექსის განმარტება“, ზოგადი ნაწილი, I ნიჭი, საქართველოს მეცნიერებათა აკადემიის თინათინ წერეთლის სახელობის სახელმწიფოსა და სამართლის ინსტიტუტი, თბ. 20056. გვ. 207

შაული, მაგრამ რადგან სასამართლომ ეს ასე მიიჩნია, მაშინ განაჩენში გარდა 286-ე მუხლისმე-3 ნაწილის „ა“ ქვეპუნქტისა, უნდა მიეთითებინა 25-ე მუხლიც.

სამართალწარმოების პრაქტიკაში მსგავსი ქმედების, ანუ კომპიუტერული მონაცემის შეცვლის ფაქტის ბუნდოვანი კვალიფიკაციის სხვა შემთხვევებიც გვხვდება. საუბარია საქართველოს მთავარი პროკურატურის საგამოძიებო პრაქტიკაზე¹⁰⁸. მაგალითად, ერთ-ერთი საქმის მასალებით ირკვევა, რომ დაკავებულ იქნა რამდენიმე პირი, რომლებსაც ბრალი ედებოდათ 286-ე მუხლის მე-3 ნაწილს „ა“ ქვეპუნქტით, მე-19, 24-ე და 180-ე მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული დანაშაულის ჩადენაში. ყველა პირის მიმართ საქმე დასრულდა საპროცესო შეთანხმებით. განაჩენში ვკითხულობთ: დ. გეჯაძემ ზ. მუსერიძესთან და ნ. კალანდიასთან წინასწარი შეთანხმებით, 2010 წლის 17 დეკემბერს 300 ლარის საფასურად, „მერსედესის“ მარკის ავტომანქანაზე კომპიუტერული ჩარევის გზით შეამცირა ავტომობილის გარბენის საერთო მანძილის მაჩვენებელი 300235 კილომეტრიდან 25764 კილომეტრამდე, რითაც აღნიშნული ავტომანქანის კომპიუტერული მონაცემი (ავტომობილის გარბენის მაჩვენებელი) უნებართვოდ შეცვალა და ამით დანაშაულებრივ ჯგუფში შესაბამისი ლეგენდით ჩართულ საქართველოს შსს-ს თანამშრომელს სცადა დახმარებოდა მისი „მერსედესის“ მარკის ავტომობილის საბაზრო ღირებულების ხელოვნურად გაზრდაში მყიდველი მოქალაქის მოტყუების მიზნით (იგულისხმება მყიდველისთვის ავტომობილის გარბენის საერთო მანძილის რეალური მაჩვენებლის დამალვა, რაც უკუპროპორციულად განაპირობებს ავტომანქანის ფასს).

ამის შემდეგ სასამართლო ასკენის, რომ დ. გეჯაძე, ზ. მუსერიძე და ნ. კალანდია ცნობილნი უნდა იქნენ დამნაშავედ 286-ე მუხლის მე-3 ნაწილის „ა“ ქვეპუნქტით, მე-19, 24-ე და 180-ე მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული დანაშაულის ჩადენაში, ვინაიდან მათ წინასწარი შეთანხმებით ჩადიდნეს კომპიუტერული

108 კაზუსში დასახელებული ყველა თარიღი, ნომერი, დასახელება და პირის ვინაობა შეცვლილია.

მონაცემის შეცვლა და თაღლითობის მცდელობა, ე.ი. მართლსაწინააღმდეგო მისაკუთრების მიზნით სხვისი ნივთის მოტყუებით დაუფლებაში დახმარების მცდელობა.

აღნიშნულ საქმეზე ჩემს მიერ მოპოვებულ იქნა მხოლოდ განაჩენი, ამდენად, დანაშაულის ჩადენაში კონკრეტულად როგორი იყო როლების გადანაწილება დ. გეჯაძე, ზ. მუსერიძე და ნ. კალანდიას შორის რთული სათქმელია. თუმცა, რადგან სასამართლო 286-ე მუხლით გათვალისწინებული დანაშაულის ნაწილში არ მიუთითებს 24-ე მუხლზე, გამოდის, რომ სამივე დამნაშავე თანამსრულებლადაა მიჩნეული, თანახმად 25-ე მუხლის მე-3 ნაწილისა.

განხილული კაზუსის შემთხვევაშიც, სასამართლოს არ უცდია დაესაბუთებინა უშუალოდ რაში გამოიხატა კომპიუტერული მონაცემის უნებართვო შეცვლა, როცა აშკარად სახეზე იყო მანქანის და შესაბამისად მისი კომპიუტერული სისტემის მესაკუთრის თანხმობა. საუბარია დანაშაულის ჯგუფში შესაბამისი ლეგენდით ჩართულ შსს-ს თანამშრომლის თანხმობაზე, რადგან როგორც განაჩენიდან ირკვევა იგი მივიდა დ. გეჯაძესთან და სთხოვა შეეცვალა მისი ავტომანქანის კომპიუტერული მონაცემი. ვერც კომპიუტერული სისტემის უკანონო შეცვლაზე ვისაუბრებთ, რადგან ავტომობილის გარბენის მაჩვენებლის შეცვლა კანონით აკრძალული ქმედება არაა.

რთულია, სასამართლოს დავეთანხმოთ ქმედების კვალიფიკაციაში, რადგან დ. გეჯაძეს, ზ. მუსერიძეს და ნ. კალანდიას 286-ე მუხლით გათვალისწინებული დანაშაული არ ჩაუდენიათ. გასაგებია, რომ სასამართლო აკეღირებს შესაბამისი ლეგენდით დანაშაულებრივ ჯგუფში შეგზავნილ პირზე, რომელმაც პროვოცირება გაუწია ერთი შეხედვით დანაშაულებრივი ქმედების ჩადენას, მაგრამ ამ შემთხვევაშიც კომპიუტერული მონაცემის უნებართვო შეცვლაზე საუბარი შეუძლებელია, რადგან, როგორც ზემოთაც აღინიშნა კოდექსით განმარტებული ტერმინი „უნებართვო“ არ შეიძლება შეუსაბამოთ დ. გეჯაძის, ზ. მუსერიძის და ნ. კალანდიას მიერ ჩადენილ ქმედებას, რადგან უნებართვოში იგულისხმება შემთხვევა როცა უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისთვის ან ქმედება არის უკანონო.

თუ დანაშაულებრივ ჯგუფში შესაბამისი ლეგენდით ჩართული პირი თავისი ინიციატივით არ მივიდოდა დ. გეჯაძესთან და არ

სიზოვდა შეეცვალა მისი ავტომანქანის გარბენის მაჩვენებელი, დ. გეჯაძედა მისი თანამოაზრეები ვერც შეცვლიდნენ მას. გამოდის, რომ დ. გეჯაძის, ზ. მუსერიძის და ს. კალანდიას ქმედება არ იყო უკანონო და არც კომპიუტერული სისტემის მფლობელის ნების საინინაარმდეგო. კომპიუტერული მონაცემის უნებართვო შეცვლა მაშინ გვექნებოდა სახეზე, თუ დ. გეჯაძე და მისი თანამოაზრეები ავტომანქანის მესაკუთრესთან შეუთანხმებლად შეცვლიდნენ ავტომობილის გარბენის მაჩვენებელს ან აუ ამ მონაცემის შეცვლა იქნებოდა კანონით აკრძალული ქმედება.

სასამართლომ განაჩენში მე-19, 24-ე და 180-ე მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტიც მიუთითა.

24-ე მუხლის მითითება დაკავშირებულია იმ ფაქტთან, რომ სასამართლომ დ. გეჯაძის, ზ. მუსერიძის და ნ. კალანდიას ქმედება თაღლითობის ჩადენის მცდელობაში შეაფასა როგორც დახმარება. ანუ სასამართლომ მიიჩნია, რომ შსს-ს თანამშრომელს, რომელიც შესაბამისი ლეგენდით ჩაერთო დანაშაულებრივ ჯგუფში განზრახული ჰქონდა ჩადენა თაღლითობა და მას დახმარება სწორედ დ. გეჯაძემ და მისმა თანამოაზრეებმა გაუწიეს.

მე-19 მუხლი, როგორც ვიცით ეხება დანაშაულის მცდელობას. იგი განმარტებულია შემდეგნაირად: დანაშაულის მცდელობად ითვლება განზრახი ქმედება, რომელიც თუმცა უშუალოდ მიმართული იყო დანაშაულის ჩასადენად, მაგრამ დანაშაული ბოლომდე არ იქნა მიყვანილი. ამავე მუხლის მიხედვით სისხლისსამართლებრივი პასუხისმგებლობა მცდელობისთვის განისაზღვრება ამ კოდექსის შესაბამისი მუხლით, რომლითაც გათვალისწინებულია პასუხისმგებლობა დამთავრებული დანაშაულისთვის, ამ მუხლზე მითითებით.

ჩემი აზრით, სასამართლოს დასკვნა თაღლითობის მცდელობასთან დაკავშირებით აბსურდულია. ჯერ ერთი, მე-19 მუხლის შესაბამისად, იმისთვის, რომ ვისაუბროთ დანაშაულის მცდელობაზე სახეზე უნდა გვექონდეს განზრახი ქმედება, რომელიც უშუალოდ მიმართული იყო დანაშაულის ჩასადენად. რადგან ბრალდებულები დამნაშავედ ცნეს თაღლითობის ჩადენის მცდელობისთვის, კერძოდ კი დახმარების აღმოჩენისთვის, ბუნებრივია ჩნდება კითხვა, რომელი განზრახი ქმედება ჩადინა შსს-ს თანამშრომელმა თაღლითობის ჩასადენად? და თუ არ ჩაუდენია, მაშინ როგორ ვსაუბრობთ თაღლი-

თობის მცდელობაზე და მით უმეტეს დახმარებაზე? თუ შსს-ს თანამშრომელი დანაშაულებრივ ჯგუფში იმ მიზნით იყო ჩართული, რომ გამოეყენებინა დანაშაულის ფაქტი, მაშინ გამოდის, რომ მას ბოლომდე უნდა შეესრულებინა დამნაშავის როლი, ანუ მანქანის გარბენის მაჩვენებლის შეცვლის შემდეგ უნდა წასულიყო და გაეყიდა ან ეცადა ავტომანქანის გაყიდვა, ე.ი. ჩადენა თაღლითობა, მართლსაწინააღმდეგო მისაკუთრების მიზნით სხვისი ნივთის მოტყუებით დაუფლება და ამ შემთხვევაში დ. გეჯაძე, ზ. მუსერიძე და ნ. კალანდია შესაძლოა, მართლა მიგვეჩნია დამხმარებად. სხვა შემთხვევაში აბსტრაქტული მსჯელობიდან ვერ გამოვალთ. პირის მიმართ აბსტრაქტული ბრალდების გამო დაპატიმრებას კი სისხლისსამართლებრივი კანონმდებლობა არ ითვალისწინებს.

ჩემი აზრით თეზისი, რომლსაც დაეყრდნო სასამართლო, თითქოს მანქანის გარბენის მაჩვენებლის შეცვლა, კერძოდ კი ავტომობილით რეალურად დაფარული მანძილის შემცირება ზრდის მის საბაზრო ფასს, არის მხოლოდ ვარაუდი და არა აბსოლუტური ჭეშმარიტება. ავტოტრანსპორტის ფასი არაა დამოკიდებული მხოლოდ გარბენზე. მას განაპირობებს ავტომობილის მარკა, მისი გამოშვების წელი, ვიზუალური მხარე, სალონის მდგომარეობა, საბურავები, ძრავი და ა.შ. ამ მრავალ განმეორებად ფაქტორთან ერთად, გარბენი შესაძლოა იყოს ფასის განსაზღვრის ერთ-ერთი და არა ერთადერთი პირობა. ამიტომ, სასამართლოს მხრიდან იმის მტკიცება, რომ ზემოაღნიშნული მონაცემის შეამცირებით დამნაშავეებმა დახმარება აღმოუჩინეს შსს-ს თანამშრომელს თაღლითობის ჩადენის მცდელობაში, არის დაუსაბუთებელი.

თუ შსს-ს თანამშრომელი დ. გეჯაძესთან, ზ. მუსერიძესთან და ნ. კალანდიასთან საუბარში მართლაც გააცხადებდა, რომ ავტომანქანის გარბენის შემცირება სჭირდებოდა სატრანსპორტო საშუალების ფასის გასაზრდელად, ეს ხომ არ ნიშნავს, რომ მას თაღლითობის ჩასადენად მოქმედება დაწყებული ჰქონდა? თაღლითობა, ისევე, როგორც სხვა დანაშაული კონკრეტული დაზარალებულის გარეშე არ არსებობს. თუ ცნობილ ფრაზას გამოვიყენებთ, „თუ არ არის გვამი, ვერ ვისაუბრებთ მკვლელობაზე“. იმისთვის, რომ განხილული კაზუსის შემთხვევაში თაღლითობა სახეზე იყოს, მინიმუმ უნდა არსებობდეს პოტენციური მსხვერპლი, რომელთანაც მიმდი-

ნარეობს მოლაპარაკება ავტომობილის მიყიდვასთან დაკავშირებით. წინააღმდეგ შემთხვევაში, სასამართლოს ლოგიკით გამოდის, რომ თუ დ. გეჯაძე განაცხადებდა, რომ აპირებდა ნ. კალანდიას მოკვლას, მაგრამ არც ერთ ნაბიჯს გადადგამდა დანაშაულის მოსაძებნად და განსახოციელებლად, ჩვენ ის მაინც მკვლელობის მცდელობისთვის უნდა დაგვეპატიმრებინა! რა თქმა უნდა, აღნიშნულ მიდგომას ვერ გავიზიარებ.

განხილული პირველი კაზუსის შესაფასად სასამართლომ განაჩენში გამოიყენა 286-ე მუხლის მე-3 ნაწილი, რაც წინასწარი შეთანხმებით ჯგუფის მიერ კომპიუტერული მონაცემის ისეთ უნებართვო შეცვლას გულისხმობს, რამაც კომპიუტერული სისტემის განზრახ მნიშვნელოვანი შეფერხება გამოიწვია. გამოდის, რომ ავტომანქანის გარბენის მაჩვენებლის შეცვლამ არათუ განზრახ შეაფერხა კომპიუტერული სისტემის ფუნქციონირება, არამედ მნიშვნელოვანი შეფარხებაც კი გამოიწვია, რაც არა მარტო დაუსაბუთებელია, არამედ წარმოუდგენელიც. საინტერესოა აღინიშნოს, რომ განხილულ პირველ კაზუსში, სალარო აპარატის კომპიუტერული სისტემის მონაცემის სისწორე მნიშვნელოვანია მასზე გადასახადის დაკისრებისთვის და აქედან გამომდინარე სასამართლოს ლოგიკა მეტნაკლებად გასაგებია, მაგრამ მეორე შემთხვევაში ავტომანქანის გარბენის მაჩვენებლის სიზუსტე მსგავს მიზანს არ ემსახურება და მით უფრო გაურკვეველია საიდან გამომდინარე მივიდა სასამართლო იმ დასკვნამდე, რომ ამ მონაცემის შეცვლით კომპიუტერული სისტემის ფუნქციონირება განზრახ მნიშვნელოვნად შეფერხდა?!

დასკვნის სახით აღვნიშნავ, რომ განხილული კაზუსის შემთხვევაში სასამართლოს პოზიციას არც ერთ ნაწილში ვიზიარებ, რადგან ჩემი აზრით, დ. გეჯაძეს, ზ. მუსხერიძეს და ნ. კალანდიას სისხლის სამართლის კოდექსით გათვალისწინებული არც ერთი ქმედება ჩაუდენიათ.

უნდა შევნიშნოთ, რომ სისხლის სამართლის კოდექსის ძველი რედაქციით, კომპიუტერული ვირუსის შექმნა-გავრცელება ცალკე მუხლად იყო გათვალისწინებული. კერძოდ, 285-ე მუხლის ძველი რედაქცია უშუალოდ კომპიუტერული ვირუსის შექმნა-გავრცელებას კრძალავდა. იგი ჩამოყალიბებული იყო შემდეგნაირად: „1. ეგმ-ის დამაზიანებელი პროგრამის შექმნა ან არსებულ პროგრამაში

ცვლილების შეტანა, რაც განზრახ იწვევს ინფორმაციის არასანქცირებულ განადგურებას, ბლოკირებას, მოდიფიცირებას ან გადაღებას ანდა ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლას, აგრეთვე ასეთი პროგრამის ან ასეთი პროგრამის შემცველი მანქანა-მატარებლის გამოყენება ან გავრცელება.”

პროფ. გ. მამულაშვილის აზრით „მასში საუბარია კომპიუტერული ვირუსების შემუშავებაზე და გავრცელებაზე ელექტროგამომთვლელი მანქანისათვის პროგრამის შექმნის, ანდა არსებულ პროგრამაში ცვლილებების შეტანის გზით. კომპიუტერულ ვირუსს უწოდებენ სპეციალურ პროგრამას, რომელსაც უნარი შესწევს თვითნებურად მიუერთდეს სხვა პროგრამებს (ე.ი. „დაავადოს“ ისინი) და ამ უკანასკნელის გამოყენებისას შეასრულოს სხვადასხვა არასასურველი მოქმედება: ფაილებისა და კატალოგების გაფუჭება, ინფორმაციის დამახინჯება, მეხსიერების დაბინძურება ან წაშლა და ა.შ.¹⁰⁹“, ხოლო დამაზიანებელ პროგრამას გ. მამულაშვილი განმარტავს, როგორც „პროგრამა რომელიც იწვევს ინფორმაციის არასანქცირებულ განადგურებას, ბლოკირებას, მოდიფიცირებას ან გადაღებას, ანდა ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლას.“¹¹⁰”

გ. მამულაშვილის პოზიცია მისაღებია, თუმცა უნდა აღინიშნოს, რომ მოცემული მუხლის მთავარ ნაკლოვანებას სწორედ დამაზიანებელ პროგრამაზე ფოკუსირება განსაზღვრავს. კერძოდ, აღნიშნული დისპოზიციის ანალიზიდან გამომდინარე, ცხადია, რომ თუ კომპიუტერში არსებული ინფორმაციის კოპირება ან მოდიფიცირება მოხდება ისეთი პროგრამით, რომელიც არ აზიანებს ეგმ-ს, არ იარსებებს დანაშაული. თუმცა, როგორც ცნობილია, არსებობს პროგრამები (მაგ. „ტროას ცხენის“ ერთ-ერთი ტიპი), რომელიც არ აზიანებს კომპიუტერს და დამნაშავეს აძლევს საშუალებას განახორციელოს ნებისმიერი მოქმედება სამიზნე კომპიუტერულ სისტემაში. გამოდის, რომ თუ დამნაშავე კომპიუტერულ მონაცემს ეგმ-ის არა-

109 იხ. ავტორთა კოლექტივი, „სისხლის საქართლის კერძო ნაწილი“, წიგნი II, გამომც. „მერიდიანი“, იბ. 2012.გვ. 49

110 იხ. იქვე.

დამაზიანებელი პროგრამის გამოყენებით დაეუფლებოდა, შეცვლიდა ან გაანადგურებდა მისი ქმედება ვერ დაკვალიფიცირდებოდა როგორც დანაშაული. ეს გარემოება დამნაშავეს უქმნიდა კომფორტს დანაშაულებრივი ცხოვრებისთვის, ხოლო კანონმდებლობა იტოვებდა სერიოზულ „ხერელს“ სისხლისსამართლებრივი პასუხისმგებლობისგან თავის ასარიდებლად.

დღეს, 286-ე მუხლის მე-2 ნაწილი, სრულად მოიცავს როგორც სისტემის დამაზიანებელ, ასევე, არადამაზიანებელი პროგრამებისგან მომავალ საფრთხეს, რადგან აღნიშნული მუხლში აქცენტი გაკეთებულია დანაშაულის შედეგზე. კერძოდ, კი კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვან შეფერხებაზე კომპიუტერული მონაცემის უნებართვო დაზიანება, ნაშლა, შეცვლა, დაფარვა, ჩასმა ან გადაცემის გზით და დამაზიანებელია თუ არა ეს კომპიუტერული მონაცემი მნიშვნელობა არ აქვს.

5. კიბერდანაშაულის სუბიექტური შემადგენლობა

აღსანიშნავია, რომ ევროპის საბჭოს კონვენცია „კიბერდანაშაულის შესახებ“, კომპიუტერულ დანაშაულის ყველა შემადგენლობასთან მიმართებაში იყენებს ტერმინს „თუ ეს ქმედება წინასწარი განზრახვითაა ჩადენილი“. იმ სახელმწიფოებს, რომლებიც შეუერთდნენ კონვენციას მიაჩნიათ, რომ დასჯადი უნდა იყოს განზრახ ჩადენილი კომპიუტერული დანაშაული.

კონვენცია, რა თქმა უნდა, არ კრძალავს კომპიუტერული დანაშაულის გაუფრთხილებლობით ჩადენისთვის პასუხისმგებლობის დანესებას. უფრო მეტიც, აშშ, მართალია, ქეუერთდა კონვენციას, თუმცა კანონმდებლობაში დატოვა ჩანაწერი, რომლის მიხედვითაც წინასწარი განზრახვით ან გაუფრთხილებლობით დაცული კომპიუტერის დაზიანება გამოიწვევს სისხლისსამართლებრივ პასუხისმგებლობას. მსგავსი ჩანაწერი გვხვდება გაერთიანებულ სამეფოშიც. კერძოდ, „კომპიუტერის ბოროტად გამოყენების შესახებ“ კანონის XVIII თავის მე-3 მუხლის მიხედვით დასჯადია ისეთი არაავტორიზებული ქმედება, რომელიც ხელყოფს კომპიუტერის მუშაობას, ხელს უშლის ან აბრკოლებს კომპიუტერში არსებულ პროგრამასთან ან ინფორმაციასთან დაშვებას, ხელყოფს ამგვარი პროგრამის საიმე-

დობას. ასევე, დასჯადია წინასწარი განზრახვით სხვა პირისთვის ზემოაღნიშნულიდან რომელიმე ქმედების განხორციელების ტექნიკური საშუალების გადაცემა.

ზოგიერთი ქვეყნის კანონმდებლობაში, სისხლის სამართლის კოდექსის მუხლებში პირდაპირ ვხვდებით მითითებას წინასწარი განზრახვის თაობაზე.

საქართველოს სისხლის სამართლის კოდექსის მე-9 მუხლის მიხედვით, განზრახვა სამ კომპონენტია, რომელიც ზოგადად შეიძლება შემდეგი ფორმულირებით გამოიხატოს: „ცოდნა იმისა, რასაც ვაკეთებ, ნებელობა იმისა, რასაც ვაკეთებ და მართლწინააღმდეგობის შეგნება“¹¹¹.

მაგალითად, ა. სურმაევამ შურისძიების მიზნით, მომგებიან ლოტოში ათი ათასი ლარის ნაგების შემდეგ, უნებართვოდ შეაღწია მის „ბინგოს“ კომპიუტერულ სისტემაში და გაანადგურა გათამაშების შესახებ არსებული მთელი ინფორმაცია, მათ შორის ბოლო გათამაშებაში გამარჯვებული პირების შესახებ. მას არ სურდა მის მეზობელ ბ. დუნდუას გაენაღდებინა მოგებული მილიონი ლარი, მაგრამ შეგნებულად უშვებდა ამ შედეგის დადგომის შესაძლებლობას, რადგან მონაცემების ნაშლით იგი ბ. დუნდუას შესახებ არსებულ მონაცემსაც ანადგურებდა. შედეგად, მის „ბინგოს“ კომპიუტერული სისტემის ფუნქციონირება შეფერხდა და ველარ მოხერხდა ნაშლილი ინფორმაციის აღდგენა, რის გამოც ლოტოს გათამაშების შესახებ ოფიციალური ინფორმაცია დაიკარგა.

გამოდის, რომ სახეზე გვაქვს პირდაპირი განზრახვის სამივე ნიშანი:

ცოდნა – დამნაშავემ იცოდა, რომ შეაღწია იმ კომპიუტერულ სისტემაში, რომლის მფლობელსაც მისთვის პირდაპირ ან არაპირდაპირ არ გადაუცია ამ სისტემით სარგებლობის უფლება. მან ასევე იცოდა კონკრეტულად რომელი ინფორმაცია უნდა გაენადგურებინა და იცოდა რომ ის ქმედება რომელსაც სჩადიოდა აკრძალული იყო კანონით.

მართლწინააღმდეგობის შეგნება – დამნაშავეს შეგნებული ჰქონდა ქმედების როგორც ფაქტობრივი, ასევე მისი სოციალური ხასიათი.

111 იხ. მ. ტურავა, „სისხლის სამართალი, ზოგადი ნაწილის მიმოხილვა“, გამომცემლობა „ბონა კაუზა, თბ. 2010წ. გვ 127.

ნებელობა - დამნაშავეს სურდა სწორედ მას „ბინგოს“ კომპიუტერულ სისტემაში უნებარეოდ მელნევა და გამარჯვებული პირების შესახებ ინფორმაციის განადგურება. თუმცა აღსანიშნავია, რომ ზოგიერთი მეცნიერი ნებელობას მიიწევს არა განზრახვის კომპონენტად, არამედ ქმედების სისხლისსამართლებრივად რეველანტური და არარეველანტური ქმედებების ურთიერთგამიჯვნის კრიტერიუმად. ამ საკითხთან დაკავშირებით, საინტერესოა პროფ. ქ. მჭედლიშვილი-პედრიხის მოსაზრება, რომლის თანახმადაც ის ფაქტი რომ ევენტუალური განზრახვით განხორციელებული ქმედება ნებელობითია არ ადასტურებს იმას, რომ ქმედება ამ დროს დანაშაულის უშუალოდ ჩასადენადაა მიქართული. ნებელობა სისხლის სამართლის რეველანტური და არარეველანტური ქმედებების ურთიერთ გამიჯვნის კრიტერიუმია და მისი არარსებობა სისხლისსამართლებრივ პასუხისმგებლობას საერთოდ გამოორიცხავს (გაუფრთხილებლობისთვისაც). რადგან ნებელობითი ქმედება შეგნებული ქმედებაა და მის გარეშე სისხლის სამართლის პასუხისმგებლობა საერთოდ არ არსებობს.¹¹² მართალია, ავტორი ევენტუალურ განზრახვაზე საუბრობს, მაგრამ იგი აკონკრეტებს, რომ ნებელობის არარსებობა სისხლისსამართლებრივ პასუხისმგებლობას საერთოდ გამოორიცხავს. აქედან გამომდინარე ხომ არ უნდა ვიგულისხმოთ, რომ ის საერთოდ არაა განზრახვის კომპონენტი? ჩემი აზრით, უფრო მისაღებია მ. ტურავას ზემოთმოყვანილი მოსაზრება, რომელშიც საუბარია განზრახვის სამ კომპონენტზე, რადგან სისხლის სამართლის კოდექსი მასზე პირდაპირ მინიშნებას აკეთებს. კერძოდ, მე-9 მუხლის მე-2 ნაწილში პირდაპირ ვხვდებით მითითებას პირის სურვილზე მართლსაწინააღმდეგო ქმედების შედეგთან მიმართებაში. ამ ლოგიკით, არაპირდაპირი განზრახვისას უკვე პირიქით, საუბარია, რომ დამნაშავეს არ სურს ეს შედეგი, თუმცა ჩემი აზრით, სურვილიც და სურვილის არ ქონაც ნებელობის მდგომარეობაა და ორივე მათგანი გამოხატავს პირის ნებელობას დანაშაულის შედეგთან მიმართებაში.

უნდა აღინიშნოს, რომ 284-ე მუხლით გათვალისწინებული ქმედების არაპირდაპირი განზრახვით ჩადენა მეუძლებელია. განვიხი-

112 იხ. ქ. მჭედლიშვილი-პედრიხი, „სისხლის სამართალი ზოგადი ნაწილი II. დანაშაულის გამოვლენის ცალკეული ფორმები“, გამომც. „ქერდინი“ თბ. 2011წ. გვ. 80

ლოთ საქმე სასამართლო პრაქტიკიდან. მოქ. ბ. დიდავა იმყოფებოდა ინტერნეტ-კაფეში, სადაც მან დაიმახსოვრა იქვე მყოფი მოქალაქე ნ. თოდაძის მიერ პირადი გვერდზე შესვლისას გამოყენებული მომხმარებლის სახელი და პაროლი, რომლის გამოყენებითაც, მოგვიანებით, საკუთარი სახლიდან უნებართვოდ შეაღწია ნ. თოდაძის პირად გვერდზე. სასამართლომ აღნიშნული ქმედება შეაფასა, როგორც 284-ე მუხლის პირველი ნაწილით გათვალისწინებული ქმედება. კაზუსში თვალსაჩინოდ ჩანს სისხლის სამართლის კოდექსის 18-ე მუხლით გათვალისწინებული დანაშაულის მომზადება ანუ დანაშაულის ჩადენისთვის პირობების შექმნის ეტაპი, რაც გამოიხატა ბ. დიდავას მიერ ნ. თოდაძის თვალთვალში, რის შედეგადაც მან შეძლო ნ. თოდაძის მიერ პირად გვერდის დაცვის მიზნით დაყენებული პაროლის დამახსოვრება, რომლის გარეშეც იგი კომპიუტერულ სისტემაში უნებართვოდ ვერ შეაღწევდა. ამის შემდეგ, ბ. დიდავა ნავიდა სახლში და საკუთარი კომპიუტერის გამოყენებით, ჯერ შევიდა იმ ინტერნეტ-საიტზე, რომლითაც ნ. თოდაძე სარგებლობდა, ხოლო შემდეგ შეაღწია უშუალოდ მის პირად გვერდზე. ამ კაზუსიდან აშკარად ჩანს კოდექსის მე-9 მუხლის მე-2 ნაწილით გათვალისწინებული პირდაპირი განზრახვა. ფაქტია, რომ ბ. დიდავას ნებელობა, – ჩაიდინოს აღწერილი ქმედება თვალსაჩინოა, მაგრამ თუ არ იქნებოდა ნებელობა, ხომ ვერ ვისაუბრებდით ვერც პირდაპირი განზრახვით ჩადენილ დანაშაულზე? რადგან ავტომატურად, ბ. დიდავა არ მივიდოდა ინტერნეტ-კაფეში, არ უთვალთვალებდა ნ. თოდაძეს, არ დაიმახსოვრებდა პაროლს და არ შეაღწევდა კომპიუტერულ სისტემაში უნებართვოდ¹¹³.

განხილული კაზუსიდან გამომდინარე, წარმოუდგენელია ბ. დიდავას, რომელმაც ჯერ მოამზადა დანაშაული, შემდეგ მოკალათდა საკუთარ კომპიუტერთან, შევიდა ინტერნეტ-საიტზე, შესაბამის ველში ჩაწერა მომხმარებლის პაროლი, დაანვა ლილაქს „შესვლა“, კომპიუტერულ სისტემაში უნებართვო შეღწევისას ემოქმედა არა-პირდაპირი განზრახვით. გარდა ამისა, 284-ე მუხლის პირველი ნაწილი წარმოადგენს ფორმალურ შემადგენლობას, რომელსაც კონკრეტული შედეგი არ გააჩნია. იგი სისხლის სამართლის 284-ე მუხლით

113 კაზუსში დასახელებული ორივე პირის ვინაობა შეცვლილია

გათვალისწინებული ქმედების ჩადენიდან ითვლება დამთავრებულ დანაშაულად. ამდენად, ვერც კონკრეტული შედეგის დადგომარეადგომის მიმართ არსებული სურვილის შესახებ ვისაუბრებთ, რაც განაპირობებს კიდევ განზრახვის სახეს. კერძოდ არაპირდაპირი განზრახვის შემთხვევაში კოდექსის მკ-3 მუხლი მიუთითებს, რომ პირს არ სურს მართლსაწინააღმდეგო ქედების დადგომა, მაგრამ შეგნებულად უშვებს ან გულგრილად ეკიდება მის დადგომას. 284-ე მუხლის შემთხვევაში შედეგზე საერთოდ ვერ ვისაუბრებთ, რადგან თავად კომპიუტერულ სისტემაში უნებართვო შეღწევა უკვე დამთავრებული დანაშაულია.

უნდა აღინიშნოს, რომ 284-ე მუხლის მე-2 ნაწილის „დ“ ქვეპუნქტში დამამძიმებელ გარემოებად მითითებულია „რამაც მნიშვნელოვანი ზიანი გამოიწვია“, რომელიც თავის მხრივ გულისხმობს 2000 ლარზე მეტი ოდენობის ზიანს. გამოდის რომ თეორიულად, შესაძლებელია პირი უნებართვოდ აღწევდეს კომპიუტერულ სისტემაში, თუმცა მნიშვნელოვანი ზიანის დადგომა არ სურდეს, მაგრამ შეგნებულად უშვებდეს ან გულგრილად ეკიდებოდეს მის დადგომას. ჩემი აზრით, ეს თეორიული შესაძლებლობა ევრასდროს განხორციელდება, რადგან მხოლოდ კომპიუტერულ სისტემაში უნებართვო შეღწევა ევრასდროს გამოიწვევს ზიანს თუ მას არ მოჰყვება სხვა კონკრეტული მოქმედება, მაგალითად, კომპიუტერული მონაცემის დაზიანება, წაშლა, შეცვლა ან/და დაფარვა, ეს მოქმედებები კი უკვე სულ სხვა დანაშაულის შემადგენლობას ქმნის, კერძოდ კი 286-ე მუხლის პირველი ნაწილის. ჩემი აზრით, კანონმდებელს მხედველობიდან გამორჩა 284-ე მუხლით გათვალისწინებული დანაშაულის ფორმალური ხასიათი, წინააღმდეგ შემთხვევაში დამამძიმებელ გარემოებებში „მნიშვნელოვან ზიანს“ არ მიუთითებდა და შესაბამისად, ამ მუხლის მეორე ნაწილის „დ“ ქვეპუნქტით გათვალისწინებული ქმედების არაპირდაპირი განზრახვით ჩადენის აბსტრაქტულ შესაძლებლობასაც გამორიცხავდა, რომელიც როგორც აღვნიშნეთ პრაქტიკულად განუხორციელებადია. შესაბამისად, უნდა დავასკვნათ, რომ 284-ე მუხლით გათვალისწინებული 1-ლი და მე-2 ნაწილით გათვალისწინებული ქმედების ჩადენა შესაძლებელია მხოლოდ პირდაპირი განზრახვით, მე-2 ნაწილის „დ“ ქვეპუნქტი კი საერთოდ ზედმეტია 284-ე მუხლში.

საინტერესოა, რომ გ. მამულაშვილის აზრით, არა მხოლოდ 284-ე მუხლი, არამედ კიბერდანაშაულის თავში შესული დანარჩენი მუხლებიც მხოლოდ პირდაპირი განზრახვას გულისხმობს.¹¹⁴

285-ე მუხლთან დაკავშირებით გ. მამულაშვილი გამოთქვამს მოსაზრებას, რომ „ქმედების სუბიექტური შემადგენლობა პირდაპირ განზრახვას გულისხმობს, რამდენადაც მიზნით დაფუძნებულ დელიქტთან გვაქვს საქმე. მსგავსი დანაშაულისთვის ევროკონვენციაც წინასწარ განზრახვას უკავშირებს პასუხისმგებლობას. მთავარი არგუმენტი ტექნიკის არაკანონიერ გამოყენებასთან დაკავშირებით, არის მტკიცებულება, რომ ურთიერთობა მოხდა დანაშაულის ჩადენის მიზნით. ტექნიკის უბრალო ფლობა არ მიანიშნებს დანაშაულის ჩადენის გეგმაზე, რადგან კომპიუტერული უზრუნველყოფა სრულიად ლეგიტიმური მიზნებისთვისაც გამოიყენება. ამიტომ საჭიროა სპეციალური განზრახვის დასაბუთება“.¹¹⁵

გ. მამულაშვილის პოზიცია სრულიად მისაღებია, რადგან მუხლის შინაარსიდან გამომდინარე კითხვის ნიშნის ქვეშ არ დგება პირის პირდაპირი განზრახვა ჩაიდინოს კიბერდანაშაულის თავით და 158-ე მუხლით გათვალისწინებული დანაშაული. ეს კი გამორიცხავს ორაზროვნებას, კერძოდ, ამ ქმედების არაპირდაპირი განზრახვით ჩადენის შესაძლებლობას.

მაგალითად, თუ დ. დონაძე დამამტკიცებელს კომპიუტერულ მონაცემს იმ მიზნით, რომ შემდგომ მან უნებართვოდ შეაღწიოს ბ. ბიგვაჟას კომპიუტერულ სისტემაში, ანუ ჩაიდინოს კიბერდანაშაულის თავით განსაზღვრული დანაშაული და ამავე დროს ხელყოს ბ. ბიგვაჟას კერძო კომუნიკაციის საიდუმლოება, კერძოდ კი ფარულად გაეცნოს მის მიმონერას სოციალური ქსელით ანუ ჩაიდინოს 158-ე მუხლით გათვალისწინებული დანაშაული, საუბარი არაპირდაპირ განზრახვაზე შეუძლებელია. სწორედ ამიტომ მიმაჩნია, რომ გ. მამულაშვილი არ ცდება, როცა მთავარ არგუმენტად იშველიებს 285-ე მუხლის დათქმას ქმედების ჩამდენი პირის მიზანთან დაკავშირებით, რაც ცალსახად ავლენს, რომ როდესაც დამნაშავე სჩადის

114 იხ. ავტორთა კოლექტივი. „სისხლის სამართლის კერძო ნაწილი“, ნიჭი II, გამომც. „მერიდიანი“, თბ. 2012წ. გვ. 33

115 იხ. იქვე.

285-ე მუხლით გათვალისწინებულ ქმედებას მიზნად ისახავს სხვა დანაშაულის ჩადენას.

აღსანიშნავია, რომ ისევე როგორც 284-ე, 285-ე მუხლიც ფორმალური შინაარსისაა, ანუ ქმედების დანაშაულად კვალიფიკაციისთვის საკმარისია, კომპიუტერული პროგრამის ან/და სხვა მონყობილობის, აგრეთვე კომპიუტერულ სისტემაში მელნევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადების, შენახვის, გაყიდვის, გავრცელების ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფის ყაჩქის და სპეციალური განზრახვის დადგენა. შესაბამისად, კანონმდებელი სისხლისსამართლებრივ პასუხისმგებლობას მართლასწინააღმდეგო შედეგის დადგომას არ უკავშირებს. აქედან გამომდინარე, 285-ე მუხლი დამნაშავის დამოკიდებულებას მოსალოდნელ მართლასწინააღმდეგო შედეგთან მიმართებაში მნიშვნელობას არ ანიჭებს და შესაბამისად არაპირდაპირ განზრახვაზე საუბარი მით უფრო უადგილოა. თუმცა, მსგავსად 284-ე მუხლისა, 285-ე მუხლის მე-2 ნაწილის „დ“ ქვეპუნქტშიც დამამძიმებელ გარემოებად ჩითითებულია „მნიშვნელოვანი ზიანი“. გამოდის, რომ ამ ნაწილში შემადგენლობა მატერიალურია და თეორიულად, აქაც არსებობს მისი არაპირდაპირი განზრახვით ჩადენის შესაძლებლობა ანუ თეორიულად შესაძლებელია პირს მნიშვნელოვანი ზიანის დადგომა არ სურდეს, მაგრამ შეგნებულად უშვებდეს ან გულგრილად ეკიდებოდეს მის დადგომას, მაგრამ ამ მოსაზრებას იმ შემთხვევაში ექნებოდა არსებობის უფლება, თუ, როგორც გ. მამულაშვილი აღნიშნავს, 285-ე მუხლით გათვალისწინებული დანაშაული მიზნით დაფუძვნებული დელიქტი არ იქნებოდა. აღსანიშნავია, რომ თვითონ ტერმინი „არაპირდაპირი განზრახვით სხვა დანაშაულის ჩადენის მიზანი“ სრულიად ურთიერთგამომრიცხავი შინაარსისაა და თუ პირის ქმედების შედეგად მართლაც დადგება „მნიშვნელოვანი ზიანი“, გამოდის რომ დამნაშავე პირდაპირი განზრახვით მოქმედებდა, რადგან კომპიუტერული პროგრამის და ა.შ. სხვა დანაშაულის ჩადენის მიზნით არაპირდაპირი განზრახვით დამზადება, გავრცელება და ა.შ. ნარმოუდგენელია. ეს იეზისი გამორიცხავს 285-ე მუხლის მე-2 ნაწილის „დ“ ქვეპუნქტით გათვალისწინებული დანაშაულის არაპირდაპირი განზრახვით ჩადენის როგორც თეორიულ ასევე, პრაქტიკულ შესაძლებლობასაც.

გ. მამულაშვილის აზრით, 286-ე მუხლით გათვალისწინებული დანაშაულის ჩადენაც მხოლოდ პირდაპირი განზრახვითაა შესაძლებელი. თუმცა, საინტერესოა, არ შეიძლება კომპიუტერული მონაცემის უნებართვო დაზიანება, ნაშლა, შეცვლა ან დაფარვა განხორციელდეს გაუფრთხილებლობით? ჩემი აზრით, კომპიუტერული მონაცემის უნებართვო შეცვლა ან დაფარვა შესაძლებელია მხოლოდ პირდაპირი განზრახვით, რადგან ტექნიკურად წარმოუდგენელია დამნაშავეს მიზანმიმართული მოქმედების, ან სურვილის გარეშე ასეთი ქმედება განხორციელდეს. მონაცემის შეცვლა გულისხმობს მისი შინაარსის შეცვლას, დაფარვა კი მისი ადამიანისთვის ვიზუალურად არააღქმად რეჟიმში გადაყვანას, რაც შესაძლებელია კონკრეტული კომპიუტერული მონაცემის ე.წ. „მახასიათებლების“ შეცვლით. აღნიშნული ხორციელდება კომპიუტერული ფაილის შესაბამის ველში „დამალულ“ რეჟიმში გადასვლის ბრძანების დაფიქსირებით. აღწერილი მოქმედების პირდაპირი განზრახვის გარეშე განხორციელება კი შეუძლებელია. წარმოუდგენელია, დამნაშავემ „შეცდომით“ შეცვალოს კომპიუტერული მონაცემის შინაარსი ან დაფაროს იგი, რადგან, როგორც უკვე აღინიშნა, ორივე ქმედება გულისხმობს კონკრეტული, მიზანმიმართული და თანმიმდევრული ქმედებების განხორციელებას. რაც შეეხება კომპიუტერული მონაცემის უნებართვო დაზიანების და ნაშლის შემთხვევას, აქ ოდნავ სხვაგვარადაა საქმე, თუმცა მათი არაპირდაპირი განზრახვით განხორციელება გ. მამულაშვილის მსგავსად, მეც არ მიმაჩნია შესაძლებლად. მაგალითად, განვიხილოთ კაზუსი. ბ. ბიგვაჟა, მუშაობდა კომპიუტერული ტექნიკის ხელოსნად. მას დაუკავშირდა შპს „გულის“ წარმომადგენელი და სთხოვა თავიდან „დაეინსტალირებინა“ ფირმის საკუთრებაში არსებული კომპიუტერის პროგრამა „ვინდოუსი“, რადგან რამდენიმე წელიწადის განმავლობაში მათ მიერ არ განახლებულა იგი და შესაბამისად. მუშაობდა შეფერხებით. შპს „გულის“ წარმომადგენელს ბ. ბიგვაჟასთვის არ მიუთითებია ინახავდა თუ არა იგი კომპიუტერში მისთვის მნიშვნელოვან კომპიუტერულ მონაცემს და შესაბამისად, ბ. ბიგვაჟამ კომპიუტერს ჩაუტარა ე.წ. „დაფორმატება“, რაც გულისხმობს კომპიუტერში არსებული ოპერაციული სისტემის სრულ ნაშლას, მასში შენახული მონაცემებითურთ, ხოლო ამის შემდეგ ხელახლა ჩაწერა „ვინდოუსი“. აღსან-

იმნავია, რომ ე.წ. „დაფორმატება“, „ვინდოუსის“ ხელახლა ინსტალაციის ჩვეულებრივი შემადგენელი ნაწილია. იმ შემთხვევაში თუ პირს სურს გადაარჩინოს კომპიუტერულ სისტემაში შენახული მონაცემი, იგი ინსტალაციის პროცესის დაწყებამდე, დროებით სხვაგან ინახავს მათ. მაგალითად, გადააქვს კომპაქტ-დისკზე, ან იმავე კომპიუტერში შექმნილ დისკზე, რომელზეც ოპერაციული სისტემის ინსტალაცია გავლენას ვერ ახდენს. ბ. ბიგვას არანაირი ინტერესი არ გააჩნდა ამ მონაცემების ნაშლის მიმართ და არც სურდა, რომ დამდგარიყო ეს შედეგი, გათვალისწინებული ჰქონდა წინდახედულების ნორმით აკრძალული ქმედება, ანუ შესაძლებლობა, რომ ინსტალაციის შედეგად ნაიძლებოდა კომპიუტერული მონაცემი, იმედოვნებდა, რომ შპს „გულის“ წარმომადგენელი მის მისვლამდე შეინახავდა მისთვის საჭირო კომპიუტერულ მონაცემს და „ვინდოუსის“ ინსტალაციით იგი არ ნაშლიდა მათ. თუმცა, აღმოჩნდა, რომ შპს „გულის“ წარმომადგენელი ვერ ერკვეოდა კომპიუტერულ ტექნიკაში და შესაბამისად, კომპიუტერული მონაცემის შენახვა არ მოუხდენია.

რა დანაშაულთან გვაქვს საქმე? ერთი შეხედვით სახეზეა ბ. ბიგვას თვითიმედოვნება, მაგრამ კოდექსის 10-ე მუხლის მე-4 ნაწილით გაუფრთხილებლობით ჩადენილი ქმედება მხოლოდ მაშინ ჩაითვლება დანაშაულად, თუ ამის შესახებ მითითებულია ამ კოდექსის შესაბამის მუხლში. ასეთ მითითებას 286-ე მუხლში ვერ ვხვდებით, თუმცა ესეც რომ არ იყოს, უნდა ჩაგვეთვალა თუ არა ბ. ბიგვას ქმედება გაუფრთხილებლობით ჩადენილ კომპიუტერული მონაცემის უნებართვო ნაშლად? კაზუსიდან ირკვევა, რომ ბ. ბიგვას არ მოქმედებდა უნებართვოდ, რადგან შპს „გულის“ წარმომადგენელმა მას გადასცა უფლება განეხორციელებინა „ვინდოუსის“ ინსტალაცია, რაც როგორც ავლნიშნეთ გულისხმობს კომპიუტერული მონაცემების ნაშლას, ხოლო შემდეგ ოპერაციული სისტემის ხელახალ ჩაწერას. ჩემი აზრით, ის ფაქტი, რომ შპს „გულის“ წარმომადგენელი ვერ ერკვეოდა კომპიუტერულ ტექნიკაში არ ქმნის ბ. ბიგვას სისხლისსამართლებრივი პასუხისმგებლობის საფუძველს იმ შემთხვევაშიც, თუ 286-ე მუხლით გათვალისწინებული იქნებოდა ამ ქმედების ჩადენა გაუფრთხილებლობით, ვინაიდან, სახეზე არ გვაქვს „უნებართვობა“ – ბ. ბიგვას არ ჩაუდენია არც უკანონო და

არც კომპიუტერული სისტემის მფლობელის ნების სანინალმდეგო ქმედება.

თუ ბ. ბიგვაჟა შპს „გულის“ კომპიუტერული ქსელის ოპერატორია, და მას სამსახურებრივად ევალება კომპიუტერული სისტემის მოვლა-პატრონობა თუმცა, მის მიერ დაუდევრობით ან შეცდომით მოხდა კომპიუტერული სისტემის ექსპლუატაციის წესის დარღვევა და ამ მიზეზით კომპიუტერული მონაცემის წაშლა, უკვე შესაძლებელია ვისაუბროთ გაუფრთხილებლობაზე. მაგალითად, შევხუტულბაში წასვლამდე ბ. ბიგვაჟას დაავინყდა პირად სარგებლობაში არსებული კომპიუტერის გამორთვა. სამსახურში დაბრუნების შემდეგ აღმოაჩინა, რომ იგი გადაინჟა და მასში შენახული ინფორმაცია სრულად განადგურდა. ხოლო ტექნიკური ექსპერტიზის დასკვნამ დაადგინა, რომ კომპიუტერის გადანჟა გამოინჟია იმ გარემოებამ რომ ის იდგა მზის სხივებისგან დაუცველ ადგილას, ჩართულ მდგომარეობაში, რის გამოც კომპიუტერის ინტეგრირებულმა გაგრილების მონყობილობამ ველარ უზრუნველყო ფუნქციის შესრულება, შედეგად, დაზიანდა კომპიუტერი და განადგურდა კომპიუტერული მონაცემი.

ბ. ბიგვაჟას არ სურდა კომპიუტერული მონაცემის წაშლა. მეტიც, მას სამსახურებრივად ევალებოდა მისი დაცვა, მან ასევე იცოდა, რომ კომპიუტერის გამორთიველ მდგომარეობაში დატოვებით შესაძლოა მომხდარიყო მისი დაზიანება, მაგრამ იმედოვნებდა, რომ გამორთო და ქესაბამისად, არ დადგებოდა ეს შედეგი. სახეზე გვაქეს კოდექსი მე-10 მუხლის მე-2 ნაწილში აღწერილი ოვი-თიმედოვნება, მაგრამ როგორ დავაკვალიფიკიროთ ქმედება? 286-ე მუხლით გათვალისწინებული დანაშაულის ჩადენისთვის გაუფრთხილებლობისთვის პირს პასუხს ვერ ვაგებინებთ, მაგრამ კოდექსის 188-ე მუხლი სასჯელს ადგენს ნივთის დაზიანებისთვის ან განადგურებისთვის გაუფრთხილებლობით, რამაც მნიშვნელოვანი ზიანი გამოინჟია. თუ დადგინდება, რომ შპს „გულს“ მიადგა 150 ლარზე მეტი ოდენობის ზიანი, მაშინ ბ. ბიგვაჟა პასუხისგებაში უნდა მიეცეს, სწორედ ამ მუხლის პირველი ნაწილით გათვალისწინებული დანაშაულის ჩადენისთვის.

286-ე მუხლის ქეორე ნაწილით გათვალისწინებული დანაშაულიც გულისხმობს პირდაპირ განზრახვას, რადგან თავად მუხლი აკონკრეტებს, რომ სახეზე უნდა გექონდეს კომპიუტერული

სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება. აქედან გამომდინარე, თუ დამნაშავე არ იმოქმედებს კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხების მიზნით და თუ არ დადგება ეს შედეგი, ანუ თუ მას არ ექნება სურვილი, მნიშვნელოვნად შეაფერხოს კომპიუტერული სისტემის ფუნქციონირება და ამ შედეგის მისაღწევად იგი უნებართვოდ არ ნაშლის, შეცვლის, დაფარავს, დააზიანებს, ჩასვავს ან გადაცემს კომპიუტერულ მონაცემს, ანუ თუ არ ჩაიდენს მართლსაწინააღმდეგო ქმედებას, შესაბამისად, ვერ ვისაუბრებთ 286-ე მუხლით გათვალისწინებული დანაშაულის ჩადენაზე.

კომპიუტერული დანაშაულის ჩადენის მოტივი შეიძლება იყოს როგორც შურისძიება, ანგარება, ან სხვა დანაშაულის ჩადენისთვის მომზადება და სხვ. გ. მაშულაშვილი მოტივში დამატებით გამოყოფს ხულიგნობას და სამეცნიერო-კვლევით ინტერესს.¹¹⁶ უნდა ითქვას, რომ ეს მოტივები საერთოა კოდექსში გათვალისწინებული ყველა კიბერდანაშაულისთვის.

ხაზგასმით უნდა აღინიშნოს, რომ დამამძიმებელ გარემოებებში ანგარება როგორც დანაშაულის ჩადენის მოტივი არც ერთ კიბერდანაშაულთან მიმართებაში არ გვხვდება. თუმცა ფაქტია, რომ ანგარება ერთ-ერთი მამოძრავებელი ძალაა ამ ტიპის დანაშაულისთვის. ანგარების მოტივი ერთ-ერთი ყველაზე გამორჩეულია თავისი შინაარსით. მასში, როგორც წესი, მატერიალური გამორჩენის მიღების მიზანი იგულისხმება.

„ანგარება არის ძლიერი სურვილი იმისა, რომ შევიძინოთ სიმდიდრე, განსაკუთრებით ყოველგვარი სიმდიდრის წარმომადგენელი – ფული. ამ ვნების განმასხვავებელი ნიშანი ისაა, რომ ის სხვებზე ძლიერადაა გავრცელებული ადამიანებს შორის, ისე რომ არ არსებობს თითქმის არც ერთი ადამიანი, რომელიც მეტ-ნაკლებად არ იყოს მისით დასნებოვნებული. ეს იმიტომ ხდება, რომ სიმდიდრე არის ყველა სხვა სიამოვნების შეძენის საშუალება, ხოლო ცნობილია, რომ ქვეყანაზე ცოტაა ადამიანი, რაიმე სიამოვნებისკენ რომ არ ისწრაფვოდეს და თავისი მდგომარეობის გამოსწორება არ სურდეს.“ – წერს წმ. ეპისკოპოსი გაბრიელ ქიქოძე საკუთარ ნაშ-

116 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი II, გამოცე. „მერიდიანი“, თბ. 2012წ. გვ. 33

რომში „ცდისეული ფსიქოლოგიის საფუძვლები“¹¹⁷ და რთულია არ დაეთანხმო.

ნაშრომში განხილული სასამართლოს პრაქტიკის ანალიზით კი შეგვიძლია დავასკვნათ, რომ კიბერდანაშაულის ჩამდენი დამნაშავეების უმრავლესობა მოქმედებდა ანგარების მოტივით. მაგალითად, განხილულ ერთ-ერთ საქმეში ჩანს, რომ კომპიუტერულ სისტემაში უნებართვო შეღწევა განხორციელდა იმიტომ, რომ დამნაშავეს დაზარალებულის ანგარიშიდან მოეპარა არსებული თანხა, სხვა კაზუსიდან ირკვევა, რომ პირებმა კომპიუტერულ სისტემაში უნებართვოდ იმ მიზნით შეაღწიეს, რომ მოპოვებული ინფორმაციით დაემზადებინათ ყალბი საკრედიტო ბარათები და მიეღოთ მატერიალური შემოსავალი, სხვა კაზუსიდან ირკვევა, რომ დამნაშავემ კომპიუტერული მონაცემი უნებართვოდ შეცვალა მატერიალური ანაზღაურების სანაცვლოდ და ა.შ. კიდევ ბევრი მაგალითის მოყვანა შეიძლება სასამართლო პრაქტიკიდან, თუმცა ისედაც ცხადია, რომ კიბერდანაშაულში ანგარების მოტივს განსაკუთრებული ადგილი უჭირავს.

კომპიუტერული დანაშაულის მიზანი მრავალფეროვნია. 284-ე მუხლში მიზანი მითითებული არ არის. თან აღსანიშნავია, რომ ეს მუხლი ფორმალური შემადგენლობისაა და მასში დანაშაულებრივი შედეგი გათვალისწინებული არაა.

ევროპის საბჭოს კონვენციის მე-6 მუხლში აღნიშნულია, რომ კომპიუტერული პროგრამის ან/და სხვა მონეობილობის, აგრეთვე კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დამეხების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა დასჯადია მხოლოდ იმ შემთხვევაში, თუ მისი მიზანია სხვა კიბერდანაშაულის ჩადენა. ქართველმა კანონმდებელმა კი დასჯადად გამოაცხადა სისხლის სამართლის კოდექსის XXXV თავით და 158-ე მუხლით (რომელიც ეხება კერძო კომუნიკაციის საიდუმლოების დარღვევას) გათვალისწინებული დანაშაულის ჩადენის მიზნით კომპიუტერული პროგრამის ან/და სხვა მონეობილობის

117 იხ. გ. ქიქოძე, „ცდისეული ფსიქოლოგიის საფუძვლები“ (ნაშრომში გამოყენებულია ნიგნის ელექტრონული ვერსია, რომელშიც გვერდები და გამოცემის თარიღი მითითებული არ არის. იხ. <http://www.orthodoxy.ge/psiqologia/gabriel/psiqologia-4-2.htm#116>)

უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა და ჩემი აზრით შეცდომაც დაუშვა, რადგან სახეზე მივიღეთ სრულიად უცნაური ვითარება. თუ პირი ერთდროულად არ იმოქმედებს კიბერდანაშაულის თავით განსაზღვრული და 158-ე მუხლით გათვალისწინებული დანაშაულის მიზნით, სახეზე არ გვექსება 285-ე მუხლით გათვალისწინებული ქმედება. შესაძლოა ეს ტექნიკური ხასიათის შეცდომაა, რადგან რთულია მოძებნო ლოგიკა იმაში, თუ რატიმ არაა დანაშაული კომპიუტერული პროგრამის ან/და სხვა მონაცემების უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა კომპიუტერულ სისტემაში უნებართვო შეღწევის მიზნით და რატიმ იქნება ის დანაშაული იმ შემთხვევაში, თუ დამნაშავეს პარალელურად კერძო კომუნიკაციის საიდუმლოების ხელყოფის მიზანიც აქვს. იმის თქმა ხელალებით შეიძლება, რომ ევროპის საბჭოს კონვენციას და მსოფლიოს იმ ქვეყნებს, რომლებმაც კონვენციის აღნიშნული მუხლი, მისი მნიშვნელობის გამო კონვენციის რატიფიცირებამდე აამოქმედეს, მსგავსი ჩანაწერი არ გაუჩენიათ. ამ სახით 285-ე მუხლის არსებობა ფაქტობრივად უსაგნოა, რადგან რეალურად კონვენციის მე-6 მუხლი ებრძვის მსოფლიოში ძალიან გავრცელებულ დანაშაულს, რასაც კომპიუტერული პროგრამის ან/და სხვა მონაცემების უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ჰქვია, კერძო კომუნიკაციის საიდუმლოების დარღვევა კი მხედველობაში მიღებული არ არის. ჩემთვის რთულია დავინახო არსებული რედაქციის უპირატესობა კონვენციის მე-6 მუხლთან შედარებით. უფრო მეტიც, მიმაჩნია, რომ 285-ე მუხლით დამნაშავეს დასჯა იქნება ურთულესი, რადგან გარდა კლასიკური კიბერდანაშაულის შემადგენლობისა, მის ქმედებაში აღმოსაჩენი გვაქვს კერძო კომუნიკაციის საიდუმლოების დარღვევის მიზანი. ეს ფაქტი დამნაშავეებისთვის ქმნის კიდევ ერთ დამატებით მოტივაციას სრულიად უპრობლემოდ დაამზადონ, შეინახონ, გაავრცელონ და ა.შ. კიბერდანაშაულის თავით გათვალისწინებული დანაშაულის ჩასადენი პროგრამა, მონაცემებისა, ან კომპიუტერულ სისტემაში შესაღწევი პაროლი, კოდი და ა.შ. ისე, რომ არ იქონიონ კერძო კომუნიკაციის საიდუმლოების დარღვევის მიზანი, რაც რა კავშირშია ამ კონკრეტულ კიბერდანაშაულთან რთული გასარკვევია.

ამ საკითხთან მიმართებაში აღსანიშნავია, რომ, საქართველოს პრეზიდენტმა 2012 წელის 1-ლ ივნისს გამოსცა ბრძანებულება „კიბერდანაშაულის შესახებ“ კონვენციის დამტკიცების თაობაზე. აღნიშნული აქტის საფუძველზე, კონვენციის მე-6 მუხლის მე-3 პუნქტის თანახმად, საქართველო აცხადებს, რომ მე-6 მუხლის 1-ლი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული ქმედებისთვის სისხლისსამართლებრივი პასუხისმგებლობა შეიძლება დადგეს იმ შემთხვევაში, როდესაც მოწყობილობა, კომპიუტერული პროგრამის ჩათვლით, განკუთვნილია ან ადაპტირებულია კონვენციის მე-2-დან მე-5 მუხლის ჩათვლით განსაზღვრული ქმედების ჩადენის მიზნით. ამდენად, საქართველო ადგენს, რომ 285-ე მუხლში და შესაბამისად, ევროპია საბჭოს კონვენციის მე-6 მუხლში განსაზღვრული ქმედება მხოლოდ მაშინ უნდა იყოს დასჯადი თუ მისი მიზანი სხვა კიბერდანაშაულის ჩადენაა, თუმცა ამ აქტს კოდექსთან შედარებით უპირატესი ძალა ვერ ექნება და ამიტომ არაფრისმოძვემია.

ევროპის საბჭოს კონვენციის ავტორების აზრით იმ უკანონო ტექნიკური მოწყობილობის ჩამონათვალი, რომლის მეშვეობითაც ხდება ზემოაღნიშნული დანაშაულის ჩადენა ძალზე შეზღუდულია და ქმედების დანაშაულად კვალიფიკაციისას ართულებს მუხლის გამოყენებას, რადგან მასში ასევე უნდა ვიგულისხმოთ ისეთი ტექნიკური მოწყობილობა, რომლის გამოყენება შესაძლებელია კანონიერადაც. ქმედების დანაშაულად კვალიფიკაციისას განსაკუთრებული ყურადღება უნდა მივაქციოთ არა მხოლოდ ქმედების შინაარსს, არამედ დამნაშავის მიზანს, რადგან სისხლის სამართლის პასუხისმგებლობის წინაპირობას არ წარმოადგენს ისეთი სპეციალური მოწყობილობის, პროგრამის და ა.შ. წარმოება, გაყიდვა, შეძენა და ა.შ. რომელთა გავრცელება არ ხდება დანაშაულის ჩადენის მიზნით. უფრო მეტიც, მსგავსი ტექნიკური მოწყობილობის, პროგრამის და ა.შ. შექმნის მიზანი ხშირად მხოლოდ კომპიუტერული სისტემის ტესტირება ან მისი დაცვაა¹¹⁸.

ამდენად, მოცემული პოზიციის მიხედვით, ისეთი სპეციალური მოწყობილობის, პროგრამის ან პაროლის, რომლის საშუალებითაც

118 იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ: ტრენინგის სახელმძღვანელო“, ევროსაბჭო, სტრასბურგი, 2010წ. გვ. 58-59

შესაძლებელია კომპიუტერულ სისტემაში უნებართვო შეღწევა ან კერძო კომუნიკაციის საიდუმლოების დარღვევა, მხოლოდ წარმოება, გაყიდვა, შეძენა და ა.შ. არ უნდა მივიჩნიოთ დანაშაულად იმ შემთხვევაში, როცა პირის მიზანი საკუთარი კომპიუტერული სისტემის ინტეგრირებულობის შემოსმება და დაცვაა. შესაბამისად, განსაკუთრებული ყურადღება უნდა მიენიჭოს პირის მიზანს. თუ დადგინდება, რომ სპეციალური მოწყობილობის, პროგრამის ან პაროლის წარმოება, გაყიდვა, შეძენა და ა.შ. კონკრეტული კიბერ-დანაშაულის ჩადენის მიზანს და კერძო კომუნიკაციის საიდუმლოების დარღვევას ემსახურება, მხოლოდ ამ შემთხვევაში უნდა ვისაუბროთ 285-ე მუხლით გათვალისწინებულ დანაშაულზე.

286-ე მუხლით გათვალისწინებული დანაშაულის ჩადენისას დამსაშვევ შესაძლოა მოქმედებდეს მრავალფეროვანი მიზნით. მაგალითად, წარმოვიდგინოთ ორი შემთხვევა. პირველი: ა. ალფენიძემ შეაღწია „საჯარო რეესტრის ეროვნული სააგენტოს“ ელექტრონულ ბაზაში და გაანადგურა ინფორმაცია რუსთაველის ქ. №3-ში არსებული უძრავი ქონების შესახებ, რომელიც ეკუთვნოდა მოქ. ბ. ვანაძეს. ბ. ვანაძემ აღნიშნული უძრავი ნივთი ერთი წლის წინ სწორედ ა. ალფენიძისგან შეიძინა და ახლა, ა. ალფენიძეს ამ მონაცემების ნაშლით სურდა მომავალში ჩაედინა თაღლითობა, კერძოდ კი ხელახლა გაეყიდა რუსთაველის ქ. №3-ში მდებარე უძრავი ნივთი.

მეორე შემთხვევა: ა. დუმბაძეს ჰქონდა კომპანია, რომელიც უზრუნველყოფდა საქართველოს მოქალაქეების მიერ ამერიკულ ინტერნეტ-მაღაზიებში ინტერნეტის სამუშაოებით შეძენილი ნივთების გადაზიდვას. მისი კომპანია ახალი შექმნილი იყო და კონკურენციას ვერ უწევდა მსგავსი მომსახურების მქონე სხვა ფირმებს. ამიტომ ა. დუმბაძემ განახორციელა ე.წ. „დოს“ იქროში კონკურენტი კომპანიების ვებ-გვერდების მიმართ, რის შედეგადაც მოახერხა მათი დაზიანება 10-14 დღით. ამ ვადაში კი მან შეძლო ბაზარზე თავის დამკვიდრება, რადგან ქართულ ინტერნეტ-სივრცეში ამ პერიოდში მხოლოდ მისი საიტი ფუნქციონირებდა და ემსახურებოდა მომხმარებლებს.

პირველი კაზუსის შემთხვევაში, დამნაშავის მიზანი სხვა დანაშაულის ჩადენისთვის მზადება, მეორე შემთხვევაში კი მიზანი კონკურენტი კომპანიების კომპიუტერული სისტემის ფუნქციონირების შეფერხების გზით საკუთარი ბიზნეს-საქმიანობის განვითარებაა. მოტივი ორივე კაზუსის შემთხვევაში ანგარებაა.

6. კიბერდანაშაულის სუბიექტი

კიბერდანაშაულის თავით განსაზღვრული დანაშაულის სუბიექტია პირი, რომელსაც მიუხსოვდა 14 წელი. მათ შორის, შეიძლება სახეზე გვყავდეს სპეციალური სუბიექტიც, მაშინ როცა ქმედებას ჩადის პირი სამსახურებრივი მდგომარეობის გამოყენებით. ბუნებრივია, სამსახურებრივი მდგომარეობის გამოყენებით ჩადენილი დანაშაულის სუბიექტში არ უნდა ვიგულისხმოდ მხოლოდ საჯარო მოხელე და მასთან გათანაბრებული პირი. სამსახურებრივი მდგომარეობით დანაშაული შეიძლება ჩაიდინოს ნებისმიერმა პირმა, რომელიც მუშაობს რიგორც კერძო, ასევე, სახელმწიფო სექტორში. ასეთ პირებს, როგორც წესი, ხელი მიუწვდებათ კომპიუტერულ სისტემაზე და სამსახურებრივი მდგომარეობიდან გამომდინარე არიან ამ კომპიუტერული სისტემის ოპერატორი, ადმინისტრატორი, ტექნიკური უზრუნველყოფის სამსახურის თანამშრომლები და ა.შ. უნდა გავითვალისწინოთ, რომ კომპიუტერული ტექნიკა ადრეული წლებიდანვე ხელმისაწვდომია ადამიანებისთვის. კომპიუტერული დანაშაულის ცალკეული შემადგენლობის ჩადენა კი ხშირ შემთხვევაში არ მოითხოვს უმაღლეს განსწავლულობას ამ დარგში (მაგალითად, კომპიუტერის დამაზიანებელი პროგრამის გავრცელება).

როდესაც ვსაუბრობთ კიბერდანაშაულის სუბიექტზე, საინტერესოა განვიხილოთ კიდეცის 220-ე მუხლით გათვალისწინებული უფლებამოსილების ბოროტად გამოყენება ანუ „საწარმოში ან სხვა ორგანიზაციაში ხელმძღვანელობითი, წარმომადგენლობითი ან სხვა სპეციალური უფლებამოსილების გამოყენება ამ ორგანიზაციის კანონიერი ინტერესის საწინააღმდეგოდ, თავისთვის ან სხვისთვის-გამორჩენის ან უპირატესობის მიღების მიზნით, რამაც მნიშვნელოვანი ზიანი გამოიწვია.“

როგორც ვხედავთ, 220-ე მუხლში მითითებულია სპეციალური სუბიექტი, ანუ საუბარი, პირის მიერ სამსახურებრივი მდგომარეობით ჩადენილ დანაშაულზე. თუმცა, აქ ზოგადად სამსახურებრივი მდგომარეობის გამოყენებაზე საუბარი არაა. კონკრეტულად სახეზე უნდა გვექონდეს საწარმოში ან სხვა ორგანიზაციაში ხელმძღვანელობითი, წარმომადგენლობითი ან სხვა სპეციალური უფლებამო-

სიღების მქონე პირი, რომელიც ბოროტად იყესებს მისთვის მინიჭებულ უფლებამოსილებას.

განვიხილოთ კაზუსი. გ. სორდია იყო ბანკის ფილიალის მმართველი და ხელი მიუწვდებოდა კლიენტების საკრედიტო ბარათების მონაცემებზე. მან ისარგებლა საკუთარი სამსახურებრივი მდგომარეობით, შეაღწია მონაცემთა ბაზაში, გადმოწერა კლიენტის საკრედიტო ბარათების მონაცემები. შემდეგ შეიძინა ყალბი საკრედიტო ბარათის დამამზადებელი მონეობილობა, დაამზადა ბარათები და მათი გამოყენებით სხვადასხვა პირს ჯამში ჩაიყენა 20 ათას ლარზე მეტი ოდენობის ზიანი.

განხილულ კაზუსში, უფლებამოსილების ბოროტად გამოყენების ფაქტი აშკარაა, რადგან გ. სორდია იყენებდა უფლებამოსილებას, კერძოდ, იმ ფაქტს, რომ მას ხელი კანონიერად მიუწვდებოდა ბანკის მომხმარებლების საკრედიტო ბარათების მონაცემებზე და მოქმედებდა პირადი გამორჩენის მიღების მიზნით. გვაქვს თუ არა სახეზე 284-ე მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული კომპიუტერულ სისტემაში უსებართვო შეღწევა სამსახურებრივი მდგომარეობის გამოყენებით? არა, რადგან გ. სორდიას უნებართვოდ არ უმოქმედია. მას სამსახურებრივი უფლებამოსილების ფარგლებში ხელი კანონიერად მიუწვდებოდა ამ მონაცემებზე. მას არც, 285-ე და 286-ე მუხლით გათვალისწინებული დანაშაულები ჩაუდენია, რადგან არ განუხორციელებია არც კომპიუტერული პროგრამის, მონაცემის და ა.შ. შექმნა, გავრცელება და ა.შ. კიბერდანაშაულის თავით და 158-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის მიზნით და არც კომპიუტერული მონაცემი შეუცვლია, წაუშლია, გაუნადგურებია და დაუფარია უნებართვოდ. თუმცა, ჩაიდინა ყალბი საკრედიტო ბარათის დამზადება, ანუ 210 მუხლის 1-ლი ნაწილით გათვალისწინებული ქმედება. გამოდის, რომ დანაშაულთა ერთობლიობა სახეზეა, ოღონდ არა კიბერდანაშაულთან.

თუ პირს არ გააჩნია აღნიშნულ კომპიუტერულ სისტემაში შესვლის უფლებამოსილება, მაგრამ ის სამსახურებრივი მდგომარეობის გამოყენებით მოიპოვებს მას, რა დანაშაულთან გვექნება საქმე?

მაგალითად, გ. სორდია იყო ქსელის ადმინისტრატორის თანაშემწე, მართალია, მას ხელი არ მიუწვდებოდა ბანკის მომხმარებლის საკრედიტო ბარათის მონაცემზე, მაგრამ მან ისარგებლა

ადმინისტრატორის სამსახურში არყოფნით და მისი ოთახიდან, მისი კომპიუტერის გამოყენებით შეაღწია აღნიშნულ მონაცემთა ბაზაში. შედეგად, ამონერა მისთვის სასურველი ინფორმაცია, რომლის გამოყენებითაც მოგვიანებით დაამზადა ყალბი საკრედიტო ბარათი.

ჩემი აზრით, ეს უფლებამოსილების ბოროტად გამოყენების შემთხვევა არ არის, რადგან ბ. სორდიას არ აქვს ისეთი სპეციალური უფლებამოსილება, როგორც ადმინისტრატორს გააჩნია, მაგრამ იყენებს რა სამსახურებრივ მდგომარეობას, სარგებლობს ადმინისტრატორის სამსახურში არყოფნით, უნებართვოდ აღწევს კომპიუტერულ სისტემაში და ამის შემდეგ ახორციელებს 210-ე მუხლის 1-ლი ნაწილით გათვალისწინებულ დანაშაულს. გამოდის რომ, სახეზეა 284-ე მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტით და 210-ე მუხლის 1-ლი ნაწილით გათვალისწინებული დანაშაული.

ჩემი აზრით, კიბერდანაშაულის სუბიექტის კვლევა ბევრად უფრო საინტერესოა კრიმინოლოგიური თვალსაზრისით, რადგან როგორც მრავალი მეცნიერი აღნიშნავს ე.წ. პაკერობა შესაძლებელია შევადაროთ გარკვეულ მიმდინარეობას, სტილს, მოდას. თუმცა ეს აღნიშნული ნაშრომის კვლევის საგანს არ უკავშირდება, ამიტომ მასზე აღარ შევჩერდები.

7. პასუხისმგებლობის დამამძიმებელი გარემოებები კიბერდანაშაულის ჩადენისთვის

კიბერდანაშაულის თავში შესული სამივე მუხლი ითვალისწინებს დამამძიმებელი გარემოებებს. ესენია: დანაშაული ჩადენილი „წინასწარი შეთანხმებით ჯგუფის მიერ“, „სამსახურებრივი მდგომარეობის გამოყენებით“, „არაერთგზის“, „რამაც მნიშვნელოვანი ზიანი გამოიწვია“ და „რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია“.

წინასწარი შეთანხმებით ჯგუფის მიერ კიბერდანაშაულის ჩადენაზე უკვე ვისაუბრეთ ნაშრომში განხილული სასამართლო პრაქტიკის ანალიზისას.

კიბერდანაშაულის თავში მოცემული მუხლებისთვის დამამძიმებელ გარემოებად ითვლება არაერთგზისობა, რომელიც გათვა-

ლისწინებულია სისხლის სამართლის კოდექსის მე-15 მუხლში: „არაერთგზისი დააშაული ნიშნავს წინათ ნასამართლევი პირის მიერ ამ კოდექსის იმავე მუხლით გათვალისწინებული დანაშაულის ჩადენას.“ ამავე მუხლის შესაბამისად: „კოდექსის სხვადასხვა მუხლით გათვალისწინებული ორი ან მეტი დანაშაული მხოლოდ მაშინ ჩაითვლება არაერთგზის დანაშაულად, თუ ამის შესახებ პირობებულია ამ კოდექსის შესაბამის მუხლში“. ვინაიდან, კიბერდანაშაულის თავში მსგავსი მითითება არ გვხვდება, გამოდის, რომთუ პირი წინათ პასუხისგებაში მიცემული იყო 284-ე მუხლით გათვალისწინებული კომპიუტერულ სისტემაში უნებართვოდ შეღწევისთვის, ხოლო შემდეგ მან ჩაიდინა 286-ე მუხლის მე-2 ნაწილით გათვალისწინებული ქმედება, კერძოდ, განზრახ მნიშვნელოვნად შეაფერხა კომპიუტერული სისტემის ფუნქციონირება, სახეზე არ გვექნება არაერთგზისობა.

ჩემი აზრით, ეს არასწორი მიდგომაა. კიბერდანაშაულის პრევენციისთვის სასურველი იქნებოდა კოდექსში გვექონოდა დათქმა, რომლის მიხედვითაც არაერთგზისობას განაპირობებდა კიბერდანაშაულის თავით განსაზღვრული დანაშაულის ჩადენა და არა ამ თავში შესულ ერთი კონკრეტული მუხლით გათვალისწინებული დანაშაულისთვის ნასამართლეობა.

შემდეგი დამამძიმებელი გარემოება, რომელსაც სისხლის სამართლის კოდექსი ითვალისწინებს კომპიუტერული დანაშაულის ჩადენისთვის არის ისეთი ქმედება, რამაც მნიშვნელოვანი ზიანი გამოიწვია. კანონმდებელი კონკრეტულად განსაზღვრავს რა ოდენობა უნდა ვიგულისხმოთ მნიშვნელოვან ზიანში, კერძოდ, ესაა ზიანი 2000 ლარზე მეტი ოდენობით.

ნაშრომში უკვე აღინიშნა 284-ე მუხლის მე-2 ნაწილის „დ“ ქვეპუნქტთან დაკავშირებით. კერძოდ, გაურკვეველია, როგორ უნდა გამოვთვალოთ მნიშვნელოვანი ზიანი კომპიუტერულ სისტემაში უნებართვოდ შეღწევისას, მაშინ როცა აღნიშნული მუხლი არანაირ თანმდევ შედეგს არ ითვალისწინებს? იმ შემთხვევაში თუ კომპიუტერულ სისტემაში უნებართვოდ შეღწევა გამოიწვევს უარყოფით შედეგს, ავტომატურად სახეზე გვექნება 286-ე მუხლის 1-ლი ნაწილით გათვალისწინებული დანაშაული და შესაბამისად, 284-ე მუხლის „დ“ ქვეპუნქტის გამოყენება აზრს დაკარგავს. აქედან გამომდინარე, მიმაჩნია, რომ იგი ამოღებულ უნდა იქნეს.

აღსანიშნავია, რომ კოდექსის ძველი რედაქცია დამამძიმებელ გარემოებებში არ მიუთითებდა მნიშვნელოვან ზიანზე, თუმცა პასუხისმგებლობის დამძიმებას უკავშირებდა „მძიმე შედეგის“ დადგომას.

„მძიმე შედეგი“ შეფასებითი ცნებაა და იგი ყოველ კონკრეტულ შემთხვევაში საქმის თავისებურების მიხედვით უნდა განსაზღვროს სასამართლომ. ეს შეიძლება იყოს ადამიანის ჯანმრთელობის დაზიანება, ტრანსპორტიდან და კავშირგაბმულობის მუშაობის დეზორგანიზაცია, მნიშვნელოვანი ქონებრივი ზიანი და სხვა. რთულია ვისაუბროთ, რომელი მიდგომაა უფრო სწორი, ზიანის კონკრეტულ თანხაში გამოხატვა თუ შეფასებითი კრიტერიუმის დადგენა, რადგან არ ვართ დაზღვეული სასამართლოს მიერ სუბიექტური გადანყვეტილების მიღებისგან. კერძოდ, თუ არ იქნება დადგენილი შეფასების კრიტერიუმი შესაძლებელია, სხვადასხვა მოსამართლემ „მძიმე შედეგი“ განმარტოს სხვადასხვაგვარად, მაგრამ ისიც უნდა აღინიშნოს, რომ ზიანის კონკრეტული თანხით განსაზღვრაც არ გამორიცხავს უსამართლო გადანყვეტილების მიღების შესაძლებლობას. მაგალითად, იმ შემთხვევებში როდესაც კიბერდამნაშავე კომპიუტერულ სისტემაში უნებართვო შეღწევის გზით 1997 ლარის ოდენობის ზიანი მიაყენებს ვინმეს, დაისჯება 284-ე მუხლის 1-ლი ნაწილით გათვალისწინებული ქმედების ჩადენისთვის, თავისუფლების აღკვეთით 2 წლამდე, ხოლო სხვა პირი ვინც ჩაიდინა იგივე ქმედება და ზიანმა 2001 ლარი შეადგინა, დაისჯება 284-ე მუხლის მე-2 ნაწილით გათვალისწინებული ქმედების ჩადენისთვის და შესაძლოა სასჯელად განესაზღვროს თავისუფლების აღკვეთა ორიდან ხუთ წლამდე. გამოდის, რომ 4 ლარის ოდენობის ზიანმა შესაძლოა განაპირობოს სამი წლით გაზრდილი სასჯელი, რაც აშკარად ბაღებს კითხვას, რომ ხომ არ ჯობია, კოდექსში დამამძიმებელ გარემოებად დარჩენილიყო „მძიმე შედეგი“, კანონმდებელს ან თუნდაც უზენაეს სასამართლოს დაედგინა შეფასების კრიტერიუმები და შემდეგ სასამართლოს თავად შეეფასებინა ყველა გარემოება კონკრეტული საქმის განხილვისას და განესაზღვრა მუხლის რომელი ნაწილით უნდა ეცნო ბრალეულად კიბერდამნაშავე? ჩემი აზრით, ეს ბევრად სამართლიანი იქნებოდა.

კიდევ ერთ დამამძიმებელ გარემოებას, ვხვდებით 286-ე მუხლის მე-2 ნაწილში „ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, აგრეთვე კომპიუტერული მონაცემის უნებართვო ჩასმა

ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია". ზემოთ უკვე განვიხილეთ, ამ დანაშაულის ობიექტური მხარე და ახლა მარტივია დავასკვნათ, რა სახის შეიძლება იყოს ეს შეფერხება. მნიშვნელოვანია თუ არა შეფერხება, განისაზღვრება დაქმდარი ზიანის ოდენობით, შეფერხების ხანგრძლივობით, კერძოდ, თუ დაზიანდება ავიაკომპანიის კომპიუტერული სისტემის მონაცემები, რის გამოც შეფერხდება მისი კომპიუტერული სისტემის ფუნქციონირება, საინტერესოა, რა ვადით ველარ ღირსება ბილეთების დაჯავშნა, ფრენის განხორციელება და ა.შ. რადგან ამ შემთხვევაში შეფერხების სირთულე, სიმძიმე და მნიშვნელობა დაშოკებულია სწორედ მსგავს ფაქტორებზე.

კოდექსის ძველ რედაქციაში გათვალისწინებული იყო ერთი ისეთი დამამძიმებელი გარემოება, რომელსაც ახალი რედაქცია არ ითვალისწინებს. კერძოდ, 284-ე მუხლის მე-2 ნაწილის „გ“ ქვეპუნქტის მიხედვით 284-ე მუხლის 1-ლი ნაწილით გათვალისწინებული დანაშაულის, კერძოდ, „კანონით დაცულ ინფორმაციასთან არამართლზომიერი შელწევა, რამაც გამოიწვია ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან მოპოვება, ანდა ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლა, ასევე მობილური მონაცემების საერთაშორისო იდენტიფიკატორის შეცვლა“ იმ პირის მიერ ჩადენა, ვისაც ხელი მიუწვდებოდა ეგმ-ზე, ეგმ-ის სისტემაზე ან მათ ქსელზე. ასეთ პირად უნდა მივიჩნიოთ აღნიშნული ეგმ-ის, ეგმ-ის სისტემის და მათი ქსელის ოპერატორი, ადმინისტრატორი, დაქირავებული პირი, რომელსაც ევალება ეგმ-ის შეკეთება, მაგრამ ბოროტად სარგებლობს ამ უფლებით და ა.შ.

ჩემი აზრით, იმ პირის მიერ კიბერდანაშაულის ჩადენა, რომელსაც ხელი მიუწვდებოდა ეგმ-ის, ეგმ-ის სისტემის ან მათ ქსელზე უნდა განვიხილოთ როგორც სამსახურებრივი მდგომარეობის გამოყენებით ჩადენილი დანაშაული. თუმცა შესაძლოა სახეზე გვექონდეს გამონაკლისიც. მაგალითად, როცა ხდება კერძო პირის ერთჯერადი დაქირავება კომპიუტერის შეკეთების მიზნით, თუმცა ის ბოროტად სარგებლობს ამ უფლებით და სჩადის კიბერდანაშაულის თავით განსაზღვრულ რომელიმე ქმედებას. ალბათ, სწორედ ამ მოტივით კანონმდებელი კოდექსის ძველ რედაქციაში ითვალისწინებდა

როგორც, სამსახურებრივი მდგომარეობის გამოყენებით დანაშაულის ჩადენისთვის დამძიმებულ პასუხისმგებლობას, ასევე, იმ პირის მიერ ვისაც ხელი მიუწვდებოდა ეგმ-ზე, ეგემ-ის სისტემაზე ან მათ ქსელზე. ამ შემთხვევაში ძველი რედაქციის მიდგომა უფრო სრულყოფილად უნდა მივიჩნიოთ.

ზემოთ უკვე აღინიშნა, რომ კიბერდანაშაულის თავში დამამძიმებელ გარემოებად არ გეხვდება „ანგარება“. ვინაიდან იგი კომპიუტერული დანაშაულის ჩადენის ერთ-ერთ მთავარი მამოძრავებელი მოტივია. ჩიზანშენონილია, კიბერდანაშაულის თავში შემავალი თითოეული მუხლისთვის მისი დამამძიმებელ გარემოებად მითითება.

8. იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობა კიბერდანაშაულის ჩადენისთვის 11

„კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციის მე-12 მუხლის შესაბამისად, „ყველა მონაწილე სახელმწიფო ვალდებულია, მიიღოს ისეთი საჭირო საკანონმდებლო და სხვა ზომები, რომელიც უზრუნველყოფს ამ კონვენციის მიერ გათვალისწინებულ დანაშაულთა ჩამდენ იურიდიულ პირთა პასუხისმგებლობას, თუ ეს ქმდება ჩადენილია მათ სასარგებლოდ ნებისმიერი ფიზიკური პირის მიერ ინდივიდუალურად, თუ როგორც იურიდიული პირის ორგანოს იმ წარმომადგენლის მიერ, რომელსაც ამ დანესებულებაში უკავია ნამყვანი თანამდებობა, რაც თავის მხრივ ეფუძნება: იურიდიული პირის წარმომადგენლის, იურიდიული პირის სახელით გადანყვეტილების მიღების და იურიდიული პირის მართვის უფლებამოსილებას.“

მსგავსად კონვენციისა, ევროკავშირის საბჭოს 2005 წლის 24 თებერვლის ჩარჩო გადანყვეტილება ადგენს იურიდიული პირის სისხლისსამართლებრივ პასუხისმგებლობას, თუმცა განსხვავებით კონვენციისგან, მისი მოქმედების სავალდებულობა ვრცელდება მხოლოდ ევროკავშირის წევრ ქვეყნებზე. გადანყვეტილებაში ეხვდებით, როგორც კონვენციის მსგავს, ასევე განსხვავებულ სასჯელის სახეებს. კერძოდ, იურიდიული პირისთვის საზოგადოებრივი სარგებლის ან დახმარების მიღების უფლებამოსილების ჩამორთმევა, კომერციულ საქმიანობაში დროებითი ან მუდმივი დისკვალიფი-

კაცია, იურიდიული ზედამხედველობის დანესება, სამართლებრივი ლიკვიდაცია¹¹⁹.

აღნიშნული გადანაცვეტილებაც და კონვენციაც მოითხოვს, რომ ყველა სახელმწიფომ დაადგინოს იმ ფიზიკური პირის პასუხისმგებლობა, რომლის მხრიდანაც, კომპანიის მართვაში განუღმე არა-ჯეროვანმა ძალისხმევამ ან/და კონტროლმა შესაძლებელი გახადა იმ იურიდიული პირის სასარგებლოდ დანაშაულის ჩადენა, რომლის მართვის ან/და წარმომადგენლობის უფლებამოსილებითაც სარგებლობდა აღნიშნული ფიზიკური პირი. ეს დათქმა შეიძლება შევადაროთ საქართველოს სისხლის სამართლის კოდექსის 220¹ მუხლით გათვალისწინებულ დანაშაულს, რომელიც დასჯადად აცხადებს „გულგრილობას,“ ესე იგი სანარმოში ან სხვა ორგანიზაციაში ხელმძღვანელობითი, წარმომადგენლობითი ან სხვა სპეციალური უფლებამოსილების მქონე პირის მიერ თავისი სამსახურებრივი მოვალეობის შეუსრულებლობას ან არაჯეროვნად შესრულებას მისდამი დაუდევარი დამოკიდებულების გამო, რამაც გამოიწვია სახელმწიფოს კანონიერი ინტერესების არსებითი დარღვევა.“ უნდა ითქვას, რომ თუ არ ჩავთვლით მითითებას დანაშაულის შედეგზე, ეს მუხლი კონვენციის სპეციალურ დათქმას ფიზიკური პირის სისხლისსამართლებრივ პასუხისმგებლობაზე სრულად შეესაბამება.

აღსანიშნავია, რომ ზემოაღნიშნულ დათქმასთან და ზოგადად იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობის დანესებასთან დაკავშირებით განსხვავებული მიდგომა აქვთ ევროპის ზოგიერთ ქვეყანაში. კერძოდ, საფრანგეთში და ესტონეთში მიიჩნევენ, რომ ეს სამოქალაქო სამართლის რეგულირების სფეროა. იურიდიული პირების მიმართ სისხლისსამართლებრივი პასუხისმგებლობის დანესება არ მოუხდენია ასევე, ჩეხეთს, ლატვიას, ლუქსემბურგს, დანიას, ფინეთსა და პორტუგალიას. ამ ქვეყნების პოზიციის გაზიარება მიზანშეწონილად მიმაჩნია. მათ რიცხვში არ აღმოჩნდა საქართველო, რომელმაც დაადგინა იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობა კომპიუტერული დანაშაულის ჩადენისთვის.

119 იხ. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Article 8-9. (Official journal of the European Union L69/67, from 16.3.2005)

მიუხედავად ამისა, საქართველოში იურიდიული პირის სისხლის-სამართლებრივი პასუხისმგებლობის მიზანშეუწონლობაზე, მრავალი საინტერესო მოსაზრება გამოითქვა.

პროფ. მ. ტურავას ნაშრომში „დანაშაულის მოძღვრება“ მოჰყავს გერმანიის მაგალითი და აღნიშნავს, „იურიდიული პირი ბუნებრივი თვალსაზრისით არ არის ქმედუნარიანი და არ არის შესაძლებელი მასზე სისხლისსამართლებრივი პასუხისმგებლობის დაკისრება. ასეთ დასჯადობას მიიჩნევენ ასევე ბრალეული პასუხისმგებლობის პრინციპთან შეუსაბამოდ.“¹²⁰

გერმანული მიდგომის საწინააღმდეგოდ ა. ოხანაშვილის მიერ გამოითქვა საგულისხმო შეფასება: „საქმე ის გახლავთ, რომ იურიდიული პირის სისხლისსამართლებრივი წესით დაუსჯელობა ღიად ტოვებს ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის პრობლემას. კერძოდ, სამენარმო საქმიანობის სფეროში იშვიათად ხდება კორპორაციების მხრივ რიგი დანაშაულებრივი ქმედებების ჩადენა (მაგალითად, სამენარმო დანაშაულის მფარველობა, ორგანიზაციული ხასიათის უპასუხისმგებლობა, რაც შესაძლებელს ხდის დანაშაულის ჩადენას და სხვა.).“¹²¹

„სისხლის სამართლის კერძო ნაწილის“ ავტორების შეფასებით: „სისხლისსამართლებრივი პასუხისმგებლობა მკაცრად პერსონალურია. საზოგადოება (კორპორაცია) ყოველთვის მოქმედებს მხოლოდ ფიზიკური პირების მეშვეობით, სწორედ ისინი არიან დანაშაულის უშუალო ამსრულებლები და უნდა იდევნებოდნენ სისხლის სამართლის წესით. იურიდიული პირისთვის იმანენტური არ არის ბრალუნარიანობა და დასჯადუნარიანობა. კერძოდ, შეუძლებელია იურიდიული პირის ბრალეულობის დასაბუთება, ბრალის ტრადიციული გაგების საფუძველზე. იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობის იდეა წინააღმდეგობაში მოდის დასჯის პერსო-

120 იხ. მ. ტურავა, „დანაშაულის მოძღვრება“, წიგნი I, გამომც. „მერიდიანი“, თბ. 2011წ. გვ.619-620

121 იხ. ა. ოხანაშვილი, „იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობა“, თბილისის ივ. ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ჟურნალი, 2009წ. №2, გვ. 200

ნალურობის პრინციპთანაც.¹²² ამ პირობის სრულად ვიზირება.

გ. ნაჭყებია აზრით, „ამკარაა, რომ ბრალის ფსიქოლოგიური თეორია, რომლის თანახმად, ბრალი არის ქმედებისა და მისი შედეგებისადმი სუბიექტის ფსიქიკური დამოკიდებულება, მით უფრო გამოუსადეგარია იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობის დასაბუთებისთვის. მით უმეტეს, რომ იურიდიული პირის საქმიანობაში საქმე ეხება არა ფსიქოლოგიის სფეროს, არამედ, საზოგადოებრივ ურთიერთობათა მრავალფეროვნებას“.¹²³

ზემოაღნიშნული მსჯელობებს ნაწილობრივ ვეთანხმები, მაგრამ ზოგადად იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობის საკითხის მიზანშეწონილობის განხილვა სცდება ნაშრომის კვლევის მიზანს და შესაბამისად მასზე ზოგადად არ ვისაუბრებ. თუმცა მიმაჩნია, რომ კიბერდანაშაულის შემთხვევაში, იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობა განსაკუთრებულად მიუღებელია. განვიხილოთ თუნდაც საქართველოს სისხლის სამართლის კოდექსის ის დათქმა, რომლის მიხედვითაც იურიდიული პირი პასუხს აგებს იმ შემთხვევაშიც, დადგინდება თუ არა დანაშაულის ჩამდენი ფიზიკური პირი. ასეთი რეგულაციის პირობებში ძალიან იოლია პაკერის დაქირავება კონკურენტი იურიდიული პირის სასარგებლოდ გარკვეული დანაშაულებრივი ქმედების განსახორციელებლად, რომ მომავალში ამ მანიპულაციის შედეგად აღნიშნულმა ფაქტმა კონკურენტი იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობა გამოიწვიოს. ცხადია, რომ ფარული მანიპულაციის და ლავირების საშუალებას ყველაზე მეტად კომპიუტერული სისტემა და კომპიუტერული დანაშაული იძლევა. ამ დებულების სასარგებლოდ განვიხილოთ მაგალითი: შესაძლებელია ისეთი დამაზიანებელი კომპიუტერული პროგრამის შექმნა, რომელიც ადრესატის სიტყვაში მოხედება ჩვეულებრივი ელექტრონული საფოსტო გზავნილის სახით. მისი გამომგზავნის გრაფაში კი მინიშნებული იქნება საზოგადოებისთვის სანდო რომელიმე ორგანიზა-

122 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი I, გამომც. „მერიდიანი“, თბ. 2011წ. გვ.11

123 იხ. გ. ნაჭყებია, „სისხლის სამართალი, ზოგადი ნაწილი“, საგამომცემლო სახლი „ინოვაცია“, თბ. 2011წ. გვ. 444

ცია, მაგალითად: „საჯარო რეესტრის ეროვნული სააგენტო“, „თიბისი ბანკი“ და ა.შ. ის პირები, ვინც გზავნილს გახსნიან, საკუთარ კომპიუტერულ სისტემაში გააქტიურებენ აღნიშნულ დამაზიანებელ პროგრამას, რის შედეგადაც მიაღებათ ზიანი, იქნება ეს ინფორმაციის განადგურება, კოპირება, შეცვლა თუ სხვა. ამ შემთხვევაში თუკი ვერ ვიპოვნით რეალურ დამნაშავეს უნდა გავასამართლოთ „საჯარო რეესტრის ეროვნული სააგენტო“ და „თიბისი ბანკი“? როგორ დავამტკიცოთ, რომ დამაზიანებელი პროგრამის გამომგზავნში აღნიშნული ორგანიზაცია შეგნებულად მიუთითეს, მაშინ როცა კომპიუტერული დანაშაულის ჩადენასთან დაკავშირებული მტკიცებულების მოპოვება ურთულესი პროცესია.

სისხლის სამართლის კოდექსის ასეთი მიდგომა, ჩემი აზრით, გაუმართლებელია, რადგან კომპიუტერული დანაშაულის მასშტაბი სცილდება ყოველგვარ ფიზიკურ და ნარმოსახვით საზღვარს და მსგავსმა საკანონმდებლო ჩანაწერმა შეიძლება დიდი ზიანი მიაყენოს სრულიად უდანაშაულო იურიდიულ პირსაც. ამიტომ, საჭიროა სამეცნიერო ნრევებში დისკუსიის გაგრძელება და მისი შედეგის ანალიზი.

აქვე ხაზგასმით უნდა აღინიშნოს, რომ კომპიუტერული დანაშაულის ჩადენისთვის იურიდიული პირის პასუხისმგებლობაში მიცემის საქმე საგამოძიებო ან/და სასამართლო პრაქტიკაში ჯერ არ მოიძებნება.

საქართველოს სისხლის სამართლის კოდექსში ასახული „კიბერდანაშაულის შესახებ“ კონვენციით გათვალისწინებული დანაშაულები, რომლებიც დაკავშირებულია კომპიუტერის გამოყენებასთან

1. კერძო კომუნიკაციის საიდუმლოების დარღვევა

საქართველოს კონსტიტუციის მე-20 მუხლის შესაბამისად, „ყოველი ადამიანის პირადი ცხოვრება, პირადი საქმიანობის ადგილი, პირადი ჩანაწერი, მიმოწერა, საუბარი სატელეფონო და სხვა სახის ტექნიკური საშუალებით, აგრეთვე ტექნიკური საშუალებებით მიღებული შეტყობინებანი ხელშეუხებელია. აღნიშნული უფლებების შეზღუდვა დაიშვება სასამართლოს გადაწყვეტილებით ან მის გარეშეც, კანონით გათვალისწინებული გადაუდებელი აუცილებლობისას.“

საქართველოს სისხლის სამართლის კოდექსის 158-ე მუხლი წარმოადგენს პირადი ცხოვრების ხელშეუვალობის დაცვის ერთ-ერთ გარანტიას. იგი დღეს არსებული სახით ჩამოყალიბდა „კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციის მე-3 მუხლის და საქართველოს სისხლის სამართლის კოდექსში მანამდე არსებული 158-ე მუხლის რედაქციების შერწყმის შედეგად.

ევროპის საბჭოს კონვენციის მე-3 მუხლის შესაბამისად აკრძალულია მონაცემთა უნებართვოდ ხელში ჩაგდება. მუხლი ჩამოყალიბებულია შემდეგნაირად: „იქველა პირი, რომელიც სახელმწიფო ვალდებულია მიიღოს ისეთი საჭირო საკანონმდებლო და სხვა ზომები, რომლებიც ეროვნული კანონმდებლობით მოახდენს კომპიუტერული სისტემისთვის, სისტემიდან ან მის ფარგლებში არასაჯარო კომპიუტერულ მონაცემთა გაცემის, მათ შორის კომპიუტერული სისტემიდან ამგვარ კომპიუტერულ მონაცემთა მატარებელი ელექტრომაგნიტური ტალღების ემისიის უნებართვოდ ხელში ჩაგდების კრიმინალიზაციას, როცა ეს ქმედება ტექნიკური საშუალებითაა განხორციელებული და თუ იგი წინასწარი გახიზნავითაა ჩადენილი.“

ქართველმა კანონმდებელმა ევროპის საბჭოს კონვენციის მე-3 მუხლით გათვალისწინებული დანაშაული დამოუკიდებელ მუხლად არ გაითვალისწინა და უკვე არსებული 158-ე მუხლი შეცვალა. 158-ე მუხლი კერძო კომუნიკაციის საიდუმლოების დარღვევას ეხება და მასში გათვალისწინებულია პასუხისმგებლობა კერძო საუბრის უნებართვო ჩანერა ან მიყურადებაზე, აგრეთვე კომპიუტერულ სისტემაში ან სისტემაიდან კერძო კომუნიკაციისას გადაცემული კომპიუტერული მოსაცემის ან ამგვარი მონაცემის მატარებელი ელექტრომაგნიტური ტალღების, უნებართვო მოპოვებაზე ტექნიკური საშუალების გამოყენებით.

კანონმდებელი ამიძიებს პასუხისმგებლობას კერძო კომუნიკაციის ჩანანერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ გამოყენებისა ან გავრცელებისთვის. გარდა, ამისა მუხლის მე-3 ნაწილი დამამძიმებელ გარემოებად გამოყოფს 158-ე მუხლის 1-ლი და მე-2 ნაწილში გათვალისწინებული ქმედებას ჩადენილს: ანგარებით, არაერთგზის, რამაც მნიშვნელოვანი ზიანი გამოიწვია და სამსახურებრივი მდგომარეობის გამოყენებით.

სანამ მუხლის დეტალურ განხილვაზე გადავალთ, ყურადღება უნდა გავამახვილოთ სისხლის სამართლის კოდექსის 159-ე მუხლზე, რომელიც ეხება პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევას. მუხლის შესაბამისად დასჯადია: „პირადი მიმოწერის ან საფოსტო გზავნილის, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ან/და ტელეგრაფით, ფაქსით ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების საიდუმლოების უკანონოდ დარღვევა“ ტერმინი „საიდუმლოების დარღვევა“ ფართო მნიშვნელობისაა და მასში უნდა ვიგულისხმოთ როგორც საუბრის ჩანერა, ასევე ამ ჩანანერის გადაცემა, გავრცელება და ა.შ. 159-ე მუხლის დისპოზიცია ბევრად ზოგადია და ის არ არის შეზღუდული ქმედების ჩადენის ხერხით. ის მოიცავს ნებისმიერი ტექნიკური საშუალებით გადაცემული და მიღებული შეტყობინების, საუბრის და ა.შ. საიდუმლოების დარღვევას. ამიტომ მასში უნდა ვიგულისხმოთ ინფორმაციის გადაცემის ნებისმიერი საშუალება, მათ შორის კომპიუტერული ტექნიკა, სისტემა და სხვა მონაცემილობა.

158-ე მუხლში მითითებულია არა მხოლოდ საუბარსა ან შეტყობინებაზე, არამედ კომპიუტერულ მონაცემის გადაცემაზეც. კომპიუტერული მონაცემის ქვეშ კი იგულისხმება: ფოტო, ვიდეო, აუდიო ფაილები, კომპიუტერული პროგრამები, ელექტრონული ფორმით ნაწარმოები საბუღალტრო დოკუმენტები და ა.შ. ეს კი რამდენად შეიძლება მოექცეს პირად ჩიმონერაში, საფოსტო გზავნილში, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ან/და ტელეგრაფით, ფაქსით ან სხვა ტექნიკური საშუალებით მიღებულ ან გადაცემულ შეტყობინებაში? ჩემი აზრით, შესაძლებელია მოექცეს, რადგან 159-ე მუხლი არ აკონკრეტებს პირადი მიმოწერის და შეტყობინების შინაარსს, ხასიათს, ზომას, ტიპს. აქედან გამომდინარე, მასში უნდა ვიგულისხმოთ ნებისმიერი შინაარსის ინფორმაცია, რისი გადაცემაც შესაძლებელია ფოსტით, ტელეგრაფით ან სხვა ტექნიკური საშუალებით. ეს უკანასკნელი კი სრულ შესაძლებლობას იძლევა გადაეცეთ ან მივიღოთ ნებისმიერი ტიპის კომპიუტერული მონაცემი.

იგივე შეიძლება ითქვას 158-ე მუხლის მეორე ნაწილზეც, რადგან კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ გამოყენება და გავრცელება აბსოლუტურად შეესაბამება 159-ე მუხლით გათვალისწინებულ პირადი მიმოწერის ან საფოსტო გზავნილის ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების საიდუმლოების უკანონოდ დარღვევას. თუ კანონმდებელს სურდა პირად მიმოწერაში პირადი ხასიათის წერილები, სასიყვარულო ბარათები, სამსახურებრივი მოხსენებითი ბარათები და ა.შ. ეგულისხმა მაშინ უნდა გამოეყენებინა უფრო კონკრეტული ტერმინები.

საინტერესოა, მობილური ტელეფონის საშუალებით ე.წ. ბლუ-თუსით ვიდეო ფაილის მეგობრისთვის გადაგზავნა რამდენად შეესაბამება პირად საუბარს, ან „სკაიპით“ სამეცნიერო კვლევის შესახებ ფაილის გადაცემის პროცესი, როგორ შეიძლება გავავიგოთ ფაქსით შეტყობინების გადაცემასთან? ჩემი აზრით, შეესაბამება, რადგან შეტყობინების მნიშვნელობაში უნდა ვიგულისხმოთ ნებისმიერი შინაარსის თუ ტიპის დოკუმენტი და ინფორმაცია.

მიმაჩნია, რომ 158-ე და 159-ე მუხლები შინაარსობრივად იმდენად ერწყმის ერთმანეთს, უმჯობესი იქნებოდა მათი ერთ შემადგენლობად გაერთიანება, უფრო მეტიც, რთულია, გადაჭრით ვთქვათ, რომელია მათგან უფრო ზოგადი ან კონკრეტული მუხლი.

ახლა, კი უფრო დეტალურად 158-ე მუხლის შესახებ. მისი ინტეგრირება სისხლის სამართლის კოდექსში ევროპის საბჭოს კონვენციის მოთხოვნათა დაცვით განხორციელდა და იგი სრულად შეესაბამება მას. ზოგადად ამ ტიპის დანამაულებრივი შემადგენლობის სისხლის სამართლის კოდექსში არსებობა ძალიან მნიშვნელოვანია კომპიუტერული დანამაულის წინააღმდეგ ბრძოლაში, რადგან ინფორმაციის გადაცემის დროს, შესაძლებელია გადაცემის პროცესში არსებული მოწინავემის ხელში ჩაგდება, რისი ერთ-ერთი მაგალითიც გახლავთ ისტორიის გადაცემის დროს კომუნიკაციის ჩანერა უკაბელო ქსელში. მაგალითად, თუ დამნაშავე ხელში ჩაიგდება გადაცემის პროცესში არსებულ კომუნიკაციას კომპიუტერულ სისტემასა და შელწევის უკაბელო პუნქტს შორის, მას შეუძლია მოიპოვოს ნებისმიერი დაუშიფრავი კომუნიკაცია, როგორცაა გზავნილი ან მიღებული ელექტრონული საფოსტო შეტყობინება ან გახსნილი ვებ-გვერდი. თუ მხედველობაში მივიღებთ საკომუნიკაციო საშუალებასთან უკაბელო კავშირის ხელმისაწვდომობას (მობილური კავშირი ე.წ. ბლუთუსის საშუალებით), აუცილებელი ხდება ყურადღება მივაქციოთ უნებართვო შელწევისგან ტექნოლოგიების დაუცველობას¹²⁴. გარდა ამისა, აღნიშნული ქმედების კრიმინალიზაციით ევროპის საბჭოს კონვენცია მიზნად ისახავდა სატელეფონო საუბრის უკანონო მოსმენისგან დაცვის გათანაბრებას ინფორმაციის ელექტრონული გადაცემის დაცვასთან¹²⁵.

ევროპის საბჭოს კონვენციის განმარტებით ბარათში აღნიშნულია, რომ თუ ინფორმაციის გადაცემის პროცესი კონფიდენციალურია, იგი არ არის საჯარო. გარდა ამისა, ქმედება ჩადენილი უნდა იყოს წინასწარი განზრახვით და უნებართვოდ. ასევე უნდა ითქვას,

124 იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანამაულის შესახებ: ტრენინგის სახელმძღვანელო“, ევროსაბჭო, სტრასბურგი, 2010წ. გვ. 49

125 იხ. იქვე.

რომ მოცემული დისპოზიცია მოიცავს მხოლოდ გადაცემული მონაცემის ხელში ჩაგდებას და არ ეხება კომპიუტერში შენახული ინფორმაციის ხელში ჩაგდებას, ხოლო კომპიუტერში შენახულ ინფორმაციაში შეღწევა, თავის მხრივ, ვერ ჩაითვლება კერძო კომუნიკაციის საიდუმლოების დარღვევად, რადგან სახეზე არ გვექნება ინფორმაციის გადაცემის მიმდინარე პროცესი¹²⁶. ცხადია, ეს უკანასკნელი არ შეიძლება ჩაითვალოს ხარვეზად, რადგან უნებართვო შეღწევისთვის პასუხისმგებლობას კოდექსი ცალკე ითვალისწინებს. ეს გამორიცხავს რაიმე სახის გაუგებრობას ქმედების დანაშაულად კვალიფიკაციისას.

მოცემული ნორმით დაცულ ძირითად ინტერესს წარმოადგენს პირადი ცხოვრების ხელშეუხებლობა, ხოლო დამატებითი ობიექტი შესაძლოა იყოს საკუთრების უფლება ინფორმაციაზე ან იმ კომპიუტერული სისტემების უსაფრთხოება, რომელთა შორისაც დამყარებულია კავშირი ინფორმაციის გადაცემის მიზნით.

დანაშაულის ობიექტური შემადგენლობა გულისხმობს კერძო საუბრის უნებართვო ჩანერას ან მიყურადებას, აგრეთვე კომპიუტერულ სისტემაში ან სისტემიდან კერძო კომუნიკაციისას გადაცემული კომპიუტერული მონაცემის ან ამგვარი მონაცემის მატარებელი ელექტრომაგნიტური ტალღების უნებართვო მოპოვებას ტექნიკური საშუალების გამოყენებით. ეს გულისხმობს საუბრის შინაარსის ჩანერას იმ პირის თანხმობის გარეშე, რომელიც საუბრობს და, მეორეს მხრივ, ამგვარი საუბრის მოსმენას ან კომპიუტერული მონაცემის მოპოვებას კანონიერი საფუძვლის გარეშე.¹²⁷ ამ დანაშაულში უნებართვო გულისხმობს იმ შემთხვევას, როცა უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისთვის.

კომპიუტერული მონაცემების გადაცემისას უნებართვო ხელში ჩაგდება ტექნიკურად მხოლოდ ამ საკომუნიკაციო ურთიერთობაში უნებართვო შეღწევითაა შესაძლებელი. შეგვიძლია წარმოვიდგინოთ

126 იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ: ტრენინგის სახელმძღვანელო“. ევროსაბჭო, სტრასბურგი, 20106. გვ. 50

127 ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, ნიგნი I, გამოშვ. „მერიდიანი“, თბ. 2011წ. გვ. 302

საქართველოში საკმაოდ პოპულარული მომსახურება: ე.წ. „ვაი-ფაი“ (Wi-Fi¹²⁸). მასში შეღწევა არ წარმოადგენს ტექნიკურ სირთულეს. ამისთვის საკმარისია მხოლოდ იმ ტერიტორიაზე ყოფნა, სადაც მიიღება სათანადო სიგნალი. იმ შემთხვევაში, თუ მისი მფლობელი ე.წ. „ვაი-ფაით“ სარგებლობისას არ ახდენს მისი პაროლით დაცვას, მასში შეღწევა შეუძლია ნებისმიერ პირს. მაგალითად, მეზობელ სახლში მაცხოვრებელს და აქის შემდეგ, ბუნებრივია, დამნაშავეს ეძლევა საშუალება, სპეციალური კომპიუტერული პროგრამის დახმარებით, უშუალოდ და უნებართვოდ ჩაერიოს საკომუნიკაციო პროცესში.

158-ე მუხლის მეორე ნაწილში ობიექტურ შემადგენლობას ქმნის მოპოვებული ინფორმაციის უკანონო გამოყენება ან გავრცელება. გამოყენება შეიძლება მიზნად ისახედეს შანტაჟს, პირის რეპუტაციის შელახვას.

მუხლის მე-3 ნაწილში დამამძიმებელ გარემოებად მითითებულია 158-ე მუხლით გათვალისწინებული ქმედების ჩადენა ანგარებით, არაერთგზის, რამაც მნიშვნელოვანი ზიანი გამოიწვია, სამსახურებრივი მდგომარეობის გამოყენებით. მათზე აღარ შეეჩერდები, ვინაიდან ისინი ნაშრომში უკვე განხილულია.

სუბიექტური შემადგენლობა პირდაპირ განზრახვას გულისხმობს, რადგან უნებართვო ჩანჩრა, მიყურადება, მონაცემის მოპოვება ისეთი ქმედებაა, რომელიც საჭიროებს მკაცრად განსაზღვრულ გეგმას და პირის ცალსახა გადაწყვეტილებას, ჩაიდინოს იგი. ევროპის კონვენციაში მითითებულია, რომ მსგავსი ქმედება დანაშაულად უნდა ჩაითვალოს თუ ის ჩადენილია წინასწარი განზრახვითა და უნებართვოდ.

128 Wi-Fi - Wireless Fidelity - „უკაბელო სიზუსტე“ - უკაბელო ინტერნეტი, რომელსაც გააჩნია დაფარვის ზონა, სადაც, როგორც წესი, ერთ ან მეტ პირს როგორც კომპიუტერით, ასევე მობილურით შეუძლია ჩაერთოს და ისარგებლოს ამ მომსახურებით. აღნიშნული მომსახურების ერთ-ერთ ნაკლად სწორედ მასში უნებართვოდ ადვილად შეღწევადობა სახელდება (<http://ru.wikipedia.org/wiki/Wi-Fi>).

2 პორნოგრაფიული ნაწარმოების ან სხვა საგნის უკანონოდ დამზადება ან გასაღება

ბოლო წლებში ინტერნეტი გახდა ბავშვთა პორნოგრაფიით ვაჭრობის ძირითადი საშუალება. ამ მოვლენას ხელს უწყობს ორი ძირითადი ფაქტორი:

1. ინტერნეტი უნიკალურ საშუალებას იძლევა ინფორმაციის გავრცელებისთვის. მასში ფაილის განთავსება მილიონობით აბონენტს აძლევს საშუალებას გადანეროს ის. აღნიშნული ფაქტორი კი ხელს უწყობს ბავშვთა პორნოგრაფიის მომხმარებელთა რაოდენობის ზრდას დისტრიბუციის სხვა ტრადიციულ გზებთან შედარებით.

2. პორნოგრაფიული მასალის შემცველი ვებ-გვერდის პოპულარობას განაპირობებს ის გარემოება, რომ მომხმარებელს აქვს მეტი კონსპირაციის საშუალება, რადგან პირდაპირი გაგებით „არ ჩანან“. ჩვეულებრივ მაღაზიაში პორნოგრაფიული მასალის შეძენა კი ინვესტ გარკვეულ დისკომფორტს.¹²⁹

ევროპის საბჭოს კონვენციის მე-9 მუხლით განსაზღვრულია ბავშვთა პორნოგრაფიასთან დაკავშირებული დანაშაული. ამ მუხლის მიხედვით: „ყველა მონაწილე სახელმწიფო ვალდებულია მიიღოს ისეთი საჭირო საკანონმდებლო და სხვა ზომები, რომლებიც ეროვნული კანონმდებლობით მოახდენს წინაწარი განზრახვითა და მართლსაწინააღმდეგოდ ჩადენილ შემდეგ ქმედებათა კრიმინალიზაციას, სახელდობრ:

ა) კომპიუტერული სისტემის საშუალებით ბავშვთა პორნოგრაფიის შექმნა მისი გავრცელების მიზნით;

ბ) ბავშვთა პორნოგრაფიის შეთავაზება ან ხელმისაწვდომობის უზრუნველყოფა კომპიუტერული სისტემის მეშვეობით;

გ) ბავშვთა პორნოგრაფიის გავრცელება ან გადაცემა კომპიუტერული სისტემის საშუალებით;

დ) ბავშვთა პორნოგრაფიის გადანერა თავისთვის ან სხვისთვის, კომპიუტერული სისტემის საშუალებით;

¹²⁹ იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ: ტრენინგის სახელმძღვანელო“. ევროსაბჭო, სტრასბურგი, 20106. გვ. 65

ე) ბავშვთა პორნოგრაფიის ფლობა კომპიუტერული სისტემის ან კომპიუტერული მონაცემების შესანახი ნებისმიერი საშუალებით."

კონვენცია ბავშვთა პორნოგრაფიას განმარტავს, როგორც ვიზუალურ მასალას, რომელიც გამოისახავს აშკარა სექსობრივი ხასიათის ქმედებით დაკავებულ არასრულწლოვანს ან ადამიანს, რომელიც გამოიყურება როგორც არასრულწლოვანი.

კონვენციის შესაბამისად, არასრულწლოვანში იგულისხმება 18 წლამდე ყველა პირი, თუმცა კონვენციის მონაწილე ნებისმიერ სახელმწიფოს უფლება აქვს ასაკობრივი ზღვარი დანიოს 16 წლამდე.

აღსანიშნავია, რომ არასრულწლოვანთა სექსუალური ექსპლუატაციისგან დასაცავად ევროპის საბჭომ 2007 წლის 25 ოქტომბერს ახალი კონვენცია მიიღო. კერძოდ „ბავშვთა სექსუალური ექსპლუატაციისა და ძალადობისგან დაცვის შესახებ“¹³⁰. კონვენციამ, გარდა ბავშვების სექსუალური ექსპლუატაციისა, აკრძალა პორნოგრაფიული მასალის გაცემა და ბავშვთა სექსუალური მიზნით ცდუნება. ასევე, კონვენციამ დანაშაულს მიაკუთვნა ბავშვთა პორნოგრაფიასთან დაკავშირებული მასალის დამზადება, მოპოვება, მესამე პირისთვის შეთავაზება, გავრცელება, თავისთვის ან სხვისთვის შეძენა, ფლობა. კონვენციამ ბავშვთა პორნოგრაფია განმარტა, როგორც მასალა, რომელიც ეიზუალურად ასახავს ბავშვს, რომელიც მონაწილეობს ნამდვილ ან სიმულირებულ სექსუალურად აღმგზნებ საქციელში; ასევე ბავშვის სექსუალური ორგანოების გამოსახვას სექსუალური მიზნისთვის.

უნდა აღინიშნოს, რომ „კიბერდნაშაულის შესახებ“ კონვენცია აქცენტს აკეთებს ბავშვთა პორნოგრაფიაზე იმდენად, რამდენადაც მის გავრცელებას შესაძლოა, ხელი შეუწყოს გლობალურმა ქსელმა. „ბავშვთა სექსუალური ექსპლუატაციისა და ძალადობისგან დაცვის შესახებ“ კონვენცია კი ამ პრობლემას უფრო ფართო ჭრილში განიხილავს და არ აკონკრეტებს ბავშვთა პორნოგრაფიის გავრცელების გზას. ასევე აღსანიშნავია, რომ ახალი კონვენცია კრძალავს ბავშვთა პორნოგრაფიის მოპოვებას ან/და საინფორმაციო და საკომუნი-

130 იხ. Council of Europe Convention on the Protection of children against Exploitation and Sexual Abuse, CETS No 201 (<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CL=ENG>)

კაციო საშუალებით სექსუალური მიზნისთვის ბავშვის ცდუნებას, განსხვავებით „კიბერდანამაჟულის შესახებ“ კონვენციისგან.¹³¹

მსოფლიოში მიმდინარე ტენდენციებიდან გამომდინარე, როცა ძალიან პოპულარულია სხვადასხვა სოციალური ქსელი, რომლის საშუალებითაც მილიონობით ადამიანი იცნობს და მეგობრობს ერთმანეთთან, საგულისხმო სიახლეა საკომუნიკაციო საშუალების გამოყენებით ბავშვის ცდუნება სექსუალური მიზნისთვის. აღნიშნულთან დაკავშირებული პასუხისმგებლობის დანეხება, ვფიქრობ, ყველა სახელმწიფოსთვის გასათვალისწინებელია.

საქართველოს სისხლის სამართლის კოდექსის 255-ე მუხლის 1-ლი ნაწილით დასჯადია პორნოგრაფიული ნაწარმოების, ნაბეჭდი გამოცემის, გამოსახულების ან პორნოგრაფიული ხასიათის სხვა საგნის უკანონოდ დამზადება, გავრცელება ან რეკლამირება, აგრეთვე ასეთი საგნით ვაჭრობა ან/და მისი შენახვა გაყიდვის ან გავრცელების მიზნით. მე-2 ნაწილით ისჯება წინასწარი შეცნობით არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოების შეძენა, შენახვა, შეთავაზება, გავრცელება, გადაცემა, რეკლამირება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა. მუხლის მე-3 ნაწილი ადგენს სისხლისსამართლებრივ პასუხისმგებლობას წინასწარი შეცნობით არასრულწლოვანის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოების დამზადება და გასაღებისთვის.

მუხლის შენიშვნა განსაზღვრავს რა უნდა ჩაითვალოს არასრულწლოვნის გამოსახულების შემცველ პორნოგრაფიულ ნაწარმოებად და აღნიშნულია, რომ არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოები არის, ნებისმიერი მეთოდით შექმნილი ვიზუალური მასალა ან აუდიომასალა, რომელიც სხვადასხვა საშუალებებით წარმოდგენილია არასრულწლოვანის ან არასრულწლოვნის გამოსახულების მქონე პირის მონაწილეობა ნამდვილ, სიმულირებულ ან კომპიუტერული ტექნოლოგიის მეშვეობით გენერირებულ სექსუალურ სცენებში, მომხმარებლის

131 იხ. ავტორთა კოლექტივი, „მოსამართლეების ტრენინგი კომპიუტერული დანამაჟულის შესახებ: ტრენინგის სახელმძღვანელო“, ევროსაბჭო, სტრასბურგი, 2010წ. გვ. 68

სექსუალური მოთხოვნილებების დაკმაყოფილების მიზნით ნაჩვენებია არასრულწლოვნის გენიტალური ორგანოები. პორნოგრაფიულად არ ჩაითვლება ნაწარმოები, რომელიც შექმნილია სამედიცინო, სამეცნიერო, კულტურული და სხვა კანონიერი მიზნისთვის.

255-ე მუხლით, დადგენილია იურიდიული პირის პასუხისმგებლობაც.

უნდა აღინიშნოს, რომ ეს დანაშაული არ შეიძლება განიხილებოდეს როგორც კომპიუტერული დანაშაული, რადგან პორნოგრაფიის გადაღება, დამზადება, და ყველა სხვა ქმედება რაც მის შექმნას სჭირდება, უკავშირდება სხვადასხვა ვიდეო-აპარატურას, ხოლო კომპიუტერი შემდგომში შეიძლება გამოყენებულ იქნეს პორნოგრაფიული მასალის გადასამუშავებლად, ინტერნეტი კი მის გასავრცელებლად გამოიყენება. „კიბერდანაშაულის შესახებ“ კონვენციის შემქმნელები ბავშვთა პორნოგრაფიის გავრცელების ერთ-ერთ მთავარ ხელშემწყობ საშუალებად განიხილავენ პორნო-საიტებს, რომლებზეც ხდება მსგავსი შინაარსის შემცველი ფაილების განთავსება. ამდენად, მათი ჩიზანი იყო, სწორედ ასეთი სახის სისტემის წინააღმდეგ ბრძოლა და, ბუნებრივია, აღნიშნული არ გულისხმობს, რომ ბავშვთა პორნოგრაფია განხილული უნდა იქნეს როგორც კომპიუტერული დანაშაული.

მოკლედ შევხები 255-ე მუხლის დახასიათებას. მოცემული დანაშაულის ხელყოფის ობიექტი საზოგადოებრივი ზნეობა და პიროვნების ნორმალური ზნეობრივი და სექსუალური განვითარებაა. ამგვარად, სისხლის სამართლის კოდექსის დაცვის ობიექტი საზოგადოების ზნეობაა. დანაშაულის საგანია პორნოგრაფიული ნაწარმოები, ნაბეჭდი, გამოცემა, ფოტო, კინო და ა.შ.

დანაშაულის ობიექტური მხარე გამოიხატება ისეთ მოქმედებებში როგორიცაა პორნოგრაფიული ნაწარმოების დამზადება, შენახვა, გავრცელება და ა.შ. მოცემული დანაშაული ფორმალური შემადგენლობისაა და ის დამთავრებულად ჩაითვლება კანონში მითითებული ერთ-ერთი მოქმედების ჩადენის მომენტიდან.

დანაშაულის სუბიექტური მხარე გულისხმობს პირდაპირ განზრახვას. კერძოდ, დამნაშავეს გაცნობიერებული აქვს, რომ მის მიერ დამზადებული, რეკლამირებული და ა.შ. ნივთი პორნო-

გრაფიული შინაარსისაა.¹³² განსხვავებით 255-ე მუხლის მე-2 ნაწილისგან, პორნოგრაფიის საგნის შენახვისთვის აუცილებელია მისი გაყიდვის ან გავრცელების მიზანი.

უნდა აღინიშნოს, რომ 255-ე მუხლის მე-2 ნაწილი ბევრად ფართო შინაარსს მოიცავს. კონვენციის შესაბამისად, აკრძალულია პორნოგრაფიული მასალის შენახვაც კი. მუხლის მე-3 ნაწილი კი დამამძიმებელ გარემოებად ითვალისწინებს დანაშაულის ჩადენას ნინასწარი შეცნობით არასრულწლოვნის მიმართ.

დანაშაულის მოტივი შესაძლოა იყოს ანგარება, შურისძიება და ა.შ.

კომპიუტერის და ინტერნეტის გამოყენება უნდა მივიჩნიოთ არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოების დამზადების, გაყიდვის, შენახვის და გავრცელების ხერხად.

ჩემი აზრით, 255-ე მუხლის ახალი რედაქცია წინგადადგმულ ნაბიჯად უნდა ჩაითვალოს, მაგრამ თუ რეალობას თვალს გაეუხსნორებთ, აღმოვაჩენთ, რომ ისეთი ქართული ვიდეო-პორტალებიც კი, რომლებიც ძალიან პოპულარულია საქართველოში, ხშირად ვერ უზრუნველყოფენ პორნოგრაფიული ფაილების კონტროლს და მათი საშუალებით, ნებით თუ უნებლიედ, ნებისმიერი ასაკის ადამიანისთვის უზრუნველყოფილია პორნოგრაფიის და ბავშვთა პორნოგრაფიის ხელმისაწვდომობა სრულიად უფასოდ, რაც ჩემი აზრით, საჭიროებს კონტროლს და დამნაშავეების მიმართ სისხლის სამართლის კოდექსით გათვალისწინებული სანქციების გატარებას.

132 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი I, გამოქვეყნებულია „მერიდიანი“, თბილისი, 2011წ. გვ. 657-658

3. საავტორო, მომიჯნავე უფლების მფლობელის და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა

მსგავსად ბავშვთა პორნოგრაფიისა, ევროპის საბჭოს კონვენციამ დაადგინა პასუხისმგებლობა კომპიუტერული სისტემის გამოყენებით საავტორო და მომიჯნავე უფლებების დარღვევისთვის. კონვენციის მე-10 მუხლის შესაბამისად: „ყველა მონაწილე სახელმწიფო ვალდებულია მიიღოს ისეთი საჭირო საკანონმდებლო და სხვა ზომა, რომელიც ეროვნული კანონმდებლობით მოახდენს კომპიუტერული სისტემის საშუალებით, სარგებლის მიღების მიზნით, განზრახი ქმედებით ჩადენილ საავტორო უფლებათა დარღვევის კრიმინალიზაციას, როგორც ეს განსაზღვრულია ამ სახელმწიფოს კანონმდებლობით და რისი ვალდებულებაც ამ სახელმწიფომ იკისრა ლიტერატურულ და მხატვრულ ნაშრომთა დაცვის ბერნის კონვენციის, ინტელექტუალური საკუთრების უფლებათა ვაჭრობასთან დაკავშირებულ ასპექტებზე ხელშეკრულებისა და ინტელექტუალური საკუთრების მსოფლიო ორგანიზაციის ხელშეკრულებაზე დაყრდნობით მიღებული 1971 წლის 24 ივლისის პარიზის აქტით.“

კონვენციის მე-10 მუხლის მე-2 ნაწილის მიხედვით კი: „ყველა მონაწილე სახელმწიფო ვალდებულია მიიღოს ისეთი საჭირო საკანონმდებლო და სხვა ზომა, რომელიც ეროვნული კანონმდებლობით მოახდენს კომპიუტერული სისტემის საშუალებით, სარგებლის მიღების მიზნით, განზრახი ქმედებით ჩადენილ მომიჯნავე უფლებათა დარღვევის კრიმინალიზაციას.“

მუსიკისა და ვიდეო-ფაილების ტრადიციულიდან ინტერნეტ დისტრიბუციაზე გადასვლამ საავტორო უფლების დარღვევის ახალი ფორმა წარმოშვა. საინტერესოა, რომ ზოგიერთი გახმაურებული კინოფილმი ინტერნეტის საშუალებით მსოფლიო პრემიერამდე გავრცელდა. აღნიშნული არგუმენტი გახდა ერთ-ერთი მთავარი საფუძველი ევროპის საბჭოს კონვენციაში მე-10 მუხლის დამატებისთვის.

გარდა ამისა, უნდა აღინიშნოს კომპიუტერული პროგრამების სამართლებრივი დაცვის საკითხი, რადგან „კიბერდანაშაულის შესახებ“ კონვენცია მათზე საავტორო უფლების დაცვასაც გულისხმობს.

სავსებით სამართლიანია მ. ივანოვიჩის პოზიცია, რომელიც წერს, რომ „კომპიუტერული პროგრამების (და თავად კომპიუტერული ტექნოლოგიების დარგის) ტექნოლოგიური და კომერციული ბუნება მკვეთრად განასხვავებს მას ინტელექტუალური საკუთრების სხვა ნაწარმოებებისგან, რაც განაპირობებს, აგრეთვე, კომპიუტერული პროგრამის შემქმნელისათვის დადგენილი ინტელექტუალური საკუთრების უფლების გამიჯვნას.“¹³³

ცხადია, რომ კომპიუტერი არის არა მხოლოდ კომპიუტერული დანამაჟლის ჩადენის საშუალება, არამედ, იგი შეეხო სხვა სფეროებსაც. როდესაც პირი ქმნის კომპიუტერულ პროგრამას, გარდა ტრადიციული ხერხებისა, მისი საავტორო უფლების ხელყოფა შესაძლოა განხორციელდეს კომპიუტერული სისტემის საშუალებით. მაგალითად, საავტორო კომპიუტერული პროგრამის უნებართვო გავრცელება სოციალური ქსელით სწორედ კონვენციის მე-10 მუხლით გათვალისწინებული დანამაჟლია.

საქართველოს სისხლის სამართლის კოდექსის 189-ე მუხლი ეხება საავტორო, მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფას. 2010 წლის 24 სექტემბრის ცვლილება აღნიშნულ მუხლსაც შეეხო. მუხლის პირველი ნაწილი დარჩა უცვლელი, რომლის მიხედვითაც დასჯადია საავტორო უფლების ობიექტზე ავტორობის მითვისება ან თანაავტორობის იძულება. მე-2 ნაწილით დადგენილია პასუხისმგებლობა 1-ლი ნაწილით გათვალისწინებული ქმედების არაერთგზის ჩადენისთვის.

შეიცვალა მე-3 ნაწილი და ჩამოყალიბდა შემდეგნაირად: „საავტორო და მომიჯნავე უფლებების შესახებ“ კანონის დარღვევით ნაწარმოების, ფონოგრამის, ვიდეოგრამის ან მონაცემთა ბაზის რეპორდუცირება ან მათი ასლების უნებართვო შეძენა, იმპორტი, შენახვა, გაყიდვა, გაქირავება, გადაცემა, ან/და საავტორო, მომიჯნავე უფლების მფლობელის და მონაცემთა ბაზის დამამზადებლის უფლების სხვა ხელყოფა, ჩადენილი დიდი ოდენობის შემოსავლის მიღების მიზნით“. განსხვავებულად ჩამოყალიბდა მუხლის მენიშვნაც: „ამ მუხლით გათვალისწინებული ქმედება დიდი ოდენო-

133 მ. ივანოვიჩი, „კომპიუტერული პროგრამების სამართლებრივი დაცვის უზრუნველყოფის საკითხები, ჟურნ. „მართლმსაჯულება“ 2008წ. №3, გვ. 67.

ბით შემოსავლის მიღების მიზნით ჩადენილად ითვლება, თუ ნაწარმოების, ფონოგრამის, ვიდეოგრამის ან მონაცემთა ბაზის ასლების ღირებულება ან სააქტორო, მომიჯნავე უფლების მფლობელის და მონაცემთა ბაზის დამამზადებლის უფლების კანონიერი გამოყენების შემთხვევაში სააქტორო, მომიჯნავე უფლების მფლობელის ან მოცანემთა ბაზის დამამზადებლის მიერ მისაღები შემოსავალი ალემატება ხუთი ათას ლარს, ხოლო განსაკუთრებით დიდი ოდენობით – თუ ზემოაღნიშნული ღირებულება ან შემოსავალი ალემატება ათი ათას ლარს."

მე-4 ნაწილით გათვალისწინებული ქმედების დამამძიმებელ გარემოებად დადგენილია, მისი ჩადენა დიდი ოდენობით შემოსავლის მიღების მიზნით და წინასწარი შეთანხმებით ჯგუფის მიერ.

ამავე მუხლით დადგენილია პასუხისმგებლობა იურიდიული პირებისთვისაც.

აღნიშნული შემადგენლობა, ისევე როგორც 255-ე მუხლით აღწერილი ქმედება არაა კიბერდანაშაული და 189-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის შემთხვევაშიც კომპიუტერი უნდა განვიხილოთ დანაშაულის ჩადენის ხერხად.

კიბერტერორიზმი

ტერორიზმი მსოფლიოს პრობლემად იქცა. 2001 წლის 11 სექტემბრის ტერაქტის შემდეგ შეიცვალა ადამიანების წარმოდგენა ამ დანაშაულის მასშტაბზე და საფრთხეზე. ტერორიზმის შესახებ ყოველდღიურად საუბრობენ ექსპერტები, საინფორმაციო გამოშვებები. ტერორიზმის შესახებ ცნობის მიღება ჩვენი ყოველდღიური ცხოვრების ნაწილი გახდა. საქართველოს სისხლის სამართლის კოდექსის 323-ე მუხლი ითვალისწინებს პასუხისმგებლობას ტერორისტული აქტისთვის. თუმცა, კანონმდებელმა საჭიროდ ჩათვალა კოდექსისთვის დამატებინა 324¹-ე მუხლი, რომელიც ადგენს პასუხისმგებლობას კიბერტერორიზმისთვის. კოდექსის ძველი რედაქციით კიბერტერორიზმი შემდეგნაირად იყო განმარტებული: „კიბერტერორიზმი, ესე იგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას და ხელყოფს საზოგადოებრივ უსაფრთხოებას, სახელმწიფოს სტრატეგიულ, პოლიტიკურ ან ეკონომიკურ ინტერესს, ჩადენილი მოსახლეობის დაშინების ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით.“ 2012 წლის 2 მარტის ცვლილების შემდეგ კი მუხლი ჩამოყალიბდა შემდეგნაირად: „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.“

ლ. ბოძაშვილის და ნ. კოხრეიძის აზრით: „კიბერტერორიზმი წარმოადგენს კიბერშეტევის ერთ-ერთ სახეს. საკმაოდ ხშირად ტერმინს კიბერტერორიზმსა და კიბერშეტევას ურთიერთ ჩანაცვლებით ხმარობენ, რაც იწვევს ზოგადად კიბერსაფრთხისა და თვითონ კიბერტერორიზმის არასწორად გაგებას. კიბერტერორიზმის მაგალითი იქნება პოლიტიკური მოტივაციის მქონე კიბერშეტევა, რომე-

ლიც ინვევს სიკვდილიანობას, სხეულის დაზიანებას, აფეთქებას ან მნიშვნელოვან ეკონომიკურ დანაკლისს".¹³⁴

მოცემული მსჯელობას ვეთანხმები და მიმაჩნია, რომ იგი შეესაბამება კოდექსის 324¹-ე მუხლში აღწერილ დანაშაულს.

კოდექსის ძველი რედაქციის შესაბამისად კიბერტერორიზმის დაცვის უშუალო ობიექტი იყო სახელმწიფოს ინტერესი (სტრატეგიული, პოლიტიკური, ან ეკონომიკური), დამატებითი ობიექტი კი შეიძლება ყოფილიყო ადამიანის სიცოცხლე, ჯანმრთელობა, ქონება. მიუხედავად იმისა, რომ 324¹ მუხლის ახალი რედაქციაში სახელმწიფოს სტრატეგიულ და სხვა ინტერესზე მითითებას აღარ ვხვდებით, დანაშაულის უშუალო ობიექტი იგივე დარჩება, რადგან ხელისუფლების ორგანოზე ზემოქმედება მიმართულია სწორედ სახელმწიფო სტრატეგიულ და სხვა ინტერესების წინააღმდეგ. დამატებით ობიექტთან დაკავშირებითაც შეიძლება იგივე ითქვას.

კიბერტერორიზმი, კერძოდ კი 324¹ მუხლის 1-ლი ნაწილით გთვალისწინებული დანაშაული ობიექტური ნიშნებით კონკრეტული საფრთხის შემქმნელი დელიქტია. მისი ობიექტური მხარე გამოიხატება კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლებაში, მის გამოყენებაში ან გამოყენების მუქარაში, რაც ქმნის მძიმე შედეგის განხორციელების საშიშროებას. მძიმე შედეგის განხორციელების შესაძლებლობა შეიძლება შეიქმნას მაგალითად, ტრანსპორტის მუშაობის ბლოკირებით, მასობრივი განადგურების იარაღის შექმნის ტექნოლოგიის ხელში ჩაგდებათ, ენერგომომხმარებლის შეფერხებით და ა.შ.¹³⁵

კიბერტერორიზმი დანაშაულია, რომლის მოტივიც შეიძლება იყოს ანგარება, შურისძიება, პოლიტიკური და ა.შ.

აღსანიშნავია, რომ ამ დანაშაულთან მიმართებაში მიზანს განსაკუთრებული მნიშვნელობა აქვს.

ლ. ბოძაშვილი და ს. კოხრეიძე აღნიშნავენ, რომ „კიბერსივრცეში ტერორიზმი გაგებულია, როგორც კომპიუტერის, ქსელისა და

134 იხ. ლ. ბოძაშვილი, ს. კოხრეიძე, „კიბერსივრცის სამართალი“, 20126. (ნაშრომში გამოყენებულია ნიგნის ოფიციალური ელ-ვერსია გამოქვეყნებული საიტზე www.lit.ge, რომელშიც გვერდები მითითებული არაა).

135 იხ. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, ნიგნი I, გამომცემლობა „მერიდიანი“, თბილისი, 20116. გვ. 159-160

მათში შენახული ინფორმაციის წინააღმდეგ მიმართული უკანონო შეტევა და შეტევით დაშინება, რომლის მიზანიცაა მთავრობის ან ხალხის პოლიტიკური ან სოციალური დაშინება“¹³⁶. თუმცა, როგორც ჩანს ავტორები არ ეთანხმებიან ამ შეხედულებას, რადგან ამის შემდეგ ისინი ცდილობენ ერთმანეთისგან გამიჯნონ კიბერდანაშაული და კიბერტერორიზმი და განმასხვავებელ ნიშნად გამოყოფენ დანაშაულის მიზანს: „კიბერტერორიზმის მიზანია კიბერსივრცისთვის ზიანის მიყენება და განადგურება, რაც შემტევებს სამიზნიდან მოპოვებით ყოფნის საშუალებას აძლევთ. ამის საპირისპიროდ კი, კიბერკრიმინალების მიზანია გარკვეული მოგების ნახვა და ეს შეიძლება გამოიხატოს სახსრების უკანონო გადარიცხვებში, ფულის გათეთრებაში...“¹³⁷

აღნიშნულ მოსაზრებას ვერ დავეთანხმები, რადგან კიბერსივრცე, როგორც დანაშაულის კონკრეტული ხელყოფის ობიექტი არ არსებობს, რადგან იგი ძალიან ზოგადი ცნებაა. შესაბამისად, მისი ხელყოფა არ შეიძლება დანაშაულის მიზანი იყოს. კოდექსის 324¹-ე მუხლის შესაბამისად, კიბერტერორიზმის ხელყოფის მიზანი კიბერსივრცისთვის ზიანის მიყენება კი არა, მოსახლეობის დაშინება და ხელისუფლების ორგანოზე ზემოქმედებაა. ამ შემთხვევაში კანონმდებლის პოზიციას სრულად ვიზიარებ.

დანაშაულის მიზანთან დაკავშირებით საინტერესოა კიბერტერორიზმის ტერორისტულ აქტთან შედარება.

კოდექსის 323-ე მუხლისმიხედვით ტერორისტული აქტის დეფინიცია შემდეგნაირადაა ჩამოყალიბებული: „ტერორისტული აქტი, ესე იგი აფეთქება, ცეცხლის ნაქიდება, იარაღის გამოყენება ან სხვა ქმედება, რაც ქმნის ადამიანის სიცოცხლის მოსპობის, მნიშვნელოვანი ქონებრივი ზიანის ან სხვა მძიმე შედეგის განხორციელების საშიშროებას, ჩადენილი მოსახლეობის დაშინების ან ხელისუფლების ორგანოზე, უცხო ქვეყნის ხელისუფლების ორგანოზე ან საერთაშორისო ორგანიზაციაზე ზემოქმედების მიზნით.“

136 იხ. ლ. ბოძაშვილი, ნ. კოხრიძე, „კიბერსივრცის სამართალი“, 2012წ. (ნაშრომში გამოყენებულია ნიგნის ოფიციალური ელ-კერსია გამოქვეყნებული საიტზე www.lit.ge, რომელშიც გვერდები მითითებული არაა).

137 იხ. იქვე.

კანონმდებელმა უცნაური გადაწყვეტილება მიიღო, როცა კიბერტერორიზმი და ტერორისტული აქტი ერთმანეთისგან განასხვავა დანაშაულის მიზნით. კერძოდ, ტერორისტული აქტი შეიძლება უცხო ქვეყნის ხელისუფლების ორგანოზე ან საერთაშორისო ორგანიზაციაზე ზემოქმედების მიზნით განხორციელდეს, კიბერტერორიზმი კი მხოლოდ მოსახლეობის და ხელისუფლების ორგანოზე ზემოქმედების მიზნით, რთულია ამ მოსაზრებას მოუძებნო ლოგიკა. მით უფრო მაშინ, რომ კომპიუტერული დანაშაულის ერთ-ერთი მთავარი სირთულე სწორედ ისაა, რომ არაა შეზღუდული სახელმწიფო საზღვრებით და მარტივია მისი ჩადენა მაგალითად, საქართველოში შინიდას გაუსვლელად, სხვა სახელმწიფოს წინააღმდეგ. განვიხილოთ კაზუსი: ბ. კრასოვსკიმ, რომელიც იყო საქართველოს მოქალაქე და ცხოვრობდა ქ. თბილისში შეაღწია აეროპორტის კომპიუტერულ სისტემაში და მონაცემთა გადაცემის პროცესზე გავლენით შეძლო, თბილისის მიმართულებით მფრინავ შვედეთის მთავრობის საკუთრებაში არსებულ ავია-ეკიპაჟისთვის არასწორი კოორდინატების მიწოდება, რამაც ამ თვითმფრინავის ავია-კატასტროფა გამოიწვია. მოგვიანებით, ინტერნეტში გავრცელდა ბ. კრასოვსკის მიმართვა, სადაც იგი იმუქრებოდა, რომ თუ შვედეთის ხელისუფლება არ გაათავისუფლებდა მის მოკავშირე პატიმრებს, მომავალში შვედეთის საკუთრებაში არსებული სხვა თვითმფრინავებსაც ჩამოაგდება.

ზემოაღნიშნული დანაშაულის შინაარსი შეესაბამება 324¹-ე მუხლის მე-2 ნაწილით აღწერილ ქმედებას. სახეზე გვაქვს კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება და მისი გამოყენება. კერძოდ, ბ. კრასოვსკიმ კომპიუტერულ სისტემაში უნებართვო შეღწევის გზით მოიპოვა ისეთი კომპიუტერული მონაცემი, რომლის გამოყენებითაც შეძლო მონაცემთა გადაცემის პროცესზე გავლენის მოხდენა და შვედეთის მთავრობის საკუთრებაში არსებულ თვითმფრინავის ეკიპაჟს მიაწოდა არასწორი კოორდინატები, რამაც არათუ შექმნა მძიმე შედეგის დადგომის საფრთხე, არამედ ეს შედეგი დადგა კიდევ, რადგან თვითმფრინავმა განიცადა ავია-კატასტროფა და დაიღუპნენ ადამიანები. მიუხედავად ამისა, სახეზე კიბერტერორიზმი მაინც არ გვაქვს, რადგან დამნაშავის მიზანი არ იყო არც მოსახლეობის დაშინება და არც

საქართველოს ხელისუფლებაზე ზემოქმედების მოხდენა. ბ. კრასოვსკის მიზნად ჰქონდა დასახული შვედეთის მთავრობაზე ზეგავლენის მოხდენა.

შედეგად ვიღებთ უცნაურ ვითარებას: გამოდის, რომ ბ. კრასოვ-კიმ ჩაიდინა 324¹ მუხლში აღწერილი ქმედება, რომლის მიზანი იყო კოდექსის 323-ე მუხლით გათვალისწინებული უცხო ქვეყნის ხელისუფლების ორგანოზე ზემოქმედების მოხდენა.

გაუგებარია, კანონმდებელმა კიბერტერორიზმი რატომ ჩაკე-ტა ერთი ქვეყნის საზღვრებში და დაანამაულის მიზნად მხოლოდ მოსახლეობის დაშინება და ხელისუფლების ორგანოზე ზემოქმედებ-ის მოხდენა დაანესა, მაშინ, როცა ტერორისტული აქტი, პირიქით სრულყოფილად გამოხატავს ამ დაანამაულის ბუნებას და არ კმაყო-ფილდება მხოლოდ ქვეყნის შიდა ინტერესებით და დაანამაულის მიზნად მიუთითებს, როგორც უცხო ქვეყნის ხელისუფლების ორგა-ნოსა, ასევე საერთაშორისო ორგანიზაციაზე ზემოქმედებას.

აქედან გამომდინარე, კომპიუტერული მონაცემის გამოყენებით ჩადენილი ნებისმიერი დაანამაულის მხოლოდ ერთ სახელმწიფოს ფარგლებში განხილვა გაუმართლებელია.

მოცემული მსჯელობის საფუძველზე შეიძლება დავასკვნათ, რომ კიბერტერორიზმის მუხლი შეიცავს ხარვეზებს და პრაქტიკაში რთული იქნება მისი გამოყენება.

„იურიდიული დეფინიციის არარსებობის პირობებში, როგორც დოქტრინაში, აგრეთვე, ოფიციალურ ნორმატიულ აქტებში, ხშირია ტერორიზმის აღრევა სხვა სოციალურ-სამართლებრივ მოვლენ-ებთან. განსაკუთრებით ხშირია ომის, პარტიზანული ბრძოლის, ეროვნულ-გამათავისუფლებელი მოძრაობის, დეკოლონიზაციის პროცესების ტერორიზმთან გაიგივება¹³⁸ – აღსიშნავს გ. გორაშვი-ლი. დავამატებ, რომ გარდა ჩამოთვლილისა, ტერორიზმის კომპი-უტერულ დაანამაულში აღრევაც არასწორია: კიბერტერორიზმი, არის ტერორისტული აქტი, ჩადენილი კომპიუტერულ სისტემაში შეღწევის და კომპიუტერული მონაცემების უნებართვო გამოყენების

138 იხ. გ. გორაშვილი, „ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები“ გამომც. „უნივერსა-ლი“, თბ. 2010წ. გვ. 59

გზით. ამდენად, ჩემი აზრით, კომპიუტერული მონაცემის დაუფლება შეგვიძლია განვიხილოთ ტერორიზმის ჩადენის ხერხად და არა დამოუკიდებელ დანაშაულად, რადგან კოდექსის 323-ე მუხლის მიხედვით ტერორისტული აქტია აფეთქება, ცეცხლის წაქიფება, იარაღის გამოყენება ან სხვა ქმედება, რომელიც ქმნის ადამიანის სიცოცხლის მოსპობის, მნიშვნელოვანი ქონებრივი ზიანის ან სხვა მძიმე შედეგის განხორციელების საშიშროებას ჩადენილი მოსახლეობის დამინების ან ხელისუფლების ორგანოზე ზემოქმედების მიზნით და არა აქვს მნიშვნელობა, როგორ იქნება ეს ქმედება ჩადენილი, რა გზით, რა ხერხით: დამნაშავე კომპიუტერს გამოიყენებს, ავტომატს თუ ასაფეთქებელ ნივთიერებას, ამით დანაშაულის არსი არ შეიცვლება.

კანონმდებელმა კომპიუტერული მონაცემების საშუალებით ჩადენილი ტერორისტული აქტი კიბერტერორიზმად ჩათვალა. ამ ლოგიკით გამოდის, რომ დანაშაულის ჩადენის ხერხის მიხედვით უნდა დავეყნოთ ტერორისტული აქტის სახეობები და გარდა, კიბერტერორიზმისა, მივიღებთ: ტერორისტულ აქტს აფეთქებით, ტერორისტულ აქტს ავტომატის სასხლეტზე ხელის გამოკვრით ან ტერორისტულ აქტს „მოლოტოვის“ კოქტილის გამოყენებით. შესაძლებელია კიდევ ეფრო გავაფართოვოთ ფანტაზია და ვისაუბროთ ტერორისტულ აქტზე სხვა სახელმწიფოს ტერიტორიაზე შეღწევით. ეს მიდგომა არ უნდა იყოს სწორი და დასაბუთებული. ჩემი აზრით, 324'-ე მუხლში ხაზგასმულია მხოლოდ კანონით დაცული კომპიუტერული ინფორმაციის დაუფლების, მისი გამოყენების ან გამოყენების მუქარის გზით ჩადენილი ტერორისტულ აქტი. ვფიქრობ, ამ უკანასკნელს გულისხმობს 323-ე მუხლში მითითებული „სხვა ქმედება“. თუმცა, ეს მსჯელობა არ გამორიცხავს იმ გარემოებას, რომ კიბერტერორიზმისთვის სისხლისსამართლებრივ პასუხისმგებლობას ცალკე მუხლი ადგენდეს. ამ შემთხვევაში არსებული რედაქცია სერიოზულ დახვეწას საჭრიობს.

გარდა ზემოაღნიშნულისა, კიბერტერორიზმის მუხლი სხვა კითხვებსაც ბადებს. მაგალითად, განვიხილოთ დამამძიმებელი გარემოებები. 324'-ე მუხლის მე-2 ნაწილი ითვალისწინებს ადამიანის სიკვდილს, ან სხვა მძიმე შედეგს. მძიმე შედეგი შესაძლოა გამოიხატოს სტრატეგიული ობიექტის ფუნქციონირების შეფერხებაში, დაზიანებაში, ქონებრივ ზიანში და ა.შ. აქედან გამომდინარე იბადება

კითხვა: თუ ტერორისტული აქტისთვის დამამძიმებელი გარემოებაა მისი ჩადენა ჯგუფურად და არაერთგზის, რატომ არ უნდა იყოს იგივე დამამძიმებელი გარემოება კიბერტერორიზმისთვის?

ყოველივე ზემოაღნიშნულის გათვალისწინებით მიმაჩნია, რომ „კოდექსში 324¹-ე მუხლის მოცემული სახით არსებობა არის კანონმდებლობის ხარვეზი და იგი საჭიროებს მთელ რიგ ცვლილებას. კერძოდ, როგორც მინიმუმ, აუცილებლად მიმაჩნია ტერმინი „კანონით დაცული ინფორმაციის“ საერთოდ ამოღება, რადგან მისი შინაარსის ბუნდოვანებასთან დაკავშირებით უკვე ვისაუბრეთ ნაშრომის შესაბამის თავში. რაც შეეხება იმ უზუსტობებს, რომელიც ჩემს მიერ აღინიშნა საჭიროებს დამატებით განხილვას და მსჯელობას.

კიბერდანაშაულის სამართლებრივი რეგულირება მსოფლიოს ზოგიერთ ქვეყანაში

ამერიკაში კომპიუტერულ დანაშაულთან დაკავშირებით საკანონმდებლო ცვლილებები მუდმივად მიმდინარეობდა. მისი ახალი ტალღა კი XXI საუკუნის დასაწყისიდანვე აგორდა. 2001 წლის ოქტომბერში მიღებული იქნა ფედერალური კანონი, ე.წ. „პატრიოტთა აქტი“. მისი შემუშავება 2001 წლის 11 სექტემბრის ტერაქტმა განაპირობა. აღნიშნულმა აქტმა გააფართოვა ფედერალური გამოძიების ბიუროს უფლებამოსილება ელექტრონული თვალთვალის და მოსმენის სფეროში.

ამავე აქტის 814-ე მუხლით ცვლილება შევიდა კანონთა კრების მე-18 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 დაქანაშავის მიზნის დადგენა.¹³⁹

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 გაისაზღვრა 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.

139 იხ. Field Guidance New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot act of 2001, Computer Crime and Intellectual Property Section(CCIPS), Перевод М. Буряк (<http://kiev-security.org.ua/box/4/94.shtml>)

კარგი იქნება ეს მუხლი იყოს ნებისმიერი ქვეყნის სისხლის სამართლის კოდექსში, რადგან ხაზს უსვამს სახელმწიფოს ნაციონალური უსაფრთხოების დაცვის უდიდეს მნიშვნელობას. მსოფლიოში შექმნილი რეალობიდან გამომდინარე კი კომპიუტერული სისტემის უსაფრთხოების დაცვა შეიძლება ქვეყნის უსაფრთხოების დაცვას გაუუთხოლოთ. ზემოთაც აღინიშნა და კიდევ გავიმეორებ, რომ ქართველი კანონმდებლის მიერ სახელმწიფოს, როგორც გასსაკუთრებული დაცვის ობიექტის შესახებ ხაზგასმა კიბერდანაშაულის თავში არ გვხვდება.

გარდა ზემოაღნიშნულისა, დასჯადია კომპიუტერული თაღლითობა, ესე იგი თაღლითური განზრახვით და უკანონო სარგებლის მიღების მიზნით კომპიუტერულ სისტემაში შეღწევა.

ჩემი აზრით, მნიშვნელობა არ უნდა ჰქონდეს პირი თაღლითობას რა ხერხით ჩაიდენს: კომპიუტერულ სისტემაში შეღწევით, ყალბი საკრედიტო ბარათის დამზადებით თუ ყალბი პირადობის მოწმობის დამზადებით, მისი ქმედება უნდა შეფასდეს როგორც თაღლითობა და მისი ცალკე დანაშაულად გამოყოფა არ მიმაჩნია მიზანშეწონილად.

აღსანიშნავია, რომ აშშ-ს ყველა შტატს გააჩნია საკუთარი ნორმატიული აქტი კომპიუტერული დანაშაულის რეგულირებასთან დაკავშირებით და ხშირად მათი შინაარსი განსხვავდება ფედერალური კანონმდებლობით დადგენილი დანაშაულებრივი შემადგენლობებიდან. 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 სისტემაში¹⁴⁰.

140 იხ. Интернет-Университет Информационных Технологий, Лекция №5: Юридические вопросы информационной безопасности, автор Ерик Мэйволд (<http://www.intuit.ru/departments/security/netsec/5/>)

ეს უკანასკნელი თეზისი მით უფრო აქტუალური ხდება მას შემდეგ, რაც ქართულ რეალობაში სულ უფრო ხშირად გვხვდება, ე.წ. „დოს“ შეტევები. იმ ფონზე, როცა სხვადასხვა საინფორმაციო სააგენტო ან სახელმწიფო დაწესებულება კიბერშეტვის მსხვერპლია, გარდა ტექნიკური ცოდნის მქონე ექსპერტების მხრიდან განუღივლი თავდაცვითი ზომებისა, ხშირად აუცილებელია თავდასხმის წყაროს განეიტრალება, რაც ოაგის მხრივ, გულისხმობს იგივე ე.წ. „დოს“ შეტევას, როსიელიც მოსართულია თავდამსხმელის მისამართით. ამდენად, აშშ-ში იუტას მტატის მხიდგომა ამ კუთხით ემყარება მრავალწლიან გამოცდილებას და კარგია, რომ მსგავს შემთხვევაში ქართული კანონმდებლობაც იძლევა მსგავს შესაძლებლობას. კერძოდ, საუბარია სისხლის სამართლის კოდექსის 28-ე მუხლზე, რომელიც ითვალისწინებს აუცილებელ მოგერიებას, როგორც მართლწინააღმდეგობის გამომრიცხველ გარემოებას. გამოდის, რომ თუ საქართველოში, რომელიმე ორგანიზაციაზე ე.წ. „დოს“ შეტევა განხორციელდება და ეს ორგანიზაცია აუცილებელი მოგერიების ფარგლებში ანალოგიური იერიშით უპასუხებს ხელმყოფს, სახეზე არ გვექნება სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაული.

გერმანიაში 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 გერმანიის 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 აზრით, უნდა მომხდარიყო „კიბერდანაშაულის შესახებ“ კონვენციის მე-6 მუხლით გათვალისწინებული ქმედების კრიმინალიზაცია. მისი შეხედულებით, ცვლილება უნდა შეხებოდა გერმანიის სისხლის სამართლის 303-ბ მუხლსაც, რომლის ძველი

რედაქციით დასჯადი იყო იმ ინფორმაციის დაშუშავების 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 დაშუშავების პროცესის ხელყოფა, რომელიც ისახებოდა კერძო პირის კომპიუტერში.¹⁴¹

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, როგორც მ. გერკეს პოზიცია, ასევე მასში ასახულია კონვენციით გათვალისწინებული ყველა ის დანაშაულებრივი ქმედება, რომელზეც ნაშრომში უკვე ვისაუბრეთ.

გაერთიანებული სამეფო (ინგლისი, უელსი) ხანგრძლივი დროის განმავლობაში არ ახდენდა „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირებას, რის გამოც ხდებოდა კრიტიკის ობიექტი. „კასპერსკის ლაბორატორიის“ ექსპერტი დევიდ ემი ჯერ კიდევ 2009 წლის ივნისში წერდა, რომ გაერთიანებულ სამეფოში კონვენციის ხელმოწერის და შემდგომი რატიფიცირების პროცესი 2009 წელსვე დასრულდებოდა.¹⁴² თუმცა, ეს პროგნოზი არ გაძარტლდა. საბოლოოდ, გაერთიანებულ სამეფოში კონვენციის რატიფიცირება 2011 წლის 25 მაისს განხორციელდა.

პროფესორი პიტერ სომერი „კიბერდანაშაულის შესახებ“ კონვენციას დადებითად აფასებს, მაგრამ სკეპტიკურად უდგება სხვადასხვა საერთაშორისო ორგანიზაციის ძალისხმევას მოაგვაროს კომპიუტერული დანაშაულის პრობლემა მხოლოდ ცოდნის გაზიარების გზით და რეკომენდაციების გაცემით. გარდა ზემოაღნიშნულისა, პ. სომერი მიუთითებს, რომ ევროპული ქვეყნების სამართალი დაფუძნებულია კოდექსებზე, ინგლისში კი „საერთო სამართალი“,

141 იხ. <http://www.crime-research.org/interviews/Interview-Germany-and-new-cybercrime-law/>

142 იხ. http://www.securelist.com/ru/analysis/208050513/Kiberprestupnost_i_zakon_obzor_polozheniy_zakonodatelstva_Velikobritanii

რომლის მიხედვითაც სამართლის უფრო მნიშვნელოვანი ნაწილი თავმოყრილია სასამართლო პრეცედენტებში. მისი აზრით, სწორედ ეს გარემოება აბრკოლებდა დიდ ბრიტანეთში კონვენციის რატიფიცირებას.¹⁴³

პ. სომერის შეფასებით, კონვენციაში დადებითია ის, რომ ევროპის ქვეყნები გადადიან საერთო სახელმძღვანელო სტანდარტებზე და პრინციპებზე. ამის კარგი მაგალითია, რეკომენდაცია მონაცემთა დაცვის, ელექტრონული შეტყობინების და პირადი ცხოვრების ხელშეუხებლობის ან თუნდაც მონაცემთა შენახვის შესახებ. მაგრამ იმ შემთხვევაში თუ საკითხი ჰიდგება, იმ ვადაზე რომლის განმარტებაშიც სახელმწიფო ვალდებულია შეინახოს ესა თუ ის მონაცემი, შეუძლებელია გავეჩვენოთ წინააღმდეგობას, იმასთან დაკავშირებით, შენახვის რა ვადაა ყველაზე გონივრული. რა ექნათ, თუ გარკვეული გარემოებები აბრკოლებენ ამ ფაქტს? ან როდისაა უკეთესი გამოქვეყნდეს ეს მონაცემი? – სეაჩს კითხვას პ. სომერი. ფიქრობ, მისი შეფასება სწორია, თუმცა ეს საკითხი არაა ისეთი მნიშვნელოვანი, რომ კონვენციის საჭიროება უარყოს. მიუხედავად ამისა, პ. სომერი ამ არგუმენტითაც ცდილობდა გაემართლებინა გაერთიანებული სამეფოს რუსეთის და ანდორის (ამ ქვეყნებს კონვენციის რატიფიცირება დღემდე არ მოუხდენიათ) კამპანიაში ყოფნა.

ალსანიშნავია, რომ გაერთიანებულ სამეფოში კიბერდანაშაულის პრობლემის თაობაზე დისკუსიის ახალი ტალღა ჯერ კიდევ 2007 წლის აგვისტოდან დაიწყო, როცა ლორდთა პალატის მეცნიერების და ტექნიკის კომიტეტმა გამოაქვეყნა ანგარიში. მასში გაკრიტიკებული იყო მთავრობა, რადგან მათ კომპიუტერული სისტემის უსაფრთხოებაზე პასუხისმგებლობა ინტერნეტ-მომხმარებლებს მიანდეს: ყველა ინტერნეტ-მომხმარებელი ვალდებული იყო თავად დაეცვა საკუთარი კომპიუტერული სისტემის უსაფრთხოება. კომიტეტის შეფასებით ეს ნიშნავდა ინტერნეტის უკონტროლო სივრცედ გადაქცევას. ანგარიშში ნათქვამია, რომ „ინტერნეტი წარმოადგენს სათაჩამო მოედანს კიბერდანაშაულებებისთვის და ბევრ ორგანიზაციას, რომელსაც საქმე აქვს ინტერნეტთან, შეეძლო უკეთ

143 იხ. Peter Sommer, Cybercrime Happens In An Instant, E-Newsletter "Electronic Newsletter on the Fight Against Cybercrime" (ENAC) №2, August, 2009, გვ. 2-3

დაეცვა ინტერნეტ-მომხმარებელთა უსაფრთხოება. ამ ორგანიზაციითაა რიგებში ჩამოთვლილი: აპარატული და პროგრამული საშუალების მწარმოებელი კომპანიები, ინტერნეტ-პროვაიდერები, ონლაინ-ბიზნესის წარმომადგენლები, ბანკები და სახელმწიფო."

კომიტეტი ყველა დაინტერესებულ ორგანიზაციას სთავაზობდა მოეხდინა უსაფრთხოებაზე პასუხისმგებლობის გადანაწილება. ინტერნეტ-პროვაიდერებს ეზრუნათ მათი ქსელის საშუალებით ჩართულ კომპიუტერული ვირუსის მატარებელი კომპიუტერების გაუვნებელყოფაზე, კომპიუტერული პროგრამის მწარმოებლებს აელოთ პასუხისმგებლობა ნაწარმის ნაკლოვანებაზე, ბანკებს აენახლაურებიანათ კლიენტისთვის ინტერნეტ-თაღლითობის გზით მიყენებული ზიანი და ა.შ. ანგარიშის ავტორები მოუწოდებდნენ სახელმწიფოს, დაესრულებინა „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირების პროცესი¹⁴⁴.

2007 წლის ოქტომბერში გაერთიანებული სამეფოს ხელისუფლებამ უარყო კომიტეტის რეკომენდაციითაა უმრავლესობა.¹⁴⁵

ლორდთა პალატის მეცნიერების და ტექნიკის კომიტეტის რეკომენდაციის ძირითადი ნაწილი ერთი შეხედვით იდეალურია. თუმცა ის განუხორციელებელი იქნებოდა იმ შემთხვევაშიც თუ მას მთავრობა მხარს დაუჭერდა. ჩემი აზრით, უკანონოა აიძულო ბანკი საკუთარ კლიენტს აუნახლაუროს ინტერნეტ-თაღლითობის გზით მიღებული ზიანი, ან/და ინტერნეტ-პროვაიდერს დაავალდებულო მის ქსელში არსებული კომპიუტერების კომპიუტერული ვირუსებისგან განმენდა. რა თქმა უნდა, ინტერნეტ-მომხმარებლისთვის მსგავსი მიდგომა ძალიან კარგია. მაგრამ არ უნდა დავივიწყოთ ბანკის და ინტერნეტ-პროვაიდერის უფლებები. აქედან გამომდინარე, დიდი ბრიტანეთის მთავრობის პოზიცია, როცა მან არ გაიზიარა აღნიშნული რეკომენდაცია, სრულიად მისაღებად მიმაჩნია.

როგორც უკვე აღინიშნა, კონვენციის რატიფიცირება დიდმა

144 იხ. Дэвид Эмм, Киберпреступность и закон, 19.06.2009(www.crime-research.ru/articles/depo24, http://www.securelist.com/ru/analysis/208050513/Kiberprestupnost_i_zakon_obzor_polozeniy_zakonodatelstva_Velikobritanii)

145 იხ. The Government Reply To The Fifth Report From The House Of Lords Science And Technology Committee Sesion 2006-2007 HI p.165 (<http://www.official-documents.gov.uk/document/cm72/7234/7234.pdf>).

ბრიტანეთმა 2011 წლის 25 მაისს განახორციელა, შესაბამისად, ბრიტანულ კანონმდებლობაში ასახულია კონვენციაში გათვალისწინებული დებულებები და მათ განხილვაზე აღარ შეეჩერდები.

იტალიაში „კიბერდანაშაულის შესახებ“ კონვენცია ძალაში შევიდა 2008 წლის 1 ოქტომბრიდან.¹⁴⁶ 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 შეუერთდა, ანუ საკუთარ კანონმდებლობაში გადაიტანა ყველა ის პრინციპი და ტერმინი, რომელიც კონვენციამ განსაზღვრა. იტალიელი მეცნიერი 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.¹⁴⁷

იტალიური სისხლის სამართლის კოდექსში განსაკუთრებით საინტერესოა ახალი რეგულაცია, რომელიც ეხება კომპიუტერულ თაღლითობას (იტალიის სისხლის სამართლის 640-მეოთხე მუხლი). იგი გულისხმობს ელექტრონული ხელმოწერის უკანონო გამოყენებას, რომლის საშუალებითაც დამნაშავე საკუთარი ან სხვა პირისათვის იღებს არალეგალურ შემოსავალს. ეს მუხლი საინტერესო იმითაა, რომ მისი სუბიექტი შეიძლება იყოს მხოლოდ ელექტრონული ხელმოწერის გამოყენებაზე უფლებამოსილი პირი. ეს განსაკუთრებული სიახლეა, რადგან მსოფლიოში ელექტრონული ხელმოწერის გამოყენება აქტიურად ხდება. შესაბამისად, გაზრდილია მისი გაყალბების საფრთხეც და სწორედ ამიტომ იტალიელმა კანონმდებელმა გადანაცვლა ქმედების კრიმინალიზაცია.

უნდა აღინიშნოს, რომ მსგავსი დანაშაულის გავრცელების საფრთხე საქართველოს ჯერ არ ემუქრება, რადგან ელექტრონული

146 იხ. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&D-F=&CL=ENG>

147 იხ. Giuseppe Corasaniti, Implementation Of The 2001 Convention on Cybercrime By Italy with transposition into Law No.48. Of 18 March 2008, E-Newsletter "Electronic Newsletter on the Fight Against Cybercrime"(ENAC)" №2, August, 2009, გვ. 7

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 მონეობილობა 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.

გამოდის, რომ სახეზე გვაქვს კიდევ ერთი სპეციალური სუბიექტი - კომპიუტერული ქსელის ოპერატორი. ასევე წინასწარ განსაზღვრულია მისი მოტივი - ანგარება.

გარდა ამისა, იტალიელ კანონმდებელს შანტაჟი დამამძიმებელ გარემოებად მიაჩნია, რაც ჩემი აზრით, გასათვალისწინებელი მიდგომაა.

2008 წელს ჟურნალი „მართლმსაჯულების“ ფურცლებზე გ. ლანჩავა წერდა, რომ კომპიუტერულ დანაშაულთან დაკავშირებული ნორმები უკრაინაში, საქართველოში, აზერბაიჯანში, ყაზახეთსა და რუსეთის ფედერაციაში გამოირჩეოდა „სამართლებრივი განუვითარებლობით და სამართლებრივი ტექნიკის გაუმართაობით“¹⁴⁸. აღნიშნულ მოსაზრებას ძნელია არ დაეთანხმო. ჩამოთვლილი ქვეყნები, გარდა საქართველოსი, დღესაც არ გამოირჩევა განსაკუთრებული წინსვლით ამ სფეროში, თუმცა რუსეთის სისხლის სამართლის კოდექსში 2011 წლის 7 დეკემბერს შევიდა ცვლილება, რომლის შედეგადაც შეიცვალა 272-ე, 273-ე და 274-ე მუხლები.

272-ე მუხლით დასჯადია კანონით დაცულ კომპიუტერულ ინფორმაციაში არამართლზომიერი შეღწევა, თუ ამ ქმედებამ გამოიწვია კომპიუტერული ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან კოპირება. მუხლის მე-2 ნაწილში დამამძიმებელ

148 იხ. გ. ლანჩავა „უკრაინის, საქართველოს, აზერბაიჯანის, ყაზახეთის რესპუბლიკისა და რუსეთის ფედერაციის სისხლის სამართლის კოდექსებში კომპიუტერული დანაშაულის ნორმები“. ჟურნ. მართლმსაჯულება, 2008წ. №3, გვ. 45

გარემოებად განსაზღვრულია 1-ლი ნაწილით გათვალისწინებული ქმედების ჩადენა ანგარებით ან თუ ამ ქმედებამ გამოიწვია მნიშვნელოვან ზიანი. მუხლის პენიშენაში 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 პენიშენაში განსაზღვრულია კომპიუტერული ინფორმაციის ცნება: „კომპიუტერული ინფორმაცია არის მონაცემი რომელიც წარმოდგენილია ელექტროსიგნალის ფორმით. მისი შენახვის, დამუშავების და გადაცემის ფორმას მნიშვნელობა არ აქვს.“

სავარაუდოდ რუს კანონმდებელს სურდა, ტერმინი „კომპიუტერული მონაცემი“ ორიგინალურად განემარტა. 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 ვიგულისხმოთ ნებისმიერი კომპიუტერული პროგრამაც.

რუსული კანონმდებლის ვინრო მიდგომა არასრულყოფილია, რადგან დანაშაული ისყება კომპიუტერულ სისტემაში უნებართვო შეღწევიდან და მხოლოდ ამის შემდეგ ხდება კომპიუტერული ინფორმაციის ხელყოფა. თუმცა, როგორც ჩანს, ეს გარემოება რუსეთში ყურადღების მიღმა დარჩა.

რუსი მეცნიერი პაველ დომკინი განმარტავს თუ რა უნდა ვიგულისხმოთ რუსეთის სისხლის სამართლის კოდექსის 272-ე მუხლის 1 ნაწილში მითითებულ ტერმინ „არამართლზომიერი“ არამართლზომიერი, ესე იგი კომპიუტერული ინფორმაციის ძალის და მიღების დადგენილი წესის დარღვევით განხორციელებული ეჭვი-

ბა. კანონით დაცულ კომპიუტერულ ინფორმაციაში შეღწევა არამართლზომიერია, როდესაც ხდება ჩამოთვლილთაგან ერთ-ერთი ნესის 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 შინაგანანესით, გარკვეულ ინფორმაციაში შესვლა აკრძალული აქვს. იმ ქმედებებში, 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 კონფიდენციალური ინფორმაცია. სახელმწიფო საიდუმლო განსაზღვრულია კანონით „სახელმწიფო საიდუმლოების შესახებ“ და მასში შედის სამხედრო, ეკონომიკური, სამეცნიერო, შიდა პოლიტიკასთან დაკავშირებული, კონტრდაზვერვის, ოპერატიულ-სამძებრო და სხვა ინფორმაცია. კონფიდენციალური მონაცემებია: პერსონალური, საგამოძიებო და სამართალწარმოების მონაცემი, ასევე სამსახურებრივი საიდუმლო (განსაზღვრულია რუსეთის სამოქალაქო კოდექსით), საადვოკატო, საექიმო საიდუმლო, სატელეკომუნიკაციო კავშირის, პირადი მიმოწერის საიდუმლო, კომერციული საიდუმლო და ა.შ.¹⁴⁹

ჩემი აზრით, პ. დომკინის მიერ სრულყოფილადაა განმარტებული ტერმინი „არამართლზომიერი“. ის ქართულ კოდექსში მითითებულ ტერმინ „უნებართვოს“ შეიძლება შევადაროთ, ან სულაც გავიგვივოთ, რადგან მათ შორის არსობრივი სხვაობა არ არსებობს.

ასევე საინტერესოა, რომ რუსი კანონმდებელი 272-ე მუხლით გათვალისწინებული ქმედებისთვის სისხლისსამართლებრივ

149 იხ. <http://www.advodom.ru/practice/cybercrime-5.php>

პასუხისმგებლობას კონკრეტული შედეგის დადგომას უკავშირებს, რაც არასწორად უნდა იქნეს მიჩნეული. კიბერდანაშაულის დასჯადობა უნდა უკავშირდებოდეს თუ არა შედეგს, აღნიშნულთან დაკავშირებით ნაშრომში უკვე ვისაუბროთ, ამიტომ ამ საკითხზე აღარ შევჩერდები.

ცვლილება განიცადა 273-ე მუხლმაც, რომლის განხილვას სათაურიდანვე დაეიწყებ, რადგან იგი განსხვავდება მუხლის შინაარსისგან: „დამაზიანებელი კომპიუტერული პროგრამის შექმნა, გამოყენება და გავრცელება“. მუხლის დისპოზიცია შემდეგნაირადაა ჩამოყალიბებული: „ისეთი კომპიუტერული პროგრამის ან ინფორმაციის შექმნა, გავრცელება ან გამოყენება, რომელიც გამიზნულია კომპიუტერული ინფორმაციის არასანქცირებული განადგურების, ბლოკირების, მოდიფიცირების, კოპირების ან კომპიუტერული ინფორმაციის დაცვის საშუალების განადგურებისთვის“. დამამძიმებელი გარემოებები ამ მუხლისთვისაც იგივეა, რაც 272-ე მუხლისთვის.

აღნიშნული მუხლი შეიძლება შევადაროთ საქართველოს სისხლის სამართლის კოდექსის 285-ე მუხლს, რომლის მიხედვითაც დასჯადია ისეთი კომპიუტერული პროგრამის ან/და სხვა მონყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეღწევისთვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა. ძირითადი განმასხვავებელი ნიშანი ამ ორ მუხლს შორის არის შედეგი. თუ რუსი კანონმდებელი აუცილებელ პირობად აყენებს ამ კომპიუტერული პროგრამის მავნე ხასიათს, რომლის გამოყენებითაც აუცილებლად უნდა დაზიანდეს კომპიუტერული ინფორმაცია, ქართული და ევროპული კანონმდებლობა მნიშვნელობას არ ანიჭებს ამ კომპიუტერული პროგრამის მოქმედების მავნე შედეგს. საქმარისია იმის დადგენა, რომ ის შექმნილია კიბერდანაშაულის თავით განსაზღვრული რომელიმე დანაშაულის და კოდექსის 158-ე მუხლით გათვალისწინებული დანაშაულის ჩასადენად.

საგულისხმოა ის გარემოება, რომ შესაძლოა რუსეთში 273-ე მუხლის დისპოზიციის არსებობის გამო დაუსჯელი დარჩეს, მაგალითად, ისეთი ქმედება, როგორიცაა კომპიუტერულ სისტემაში შეღწევა და გარკვეული ინფორმაციის გაცნობა მისი კოპირების,

განადგურების, ბლოკირების და მოდიფიცირების გარეშე. ეს კანონმდებლობის ნაკლად უნდა ჩაითვალოს. ასევე, ძალიან გაუგებარი ტერმინია „დამაზიანებელი“, რადგან კომპიუტერული ინფორმაციის განადგურების, ბლოკირების, მოდიფიცირების და კოპირებისთვის, ხშირად არაა აუცილებელი დამაზიანებელი პროგრამის გამოყენება. მაგალითად, ე.წ. „ტროას ცხენი“.

რუსი კანონმდებელი იჩენს ორიგინალობას და ამავე მუხლით იცავს კომპიუტერული ინფორმაციის დაცვის პროგრამულ საშუალებას, რაც აბსოლუტურად გაუმართლებელია. გამოდის, რომ საგამოძიებო ორგანო ვალდებულია ჯერ გასოიკვლიოს რა იყო კომპიუტერული ინფორმაციის დაცვის პროგრამული საშუალება (მაგალითად, პაროლი, კოდი, სპეციალური პროგრამა), როცა კომპიუტერული სისტემის შემთხვევაში, ჩვენ ისედაც ვგულისხმობთ, რომ სისტემა არის მთლიანი, დაცული და, მაშასადამე, მასში შესვლა აკრძალულია სისხლის სამართლის კანონით. ბუნებრივია, დანაშაულის ობიექტის დამატებითი დამცავი საშუალებით აღარ ვინტერესდებით, რადგან მისი დადგენა ელემენტარულად არაპრაქტიკულია.

თუ რუსი კანონმდებელი სისხლის სამართლის კოდექსის დაცვის ობიექტად თავიდანვე გამოაცხადებდა კომპიუტერულ სისტემას და არა ვინრო შინაარსის მატარებელ ტერმინ „კომპიუტერულ ინფორმაციას“ 272-ე და 273-ე მუხლებიც შედარებით უკეთეს შეფასებას დაიმსახურებდნენ.

ასევე გაუგებარია, რატომ არის 272-ე მუხლში აკრძალული „კანონით დაცულ კომპიუტერულ ინფორმაციაში არამართლზომიერი შეღწევა, თუ ამ ქმედებამ გამოიწვია კომპიუტერული ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან კოპირება“, როცა 273-ე მუხლში მხოლოდ „კომპიუტერულ ინფორმაციაში“ სხვადასხვა მანიპულაციისთვისაა დადგენილი სასჯელი? რა ისეთი მნიშვნელოვანი განსხვავება იპოვა კანონმდებელმა 272-ე და 273-ე მუხლებს შორის, რომ თუკი დამნაშავე არამართლზომიერად შეაღწევს კომპიუტერულ ინფორმაციაში, ის აუცილებლად კანონით დაცული ინფორმაცია უნდა იყოს, ხოლო თუ დამნაშავე ამ ინფორმაციის განადგურებას გადაწყვეტს, საკმარისია, ეს ინფორმაცია უბრალოდ კომპიუტერული ინფორმაცია იყოს. სავარაუდოდ, კანონ-

მდებელს გარკვეული არგუმენტები ექნებოდა ამ საკითხზე, თუმცა რთულია ამ ფაქტს მოეძებნოს რაციონალური ახსნა.

✓განვიხილოთ ასევე 274-ე მუხლი. იგი ჩამოყალიბებულია შემდეგნაირად: „კომპიუტერული ინფორმაციის ან ინფორმაციის ექსპლუატაციის, შენახვის, დამუშავების ან გადაცემის ნესების დარღვევა.“ ამ შემთხვევაშიც კანონმდებელი იცავს მხოლოდ „კომპიუტერულ ინფორმაციას“, ან უბრალოდ „ინფორმაციას“.

განვიხილოთ რა განსხვავებაა ამ სამ ტერმინს შორის. „კანონით დაცული ინფორმაცია“ არის ის ინფორმაცია, რომელიც დაცულია, კანონით. კომპიუტერული ინფორმაციის განმარტება, რუსეთის სისხლის სამართლის კოდექსით არის მონაცემი რომელიც წარმოდგენილია ელექტრონული სიგნალის ფორმით. მისი შენახვის, დამუშავების და გადაცემის ფორმას ჩნიშვნელობა არ აქვს. ხილო ინფორმაცია ძალიან ზოგადი ტერმინია და მას შეიძლება საერთოდ არანაირი კავშირი არ ჰქონდეს კომპიუტერთან. ამდენად, ამ სხვადასხვა ტერმინებს რუსულ კანონმდებლობაში შეაქვს ბუნდოვანება, უფრო მეტიც, მოცემული რედაქციით 274-ე მუხლით გათვალისწინებული ქმედება საერთოდ კავშირში არაა კომპიუტერულ დანაშაულთან, რადგან ინფორმაციის შენახვის ნესის დარღვევა არ უკავშირდება მხოლოდ კომპიუტერულ სისტემას და კომპიუტერულ მონაცემს.

რუსეთი ემიჯნება ევროპის საბჭოს „კიბერდანაშაულის შესახებ“ კონვენციას იმ არგუმენტით, რომ მისი 32-ე მუხლის „ბ“ პუნქტი არღვევს სახელმწიფოს სუვერენიტეტს, უსაფრთხოებას და მოქალაქეების უფლებებს¹⁵⁰. ამ პუნქტში განსაზღვრულია, რომ: „წევრ-სახელმწიფოს უფლება აქვს სხვა წევრი სახელმწიფოს ნებართვის გარეშე, მის ტერიტორიაზე არსებული კომპიუტერული სისტემის საშუალებით მიიღოს კომპიუტერული მონაცემი, თუ ეს წევრი სახელმწიფო მონაცემის გადაცემაზე კანონიერ უფლებას მიიღებს იმ პირისგან, რომელსაც აქვს უფლებამოსილება გადასცეს კომპიუტერული მონაცემები ამ წევრ-სახელმწიფოს კომპიუტერული სისტემის საშუალებით“. ქეტი სიცხადისთვის აღვნიშნავ, რომ მაგალითად, საქართველოს ოფიციალური თანხმობის გარეშე,

უნგრეთს, შეუძლია ინტერნეტ-პროვაიდერი კავკასუს ონლაინისგან მიიღოს ის ინფორმაცია, რომლის გაცემაზეც უფლებამოსილია სწორედ ეს კომპანია. საფიქრებელია, რომ სახელმწიფო სუვერენიტეტის დარღვევის საფრთხის ხელაღებით მტკიცება ან უარყოფა რთულია. თეორიულად, კი სახელმწიფოებს შორის თანამშრომლობა ყოველთვის დგას პირველ რიგში ამ სახელმწიფოების ნებაზე ითანამშრომლონ. სუვერენიტეტის დარღვევა კი ყოველთვის უნდა შეფასდეს, როგორც იძულების ან ძალადობის ფაქტი და მას თანამშრომლობასთან კავშირი არ აქვს.

აქედან გამომდინარე, რუსეთის მიერ ამ არგუმენტით აპელირება ნიშნავს, რომ ამ სახელმწიფოს არ აქვს სურვილი კიბერდანაშაულის სფეროში ითანამშრომლოს ევროულ ქვეყნებთან.

„კასპერსკის ლაბორატორიის“¹⁵¹ გენერალური დირექტორის ევგენი კასპერსკის აზრით კი ევროპის საბჭოს კონვენციასთან შედარებით ბევრად ეფექტური იქნებოდა მაღალიზიის¹⁵² მიერ ინიცირებულ პროექტში მონაწილეობა, რომელიც უფრო პერსპექტიულია კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლაში საერთაშორისო ძალისხმევისთვის.¹⁵³ ე. კასპერსკის აზრით, კონვენციას

151 ცნობილი კორპორაცია კომპიუტერულ ტექნოლოგიებში, იგი ანარმოებს მსოფლიოში ერთ-ერთ ყველაზე პოპულარულ ანტი-ვირუსს.

152 პროექტის ფუძემდებელი ორგანიზაციის დასახელებაა IMPACT. შტაბ-ბინა ჩდებარეობს მაღალიზიაში. ორგანიზაციის მიზანია კიბერტერორიზმთან ბრძოლა, კიბერდანაშაულის წინააღმდეგ საერთაშორისო სტრატეგიის შემუშავება. ორგანიზაციაში განეკუთვნებული არიან კომპიუტერულ ტექნოლოგიებზე მომუშავე უმსხვილესი კომპანიების წარმომადგენლები (და არა სახელმწიფოები), მათ შორის კასპერსკის ლაბორატორიის, გუგლის და ა.შ. ხელმძღვანელი პირები. ორგანიზაციის მუშაობის ძირითადი მიმართულებებია: რეაგირების გლობალური ცენტრის საშუალებით კიბერსაფრთხის მუდმივი მონიტორინგი. საერთაშორისო თანამშრომლობის ცენტრის საშუალებით მუდმივად მიმდინარეობს საკანონმდებლო ნორმების შემუშავება, ხოლო ჯადაშაადების ცენტრის საშუალებით ორგანიზაცია ამ სფეროში მოღვაწე ადამიანებს ეხმარება ეფექტურ გადამზადებაში. ამავე ორგანიზაციის უსაფრთხოების და სამეცნიერო კვლევის ცენტრი უზრუნველყოფს საექსპერტო კვლევის და სათანადო დასკვნის შემუშავებას კიბერუსაფრთხოების საკითხებთან დაკავშირებით. (www.impact-alliance.org).

153 იხ. www.gz-jurnal.ru/602

შეუერთდნენ მხოლოდ ის ქვეყნები, რომლებსაც აერთიანებთ ისტორიულად ჩამოყალიბებული კავშირი და რომელთაც საერთო პოლიტიკური და ეკონომიკური ინტერესები გააჩნიათ¹⁵⁴.

ფაქტია, რომ ე. კასპერსკის მოსაზრება არაა საფუძველს მოკლებული. თუმცა მიმაჩნია, რომ კიბერდანაშაულის წინააღმდეგ ბრძოლა იქნებოდა ბევრად ეფექტური თუ რუსეთის და ევროპის ქვეყნების ინტერესი ამ ბრძოლაში გაერთიანდებოდა.

ხაზგასასმელია, რომ სანამ რუსეთი არ შეუერთდება კონვენციას, ევროპის ქვეყნების უმრავლესობა დარჩება თეორიული საფრთხის წინაშე – საკუთარ თავზე გამოსცადოს 2007 წელს ესტონეთზე და 2008 წელს საქართველოზე განხორციელებული ე.წ. „დოს“ შეტევა, რომელიც სწორედ რუსეთიდან განხორციელდა.

154 იხ. <http://www.cnews.ru/news/top/index.shtml?2008/03/27/293913>

კომპიუტერული დანაშაული არასდროს ყოფილა ქართველი მეცნიერების ღრმა კვლევის ობიექტი და ის უმეტესად შემოიფარგლებოდა სხვადასხვა უცხოენოვანი ნაშრომების, პუბლიკაციების, კომენტარების თარგმნით. თუმცა, მკვლევარების გარკვეული ნაწილის პლაგიატობა რა გასაკვირია მაშინ, როცა საქართველოს სისხლის სამართლის კოდექსი ევროპის საბჭოს კონვენციის რატიფიცირებამდე 284-ე, 285-ე და 286-ე მუხლები პირდაპირ იყო გადმონერული რუსეთის ფედერაციის სისხლის სამართლის კოდექსის 272-ე, 273-ე და 274-ე მუხლებიდან. გარდა ამისა, ოფიციალური სტატისტიკა 2010 წლამდე ამტკიცებდა, რომ კიბერდანაშაული საქართველოში თითქმის არ არსებობს. 2010 წლის 24 სექტემბერს განხორციელებული საკანონმდებლო ცვლილება, ისევე, როგორც ევროპის საბჭოს კონვენციაზე მიერთება წინგადადგმული ნაბიჯებია, თუმცა, არასაკმარისი. სასამართლო პრაქტიკის ანალიზი მიწმობს, რომ გარკვეულ შემთხვევებში ადგილი აქვს კომპიუტერულ დანაშაულთან დაკავშირებული ტერმინების ბუნდოვანი ინტერპრეტაციას, ან ხდება დანაშაულებრივი ქმედების არასწორი კვალიფიკაცია.

წარმოდგენილ ნაშრომში დეტალურადაა განხილული, როგორც ევროპის საბჭოს კონვენცია, კიბერდანაშაულთან მიმართებაში სხვა საერთაშორისო აქტები, ასევე ქართული კანონმდებლობა და სასამართლო პრაქტიკა. ქვემოთ მოცემულია ის ძირითადი თეზისები, რაც დასკვნის სახით შეიძლება გამოვყოთ. ყველა აღნიშნული მოსაზრება ნაშრომში დეტალურადაა დასაბუთებული, ამიტომ აქ მოკლედ შევხები:

ა) გაუგებარია, 284-ე მუხლის მე-2 ნაწილში დამამძიმებელ გარემოებად მნიშვნელოვანი ზიანის მითითება, რადგან დანაშაული ფორმალური შინაარსიისა. გაურკვეველია, როგორ უნდა გამოისახოს ფულად თანხაში კომპიუტერულ სისტემაში უნებართვო მელნევის ფაქტი, როცა მისი განხორციელება არანაირი უარყოფითი შედეგის დადგომას არ უკავშირდება? იმ შემთხვევაში თუ ეს ქმედება გამოიწვევს კომპიუტერული მონაცემის დაზიანებას, შეცვლას და ა.შ. სახეზე გვექნება 286-ე მუხლით განსაზღვრული ქმედება, ხოლო

თუ მაგალითად, კომპიუტერულ სისტემაში უნებართვო შეღწევის შედეგად განხორციელდება სხვისი ქონების მართლსაწინააღმდეგო მისაკუთრება, ქმედება უნდა დაკვალიფიცირდეს, როგორც 177-ე მუხლის 1-ლი ნაწილით გათვალისწინებული ქმედება, კერძოდ, ქურდობა. შესაბამისად, 150 ლარზე მეტი ოდენობის ზიანის დადგომის შემთხვევაში 177-ე მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით, ან მე-4 ნაწილის „ბ“ ქვეპუნქტით.

აქედან გამომდინარე მიზანშეწონილი იქნება ამოღებულ იქნეს 284-ე მუხლის მე-2 ნაწილის „დ“ ქვეპუნქტი.

ბ) 284-ე მუხლი ღიად ტოვებს კომპიუტერულ სისტემაში შესვლის უფლებამოსილების ფარგლების გადამეტების საკითხს, რაც განსაკუთრებით მნიშვნელობას იძენს მაშინ, როცა კომპიუტერულ სისტემაში შეღწევა განხორციელდა სამსახურებრივი მდგომარეობის გამოყენებით. შესაძლოა, გარკვეულ დონეზე რომელიმე ორგანიზაციის თანამშრომელს ჰქონდეს უფლება შეაღწიოს კომპიუტერულ სისტემაში, თუმცა აკრძალული ჰქონდეს კომპიუტერული სისტემის ცალკეულ პროგრამაში ან ჩანაწერში შესვლა. ამიტომ სასურველია 284-ე მუხლის შენიშვნას დაემატოს შემდეგი სახის ჩანაწერი: „კომპიუტერულ სისტემაში უნებართვო შეღწევად განიხილება კომპიუტერულ სისტემაში შეღწევის უფლებამოსილების ფარგლების გადამეტება“.

გ) ქართველმა კანონმდებელმა 285-ე მუხლით დასჯადად გამოაცხადა სისხლის სამართლის კოდექსის XXXV თავით და 158-ე მუხლით (რომელიც ეხება კერძო კომუნიკაციის საიდუმლოების დარღვევას) გათვალისწინებული დანაშაულის ჩადენის მიზნით კომპიუტერული პროგრამის ან/და სხვა მოწყობილობის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა და ჩემი აზრით შეცდომაც დაუშვა, რადგან სახეზე მივიღეთ სრულიად უცნაური ვითარება. თუ პირი ერთდროულად არ იმუქმედებს კიბერდანაშაულის თავით განსაზღვრული და 158-ე მუხლით გათვალისწინებული დანაშაულის მიზნით, სახეზე არ გვიქნება 285-ე მუხლით გათვალისწინებული ქმედება. შესაძლოა ეს ტექნიკური ხასიათის შეცდომაა. ამ ჩანაწერის პრაქტიკაში გამოყენების სირთულზე ნაშრომში დეტალურად ვისაუბრეთ. აღსანიშნავია, რომ პრობლემის გადაჭრა იოლად არის

შესაძლებელი. კერძოდ, 285-ე მუხლის მეორე ნაწილში „და“ კავშირის ნაცვლად უნდა მიეთითოს „ან/და“: კომპიუტერული პროგრამის ან/და სხვა მოწყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ამ თავით ან/და ამ კოდექსის 158-ე მუხლით გათვალისწინებულ დანაშაულის ჩადენის მიზნით.

დ) აღსანიშნავია, რომ ე.წ. „დოს“ შეტყევის შემთხვევაში, მართალია, ხორციელდება კომპიუტერული მონაცემის გადაცემა, თუმცა „უნებართვობა“ სახეზე არ გვაქვს, რადგან ე.წ. „დოს“ შეტყევა გულისხმობს საიტზე შესვლის ერთდროულად ათასობით მოთხოვნას, რაშიც უკანონო და მფლობელის ნების საწინააღმდეგო არაფერია. უფრო, მეტიც ინტერნეტ-საიტი არის საჯარო ელექტრონული სივრცე, რომლით სარგებლობა ნებისმიერ ინტერნეტ-მომხმარებელს შეუძლია. გამოდის რომ თუ სისხლის სამართლის კოდექსი არ მოგვცემს უფრო ზუსტ განმარტებას, იმ შემთხვევაშიც კი თუ დამტკიცდება, რომ კიბერშეტყევის შედეგად სამიზნე კომპიუტერული სისტემის ფუნქციონირება შეფერხდა განზრახ და მნიშვნელოვნად, ამ ქმედებებს 286-ე მუხლით მაინც ვერ დავაკვალიფიცირებთ.

მიზანშეწონილია, რომ ე.წ. „დოს“ შეტყევა განხილულ იქნას როგორც დამოუკიდებელი კომპიუტერული დანაშაული და კიბერ-დანაშაულის თავს დაემატოს ცალკე მუხლად. ასევე, სასურველია მასში არ მიეთითოს დათქმა „მნიშვნელოვან შეფერხებაზე“, რადგან საკმარისია მიუთითოთ „კომპიუტერული სისტემის ფუნქციონირების შეფერხება“, ხოლო თუ კანონმდებელი აუცილებლად მიიჩნევს ზემოაღნიშნული ტერმინის გამოყენებას, მაშინ შეიტანოს მეტი სიცხადე მის განმარტებაში და მუხლს დაურთოს შესაბამისი პენიშენა.

ე) კიბერდანაშაულში არასრულყოფილად არის წარმოდგენილი ზოგიერთი დანაშაულებრივი ქმედების დაჰამჩიმებელი გარემოებები. მათში არ არის გათვალისწინებული ამ დანაშაულთა ჩადენა ანგარებით და შანტაჟით.

ჩემი პოზიცია, განსხვავებით ქართველი კანონმდებლისგან, ემთხვევა გერმანიის, იტალიის, ამერიკის და ბევრი სხვა ქვეყნის კანონმდებლის პოზიციას, რომლებმაც კიბერდანაშაულის დამამძიმებელ გარემოებად მიიჩნიეს ისეთი ქმედების ჩადენა, რომლის შედეგადაც ხდება სახელმწიფო ინტერესის და საზოგადოებრივი მნიშვნელობის მომსახურების ხელყოფა და ამიტომ მიმაჩნია, რომ, კიბერდანაშაულის თავში შესულ სამივე მუხლს დამამძიმებელ გარემოებად უნდა დავამატოს პუნქტი: „თუ ამ ქმედებამ ხელყო სახელმწიფოს ინტერესებში არსებული ან საზოგადოებრივი მომსახურებისთვის მნიშვნელოვანი კომპიუტერული სისტემა.“

ვ) სისხლის საქართლის კოდექსი სხვა ტიპის დანაშაულებზეც ითვალისწინებს იურიდიული პირის სისხლისსამართლებრივ პასუხისმგებლობას, თუმცა კიბერდანაშაულთან მიმართებაში, მიმაჩნია, რომ აღნიშნული საკითხი მოითხოვს სიღრმისეულ გააზრებას. განსაკუთრებულ ორაზროვნებას იწვევს კოდექსის 107¹-ე მუხლის მე-4 ნაწილი, რომლის მიხედვითაც იურიდიული პირი პასუხს აგებს იმ შემთხვევაშიც, დადგინდება თუ არა დანაშაულის ჩამდენი ფიზიკური პირი. ეს გარემოება, კი იმ პირობებში, როდესაც კომპიუტერული დანაშაულის მასშტაბი სცილდება ყოველგვარ ფიზიკურ და წარმოსახვითი საზღვარს, ბადებს შესაძლებლობას ზიანი მიადგეთ სრულიად უდანაშაულო იურიდიულ პირებს.

ზ) 324¹-ე მუხლი გულისხმობს არა დამოუკიდებელ დანაშაულს, არამედ მხოლოდ კასონით დაცული კომპიუტერული ინფორმაციის დაუფლების, მისი გამოყენების ან გამოყენების მუქარის გზით ჩადენილ ტერორისტულ აქტს. 324¹-ე მუხლში აღწერილი ქმედება რეალურად არის ტერორისტული აქტის ჩადენის საშუალება. 323-ე მუხლის შესაბამისად: „ტერორისტული აქტი, ესე იგი აფეთქება, ცეცხლის წაქიდება, იარაღის გაშოყენება ან სხვა ქმედება, რაც ქმნის ადამიანის სიცოცხლის მოსპობის, მნიშვნელოვანი ქონებრივი ზიანის ან სხვა მძიმე შედეგის განხორციელების საშიშროებას, ჩადენილი მოსახლეობის დამინების ან ხელისუფლების ორგანოზე, უცხო ქვეყნის ხელისუფლების ორგანოზე ან საერთაშორისო ორგანიზაციაზე ზემოქმედების მიზნით.“

324¹-ე მუხლში აღწერილი დანაშაული ფაქტობრივად 323-ე მუხლში მითითებული „სხვა ქმედებაა“. გარდა ამისა, 324¹-ე მუხლი

მოიცავს მთელ რიგ ბუნდოვან ტერმინებს, რომელზეც ნაშრომის შესაბამის თავში დეტალურადაა საუბარი. ამდენად მიმაჩნია, რომ აღნიშნული მუხლი საჭიროებს სერიოზულ გადამუშავებას.

თ) კიბერდანაშაულის თავში შესული მუხლებით გათვალისწინებული დანაშაულის ჩადენისთვის ქაქსიმალურ სასჯელის ვადად განსაზღვრულია 6 წლამდე თავისუფლების აღკვეთა.

ნაშრომში განხილულ იქნა ე.წ. „დოს“ შექცევის, კომპიუტერული ვირუსების და ა.შ. საფრთხე და მისი შესაძლო საკმაოდ მძიმე შედეგები. ამიტომ, სასურველია, გადაიხედოს სასჯელის ზომები. მართალია, ჩემი პირადი აზრით, სასჯელის დამძიმება არაა გამოსავალი, მაგრამ კიბერდანაშაულის საფრთხის გათვალისწინებით მიმაჩნია, რომ პრევენციის მიზნით ისეთი დანაშაულებრივ ქმედებებზე რის შედეგედაც ზიანდება სახელმწიფო ინტერესები ან საზოგადოებისთვის მნიშვნელოვანი მომსახურებები, სასჯელის ზედა ზღვრად დანესდეს უფრო მაღალი სასჯელი.

ი) სპეციალისტების აღზრდის მიზნით, ჩატარებული ტრენინგები არასაკმარისია. საჭიროა სახელმწიფოს მხრიდან მეტი აქტიობა, სასწავლო პროგრამის დაფინანსება, რათა რამდენიმე წელიწადში საქართველოს ჰყავდეს საკმარისი კვალიფიკაციური სპეციალისტები კიბერდანაშაულის წინააღმდეგ საბრძოლველად.

კ) როგორც სასამართლო პრაქტიკის ანალიზმა ცხადყო უმრავლეს შემთხვევებში კომპიუტერულ ტექნოლოგიებში სპეციალური ცოდნის მქონე ადამიანების ჩართვა არ ხდებოდა.

სასურველია, სასამართლო გამოძიების პროცესში სასამართლო აქტიურად იყენებდეს კიბერუსაფრთხოების ექსპერტებს, რათა რიგ ტექნიკურ საკითხზე შეიქმნას უფრო ნათელი სურათი და მოხდეს დანაშაულის სწორი კვალიფიკაცია.

იმედს ვიტოვებ, რომ უახლოეს წლებში საქართველოს კანონმდებლობა გახდება უფრო სრულყოფილი, ხილო კომპიუტერულ დანაშაულთან ბრძოლა კიდევ უფრო ეფექტური.

სახელმძღვანელოები, მონოგრაფიები და სტატიები:

1. ნერეთელი თ. ცყეშელიაძე გ. „მოძღვრება დანაშაულზე“. გამომც. „მეცნიერება“, თბ. 1969წ.
2. ნერეთელი თ. „სისხლის სამართლის პრობლემები“, I ტომი, გამომც. „მერიდიანი“, თბ. 2007წ.
3. სურგულაძე ლ. „სისხლის სამართალი“, გამომც. „ქრონოგრაფი“, თბ. 1997წ.
4. ცაცანაშვილი მ. „ინფორმაციული საზოგადოება და ინფორმაციის სამართლებრივი რეგულირება“, გამომც. „ტექნიფორმი“ თბ. 1999წ.
5. კაცმანი ა. სადისერტაციო ნაშრომი „კომპიუტერული დანაშაული“, თბ. 2004წ.
6. გამყრელიძე ი. „საქართველოს სისხლის სამართლის კოდექსის განმარტება“, ზოგადი ნაწილი, I წიგნი, საქართველოს მეცნიერებათა აკადემიის იურიდიული ინსტიტუტის სახელობის სახელმწიფოსა და სამართლის ინსტიტუტი, თბ. 2005წ.
7. ნაჭყებია გ. „სისხლის სამართალი, ზოგადი ნაწილი“, გამომც. „ინოვაცია“, თბ. 2011წ.
8. მჭედლიშვილი ჰედრიხი ქ. „სისხლის სამართალი ზოგადი ნაწილი II. დანაშაულის გამოვლენის ცალკეული ფორმები“, გამომც. „მერიდიანი“ თბ. 2011წ.
9. ავტორთა კოლექტივი „სისხლის სამართლის ზოგადი ნაწილი“, გამომც. „მერიდიანი“ თბ. 2007წ.
10. ავტორთა კოლექტივი „სისხლის სამართლის კერძო ნაწილი“, წიგნი I, გამომც. „მერიდიანი“, თბ. 2011წ.
11. ავტორთა კოლექტივი „სისხლის სამართლის კერძო ნაწილი“, წიგნი II, გამომც. „მერიდიანი“, თბ. 2012.
12. ავტორთა კოლექტივი. „ორგანიზებული დანაშაულის თანამედროვე გამოვლინებები: კრიმინალიზაციისა და სამართალშეუარდების პრობლემები ქართულ სისხლის სამართალში“, შ. რუსთაველის ეროვნული სამეცნიერო ფონდი, თბ. 2012წ.

13. ტურავეა მ. „სისხლის სამართალი, ზოგადი ნაწილის მიმოხილვა“, გამომც. „ბონა კაუზა, თბ. 2010წ.
14. ტურავეა მ. „დანაშაულის მოძღვრება“, წიგნი I, გამომც. „მერიდიანი“, თბ. 2011წ.
15. ლეკვეიშვილი მ. მამულაშვილი გ. „დანაშაული სახელმწიფო-სა და სასამართლო ხელისუფლების წინააღმდეგ“, გამომც. „მერიდიანი“, თბ. 2002წ.
16. გორაშვილი გ. „ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები“ გამომც. „უნივერსალი“, თბ. 2010წ.
17. კაცმანი ა. „კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება“, ჟურნ. „სამართალი“ 2000წ. №2.
18. ლანჩავა გ. „უკრაინის, საქართველოს, აზერბაიჯანის, ყაზახეთის რესპუბლიკისა და რუსეთის ფედერაციის სისხლის სამართლის კოდექსებში კომპიუტერული დანაშაულის ნორმები“, ჟურნ. მართლმსაჯულება, 2008წ. №3.
19. ლანჩავა გ. „კომპიუტერული დანაშაული“, ჟურნ. „მართლმსაჯულება“, 2008წ. №2.
20. ბოძაშვილი ლ. კობხეიძე ნ. „კიბერსივრცის სამართალი“, 2012წ. (წიგნის ოფიციალური ელ-ვერსია გამოქვეყნებულია საიტზე www.lit.ge).
21. ცომაია ნ. „სახელმწიფოს მხრიდან კომპიუტერულ სისტემებში ფარული შეღწევა და ამ ღონისძიების კონსტიტუციურ-სამართლებრივი საზღვრები“, ჟურნ. „მართლმსაჯულება და კანონი“, 2008წ. №2.
22. ოხანაშვილი ა. „იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობა“, თბილისის ივ. ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ჟურნალი, 2009წ. №2
23. ავტორთა კოლექტივი „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ: ტრენინგის სახელმძღვანელო“, ევროსაბჭო, სტრასბურგი, 2010წ.
24. ავტორთა კოლექტივი „ელექტრონული მტკიცებულების ამოღება“, ევროკავშირი, 2003წ.

25. იოვანოვიჩი მ. „კომპიუტერული პროგრამების სამართლებრივი დაცვის უზრუნველყოფის საკითხები, ჟურნ. „მართლმსაჯულება“ 2008წ. №3.
26. ქიქოძე გ. (ნმ. ეპისკოპოსი) „ცდისეული ფსიქოლოგიის საფუძვლები“ (ნაშრომში გამოყენებულია ნიგნის ელექტრონული ვერსია, იხ. წყარო <http://www.orthodoxy.ge/fsiqologia/gabriel/fsiqologia-4-2.htm#116>).
27. Тропина Т. “Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы” (იხ. <http://www.crime.vl.ru/index.php?p=3626&print=1&more=1>)
28. Мандиа К. Просис К. “Защита от вторжении: Расследование компьютерных преступлений”, Переводчик О.Труфанов, Изд. “Лори”, Москва, 2005 г.
29. Черкасов В.Н. “О понятии Компьютерная преступность”, Проблемы компьютерной преступности: Выпуск 2. - Мн.: НИИ ПККСЭ МЮ РБ, 1992. С.5.
30. Карчевский Н.В. “Компьютерные преступления:определение, объект и предмет”, Доклад V Международной конференции “Право и Интернет: теория и практика” 2003г. (www.ifar.ru/pi/05/karchev.htm).
31. Мэйволд Е. Интернет-Университет Информационных Технологий, Лекция №5: Юридические вопросы информационной безопасности 31.07.2006 (<http://www.intuit.ru/department/security/netsec/5/>).
32. Эмм Д. “Киберпреступность и закон”, 19.06.2009 (www.crime-research.ru/articles/depo24).
33. Charney S. Alexander K. Types of computer crime,25.11.2005 თ. იაშვილის თარგმანი. (<http://www.crime-research.org/articles/types-of-computer-crime/2>).
34. Kristin M. Finklea, Catherine A. Theohary, „Cybercrime:Conceptual Issues for Congress and U.S. Law Enforcement“, US Congressional Research Service Reports, 2012
35. Sommer P. “Cybercrime Happens In An Instant”, E-Newsletter “Electronic Newsletter on the Fight Against Cybercrime” (ENAC) №2, August, 2009.
36. Verdelho P. Cybercrime and Electronic Evidence, E-Newsletter

"Electronic Newsletter on the Fight Against Cybercrime"(ENAC)" №1, jule, 2009.

37. *Corasaniti G.* "Implementation Of The 2001 Convention on Cybercrime By Italy with transposition into Law No.48. Of 18 March 2008", E-Newsletter "Electronic Newsletter on the Fight Against Cybercrime"(ENAC) №2, August, 2009.

38. *Biancuzzi F.* Interview: "Germany and new cybercrime law" 11.07.2007. (<http://www.crime-research.org/interviews/Interview-Germany-and-new-cybercrime-law/>).

39. *MARKOFF J.* "Before the Gunfire, Cyberattacks", 12.08.2008 (http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=2&ref=world&oref=slogin&oref=slogin).

40. Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448(Based on article 12 of the Council Framework Decision of 24.02.2005 on attacks against information systems).

41. Field Guidance New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot act of 2001, Computer Crime and Intellectual Property Section (CCIPS), Перевод М. Буряк (<http://kiev-security.org.ua/box/4/94.shtml>).

42. The Internet Crime Complaint Center 2006 Internet Fraud Crime Report: January 1, 2006-December 31, 2006 (http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf).

43. *Schulman C.* Council of Europe measures for fighting against cybercrime, E-Newsletter "Electronic Newsletter on the Fight Against Cybercrime" (ENAC)" №2, August, 2009.

44. The Government Reply To The Fifth Report From The House Of Lords Science And Technology Committee Sesion 2006-2007 HI p.165 (<http://www.official-documents.gov.uk/document/cm72/7234/7234.pdf>).

45. *Aldrich Richard W.*, "CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME", USAF Institute for National Security Studies USAF Academy, Colorado, April 2000

46. United Nations A/CONF.187/10, (об. <http://ebookuniverse.net/aconf18710-pdf-d8490066>)

47. *Shinder Littlejohn Debra*, "Scene of the Cybercrime: Computer Forensics Handbook", USA, Rockland, Syngress Publishing Inc. 2002.

სასამართლო პრაქტიკის მასალები:

1. თბილისის საოლქო სასამართლოს 2004 წლის 19 მაისის განაჩენი, საქმე №1/ა-74.
2. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2011 წლის 24 თებერვლის განაჩენი, საქმე №1/6833-10.
3. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2011 წლის 4 მარტის განაჩენი, საქმე №1/1144-11.
4. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2011 წლის 23 სექტემბრის განაჩენი, საქმე №1/3979-11.
5. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2011 წლის 30 მაისის განაჩენი, საქმე №1/1992-11.
6. თბილისის სააპელაციო სასამართლოს სისხლის სამართლის საქმეთა პალატის 2011 წლის 3 ივნისის განაჩენი, საქმე №1/ბ-274-11.
7. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 25 ოქტომბრის განაჩენი, საქმე №1/3106-12.
8. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 5 ივლისის განაჩენი, საქმე №1/2962-12.
9. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 22 მაისის განაჩენი, საქმე №1/2263.
10. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 18 სექტემბრის განაჩენი, საქმე №1/3126.
11. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 26 აპრილის განაჩენი, საქმე №1/1829.
12. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 2 აგვისტოს განაჩენი, საქმე №1/3140.
13. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 13 ივნისის განაჩენი, საქმე №1/2559.
14. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 14 ივნისის განაჩენი, საქმე №1/2551.
15. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 25 აპრილის განაჩენი, საქმე №1/1756.
16. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის 2012 წლის 29 ივნისის განაჩენი, საქმე №1/2814-12.

ნორმატიული მასალა:

1. საქართველოს კონსტიტუცია, 1995 წ. 24 აგვისტო
2. საქართველოს სისხლის სამართლის კოდექსი, 1999 წ. 22 ივლისი
3. საქართველოს კანონი „საქართველოს ზოგიერთ საკანონმდებლო აქტში ცვლილებების და დამატებების შეტანის შესახებ“ 2010 წ. 24 სექტემბერი
4. ევროპის საბჭოს კონვენცია „კიბერდანაშაულის შესახებ“, 2001 წ. 23 ნოემბერი
5. საქართველოს პრეზიდენტის ბრძანებულება „კიბერდანაშაულის შესახებ“, 2012წ. 1 ივნისი
6. საქართველოს პრეზიდენტის განკარგულება „კიბერდამნაშაულობის შესახებ“ კონვენციის ხელმოწერის თაობაზე, 2008წ. 28 მარტი
7. საქართველოს პრეზიდენტის ბრძანებულება „საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013-2015წ.წ. სამოქმედო გეგმის დამტკიცების შესახებ“, 2013 წლის 17 მაისი;
8. „ამერიკის შეერთებული შტატები – საქართველოსქარტიასტრატეგიული პარტნიორობის შესახებ“ 2009წ. 9 იანვარი
9. საქართველოს ფინანსთა მინისტრის ბრძანება „საგადასახადო საიდუმლოების შემცველი ინფორმაციის შენახვის რეჟიმის და დაშვების წესის შესახებ ინსტრუქციის დამტკიცების თაობაზე“ 2005 წ. 4 მაისი
10. საქართველოს თავდაცვის მინისტრის ბრძანება „საქართველოს შეიარაღებული ძალების გაერთიანებული შტაბის J-6 კავშირგაბმულობის და ინფორმაციული სისტემების (CIS) დეპარტამენტის დებულების დამტკიცების შესახებ“ 2008 წ. 22 მაისი
11. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems ,Official journal of the European Union L69/67, from 16.3.2005
12. U.S. Code ,Title 18, part I, Chapter 47, § 1030, Fraud and related activity in connection with computers (<http://www.law.cornell.edu/us-code/18/1030.html>).

ინტერნეტ-მასალები:

1. <http://www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf>
2. http://www.mfa.gov.ge/index.php?lang_id=GEO&sec_id=59&info_id=-15216
3. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>
4. <http://24saati.ge/index.php/category/news/justice/2010-02-01/3148.html>
5. http://en.wikipedia.org/wiki/Convention_on_Cybercrime
6. <http://www.today.az/news/society/46054.html>
7. http://www.usa.mfa.gov.ge/index.php?lang_id=GEO&sec_id=131&info_id=183
8. <http://www.cybercrimelaw.net/laws/countries/australia.html>
9. http://www.gesetze-im-internet.de/stgb/_303b.html
10. <http://www.cybercrimelaw.net/laws/countries/Singapore.html>
11. <http://www.gesetze-im-internet.de/stgb/>
12. <http://www.cybercrimelaw.net/Hungary.html>
13. <http://www.cybercrimelaw.net/UK.html>
14. <http://www.cybercrimelaw.net/Hungary.html>
15. <http://www.crime-research.ru/news/13.08.2008/4727/>
16. <http://www.crime-research.ru/news/12.08.2008/4722/>
17. <http://presa.ge/index.php?text=news&i=4413>