ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

იურიდიული ფაკულტეტი

მარიამ სალუქვაძე

თემის სათაური:

ფინანსურად მოტივირებული კიბერდანაშაულების კვალიფიკაციასთან დაკავშირებული პრობლემები

წარდგენილია სამართლის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: მაია ივანიძე - თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის სრული პროფესორი

თბილისი
2022

სარჩევი

შემოკლებანი

§	პარაგრაფი
№	ნომერი
მუხ.	მუხლი
გვ.	გვერდი
იხ.	იხილე
შეად.	შეადარე
სსკ	საქართველოს სისხლის სამართლის კოდექსი
სსსკ	საქართველოს სისხლის სამართლის საპროცესო კოდექსი
სს	სისხლისსამართლებრივი
ა.შ.	ასე შემდეგ
ე.წ.	ეგრეთ წოდებული
რედ.	გამოცემის რედაქტორი
სხვ.	სხვა
ჟურნ.	ჟურნალი
ელ. ფოსტა	ელექტრონული ფოსტა
თბ.	თბილისი
აშშ	ამერიკის შეერთებული შტატები
გაერო	გაერთიანებული ერების ორგანიზაცია
ევროსაბჭო	ევროპის საბჭო
აშშ	ამერიკის შეერთებული შტატები
გაერო	გაერთიანებული ერების ორგანიზაცია

შსს	შინაგან საქმეთა სამინისტრო
OECD	Organisation for Economic Co-operation and Developmens
APEC	Asia-Pacific Economic Cooperation
AU	African Union
WB	World Bank
WSIS	The World Summit on the Information Society
EC3	European Cybercrime Centre
DDoS	Distributed Denial of Service
IP	Internet Protocol
MITM	Man in the Middle
v.	versus
art.	Article
StGB	Strafgesetzbuch

შესავალი

დღეს განსაკუთრებით აქტუალურია ინფორმაციული უსაფრთხოების უზრუნველყოფის საკითხები. არავისთვის არ არის სადავო, რომ ინფორმაციულ-საკომუნიკაციო ტექნოლოგიები (ICT) უზარმაზარ გავლენას ახდენს საზოგადოების ცხოვრების ყველა ასპექტებზე. დღევანდელ რეალობაში თითქმის წარმოუდგენელია ცხოვრება ინტერნეტისა და კომპიუტერული მოწყობილობების მონაწილეობის გარეშე. დღეს ინფორმაცია წარმოადგენს „ინფორმაციული საზოგადოების“ საგანძურს.

ტექნოლოგიური განვითარების უპირატესობების გამოყენებასთან ერთად, ინფორმაციული საზოგადოება დადგა ახალი გამოწვევების წინაშე, როგორიცაა ინტერნეტ ტექნოლოგიების ბოროტად გამოყენება და დანაშაულთა გადანაცვლება ვირტუალურ სივრცეში. ციფრულ სივრცეში გარანტირებულმა ანონიმურობამ უფრო მეტად მიმზიდველი გახადა ბოროტმოქმედებისთვის კიბერდანაშაულთა ჩადენა. ამასთან ერთად, უნდა გვახსოვდეს, რომ ინფორმაციულ-საკომუნიკაციო ტექნოლოგიები უნდა წარმოადგენდეს, პირველ რიგში, ინსტრუმენტს, მიზნის მიღწევის საშუალებას და არა თვითმიზანს. ამიტომ, მნიშვნელოვანია უზრუნველყოფილი იყოს ინფორმაციული უსაფრთხოება და კონფიდენციალურობის დაცვა.

სისხლის სამართლის კანონმდებლობისა და კიბერსივრცეში კრიმინალური ქცევის პრაქტიკის ანალიზი მიზნად ისახავს ეროვნული ეკონომიკის დიგიტალიზაციის პროცესში, ადამიანის ფუნდამენტური უფლებების ეფექტურ დაცვას. გლობალურ საინფორმაციო სივრცეში ჩადენილ ეკონომიკურ დანაშაულების ბრძოლის ეფექტური სამართალდამცავი პოლიტიკა, მოითხოვს საერთაშორისო კონსენსუსს, ასევე საჯარო და კერძო სექტორის პარტნიორობის განვითარებას. სწორედ დანაშაულის მომეტებულმა საფრთხემ და მისი ტრანსსასაზღვრო ხასიათიდან გამომდინარე, აუცილებელი გახდა სახელმწიფოს სუვერენიტეტის ახლებური ხედვის ჩამოყალიბება და საერთაშორისო ინსტრუმენტების შემუშავება.

დღეს ყველაზე მნიშვნელოვან საერთაშორისო დოკუმენტად აღიარებულია ევროპის საბჭოს კიბერდანაშაულთან ბრძოლის კონვენცია, რომელიც საქართველოს მიერ არის რატიფიცირებული. აღსანიშნავია, რომ საქართველოს სისხლის სამართლის კოდექსში განხორციელებული საკანონმდებლო ცვლილებები მიმართულია კონვენციის დებულებებთან შესაბამისობაში ყოფნასთან. თუმცა, საკანონმდებლო ცვლილებების მიუხედავად, კვლავ დგება სწორი კვალიფიკაციის შერჩევის პრობლემა.

აღსანიშნავია, რომ განსახილველი დანაშაულების კვალიფიკაციის პრობლემებზე მეტად მწირი ინფორმაცია მოიპოვება ქართულ ლიტერატურაში. არ არის გაანალიზებული კიბერდანაშაულების გამიჯვნა სხვა ტრადიციული დანაშაულებთან, რაზეც მიანიშნებს საჯარო უწყებებიდან გამოთხოვილი სტატისტიკური მონაცემები.

გამოძიებათა უმეტესობა იწყება საკუთრების წინააღმდეგ მიმართული დანაშაულის მუხლით და კიბერდანაშაული სტატისტიკის მიღმა რჩება.

ნაშრომის მიზანია დოგმატურ-სამართლებრივი, თეორიულ-სამართლებრივი, ფორმალურ-ლოგიკური, სისტემური და შედარებით-სამართლებრივი კვლევის მეთოდების გამოყენებით, შეაფასოს საკვლევ მუხლებზე კვალიფიკაციის პრობლემები, პრაქტიკის გაანალიზებით გამოკვეთოს არსებითი გამოწვევები და, თავის მხრივ, მისი მიზანია განხილული პრობლემების გადაჭრის გზებზე რეკომენდაციების შემოთავაზება. ამ მიზნის მიღწევისთვის, ასევე, აუცილებელია, საკანონმდებლო მოწესრიგებამ ასახოს არსებული რეალობიდან გამომდინარე საჭიროებები. ამ მხრივ, ნაშრომში განხილულია ზოგიერთი საკანონმდებლო ბარიერი, რომლის შეცვლა სასურველია კიბერდანაშაულთა მოწესრიგების კონტექსტში. ნაშრომის მთავარ ღირებულებას წარმოადგენს სწორედ ის გარემოება, რომ ის პირველი მცდელობაა სიღრმისეულად იკვლიოს კიბერდანაშაულთა კვალიფიკაციის პრობლემის სპეციფიკა.

პირველი თავი ეთმობა კიბერდანაშაულის და კიბერ სივრცის კონცეფციის ჩამოყალიბებას, მის რაობას და მასთან დაკავშირებული საჭირო ცნებებს. ნაშრომში გაანალიზებულია კიბერდანაშაულთან, როგორც გლობალურ საფრთხესთან ბრძოლის მნიშვნელობა და ამ პროცესთან დაკავშირებული გამოწვევები. წარმოჩენილია რამდენად პრიორიტეტულია დღეს ინფორმაციული უსაფრთხოება როგორც მსოფლიოსთვის, ასევე საქართველოსთვის. ნაშრომში მიმოხილული იქნება საქართველოში მოკლე ისტორიული ექსკურსი კიბერუსაფრთხოების პრიორიტეტიზაციასთან და დაკვშირებით და მის მიერ გადადგმული ნაბიჯები.

მეორე თავში გაანალიზებულია საერთაშორისო გამოცდილება კიბერდანაშაულთან ბრძოლისას და სახელმწიფოს მიერ კანონმდებლობის ჰარმონიზაციის საკითხები. მიმოხილულია, როგორც საერთაშორისო, ასევე რეგიონალური ინსტრუმენტები. მნიშვნელოვანი ყურადღება ეთმობა მატერიალურ-სამართლებრივ ნაწილს, თუ როგორი კიბერდანაშაულის მოწესრიგების მოდელები არსებობს უცხო ქვეყნებში და როგორ ემიჯნება ტრადიციული დანაშაულები მათთან ახლოს მდგომ ფინანსურად მოტივირებულ კიბერდანაშაულებს.

მესამე თავში ეთმობა ქმედების შემადგენლობისთვის საჭირო ცნებების განხილვას. კერძოდ, განხილულია ფინანსურად მოტივირებული კიბერდანაშაულების სახეები, მათი განხორციელების ხერხები, პრაქტიკული მაგალითების საფუძველზე. გამოკვეთილია მათი ურთიერთგამიჯვნის პრობლემა ე.წ. „ტრადიციულ“ დანაშაულებთან, რომლებიც ჩადენილია უახლესი ტექნოლოგიების გამოყენებით. ამ თავის ფარგლებში იქნება განხილული მუხლები, რომლებიც ახლოს დგანან ერთმანეთთან ქმედების შემადგენლობით და გამოყოფილი იქნება ძირითადი გამიჯვნის კრიტერიუმები.

ნაშრომში ყურადღება გამახვილებულია პრაქტიკულ გამოწვევებზე და მოსამართლეთა მიდგომებზე. მატერიალურ-სამართლებრივი ცოდნის გარეშე, რაც

დაკავშირებულია ქმედების შემადგენლობის გააზრებასთან, შეუძლებელია სწორი კვალიფიკაციისა და რელევანტური საგამოძიებო ქმედებათა დაგეგმვა. კვალიფიკაციისთვის მიმოხილული იქნება უცხოური პრეცედენტული სამართლით დადგენილი მიდგომები. ვინაიდან ამ მხრივ გარკვეული სადავო პოზიციები არსებობს როგორც ლიტერატურაში, ისე - სასამართლო პრაქტიკაში, აღნიშნული ნაშრომი სწორედ მათ ეთმობა. ნაშრომის კულმინაციურ ნაწილში განხილულია ძირითადი მიგნებები და საჭირო რეკომენდაციები დანაშაულთა კვალიფიკაციისათვის.

თავი I. კიბერდანაშაული, როგორც საზოგადოებრივი საფრთხე

1.1 კიბერდანაშაული, როგორც გლობალური გამოწვევა

დანაშაულის ერთ-ერთი მთავარი მახასიათებელი არის მისი ისტორიული ცვალებადობა, რაც ყველაზე მკაფიოდ გამოვლინდა ტექნოლოგიური რევოლუციის შედეგად, საიდანაც კიბერდანაშაული ყველაზე მეტად გამოირჩევა სწრაფი განვითარებით და ყოველწლიურად მზარდი საზოგადოებრივი საშიშროებით.

კიბერდანაშაულის იქცა ინფორმაციული საზოგადოების ეპოქაში უმწვავეს პრობლემად, როდესაც კომპიუტერი და ტელესაკომუნიკაციო სისტემებმა მოიცვა ცხოვრების ყველა სფერო და ადაპტირდა საზოგადოების საჭიროებებზე.[1] მზარდი დამოკიდებულება ინტერნეტ კომუნიკაციურ ტექნოლოგიებზე მისი სერვისების მომხმარებლებს უფრო მოწყვლადს ხდის.[2]

ტექნოლოგიური განვითარების კვალდაკვალ, კიბერსფეროში შეიქმნა დანაშაულებრივი გარემო, რომელშიც ვხდებით ახალ-ახალ სახეებს და ესენია ჰაკერები,[3] ქარდერები,[4] და ფიშერები.[5] ტექნოლოგიურმა განვითარებამ გამოიწვია კიბერდამნაშავის გამოვლენასა და გამოძიებასთან დაკავშირებული სირთულეები, რის გამოც ეს სფერო მეტად მიზიდული გახდა ბოროტმოქმედებებისთვის.

პირველი მიმზიდველი ფაქტორი დამნაშავეთათვის არის ინფორმაციის მარტივი ხელმისაწვდომობა. ახალი ინფორმაციის მოძიება უმოკლეს ვადაში შესაძლებელია იმ საძიებო სისტემების დახმარებით, რომლებიც ინტერნეტ-მომხმარებლებს საშუალებას აძლევს მოძებნონ მილიონობით ვებ-გვერდები წამებში.[6] ეს ტექნოლოგია შეიძლება

---

[1] ISTAG's Report on Revising Europe's ICT Strategy, 2009, 4

[2] *Lucky L. and Eisenberg J.,* Renewing U.S. Telecommunications Research, Washington, DC: The National Academies Press, 2006, ხელმისაწვდომია ბმულზე: https://doi.org/10.17226/11711 [18.04.2022].

[3] *Granger,* Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, ხელმისაწვდომია: www.securityfocus.com/infocus/1527 [18.04.2022].

[4] *Kigerl A.,* Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories, Social Science Computer Review, 20(10), 2017, 1-19.

[5] *Gecko*, The criminalization of Phishing and Identity Theft, Computer und Resht, 2005, 606.

[6] *Gercke M.,* Understanding cybercrime: Phenomena, challenges and legal response, International Telecommunication Union, 2012, 76-77.

გამოყენებულ იქნას როგორც ლეგიტიმური, ასევე კრიმინალური მიზნებისთვის.[7] მავნე პროგრამები, მათი მოხმარების ინსტრუქციები მარტივად ხელმისაწვდომია ღია წყაროებში. გარდა ამისა, სოციალური ინჟინერიის მეთოდის გამოყენებით, ბოროტმოქმედებს შეუძლიათ ინტერნეტსივრცეში არსებული ინფორმაცია მოიძიონ პოტენციური მსხვერპლის შესახებ.[8]

კიბერდანაშაულის მეორე დამახასიათებელი ნიშანი, რომელიც დიდ პრობლემას უქმნის საგამოძიებო ორგანოებს, ეს არის დანაშაულის ლატენტური ხასიათი.[9] კომპიუტერული ქსელები გვთავაზობენ როგორც ანონიმურობის უზრუნველმყოფელ ინსტრუმენტებს,[10] მონაცემების დაშიფვრის მეთოდებს, ასევე პლატფორმებს, როგორიცაა მაგალითად "Dark Web".[11]

მესამე, დანაშაულის ჩადენის ტრანსსასაზღვრო უპირატესობები: გეოგრაფიული შეუზღუდაობის გათვალისწინებით, ხშირად დამრღვევი პოლიციის ფაქტობრივი იურისდიქციის მიღმა რჩება, დისტანციური მეთოდი დანაშაულის ჩადენას კიდევ უფრო მიმზიდველს ხდის, აქ არაა აუცილებელი უშუალო კონტაქტი დანაშაულის სამიზნესთან.[12]

მეოთხე, ძირითად შემთხვევაში, ბოროტმოქმედები უფრო მაღალ ინტელექტუალურ მომზადებას საჭიროებენ,[13] რადგან კიბერდანაშაულის ჩადენისათვის საჭიროა გარკვეული სოფისტიკური ცოდნის ფლობა. ისინი რაციონალური, ტექნოლოგიურად განსწავლული პირები არიან.

მეხუთე, დანაშაული შეიძლება ავტომატიზებულ რეჟიმში ჩაიდინონ, რაც გულისხმობს, რომ შეიძლება რამდენიმე ადგილას ჩადენილ იქნას ერთდროულად, რამდენიმე მიზანი ჰქონდეს. ავტომატიზაციას აქვს მნიშვნელოვანი უპირატესობები, ის

---

[7] Nogguchi, Search engines lift cover of privacy, The Washington Post, 2004, ხელმისაწვდომია: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/ [18.04.2022].

[8] იქვე. ასევე იხ.: Mitnick K, Simon W., The Art of Deception: Controlling the Human Element of Security, Chapter 4 "Building Trust", 2002.

[9] *Трофимова Д. Н.*, Базавлуцкая С. В., Киберпреступность, жур. Молодой ученый, 2020, № 15 (30), 259-261.

[10] მაგალითად, "Tor" (The Onion Router) - უზრუნველყოფს მომხმარებლის კონფიდენციალურობას იდენტობის ანონიმიზაციის გზით და მისი მომხრეები აცხადებენ, რომ "Tor" არის საუკეთესო გამოვალი რომელიც ეხმარება ჟურნალისტებს წყაროს საიდუმლოს დაცვაში, სიტყვის თავისუფლების ხელშეწყობაში, პირად კომუნიკაციებში შეჭრის თავიდან აცილებაში. იხ.: *Yetter, R. B.*, Darknets, cybercrime & the onion router: Anonymity & security in cyberspace, 2015, 1.

[11] იხ. მეტი ანონიმურობის მეთოდებზე: *Yetter, R. B.*, Darknets, cybercrime & the onion router: Anonymity & security in cyberspace, 2015.

[12] ამ მხრივ, აქტუალურია სამართლებრივი ურთიერთდახმარების მექანიზმის უზრუნველყოფა ქვეყნებს შორის, რადგან კიბერდანაშაული ტრადიციულ საზღვრებს სცილდება. ამ მიმართულებით მნიშვნელოვანია G7 და ევროპის საბჭოს მიერ გათვალისწინებული 24/7-ზე მომუშავე პუნქტები.

[13] *Nomokonov V.A., Tropina T.L.,* Cybercrime as a New Criminal Threat, Journ. Criminology: Yesterday, Today, Tomorrow, №24, 2012 45-55.

ზრდის სიჩქარეს, ვრცელდება უფრო ფართო მასშტაბებზე და საჭიროებს ნაკლებ პირთა ჩართულობას.[14]

დაბოლოს, მსხვერპლის ცნობიერების დონე: შესაძლოა, მსხვერპლმა გარკვეული პერიოდის განმავლობაში არც იცოდეს განხორციელებული დანაშაულის შესახებ, რაც გამოძიებისთვის მნიშვნელოვანი პრობლემაა;

კიბერდამნაშავეები, ხშირ შემთხვევაში, ორგანიზებულად საქმიანობენ. მსოფლიოს გამოცდილება ცხადყოფს, რომ კრიმინალური თანამშრომლობა ორგანიზებულ დამნაშავეთა ჯგუფებსა და კიბერდამნაშავეებს შორის სულ უფრო ხშირდება. ასევე, მსოფლიო გამოცდილებაში მრავლად არის მაგალითები, როდესაც ტერორისტული დაჯგუფებები კიბერდამნაშავეთაგან სხვადასხვა ინფორმაციას ყიდულობენ და მათი გამოყენებით, სუვერენულ სახელმწიფოებს საფრთხეს უქმნიან. [15]

კიბერდანაშაულის საზოგადოებრივმა საშიროებამ გაანპირობა მასთან ბრძოლის საჭიროება და წარსული გამოცდილების საფუძველზე საერთაშორისო თუ რეგიონალურ დონეზე შემუშავდა მასთან ბრძოლის მექანიზმები.

1.2. კიბერდანაშაულის განვითარების ისტორია

ინფორმაციული ტექნოლოგიების გამოყენების გავლენა სულ უფრო და უფრო იზრდება, ტექნოლოგიები ადამიანის საქმიანობის ყველა სფეროს შეეხო: როგორც გლობალური უსაფრთოხების უზრუნველყოფას, ასევე ყოველდღიურ ცხოვრების რუტინაში გამოყენება.

ინფორმაცია, როგორც ამ პროცესის ერთ-ერთი უმთავრესი ელემენტი, სულ უფრო მნიშვნელოვან როლს თამაშობს როგორც ინდივიდის, ისე მთელი საზოგადოებისა და თითოეული სახელმწიფოს ცხოვრებაში. ამ მხრივ, ინფორმაციული უსაფრთხოება სახელმწიფო უშიშროების ერთ-ერთი მთავარი კომპონენტია.[16]

გარდა დადებითი ეფექტისა, სამეცნიერო და ტექნოლოგიურმა პროგრესმა გამოიწვია ახალი ტიპის დანაშაულთა გაჩენა, იქნება ეს კომპიუტერულ სისტემის მუშაობაში უკანონო ჩარევა ან შეფერხება, მონაცემთა ქურდობა, კომპიუტერული თაღლითობა თუ გაყალბება. ასეთ ანტისოციალურ მოვლენას მოგვიანებით მიენიჭა ახალი დანაშაულის სახელი - კიბერდანაშაული. კიბერდანაშაული ამჟამად განიხილება,

[14] იქვე. ასევე, იხ.: *Gercke M.,* Understanding cybercrime: Phenomena, challenges and legal response, International Telecommunication Union, 2012, 76-77.

[15] *Sieber,* The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, 212;

[16] ინდუსტრიული საზოგადოებისგან განსხვავებით, ინფორმაციული საზოგადოების წევრები აღარ არიან დაკავშირებული ინდუსტრიალიზაციაში მათი მონაწილეობით, არამედ ინტერნეტ საკომუნიკაციო ტექნოლოგიების ხელმისაწვდომობით და მათი გამოყენებით. იხ. მეტი ინფორმაციული საზოგადოების შესახებ: *Masuda*, The Information Society as Post-Industrial Society;

როგორც სწრაფად მზარდი საფრთხე, როგორც ცალკეული სახელმწიფოებისთვის, ასევე მთლიანად მსოფლიო საზოგადოებისთვის.[17]

კიბერდანაშაულის კონცეფციის განვითარებასა და მასთან ბრძოლის მექანიზმების ჩამოყალიბებას თავისი ისტორიული წინაპირობები აქვს. ჯერ კიდევ 1960-70-იან წლებში, უფრო ხშირი იყო კომპიუტერული დანაშაულების ტრადიციული, ფიზიკური ხელყოფის ფორმა,[18] თუმცა ნელ-ნელა ფეხს იდგამდა ახალი დანაშაულის ფორმები, რომლებიც აღიარებას იმსახურებდა, როგორებიცაა კომპიუტერული სისტემის უკანონო მოხმარება და ელექტრონული მონაცემების მანიპულირება.[19]

კომპიუტერულ დანაშაულთა გავრცელება იწყება 1990-იანი წლებიდან. იგი ორმა მასშტაბურმა ცვლილებამ განაპირობა: პირველი, ეს იყო კომპიუტერების ხელმისაწვდომობა. გორდონ მურის კანონის მსგავსად, კომპიუტერების ალგორითმები სწრაფად უმჯობესდება, რის გამოც კომპიუტერები უფრო ეფექტური და იაფი ხდება დროთა განმავლობაში.[20] 1990-იანი წლების დასაწყისში კომპიუტერების ფასმა დაიწყო სწრაფი კლება, ხოლო 1990-იანი წლების შუა პერიოდისთვის მიაღწია ისეთ წერტილს, როდესაც პერსონალური კომპიუტერები ბაზარზე მასობრივად გახდა ხელმისაწვდომი.

მეორე მნიშვნელოვანი ცვლილება იყო ქსელური ტექნოლოგიების სწრაფი განვითარება და დაკავშირების სიმარტივე, რამაც საფუძველი შეუქმნა ინტერნეტის ფართო კომერციალიზაციას.[21] ამ ცვლილებებმა გააერთიანა ადამიანები ერთიანდებიან კიბერსივრცეში, სოციალური და კომერციული ინტერაქციისთვის, თუმცა, ამავდროულად, გახადა ისინი მოწყვლადები ბოროტმოქმედებების ხელში, რომლებმაც ხელიდან არ გაუშვეს ახალი შესაძლებლობა.

ინტერნეტტექნოლოგიების პოპულარობამ და მის მომხმარებელთა ზრდამ კრიმინალებისთვის პოტენციური სამიზნეების რაოდენობაც გაზარდა. თავდაპირველ სამიზნეებს წარმოადგენენ კრიტიკული ინფრასტრუქტურის სუბიექტები: კრიმინალური აქტივობა მიზნად ისახავდა სახელმწიფო დაწესებულებებზე, საბანკო სექტორზე თავდასხმებს, თუმცა, შემდგომ, როდესაც ის მასობრივად გახდა ხელმისაწვდომი ფართო საზოგადოებისთვის ან სხვადასხვა ბიზნეს სექტორში, მისი გავრცელების არეალი ყველა სფეროს შეეხო.[22]

ინფორმაციის მარტივად ხელმისაწვდომობამ, ასევე, მისმა სწრაფმა გავრცელებამ სხვადასხვა სახის დანაშაულების გამოვლენას შეუწყო ხელი.[23] ქსელში ანონიმურად

---

[17] *Andrews*, The Legal Challenge Posed by the new Technology, Jurismetrics Journal, 1983, 43.

[18] *Gercke M.,* Understanding cybercrime: Phenomena, challenges and legal response, International Telecommunication Union, 2012, 12-13.

[19] იქვე.

[20] https://www.investopedia.com/terms/m/mooreslaw.asp [06.05.2020]

[21] *Decker*, *Ch.,* Cyber crime: an Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, 3

[22] *Schjolberg,* Computers and Penal Legislation, A study of the legal politics and a new technology, 1983, 6

[23] *Decker*, *Ch.,* Cyber crime: an Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, 3.

დარჩენის გარანტია, ინფორმაციის სწრაფი მიმოცვლა-განადგურება და დანაშაულთა ჩადენის სიმარტივე საზღვრების მიუხედავად, კიბერ მეთოდებით დანაშაულთა ჩადენა ბოროტმოქმედებებისთვის კიდევ უფრო მომხიბვლელი აღმოჩნდა და ტექნოლოგიურმა პროგრესმა განაპირობა სხვადასხვა სპეციფიკური დანაშაულთა სახის პროგრესი. დღის წესრიგში დადგა კრიმინალური სივრცესთან შესაბამისი და ადეკვატური კანონმდებლობის შექმნა და აღნიშნულ პროცესში ჩაერთნენ საერთაშორისო ორგანიზაციები.[24]

1990 წელს გაერთიანებული ერების ორგანიზაციამ მიიღო რეზოლუცია № 45/121 და 1994 წელს გამოსცა სახელმძღვანელო „კომპიუტერული დანაშაულის პრევენციისა და კონტროლის სახელმძღვანელო პრინციპები“, სადაც პირველად ჩამოაყალიბა კიბერდანაშაული და კომპიუტერული დანაშაულის ცნებები, რომლებიც შემდგომ თავში იქნება განხილული. [25]

1.3. კიბერდანაშაულის ცნება და ზოგადი დახასიათება

კანონმდებლობა კიბერდანაშაულის გამოძიებისა და სისხლსამართლებრივი დევნის საფუძველია. თუმცა, კანონმდებელი მუდმივად უნდა პასუხობდეს თანამედროვე გამოწვევებს და არ ჩამორჩეს მათ, განსაკუთრებით ტექნოლოგიური განვითარების სიჩქარის გათვალისწინებით. ისტორიულად, როგორც უკვე აღენიშნა, კომპიუტერთან დაკავშირებული სერვისების ან ინტერნეტთან დაკავშირებული ტექნოლოგიების დანერგვამ გამოიწვია დანაშაულთა ახალი ფორმების გამოვლენა, რაც პირველად აქტუალური გახდა 1970-იან წლებში აშშ-ში, როდესაც მოხდა პირველი უნებართვო წვდომა კომპიუტერულ ქსელებზე. ამ გამოწვევების საპასუხოდ, 1977 წელს აშშ-ში პირველად შემუშავდა კანონპროექტი „ფედერალური კომპიუტერული სისტემების დაცვის შესახებ“, რომელიც გარკვეულ დანაშაულებს განსაზღვრავდა, ხოლო 1984 წელს მიიღეს „კომპიუტერული თაღლითობის და კომპიუტერის ბოროტად გამოყენების შესახებ“ კანონი.[26] აშშ-ს პირველი რეგულაციის ჩამოსაყალიბებლად დაეხმარა პრაქტიკული გამოცდილება და შემთხვევათა იდენტიფიცირება.

აღსანიშნავია, რომ, გლობალური პრობლემიდან გამომდინარე, აღნიშნულზე ზრუნვა დაიწყეს ჯერ კიდევ 80-იან წლებში. მაგალითად, პირველი საერთაშორისო დეფინიცია „კიბერდანაშაულისა“ 1986 წელს შემოგვთავაზა ევროპის ეკონომიკური ხელშეწყობის და განვითარების ორგანიზაციამ“ (OECD), რომელმაც განსაზღვრა

[24] მაგალითად, ეკონომიკური ხელშეწყობის და განვითარების ორგანიზაციის და ევროპის საბჭოს მიერ იმ დროისთვის ჩამოყალიბდა მკვლევართა ჯგუფი, რომლებსაც უნდა შეეფასებინათ არსებული სიტუაცია და შესაძლებლობების განსაზღვრა.

[25] *UN General Assembly*, Crime prevention and criminal justice. Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, resolution, adopted at the 68th plenary meeting, 14 Dec. 1990.

[26] *ზაქარაშვილი უჩ.,* კიბერდანაშაულის სისხლსამართლებრივი რეგულირების პრობლემების საქართველოში, თბ., 2014, 15

კომპიუტერული დანაშაული, როგორც „ნებისმიერი უკანონო, არაეთიკური ან არაავტორიზებული ქცევა მონაცემთა ავტომატიზებულ დამუშავებასა და გადაცემასთან დაკავშირებით.“[27] ის 1983 წლიდან სწავლობს კიბერდანაშაულებს და ამზადებს შესაბამის რეკომენდაციებს. ასევე, მნიშვნელოვანია, რომ 1993 წელს ინტერპოლმა ჩაატარა სემინარი „კრიმინალისტიკა და კომპიუტერული დანაშაული. სემინარის ფარგლებში განისაზღვრა კომპიუტერული დანაშაულის ცნება, რომელიც ჩამოყალიბდა შემდეგნაირად: „სისხლის სამართლით გათვალისწინებული საზოგადოებრივად საშიში ქმედება, რომელშიც მანქანური ინფორმაცია წარმოადგენს დანაშაულებრივი ხელყოფის საშუალებას ან ობიექტს“.[28] კიბერდანაშაულის ცნების და სახეების ზოგადი განსაზღვრა სცადა ევროპის საბჭომ საკუთარ კონვენციაში, სადაც განსაზღვრა, რომ კიბერდანაშაულის წინააღმდეგ ევროპული კონვენციის თანახმად, კიბერდანაშაული არის კომპიუტერული სისტემების, ქსელების და მონაცემების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის, აგრეთვე ამ სისტემების, ქსელებისა და მონაცემების ბოროტად გამოყენება. ტერმინი აღნიშნავს დანაშაულებს, რომლებიც ჩადენილია ინტერნეტის ან სხვა კომპიუტერული ქსელის გამოყენებით, როგორც დანაშაულის კომპონენტი.

საინტერესოა, რა სახის კიბერდანაშაულები არსებობს და რა საერთო დამახასიათებელი ნიშნები აქვთ. იურიდულ ლიტერატურაში გამოთქმულია მოსაზრება, რომ მათი დაყოფა დამოკიდებულია დანაშაულის ხელყოფის ობიექტსა და საგანზე, დანაშაულის ჩადენის ხერხსა და მეთოდებზე.

აშშ-ის იუსტიციის დეპარტამენტი ფართოდ განსაზღვრავს კომპიუტერულ დანაშაულს და მიიჩნევს, როგორც „სისხლის სამართლის კანონის ნებისმიერ დარღვევას, რომელიც გულისხმობს კომპიუტერული ტექნოლოგიების ცოდნას მათი ჩადენის, გამოძიების ან დევნისთვის“.[29] იუსტიციის დეპარტამენტი (DOJ) კომპიუტერთან დაკავშირებულ დანაშაულებებს სამ კატეგორიად ყოფს, სადაც კომპიუტერი და ქსელი შეიძლება იყოს დანაშაულის სამიზნე. მაგალითად, პროგრამული უზრუნველყოფის შეფერხება - ეს კატეგორია მოიცავს ყველა დანაშაულს, რომელიც წარმოიშვა ბოლო რამდენიმე ათწლეულის ტექნოლოგიური აფეთქების შედეგად, მათ შორის ხშირად

[27] *Aldrich, R.W.,* Cyberterrorism and computer crimes: issues surrounding the establishmentof an international legal regime, 2000, 10.

[28] *ა. კაცმანი,* „კომპიუტერული დანაშაულის სისხლსამართლებრივი და კრიმინალისტიკური დახასიათება“, ჟურნ. „სამართალი“, 2000, № 2, 58.

[29] *Ditizion, R., Geddes, R., Rhodes, M.,* Computer Crimes, American Criminal Law Review, 2003, L. Rev. 285, ასევე *Adams, M.,* Comment, Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet.

ურთიერთდაკავშირებული "ვირუსების"[30], "ჭიების"[31], "ტროას ცხენების",[32] ლოგიკური ბომბების"[33], "სნაიფერების"[34] გამოყენება და "სერვისზე უარის თქმის“ (ე.წ. DDoS) თავდასხმები.[35] მეორე კომპიუტერი შეილება იყოს დანაშაულის ჩადენის "ინსტრუმენტი", რომელიც გამოიყენება ტრადიციული დანაშაულის ჩადენისთვის. ეს ტრადიციული დანაშაულები მოიცავს პირადობის ქურდობას,[36] ბავშვთა პორნოგრაფიას,[37] საავტორო უფლებების დარღვევას.[38] მესამე, კომპიუტერი შეიძლება იყოს ადგილი, სადაც ინახება მტკიცებულებები.[39]

---

[30] ვირუსი (Virus) არის პროგრამა, რომელიც ცვლის სხვა კომპიუტერულ პროგრამებს და აიძულებს მათ შეასრულონ დავალება, რისთვისაც შეიქმნა ვირუსი. ის ჩვეულებრივ ვრცელდება ერთი ჰოსტიდან მეორეზე, როდესაც მომხმარებელი გადასცემს ინფიცირებულ ფაილს ელექტრონული ფოსტით, ინტერნეტით, კომპანიის ქსელში ან დისკზე. იხ. თუ რა ზეგავლენა იქონია გლობალურმა ვირუსმა „მელისამ“ ინტერნეტ სივრცეში ელ. ბმულზე: https://www.insidehook.com/article/history/melissa-virus-changed-internet [07.05.2022].

[31] ჭიები (Worms) ვირუსების მსგავსია, მაგრამ, მაშინ როცა ვირუსები საჭიროებენ ადამიანის მოქმედებას ერთი კომპიუტერიდან მეორეზე გავრცელებისთვის, ჭიები იყენებენ კომპიუტერულ ქსელებს ან ინტერნეტს თვითგანმეორებისთვის და სხვა მომხმარებლებისთვის „გაგზავნას“, ძირითადად, ელექტრონული ფოსტით. ჭიებს გაცილებით მეტი დესტრუქციული პოტენციალი აქვთ, ვიდრე ვირუსებს, მაგ. „ILoveYou“ ჭია ცხრაჯერ უფრო სწრაფად გავრცელდა, ვიდრე მელისას ვირუსი მისი თვითგამრავლების უნარის შედეგად. იხ. განმარტება ელ. ბმულზე: https://cybercrime.org.za/worm/#:~:text=A%20computer%20worm%20is%20a,features%20found%20on%20many%20computers [07.05.2022].

[32] ტროას ცხენები (Trojan Horses) არის პროგრამები, რომლებიც ერთი შეხედვით ლეგიტიმური ფუნქციები აქვთ, მაგრამ ასევე შეიცავს დამალულ მავნე კოდს. ტროას ცხენი ატყუებს მომხმარებელს, რათა მან დააინსტალიროს, ერთი შეხედვით, უდანაშაულო პროგრამა მის კომპიუტერულ სისტემაზე, შემდეგ ააქტიურებს ფარულ კოდს, რომელმაც შესაძლოა გაათავისუფლოს ვირუსი ან დაუშვას მომხმარებელთან არაავტორიზებული წვდომა.

[33] ლოგიკური ბომბები არის პროგრამები, რომელთა გასააქტიურებლად საჭიროა კონკრეტული მოვლენის, კონკრეტული თარიღის ან დროის მოსვლა. ისინი შეიძლება გამოყენებული იყოს არალეგიტიმური მიზნებისთვის, მაგრამ ასევე ხშირად გამოიყენება პროგრამულ უზრუნველყოფაზე მომუშავე კომპანიების მიერ სალიცენზიო ხელშეკრულებების დარღვევისგან დასაცავად, პროგრამის გამორთვით დარღვევის აღმოჩენისთანავე. ამ მხრივ საინტერესო პრეცენდენტი იყო განხილული ნაშრომში იხ.: M. Hatcher, J. McDannell, S. Ostfeld, Computer Crimes, Amrican Criminal Law Review, 1999, Rev. 397.

[34] სნაიფერები (Sniffers), ასევე ცნობილი როგორც ქსელის ანალიზატორები, გამოიყენება ქსელების მონიტორინგისა და ქსელის კავშირების პრობლემების მოსაგვარებლად. თუმცა პირს შეუძლია შეაღწიოს ქსელში და დააინსტალიროს სნაიფერი, რომელიც აღრიცხავს მთელ აქტივობას ქსელში, პაროლებს, საკრედიტო ბარათის მონაცემებს და სხვა პირადი ინფორმაციას. იხ.: Rutrell Y., Sniffers Overhauled For E-Biz, 2000, 1.

[35] ITU Toolkit for Cybercrime legislation, American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law, 2010, 31, იხ. ელ. ბმული: https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/itu-toolkit-for-cybercrime-legislation-%28draft%29.pdf [07.05.2022]

[36] United States v. Petersen, 157 U.S. App. D.C. 219, 483 F.2d 1222 (1973) (საქმე შეეხებოდა პირს, რომელმაც გატეხა საკრედიტო ანგარიშგების სერვისი ფინანსური ინფორმაციის მისაღებად, რომელიც გამოიყენა სხვა პირების სახელი თაღლითური საკრედიტო ბარათების შესაკეთად).

[37] United States v. Brown, 381 U.S. 437 (1965)

[38] Unites States v. Michael D. Pirello (2001), საქმეში ბრალდებულმა განათავსა ფულის თაღლითური რეკლამის ვებ-საიტზე

[39] *Goodman M.*, Why the Police Don't Care About Computer Crime, 10 HARV. J. LAW & TEC., 1997, 465, 468-69.

დეფინიციის დაზუსტების მიზნით საჭიროა განვსაზღვროთ, რა ნიშნებით ხასიათდება კიბერდანაშაული. ესენია ანონიმურობა, ტრანსსასაზღვრო ხასიათი, დისტანციურობა, კომპიუტერის, ვირუსების, მავნე პროგრამების, საინფორმაციო კომუნიკაციური ქსელის გამოყენება.[40] თუმცა ეს არ ნიშნავს, რომ ყველა შემთხვევაში კიბერდანაშაული ამ ნიშნის მატარებელია, მაგალითად, ტრანსსასაზღვრო არ გულისხმობს, რომ ყოველთვის სხვადასხვა ქვეყნებიდან არიან მსხვერპლი და ბოროტმოქმედი. ანონიმურობას რაც შეეხება, არ ნიშნავს, რომ ყოველთვის უცნობია დანაშაულის ჩამდენის ვინაობა, (მაგ.: კიბერბულინგი). ეს არის დანაშაულის ფაკულტატიური ელემენტები და ყოველთვის არ ერთვის კიბერდანაშაულს. რაც შეეხება დისტანციურობას, ის უფრო ჰგავს აუცილებელ ნიშანს, იმიტომ რომ აქ დამნაშავე იყენებს ამ პრივილიგირებულ შესაძლებლობებს, რომლებსაც კიბერსივრცე[41] მას ანიჭებს, რათა მასა და პოტენციურ დაზარალებულს შორის არსებობდეს უსაფრთხო დისტანცია.[42] აქედან გამომდინარე, კიბერდანაშაული - ეს არის დანაშაული, ჩადენილი კიბერსივრცეში.

აუცილებელი ნიშნების დახასიათებისას უნდა ითქვას, რომ ფაკულტატიური ნიშნების გარდა, კიბერდანაშაულებს აერთიანებს დანაშაულის ჩადენის საშუალება (ინფორმაციულ საკომუნიკაციო საშუალებები, კომპიუტერული ტექნიკა და ქსელები და ა.შ.) და კიბერსივრცე.[43]

კიბერდანაშაულის შესახებ მოხსენებების გაიდლაინების ან პუბლიკაციების უმეტესობა იწყება „კომპიუტერული დანაშაულის“ და „კიბერდანაშაულის“ განმარტებით. ამ კონტექსტში, ბოლო ათწლეულების განმავლობაში განსხვავებული მიდგომები შემუშავდა ორივე ტერმინის ზუსტი განმარტების ჩამოსაყალიბებლად. მიდგომების განხილვისა და შეფასებისთვის საჭიროა „კიბერდანაშაულსა“ და „კომპიუტერულ დანაშაულს“ შორის კავშირის დადგენა.

ტერმინ „კიბერდანაშაულს“ ხშირად იყენებენ ტერმინ „კომპიუტერულ დანაშაულთან“ ან ერთმანეთის სინონიმებად. ტერმინი „კიბერდანაშაული“ უფრო ვიწროა, ვიდრე კომპიუტერთან დაკავშირებული დანაშაულები, რადგან ის უნდა მოიცავდეს კომპიუტერულ ქსელს. კომპიუტერული დანაშაული გულისხმობს იმ დანაშაულებსაც კი, რომლებიც არ არის დაკავშირებული ქსელთან, მაგრამ გავლენის მქონეა მხოლოდ ცალკეულ კომპიუტერულ სისტემებზე. გამოდის, რომ კომპიუტერული

---

[40] *Простосердов М.А.*, Экономические преступления, совершаемые в киберпространстве, и меры противодействия, Дис., 2016,, გვ. 28-30

[41] კიბერსივრცე, იგივე ვირტუალური სივრცე, ეს არის კომპიუტერული მონაცემების მოდელირებით შექმნილი სივრცე, სადაც ინახება ინფორმაცია პირებზე, ნივთებზე, მოვლენებზე, ფაქტების შესახებ მათემატიკური, სიმბოლური თუ სხვა ფორმით, რომელიც ინახება ქსელში ან მოწყობილობის მეხსიერებაში, ან მეხსიერების მატარებელში.

[42] *Простосердов М.А.*, Экономические преступления, совершаемые в киберпространстве, и меры противодействия, Дис., 2016,, გვ. 28-30

[43] იქვე.

დანაშაულების ჩადენა შესაძლებელია არა მარტო კიბერსივრცეში, არამედ მატერიალურ სამყაროშიც.

რატომ არის მნიშვნელოვანი დანაშაული კვალიფიკაციისთვის, რომ განისაზღვროს, ზუსტად რას გულისხმობს კიბერდანაშაული? მაგალითად, თუ მოცემულია კომპიუტერული დანაშაული, მაშინ ის ფარავს, ასევე კიბერმეთოდებით ჩადენილ დანაშაულსაც, როგორიცაა მუქარა, თაღლითობა, ჩადენილი ტექნიკური საშუალების გამოყენებით, ძალადობისკენ საჯაროდ მოწოდება და ა.შ. მაშინ, როდესაც კომპიუტერულ საინფორმაციო-ტექნოლოგიურ სფეროში ჩადენილი დანაშაულები მოიცავს უფრო ვიწრო დანაშაულთა სახეებს, როგორებიცაა კომპიუტერული ინფორმაციის არამიზნობრივად (ბოროტად) გამოყენება, მავნე პროგრამების შექმნა, გამოყენება, გავრცელება ან ხელმისაწვდომობისთვის სხვაგვარად უზრუნველყოფა, კომპიუტერული სისტემის არასათანადო არამიზნობრივი ექსპლუატაცია და ა.შ.[44]

ზემოთ განხილული ორი ცნება განიმარტა გაეროს X კონგრესზე, „დანაშაულის პრევენციისა და დამნაშავეთა მოპყრობის შესახებ“ სემინარის ფარგლებში, სადაც კიბერდანაშაულის ცნება განიხილებოდა ორი ასპექტის თვალსაზრისით:

1. კიბერდანაშაული ვიწრო გაგებით (კომპიუტერული დანაშაული): ელექტრონული ოპერაციების გზით ჩადენილი ნებისმიერი უკანონო ქმედება, რომლის მიზანია კომპიუტერული სისტემებისა და მათ მიერ დამუშავებული მონაცემების უსაფრთხოება.

2. კიბერდანაშაული ფართო გაგებით (როგორც კომპიუტერთან დაკავშირებული დანაშაული): ნებისმიერი უკანონო ქმედება, ჩადენილი კომპიუტერების, კომპიუტერული სისტემების ან ქსელების მეშვეობით, ან დაკავშირებული მათთან, მათ შორის ინფორმაციის უკანონო ფლობა და შეთავაზება ან გავრცელება კომპიუტერული სისტემების ან ქსელების მეშვეობით. გარდა ამისა, გაეროს X კონგრესზე შემოთავაზებული იქნა კიბერდანაშაულის რამდენიმე კატეგორია. ერთ-ერთი კლასიფიკაცია გულისხმობს დაყოფას ძალადობრივ ან სხვაგვარად პოტენციურად სახიფათო[45] და არაძალადობრივ დანაშაულებად.[46]

იურიდიულ ლიტერატურაში, ხელყოფის ობიექტის მიხედვით, გამოყოფენ ფინანსურად მოტივირებულ კიბერდანაშაულებს, პირადი ცხოვრების

[44] მხოლოდ კიბერსივრცეში ჩადენილი დანაშაულებს გააჩნიათ თავისი სპეციფიკა, რადგან საჭიროებენ გარკვეულ სოფისტურ ცოდნას, შესაბამისად, უფრო ხშირად ხასიათდებიან მაღალი საზოგადოებრივი საფრთხის მატარებლად. მაგალითად, ბუდაპეშტის კონვენციის მოთხოვნაა, რომ მოხდეს სპეციფიკური დანაშაულების კრიმინალიზაცია, საფრთხის საშიშროებიდან გამომდინარე, რადგან ბოროტმოქმედს აქვს მეტი უნარები, ცოდნა, რომ ჩაიდინოს დანაშაულები, მაგალითად, ნაშრომის თავში იქნება საუბარი კომპიუტერულ გაყალბებაზე, რაც არ გულისხმობს ნებისმიერი სახის გაყალბებას, აქ იგულისხმება სპეციალური სოფისტური ცოდნის გამოყენებით ჩადენილი გაყალბება.

[45] მაგალითად, ფიზიკური მუქარა, კიბერშევიწროება, ბავშვთა პორნოგრაფია, კიბერტერორიზმი

[46] მაგალითად, კიბერქურდობა, კიბერთაღლითობა, პროსტიტუციის სერვისების რეკლამა ინტერნეტში, ნარკოტიკებით ვაჭრობა ინტერნეტის გამოყენებით, აზარტული თამაშები ინტერნეტში, ფულის გათეთრება ელექტრონული გადარიცხვით, დესტრუქციული კიბერდანაშაული, სხვა კიბერდანაშაული.

ხელშეუხებლობის სფეროს წინააღმდეგ მიმართულ კიბერდანაშაულებსა და კიბერდანაშაულებს საზოგადოებრივი და სახელმწიფო ინტერესების წინააღმდეგ. როგორც უკვე აღინიშნა, კიბერდანაშაულები კომპიუტერულ დანაშაულთა სახეებისაგან დამოუკიდებელ დანაშაულთა სახეს წარმოადგენს. სხვადასხვა სამართლებრივი სიკეთის განსხვავებით. ამ დიდი სფეროს ნაწილი არის ფინანსურად მოტივირებული.

1.4. საქართველოს გამოწვევები კიბერდანაშაულთან ბრძოლისას

კიბერდანაშაულით გამოწვეული მავნე შედეგები საქართველოსთვისაც აქტუალურია. ის წარმოადგენს არა მარტო გლობალურ პრობლემას, არამედ ეროვნული ინტერესის საგანსაც. კიბერდანაშაული და კიბერუსაფრთხოება - ორივე ერთმანეთთან მჭიდროდ დაკავშირებული პრობლემებია იმდენად, რამდენადაც მათი ცალკე გამოყოფა რთულია, ურთიერთდამაკავშირებელი ქსელის არსებობის პირობებში.

2008 წლის აგვისტოს ომის დროს, რესეთის ფედერაციის მიერ სახმელეთო, საზღვაო თუ საჰაერო შეტევების პარალელურად, ხორციელდებოდა მიზანმიმართული კიბერთავდასხმები.[47] კიბერთავდასხმების სამიზნე იყოროგორც სახელმწიფო უწყებები, ასევე მედია და საბანკო სექტორი, რის შედეგადაც დაზიანდა ქვეყნის კრიტიკული ინფრასტრუქტურა.[48] საქართველოში კიბერდანაშაულთან ბრძოლა ეროვნული უსაფრთხოების პრიორიტეტად მას შემდეგ იქცა, რაც 2008 წელს ჩრდილოელმა მეზობელმა, კერძოდ, რუსეთის ფედერაციამ მასზე კიბერთავდასხმები განახორციელა, არჩეული პროდასავლური კურსის გამო. რუსეთის გამართული ინფორმაციული ომის იარაღი არის კიბერთავდასხმები, რომლებიც მიზნად ისახავენ, შექმნან სამიზნე სახელმწიფოს უძლურობის ილუზია, საზოგადოებაში ხელისუფლების წარმომადგენელთა მიმართ უნდობლობა, ავნონ ფინანსურად და სხვაგვარად,გამოიწვიონ ქვეყნის დესტაბილიზაცია.

წარსულმა გამოცდილებამ დღის წესრიგში დააყენა ეფექტური მექანიზმების არსებობის საჭიროება კიბერუსაფრთხოების უზრუნველსაყოფად და უდიდესი ზეგავლენა იქონია ხელისუფლების ორგანოთა ეროვნული უსაფრთხოების პოლიტიკის გადასინჯვაზე. 2008 წელს მნიშვნელოვანად შეიცვალა ეროვნული უსაფრთხოების ღირებულებები და ხელისუფლების წარმომადგენლებმა აღიარეს, თუ რამდენად მნიშვნელოვანია ქვეყნისთვის ინფორმაციული სივრცის უსაფრთხოება და ელექტრონული ინფორმაციის დაცულობა.[49]

---

[47] საქართველოს ეროვნული უსაფრთხოების კონცეფცია, საქართველოს მთავრობა, 2008.

[48] გოცირიძე, ანდრია, სვანაძე, ვლადიმერ, "კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები," სსიპ კიბერუსაფრთხოების ბიურო, საქართველოს თავდაცვის სამინისტრო, 2015, იხ.: https://dspace.nplg.gov.ge/bitstream/1234/144787/1/Kibertavdacva.pdf [07.05.2022]

[49] იქვე

კიბერუსაფრთხოება და კიბერდანაშაულთან ბრძოლა არც შემდგომ დაკარგა აქტუალობა და 2010-2013 წლებში საქართველოს კიბერუსაფრთხოების სტრატეგია შემუშავდა საქართველოს საფრთხეების შეფასების დოკუმენტისა და საქართველოს ეროვნული უსაფრთხოების კონცეფციის საფუძველზე, ხოლო 2013 წლის 17 მაისს, საქართველოს პრეზიდენტის 321-ე ბრძანებულების საფუძველზე, დამტკიცდა 2013-2015 წლების სტრატეგია და სამოქმედო გეგმა.[50] შემდგომ, 2017 წლის 13 იანვარს, საქართველოს მთავრობის დადგენილებით, დამტკიცდა კიბერუსაფრთხოების 2017-2018 წლების სტრატეგია და სამოქმედო გეგმა,[51] რომელიც ითვალისწინებდა ეფექტური მექანიზმების შემუშავებას,ისეთი პრინციპების საფუძველზე, როგორებიცაა: მთავრობის მიდგომა, მთავრობასა და კერძო სექტორის თანამშრომლობა, კვლევა და ანალიზი, საკანონმდებლო ბაზის შემუშავება, ინსტიტუციურ დონეზე კოორდინაცია, საზოგადოების ცნობიერების ამაღლება, ტრენინგები, გადამზადებები და საგანმანათლებლო ბაზის ჩამოყალიბება და, რაც მთავარია, საერთაშორისო თანამშრომლობა. სტრატეგიის პრინციპები მიმართულია არა მარტო, ზოგადად, კიბერუსაფრთხოების ეფექტურად უზრუნველსაყოფად, არამედ ქვეყნის სოციალურ-ეკონომიკური განვითარებისთვის.[52]

2008-2009 წლებში საქართველოში სრულდებოდა ევროპის საბჭოს და ევროკომისიის ეგიდით ჩატარებული პროექტი - საქართველოს კანონმდებლობის შესაბამისობის უზრუნველყოფა ბუდაპეშტის კონვენციასთან, რომლის შედეგად საქართველომ შეიტანა ცვლილებები სისხლის სამართლის კოდექსში.[53] საკანონმდებლო ცვლილებებთან ერთად, მიმდინარეობდა მოსამართლეების და სამართალდამცავი ორგანოების გადამზადება.

ჯერ კიდევ 2010 წელს განხორციელდა ცვლილებები და ახლებურად ჩამოყალიბდა კონკრეტულ დანაშაულთა დეფინიციები, ცვლილებები შეეხო ბავშვთა პორნოგრაფიას, ასევე, შეიცვალა საგამოძიებო და ოპერატიულ-სამძებრო ღონისძიებების პროცედურების წესები.[54]

2012 წელს 6 ივნისს საქართველოში რატიფიცირდა ევროპის საბჭოს „კიბერდანაშაულის შესახებ“ კონვენცია, რომელმაც საფუძველი ჩაუყარა რიგ საკანონმდებლო ცვლილებებს, ახალი დანაშაულების დეფინიციების ჩამოყალიბებას და დააჩქარა „ინფორმაციული უსაფრთხოების შესახებ კანონის“ მიღება.[55] კანონი 2012 წელს

---

[50] https://mod.gov.ge/uploads/2018/pdf/TAD-ENG.pdf [08.05.2022]

[51] იხ. სტრატეგია შემდეგ ბმულზე: https://www.gov.ge/files/469_59439_212523_14.pdf [08.05.2022]

[52] https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150 [08.05.2022]

[53] *მშვიდობაძე ხ.* საქართველოს კიბერბარომეტრი, საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი, ანგარიში, 2015, 52.

[54] საქართველოს 2010 წლის 24 სექტემბრის კანონი №3619

[55] *მშვიდობაძე ხ.* საქართველოს კიბერბარომეტრი, საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი, ანგარიში, 2015, 52.

შევიდა ძალაში. იგი არეგულირებს სახელმწიფოს კიბერუსაფრთხოების პოლიტიკას, განსაზღვრავს კრიტიკული ინფორმაციული სუბიექტის სიას,[56] ასევე, მათს ვალდებულებებს ინფორმაციული უსაფრთხოების პოლიტიკასთან დაკავშირებით.

საკანონმდებლო ცვლილებების სიახლეებთან ერთად, კიბერუსაფრთხოების ეფექტურად უზრუნველსაყოფად განხორციელდა სტრუქტურული ცვლილებები, კერძოდ, თავდაცვის სამინისტროში შეიქმნა კიბერუსაფრთხოების ბიურო,[57] იუსტიციის სამინისტროში შეიქმნა სსიპ „ციფრული მმართველობის სააგენტო“ (მანამდე - „მონაცემთა გაცვლის სააგენტო“), ხოლო შინაგან საქმეთა სამინისტროში განხორციელდა მნიშვნელოვანი სტრუქტურული რეფორმები. საქართველოს შინაგან საქმეთა სამინისტროში შემავალი ცენტრალური კრიმინალური პოლიციის დეპარტამენტმა შეითავსა 2012 წლიდან კიბერდანაშაულებზე რეაგირება, კერძოდ, პრევენციის განხორციელება, მათს გამოვლენაზე, აღკვეთაზე მუშაობა და მუდმივმოქმედი საკონტაქტო პუნქტის ფუნქციონირების უზრუნველყოფა.

დასაფასებელია სახელმწიფო ბოლო ხანებში გატარებული რეფორმები მოცემული დარგის ექსპერტების მიერ. აქ შეფასების კრიტერიუმებად განსაზღვრული იყო საკანონმდებლო ბაზა, ტექნიკური აღჭურვილობა, ორგანიზაციული სტრუქტურა, თანამშრომლობა და შესაძლებლობების შემდგომი განვითარება აღნიშნული კომპონენტების მიხედვით. გაერო-ს საერთაშორისო სატელეკომუნიკაციო ორგანიზაციის კიბერუსაფრთხოების ინდექსში საქართველო, პირველ ათეულში შედის სხვა ქვეყნებთან შედარებით.[58]

დადებითი ცვლილებების მიუხედავად, კიბერდანაშაული კვლავ პრობლემად რჩება, განსაკუთრებით, გამოძიების ხარისხის და დანაშაულთა კვალიფიკაციის ნაწილში. მაგალითად, 2020 წელს გამოძიება დაიწყო კომპიუტერული სისტემის უნაბერთვო შეღწევის, კერძოდ, 284-ე მუხლით, 2047 საქმეზე, რაც არ შეესაბამება რეალობას, რადგან ხელოვნურ ერთობლიობას ქურდობასთან. მაგალითად, თუ პირი სხვისი ანგარიშიდან თანხას უკანონოდ დაეუფლება, ქმედება საქართველოს სისხლის სამართლის კოდექსის ორი მუხლით - 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 177-ე (ქურდობა) მუხლების ერთობლიობით კვალიფიცირდება.

---

[56] საქართველოს კანონი “ინფორმაციული უსაფრთხოების შესახებ,” 2012 წლის 1 ივლისი, კრიტიკული ინფრასტრუქტურა გულისხმობს სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური და საზოგადოებრივი უსაფრთხოებისთვის. აქვე აღსანიშნავია, რომ აღსანიშნავია, რომ კანონის თანახმად, ინფორმაციული უსაფრთხოების პოლიტიკის შესრულების პასუხისმგებლობა ვრცელდება მხოლოდ იმ იურიდიულ პირებსა და სახელმწიფო ორგანოებზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტებს წარმოადგენენ.

[57] აღნიშნული ბიურო 2014 წლიდან პასუხისმგებელია თავდაცვის სფეროს კრიტიკული სისტემის სუბიექტის უსაფრთხოებასა და კიბერთავდასხმის, კომპიუტერული უსაფრთხოების ინციდენტების განეიტრალებაზე.

[58] “Georgia ranks 9th in Europe for cyber security,” Agenda.ge, April 2, 2019, ასევე, “Global Cybersecurity Index (GCI) 2018,” International Telecomincation Union (ITU).

ინფორმაციული ტექნოლოგიების განვითარებასთან ერთად კვალდაკვალ იზრდებოდა კიბერდანაშაულთა შემთხვევები, ასევე, განვითარებას ხელი შეუწყო დანაშაულთა იერსახის ცვლამ და გამოვლენის ფორმებმა. გამოწვევებზე ადეკვატური რეაგირების უზრუნველსაყოფად საქართველომ განიცადა მნიშვნელოვანი საკანონმდებლო ცვლილებები. ძველი რედაქციით, კომპიუტერის ნაცვლად, ელექტროგამომთვლელი მანქანა (ეგმ) იყო მოხსენებული, ხოლო კიბერდანაშაულთა XXXV თავი კოდექსში ნახსენები იყო, როგორც კომპიუტერული დანაშაული. არსებული დებულებები ვერ პასუხობდნენ თანამედროვე გამოწვევებს და საჭირო დეფინიციებით ვერ ხერხდებოდა მისადაგება.

სსკ-ის ახალჩამოყალიბებული XXXV თავი შედგება ხუთი დანაშაულისაგან, რომელიც შეესაბამება კიბერდანაშაულის იმ თანამედროვე ფორმებს, რომლებიც კიბერდანაშაულის შესახებ ბუდაპეშტის კონვენციაში არის ასახული. მნიშვნელოვანია, რომ ამ ცვლილებებმა სისხლის სამართლის კოდექსისათვის ახალი დეფინიციები შემოიღო, როგორებიცაა: „კომპიუტერული მონაცემი“, „კომპიუტერული სისტემა“ და ტერმინი „უნებართვო“. აღსანიშნავია, რომ სსკ-ის 107-ე მუხლში, 2010 წლის ცვლილებებით, განისაზღვრა **იურიდიული პირის** დასჯადობის საკითხი.

2021 წლის ცვლილებებით, სისხლის სამართლის კოდექსს დაემატა ახალი მუხლი კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა, ჩადენილი ფინანსური სარგებლის მიღების მიზნით წარმოადგენს სსკ-ის 286[1] მუხლი. ცვლილებების მიუხედავად, პრაქტიკაში კვლავ გამოწვევად რჩება კვალიფიკაციასთან დაკავშირებული პრობლემები და პრაქტიკული შემთხვევების იდენტიფიცირება, როგორც საგამოძიებო ორგანოებისთვის, ისე სასამართლო სისტემებისთვის. კვალიფიკაციების პრობლემებსა და სასამართლოს განმარტებებზე დეტალურად ვისაუბრებთ ნაშრომის III თავში.

თავი II. კიბერდანაშაულის საერთაშორისო-სამართლებრივი მოწესრიგება

2.1. კიბერდანაშაულთან ბრძოლა საერთაშორისო აქტებით

ტექნოლოგიურ განვითარებას მოჰყვა პირველი გამოწვევები და ჯერ კიდევ 2003 წლის 12 დეკემბერს ქ. ჟენევაში ჩატარებულმა მსოფლიო სამიტმა „ინფორმაციული საზოგადოების შესახებ“ (WSIS) მიიღო პრინციპები და დეკლარაცია, რომელიც, თავის მხრივ, მიზნად ისახავდა „ინფორმაციული საზოგადოების“ საერთო ხედვის ჩამოყალიბებას. დეკლარაცია ხაზს უსვამს, რომ ინფორმაციულ-საკომუნიკაციო ტექნოლოგიები (ICT) უზარმაზარი გავლენის მქონეა საზოგადოების ცხოვრების თითქმის ყველა ასპექტზე. სწრაფი ტექნოლოგიური პროგრესი ცხოვრების ტრადიციული დაბრკოლებების მოხსნაში დაგვეხმარა, განსაკუთრებით, დროისა და მანძილის კუთხით.

ამასთან ერთად, ICT უნდა განიხილებოდეს როგორც ინსტრუმენტი (მიზნის მიღწევის საშუალება) და არა როგორც თვითმიზანი, ამ სულისკვეთებით 35-37 პრინციპები აყალიბებენ ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების უსაფრთხო გამოყენებას. კიბერუსაფრთხოების, როგორც გლობალური კულტურის მოვლენის, ფარგლებში მნიშვნელოვანია, უზრუნველყოფილი იყოს ინფორმაციული უსაფრთხოება, ქსელის უსაფრთხოება, ავტორიზაცია, კონფიდენციალობა და მომხმარებელთა დაცვა. საჭირო იყო საინფორმაციო რესურსებისა და ტექნოლოგიების კრიმინალური და ტერორისტული მიზნებისთვის გამოყენების აღკვეთა.[59] პირველად, მთელი მსოფლიოს მასშტაბით, საერთაშორისო დონეზე გამართულ სამიტზე დადგინდა, რომ კიბერუსაფრთხოება უნდა განიხილებოდეს შესაბამის ეროვნულ და საერთაშორისო დონეზე.

კიბერდანაშაულთა უმეტესობა ტრანსნაციონალური ხასიათისაა და, შესაბამისად, კიბერსივრცეში უსაფრთხოების უზრუნველყოფის პრობლემას აწყდება ყველა სახელმწიფო, რომელიც აღიარებს, რომ წარმატება ამ დანაშაულთან ბრძოლაში შესაძლებელია იქნება მხოლოდ ყველა დაინტერესებული მხარის ერთობლივი ძალისხმევით. ეფექტური ბრძოლა კი მოიცავს, უპირველეს ყოვლისა, კრიმინალიზაციის მსგავს მიდგომას, იურისდიქციის საკითხის გადაწყვეტასა და ტრანსნაციონალური გამოძიების შესაძლებლობის მიცემას.

სხვადასხვა სახელმწიფოს კანონმდებლები სხვადასხვა გზით მიუდგნენ საინფორმაციო სივრცეში უსაფრთხოების უზრუნველყოფის პრობლემის გადაწყვეტას, მაგრამ მნიშვნელოვან ასპექტად რჩება ურთიერთჰარმონიზაცია, ამისათვის კი, საჭიროების მომენტიდან დღემდე, კიბერდანაშაულთან ბრძოლის საფუძველს ქმნიან საერთაშორისო-სამართლებრივი ხელშეკრულებები.

სწორედ ამის შედეგად, ევროპის საბჭომ 2001 წლის 23 ნოემბერს ქ. ბუდაპეშტში მიიღო კომპიუტერული დანაშაულის შესახებ კონვენცია, რომელიც ძალაში შევიდა 2004 წლის 1 ივლისს.[60] მართალია, აქტი შემუშავდა ევროპის საბჭოს ინიციირებით, თუმცა თავიდანვე იყო განზრახული, რომ იგი გასცდებოდა უბრალოდ რეგიონალური მოწესრიგების სტატუსს, ვინაიდან იმთავითვე მის შემუშავებაში მონაწილეობას იღებდნენ ევროსაბჭოს არაწევრი ქვეყნები, როგორებიცაა აშშ, კანადა იაპონია, სამხრეთი აფრიკა.

დღეს კონვენცია არის მთავარი საერთაშორისო ინსტრუმენტი და შეთანხმება კიბერდანაშაულის და ელექტრონული მტკიცებულებითების შესახებ. ის წარმოადგენს სახელმწიფოებისთვის გზამკვლევს, რათა შეიმუშაონ, მის შესაბამისად, ნორმატიული

[59] იხ.: ელ. ბმული: https://www.un.org/press/en/2003/pi1550.doc.htm [08.05.2022]

[60] 90-იან წლებში კიბერდანაშაულების მომრავლებამ უბიძგა ერთად შეკრებილიყვნენ საუკეთესო გამოცდილებების მქონე სამართალდამცავი ორგანოები, კერძო ტექნოლოგიური კომპანიები და სახელწმიფო ორგანოები, რომლებმაც შეძლეს შემოეთავაზებინათ საუკეთესო პრაქტიკა და გაერთიანდნენ პირველი დოკუმენტის შესაქმნელად, რომელიც იურიდულად სავალდებულოა და ერთიანი საერთაშორისო პრაქტიკით დაიწყებდა ბრძოლას კიბერდანაშაულთან.

ბაზა და გამოიყენონ საერთაშორისო ურთიერთთანამშრომლობის ინსტრუმენტად. ამ ეტაპზე კონვენციის ხელმომწერი 66 სახელმწიფოა და ის არის ღია ყველა დაინტერესებული ქვეყნისთვის.[61] კონვენციის გლობალურ მნიშვნელობაზე მიანიშნებს 2022 წელს ევროპის საბჭოს მიერ გამოქვეყნებული კვლევის შედეგები, სადაც მოცემულია 2022 წლის 31 იანვრის მდგომარეობით არსებული სტატისტიკა. კვლევის მიხედვით, 128 გაეროს წევრი სახელმწიფოების 66%-მა შეიმუშავა კიბერდანაშაულის მატერიალური კანონმდებლობა ბუდაპეშტის კონვენციის მიხედვით.[62]

კონვენციით, ხელმომწერმა სახელმწიფოებმა აიღეს ვალდებულება სხვადასხვა მიმართულებებით, როგორებიცაა მატერიალური და პროცესუალური სამართალი, ასევე, საერთაშორისო თანამშრომლობის ასპექტების გათვალისწინება ერთიანი მიდგომის ფარგლებში. აღნიშნულმა კონვენციამ მისცა სამართალდამცავ ორგანოებს ლეგიტიმური საფუძველი და ინსტრუმენტი გამოძიების ჩატარებისა და მტკიცებულებათა მოპოვების კუთხით, რომლებიც, თავის მხრივ ითვალისწინებენ, ასევე, უფლებების დაცვის გარანტიებსაც, რათა ვერ მოხერხდეს მათ მიერ ძალაუფლების ბოროტად გამოყენება.

პირველ რიგში, ერთიანი პრაქტიკის ჩამოყალიბების მიზნით და ეროვნული კანონმდებლობის კონვენციასთან ჰარმონიზაციის უზრუნველსაყოფად, სახელმწიფოებმა უნდა მოახდინონ იმ ცალკეული ქმედებების კიბერდანაშაულად კრიმინალიზაცია, რომლებიც, თავიანთი მახასიათებლებით, მოცემულია კიბერდანაშაულის კონვენციაში.

იმის გათვალისწინებით, თუ როგორ ვითარდებოდა ტექნოლოგიები და დანაშაულის ჩადენა, იცვლებოდა შეთანხმება და მისი დამატებით ოქმები. პირველი დამატებითი ოქმი მოიცავს კომპიუტერულ ქსელებში ქსენოფობიისა და რასიზმის ნიადაგზე ჩადენილი დანაშაულების კრიმინალიზაციას, რომელსაც ხელი მოეწერა 2003 წლის იანვარში და ძალაში შევიდა 2006 წლის მარტის თვეში.

მეორე მიმართულებით თანამშრომლობას, იგივე პროცესუალურ ასპექტს, წარმოადგენს კიბერდანაშაულის გამოძიების ეფექტური სისტემისა და შიდა სამართლებრივი მექანიზმების შექნა, რომლითაც შესაძლებელი იქნება სამართალდამცავების მიერ აღნიშნული დანაშაულის გამოძიება, ელექტრონული მტკიცებულებების მოპოვების შესაძლებლობა. მასში მოაიზრება როგორც მტკიცებულებების მოპოვებისათვის პირობებისა და გარანტიების უზრუნველყოფა, ისე ინტერნეტტრაფიკისა და შინაარსობრივი მონაცემების მოპოვება, კომპიუტერული მონაცემების ჩხრეკა/ამოღება და ა.შ.

[61] https://www.coe.int/en/web/cybercrime/parties-observers [08.05.2022]
[62] https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan2022-p/1680a564bb [08.05.2022]

დაბოლოს, მესამე მიმართულება არის ქვეყნების მონაწილეობა საერთაშორისო თანამშრომლობაში. მასში იგულისხმება ექსტრადაციის საკითხები, ორმხრივი დახმარების პროცედურები, კონფიდენციალობა, მონაცემთა დაჩქარებული დაცვისთვის ურთიერთდახმარება და ა.შ. კონვენციამ შექმნა საფუძველი საერთაშორისო თანამშრომლობისათვის, რომელიც 24/7-ზე იმუშავებს. აღსანიშნავია, რომ მეორე დამატებითი ოქმი, რომელიც გაიხსნა სახელმწიფოსათვის 2022 წლის მაისში ხელმოსაწერად, ითვალისწინებს პროცესუალურ საერთაშორისო ურთიერთანამშრომლობის გაზრდას,ეფექტურობასა და ადამიანის უფლებების დაცვის უფრო მეტი გარანტიის უზრუნველყოფას.[63]

ბუდაპეშტის კონვენცია წარმოადგენს ქვაკუთხედს ევროპის პოლიტიკის კონტექსტში კიბერდანაშაულთან ბრძოლაში. თუმცა, როგორც აღენიშნა, იგი იმაზე მეტია, ვიდრე შეთანხმება რეგიონულ ჭრილში .

პოლიტიკის განსაზღვრის მიმართულებით, საერთაშორისო დონეზე არსებობს კიბერუსაფრთხოებისა და კიბერდანაშაულთან ბრძოლის სხვა საერთაშორისო ინიციატივები. ზოგიერთი მათგანი რეგიონულ დონეზე აწესრიგებს კიბერდანაშაულისა და კიბერუსაფრთხოების საკითხებს, ზოგი კი - საერთაშორისო. კონვენცია მხარს უჭერს ყველა სხვა ორგანიზაციას, რომლებიც იყენებენ მას თავიანთი პრაქტიკისათვის. ეს ორგანიზაციებია, მაგალითად ევროპის კავშირი, ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია (OECD), აზია - წყნარი ოკეანის ეკონომიკური თანამშრომლობის ორგანიზაცია (APEC), ინტერპოლი და ა.შ.

სხვა საერთაშორისო შეთანხმებების უმრავლესობა დაფუძნებულია ბუდაპეშტის კონვენციის სამართლებრივ ბაზაზე, ხოლო ზოგი მათგანი ავსებს მას. მაგალითად, აფრიკის კავშირი (AU), რომელიც შედგება აფრიკის კონტინენტზე მდებარე სახელწმიფოებისგან. AU თანამშრომლობს ევროპის საბჭოს კიბერდანაშაულთან ბრძოლის პროგრამის ოფისთან (C-PROC) და თანმშრომლობის ფარგლებში შეიმუშავეს 2011 წელს კონვენცია კიბერუსაფრთხოებისა და პერსონალური მონაცემების დაცვის შესახებ“ (ე.წ. მალაბოს კონვენცია“).[64]

ევროპის დონეზე მიღებულია 2 უმნიშვნელოვანესი დირექტივა: 2011 წლის 13 დეკემბრის დირექტივა 2011/93/EU ბავშვთა სექსუალურ ძალადობასა და სექსუალურ ექსპლუატაციასთან და ბავშვთა პორნოგრაფიასთან ბრძოლის შესახებ[65] და 2013 წლის 12

---

[63] კიბერდანაშაულთან ბრძოლის საკითხებში ევროპის საბჭო არ შემოიფარგლა მხოლოდ კონვენციის შემუშავებითა და მიღებით. მან შექმნა კიბერდანაშაულის შესახებ კონვენციის კომიტეტი (C-CC), რომელიც წარმოადგენს მონაწილე სახელმწიფოებს, ხელს უწყობს კონვენციის დებულებების ეფექტურ გამოყენებას, განხორციელებას ინფორმაციის გაცვლას და მასში შეტანილი ცვლილებების განხილვას. გარდა ამისა, დახმარებას უწევს სახელმწიფოებს კიბერდანაშაულთან დაკავშირებულ პრობლემებთან გამკლავებაში. მათი შესაძლებლობების კონსოლიდაცია უზრუნველყოფილია ევროპის საბჭოს კიბერდანაშაულთან ბრძოლის ოფისის (C-CROS) მიერ.

[64] https://ccdcoe.org/organisations/au/ [08.05.2022]

[65] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093. იხ. მოცემული დირექტივის 26-ე პუნქტი.[08.05.2022]

აგვისტოს დირექტივა 2013/40/EU საინფორმაციო სისტემებზე თავდასხმების შესახებ.[66] ორივე დირექტივა სრულად შეესაბამება კონვენციას. ევროპის კომისიამ 2018 წელს შესთავაზა, შეემუშავებინათ რეგლამენტები და დირექტივები ტრანსნაციონალური მტკიცებულებებისა, ეს წინადადებები ცნობილია როგორც ე.წ. ელექტრონული მტკიცებულებების პაკეტი და დღემდე ევროპარლამენტის დებატების საგანია.[67]

მნიშვნელოვანია, რომ ევროკავშირის დონეზე ორი სპეციალიზებული სააგენტო განსაკუთრებულ ყურადღებას უთმობს კიბერდანაშაულს, ეს არის ევროპოლი, რომლის მიზანია ევროკავშირის წევრი ქვეყნების სამართალდამცავი ორგანოების თანამშრომლობის ეფექტურობის გაზრდა, ასევე - კიბერდანაშაულის ევროპული ცენტრი (EC3), რომელიც მოქმედებს 2013 წლიდან და რომელიც შეიქმნა ევროპოლის მიერ, რათა გააძლიეროს სამართალდამცავი ორგანოების რეაგირება კიბერდანაშაულები ევროკავშირში.[68]

თუ მივმართავთ ევროკავშირის მიღებულ დოკუმენტებს საინფორმაციო სივრცეში დანაშაულებებთან ბრძოლის სისტემის ასაშენებლად, უნდა აღინიშნოს, რომ ელექტრონულ კომერციაზე, პერსონალურ მონაცემებთან, საინფორმაციო სისტემებზე თავდასხმებთან, ბავშვთა პორნოგრაფიის წინააღმდეგ აქტებთან ერთად, 2001 წელს მიიღეს ჩარჩო გადაწყვეტილება თაღლითობისა და უნაღდო გადახდის საშუალებების გაყალბების წინააღმდეგ ბრძოლის შესახებ, რომელიც ავალდებულებდა თითოეულ მონაწილეს ასეთი ქმედებების კრიმინალიზაციას, თუ ისინი ჩადენილია განზრახ.[69]

საინტერესოა ასევე, დიდი რვიანი, რომელიც 1995 წლიდან მოყოლებული სულ უფრო მეტად აქტიურად მონაწილეობს ისეთი საკითხების გადაწყვეტაში, რომლებიც უკავშირდება კიბერდანაშაულს, ინფორმაციულ საზოგადოებას, კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას. 1995 წელს ჰალიფაქსის სამიტზე შეიქმნა უფროს ექსპერტთა ჯგუფი, რომელსაც დაევალა, შეეფასებინა და გაეანალიზებინა არსებული საერთაშორისო შეთანხმებები, ასევე, ორგანიზებულ დანაშაულთან ბრძოლის მექანიზმები.[70] მოცემული ჯგუფის მიერ ჩატარებული სამუშაოს შედეგად, შემუშავდა ორმოცი ოპერატიული რეკომენდაცია, რომლებიც დამტკიცდა 1996 წელს დიდი რვიანის ლიონის სამიტზე. ამ დროდან მოყოლებული, ლიონის ჯგუფი გახდა მუდმივმოქმედი მრავალფუნქციური ორგანო, რომლის შემადგენლობაში შევიდა მთელი რიგი სპეციალური სამუშაო ჯგუფებისა.

საერთაშორისო ორგანიზაციების მიერ, თავის ფარგლებში, მიღებულია მთელი რიგი ინიციატივები, მიმართული კოორდინირებული მოქმედების გასაუმჯობესებლად.

---

[66] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040 [08.05.2022]

[67] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en [08.05.2022]

[68] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [08.05.2022]

[69] Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA). Done at Brussels, 28 May 2001. ელ. ბმული: https://www.ejn-crimjust.europa.eu

[70] http://www.chebucto.ns.ca/Current/HalifaxSummitG7/ [08.05.2022]

კერძოდ, ეს არის რამდენიმე რეზოლუცია, მსოფლიო სამიტები ინფორმაციული საზოგადოების საკითხებზე (WSIS), გაეროს ზოგიერთი სტრუქტურის პროექტები.

2000 და 2001 წლების დეკემბერში გაეროს გენერალური ასამბლეის 55-ე და 56-ე სესიებზე მიიღეს № 55.63 და No56/121 რეზოლუციები „ინფორმაციული ტექნოლოგიების დანაშაულებრივ გამოყენებასთან ბრძოლაზე“. 2002 წლის დეკემბერში გაეროს გენერალური ასამბლეის 57-ე სესიამ მიიღო რეზოლუცია № 57/239 „კიბერუსაფრთხოების გლობალური კულტურის შექმნაზე“. 2003 წლის დეკემბერში გაეროს გენერალური ასამბლეის 58-ე სესიაზე მიიღეს რეზოლუცია No58/199 „კიბერუსაფრთხოების გლობალური კულტურის შექმნასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვაზე“. 2005 და 2006 წლებში, ასევე, მიიღეს ორი რეზოლუცია ინფორმაციული საზოგადოების საკითხებზე გაეროს მსოფლიო სამიტების შედეგების შესახებ.

კერძო სექტორის მიმართულებით აქტიურად მუშაობს მსოფლიო ბანკის ჯგუფი (WB). კომპიუტერული დანაშაულებები და ელექტრონულ ქსელებში არასანქცირებული შეღწევა მნიშვნელოვნად ვნებს ფინანსურ სექტორს. იმის გათვალისწინებით, რომ სულ უფრო იზრდება ფინანსური ინფორმაციის შენახვისა და გადაცემის მოცულობა, კომპიუტერული დამნაშავეებისთვის, ასევე, ადვილი ხდება ქსელებში არასანქცირებული შეღწევა და მავნე ქმედებების განხორციელება. ამიტომ, მსოფლიო ბანკის ჯგუფმა ბოლო პერიოდში განახორციელა მთელი რიგი ღონისძიებები, მიმართული ინფორმაციული უსაფრთხოების უზრუნველსაყოფად, განსაკუთრებით, ეს ეხება განვითარებად ქვეყნებს.

2.2. ბუდაპეშტის კონვენციის მიერ მატერიალურ-სამართლებრივი მოწესრიგება

როგორც უკვე აღინიშნა, „კიბერდანაშაულთან ბრძოლის შესახებ“ კონვენციით, სახელმწიფოებმა აიღეს ვალდებულება მატერიალურ-სამართლებრივი მოწესრიგების ნაწილში კონვენციასთან ჰარმონიზაციის უზრუნველყოფისა. დასახელებული მიზნით, ზოგიერთი ქვეყანა ახდენს ახალ დანაშაულთა კრიმინალიზაციას, ზოგი კი არსებული დანაშაულების ადაპტირებას, რომელიც ადეკვატურად პასუხობს ახალ ტექნოლოგიურ გამოწვევებს. რთულია კიბერდანაშაულთა კლასიფიკაცია,[71] თუმცა ევროპის საბჭომ სცადა და კონვენცია ითვალისწინებს კიბერდანაშაულთა ოთხ ფართო კატეგორიას:[72]

1. კომპიუტერულ მონაცემთა და სისტემათა კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის წინააღმდეგ ჩადენილი დანაშაულები;[73]

---

[71] *Gordon, F.,* On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, № 1, 2006, 13-20

[72] „კიბერდანაშაულის შესახებ“ 2001 წლის კონვენცია, ევროპის საბჭო. Council of Europe Convention on Cybercrime (CETS No. 185), Council of Europe, 2001, ხელმისაწვდომია ელ. ბმულზე: http://conventions.coe.int.

[73] „კიბერდანაშაულის შესახებ“ 2001 წლის კონვენციის მე-2-6 მუხლები.

2. კომპიუტერთან დაკავშირებული დანაშაულები[74]
3. შინაარსთან დაკავშირებული დანაშაულები [75]
4. საავტორო უფლებების დარღვევებთან დაკავშირებული დანაშაულები.[76]

დანაშაულთა პირველი კატეგორია, მესამე და მეოთხე კატეგორია კონცენტრირებულია სამართლებრივი დაცვის სიკეთეზე, მაშინ, როდესაც მეორე კატეგორიაში მოქცეული დანაშაულები, აქცენტს აკეთებს არა ხელყოფის ობიექტზე, არამედ ხელყოფის ხერხზე. შესაბამისად, ამ 4 კატეგორიას შორის მკვეთრი მიჯნა არ არსებობს, შესაძლოა, კიბერდანაშაული ჯდებოდეს რამდენიმე კატეგორიაში. განვიხილოთ თითოეული მათგანი ცალ-ცალკე.

კომპიუტერულ მონაცემთა და სისტემათა კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის წინააღმდეგ ჩადენილი დანაშაულები

პირველი კატეგორიის ყველა დანაშაული მიმართულია კომპიუტერულ მონაცემთა დაცვის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის წინააღმდეგ, საჭიროა, სულ ცოტა, ერთ-ერთის ხელყოფა. მონაცემთა კონფიდენციალურობა გულისხმობს, როდესაც სისტემები, ქსელები და მონაცემები დაცულია და მხოლოდ ავტორიზებულ მომხმარებლებს აქვთ მათზე წვდომა. მონაცემთა მთლიანობა ნიშნავს, როდესაც მონაცემები ზუსტი და მოქმედია და არ არის შეცვლილი, ხოლო ხელმისაწვდომობა - როდესაც მონაცემები, სერვისები და სისტემები ხელმისაწვდომია მოთხოვნით.

ის მოიცავს ისეთ დანაშაულებს, როგორებიცაა: უნებართვო წვდომა, მონაცემთა ხელში უკანონოდ ჩაგდება, მონაცემთა და სისტემის ხელყოფა, ასევე, მოწყობილობათა არამიზნობრივი გამოყენება.

უნებართვო წვდომა კომპიუტერულ სისტემაზე ან მის ნაწილზე გულისხმობს ჰაკინგსა ("hacking") და ქრეკინგს ("cracking"). მოცემულ შემთხვევაში ხდება პაროლით დაცული ვებ-საიტის დაცვის სისტემის გვერდის ავლა და ვებ-გვერდზე წვდომა,[77] პაროლის გატეხით წვდომა, ტექნიკის ან პროგრამული უზრუნველყოფის დაინსტალირება კომპიუტერულ სისტემაში შესასვლელად.[78] კრიმინალიზაციისთვის აუცილებელია სუბიექტური ელემენტი, როგორიცაა წინასწარი განზრახვა. [79]

---

[74] „კიბერდანაშაულის შესახებ" 2001 წლის კონვენციის მე-7-8 მუხლები.
[75] „კიბერდანაშაულის შესახებ" 2001 წლის კონვენციის მე-9 მუხლი.
[76] „კიბერდანაშაულის შესახებ" 2001 წლის კონვენციის მე-10 მუხლი.
[77] *Sieber,* Council of Europe Organised Crime Report, 2004, 65.
[78] იქვე.
[79] კონვენციის მიხედვით, სახელმწიფოს შეუძლია განზრახვაში გაითვალისწინოს უსაფრთხოების ზომების დარღვევა, კომპიუტერული მონაცემების მოპოვება, სხვა კომპიუტერულ სისტემასთან კავშირი ან სხვა არაკეთილსინდისიერი განზრახვა.

მონაცემების ხელში უკანონოდ ჩაგდება[80] აფართოებს კომპიუტერულ მონაცემთა მთლიანობისა და კონფიდენციალურობას დაცვას, რადგან ნორმა მოიცავს არა მარტო მონაცემებს, რომლებიც მოთავსებულია სისტემაში, არამედ გადამცემ მონაცემებსაც. მონაცემები შეიძლება ჩაითვალოს "გადამცემ პროცესში", სანამ არ მიაღწევს საბოლოო დანიშნულებას, იქნება ეს სისტემა თუ სავარაუდო მიმღები. მონაცემთა გადაცემა შეიძლება ჩაითვალოს დასრულებულად, როდესაც მოხდება დანიშნულების კომპიუტერული სისტემაში შეღწევა.[81] დამნაშავეები ხშირად იყენებენ მავნე „ჯაშუშურ“ პროგრამულ უზრუნველყოფას, რათა ხელში ჩაიგდონ მონაცემები.[82]

დამნაშავეებს შეუძლიათ, დაარღვიონ მონაცემთა მთლიანობა და ჩაერიონ მათში კომპიუტერული მონაცემების წაშლით, ბლოკირებით ან შეცვლით. მონაცემების წაშლის ერთ-ერთი გავრცელებული მაგალითია კომპიუტერული ვირუსი. თანამედროვე ვირუსებს შეუძლიათ დისტანციურად მართონ მსხვერპლის კომპიუტერი ან დაშიფრონ ფაილები ისე, რომ მსხვერპლს არ ჰქონდეს წვდომა საკუთარ ფაილებზე, სანამ ისინი არ გადაიხდიან ფულს.[83] რაც შეეხება მოწყობილობათა არამიზნობრივ გამოყენებას, მასში იგულისხმება პროგრამული უზრუნველყოფისა და სხვა მოწყობილობები, პაროლები და წვდომის კოდები, რომლებიც გამოიყენება კონვენციით გათვალისწინებული დანაშაულის ჩასადენად.

კომპიუტერთან დაკავშირებული დანაშაულები

როგორც აღინიშნა, ამ დანაშაულთა კატეგორიას მიეკუთვნება კომპიუტერული გაყალბება და კომპიუტერული თაღლითობა. კომპიუტერული გაყალბება მოიცავს პერსონიფიკაციის ელემენტებს, როდესაც კრიმინალები თაღლითური მიზნებისთვის ახდენენ სხვა პირების ანდა სხვა ინსტიტუტებს იმიტაციას. მაგალითად, თავს აჩვენებენ სხვა ორგანიზაციის ან დაწესებულების წარმომადგენელად, რათა დაარწმუნოს მომხმარებლები, დაიჯერონ ელფოსტის შინაარსის სისწორეში და აიძულონ, მიჰყვნენ მათს მითითებებს. ეს არის ფიშინგის კლასიკური შემთხვევა.

კომპიუტერთან დაკავშირებული თაღლითობა არის ერთ-ერთი ყველაზე პოპულარული და გავრცელებული დანაშაული კიბერსივრცეში. ეს შეიძლება იყოს ონლაინ აუქციონთან საკრედიტო ბარათებთან დაკავშირებული მანიპულაციები, ინტერნეტ-ფინანსური პირამიდები და ა.შ.[84] მიუხედავად იმისა, რომ ეს დანაშაულები ჩადენილია კომპიუტერული ტექნოლოგიების გამოყენებით, სისხლის სამართლის სისტემების უმეტესობა მათ აკვალიფიცირებს არა კომპიუტერთან დაკავშირებულ დანაშაულებად, არამედ, როგორც ჩვეულებრივ თაღლითობად, რაც განხილული იქნება

[80] ე.წ. მონაცემებზე ჯაშუშობა - “Data Espionage”

[81] *Walden, I.,* Computer Crime and Digital Investigations, Oxford: OUP, 2007, 184.

[82] იხ. მეტი „ჯაშუშურ“ პროგრამებზე *Jaeger/ Clarke*, The Awareness and Perception of Spyware amongst Home PC Computer Users, 2006

[83] მაგალითად რანსომვეარი (Ransomware), იგივე კომპიუტერული გამოძალვა.

[84] *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, 1

ნაშრომის მომდევნო თავში. მთავარი განსხვავება კომპიუტერთან დაკავშირებულ და ტრადიციულ თაღლითობას შორის არის თაღლითობის სამიზნე: თუ დამნაშავეები ცდილობენ, გავლენა იქონიონ ადამიანზე - ეს არის ტრადიციული თაღლითობა, მაგრამ თუ დამნაშავეები მიზნად ისახავენ კომპიუტერული სისტემისთვის გვერდის ავლას, დანაშაულები, როგორც წესი, კლასიფიცირდება კომპიუტერთან დაკავშირებული თაღლითობად.

შინაარსთან დაკავშირებული დანაშაულები და საავტორო და მომიჯნავე უფლებების დარღვევებთან დაკავშირებული დანაშაულები.

ეს კატეგორია მოიცავს კიბერსივრცეში განთავსებულ უკანონო შიგთავსს („კონტენტს“), მაგალითად, ბავშვთა პორნოგრაფიას, ქსენოფობიურ მასალას ან რელიგიური გრძნობების შეურაცხყოფას, კიბერბულინგს, ონლაინ კაზინოს და ა.შ.[85]

რაც შეეხება საავტორო უფლებების დარღვევასთან დაკავშირებულ დანაშაულებს, ამ კატეგორიაში განიხილება ისეთი შემთხვევები, როდესაც ინტერნეტის საშუალებით კერძო პირები ან/და კომპანიები ავრცელებენ ნებისმიერი ტიპის ფაილს, აგრეთვე, მათ მიეკუთვნება ინტელექტუალური საკუთრების ჩამოტვირთვა, კოპირება და გავრცელება.[86]

2.3. ფინანსურად მოტივირებული კიბერდანაშაულთა მატერიალურ-სამართლებრივი მოწესრიგება სხვადასხვა ქვეყნებში.

სამეცნიერო ლიტერატურაში აქტიურად დებატობენ იმის შესახებ, თუ რამდენად ერგება არსებული ტრადიციული სამართლებრივი სისტემები კიბერსივრცეში დაგეგმილ/ჩადენილ კომპიუტერულ დანაშაულს. ერთი მხრივ, დანაშაულის ობიექტი, შესაძლოა, იყოს ინდივიდი, საზოგადოებისა თუ სახელმწიფოს ინფორმაციული უსაფრთხოება. ამ კატეგორიაში შედის, მაგალითად, კომპიუტერულ ინფორმაციაზე უნებართვო წვდომა, კომპიუტერული ინფორმაციის მოდიფიკაცია, კომპიუტერული დივერსია და ა.შ.,ხოლო, მეორე მხრივ, დანაშაულის ჩადენა, შესაძლოა, ხდებოდეს სატელეკომუნიკაციო სისტემების გამოყენებით. კერძოდ, ამ ჯგუფში შედის კომპიუტერული ტექნოლოგიების გამოყენებით ჩადენილი ქურდობა, თაღლითობა და ა.შ.[87] მეცნიერების დიდი ნაწილი მივიდა იმ დასკვნამდე, რომ კიბერდანაშაულის

[85] *Tsakalidi G. Vergidis K.,* A systematic approach toward description and classification of cybercrime incidents Department of Applied Informatics, University of Macedonia, 20-23

[86] იქვე 24-24

[87] *Семыкина О. И.*, Тенденции борьбы с преступлениями в сфере информационных технологий (сравнительно-правовой аспект) // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». 2014, 49—54

წინააღმდეგ ეფექტურად ბრძოლა ახალ მიდგომებს საჭიროებს და დღის წესრიგში დგება ტრადიციული და კიბერდანაშაულთა კატეგორიების გამიჯვნა.[88]

ახალი ტიპის ზოგიერთი კიბერდანაშაული აღარ ჯდება ტრადიციული დანაშაულის კატეგორიაში, შესაბამისად, არც არსებულ კანონმდებლობას არ ერგება. მაგალითად, DoS შეტევა (იგივე „მომსახურებაზე უარის თქმა“) არ არის ქურდობა, არც მუქარა ან ხულიგნობა. შესაბამისად, თუ კონკრეტული ქმედება, დანაშაულებრივი აქტი „ტრადიციული მეთოდის“ ქმედების შემადგენლობაში ვერ ჯდება, ვერც მისი კრიმინალიზაცია მოხდება, რაც საერთაშორისო აქტებით გათვალისწინებულ მექანიზმებს არაეფექტურს ხდის.

ერთია, როდესაც გვაქვს დანაშაულის ინდივიდუალური სახე და მისი ცალკე სპეციალურ შემადგენლობად გამოყოფა ბევრად მარტივია, რადგან არსებობს ხელყოფის ერთი განსაზღვრული ობიექტი. სირთულეს წარმოადგენს ფინანსურად მოტივირებული კიბერდანაშაულების კლასიფიკაცია, საკუთრების წინააღმდეგ მიმართული დანაშაულებთან მჭიდრო კავშირის გამო.

კომპიუტერული პროგრამით სხვის ანგარიშზე უნებართვო წვდომით სხვისი ქონების დაზიანება, წარმოადგენს თუ არა კიბერდანაშაულის ერთ-ერთ სახედ. რიგი ქვეყნები, როგორიცაა დიდი ბრიტანეთი, საფრანგეთი, იყენებენ ზოგად წესებს საკუთრების დანაშაულის შესახებ, კიბერქურდობასთან დაკავშირებით, მიმართავენ დებულებებს, რომლებიც ასახავს ქმედებების შემადგენელ ელემენტებს, როგორიცაა არაავტორიზებული წვდომა, პერსონალურ მონაცემებში ჩარევა და სხვა დანაშაულები. თურქეთის კანონმდებლობაში გათვალისწინებულია კომპიუტერული ტექნოლოგიების გამოყენება, როგორც ქონებრივი დანაშაულის მაკვალიფიცირებელი ნიშანი. ხოლო, მაგალითად, აშშ-სა და გერმანიაში კომპიუტერული ინფორმაციის გამოყენებით ჩადენილი ქურდობა ცალკე დანაშაულად არის გამოყოფილი და აკრძალულია ან ქვეყნის მთავარი სისხლის სამართლის კანონით, ან სპეციალური აქტით, ან ორივეთი ერთად. ამ მხრივ, საინტერესოა, როგორია და რა ნიშნებითაა განსხვავებული უცხო ქვეყნების მიდგომები.

ამერიკის შეერთებული შტატები

ამერიკის შეერთებულ შტატებში მოქმედებს ორსაფეხურიანი სამართლებრივი სისტემა: სისხლის სამართალი კლასიფიცირებულია ფედერალურ (federal crimes) და რეგიონულ (state crimes) სამართლებრივ სისტემაზე. ამ სისტემის მიხედვით, თითოეულ შტატს აქვს უპირობო სუვერენიტეტი და საკუთარი სისხლის სამართლის დებულებები, მათ შორის კიბერდანაშაულის კრიმინალიზაცია.

აშშ-ს კიბერდანაშაულის მიმართ ერთიანი მიდგომა არ აქვს და კომპიუტერული დანაშაულის რეგულაციები შტატების მიხედვით განსხვავდება. მაგალითად, თუ

88 *Brenner, Susan W., Cybercrime and the law: Challenges, issues, and outcomes.* UPNE, 2012.

გარკვეულ შტატებში სისხლისსამართლებრივი პასუხისმგებლობა დამნაშავის მიზნიდან გამომდინარეობს, სხვაგან ეს დამოკიდებულია იმაზე, თუ რამდენად ექვემდებარება არასანქცირებული შეღწევის შედეგად დაკარგული ინფორმაცია აღდგენას. კერძოდ, იმ შემთხვევაში, თუ განადგურებული ინფორმაციის აღდგენა შესაძლებელია, დამნაშავე სისხლისსამართლებრივი პასუხისმგებლობისგან თავისუფლდება. ასევე, ზოგიერთი შტატის დონეზე[89] დასაშვებია ორგანიზაციის მიერ იმ კომპიუტერულ ქსელზე ან სისტემაზე საპასუხო თავდასხმა, რომლიდანაც საცდეს მათს კომპიუტერში ან სისტემაში შეღწევა. აღსანიშნავია, რომ მსგავსი მიდგომა მრავალწლიან გამოცდილებას ემყარება და აღნიშნული პრაქტიკა გარკვეული კიბერშეტევების განეიტრალების წინაპირობაა. მაგალითად, DoS შეტევის გასანეიტრალებლად, თავდაცვითი ზომების მიღების გარდა, ხშირად თავდამსხმელზე საპასუხო DoS შეტევა ხდება საჭირო.

აშშ-ში პირველი კანონპროექტი, რომელიც ადგენს სისხლის სამართლის პასუხისმგებლობას ინფორმაციული ტექნოლოგიების სფეროში ჩადენილი დანაშაულებისთვის, შეერთებულ შტატებში ჯერ კიდევ 1977 წელს შემუშავდა. ამ კანონპროექტის საფუძველზე, 1984 წლის ოქტომბერში მიიღეს კომპიუტერული თაღლითობისა და ბოროტად გამოყენების შესახებ კანონი (CFAA)[90], მთავარი სამართლებრივი აქტი, რომელიც ადგენს სისხლის სამართლის პასუხისმგებლობას კომპიუტერული ინფორმაციის სფეროში ჩადენილი დანაშაულებისთვის.[91] შემდგომში მასში არაერთხელ შევიდა შესწორებები.

კომპიუტერული თაღლითობისა და ბოროტად გამოყენების შესახებ კანონი ადგენს პასუხისმგებლობას რამდენიმე ძირითადი დანაშაულისთვის: კომპიუტერული ჯაშუშობა; ინფორმაციაზე უნებართვო წვდომა; კომპიუტერული თაღლითობა; დაცული კომპიუტერების განზრახ ან გაუფრთხილებლობით დაზიანება; მუქარა, გამოძალვა, კომპიუტერული ტექნოლოგიების გამოყენებით ჩადენილი შანტაჟი და სხვა. ამჟამად აშშ-ის კონგრესი განიხილავს ახალ კანონპროექტს კიბერუსაფრთხოების შესახებ, რომელიც ითვალისწინებს კიბერდანაშაულებისთვის უფრო მკაცრ ჯარიმებს და მათი საჯარო საფრთხის განმარტების რეალურ დანაშაულთან გათანაბრებას.

საქართველოს კანონმდებლობით, არაა დაყოფილი ქვესახეობებად ინფორმაცია, რომელიც ხელყოფილია კომპიუტერულ სისტემაში წვდომის გზით. კომპიუტერულ ინფორმაციაზე წვდომის შედეგად ხელყოფილი კანონით დაცული ინფორმაცია არ იყოფა ქვესახეობებად. აშშ-ის კანონმდებელი, თავის მხრივ, ადგენს

[89] მაგალითად, იუტას შტატი ითვალისწინებს აუცილებელ მოგერიებას კიბერდანაშაულებში.

[90] The Counterfeit Access Device and Computer Fraud and Abuse Law of 1984, იხ.: https://www.congress.gov/bill/98th-congress/house-bill/5112 [10.05.2022]

[91] აქტის მიღების ისტორიის უკეთ გასაცნობად იხ.: Glenn D. Baker, Note, Trespassers Will Be Prosecuted: Computer Crime in the 1990s, 1993, 61, 63-66.

სისხლისსამართლებრივ პასუხისმგებლობას კომპიუტერულ ინფორმაციაზე უკანონო წვდომისთვის, მისი მახასიათებლებიდან გამომდინარე.

კომპიუტერულ ინფორმაციაზე უკანონო წვდომისათვის სისხლის სამართლის პასუხისმგებლობის დამდგენი სისხლის სამართლის ნორმები იცავს ინფორმაციის, რომელიც ინახება ფინანსურ ინსტიტუტებში, ინფორმაციას სამთავრობო ორგანიზაციების ნებისმიერ კომპიუტერში ან კომპიუტერებში. კომპიუტერული თაღლითობისა და ბოროტად გამოყენების შესახებ კანონი[92] არ მოიცავს არაავტორიზებულ წვდომას ნებისმიერ პერსონალურ ინფორმაციაზე, რომელის დაშვებას განსაზღრავს მისი მფლობელი. ვინაიდან აქტი ფედერალურია, ის უზრუნველყოფს მხოლოდ საზოგადოებისა და სახელმწიფოსთვის ინფორმაციის ყველაზე მნიშვნელოვანი კატეგორიების დაცვას. სხვა სახეობები შტატების დონეზე რეგულირების საგანია.[93]

ფედერალური და ცალკეული შტატების სისხლის სამართლის კანონმდებლობის ანალიზი ცხადყოფს, რომ დანაშაულის ხელყოფის ობიექტია როგორც სახელმწიფო საიდუმლოება ან კომერციული საიდუმლოება, ასევე, ინფორმაცია, რომელთან წვდომის შესაძლებლობას განსაზღვრავს თავად მომხმარებელი. თავის მხრივ, პირველი კატეგორიის ინფორმაციაზე არასანქცირებული წვდომისთვის სისხლისსამართლებრივი პასუხისმგებლობა განსაზღვრულია ფედერალურ დონეზე, ხოლო მეორისაზე - შტატების დონეზე.

„ციფრული ეკონომიკის“ კონცეფციაში ინფორმაცია მისი მთავარი ღირებულება და პროდუქტია. მაშასადამე, აშშ-ს კანონმდებელმა საკვანძო ფაქტორად გამოყო, კვალიფიკაციისა და სასჯელის დადგენისას, ინფორმაციის კატეგორიები.[94] „ციფრულ საზოგადოებაში“ ინფორმაციის თვისებები განსაზღვრავს კომპიუტერული ინფორმაციულ სფეროში დანაშაულის სოციალურ საფრთხესა და ინფორმაციის, როგორც დანაშაულის ხელყოფის ობიექტის დაცვის საჭიროების გაზრდას.

გაერთიანებული სამეფო

როგორც ანგლო-საქსონური სამართლის ოჯახის წარმომადგენელი, გაერთიანებულ სამეფოში არ არის ერთიანი კოდიფიცირებული სისტემა, როგორიცაა

---

[92] Computer Fraud and Abuse Act (CFAA), იხ. ბმული: http://www.law.cornell.edu/uscode/text/18/1030

[93] მაგალითად, ვირჯინიის შტატში მოქმედებს ვირჯინიის კომპიუტერული დანაშაულის აქტი (The Virginia Computer Crimes Act). მასში გათვალისწინებულია არა მარტო სისხლის სამართლის დებულებები, ასევე სამოქალაქო სამართლის დებულებებს, მაგალითად, უნებართვო წვდომით მიყენებული ზიანის ანაზღაურების მოთხოვნა. იხ.: Virginia Computer Crimes Act, Virginia Code Section 18.2-152.1 et seq. of 11 April 1984. ელ. ბმული: https://law.lis.virginia.gov/vacode/title18.2/chapter5/, ასევე კალიფორნიის შტატის კომპიუტერულ მონაცემებთან წვდომისა და თაღლითობის აქტი (California Comprehensive Computer Data Access and Fraud Act (California Computer Act)), ელ. ბმული: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=502.&lawCode=PEN

[94] Abrams N., Beale S.S., Klein R., Federal Criminal Law and its Enforcement, 5th ed. , 2010, 205.

სისხლის სამართლის კოდექსი, თუმცა კომპიუტერული დანაშაულისთვის სისხლისსამართლებრივი პასუხისმგებლობის საკითხები რეგულირდება სხვადასხვა აქტის დონეზე: კომპიუტერული დანაშაულის აქტში, 2006 წლის თაღლითობის აქტში.

თავდაპირველად, დიდ ბრიტანეთში კომპიუტერული დანაშაულისთვის სისხლისსამართლებრივი პასუხისმგებლობის საკითხები განიხილებოდა საკუთრების წინააღმდეგ ჩადენილ დანაშაულებთან ერთად: კრიმინალები თუ ჩაიდენდნენ ქურდობას კომპიუტერული სისტემის გამოყენებით, ექვემდებარებოდნენ სისხლის სამართლის პასუხისმგებლობას 1968 წლის ქურდობის კანონის შესაბამისად (Theft Act 1968).[95] 1990 წლიდან კიბერდანაშაული ექვემდებარება წერილობით კანონს - კომპიუტერული ბოროტად გამოყენების აქტს,[96] რომელსაც ხელი შეუწყო 1988 წლის სასამართლო პრეცედენტმა (Regina v Gold. & Schifreen). [97]

დიდ ბრიტანეთში კომპიუტერული ბოროტად გამოყენების შესახებ კანონი[98] ძალაშია 1990 წლის აგვისტოდან. ამ კანონის პირველი პუნქტი ეხება „კომპიუტერულ მონაცემებზე არაავტორიზებული წვდომას“. აქტის მიხედვით, პირის ქმედება ჩაითვლება დანაშაულად, თუ ის იყენებს კომპიუტერს რაიმე ფუნქციის შესასრულებლად, იმ განზრახვით, რომ უზრუნველყოს წვდომა ნებისმიერ კომპიუტერში არსებულ პროგრამაზე ან მონაცემებზე, თუ დადგინდა, რომ ეს წვდომა არაავტორიზებულია.

ამ მხრივ საინტერესოა, რომ თაღლითური ხასიათის დანაშაულების სტრუქტურა უჩვეულოა იმით, რომ ის საშუალებას იძლევა, ქმედება ჩაითვალოს დასრულებულად, მიუხედავად იმისა, მოჰყვა თუ არა ქმედებას რეალური ფინანსური სარგებელი და გამოიწვია თუ არა რეალური ზარალი.[99]

გარდა ამისა, სატელეკომუნიკაციო სისტემების გამოყენებით თაღლითური ინფორმაციის მოპოვების მიზნით საგნების ფლობისა და მიწოდების კრიმინალიზაციის შესახებ პასუხისმგებლობის წესებს შეიცავს 1997 წლის „ტელეკომუნიკაციების შესახებ“ კანონი. კომპიუტერის გამოყენებით ქურდობის კვალიფიკაციისას გამოიყენება ქურდობის კანონის დებულებები (1968 წ.) და ქურდობის აქტი (1978 წ.).
გაერთიანებული სამეფოს მოდელი, შესაძლოა, პრობლემას ქმნიდეს,ვინაიდან ნორმები არაა სისტემატიზებული, და მეორეც, გამოყენებული აქტები (განსაკუთრებით, თაღლითობასა და კომპიუტერულ დანაშაულთან დაკავშირებით) არის

[95] *Чернякова А. В.*, Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации, Юридическая наука и правоохранительная практика, № 4 (46), 2018, 168-179.
[96] Computer Misuse Act 1990 / First Published 1990, Reprinted in the United Kingdom by The Stationery Office Limited. - London, 1997.
[97] Regina v. Gold. & Schifreen, https://swarb.co.uk/regina-v-gold-and-schifreen-cacd-17-jul-1987/ [10.05.2022]
[98] Computer Misuse Act 1990, იხ.: https://www.legislation.gov.uk/ukpga/1990/18/contents [10.05.2022]
[99] *Ashworth A. J.*, United Kingdom // The Handbook of Comparative Criminal Law / eds. by K. J. Heller, M. D. Dubber. Stanford; California, 2011. P. 552.

წინააღმდეგობრივი: ყოველი აქტი, შეიძლება, ადგენდეს მოქმედების საკუთარ საზღვრებს და ეწინააღმდეგებოდეს სხვა აქტებს, რაც იძლევა ახალი ინტერპრეტაციის საშუალებას სასამართლო პრეცენდენტისთვის. თუმცა საერთო სამართლის ქვეყნების სამართლის ძირითად წყაროს წარმოადგენენ სწორედაც პრეცედენტები.

გერმანია

გერმანიის ფედერალური კრიმინალური პოლიციის ოფისის განმარტებით, კიბერდანაშაული მოიცავს ყველა დანაშაულს, რომელიც ჩადენილია ინფორმაციის შეგროვების, დამუშავებისა და გადაცემის აღჭურვილობის გამოყენებით ან მის წინააღმდეგ, სადაც, ვიწრო გაგებით, მოიცავს ისეთ ქმედებებს, რომლებშიც ცენტრალურ როლს ასრულებს ელექტრონული მონაცემების დამუშავების ელემენტების გამოყენება.[100] გერმანიაში კომპიუტერულ დანაშაულთა კრიმინალიზაცია რეგულირდება როგორც სისხლის სამართლის კანონით, ასევე რამდენიმე აქტით. ძირითადი კანონი არის გერმანიის „ინტერნეტ ტექნოლოგიების უსაფრთხოების აქტი“, [101] გერმანიის კანონი „ტელეკომუნიკაციის შესახებ“[102], „მონაცემთა დაცვის შესახებ“ ევროკავშირის ძირითადი რეგულაცია[103]; გერმანიის ფედერალური „კანონი მონაცემთა დაცვის შესახებ“ [104] და კიბერუსაფრთხოების მომწესრიგებელი აქტები.

გერმანიის სისხლის სამართლის კანონმდებლობა არ ითვალისწინებს ცალკე თავს და კლასიკური დანაშაულებათა თავში არის მოცემული. ამავდროულად, კომპიუტერული ტექნოლოგიები გამოიყენება, როგორც დანაშაულის საშუალება ან საგანი. მაგალითად, „პირადი და საიდუმლო სივრცის დარღვევა/დაზიანება“ კოდექსის თავში[105] ინტეგრირებულია კომპიუტერულ დანაშაულთან დაკავშირებული რამდენიმე მუხლი, მათ შორის თაღლითობასთან გაერთიანებულ მუხლიც.

გერმანიის კანონმდებლობით, თაღლითობის ძირითად შემადგენლობასთან ერთად (სსკ § 263), კოდექსში გათვალისწინებულია თაღლითობის სპეციალური

---

[100] *Зигмунт О.А., Петровский А.В.*, Кибер и интернет-преступность в Германии и России: возможности сравнительного исследования, Юридическая наука и правоохранительная практика, №4 (34), 2015, 180-188. შეად.: Wiesbaden, S., Cybercrime: Bundeslagebild 2013.

[101] *IT-Sicherheitsgesetz*, ძალაში შევიდა 2015 წელს. იხ. ბმული: https://www.buzer.de/gesetz/11682/index.htm

[102] *Telekommunikationsgesetz,* https://www.gesetze-im-internet.de/tkg_2021/

[103] Regulation (EU) 2016/679

[104] *Bundesdatenschutzgesetz*, https://www.gesetze-im-internet.de/bdsg_2018/

[105] მაგალითად, გერმანიის სისხლის სამართლის კოდექსის XV თავი. პირადი და საიდუმლო სივრცის დარღვევა/დაზიანება: § 202 a. მონაცემთა მოპოვება (ჰაკერული თავდასხმა), § 202 b. მონაცემთა მოპოვება-გამოყენება (ფიშინგი), § 202 c. 202 a და 202 b მუხლებში გათვალისწინებული დანაშაულის მომზადება, § 202 d. მონაცემთა ქურდობა - აერთიანებს 202 a, 202 b და 202 c, ასევე, დამატებით მოიცავს შემთხვევას, როდესაც ამჟამინდელი ან ყოფილი თანამშრომელი არღვევს კონფიდენციალობის პირობას, რამდენადაც ასეთ დროს მას აქვს/ჰქონდა დაშვება ამ მონაცემებზე. მაგრამ, იმ შემთხვევაში, თუ დასაქმებული ცბიერებით დაარღვევს წესს, ეს დაკვალიფიცირდება, როგორც ფიშინგი.

შემადგენლობა - კომპიუტერული თაღლითობა (სსკ § 263 a),[106] რომლის მიზანია თაღლითურ სქემებში კომპიუტერული ტექნოლოგიების გამოყენებისა და სხვადასხვა პროგრამული მანიპულაციების კრიმინალიზაცია.[107]

თაღლითობის ძირითადი შემადგენლობისგან განსხვავებით, კომპიუტერული თაღლითობა მოიცავს მოტყუებას, რომელიც მიმართულია არა პიროვნების, არამედ კომპიუტერული სისტემისკენ და ამ შემთხვევაში ზიანი ვლინდება ინფორმაციის დამუშავების პროცესზე ზემოქმედებით. განსხვავებულ სიტუაციაში - როდესაც მოტყუება მიმართულია პირისკენ და არა კომპიუტერულ სისტემის ან კომპიუტერული ინფორმაციისკენ - აქტი კვალიფიცირდება, როგორც ტრადიციული თაღლითობა. აქედან გამომდინარე, გერმანიის სისხლის სამართლის კოდექსი იცავს ფულს, როგორც მატერიალურ ნივთს, ასევე „უნაღდო ფულს“, როგორც მონაცემს, რომელიც დაცულია სპეციალური შემადგენლობით.[108]

აღსანიშნავია, რომ გერმანიის სისხლის სამართლის კოდექსში კომპიუტერული დანაშაულები არ არის ერთიანად მოთავსებული ცალკეულ (თავში) და არის „ტრადიციული" ტიპის დანაშაულში ინტეგრირებული. ისინი ერთმანეთისგან განსხვავდბიან მხოლოდ დანაშაულის ელემენტებით: დანაშაულის საგნით, მეთოდით, ინსტრუმენტით. მაგალითად: § 202a მოქმედებს, როგორც § 202 „კორესპონდენციის საიდუმლოების დარღვევის“ სპეციალური წესი. ეს მუხლები არის ერთად მოთავსებული XV თავში „პირადი და საიდუმლო სივრცის დარღვევა“, აქვთ საერთო დანაშაულის ობიექტი - „კონფიდენციალურობა“, და განსხვავდებიან მხოლოდ დანაშაულის საგნით: § 202 - სხვა ადამიანების წერილები და დოკუმენტები, § 202a - ინფორმაციის მექანიზირებული მატარებელი. მსგავსი მიდგომა კრიმინალიზაციისა ჩანს საფრანგეთის სამართალში.

სხვა ქვეყნების მიდგომები

საფრანგეთის სისხლის სამართლის კოდექსში კომპიუტერულ დანაშაულთა კრიმინალიზაციის ნორმები მოცემულია ორ წიგნში.მეორე წიგნი „ადამიანის

---

[106] კომპიუტერული თაღლითობა გულისხმობს შემთხვევას, როდესაც პირი, რომელიც სხვადასხვა სახის კომპიუტერული მანიპულაციების საშუალებით (დააზიანებს მოწყობილობას ისე, რომ მისი მართვა მფლობელისთვის შეუძლებელი გახდება, გამოიყენებს არასწორ/არასრულ მონაცემებს, არასანქცირებული მეთოდებით მოახდენს მათზე ზემოქმედებას), თავისთვის ან მესამე პირზე გადასაცემად, გარკვეულ აქტივებზე უპირატესობას უკანონოდ მოიპოვებს, იხ.: German Criminal Code, Computer fraud, Section 263a (იხ. ელ. ბმული: https://www.lewik.org/term/15792/computer-fraud-section-263a-german-criminal-code/ [10.05.2022].

[107] *Semykina O.I.,* Combating Cyber Crimes in Foreign Contries, Журнал зарубежного законодательства и сравнительного правоведения, 2016, 4., შეად. *Odenthal R.,* Korruption und Mitarbeiterkriminalitat: Wirtschaftskriminalitat vorbeugen, erkennen und aufdecken. 2., vollstandig Qberarbeitete und erweiterte Auflage. Gabler I GWV Fachverlage GmbH, Wiesbaden, 2009. S. 83, 275.

[108] აღსანიშნავია, რომ ამაზე მსჯელობა იყო მოცემული საქართველოს სისხლის სამართლის კოდექსის 2021 წლის ცვლილებების კანონპროექტში. იხ. განმარტებითი ბარათი
საქართველოს კანონის პროექტზე„საქართველოს სისხლის სამართლის კოდექსში ცვლილების შეტანის შესახებ“, 2021 წ.

წინააღმდეგ ჩადენილი დანაშაულებისა და გადაცდომების შესახებ“, რომელიც მოიცავს ისეთი დანაშაულების ელემენტებს, როგორებიცაა პერსონალურ მონაცემების უკანონო ქმედებები სატელეკომუნიკაციო სისტემებში. მესამე წიგნში „ქონებრივი დანაშაულისა და გადაცდომის შესახებ“ მოცემულია თავი „მონაცემთა ავტომატური დამუშავების სისტემების ხელყოფის შესახებ“, რომლის წესები ითვალისწინებს სისხლისსამართლებრივ პასუხისმგებლობას მისი ბოროტად გამოყენებისათვის. აქედან გამომდინარეობს, რომ პერსონალური მონაცემები, ისევე, როგორც სატელეკომუნიკაციო სისტემები, დაცულია სისხლის სამართლით. საფრანგეთის სისხლის სამართლის კოდექსი არ შეიცავს სპეციალურ წესებს კომპიუტერული ინფორმაციის გამოყენებით ჩადენილი ქურდობის შესახებ.[109]

შვედეთისა და დანიის სისხლის სამართლის კოდექსებში არ არსებობს სპეციალური მუხლები, თავები, რომლებიც ეძღვნება პასუხისმგებლობას კომპიუტერული დანაშაულის ჩადენისთვის. მაგალითად, დანიის სისხლის სამართლის კოდექსის 279 ა პუნქტი ითვალისწინებს, რომ ნებისმიერი პირი, რომელიც თავისთვის ან სხვისთვის უკანონო სარგებლის მისაღებად უკანონოდ ცვლის, ავსებს ან წაშლის ინფორმაციას ან პროგრამებს, რომლებიც გამოიყენება ელექტრონული მონაცემების დამუშავებისთვის, ან რომელიც სხვა გზით ცდილობს მანიპულაცია მოახდინოს მონაცემთა დამუშავების შედეგებზე, დამნაშავედ იცნობა კომპიუტერულ თაღლითობაში.[110]

ესტონეთის სისხლის სამართლის კოდექსის მიხედვით, კომპიუტერული დანაშაულები გაერთიანებულია ისეთ ქვეთავებში, როგორებიცაა: უკანონო მოხმარება, თაღლითობა, დანაშაული ინტელექტუალური საკუთრების წინააღმდეგ.[111] ლიტვაში იგი მოთავსებულია ისეთ თავებში, როგორებიცაა საკუთრების წინააღმდეგ მიმართული სისხლის სამართლის დანაშაულები და საზოგადოებრივი წესრიგისა და უსაფრთხოების წინააღმდეგ მიმართული სისხლის სამართლის დანაშაულები.

განსხვავებული მიდგომაა ლიეტუვაში. კერძოდ, ლიეტუვის სისხლის სამართლის კოდექსში კომპიუტერულ დანაშაულს ცალკე თავი ეთმობა - „ელექტრონულ მონაცემთა და საინფორმაციო სისტემის უსაფრთხოების წინააღმდეგ მიმართული დანაშაულები“.[112]

---

[109] *Л.В. Головко, Н.Е. Крыловой; пер. с фр. Н.Е. Крыловой*, Уголовный кодекс Франции / науч. ред. СПб.: Юрид. центр Пресс, 2002, 650

[110] იხ. დანიის სისხლის სამართლის კოდექსი ელ. ბმული:

[111] მაგალითად, ესტონეთის კოდექსის მეორე თავში, რომელიც აწესრიგებს ყველა ტიპის საკუთრების წინააღმდეგ მიმართულ დანაშაულებს, მაგალითად პირველ ქვეთავში მოცემულია თაღლითობა, 213-ე მუხლი აწესრიგებს კომპიუტერთან დაკავშირებულ თაღლითობას, რაც გულისხმობს სხვა პირისთვის ქონებრივი ზიანის მიყენება კომპიუტერულ პროგრამებზე ან მონაცემებზე უკანონო შეღწევის, შეცვლის, წაშლის, დაზიანების ან დაბლოკვის გზით, ან სხვა უკანონო ჩარევა სხვისი საკუთრებით სარგებლობის მიზნით.

[112] ლიეტუვის სსკ-ს 30-ე თავი: დასახელებული თავი მოიცავს ისეთ დანაშაულებს, როგორებიცაა: მონაცემებში უკანონო ჩარევა; სისტემაში უკანონო ჩარევა; ელექტრონული მონაცემების უკანონოდ მოპოვება და გამოყენება; საინფორმაციო სისტემაში არაავტორიზებული შეღწევა და პროგრამის

შესაბამისად, გამიჯნულია ტრადიციულისგან ციფრული დანაშაული. აქვე, როგორც საქართველოს კანონმდებლობაში, ცალკე დანაშაულად გამოყოფილია მომზადების ეტაპი, როდესაც პირი დანაშაულებრივი მიზნებისთვის უკანონო საშუალებებს აწარმოებს, ინახავს, იყენებს, ხელმისაწვდომს ხდის და ა.შ. და ეს საშუალება პირდაპირ არის გამიზნული ან ადაპტირებული დანაშაულებრივი ქმედებების ჩასადენად, ასევე, უკანონოდ იყენებს პაროლებს, კოდებს ან სხვა მსგავს მონაცემებს, რომლებიც განკუთვნილია საინფორმაციო სისტემის რომელიმე ნაწილთან ან მთლიანად სისტემასთან დასაკავშირებლად.[113]

საინტერესოა მიდგომა ისრაელისა, რომლის კანონმდებლობაში კომპიუტერული დანაშაული, ტრადიციული დანაშაულისგან ცალკე არის გამოყოფილი მხოლოდ ცალკეულ შემთხვევებში. ეს ის შემთხვევებია, როდესაც დანაშაული ექსკლუზიურად კიბერსივრცეში ხდება, მაგალითად, ასეთია DoS-თავდასხმის შემთხვევა. თუმცა „ფიშინგი“ კვალიფიცირდება ელექტრონულ სივრცეში ჩადენილ ქურდობად ან თაღლითობად.[114] მიუხედავად იმისა, რომ კიბერსივრცეში ჩადენილი დანაშაულია, ტრადიციული დანაშაულისთვის განკუთვნილი მუხლების ფარგლებში ექცევა. [115]

რაც შეეხება რუსეთის ფედერაციის სისხლსამართლებრივ ნორმებს, ინტერნეტტექნოლოგიებთან დაკავშირებული ქურდობის სახეები ამოწურულია თაღლითობის მუხლში და განსაზღვრულია საკუთრების წინააღმდეგ მიმართულ კოდექსის თავში,[116] თუმცა კოდექსი ითვალისწინებს ცალკე დამოუკიდებელ თავს, სადაც წესრიგდება კიბერდანაშაული. [117]

განსხვავებით მასთან მსგავსი სამართლებრივი სისტემის მქონე ქვეყანასთან - კერძოდ, მოლდოვისაგან, სადაც „ინფორმაციული თაღლითობის“ დაცვის ობიექტს წარმოადგენს არა საკუთრებითი უფლება, არამედ კომპიუტერულ სისტემაში მოთავსებული, მიღებული და დამუშავებული ინფორმაცია.[118] ასეთი მიდგომა სავსებით

ინსტალაციების, პროგრამული უზრუნველყოფის, პაროლების, კოდებისა და სხვა მონაცემების უკანონო განკარგვა.

[113] მუხლი 198². პროგრამის ინსტალაციების, პროგრამული უზრუნველყოფის, პაროლების, კოდებისა და სხვა მონაცემების უკანონო განკარგვა

[114] ისრაელის სისხლის სამართლის 415-416 მუხლები.

[115] 1995 წლის კანონი „კომპიუტერების შესახებ“

[116] მაგალითად, თაღლითობა კომპიუტერული ინფორმაციის სფეროში, რომელიც წესრიგდება 159-ე მუხლით

[117] რუსეთის ფედერაციის სისხლის სამართლის კოდექსის 28-ე თავში მოცემულია დანაშაულები კომპიუტერულ ინფორმაციის სფეროში. მაგალითად, დასჯადია კანონით დაცულ კომპიუტერულ სისტემაში არამართლზომიერი შეღწევა, თუ ეს ქმედება იწვევს კომპიუტერული ინფორმაციის განადგურებას, ბლოკირებას, შეცვლას ან კოპირებას (272-ე მუხლი), მავნე კომპიუტერული პროგრამების შექმნა, გამოყენება და გავრცელება (273-ე მუხლი), საინფორმაციო-სატელეკომუნიკაციო ქსელებისა და კომპიუტერული ინფორმაციის დამუშავების ან გადაცემის, საექსპლუატაციო საშუალებების შენახვის წესების დარღვევა (274-ე მუხლი).

[118] Маймеску С. Информационные преступления и преступления в области электросвязи, Комментарий к Уголовному кодексу Республики Молдова. Общая и Особенная части. Кишинэу, 2010,. 792—794.

ლოგიკურია, რადგან, ერთი მხრივ, თაღლითობის დანაშაულის მიზანიაფინანსური სარგებლის მიღება, იქნება ეს ფულის, საგნის ან სხვა რაიმე ღირებულების მატარებელი ნივთი. ხოლო მონაცემების უკანონო შეყვანის, შეცვლის ანდა წაშლის, მათთან წვდომის შეზღუდვის დროს ჩარევა ხდება კომპიუტერული მონაცემების მთლიანობაში. აღნიშნულ მოსაზრებას იზიარებენ მოლდაველი მეცნიერები, რომლებიც ამბობენ, რომ კიბერთაღლითობა შეიძლება ჩადენილ იქნას პასიურად, ვირუსის გამოყენებით.[119]

შუალედური დასკვნა

კიბერდანაშაულის წინააღმდეგ ბრძოლის სისხლისსამართლებრივი ღონისძიებების შედარებით-სამართლებრივი ანალიზის შეჯამებით, უნდა აღინიშნოს, რომ ინფორმაციული უსაფრთხოების დამრღვევი ქმედებების კრიმინალიზაციის მიდგომა თითოეული სახელმწიფოს სისხლის სამართლის კანონმდებლობაში ინდივიდუალურია და განსხვავებულია დანაშაულის ობიექტის, ქმედებების სახეების დადგენისა და ამგვარი დანაშაულის ჩადენის გზების ჩამოთვლით.

ანალიზით დადგინდა, რომ სამართლებრივად დაცული სიკეთე შეიძლება იყოს არა მარტო კომპიუტერული ინფორმაციის უსაფრთხო მიმოქცევა, არამედ სხვა ობიექტებიც. მაგალითად, ადამიანის უფლებები და თავისუფლებები, როგორც დიდი ბრიტანეთის, საფრანგეთისა და გერმანიის კანონმდებლობებში არის მოწესრიგებული, თავისუფლება და საზოგადოებრივი უშიშროება - შვედეთის სისხლის სამართლის კოდექსში, ეროვნული უსაფრთხოება - აშშ სისხლის სამართლის სამართალში, საზოგადოებრივი წესრიგი და საზოგადოებრივი უსაფრთხოება - ლატვიის სისხლის სამართლის კოდექსში და ა.შ.

ანალიზის საფუძველზე შეგვიზლია გამოვყოთ 3 მიდგომა კომპიუტერული დანაშაულების მოწესრიგების კუთხით: (1) კომპიუტერული დანაშაული ინტეგრირებულია კლასიკური დანაშაულის შემადგენლობაში, როგორც სხვა დანაშაულის ჩადენის საშუალება, (2) კომპიუტერული დანაშაულის გამოცხადებულია დამოუკიდებელ დანაშაულად და მომწესრიგებელ კანონდებლობაში ცალკე გამოყოფა და (3) ჰიბრიდული მეთოდი, როდესაც იგი არის როგორც ტრადიციულ დანაშაულებში ინტეგრირებული, ასევე ცალკე შემადგენლობად გამოყოფილი.

ამ მხრივ, მიუხედავად ზემოთხსენებული სხვაობებისა, მათ შორის მაინც იგრძნობა კანონზომიერება, კერძოდ ინფორმაციული უსაფრთხოების ხელყოფა აღარ არის ამოფარებული სხვა სამართლებრივი სიკეთეების ქვეშ, ის გასცდა სისხლის სამართლის ნორმების მხოლოდ ერთი ჯგუფის - ე.წ. „ტრადიციული“ დანაშაულების ფარგლებს. კიბერტექნოლოგიების სწრაფმა განვითარებამ წინასწარ განსაზღვრა მათი, როგორც მეთოდების, საშუალებების ან დანაშაულის ფორმირების ნიშნების, კრიმინალიზაციის აუცილებლობა.

[119] იხ.: *Дмитришен М, Гончаров И.*, Мошенничество в информационных технологиях.

თავი III. საქართველოში კიბერდანაშაულის მატერიალურ-სამართლებრივი მოწესრიგება და პრაქტიკაში არსებული გამოწვევები

საქართველოს სისხლის სამართლის კოდექსის XXXV თავი აწესრიგებს კიბერდანაშაულის კრიმინალიზაციას, კერძოდ, კომპიუტერულ სისტემაში უნებართვო შეღწევას (სსკ-ს 284-ე მუხლი), კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის ან დაშვების კოდის უნებართვო გავრცელებას (სსკ-ს 285-ე მუხლი), კომპიუტერული სისტემის ანდა კომპიუტერული მონაცემის უნებართვო დაზიანებას (სსკ-ს 286-ე მუხლი), ასევე, გვხვდება ორი ახალი დამატებითი მუხლი, რომელიც შევიდა სისხლის სამართლის კოდექსის 2021 წლის ცვლილებების საფუძველზე, ესენია: კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით (286[1]-ე მუხლი) და ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნა (286[2]-ე მუხლი).[120]

კომპიუტერთან დაკავშირებული თაღლითობა და გაყალბება, როგორც წინა თავებში აღინიშნა, ბუდაპეშტის კონვენციის მიხედვით, წარმოადგენენ კომპიუტერთან დაკავშირებულ დანაშაულთა სახეს, რომლებიც მოწესრიგებულია მე-7 და მე-8 მუხლებით. გაყალბება და თაღლითობა არის ტრადიციული სისხლის სამართლის დანაშაულები, სადაც კომპიუტერული სისტემები გამოიყენება, როგორც ინსტრუმენტები კიბერსივრცეში დანაშაულთა ჩასადენად.[121] მათი პრაქტიკული მნიშვნელობა არის განპირობებული, რადგან ტრადიციული დანაშაულების მომწესრიგებელი ნორმები საკმარისად ვერ უზრუნველყოფენ სამართლებრივი ინტერესების დაცვას თავდასხმების ახალი ფორმებისგან.

სწორედ ტრადიციული და კიბერდანაშაულების ერთმანეთისგან გამიჯვნისა და ბუდაპეშტის კონვენციასთან ჰარმონიზაციის მიზნით, საქართველოს სისხლის სამართლის კოდექსში დაემატა სსკ-ს XXXV თავს ახალი 286[1] და 286[2] მუხლები. უფრო ზუსტად, 286[1] მუხლი - კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით, წარმოადგენს საკუთრების წინააღმდეგ მიმართული დანაშაულის სპეციალურ შემთხვევას, ხოლო სსკ. 286[2] მუხლი - ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნა - ყალბი დოკუმენტის დამზადების, გასაღების ან გამოყენების სპეციალურ სახეს.[122]

2021 წლის 27 აპრილის საკანონმდებლო ცვლილებების განმარტებით ბარათში აღნიშნულია, რომ ცვლილებების ინიცირების საფუძველი გახდა დანაშაულთა

---

[120] გარდა სპეციალური თავისა, კოდექსის სხვადასხვა თავებში მოწესრიგებულია სხვა კომპიუტერთან დაკავშირებული დანაშაულები, როგორებიცაა, მაგალითად, პორნოგრაფიული ნაწარმოების ან სხვა საგნის უკანონოდ დამზადება ან გასაღება (სსკ-ს 255[1]-ე მუხლი), პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა (სსკ-ს 159-ე მუხლი), კიბერტერორიზმი და ა.შ., რომლებიც მოცემულია ტრადიციული დანაშაულთა თავში.

[121] *Schjolberg S.,* Computer-related offences, 2004, 6;

[122] *საქართველოს შინაგან საქმეთა სამინისტრო.* განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის კოდექსში ცვლილების შეტანის შესახებ“, 2;

ხელოვნური ერთობლიობის თავიდან აცილება და კლასიკური დანაშაულების სპეციალური შემთხვევების მოწესრიგება.[123] სასამართლო პრაქტიკის მიხედვით, თუ პირი სხვისი ანგარიშიდან თანხას უკანონოდ დაეუფლება, ქმედება კვალიფიცირდება საქართველოს სისხლის სამართლის კოდექსის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 177-ე (ქურდობა) მუხლების ერთობლიობით.

მოცემულ ნაშრომში უცხოური საკანონმდებლო მოწესრიგების მოდელების მიმოხილვით, ერთ-ერთ პრობლემას წარმოადგენდა მატერიალური სარგებლის მიღების მიზნით ჩადენილი ტრადიციული დანაშაულების გამიჯვნა ფინანსურად მოტივირებული კიბერდანაშაულებისგან. მიმოხილული ანალიზის საფუძველზე, შესაძლოა ითქვას, რომ საქართველოს აქვს არჩეული ჰიბრიდული მოდელი, რომლის მიხედვით, სპეციალური თავი ეძღვნება კიბერდანაშაულის მოწესრიგებას, ასევე ცალკეულ მუხლებშიც არის სინთეზირებული.[124] კომპიუტერული დანაშაული სპეციფიკიდან გამომდინარე, რთულია, ზოგიერთი ქმედება მოვაქციოთ მხოლოდ კიბერდანაშაულის მოწესრიგების სფეროში, შესაძლოა, მასში არსებობდეს კიბერელემენტები, თუმცა, საბოლოოდ, კიბერდანაშაულად არ ჩაითვალოს და ტრადიციული ქმედების შემადგენლობის ფარგლებში ჯდებოდეს.

ასევე, პრობლემურია ერთი და იმავე ხერხით ჩადენილი კიბერდანაშაულების კვალიფიკაცია, მაგალითად, სსკ. 286[1] და 286[2] მუხლების ნორმათა კონკურენციის არსებობის პირობებში. განსაკუთრებით, 286[2] მუხლის იდენტიფიცირების პრობლემაა, რაზეც მეტყველებს საქართველოს შინაგან საქმეთა სამინისტროდან გამოთხოვილი სტატისტიკური მონაცემების ანალიზი. შსს საინფორმაციო-ანალიტიკური დეპარტამენტის საინფორმაციო ცენტრის მიერ მოწოდებული სტატისტიკური მონაცემების მიხედვით, 2021 წლიდან (საკანონმდებლო ცვლილებების მიღებიდან) 2022 წლის მაისის ჩათვლით გამოძიება დაიწყო 286[2] მუხლით მხოლოდ და მხოლოდ 2 საქმეზე. საკვირველია, რადგან ოფიციალური კომპიუტერული მონაცემის გაყალბება წარმოადგენს ერთ-ერთ ყველაზე გავრცელებულ დანაშაულს, მაგალითად, ვებ-გვერდის სიმულაცია და ა.შ. სტატისტიკური მონაცემები ცხადყოფს, რომ მუხლის სწორი შეფასება დანაშაულთა კვალიფიკაციის მიზნებისთვის არ ხდება.

მოცემული თავის მიზანია 2021 წლის 24 აპრილის საქართველოს კანონით მიღებული მნიშვნელოვანი ცვლილებების მიმოხილვა და პრაქტიკაში წარმოშობილი პრობლემების ანალიზი, ასევე მსგავსი ქმედებებითა და ხერხებით ჩადენილი ფინანსურად მოტივირებული კიბერდანაშაულის კვალიფიკაციის პრობლემების მიმოხილვა და რეკომენდაციების შემოთავაზება.

[123] იქვე.
[124] მაგალითად, კიბერტერორიზმი.

3.1. საქართველოს სისხლის სამართლის კოდექსის 286[1] მუხლის კვალიფიკაციის საკითხები

3.1.2. საქართველოს სისხლის სამართლის კოდექსის 286[1] მუხლის ქმედების შემადგენლობა

საქართველოს სისხლის სამართლის კოდექსის 286[1] მუხლი „კომპიუტერული მონაცემის ან/და სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით“ - გულისხმობს კომპიუტერულ სისტემაში უნებართვო შეღწევას, კომპიუტერული მონაცემის უნებართვო ჩასმას, წაშლას, შეცვლას ან დაფარვას, ასევე, გარდა ამ ქმედებებისა, ნებისმიერი სახის უნებართვო ჩარევას კომპიუტერული სისტემის ფუნქციონირებაში. კვალიფიკაციისათვის აუცილებელია, რომ მატერიალური გამორჩენის მიზანი ჰქონდეთ („თავისთვის ან სხვისთვის ქონებრივი უფლების მოპოვების ან ნებისმიერი სახის ფინანსური სარგებლის მიღების მიზნით“) და, რადგან მუხლი მატერიალური შემადგენლობისაა, იწვევდეს სხვისთვის ფინანსური ზიანის მიყენებას.

მუხლის კრიმინალიზაციის მიზანია, დასჯადად გამოაცხადოს მონაცემთა ნებისმიერი არამართლზომიერი მანიპულირება, მონაცემთა დამუშავების პროცესში ჩარევა, ფინანსური სარგებლის მიღების მიზნით.[125]

ფინანსური სარგებლის მიზნით კომპიუტერული სისტემის ხელყოფა შინაარსობრივად შეესაბამება ბუდაპეშტის კონვენციის მე-7 მუხლს, რომელიც შეეხება კომპიუტერთან დაკავშირებულ თაღლითობას.[126] კონვენციის მსგავსად, 286[1] მუხლი იტვალისწინებს დანაშაულის ცადენის მსგავს ხერხებს, კერძოდ, კონვენციის მე-8 მუხლის “a” პუნქტში გათვალისწინებულია კომპიუტერული მონაცემის უნებართვო ჩასმა, წაშლა, შეცვლა ან დაფარვა და “b” ქვეპუნქტში წარმოადგენილია კომპიუტერულ სისტემაში „ნებისმიერი სახის უნებართვო ჩარევა“. მართალია, ეს უკანასკნელი საკმაოდ ფართო ინტერპრეტაციის საშუალებას იძლევა, თუმცა ბუდაპეშტის კონვენციის განმარტებით ანგარიშში მითითებულია, რომ ასეთი ფართო მნიშვნელობის ტერმინი დაეხმარება ქვეყნებს მოიცვას ყველა შესაძლო კომპიუტერულ მონაცემთა მანიპულაციების შემთხვევები, მათი კრიმინალიზაციის მიზნით.[127] ასეთად შეიძლება ჩაითვალოს მოწყობილობების მანიპულაციები, ქმედებები, რომლებიც გავლენას ახდენენ მონაცემთა მიმოსვლაზე ან პროგრამების გაშვების თანმიმდევრობაზე და ა.შ.[128]

დაცვის ობიექტი

კომპიუტერული თაღლითობის ქმედებების განსაზღვრაში გადამწყვეტი როლი ეკუთვნის მისი ჩადენის საშუალებას - კომპიუტერულ სისტემას. კონვენციის მიხედვით,

[125] 86-ე პუნქტი.
[126] ბუდაპეშტის კონვენციის 8(b) პუნქტი.
[127] 87-ე პუნქტი
[128] 87-ე პუნქტი

კომპიუტერული სისტემა არის მოწყობილობა, რომელიც შედგება მოწყობილობისა და პროგრამული უზრუნველყოფისგან, და რომელიც შექმნილია ციფრული მონაცემების ავტომატური დამუშავებისთვის. ის შეიძლება მუშაობდეს ავტომატურად ან ქსელით იყოს დაკავშირებული სხვა მსგავს მოწყობილობებთან.

ქსელი არის ურთიერთკავშირი ორ ან მეტ კომპიუტერულ სისტემას შორის. ქსელი შეიძლება გეოგრაფიულად შემოიფარგლოს მცირე ფართობით (ლოკალური ქსელები) ან შეიძლება მოიცავდეს დიდ არეალს (ფართო არეალის ქსელები) და ასეთი ქსელები თავად შეიძლება იყოს ერთმანეთთან დაკავშირებული. ინტერნეტი არის გლობალური ქსელი, რომელიც შედგება მრავალი ურთიერთდაკავშირებული ქსელისგან, ყველა ერთი და იმავე პროტოკოლის გამოყენებით.[129]

რაც შეეხება "ავტომატურს" - ეს ნიშნავს, ადამიანის უშუალო ჩარევის გარეშე, მოქმედებას. "მონაცემების დამუშავება" ნიშნავს, რომ კომპიუტერულ სისტემაში მონაცემების მართვა ხდება კომპიუტერული პროგრამის შესრულებით.[130] საქართველოს სისხლის სამართლის კოდექსი მსგავს ტერმინის დეფინიციას გვთავაზობს 284-ე მუხლის შენიშვნის პირველ ნაწილში,[131] რომელიც მთლიანად შეესაბამება ბუდაპეშტის კონვენციასთან.[132]

პროგრამული უზრუნველყოფა - არის ინსტრუქციების ერთობლიობა, რომელიც შეიძლება შესრულდეს კომპიუტერის მიერ დასახული შედეგის მისაღწევად. შეიძლება ჩაითვალოს როგორც კომპიუტერული სისტემის ნაწილად, ასევე დამოუკიდებლად, როგორც კომპიუტერული სივრცე.

აქედან გამომდინარე, ამ ურთიერთობის ძირითადი ობიექტებია კომპიუტერები, კომპიუტერული სისტემები და სატელეკომუნიკაციო ქსელები. ტრადიციული თაღლითობის შემთხვევაში, საგანი იდენტიფიცირებულია ქონებრივი ურთიერთობის საგანთან, რადგან ირღვევა სოციალური კავშირი, ქონებრივი უფლების განხორციელების ნორმალური პროცედურა. თაღლითობის ჩადენის შემდეგ, თაღლითი იძენს საკუთრების უფლებას საგანზე.

იურიდულ ლიტერატურაში აღნიშნულია, რომ კომპიუტერთან დაკავშირებული თაღლითობს ხელყოფის ობიექტს წარმოადგენს საკუთრების საგანი, რადგან ამ ურთიერთობაში კავშირი მდგომარეობს კომპიუტერების, სისტემების და კომპიუტერული და სატელეკომუნიკაციო ქსელების ნორმალურ ფუნქციონირებაში.[133]

---

[129] ბუდაპესტის კონვენციის განმარტებითი ანგარიში, ევროპის საბჭო, 24-ე პუნქტი.

[130] იქვე, 23-ე პუნქტი.

[131] „კომპიუტერული სისტემა არის ნებისმიერი მოწყობილობა/მექანიზმი ან ერთმანეთთან დაკავშირებულ მოწყობილობათა/მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის, პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, მობილური ტელეფონი)“

[132] Council of Europe, Convention on Cybercrime, Budapest, 2001, article 1. ხელმისაწვდომია ბმულზე https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 [12.05.2022].

[133] *Kryshevych O., Andrushchenko I., Striltsiv O., Pyvovar Y., Rivchachenko O.,* Modern methods of computer-related fraud: legal characteristics and qualification, jour. Cuestiones Politicas, Vol. 39 № 68, 2021), 856

ამ მოსაზრების მიხედვით, კომპიუტერთან დაკავშირებული თაღლითობის ჩადენისას ხელყოფის ობიექტია არა კომპიუტერული სისტემების და კომპიუტერული და სატელეკომუნიკაციო ქსელების ნორმალურ ფუნქციონირება, არამედ ქონებრივი ურთიერთობები, ფული და სხვა ფასეულობები, მისაკუთრების მიზნით.[134] აღნიშნულ მოსაზრებას ვერ დავეთანხმები, რადგან ისეთი ხერხები, როგორებიცაა მონაცემთა უნებართვო წაშლა, შეცვლა ხელყოფს მონაცემთა მთლიანობას,[135] ასევე, სხვაგვარი უნებართვო შეღწევაც ხელყოფს კომპიუტერული სისტემის კონფიდენციალობას, მის მთლიანობას და ხელმისაწვდომობას.

ამრიგად, სამართლებრივ სიკეთეს წარმოადგენს, ერთი მხრივ, კომპიუტერული სისტემისა და მონაცემების უსაფრთხოება, მისი კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა, ხოლო დანაშაულის საგანია ის კომპიუტერული მონაცემი, რომლის უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვა ექვემდებარება ხელყოფას. ასევე, ის კომპიუტერული სისტემა, რომელშიც მოხდა უნებართვო შეღწევა და მის ფუნქციონირებაში ჩარევა.[136]

რაც შეეხება ქმედებებს, მიმოვიხილოთ დანაშაულის განხორციელების ხერხი ცალ-ცალკე.

კომპიუტერულ სისტემაში უნებართვო შეღწევა.

ქმედების შემადგენლობის ერთ-ერთი ხერხს წარმოადგენს კომპიუტერულ სისტემაში უნებართვო შეღწევა, რომელსაც, ძირითადად, მოსდევს სხვა კიბერდანაშაულის ჩადენაც. აღნიშნული ქმედება არის ძალიან ხშირი პრაქტიკაში, განსაკუთრებით, ფინანსური სარგებლის მიღების მიზნით, მაგალითად, ონლაინკაზინოს ანგარიშებზე უნებართვო შეღწევა.[137] კომპიუტერულ სისტემაში უნებართვო შეღწევაა უნდა გავიგოთ, როგორც მოცემულია 284-ე მუხლის დისპოზიციაში და მის შენიშვნაში. იურიდიულ ლიტერატურაში გამოთქმულია საინტერესო მოსაზრება ტერმინთან დაკავშირებით, რომ ტერმინი „შეღწევა“ ტექნიკურად არ შეესაბამება რეალობას და გამოყენებული უნდა იყოს სიტყვა „წვდომა“.[138]

მოსაზრების ავტორი მიიჩნევს, რომ სიტყვა „შეღწევა“ ტექნიკურად გულისხმობს „დაცვის სისტემის გადალახვას, რა დროსაც წვდომის შემთხვევაში მნიშვნელოვანია პირს ჰქონდეს „კონტროლის“ შესაძლებლობა, ე.ი. კომპიუტერულ სისტემაზე თავისი

---

[134] *Kryshevych O., Andrushchenko I., Striltsiv O., Pyvovar Y., Rivchachenko O.,* Modern methods of computer-related fraud: legal characteristics and qualification, jour. Cuestiones Politicas, Vol. 39 № 68, 2021), 857-858

[135] ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013, 60.

[136] იქვე.

[137] სტატისტიკა იხ. https://info.police.ge/page?id=115 [18.05.2022].

[138] „კიბერდანაშაულის შესახებ“ ევროსაბჭოს კონვენციის მე-2 მუხლის მიხედვით, გათვალისწინებულია კომპიუტერულ სისტემაზე „წვდომა“ (Access).

შეხედულებების მიერ განახორციელოს სხვადასხვა მოქმედებები.[139] ტექნიკური სხვაობის თვალსაჩინოებისთვის მოცემულია მაგალითად, თუ პირს დარჩა სოციალური ქსელი გახსნილი სხვის ტელეფონში და დაავიწყდა პირადი ანგარიშიდან გამოსვლა, ხოლო სხვა პირმა ისარგებლა ამით და შევიდა მის სოციალურ ანგარიშში, ამით მას არ გადაულახავს დაცვის ბარიერი, მან უბრალოდ გამოიყენა შესაძლებლობა და განახორციელა წვდომა პირის პირად ანგარიშზე.[140]

კომიუტერულ ისტემაში უნებართვო შეღწევად ჩაითვლება, როდესაც ბოროტმოქმედი დისტანციურად ახროციელებს სხვა ლოკაციიდან კომპიუტერულ სისტემაზე წვდომას, ასევე ლოკალური ქსელის გამოყენებით ან უშუალო კომპიუტერულ სისტემასთან დიზიკური შემხბლობით განახორციელებს წვდომას.[141]

რაც შეეხება უნებართვოს, კომპიუტერულ სისტემაში შეღწევა აუცილებლად დანაშაულად მიჩნევისათვის, უნდა განხორციელდეს უნებართვოდ. მუხლის შენიშვნის მიხედვით, უნებართვო გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისათვის. ამგვარად, სსკ-ის 284-ე მუხლის ძველი რედაქციისგან განსხვავებით, იმისათვის რომ ქმედება დანაშაულად ჩაითვალოს არსებითია არა ის, თუ რამდენადაა კანონით დაცული ინფორმაცია, რომელშიც ხორციელდება შეღწევა, არამედ ის, რომ განხორციელდა მოქმედება - კომპიუტერულ სისტემაში უნებართვო შეღწევა.[142]

დანაშაულის ჩადენის სხვა ხერხები

შეღწევის გარდა, ფინანსური სარგებლის მიზნით კომპიუტერული სისტემის ხელყოფა შესაძლებელია კომპიუტერული მონაცემის უნებართვო ჩასმით, წაშლით, შეცვლით ან დაფარვით, ასევე, კომპიუტერულ სისტემას სხვა ნებისმიერი ჩარევის გზით. განვიხილოთ თითოეული ქმედება ცალ-ცალკე.

მონაცემთა ჩასმა გულისხმობს სწორი ან არასწორი მონაცემების უნებართვო „შეყვანას“ სისტემაში. მონაცემთა წაშლა - მონაცემის განადგურებას, როდესაც მისი აღქმა შეუძლებელია, მათ ამოღებას მონაცემთა შენახვის საშუალებიდან. მაგალითად, მონაცემი გადატანილია სხვა კომპიუტერში, თუმცა აღარ მოიძებნება იმ კომპიუტერულ

---

[139] იხ.: პირველი, გ., „კიბერდანაშაულის შესახებ“ ევროპულ კონვენციასთან საქართველოს სისხლის სამართლის კანონმდებლობის შეუსაბამობით გამოწვეული პრობლემები, სამეცნიერო ჟურნ. „პოლიცია და უსაფრთხოება“, თბ., 2018, №1,67.

[140] იქვე

[141] პირველი,გ., საინფორმაციო ტექნოლოგიების გამოყენებით ჩადენილ დანაშაულთა კრიმინოლოგიური ანალიზი, თბ., 2017, 22.

[142] ლეკვეიშვილიმ., თოდუა, ნ., მამულაშვილი, გ., სისხლის სამართლის კერძო ნაწილი, ნაწილი II, თბ., 2019, 192-193. ამ კუთხით აშშ-ში განსხვავებული მიდგომაა დამკვიდრებული, კერძოდ, ქმედების დანაშაულად კვალიფიკაციისთვის აუცილებელია დადგინდეს არა შეღწევის უნებართვო ხასიათი, არამედ დამნაშავის მიზანი, რომელიც უნდა შეიცავდეს ზოგადად ზიანის მიყენების სურვილს და არაა აუცილებელი რაიმე კონკრეტული ზიანი მიყენების მიზნის დადგენა. იხ.: უ.ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013, 43.

სისტემაში, სადაც ინახებოდა. ასეთი შემთხვევა იქნება წაშლა, თუნდაც იმ შემთხვევაში, რომ სრულად არ იყოს განადგურებული და მისი მოძიება შეიძლებოდეს.[143] იმ შემთხვევაში, თუ წაშლილი ფაილების აღდგენა შესაძლებელი იქნება, მაგალითად, პროგრამული უზრუნველყოფის გამოყენებით, წაშლა მაინც სახეზე იქნება.[144]

შეცვლა - უკვე არსებული მონაცემების მოდიფიკაციას გულისხმობს. გულისხმობს როგორ სრულ, ასევე ნაწილობრივ მოდიფიკაციას. მაგალითად, „ვირუსების“, „ტროას ცხენების“ გამოყენებით.[145]

მონაცემთა დაფარვა - ვფიქრობ უფრო სწორი იქნება ტერმინი მონაცემთა „ბლოკირება“. ბუდაპეშტის კონვენციის განმარტებითი ანგარიშის მიხედვით, სახეზე გვაქვს მონაცემთა შეკავების, მონაცემთა დამალვის მაგალითები. შინაარსობრივად კი გულისხმობს ნებისმიერ ქმედებას, რომელიც პირს ხელს უშლის ან უწყვეტს მონაცემებთან წვდომას, ამიტომ ლოგიკური განმარტებაა ბლოკირება. დაფარვაში იგულისხმება ასევე ფაილის დაშიფვრა, რის გამოც ფაილი ხელმიუწვდომელი ხდება მისი მფლობელისთვის.[146]

ზემოთ ხსენებული ქმედებები უნდა იყოს ჩადენილი უნებართვოდ, რათა ჩაითვალოს დანაშაულად, სხვა შემთხვევაში ვერ იქნება ქმედება კრიმინალიზებული, რადგან ამ ხერხების გამოყენება შესაძლებელია ლეგალური მიზნებისთვისაც, მაგალითად, მონაცემთა მოდიფიკაცია უსაფრთხო კომუნიკაციის მიზნით (მაგ. დაშიფვრა).

„კომპიუტერულ სისტემაში ნებისმიერი სახის უნებართვო ჩარევა“ - როგორც უკვე აღენიშნა, ეს ქმედება ფართო ინტერპრეტაციის საშუალებას იძლევა, ასეთად შეიძლება ჩაითვალოს მოწყობილობების მანიპულაციები, ქმედებები, რომლებიც გავლენას ახდენენ მონაცემთა მიმოსვლაზე ან პროგრამების გაშვების თანმიმდევრობაზე და ა.შ.[147]

3.1.2. პრაქტიკაში არსებული გამოწვევები

როგორც უკვე არაერთხელ აღინიშნა, კომპიუტერთან დაკავშირებული თაღლითობა მჭიდროდ არის დაკავშირებული ტრადიციულ თაღლითობასთან. მთავარი საერთო, რაც აქვს თაღლითობას და კომპიუტერთან დაკავშირებულ თაღლითობას, არის დანაშაულის განხორციელების ხერხი, ეს არის მოტყუება ან ნდობის ბოროტად გამოყენება. კომპიუტერთან დაკავშირებული თაღლითობა, მიუხედავად მისი ევოლუციური განვითარებისა, პრაქტიკაში მაინც რჩება საკუთრების წინააღმდეგ მიმართულ დანაშაულის კატეგორიაში, მიუხედავად არსებული განსხვავებებისა.

---

[143] ზაქაშვილი, უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013, 64;

[144] პირველი, გ., საინფორმაციო ტექნოლოგიების გამოყენებით ჩადენილ დანაშაულთა კრიმინოლოგიური ანალიზი, თბ., 2017, 29.

[145] 61-ე პუნქტი

[146] იქვე.

[147] 87-ე პუნქტი

თაღლითობა, რომელიც ჩადენილია უახლესი ტექნოლოგიების გამოყენებით, ხასიათდება მრავალფეროვანი ფორმებითა და მეთოდებით. თუმცა, საქართველოს სისხლის სამართლის კოდექსის 180-ე მუხლი არ ასახავს თაღლითობის ჩადენის ყველა შესაძლო გზას კომპიუტერული ტექნიკის, ინტერნეტის, მობილური კავშირის გამოყენებით და ა.შ. მაგალითად, არ ითვალისწინებს, ფასიანის ზარის გაშვების მიუხედავად, აბონენტის ანგარიშიდან თანხის ანებართვო ჩამოჭრას და ა.შ.

განსხვავება ტრადიციული თაღლითობისგან მდგომარეობს შემდეგში, რომ ტყუილი და ნდობაში შესვლა ხორციელდება კომპიუტერული ტექნოლოგიების უპირატესობების გამოყენებით, ე.ი. დისტანციურად, დანაშაულის სამიზნესთან პირდაპირი კონტაქტის გარეშე (კიბერ მეთოდით ჩადენილი თაღლითობა). თაღლითური მოტყუების არსი უცვლელი რჩება, ერთადერთი ის არის, რომ თაღლითობა ხდება ელექტრონული კომპიუტერებისა და ტექნოლოგიების გამოყენებით, რაც მოითხოვს უფრო დახვეწილ და ინოვაციურ ტექნიკასა თუ უნარებს. დანაშაულის მომეტებული საზოგადოებრივი საშიშროება განპირობებულია სწორედ დანაშაულის განხორციელების სიმარტივითა და მისი დაფარვის მარტივი საშუალებით.[148] ეს ისეთი შემთხვევაა, როდესაც თაღლითობის დროს ინტერნეტ ტექნოლოგიების გამოყენება შესაძლებელია ლეგიტიმური იყოს და არ მოხდეს მონაცემებში პირდაპირი ჩარევა.[149] მესამე შემთხვევას თაღლითობის წარმოადგენს უშუალოდ სისტემაში ჩარევა, როდესაც სახეზეა სისტემის მოტყუება, რომელიც თაღლითობისგან და კიბერ მეთოდით ჩადენილი თაღლითობისგან განსხვავებულ შეფასება საჭიროებს.

ამრიგად, კომპიუტერთან დაკავშირებული თაღლითობა შეგვიძლია დავყოთ:

- კიბერთაღლითობა თანხების მითვისების მიზნით.
- კიბერთაღლითობა ინფორმაციის მოპოვების მიზნით (პირადი გამოყენების ან გადაყიდვის მიზნით).[150]

განვიხილოთ კომპიუტერთან დაკავშირებული თაღლითობის პრაქტიკაში გავრცელებული შემთხვევები და არსებული სასამართლოს მიდგომა.

კომპიუტერთან დაკავშირებული თაღლითობის ერთ-ერთი გავრცელებული შემთხვევაა ქონების მისაკუთრება ცრუ ინფორმაციის მიწოდების გზით, რა დროსაც დამნაშავე იყენებს კომპიუტერულ სისტემას. მაგალითად, ეს შეიძლება იყოს არარსებული პროდუქციის გაყიდვა ინტერნეტმაღაზიაში, ცრუ აუქციონი, სოციალური ქსელის გამოყენებით ცრუ ინფორმაციის განთავსება და შეცდომაში შეყვანის გზით სხვისი ქონების დაუფლება.

---

[148] *Rachavelias, M. G.,* Online financial crimes and fraud committed with electronic means of payment—a general approach and case studies in Greece, ERA-Forum, Vol.19 (3), 2018, 339-355

[149] *Kryshevych O., Andrushchenko I., Striltsiv O., Pyvovar Y., Rivchachenko O.,* Modern methods of computer-related fraud: legal characteristics and qualification, jour. Cuestiones Politicas, Vol. 39 № 68, 2021), 864-865

[150] იქვე, 858

მაგალითად, თბილისის საქალაქო სასამართლოს 2021 წლის 26 ნოემბრის განაჩენით, ერთ-ერთი პირი პასუხისმგებაში მიეცა თაღლითობისთვის, განხორციელებული შენიღბული ქველმოქმედების მიზნით. კერძოდ, 2019 წელს, დამნაშავემ სოციალურ ქსელ „Facebook“-ში შექმნა ცრუ საქველმოქმედო დანიშნულების გვერდი მოქალაქეთა მოტყუებისა და ნდობის მოპოვების მიზნით. ის სისტემატურად ათავსებდა იმ სხვადასხვა ბენეფიციარის ვებ-გვერდებიდან მოპოვებულ ფოტომასალას, რომელებსაც ჰქონდათ ფინანსური ან/და ჯანმრთელობასთან დაკავშირებული პრობლემები, რის გამოც სოციალურ ქსელ „Facebook“-ის მომხმარებლებმა ბენეფიციარების დახმარების მიზნით, მას ჩაურიცხეს დიდ ოდენობის თანხა პირად ანგარიშზე. მისი ქმედება დაკვალიფიცირდა, როგორც დიდი ოდენობით ჩადენილი თაღლითობა, დანაშაული გათვალისწინებული საქართველოს სისხლის სამართლის კოდექსის 180-ე მუხლის მესამე ნაწილის „ბ“ ქვეპუნქტით. [151]

ცრუ ვებ-გვერდის გარდა, სოციალური ქსელში ფართოდ გავრცელებულ არამართლზომიერ ქმედებას წარმოადგენს ყალბი პირადი ანგარიშის შედგენა. აღნიშნული ქმედება წარმოადგენს პიროვნების საიდენტიფიკაციო მონაცემის მოპარვის ერთ-ერთ შემთხვევას (ცნობილია, როგორც “Identity Theft” შემთხვევა), რომლის არსიც დეტალურად იქნება მიმოხილული კომპიუტერული გაყალბების თავში, თუმცა კერძოდ ეს შემთხვევა ხშირად არის გავრცელებული პრაქტიკაში თაღლითობის ჩასადენად.

მაგალითად, 2022 წლის თებერვლის განაჩენით, პასუხისგებაში მიეცა პირი, პირობითად - „ა“, რომელმაც შექმნა „ბ“ პიროვნების მსგავსი ყალბი ანგარიში სოციალურ ქსელ “Facebook”-ში, დაიმატა „ბ“-ს მეგობრები. „ბ“ პიროვნებით ამოფარებულმა „ა“-მ მისწერა „ბ“-ს მეგობრებს და მოტყუებით ჩაარიცხინა ფულადი თანხა ტოტალიზატორ „აჭარაბეთის“ ანგარიშზე. აღნიშნული ქმედება დაკვალიფიცირდა, როგორც თაღლითობა.

მნიშვნელოვანია, აქვე მიმოვიხილოთ ერთი შეხედვით მსგავსი ფაქტი, თუმცა გარკვეული თავისებურებებით, რომელმაც, დანაშაულის კვალიფიკაცია, შესაძლოა, არსობრივად შეცვალა. თბილისის საქალაქო სასამართლოს 2021 წლის 15 ნოემბრის განაჩენში, ვინმე „ა“, რომელმაც უნებართვოდ შეაღწია „ბ“ პიროვნების კომპიუტერულ სისტემაში, კერძოდ, ჰაკერული გზით მოიპოვა „Facebook” ანგარიშის ავტორიზაციისთვის საჭირო მონაცემები, შევიდა სისტემაში და მისწერა „ბ“-ს დედას, (რომელიც ცხოვრობდა იტალიაში) ფულადი გზავნილის მოთხოვნით. „ბ“-ს დედამ, ჩათვალა, რომ მისმა შვილმა სთხოვა ფული და ფულადი გზავნილების სისტემის მეშვეობით, 50 ევროს ოდენობით თანხა დაუყოვნებლივ გამოაგზავნა „ა“-ს ანგარიშზე. „ა“-მ თავისი კუთვნილი ბარათის მეშვეობით გაანაღდა თანხა, რითაც უკანონოდ დაეუფლა თანხას.[152]

[151] თბილისის საქალაქო სასამართლოს №1/3199-21 26 ნოემბრის 2021 წლის განაჩენი

[152] თბილისის საქალაქო სასამართლოს 15 ნოემბრის 2021 წლის № 1/2544-21 განაჩენი.

ორივე შემთხვევაში, გამოყენებულია ერთი და იგივე პლატფორმა „Facebook" და ორივე შემთხვევაში ბოროტმოქმედებმა მოატყუეს ფიზიკური პირი. მოტყუება არის ადამიანის გონებაზე ზემოქმედების საშუალება, ამასთან ერთად შეიძლება კომპიუტერული სისტემის მოტყუება, როდესაც დამნაშავის ქმედებებით მას საშუალება ეძლევა მოიპოვოს არაავტორიზებული წვდომა სისტემებში შენახულ ან დამუშავებულ ინფორმაციაზე, უფლებამოსილი პირის იმიტაციის გზით. ნდობის ბოროტად გამოყენება, როგორც თაღლითობის მეთოდი ელექტრონული კომპიუტერების გამოყენებით, ხდება მაშინ, როდესაც დამნაშავე პირი იყენებს ნდობის ურთიერთობას (ოფიციალური ურთიერთობები, მეგობრული ურთიერთობა და ა.შ.) და აქვს თავისუფალი წვდომა შესაბამის ოპერაციებზე, რასაც ბოროტად იყენებს იმ განზრახვით, რომ საკუთრება ან მასზე უფლება მიითვისოს. ამ გზით შესაბამის ელექტრონულ სისტემაში შეღწევის შემდეგ, დამნაშავე ახორციელებს გარკვეულ ოპერაციებს, როგორც ამას უფლებამოსილი პირი გააკეთებდა, რაც მოხდა მეორე კაზუსში.[153]

მოცემულ ორ შემთხვევაში დამნაშავეები მოქმედებდნენ სხვა პირის სახელით, თუმცა პირველ კაზუსში საქმე არ გვქონდა უნებართვო შეღწევასთან. ეს ელემენტი ცვლის არსებითად კვალიფიკაციის შეფასებისას. მეორე შემთხვევა, ვერ ჩაითლება თაღლითობად, რადგან, მართალია მოხდა ფიზიკურ პირზე ზემოქმედება, თუმცა პირმა გამოიყენა ე.წ. „ჰაკერული მეთოდი", რითაც შეაღწია სხვა პირის კომპიუტერულ სისტემაში, რომელმაც საბოლოო სასურველ შედეგამდე მიიყვანა. სოციალური ქსელის ანგარიშის „გატეხვა" ხელყოფს ინფორმაციულ უსაფრთხოებას, როგორც სამართლებრივად დაცულ დამოუკიდებელ სიკეთეს.

საბოლოდ უნდა ითქვას, რომ პირველი შემთხვევა უნდა დაკვალიფიცირდეს, როგორც 180-ე მუხლი, ტრადიციული თაღლითობის სახით, ხოლო მეორე შემთხვევა, ვინაიდან მოხდა კომპიუტერულ სისტემაში უნებართვო შეღწევა და საბოლოოდ ამ მეთოდმა დამნაშავე მიიყვანა სასურველ შედეგამდე, უნდა დაკვალიფიცირდეს 286[1] მუხლით, როგორც კომპიუტერულ სისტემაში უნებართვო შეღწევა ფინანსური სარგებლის მიღების მიზნით. მართალია, მან შეღწევის შემდეგ მოატყუა პირი გზავნილის მისაღებად, თუმცა შეღწევის განზრახვა იმთავიდანვე იყო ფინანსური სარგებლის მიღება და არ საჭიროებს დანაშაულთა ერთობლიობას შეღწევით 284-ე მუხლით და თაღლითობით 180-ე მუხლი.

ფინანსური ოპერაციების მიმართულებით, ერთ-ერთ ყველაზე გავრცელებული შემთხვევები არის სიმ ბოქსის დახმარებით თაღლითობის ჩადენა. სიმ ბოქსი წარმოადგენს მოწყობილობას, რომელიც ცვლის ტელეფონის ნომრის ქვეყნის კოდს, რასაც ხშირად იყენებენ ე.წ. ქოლ ცენტრები. ამ შემთხვევაში, ბოროტმოქმედები უკავშირდებიან დაზარალებულებს, თითქოსდა სხვა ქვეყნიდან, რათა შევიდნენ მათთან

[153] *Kryshevych O., Andrushchenko I., Striltsiv O., Pyvovar Y., Rivchachenko O.,* Modern methods of computer-related fraud: legal characteristics and qualification, jour. Cuestiones Politicas, Vol. 39 № 68, 2021), 859

ნდობაში, თანხის გამოტყუების მიზნით. ასეთი ქმედებები კვალიფიცირდება, როგორც ტრადიციული თაღლითობა.

ზემოთ მოყვანილ შემთხვევებში, საქმეები შეეხებოდა უშუალოდ ფიზიკური პირის მოტყუებას. საინტერესოა რა ხდება მაშინ, როდესაც დამნაშავე შემოდის უსაფრთხოების ზომებით დაცულ ელექტრონულ სისტემაში, მაგალითად, უსაფრთხოების კოდების დაბლოკვით ან გატეხვით და ახორციელებს უკანონო ტრანზაქციებს სხვისი ქონების ან ქონებრივი უფლებების მითვისების მიზნით? თაღლითობის არსი არის, რომ პირი ქონებრივ უფლებას ეუფლება ნებაყოფლობით, მსხვერპლის ხელიდან: ამ შემთხვევაში შეცდომაში შეყვანილი პირი, თავისი კეთილი ნებით გადასცემს ქონებას, ხოლო თანხის მიღების მიზნით, კომპიუტერულ მონაცემებზე ზემოქმედების და სისტემის მოტყუების დროს არ ხდება დაზარალებულზე უშუალო ზემოქმედება.[154]

მაგალითად, საბანკო ანგარიშებზე უკანონოდ წვდომის მეთოდები წარმოადგენს ერთ-ერთ ყველაზე ფართოდ გავრცელებულ დანაშაულს.[155] დისტანციური საბანკო სერვისები უზრუნველყოფენ საბანკო მომსახურებას კლიენტის მიერ დისტანციურად გადაცემული მოთხოვნების საფუძველზე (ბანკში მისი პირდაპირი ვიზიტის გარეშე). ეს სისტემა წარმოადგენს მრავალფუნქციური პროგრამულ და აპარატურულ კომპლექსს, რომელიც საშუალებას აძლევს ბანკის კლიენტებს, განახორციელონ დისტანციურად სხვადასხვა გადახდები, აკონტროლონ ბიუჯეტი, დაათვალიერონ ანგარიშის ნაშთები, ასევე მიიღონ სხვადასხვა ფინანსური სერვისი.[156]

ერთ-ერთი საქმეში, ვინმე პიროვნება „ა“-მ იცოდა, რომ დედამისს ჰქონდა ვადიანი ანაბარი საქართველოს ბანკში. ვინაიდან მას არ გააჩნდა ზემოაღნიშნული თანხის დაუფლების კანონიერი საშუალება, მან, აღნიშნული თანხის მართლსაწინააღმდეგო დაუფლების მიზნით, დედის ნებართვის გარეშე, ვინაიდან ის იმყოფებოდა რეანიმაციულ განყოფილებაში, საავადმყოფოში, მისი საიდენტიფიკაციო მონაცემების, კერძოდ, პირადი ნომრის, ტელეფონის ნომრის, აგრეთვე, მის სახელზე გაცემული საქართველოს ბანკის პლასტიკური ბარათის ნომრისა და ე.წ. CVC კოდის მითითებით, შეაღწია ქალბატონის ტელეფონის კომპიუტერულ სისტემაში, გააქტიურა მობილბანკი და აღნიშნული მობილბანკის საშუალებით დაიმტკიცა სესხი.

როგორც ჩანს, კომპიუტერული მონაცემის ხელყოფას ფინანსური სარგებლის მიღების მიზნით აქვს საერთო ნიშნები არა მარტო თაღლითობასთან, არამედ საკუთრების წინააღმდეგ მიმართულ სხვა დანაშაულებთან, მაგალითად, ქურდობასთან. საქართველოში არსებული პრაქტიკის მიხედვით, მობილური ბანკის, ბარათების ქურდობის და მათი გადახდის შემთხვევები კვალიფიცირდებოდა კომპიუტერულ

---

[154] *Kryshevych O., Andrushchenko I., Striltsiv O., Pyvovar Y., Rivchachenko O.,* Modern methods of computer-related fraud: legal characteristics and qualification, jour. Cuestiones Politicas, Vol. 39 № 68, 2021), 861-862

[155] *იქვე,* 849

[156] *იქვე,* 857

სისტემაში შეღწევითა და ქურდობით, 284-ე მუხლისა და 177-ე მუხლების ერთობლიობით. მაგალითად, როდესაც დამნაშავეები ეუფლებოდნენ დაზარალებულების ბარათებს და უნებართვოდ იყენებდნენ მათ მაღაზიებში ან ბანკომატებში. კვალიფიკაციისთვის მნიშვნელოვანი ის იყო, რომ ქონების დაუფლების ხერხს იყო ფარული, მაგალითად, როგორიცაა ბარათის ქურდობა. ამ მოსაზრებას მხარდამჭერები მიიჩნევენ, რომ ბანკომატის კომპიუტერული სისტემა, განიხილება, როგორც შეღწევა ბანკომატის დახურულ სისტემაში, რაც კვალიფიცირდება, როგორც ქურდობა.[157]

მეორე მხრივ, რამდენად იგულისხმება დახურულ სისტემაში შესვლა? მოცემულ შემთხვევაში, აქ ხდება არაავტორიზებული პირის მიერ კომპიუტერულ სისტემაში შესვლა, რადგან კომპიუტერი არ ინახავს ფულს ან ქონებას, არამედ მხოლოდ ინფორმაციას ამ ქონების ან ამ ქონებასთან დაკავშირებული ტრანზაქციების შესახებ.[158] დანაშაულებრივი მიზნებისთვის, შესვლა არის უნებართვო. მოპარული მობაილ ბანკის პაროლი და მისი საშუალებით სისტემაში შესვლა, ასევე მოპარული ბარათით და პაროლით ბანკომატის სისტემაში შეღწევა წარმოადგენს კიბერთაღლითობის შემთხვევას, რადგან ხდება ავტორიზებული პირის იმიტაცია. ვინაიდან ბარათი, პაროლი არის მაიდენტიფიცირებელი საშუალება, შესაბამისად, ვატყუებთ სისტემას, რომ ვართ უფლებამოსილი პირები. ამ მსჯელობიდან გამომდინარე, თუ პირი დაეუფლა ქონებას უნებართვო შეღწევის გზით, სახეზეა 286[1] მუხლი.

რაც შეეხება ხელყოფის ობიექტს, მართალია, ერთი მხრივ, ხელყოფილია იმ კომპიუტერული სისტემის ხელშეუხებლობა, რომელიც ინახავს ინფორმაციას ელექტრონული საფულის შესახებ, თუმცა, ამ შემთხვევაშიც, როგორც თაღლითობის დროს, დგება მატერიალური ზიანი. ტერმინი „ქონებრივი ზიანი“, როგორც ფართო ცნება, მოიცავს როგორც ფულის, მატერიალური ნივთების, ასევე ეკონომიკური ღირებულების მქონე არამატერიალური ნივთების დაკარგვასაც.[159] ამის შესახებ, ასევე, ნახსენებია 286[1] მუხლის ცვლილებების განმარტებით ბარათში, სადაც სამართლებრივად მიზანშეწონილია გაიმიჯნოს ფული, როგორც მოძრავი ნივთი (მატერიალური სახით, მაგალითად, ბანკნოტი, მონეტა) და ასევე საბანკო ანგარიშზე არსებული (უნაღდო) თანხა. სწორედ უნაღდო თანხებს ხელყოფისგან იცავს 286[1]-ე მუხლი. ეს მიდგომა

[157] მაგალითად, სლოვენიის უზენაესი სასამართლოს გადაწყვეტილებებში № I Ips 98/2004 და № I Ips 461/2007 გადაწყვეტილებებში, იხ.: *Sepec, M.,* Slovenian criminal code and modern criminal law approach to computer-related fraud: A comparative legal analysis., International Journal of Cyber Criminology, 6(2), 2012, 985-986). იხ. ასევე *Kryshevych O., Andrushchenko I., Striltsiv O., Pyvovar Y., Rivchachenko O.,* Modern methods of computer-related fraud: legal characteristics and qualification, jour. Cuestiones Politicas, Vol. 39 № 68, 2021), 860

[158] Council of Europe Framework Decision “On Combating Fraud and Counterfeiting Non-cash Means of Payment” (CF, 2001).

[159] 88-ე პუნქტი.

აღებულია გერმანიის სისხლის სამართლის კოდექსის 263ა პარაგრაფით, რომელიც ეხება კომპიუტერულ მოტყუებას.[160]

გარდა ამისა, კონვენციის მე-8 მუხლი, რომელიც დანაშაულად აცხადებს კომპიუტერთან დაკავშირებულ თაღლითობას, მოითხოვს, რომ დაცული იყოს პირის საკუთრება. თავად აქტი ჰგავს ტრადიციულს თუმცა, იმ განსხვავებით, რომ ჩადენილია კიბერსივრცეში ან დაკავშირებულია მასთან.[161] კონვენცია მოითხოვს მხარეებს მოახდინონ პირდაპირი თაღლითობის და ირიბი თაღლითობის კრიმინალიზაცია.

აქედან გამომდინარე, პირდაპირი თაღლითობის შემთხვევაში, ბოროტმოქმედი ატყუებს ადამიანს კომპიუტერული სისტემის დახმარებით. ირიბი თაღლითობა ისეთი შემთხვევაა, როდესაც ბოროტმოქმედი ატყუებს კომპიუტერულ სისტემას, რადგან ეს უკანასკნელი დაპროგრამებულია, მაგალითად ბანკომატი, ბარათის მფლობელზე და საიდუმლო კოდის მცოდნე პირზე. აქ მოტყუებული გამოდის, მართალია ირიბად, პირი, რომელიც ბანკომატის მომსახურების უკან დგას, როგორიცაა ბანკი, ინტერნეტ-მაღაზიის მფლობელი და ა.შ.[162]

კვალიფიკაციისთვის იმიტომ არის მნიშვნელოვანი მათი გამიჯვნა, რომ, თუ პირველ შემთხვევაში, როდესაც კომპიუტერული სისტემა გამოიყენება როგორც დანაშაულის ჩასადენად, გვაქვს ტრადიციული თაღლითობა, მეორე შემთხვევაში, როდესაც სისტემას ვატყუებთ, არის სპეციალური შემთხვევა - კომპიუტერული თაღლითობა.[163]

3.1.3. კომპიუტერთან დაკავშირებული თაღლითობის სპეციალური შემთხვევები

286[1] მუხლის კვალიფიკაციისთვის კიდევ ერთ პრობლემას წარმოადგენს ისეთი შემთხვევები, როდესაც არ არის ავტორიზაციის საჭიროება ან როდესაც სადავოა, მოხდა თუ არა კომპიუტერულ სისტემაში შეღწევა. მარტივად, ელექტრონულმა ტრანზაქციებმა გამოიწვია დანაშაულის ახალი ტიპის გაჩენა, როგორიცაა ქარდინგი. მოპარულ პლასტიკურ ბარათებსა და ბანკომატებთან დაკავშირებული დანაშაულები წარმოადგენს საკმაოდ გავრცელებულ დანაშაულთა სახეებს, მათი განხორციელების

[160] განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის კოდექსში ცვლილების შეტანის შესახებ“, ხელმისაწვდომია ბმულზე: https://info.parliament.ge/file/1/BillReviewContent/268580 [02.06.2022].

[161] Sepec, M., Slovenian criminal code and modern criminal law approach to computer-related fraud: A comparative legal analysis., International Journal of Cyber Criminology, 6(2), 2012, 984

[162] იქვე.

[163] იქვე, 985-986

ხერხი მრავალფეროვანია,[164]მაგრამ ყველა მათგანი მიზნად ისახავს ფულის, გადახდის ბარათის ან მისი მონაცემების მოპარვას.[165]

ბანკომატის თაღლითობა - ეს არის ბანკომატის მუშაობაში ჩარევა, ფულადი სახსრების განაღდების ოპერაციების დროს. ერთ-ერთი შემთხვევაა სქიმინგი („Skimming„„), როდესაც გამოიყენება ბანკომატზე სპეციალური მოწყობილობის დამზადება და მასში ინსტალაცია ხორციელდება. არსი ისაა, რომ ასეთი სპეციალური ბანკომატები კითხულობენ ინფორმაციას ბარათის მაგნიტური ზოლიდან და აკოპირებენ მას. ტრეფინგი („Cash Trapping“), მსგავსად სქიმინგისა, ამ შემთხვევაში ხდება უშუალოდ ბანკომატის უშუალო მოწყობილობაზე ზემოქმედებაა, რა დროსაც ხდება გამოსატანი ნაღდი ფულის დაკავება სპეციალური შემაკავებელი ბალიშის გამოყენებით. მსხვერპლს მისდის შეტყობინება, რომ თანხა არის განაღდებული, თუმცა, უშუალოდ, თანხა დაკავებულია ბანკომატის მიერ, რის შემდგომაც ბოროტმოქმედები ეუფლებიან თანხას. კიდევ ერთ გავრცელებულ შემთხვევას წარმოადგენს კარდინგი („Carding“) - უკანონო ფინანსური ოპერაციები, საგადასახადო ბარათის ან მისი მონაცემების გამოყენებით, რომელიც არ არის ინიციირებული ან დადასტურებული მისი მფლობელის მიერ.

ამ შემთხვევებს აქვთ ერთი საერთო რამ: ვატყუებთ კომპიუტერულ სისტემას. კომპიუტერული სისტემის უშუალო მოტყუება, როგორც ხდება უშუალოდ ტრდიციული თაღლითობის დროს, ტექნიკურად შეუძლებელია, რადგან სისტემა ამუშავებს იმთავითვე სწორ ინფორმაციას, მაგალითად, ბარათის მონაცემებს. რადგან პირდაპირი გაგებით შეუძლებელია კომპიუტერის მოტყუება, როგორც ფიზიკური პირის, ამიტომ ეს შემთხვევა სცილდება 180-ე მუხლის შემადგენლობას. კიბერთაღლითობის შემთხვევაში, კომპიუტერული სისტემის მოტყუებაზე კი არ არის საუბარი, არამედ ბოროტმოქმედის უფლებამოსილება გამოიყენოს მონაცემი დგება კითხვის ნიშნის ქვეშ. აქ მცდარ, არასწორში იგულისხმება პროგრამის გამოყენებით მიღწეული შედეგი, რომელიც რეალობას არ შეესაბამება, რადგან სისტემა ფიქრობს, რომ უფლებამოსილ პირს წარმოადგენს ბარათის მფლობელი.

მაგალითად, იმ შემთხვევაში, როდესაც პირი მართლსაწინააღმდეგოდ დაეუფლა სხვის ბარათსა და პაროლს, ქმედება უნდა დაკვალიფიცირდეს ქურდობისა და სსკ-ის 286[1]-ე მუხლით გათვალისწინებული კომპიუტერული თაღლითობის ერთობლიობით. საქმე ისაა, რომ, ერთი მხრივ, მოპარული ბარათი მატერიალური სახისაა და მისი მართლსაწინააღმდეგო დაუფლება ცალკე იმსახურებს სამართლებრივ გაკიცხვას, ხოლო, მეორე მხრივ, პირმა მოატყუა კომპიუტერული სისტემაც, რადგან დაცვის

[164] ფიშინგი და ფარმინგი, სკიმინგი, ტრეპინგი და ფანტომ ბარათები და ა.შ.

[165] მაგ.: ბარათის საიდენტიფიკაციო ნომერი, ბარათის გაცემის/ვადის გასვლის თარიღი, CVV2 კოდი (სამნიშნა ნომერი გადახდის ბარათის უკანა მხარეს მოცემული კოდი, კლიენტის სახელი და გვარი ლათინურად, პინ კოდი და ა.შ.

საშუალებების გვერდის ავლით უნებართვოდ შეაღწია მასში და გამოიწვია ფინანსური ზიანი.

საინტერესოა, შედეგობრივად განსხვავდება თუ არა ერთმანეთისგან შემთხვევა, როდესაც უშუალოდ ბარათის მოპარვამ გამოიწვია პირის მატერიალური ზიანი თუ კიბერთაღლითობისთვის არსებითია დამცავი სისტემის გადალახვა. მაგალითად, „ა“-მ მოიპარა „ბ“-ს პლასტიკური ბარათი, თუმცა არ იცოდა ბარათის PIN კოდი და ვერ შეძლო ბანკომტიდან თანხის გამოტანა და გამოიყენა გადახდის ტერმინალებთან, რა დროსაც გამოიწვია „ბ“-ს ფინანსური ზიანი. მეორე შემთხვევას წარმოადგენს, როდესაც „ა“-მ მოიპოვა პაროლი, მოიპარა ბარათი და ბანკომატიდან გამოიტან თანხა.

მეორე შემთხვევა ცალსახად წარმოადგენს 286[1] მუხლს, რადგან მოხდა კომპიუტერულ სისტემაში უნებართვო შეღწევა. პრობლემურია პირველი შემთხვევა, როდესაც სადავოა მოხდა თუ არა კომპიუტერულ სისტემაში შეღწევა. სასამართლო პრაქტიკის მიხედვით, გადახდის ტერმინალებთან ბარათის გამოყენება კვალიფიცირდებოდა ქურდობად, რადგან, ერთი მხრივ, სისტემაში უშუალო ჩარევა არ ხდება და ამავდროულად, ბარათზე, როგორც ინფორმაციის მატერიალურ მატარებელზეა საუბარი.

ბარათის ფლობა არ უნდა გულისხმობდეს, რომ სახეზე არის უფლებამოსილი პირი. გადახდის ტერმინალს არ შეუძლია გადაამოწმოს პირის ვინაობა და უბრალოდ ტერმინალით გადახდა არსობრივად არ უნდა წარმოადგენდეს კლასიკური გაგებით კიბერდანაშაულს.

ამ მხრივ საინტერესოა, გერმანიის ფედერალურმა სასამართლომ იმსჯელა რამდენად არსებითია დამცავი საშუალებები თაღლითობისა და კიბერთაღლითობის გამიჯვნის კუთხით.

პირველი განმარტების, ე.წ. „სუბიექტური მიდგომის“ მიხედვით, მნიშვნელობა ენიჭება ბარათის მესაკუთრის მიერ აშკარა/ცხადად გამოვლენილ ნებას, ბარათის გამოყენების თაობაზე. ეს მოსაზრება გაკრიტიკებულია, რადგან ზედმეტად ფართოდ განიმარტება და არარელევანტრუ შემთხვევებსაც მოიცავს.

მეორე განმარტება მხედველობაში ირებს სისტემის სპეციფიკას, მას ასევე უწოდებენ კომპიუტერული სპეციფიკის განმარტებას.[166] აღნიშნული მიდგომის თანახმად, სახეზეა კიბერთაღლითობა, როდესაც მონაცემთა დამუშავების დროს პროგრამა მოითხოვს პიროვნულ იდენტიფიკაციასათვის საჭირო მონაცემების შეყვანას, მაგ: პაროლს, დაშვების კოდს. ამ მოსაზრების კრიტიკოსები აღნიშნავენ, რომ პროგრამის მიერ იდენტიფიკაციის სისტემის მოთხოვნა ავიწროებს შემთხვევებს და სცილდება ნორმის დაცვის მიზანს: დაიცვას ბარათის მფლობელის ინტერესი.

მესამე მიდგომა, რომელიც წარმოადგენს გაბატონებულ მოსაზრებას, ბარათის ,,უნებართვო გამოყენებად'' შეფასება უნდა მოხდეს მაშინ, როდესაც შემთხვევა ,,ახლოს

[166] ე.წ. „ Computerspezifische Auffassung“

დგას'' ,,კლასიკური თაღლითობის'' შემადგენლობასთან. მესამე მიდგომის მიხედვით, პირი ახორციელებს კლასიკური თაღლითობისთვის დამახასიათებელ „მოტყუების“ ელემენტს, მაგალითად, მაღაზიაში შესვლისთვის ქმნის წარმოადგენას, რომ აქვს ბარათის გამოყენების უფლება. ეს შემთხვევა, როგორც აღენიშნა კვალიფიცირდება კომპიუტერთან დაკავშირებულ თაღლითობად, კერძოდ გერმანიის სისხლის სამართლის კოდექსის 263 a პარაგრაფით.

რაც შეეხება ბარათის გამოყენება გადახდის ტერმინალებთან საქართველოს სისხლის სამართლის კოდექსის მიხედვით ნორმის მიზნიდან და ინტერპრეტაციიდან გამომდინარე უნდა დაკვალიფიცირდეს 286[1] მუხლით. მართალია თავისი არსით გადახდის ტერმინალებთან ბარათის მიდება კიბერთარლითობას არ წარმოადგენს .

286[2] მუხლი მოთავსებულია კიბერდანაშაულის თავში, ნებისმიერ მოწყობილობაზე ზემოქმედება არ უნდა ნიშნავდეს თავისი არსით კიბერდანაშაულს. როგორ შეიძლება გავაიგივოთ კიბერდანაშაული, ჰაკერული გზით ჩადენილი და უბრალოდ მატერიალური ბარათის მოპარვა, სადაც არანაირი სოფისტური უნარ-ჩვევების გამოყენება არ ხდება. კიბერდანაშაულად მიჩნევისათვის სწორედ მოწყობილობის სპეციფიკას ვითვალისწინებთ. თუმცა მიუხედავად ამისა, ამოსავალი წერტილია კანონმდებლის ნება. კანონმდებელმა ნორმა 286[1] მუხლი, არსობრივად გადმოტანილია ბუდაპეშტის კონვენციის მე-8 მუხლიდან, რომლის მოთხოვნა იყო პლასტიკურ ბარათებთან დაკავშირებული მრავალფეროვანი თაღლითობების კანონმდებლობაში გათვალისწინება. როგორც კონვენციაში, ასევე ნორმაში ხვდებით ქმედების ერთ-ერთ ხერხს - ესაა „კომპიუტერული სისტემის ფუნქციონირებაში ნებისმიერი სახის უნებართვო ჩარევა“, რომელიც მოიცავს, ასევე, შემთხვევებს, როდესაც არ მოხდა კომპიუტერულ სისტემაში შეღწევა, მაგალითად, დამცავი სისტემის გადალახვით. ასეთ შემთვევებს წარმოადგენს გადახდის ტერმინალთან ბარათის დადება, ბანკომატის მიერ თანხის დაკავება. აქედან გამომდინარე 286[1] მუხლი არ არის უბრალოდ კიბერთაღლითობის მუხლი, ის წარმოადგენს უფრო ფართო ცნებას, რაც გულისხმობს კომპიუტერთან დაკავშირებულ თაღლითობას.

ამ თემასთან ერთად, კომპიუტერთან დაკავშირებული თაღლითობისთვის ერთ-ერთ ყველაზე საინტერესო და გავრცელებულ დანაშაულს წარმოადგენს ფიშინგი, რომელიც შეიცვას როგორც 286[1] და ასევე 286[2] მუხლების ხერხებს, შესაბამისად, მისი კვალიფიკაციის შეფასების მიზნით, მნიშვნელოვანია კომპიუტერული გაყალბების მუხლის მიმოხილვა.

3.2. საქართველოს სისხლის სამართლის კოდექსის 286[2] მუხლის კვალიფიკაციის საკითხები

3.2.1. საქართველოს სისხლის სამართლის კოდექსის 286[2] მუხლის ქმედების შემადგენლობა

კომპიუტერთან დაკავშირებული გაყალბება, რომელიც გათვალისწინებულია საქართველოს სისხლის სამართლის კოდექსის 286[2] მუხლით, თავისი არსით წარმოადგენს ერთ-ერთ ყველაზე ხშირ კიბერდანაშაულს, მისი მრავალფეროვანი განხორციელების ხერხის გათვალისწინებით. თუმცა საქართველოში ამ ეტაპზე არ არსებობს პრეცედენტი აღნიშნული მუხლის შესახებ. შეიძლება ითქვას, ერთი მხრივ, ეს განპირობებულია მისი სიახლით, რადგან კოდექსში ის დამოუკიდებელ დანაშაულად შევიდა 2021 წლის ცვლილებებით საფუძველზე, ხოლო მეორე მხრივ, მისი განხორციელების ხერხები არსებითად ჰგავს სხვა დანაშაულის ქმედების შემადგენლობებს.

პრაქტიკაში კვლავ პრობლემად რჩება საკითხი, თუ როგორ უნდა დაკვალიფიცირდეს ქმედება, რომელიც შეიცავს ოფიციალური კომპიუტერული მონაცემის გაყალბების ან/და თაღლითობის ნიშნებს, რომელიც ხორციელდება ვირტუალურ სივრცეში და ელექტრონული ხერხებით.

სისხლის სამართლის კოდექსის 286[1] და 286[2] მუხლები მსგავსი ხერხებით ხორციელდება, ესაა კომპიუტერული მონაცემის უნებართვო ჩასმა, წაშლა, შეცვლა ან დაფარვა, თუმცა განსხვავებულია დამნაშავის სუბიექტური განწყობა. თუ პირველი მუხლი ითვალისწინებს მატერიალური სარგებლის მიღების მიზანს, ხოლო მეორე მუხლი ითვალისწინებს მიღებული ყალბი ოფიციალური დოკუმენტის ნამდვილ/უტყუარ მონაცემად გასაღების ანდა გამოყენების მიზანს. საინტერესოა, რა ხდება მაშინ, როდესაც პირმა შექმნა ყალბი ოფიციალური დოკუმენტი და ამით ფინანსური სარგებელი მიიღო?

ერთი ხერხი სახეზე არის, თუმცა ისმის კითხვა - სხვადასხვა მიზნები ცვლის თუ არა არსებითად კვალიფიკაციის საკითხს? ამის ნათელი მაგალითია, კლასიკური ფიშინგის შემთხვევა, როდესაც იქნება ყალბი კომპიუტერული მონაცემები, რომლის დახმარებითაც ბოროტმოქმედები ადრესატებს აჯერებენ მის ნამდვილ/უტყუარობაში, შედიან ნდობაში პოტენციურ მსხვერპლებთან, რის საფუძველზეც ეუფლებიან თანხას. ამ კითხვაზე და სხვა მსგავს შემთხვევებზე საჭიროა და 286[2] მუხლის ქმედების შემადგენლობის ელემენტების მიმოხილვა.

დანაშაულის ობიექტური შემადგენლობა

კომპიუტერული მონაცემები, რომლებიც მნიშვნელოვანია როგორც ნებისმიერი უფლების, ვალდებულების შეძენის ან მათგან გათავისუფლების მტკიცებულება, უნდა იყოს დაცული ისევე, როგორც მატერიალურად ასახული დოკუმენტები. ასეთი მონაცემების მანიპულირებას შეიძლება მოჰყვეს სერიოზული შედეგები და უნდა იყოს

დანაშაული ისევე, როგორც დოკუმენტების ტრადიციული გაყალბება. კომპიუტერული მონაცემების უსაფრთხოება და საიმედოობა, რამაც შეიძლება გავლენა იქონიოს სამართლებრივ შედეგებზე და იურიდიულად მნიშვნელობის მქონე იყოს, დაცული უნდა იყოს.[167]

შეიძლება ითქვას, რომ სსკ. 286[2] მუხლი წარმოადგენს სსკ. 362-ე მუხლის სპეციფიკურ გამოვლინებას, კერძოდ, ვირტუალური და ელექტრონული საშუალებებით ჩადენილ გაყალბებას. ზოგადად, ყალბი კომპიუტერული მონაცემის შექმნა გაიგივებულია გაყალბების ჩვეულებრივ დანაშაულებრივ შემადგენლობასთან, განსხვავებულია მხოლოდ დანაშაულის ჩადენის ხერხი. მაგალითად, ფრანგული კანონმდებლობა, რომელსაც არ აქვს სპეციალური რეგულაცია კომპიუტერულ მონაცემთან მიმართებით ჩადენილი დანაშაულების შესახებ, ადგენს სპეციფიკური სახელწოდების მქონე დანაშაულს - „კომპიუტერის საშუალებით შექმნილი დოკუმენტის გაყალბება“.[168]

აქ იგულისხმება ვირტუალურ სივრცეში განთავსებული და შენახული, ელექტრონული საშუალებებით შექმნილი და შეცვლილი დოკუმენტები. უფრო მეტიც, როდესაც ხდება ამა თუ იმ მატერიალური პარამეტრების მქონე დოკუმენტის ნებისმიერი ფორმით მის ელექტრონულ ვერსიად გადაქცევა, უკვე სახეზეა გაყალბების სპეციფიკური - ელექტრონული შემთხვევა. სსკ. 286[2] მუხლი მიზნად ისახავს სწორედ ელექტრონული საშუალებების გამოყენებით ჩადენილი გაყალბების კრიმინალიზებას. კრიმინალიზებას საჭიროება კი დადგა მას მერე, რაც პრაქტიკაში გამოიკვეთა ტენდენცია ხელოვნური ერთობლიობის შექმნისა მაშინ, როცა დოკუმენტი ელექტრონულად ყალბდებოდა. 362 მუხლი ფარავდა უშუალოდ გაყალბების ფაქტს, ხოლო სსკ-ს XXXV თავით გათვალისწინებული რომელიმე დანაშაული - გაყალბებისას ელექტრონული საშუალებების გამოყენებას.

უპირველეს ყოვლისა სპეციალური ნორმის მიზნის შემოტანა გამართლებულია, ჩემი აზრით, იმით, რომ დანაშაული იმის გათვალისწინებით თუ რა მეთოდით იქნა ჩადენილი, გულისხმობს საშუალოზე მაღალ სოციალურ უნარებს და ტექნიკურ ცოდნას კომპიუტერების გამოყენებასთან დაკავშირებით, რაც განაპირობებს დანაშაულის მაღალ საშიშროებას, ასევე მონაცემის/ინფორმაციის ხელყოფისგან დაცვის მაღალი ინტერესი .

საქართველოს სისხლის სამართლის კოდექსის 286[2]-ე მუხლი თავის მიზნითა და შემადგენლობით ჰგავს „კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციის მე-7 მუხლს, რომელიც აწესრიგებს კომპიუტერთან დაკავშირებულ გაყალბებას. კონვენციის მე-7 მუხლი განმარტავს კომპიუტერულ გაყალბებას შემდეგნაირად: წინასწარი განზრახვით და უნებართვოდ კომპიუტერული მონაცემების ჩადება, შეცვლა, წაშლა, ან დაფარვა, რომლის შედეგიცაა გაყალბებული მონაცემების მიღება, მისი, როგორც

[167] Stein Schjolberg COMPUTER-RELATED OFFENCES (2004) გვ.10

[168] *Dr. Roberto Flor,* “Fraud, Computer-related fraud and Identity-related fraud”, Faculty of Law – University of Verona, March 2009, გვ. 7

უტყუარად გასაღება ან გამოყენება, მიუხედავად იმისა რამდენად კითხვადი და გარჩევადია ეს მონაცემი. დანაშაულის მთავარ მიზანს წარმოადგენს დოკუმენტის ავთენტიკურების ილუზიის შექმნა.

აღნიშნული დანაშაულის სისხლისსამართლებრივი **დაცვის ობიექტი** არის კომპიუტერული მონაცემის უსაფრთხოება და მისი საიმედოობა.[169] კომპიუტერული გაყალბების დანაშაულის სპეციალური სამართლებრივი ობიექტი ეხება კომპიუტერული სისტემის მფლობელის ან კანონიერი მომხმარებლის კანონიერი ინტერესების დაცვას ან იმ კომპიუტერული მონაცემების, რომლებიც ინახება შესაბამის კომპიუტერულ სისტემაში.[170] რაც შეეხება **დანაშაულის საგანს**, ეს არის ოფიციალური კომპიუტერული მონაცემი.[171] ოფიციალური კომპიუტერული მონაცემი განსხვავდება სხვა მუხლების ქმედების შემადგენლობებისგან, სადაც მითითებულია უბრალოდ კომპიუტერული მონაცემი. კონვენცია უთითებს, რომ ასეთი კომპიუტერთან დაკავშირებული გაყალბება, რომელიც რეგულირდება კონვენციის მე-7 მუხლით, გულისხმობს, რომ მონაცემის მიმართ დამნაშავეს აქვს მიზანი, რომ გაასაღოს იგი ან გამოიყენოს კანონიერი მიზნებისთვის. ხოლო კონვენციის განმარტებით ანგარიშში აღნიშნულია, რომ კომპიუტერული სისტემის გამოყენებით ჩადენილი გაყალბება გულისხმობს არსებული კომპიუტერული მონაცემის უნებართვო შექმნას ან შეცვლას იმ მიზნით, რომ მას განსხვავებული მტკიცებითი ძალა მიენიჭოს კანონიერი ოპერაციებისთვის[172]

აქედან გამომდინარე, ოფიციალური კომპიუტერული მონაცემი უნდა განვმარტოთ, როგორც კომპიუტერული მონაცემი, რომელიც ადასტურებს ამა თუ იმ უფლების ან/და ფაქტის არსებობას/არარსებობას და იგი შესაძლებელია გამოყენებულ იქნეს კანონიერი საქმიანობისთვის. რაც შეეხება კომპიუტერული მონაცემის **სიყალბეს,** მასში იგულისხმება ნამდვილი მონაცემის უკანონო ასლის შექმნა, ნიშან-თვისებების გაქრობა ან დამატება, მის მიმართ სხვადასხვაგვარი მანიპულაციების განხორციელება. სიყალბის მთავარი განმსაზღვრელი კი არის ის, რომ პირს აღნიშნული ოფიციალური კომპიუტერული მონაცემი არ ეკუთვნის, არ აქვს მინიჭებული მასზე უფლება.

286[2] მუხლით გათვალისწინებული დანაშაული არის ფორმალური შემადგენლობის, რადგან მუხლი არ უთითებს კონკრეტული მძიმე შედეგის დადგომაზე (განსხვავებით 286[1] მუხლისგან), შესაბამისად, ნებისმიერი ქმედების განხორციელების

---

[169] *Council of Europe* , Explanatory Report to the Convention on Cybercrime, 2001, პუნქტი 81 https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf

[170] *Moise, A.C.,* Some Remarks Regarding the Criminalization and the Forensic Investigation of the Crime of Computer Forgery in the Romanian Legislation, Bulletin of the *Transilvania* University of Braşov, Series VII: Social Sciences and Law, Vol. 14(63) Special Issue, 2021, 198

[171] სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის 28-ე ნაწილის თანახმად, კომპიუტერული მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას.

[172] *იქვე.*

მომენტიდან, რომელიც დისპოზიციაში არის მოცემული, გვაძლევს დამთავრებულ დანაშაულს. რაც შეეხება ამავე მუხლის მეორე ნაწილს, ის ითვალისწინებს მძიმე შედეგის დადგომას, რაც ქმნის მატერიალურ დანაშაულს, კერძოდ, 286[2] მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტით აუცილებელია, სახეზე იყოს მნიშვნელოვანი ზიანი.

ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნა შეიძლება განხორციელდეს შემდეგი ალტერნატიული ქმედებების ჩადენით:

1. კომპიუტერული მონაცემის უნებართვო ჩასმით, წაშლით, შეცვლით ან დაფარვით ყალბი ოფიციალური კომპიუტერული მონაცემის მიღება მისი ნამდვილ/უტყუარ მონაცემად გასაღების ანდა გამოყენების მიზნით;
2. მიღებული ყალბი ოფიციალური კომპიუტერული მონაცემის გასაღება;
3. მისი გამოყენება.

მნიშვნელოვანია, რომ დანაშაულის ჩადენის ხერხებია კომპიუტერული მონაცემის უნებართვო ჩასმა, წაშლა, შეცვლა ან დაფარვა, რაც, ასევე მოცემულია 286[1] მუხლის დისპოზიციაში. განსხვავებაა მხოლოდ მათი მიზანი.

კომპიუტერული მონაცემების შეყვანა გულისხმობს იმ კომპიუტერული მონაცემების ჩასმას სხვის კომპიუტერულ სისტემაში, რომლები მანამდე მასში არ არსებულა.[173] კომპიუტერული მონაცემის უნებართვო **ჩასმა**[174] უნდა იყოს გაიგივებული ისეთ ქმედებებთან, რომლებიც უკავშირდება ამა თუ იმ კომპიუტერული მონაცემის სისტემაში ჩაწერას, ატვირთვას, განთავსებას ან მის სისტემაში სხვაგვარი გზით მოქცევას. სწორი ან არასწორი მონაცემების არაავტორიზებული ჩასმა ქმნის ისეთ მდგომარეობას, რომელიც უტოლდება ყალბი დოკუმენტის შექმნას.[175] მაგალითად, მავნე კოდების შეყვანა, როგორებიცაა „ვირუსები“ და „ტრუას ცხენები“, რომლებიც იწვევს კომპიუტერული მონაცემების მოდიფიკაციას.[176] ასევე, მაგალითად, როდესაც პირი მოიძიებს საიდენტიფიკაციო საბუთის შაბლონს და, მაგალითად, პროგრამით ჩასვამს საკუთარ პირად მონაცემებსა და ფოტოსურათს, რათა იგი გაასაღოს ნამდვილ დოკუმენტად.[177]

---

[173] *Bucur, A.* Legal provisions Regarding the Judical Analysis of computer Forgery and Computer Fraud, Union of Jurists of Romanian, Law Review, vol. VII (2), 2017, 69.

[174] „კიბერდანაშაულის შესახებ“ ევროპული კონვენცია იყენებს ტერმინს „***input***“, რაც გულისხმობს კომპიუტერული მონაცემის ჩასმას ისეთი გადამცემი საშუალებებით, როგორიც არის, მაგალითად, კლავიატურა, მიკროფონი, ვიდეო-თვალი, სკანერი და სხვ.

[175] *Council of Europe* – Explanatory Report to the Convention on Cybercrime, Computer-related Forgery (Article 7) გვ. 18
https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf [31.05.2022]

[176] The Explanatory Report to the Convention on the Cybercrime, 2001, პარაგრაფი 61

[177] *Schjolberg, S.*, Computer-related Offences - A presentation at the Octopus Interface - Conference on the Challenge of Cybercrime, Council of Europe, Strasbourg, France, 2004, 12

კომპიუტერული მონაცემის უნებართვო **წაშლა** შეიძლება განხორციელდეს ნებისმიერი ისეთი ფორმით, რომელიც მონაცემს აქრობს კომპიუტერული სისტემიდან/პროგრამიდან. მონაცემის წაშლის ერთ-ერთი ხერხია კომპიუტერულ ვირუსის გამოყენება.[178] მაგალითად, დანაშაულთა ერთობლიობისთვის ნასამართლევმა პირმა ელექტრონულ ფოსტაზე მიღებული ნასამართლობის ცნობის ასლზე განახორციელა გარკვეული მანიპულაციები, კერძოდ, წაშალა ერთ-ერთი დანაშაულის შესახებ მითითება და ყალბი ნასამართლობის ცნობა გაუგზავნა დამსაქმებელს.

კომპიუტერული მონაცემის უნებართვო **შეცვლა** გულისხმობს ამა თუ იმ მონაცემის ნიშან-თვისების თუ შინაარსის შეცვლას, ე.ი. მის პირვანდელ ინფორმაციაში ცვლილებების შეტანა. მაგალითად, ა-მ (თავისთვის/სხვის მიერ მატერიალური სარგებლის მიღების მიზნის გარეშე) ელექტრონული მაღაზიის პროდუქტის ფასს ცვლის, აკლებს ერთ ნულს, რა დროსაც დაზარალებულებად გამოდის ელექტრონული მაღაზიის მესაკუთრე.[179]

კომპიუტერული მონაცემის **დაფარვა** შინაარსობრივად გულისხმობდეს სხვადასხვა ხერხების გამოყენებით ამა თუ იმ მონაცემის დანახვის და აღქმისა ხელმისაწვდომობის შეზღუდვას. სავარაუდოდ, უნდა იგულისხმებოდეს მონაცემთა ბლოკირება („ჩახშობა“), რაც ნიშნავს მისი გამოყენების შეფერხებას მისი დაზიანების გარეშე და უნდა გავაიგივოთ აუცილებლად, როგორც მონაცემთა წვდომაზე შეზღუდვა და დაბლოკვა. ნორმის ამგვარი ინტერპრეტაცია შეესაბამება როგორც ბუდაპეშტის კონვენციის განმარტებას, ასევე იურიდიულ ლიტერატურაში არსებულ ინტერპრეტაციებს. (მაგალითად, რუმინეთის სისხლის სამართლის კოდექსის 325-ე მუხლის მიხედვით გამოყენებულია ტერმინი „restricting the access“ - ე.ი. წვდომასთან შეზღუდვა, ასევე იურიდიულ ლიტერატურაში გამოყენებულია ტერმინი დაბლოკვა, ბუდაპეშტის კონვენციის მე-7 მუხლში გვხდება ტერმინი, „დაკავება“).

ასევე, შესაძლებელია, რომ 286[2] მუხლით გათვალისწინებული ქმედება ჩადენილ იქნეს ჩამოთვლილ ხერხთა კომბინაციით, მაგალითად, წაშლითა და ჩასმით ანდა დაფარვითა და ჩასმით.

პირველ ალტერნატიულ ქმედებასთან მიმართებით კიდევ ერთხელ უნდა აღინიშნოს, რომ იგი უნდა განხორციელდეს მოპოვებული/მიღებული ყალბი ოფიციალური კომპიუტერული მონაცემის გამოყენების ან/და მის ნამდვილ/უტყუარ მონაცემად გასაღების მიზნით. ამასთან, არ აქვს მნიშვნელობა მიზანი მიღწეულ იქნა თუ არა, ოფიციალური კომპიუტერული მონაცემის შექმნისთანავე დანაშაული დამთავრებულია.

---

[178] *მამულაშვილი, გ.,* კიბერდანაშაული - 286-ე მუხლის კომენტარი, სისხლის სამართლის კერძო ნაწილი II - ავტორთა კოლექტივი, 2020 წელი. გვ. 198.

[179] *Stein Schjolberg*, COMPUTER-RELATED OFFENCES - A presentation at the Octopus Interface 2004 - Conference on the Challenge of Cybercrime, 15-17 September 2004, Council of Europe, Strasbourg, France. გვ. 12

მეორე ალტერნატიული ქმედებას წარმოადგენს უკვე შექმნილი/მოპოვებული/მიღებული ყალბი ოფიციალური კომპიუტერული მონაცემის გასაღება. 286[2]-ე მუხლის პირველი ნაწილი აკონკრეტებს, რომ ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნა ხდება მისი ნამდვილ/უტყუარ მონაცემად გასაღების მიზნით. ნორმის სისტემური ანალიზი გვკარნახობს, რომ თუ შექმნა ხდება ნამდვილ/უტყუარ მონაცემად გასაღების მიზნით, ბუნებრივია, გასაღებაც უკავშირდება მონაცემის ყალბი ბუნების დაფარვას და მის ავთენტურად მოაზრებას;

286[2] მუხლის დადგენისას კანონმდებლის მიზანი იყო მოეხდინა იმ ქმედების კრიმინალიზაცია, რომელიც თავისი არსით ჰგავს დოკუმენტის გაყალბებას, მაგრამ მისი ჩადენა ხდება ტრადიციულისგან განსხვავებული ხერხით - კომპიუტერული სისტემის/პროგრამის მეშვეობით. კანონმდებლის მიზანი იყო ის, რომ შეექმნა ისეთი ნორმა, რომელიც ანალოგიურ პირობებში გამოიწვევდა იმ პირის დასჯადობას, რომელიც არა თუ ხელშესახები, არამედ ციფრული მონაცემების მიმართ ჩადიოდა უკანონო ქმედებებს. აქედან გამომდინარე, რადგანაც 286[2] მუხლი წარმოადგენს 362-ე მუხლის სპეციალურ გამოვლინებას, გასაღებაში უნდა მოვიაზროთ ყალბი ოფიციალური კომპიუტერული მონაცემის ნებისმიერი ფორმით განკარგვა, ისევე, როგორც ეს 362-ე მუხლის შემთხვევაში ხდება.

მესამე ალტერნატიული ქმედება გულისხმობს ყალბი ოფიციალური კომპიუტერული მონაცემის გამოყენებას, მას კი თან ახლავს იურიდიული მნიშვნელობის შედეგები. გამოყენებაში უნდა მოვიაზროთ ყალბი ოფიციალური კომპიუტერული მონაცემის იმ პირისთვის წარდგენა, ვისაც აქვს მისი შემოწმების უფლება, ასევე მისი ოფიციალური წარდგენა საწარმოში, დაწესებულებასა თუ ორგანიზაციაში.[180] გამოყენება შეიძლება იყოს ერთჯერადი ან სისტემატური და იგი შეიძლება განხორციელდეს ნებისმიერი კანონიერი საქმიანობისთვის თუ ოპერაციისთვის, მთავარია, რომ მსგავს ქმედებებს არ ჰქონდეთ ფინანსური სარგებლის მიღების მიზანი. ფალსიფიცირებული ოფიციალური კომპიუტერული მონაცემის გამოყენების მაგალითად შეიძლება გამოდგეს შემდეგი: “ა”, რომელიც უმაღლესი სასწავლებლის სტუდენტია, ქმნის ყალბ ოფიციალურ კომპიუტერულ მონაცემს - ელექტრონულ მონაცემთა ბაზიდან თავისი ნიშნების ამონაწერიდან შლის რამდენიმე საგნის არასასურველ ქულას. ფალსიფიცირებულ ელექტრონულ ამონაწერს კი აგზავნის სხვადასხვა საგანმანათლებლო პროექტებში მონაწილეობის მისაღებად.

რაც შეეხება უშუალო შედეგს, ის მოიცავს კომპიუტერული მონაცემების მოპოვებას, რომლებსაც რეალურად არ გააჩნიათ შესაბამისი კორესპონდენტი და,

[180] *მამულაშვილი,გ.,* დანაშაული მმართველობის წესის წინააღმდეგ - 362-ე მუხლის კომენტარი, სისხლის სამართლის კერძო ნაწილი II - ავტორთა კოლექტივი, 2020 წელი. გვ. 500

შესაბამისად, საფრთხის შექმნას საზოგადოების ნდობა კომპიუტერული მონაცემების ავთენტურობასა და ნამდვილობაზე.[181]

ის ჩანაწერი, რომელიც 286[2] მუხლის შენიშვნის პირველ ნაწილში გვხვდება, პირდაპირ გადმოტანილია კონვენციის მე-7 მუხლიდან. ეს უკანასკნელი ადგენს, რომ ყალბი კომპიუტერული მონაცემის შექმნა წარმოადგენს სისხლისსამართლებრივად დასჯად ქმედებას, იმისდა მიუხედავად ეს მონაცემი პირდაპირი გზით კითხვადი და აღქმადია, თუ არა. ანალოგიურად აწესრიგებს საკითხს შენიშვნის პირველი ნაწილი, კერძოდ: მნიშვნელობა არა აქვს, არსებობს თუ არა ყალბი ოფიციალური კომპიუტერული მონაცემის პირდაპირ წაკითხვის ან/და აღქმის შესაძლებლობა. ნორმის (კონვენციის მე-7 მუხლის) დანიშნულება ის არის, რომ შექმნას ხელშესახები დოკუმენტების გაყალბების პარალელური დასჯადი ქმედება. მისი მიზანია შეავსოს სისხლის სამართლის ის ვაკუუმი, რომელიც დაკავშირებულია დოკუმენტების გაყალბებასთან, ეს უკანასკნელი მოითხოვს მასში არსებული განცხადებების ვიზუალურ კითხვადობას, განცხადებათა ფიზიკურ განსხეულებას დოკუმენტში, რაც არ ახასიათებს ვირტუალურ სივრცეში არსებულ მონაცემებს.[182]

ყალბი ოფიციალური კომპიუტერული მონაცემი, რომლის პირდაპირ აღქმა ან წაკითხვა შეუძლებელია, შეიძლება მოხვდეს ელექტრონულ სისტემაში სხვადასხვა გზით, მაგალითად, ე.წ. დაფარული სპამის მეშვეობით, როცა მომხმარებლის ელექტრონულ ფოსტაში პირდაპირ არ ჩანს გარკვეული ყალბი კომპიუტერული მონაცემის არსებობა ან სპეციალურად შექმნილი პროგრამა, რომელიც კომპიუტერულ სისტემაში ინსტალირების შემდეგ, სრულად ნიღბავს ყალბ კომპიუტერულ მონაცემს და იგი აღარ არის აღქმადი სისტემის ნებისმიერი მომხმარებლისთვის.

სხვაობა ტრადიციულ გაყალბებასთან

როგორც უკვე აქამდე ითქვა, 286[2] მუხლი წარმოადგენს 362-ე მუხლის სპეციალურ გამოვლინებას, შესაბამისად, მაშინ, როცა ქმედება შეიცავს როგორც ერთი, ისე მეორე მუხლის ნიშნებს, ნორმათა კონკურენცია უნდა გადაწყდეს ზოგადი და სპეციალური მუხლების ურთიერთმიმართების წესით. აქედან გამომდინარე, მიზანშეწონილია განვიხილოთ 286[2]-ე და 362-ე მუხლების გამიჯვნის კრიტერიუმების ცოდნას, რათა კვლავ არ დადგეს ის პრობლემა, რაც 286[2] მუხლის შემოღებამდე არსებობდა. გაყალბების ზოგად ნორმასა და ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნას შორის არსებული განმასხვავებელი ნიშნები:

---

[181] Moise, A.C., Some Remarks Regarding the Criminalization and the Forensic Investigation of the Crime of Computer Forgery in the Romanian Legislation, Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law, Vol. 14(63) Special Issue, 2021, 201-202.

[182] *Council of Europe* – Explanatory Report to the Convention on Cybercrime, Computer-related Forgery (Article 7) გვ. 18
https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf [31.05.2022]

დანაშაულის ჩადენის ხერხი: კომპიუტერთან დაკავშირებული გაყალბება, ჩვეულებრივი, ტრადიციული გაგების გაყალბებისგან, განსხვავდება იმით, რომ ამ დროს ხდება ციფრული დოკუმენტების მანიპულაცია. დანაშაულის ჩადენის ხერხი, 362-ე მუხლით გათვალიწინებული ქმედების შემთხვევაში, შეიძლება იყოს დოკუმენტზე/საბუთზე/ინფორმაციის შემცველ სხვა საგანზე ფიზიკურად განხორციელებული მანიპულაცია (მაგალითად, დოკუმენტის შექმნა კუსტარული წესით). დანაშაულის ჩადენის ხერხს ის სპეციფიკა ახასიათებს, რომ 362-ე მუხლით გათვალისწინებული დანაშაულის დროს პირდაპირ იქმნება ფიზიკური დოკუმენტი ან არსებული ფიზიკური სახის დოკუმენტი განიცდის სხვადასხვაგვარ მანიპულაციებს, 286[2]-ე მუხლის დროს კი, მანიპულაცია ხორციელდება დოკუმენტის ციფრულ ფორმატში.

დანაშაულის საგნის ბუნება: დანაშაულის საგანი შეიძლება არსობრივად ემთხვეოდეს ერთმანეთს ამ ორი მუხლის შემთხვევაში, მაგრამ მათი ბუნება და გამოსახვის საშუალება განსხვავებულია. 286[2] მუხლი მოითხოვს, რომ დოკუმენტი არსებობდეს ციფრული ფორმით, როგორც კომპიუტერული მონაცემი, იგი არ უნდა იყოს განსხეულებული, რაიმე ფიზიკური პარამეტრები არ უნდა ახასიათებდეს და არ უნდა იყოს ხელშესახები, 362-ე მუხლის შემთხვევაში კი დანაშაულის საგანზე მანიპულირება შესაძლებელი ხდება სწორედ იმიტომ რომ იგი ფიზიკურად არსებობს და ექვემდებარება ფიზიკურ ზემოქმედებას.

აღქმადობა და კითხვადობა: როგორც სისხლის სამართლის კოდექსი, ისე კონვენცია „კიბერდანაშაულის შესახებ“ ადგენს, რომ მნიშვნელობა არ აქვს ყალბი ოფიციალური კომპიუტერული მონაცემის პირდაპირ წაკითხვა ან აღქმა შესაძლებელი არის თუ არა. ეს რეგულაცია მიუთითებს კომპიუტერთან დაკავშირებული გაყალბების ფართო შესაძლებლობებზე. თუ ჩვეულებრივი გაყალბების შემთხვევაში აუცილებლია, რომ დანაშაულის საგანი სახეზე იყოს - განსხეულებული, ხელშესახები დანაშაულის საგანი, რომლის არა მარტო არსებობის აღქმაა შესაძლებელი, არამედ მისი შინაარსის გაცნობაც.

სუბიექტური მხარე: სუბიექტური მხრივ, ორივე შემთხვევაში ვხვდებით გასაღების ან გამოყენების მიზანს, მაგრამ რაც შეეხება მოტივს, მას არ აქვს მაკვალიფიცირებელი მნიშვნელობა არცერთი შემადგენლობისთვის. მიუხედავად ამისა, თუ 362-ე მუხლით გათვალისწინებული დანაშაულის ჩადენა (მაგ. პირადობის მოწმობაში მითითებული ასაკის შეცვლა და შემდეგ ამ ყალბი საბუთის გამოყენება) ხდება ანგარების მოტივით, ის საჭიროებს დამატებით კვალიფიკაციას თაღლითობის მუხლით (სსკ. 180).

საინტერესოა, როდესაც კომპიუტერული საშუალების გამოყენებით ხდება რაიმე ფინანსური სარგებლის მიღება (მაგ. თუ პირი სხვისი ანგარიშიდან თანხას უკანონოდ დაეუფლება) ქმედება კვალიფიცირდება სსკ. 286[1] მუხლთან ერთობლიობით, თუ 286[1] მუხლი მოიცავს გაყალბებასაც და არ საჭიროებს ერთობლიობას? მართალია

სამოსამართლო პრაქტიკით, ამაზე მსჯელობა არ ყოფილა, თუმცა კომპიუტერთან დაკავშირებული გაყალბების აღნიშნული და სხვა პრაქტიკულ პრობლემები მიმოხილული იქნება შემდეგ თავში.

3.2.2. პრაქტიკაში არსებული გამოწვევები

კომპიუტერული გაყალბების დანაშაული შეიძლება ჩადენილი იყოს სხვადასხვა მრავალფეროვანი ფორმებით, როგორებიცაა: ვებ სიმულაცია, რომელიც გულისხმობს ყალბი ვებ-გვერდის შექმნას, რომელიც მიმსგავსებულია კარგად ცნობილი კომპანიის ოფიციალურ ვებ-გვერდს, ყალბი ინფორმაციის განთავსება ინტერნეტ სივრცეში, ყალბი ელექტრონული ფოსტის შექმნა და მისი დახმარებით კომუნიკაცია, საჯარო თუ კერძო დაწესებულების კომპიუტერულ ბაზებში მონაცემების ჩასმა, მოდიფიცირება ან წაშლა, ელექტრონული დოკუმენტების შეცვლა.[183]

ერთ-ერთი ყველაზე თანამედროვე მეთოდებით, ყველაზე ხშირად კომპიუტერული გაყალბების დანაშაული შეიძლება ჩადენილი იყოს შემდეგი გზებით: სპამი; პიროვნების იდენტურობის ქურდობა (Identity Theft), ფიშინგი, MITM შეტევა (ე.წ. Man in the Middle).

სპამი:

სპამი განისაზღვრება, როგორც ნებისმიერი არასასურველი კომუნიკაცია, რომელიც ხორციელდება ელექტრონული ფოსტის გამოყენებით.[184] მას ჩვეულებრივ იყენებენ რეკლამის განმთავსებლები, რადგან არ არსებობს საოპერაციო ხარჯები, მათი საფოსტო სიების მართვის გარდა. სპამი საშუალებას აძლევს მავნე პროგრამას მიაღწიოს ადრესატამდე, რომლებიც ნაკლებად სავარაუდოა, რომ ეფექტური იყოს.[185] ევროპის საბჭოს კონვენცია კიბერდანაშაულის შესახებ და საქართველოს სისხლის სამართლის კოდექსი სპამს, როგორც დამოუკიდებელ დანაშაულად არ აცხადებს. კიბერდანაშაულის შესახებ ევროპის საბჭოს კონვენციის მიხედვით, ქმედებების კრიმინალიზაცია უნდა შემოიფარგლოს აუცილებლად მომეტებული საფრთხის და განზრახი დანაშაულებით. მიუხედავად იმისა, რომ სპამი პირდაპირ არ არის რეგულირებული საქართველოს

[183] *Schjolberg, S.,* Computer-related Offences, Council of Europe, A presentation at the Octopus Interface 2004 - Conference on the Challenge of Cybercrime, 15-17 September 2004, 11-12. ასევე, *Moise, A.C.,* Some Remarks Regarding the Criminalization and the Forensic Investigation of the Crime of Computer Forgery in the Romanian Legislation, Bulletin of the *Transilvania* University of Braşov, Series VII: Social Sciences and Law, Vol. 14(63) Special Issue, 2021, 199

[184] Zlati, G. 2020. *Tratat de criminalitate informatică* - Cybercrime Treaty, Volume I, Bucharest: Solomon, 2020, 495. თარგ. *Moise, A.C.,* Some Remarks Regarding the Criminalization and the Forensic Investigation of the Crime of Computer Forgery in the Romanian Legislation, Bulletin of the *Transilvania* University of Braşov, Series VII: Social Sciences and Law, Vol. 14(63) Special Issue, 2021, 199

[185] *Alazab, M., Broadhurst, R.*, An Analysis of the Nature of Spam as Cybercrime. Cyber-Physical Security. Protecting Critical Infrastructure, vol 3. Springer, 2017, 251–266.

სისხლის სამართლის კანონმდებლობაში, ეს ქმედება, უნდა ჩაითვალოს კომპიუტერული სისტემის გაყალბებად.

Identity Theft:

პირის მაიდენტიფიცირებელი მონაცემების ქურდობა აღწერს ისეთ დანაშაულებრივ ქმედებას, რა დროსაც დამნაშავე თაღლითური გზით მოიპოვებს და იყენებს სხვა პირის ვინაობას და მასთან დაკავშირებულ მონაცემებს, მისი ნებართვის გარეშე, რათა ჩაიდინოს დანაშაული.[186] ძირითადად, ბოროტმოქმედები უკანონოდ აგროვებენ და თაღლითური მიზნებისთვის იყენებენ შემდეგი სახის ინფორმაციას: საკრედიტო ბარათის ინფორმაცია (ბარათის ნომერი, ანგარიში), მართვის მოწმობის ინფორმაცია; ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი.[187] დამნაშავე ცდილობს მომხმარებლის მოტყუებას, მათი ბანკის, სადაზღვევო სააგენტოს და ა.შ. სახელით შემოდის კონტაქტში, რომ მოითხოვოს პირადი მონაცემების შეყვანა, რათა შემდეგ ბოროტად გამოიყენოს.[188]

ყველაზე ხშირად პირის მაიდენტიფიცირებელი მონაცემების ქურდობა გამოიყენება შემდგომი დანაშაულებრივი ქმედებებისთვის მოსამზადებლად, როგორიცაა კომპიუტერული თაღლითობა ან კომპიუტერული გაყალბება. პირის მაიდენტიფიცირებელი მონაცემების ქურდობა პირდაპირ არ არის რეგულირებული საქართველოს სისხლის სამართლის კანონმდებლობით, თუმცა შეიძლება ჩაითვალოს 286[2]-ე მუხლის, რომელიც გულისხმობს კომპიუტერული გაყალბების დანაშაულს,[189] ასევე 286[1] მუხლის ფარგლებში, როდესაც ხდება პირის პლასტიკური ბარათის ინფორმაციის მოპოვება. საქართველოში დამკვიდრებული პრაქტიკით, ყალბი სოციალური ქსელების ანგარიშებით განხორციელებული თაღლითობა კვალიფიცირდება მხოლოდ სისხლის სამართლის კოდექსის 180-ე მუხლით და შეფასების მიღმა რჩება ყალბი ანგარიშის შექმნის შეფასება, რომლის დახმარებითაც ხდება დანაშაულის ჩადენა. მიზანშეწონილია, რომ პირის მაიდენტიფიცირებელი მონაცემის ქურდობა თავისი სპეციფიკიდან გამომდინარე, ცალკე, დამოუკიდებელ დანაშაულად დარეგულირდეს.

---

[186] Moise, A.C., Some Remarks Regarding the Criminalization and the Forensic Investigation of the Crime of Computer Forgery in the Romanian Legislation, Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law, Vol. 14(63) Special Issue, 2021, 200.

[187] *Gupta, C. M.,Kumar, D.,* Identity theft: A small step towards big financial crimes. *Journal of Financial* Crime, 27 (3), 2020, 897-910.

[188] *Sepec, M.*, Slovenian criminal code and modern criminal law approach to computer-related fraud: A comparative legal analysis., International Journal of Cyber Criminology, 6(2), 2012, 986

[189] ანალოგიური მიდგომა აქვს რუმინეთის სისხლის სამართლის კოდესს, შეად.: Moise, A.C., Some Remarks Regarding the Criminalization and the Forensic Investigation of the Crime of Computer Forgery in the Romanian Legislation, Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law, Vol. 14(63) Special Issue, 2021, 201-202.

ფიშინგი

ფიშინგი არის სოციალური ინჟინერიის ავტომატიზებული ფორმა, რომლის დროსაც კრიმინალები ამყარებენ კომუნიკაციას მსხვერპლებთან ლეგიტიმური ვებ-საიტების იმიტაციის გზით, რათა მოიპოვონ სენსიტიური ინფორმაცია. ყველაზე გავრცელებული ფიშინგური თავდასხმა იწყება მსხვერპლისთვის ელექტრონული წერილის გაგზავნით, მიმსგავსებული ელ. ფოსტის მისამართიდან, რომელიც რეპუტაციის მქონე დაწესებულების შთაბეჭდილებას ქმნის, მაგრამ რეალურად ფიშერისგან არის.[190] მსხვერპლის შეცდომაში შეყვანის მიზნით, ძირითადად, გამოიყენება დამაბნეველი, ვიზუალურად მსგავსი სიმბოლოები (ე.წ. ჰომოგლიფები) დომენური სახელების შესაქმნელად. შეცდომაში შეყვანილ დანაშაულის სამიზნეს ჰგონია, რომ ოფიციალური კომპანიის ელექტრონული ფოსტა არის, რის შედეგადაც შედის ნდობაში და წერილის მოთხოვნისთანავე ბრმად აწვდის საკუთარ ინფორმაციას.[191]

ფიშინგი შეიძლება იყოს კრიმინალიზებული, როგორც კომპიუტერული გაყალბების დანაშაულის შემთხვევა, ასევე წარმოადგენდეს კომპიუტერული თაღლითობის დანაშაულსაც, რომელიც ეხება მოტყუებით ჩადენილ დანაშაულს, იმ სიტუაციაში, როდესაც ქონებრივ ზიანს აყენებს მსხვერპლს.[192] არსებობს მოსაზრება, რომ ფინანსური ზიანის მიყენების დროს, კვალიფიკაცია ხდება მხოლოდ თაღლითობით, რადგან კიბერთაღლითობის განხორციელების ერთ-ერთ ხერხს წარმოადგენს კომპიუტერთან დაკავშირებული გაყალბება. ამ მოსაზრების მომხრეები ამტკიცებენ, რომ გაყალბებით დაკვალიფიცირდება მხოლოდ ორი სახის აქტივობა, ეს არის ორიგინალური ვებ-გვერდის და ელ. ფოსტის ყალბი მონაცემების შექმნა და სხვა სამართლებრივი შედეგების დადგომის მიზნით.[193]

ფიშინგს რამდენიმე სხვადასხვა კვალიფიკაცია შეიძლება მიეცეს კონკრეტული შემთხვევების გათვალისწინებით.[194] ინტერნეტ ბანქინგი ფიშინგის მიმართ ყველაზე დაუცველი სფეროა. მაგალითად, თბილისის საქალაქო სასამართლოს 2021 წლის 23 ივნისის განაჩენით, პასუხისგებაში მიეცა პირი, რომელმაც უნებართვოდ დაამზადა ე.წ.

---

[190] *Arnell, P., Faturoti, B.,* The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. International Review of Law, Computers & Technology , 2022, 1-23.

[191] ამ დროს ხდება ვებ-საიტების შეტყობინებების გადამისამართება და ვებ-გევრდის ჩანაცვლება (საიტები დაუცველია ჯვარედინი სკრიპტირებისგან) და თავმდასხმელების მიზანმიმართულ ვებ-გვერდზე აწვდიან ინფორმაციას.

[192] ასეთ მსჯელობას ავითარებს რუმინეთის პრაქტიკა, იხ.: *Moise, A.C.,* Some Remarks Regarding the Criminalization and the Forensic Investigation of the Crime of Computer Forgery in the Romanian Legislation, Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law, Vol. 14(63) Special Issue, 2021, 201-202.

[193] იხ.: იქვე. ასევე რუმინეთის სისხლის სამართლის კოდექსის 325-ე მუხლი

[194] *Küpper, G.,* Strafrecht Besonderer Teil 1 Delikte gegen Rechtsgüter der Person und Gemeinschaft by, René Börner, 2017, 200-201.

„ფიშერული“ ბმული, რომელსაც ყალბ შეტყობინებასთან ერთად, ტექსტით: „ძვირფასო მომხმარებელო ეს არის ავტომატური შეხსენება, რომ თქვენს ანგარიშს ახლა აქვს დეპოზიტის შესახებ გაფრთხილება. გთხოვთ, შესასვლელად დააჭირეთ აქ იმისათვის, რომ ნახოთ თვენი ანგარიშზე ჩამოსული თანხა“, აგზავნიდა ელ/ფოსტით service@bankdeposits.ge, რომელიც ვიზუალურად ქმნიდა შთაბეჭდილებას, თითქოს ეკუთვნოდა ერთ-ერთ ავტორიტეტულ ბანკს, რის შემდეგაც შეცდომაში შეყვანილი მომხმარებლები გადადიოდნენ შეტყობინებაში მოთავსებულ „ფიშერულ“ ბმულზე, რომელიც იყო აღნიშნული ბანკის ინტერნეტ ბანკის ვებ-გვერდს მიმსგავსებული ყალბი ვებ-გვერდი, უთითებდნენ ინტერნეტ-ბანკში ავტორიზაციისთვის საჭირო პირად მონაცემებს და ეს ინფორმაცია იგზავნებოდა დამნაშავესთან. მონაცემების მოპოვების შემდეგ, ბოროტმოქმედმა შეაღწია უნებართვოს კომპიუტერულ სისტემაში და დაეუფლა მსხვერპლის თანხას. მოცემული ქმედება დაკვალიფიცირდა ქურდობად, რაც არ არის მართებული.[195] პირველ რიგში, პირმა შექმნა ყალბი ინფორმაცია, მეორე, რომ მოიპოვა მაიდენტიფიცირებელი ინფორმაცია (მობილური ბანკის ანგარიშის მონაცემები), მესამე, რომ შეაღწია უნებართვოთ კომპიუტერულ სისტემაში.

პირველ რიგში, მნიშვნელოვანია შეფასდეს 286[2] მუხლის შემადგენლობა, ვინაიდან დამნაშავე მონაცემებს ისე ცვლის, ამუშავებს და უგზავნის მსხვერპლს, რომ უქმნის წარმოდგენას თითქოს მას ბანკი წერს. კომპიუტერული სიყალბე მდგომარეობს, რომ თავდამსხმელი ცდილობს ელ. ფოსტის მიმღებს შეუქმნას შთაბეჭდილება, რომ გამგზავნი მათი ბანკია.

ყალბი ვებ-გვერდის შექმნაც წარმოადგენს ყალბი მონაცემების დოკუმენტს, მიუხედავად იმისა, რომ დამნაშავე იყენებს საკუთარ, ანუ სწორ IP მისამართს შექმნილი ვებ-საიტისთვის. ამ შემთხვევაში საკმარისია, რომ ადრესატს შეექმნას მცდარი წარმოდგენა. იმისათვის, რომ ვებ-გვერდი ჩაითვალოს გაყალბებულად, საკმარისია, საშუალო დამკვირვებლის პოზიციიდან ის აღიქმებოდეს ნამდვილ ვებ-გვერდთან მიმსგავსებულად, მაგალითად, მსგავსი ვებ-გვერდის დიზაინის გამო.[196] დანაშაულის მთავარი ხიბლი სწორედ ვიზუალური მიმსგავსებაა. ფიშინგური საიტის შექმნა ფაქტობრივად მონაცემების ფალსიფიკაციაა, რადგან ცრუ ინფორმაციის ნადვილად გასაღების მიზანი აქვს ბოროტმოქმედს.

იმ შემთხვევაში, თუ წარმატებით ჩაიარა და მომხმარებელი მოტყუვდა და ამით დამნაშავემ მოიპოვა მონაცემები, როგორიცაა ინტერნეტ ბანკის პაროლი ან სხვა რელევანტური კოდები, პაროლები, უსაფრთოხების ზომები კომპიუტერული სისტემის შეღწევისათვის, დამატებით დაკვალიფიცირდება 285-ე მუხლით. უბრალოდ ელ. ფოსტის გაგზავნა არ შეიცვას 285-ე მუხლით, რადგან პაროლი ჯერ არ მოუპოვებია და

[195] თბილისის საქალაქო სასამართლოს №1/713-21 23 ივნისი 2021 წლის

[196] URL, რომლის ინტერპრეტაციაც მხოლოდ ტექნიკურად მცოდნე მომხმარებლებს შეუძლიათ, ამ მხრივ არაა რელევანტური.

მხოლოდ ელ ფოსტის გაგზავნა პაროლის მოპოვების მიზნით ვერ ქმნის ქმედების შემადგენლობას, შესაბამისად ქმედება მხოლოდ გაყალბებად დაკვალიფიცირდება.

იმ შემთხვევაში, თუ მოხდა პაროლის გამოყენებით, კომპიუტერულ სისტემაში შეღწევა, დამატებით უნდა დაკვალიფიცირდეს მიზნის გათვალისწინებით 284 ან 286 მუხლით. თუ შეღწევამ გამოიწვია დაზარალებულის ფინანსური ზიანი, ამ შემთხვევაში სახეზე იქნება 286[1]-ე მუხლი.

ისმის კითხვა, კომპიუტერთან დაკავშირებულ გაყალბებასა და თაღლითობას აქვს საერთო დანაშაულის ჩადენის ხერხები და პირის მიერ მოხდა მომხმარებლის ან სისტემის მოტყუება, დაკვალიფიცირდება თუ არა მხოლოდ კიბერთაღლითობის მუხლით?

მხოლოდ თაღლითობით კვალიფიკაციის სასარგებლო შეიძლება ითქვას, რომ ისტორიულად, როდესაც ფიშინგის პირველი შემთხვევები წარმოიშვა, ნაწილობრივ ვარაუდობდნენ, რომ პლასტიკური ბარათის მონაცემების, მათ შორის PIN-ის და ანგარიშის მონაცემების გადაცემა, წარმოადგენდა აქტივების (ქონების) განკარგვას, რაც, მართალია, პირდაპირ ზიანს არ აყენებდა, მაგრამ ზიანის ექვივალენტურ საფრთხეს უქმნიდა მსხვერპლის ქონებრივ ინტერესებს. ინფორმაციის გადაცემა უდრის ზიანს, რომელიც შეიძლება მოხდეს ნებისმიერ დროს.[197]

თუმცა, ეს მოსაზრება ვერ იქნება მხედველობაში მისაღები, რადგან ერთის მხრივ, მონაცემთა გადაცემა არ ნიშნავს აქტივების გასხვისებას, რადგან აქტივები პირდაპირ არ არის ხელმისაწვდომი. მეორე მხრივ, მონაცემთა გამჟღავნება არ იწვევს რაიმე პირდაპირ ზიანს.[198] ეს განსაკუთრებით ეხება იმ შემთხვევაში, თუ დამნაშავე თავად არ იყენებს მონაცემებს, არამედ აგროვებს მონაცემთა ერთობლიობას მესამე პირებზე გასაყიდად.

საბოლოდ უნდა ითქვას, რომ როდესაც მაგალითად, თაღლითური მიზნით ქმნიან ყალბ კომპიუტერულ მონაცემს და უგზავნიან პოტენციური მსხვერპლებისთვის, ამ შემთხვევაში ქმედება უნდა დაკვალიფიცირდეს კომპიუტერულ გაყალბებად. თუ ამან გამოიწვია დაზარალებულის ფინანსური ზიანი, ქმედება უნდა დაკვალიფიცირდეს ერთობლიობით მიუხედავად იმისა, რომ საერთო განხორციელების ხერხია, რადგან, როდესაც ხდება ვებ-გვერდის გაყალბება და უბრალოდ დამნაშავე უგზავნის მონაცემს, გამოდის რომ სახეზეა მარტო კომპიუტერული გაყალბება და დანაშაულის კვალიფიკაცია იცვლება შედეგის მიხედვით, რაც არ არის სწორი, თუ გამოიწვია ზიანი და მხოლოდ 286[1] მუხლით გამოიყენება კვალიფიკაციის მიღმა რჩება ისეთი დაცვის ობიექტი, როგორიცაა მონაცემთა უტყუარობა. ფიშინგის დროს, ერთი მხრივ ყალბი ოფიციალური მონაცემის შექმნით ბოროტმოქმედებების მიერ ისეთი დაცვის ობიექტს,

---

[197] ფედერალური სასამართლო წვდომის მონაცემების გამჟღავნებას განიხილავს, როგორც სპეციფიკურ საფრთხეს აქტივებისთვის, რომელიც ეკონომიკური თვალსაზრისით ფინანსური ზარალის ტოლფასია. ასევე, იხ.: https://beck-online.beck.de/?vpath=bibdata/komm/MueKoStGB/cont/MueKoStGB%2Ehtm [06.06.2022].

[198] იხ.: Heinrich, B., Aktuelle Probleme des Internetstrafrechts, Humbolt Forum Recht, 2006, 121 - 125

როგორიცაა მონაცემთა უტყუარობა, ხოლო განხორციელებული შედეგის დროს, იმიტომ კვალიფიცირდება ერთობლიობით, რომ ასევე პირს მიადგა ქონებრივი ზიანი.

ფიშინგთან კავშირში, როდესაც თავდამსხმელები ფიშინგ ელ. წერილებში ემუქრებიან ანგარიშის დაბლოკვით, თუ დაინტერესებული პირი უარს იტყვის მათი დეტალების გამჟღავნებაზე. ასეთი საფრთხის არსებობის შემთხვევაში, სისხლის სამართლის დანაშაულის გამოძალვის სპეციალური შემთხვევა გვექნება სახეზე. კიბერგამოძალვის დამოუკიდებელი შემადგენლობა არ გვაქს, როდესაც ის საკამოდ მაღალი საშიშროებით ხასიათდება, რაც საკანონმდებლო ხარვეზად ითვლება, თუმცა მოცემული საკანონმდებლო ტექნიკის გათვალისწინებით, ეს ქმედება დაკვალიფიცირდება სსკ-ს 286[1] მუხლით.

Man-in-the-Middle შეტევა

Man-in-the-Middle შეტევა არის ციფრული შეტევის სპეციფიკური ფორმა, რომელიც ხშირად მიზნად ისახავს ბანკის კლიენტებს ონლაინ ბანკინგის გამოყენებით. ტექნიკური თვალსაზრისით, თავდამსხმელი ხდება ორ ან მეტ საკომუნიკაციო პარტნიორს შორის, როგორიცაა ბანკის კლიენტი და ბანკი, და ახდენს გავლენას ან ცვლის მათ შორის გაცვლას ისე, რომ იგი აკონტროლებს მონაცემთა ტრაფიკს.

კვალიფიკაციისთვის კიდევ ერთ პრობლემურ სემთხვევას წარმოადგენს თავდასხმა „შუაში მდგომი ადამიანი“ („man in the middle”). სახელწოდებიდან გამომდინარე გასაგები ხდება, თუ რას უნდა გულსიხმობდეს ეს შემთხვევა, მარტივა რომ ვთავქტ, პირობითად ა’ უგზავნის ადრესატს „ბ“ს, თუმცა ტექნიკური უნარ-ჩვევებით გამორჩეულმა „გ“ თავისი მოქმედებით „ა“ს მიერ გადაგზავნილი შეტყობინება გადამიმისამართა საკუთარ თავდან. მაგალითად ფულს როდესაც უგზავნი ბანკს, თუმცა ბანკის ნაცვლად, იცვლება მისამართი და ბოროტმოქმედის მიერ მითითებულ მისამართზე გვხდება.

თუ ბანკის კლიენტი განახორციელებს გადარიცხვას, დამნაშავეს შეუძლია შეცვალოს გადარიცხვის დეტალები. მსხვერპლს უტოვებს შთაბეჭდილებას, რომ ისინი ააქტიურებენ გადაცემას სურვილისამებრ. თავდამსხმელი ცვლის მონაცემებს (გადარიცხვის თანხა, მიმღების ანგარიში და ა.შ.), სანამ ბანკი მიიღებს მათ. ეს საშუალებას აძლევს მიმღებს გადარიცხოს ფული სხვა ანგარიშზე. ონლაინ გადაცემის თვალყურის დევნებით და მონაცემების შეცვლით, მოძალადეს შეუძლია, გარკვეული კომბინაციებით, ჩაიდინოს დანაშაული მტკიცებულებებთან დაკავშირებული მონაცემების გაყალბებით. ამის მიხედვით, დამრღვევს მოუწევს მონაცემების ამოღება, დამალვა, გამოუსადეგარი გამოყვანა ან უკანონოდ შეცვლა. მონაცემთა მოდიფიკაცია ნიშნავს შინაარსის რედიზაინის ნებისმიერ ფორმას. 28 თუ დამნაშავე ცვლის მონაცემებს სათანადო გზით, აძლევს მათ სხვადასხვა საინფორმაციო შინაარსს, მაშინ მონაცემები იცვლება.

დასკვნა

როგორც უკვე არაერთხელ აღენიშნა, დღეს კიბერდანაშაული წარმოადგენს მნიშვნელოვან გამოწვევას. ციფრული ტექნოლოგიების სწრაფი განვითარების უპირატესობებთან, ცხოვრების ყველა სფეროში მათი ჩარევის მასშტაბის ზრდისა და ეკონომიკის დიგიტალიზაციასთან ერთად, იზრდება ახალი საინფორმაციო და საკომუნიკაციო ტექნოლოგიების ბოროტად გამოყენების რისკებიც. კომპიუტერული საკომუნიკაციო ქსელები იქცა თაღლითობის ახალი ხერხების ფორმირების ნიადაგად.

ნაშრომის ფარგლებში მიმოხილული იყო კიბერდანაშაულის და კიბერ მეთოდებით ჩადენილი დანაშაულების დახასიათება და მათი მოწესრიგების სპეციფიკა. ანალიზმა აჩვენა, რომ განსაკუთრებულ სირთულეს წარმოადგენს ფინანსურად მოტივირებული კიბერდანაშაულების რეგულირების საკითხი, რადგან პრობლემურია მათი გამიჯვნა ტრადიციულ დანაშაულებთან, რომლებიც განხორციელებულია კომპიუტერული სისტემის გამოყენებით.

როგორც ნაშრომში წარმოჩნდა, დანაშაულების ობიექტის ხელყოფის კონტექსტში, გარკვეული სადავო პოზიციები არსებობს ქმედების კვალიფიკაციასთან დაკავშირებით. კვლევის ფარგლებში შემოთავაზებულია აღნიშნული პრობლემის შესაძლო გადაჭრის გზები, რაც დაკავშირებულია თითოეული ქმედების დამოუკიდებლად შეფასებასთან და სუბიექტური ელემენტის მხედველობაში მიღებასთან.

საქართველოს საკანონმდებლო ჩარჩოს მიმოხილვამ აჩვენა, რომ მის მოწესრიგებას აქვს არათანმიმდევრული ხასიათი. ერთი მხრივ, კიბერდანაშაულები თავმოყრილია ერთ თავში, თუმცა სხვადასხვა ტრადიციული დანაშაულების თავებში ვხდებით კიბერ მეთოდებით ჩადენილ დანაშაულებს, ძირითად შემადგენლობასთან სინთეზის გზით. მიდგომის არათანმიმდევრულობა განპირობებულია იმით, რომ ისეთი ქმედება, როგორიცაა კიბერ მეთოდებით პირდაპირი თაღლითობა, არ არის შემოთავაზებული სპეციალური შემადგენლობის სახით, როგორც დამამძიმებელი გარემოება. რამდენადაც ტექნოლოგიების გამოყენებით ჩადენილი ტრადიციული თაღლითობის დროს დაზარალებული მეტად მოწყვლადია ინტერნეტ უპირატესობების წინაშე, როგორიცაა დისტანციურობა, ანონიმურობა და სისწრაფე, შესაბამისად, ქმედებიდან მომდინარე საფრთხეებიც უფრო მაღალია. ამიტომაც მიზანშეწონილია, რომ ტრადიციული თაღლითობის მომწესრიგებელ ნორმას დამამძიმებელი გარემოების სახით დაემატოს მისი განხორციელება კომპიუტერული სისტემის გამოყენებით.

რაც შეეხება კიბერდანაშაულებს კლასიკური გაგებით, როგორიცაა ფიშინდი, პირის მაიდენტიფიცირებელი მონაცემების ქურდობა, ჰაკერული დანაშაულები და ა.შ., ისინი უნდა მოწესრიგდნენ დამოუკიდებელი დანაშაულის სახით. კვალიფიკაციასთან

დაკავშირებული პრობლემების ანალიზით დგინდება, რომ ასეთი სპეციფიკური დანაშაულების დახასიათება რთულია ზოგადი მუხლების ინტერპრეტაციით, რადგან საერთო განხორციელების ხერხები გვაქს სახეზე. ვინაიდან ასეთი დანაშაულების ჩადენა აქვს თავისი მახასიათებლები და აქვს ჩამოყალიბებული ფორმა, უნდა მოწესრიგდეს ცალკე დანაშაულად. განსაკუთრებით საკითხი ეხება პირის მაიდენტიფიცირებელი მონაცემების მოპარვას, რომელიც არა მარტო ფინანსურად მოტივირებული კიბერდანაშაულების წინაპირობაა, ასევე სხვა დანაშაულის ჩადენის წინაპირობაც შეიძლება იყოს და მისი ლატენტური ხასიათის გამო მომეტებული საზოგადოებრივი საშიშროების მატარებელია.

საბოლოოდ, ვინაიდან საინფორმაციო ტექნოლოგიები და მათთან ერთად დანაშაულის ჩადენის საშუალებებიც ყოველდღიურად ვითარდება, სამართალი კვალდაკვალ უნდა მიყვებოდეს განვითარებას და არ ჩამორჩეს მას. მართალია, საქართველოს სისხლის სამართლის კოდექსის კიბერდანაშაულის თავი შეესაბამება ბუდაპეშტის კონვენციას, თუმცა საერთაშორისო ინსტრუმენტებისგან განსხვავებით, ეროვნულ მოწესრიგებს მოითხოვს მეტ დეტალიზაციას და დიფერენცირებულ, ეროვნულ გამოწვევებზე მორგებულ მიდგომას.

ბიბლიოგრაფია

I. ნორმატიული აქტები:

1. ევროპის საბჭოს 108-ე კონვენცია: „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ (2005).
2. ევროსაბჭოს კონვენცია „კიბერდანაშაულის შესახებ“ ბუდაპეშტი (2001).
3. ევროპული კონვენცია სისხლის სამართლის საქმეებზე ურთიერთდახმარების შესახებ, სტრასბურგი, 1959 წლის 20 აპრილი.
4. საქართველოს სისხლის სამართლის კოდექსი.
5. საქართველოს სისხლის სამართლის საპროცესო კოდექსი.
6. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“.
7. საქართველოს კანონი „ელექტრონული კომუნიკაციების შესახებ“.
8. საქართველოს კანონი „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“.
9. საქართველოს შინაგან საქმეთა სამინისტრო. 2021 წლის 24 აპრილის განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის კოდექსში ცვლილების შეტანის შესახებ“.
10. საქართველოს 2010 წლის 24 სექტემბრის კანონი №3619

11. საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ," 2012 წლის 1 ივლისი
12. „ინფორმაციული ტექნოლოგიების დანაშაულებრივ გამოყენებასთან ბრძოლაზე"№55.63 და №56/121 რეზოლუციები, გაერო, 2002.
13. „კიბერუსაფრთხოების გლობალური კულტურის შექმნაზე" № 57/239 რეზოლუცია, გაერო, 2002.
14. „კიბერუსაფრთხოების გლობალური კულტურის შექმნასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვაზე" რეზოლუცია №58/199, გაერო, 2003.
15. 2011 წლის 13 დეკემბრის დირექტივა 2011/93/EU ბავშვთა სექსუალურ ძალადობასა და სექსუალურ ექსპლუატაციასთან და ბავშვთა პორნოგრაფიასთან ბრძოლის შესახებ
16. 2013 წლის 12 აგვისტოს დირექტივა 2013/40/EU საინფორმაციო სისტემებზე თავდასხმების შესახებ.
17. „კიბერდანაშაულის შესახებ" 2001 წლის კონვენცია, ევროპის საბჭო. Council of Europe Convention on Cybercrime (CETS No. 185), Council of Europe, 2001,
18. Directive 2006/24/EC of the European Parliament of The council, on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications services or of Public Communications Networks and Amending Directive 2002/58/EC.
19. Resolution adopted by the General Assembly, Combating the criminal misuse of information technologies, on the report of the Third Committee (A/55/593), 22 January 2001.
20. Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA). Done at Brussels, 28 May 2001.
21. Council of Europe Framework Decision "On Combating Fraud and Counterfeiting Non-cash Means of Payment" (CF, 2001).
22. The Virginia Computer Crimes Act Virginia Computer Crimes Act, Virginia Code Section 18.2-152.1 et seq. of 11 April 1984.
23. Computer Fraud and Abuse Act (CFAA)
24. The Counterfeit Access Device and Computer Fraud and Abuse Law of 1984
25. California Comprehensive Computer Data Access and Fraud Act (California Computer Act
26. Computer Misuse Act 1990 / First Published 1990, Reprinted in the United Kingdom by The Stationery Office Limited. - London, 1997
27. IT-Sicherheitsgesetz, ძალაში შევიდა 2015 წელს. იხ. ბმული: https://www.buzer.de/gesetz/11682/index.htm
28. Telekommunikationsgesetz, https://www.gesetze-im-internet.de/tkg_2021
29. Bundesdatenschutzgesetz, https://www.gesetze-im-internet.de/bdsg_2018
30. Council of Europe Framework Decision "On Combating Fraud and Counterfeiting Non-cash Means of Payment", 2001.

II. სასამართლოს გადაწყვეტილებები:

1. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა საგამოძიებო, წინასასამართლო და არსებითი განხილვის კოლეგიის №1/3199-21 26 ნოემბრის 2021 წლის განაჩენი
2. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა საგამოძიებო, წინასასამართლო და არსებითი განხილვის კოლეგიის 2020 წლის 30 ოქტომბრის განაჩენი საქმეზე № 1/2878-20.
3. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა საგამოძიებო, წინასასამართლო და არსებითი განხილვის კოლეგიის №1/713-21 23 ივნისი 2021 წლის
4. თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა საგამოძიებო, წინასასამართლო და არსებითი განხილვის კოლეგიის 15 ნოემბრის 2021 წლის № 1/2544-21 განაჩენი.
5. თბილისის საქალაქო სასამართლოს 2020 წლის 8 ივნისის №1/651-20 განაჩენი;
6. თბილისის საქალაქო სასამართლოს 2020 წლის 5 მარტის №1/618-20 განაჩენი;
7. თბილისის საქალაქო სასამართლოს 2020 წლის 24 ნოემბრის №1/4557-20 განაჩენი;
8. თბილისის საქალაქო სასამართლოს 2020 წლის 6 თებერვლის №1/158-20 განაჩენი;
9. თბილისის საქალაქო სასამართლოს 2020 წლის 12 ნოემბრის №1/4184-20 განაჩენი.
10. United States v. Petersen, 157 U.S. 483
11. United States v. Brown, 381 U.S. 437
12. Unites States v. Michael D. Pirello
13. Regina v. Gold. & Schifreen
14. United States v. Auernheimer
15. United States v. Seidlitz
16. სლოვენიის უზენაესი სასამართლოს გადაწყვეტილებება № I Ips 98/2004
17. სლოვენიის უზენაესი სასამართლოს გადაწყვეტილებება № I Ips 461/2007

III. ქართულენოვანი წყაროები:

1. ზაქარაშვილი უჩ., კიბერდანაშაულის სისხლსამართლებრივი რეგულირების პრობლემების საქართველოში, თბ., 2014.
2. კაცმანი, ა., „კომპიუტერული დანაშაულის სისხლსამართლებრივი და კრიმინალისტიკური დახასიათება“, ჟურნ. „სამართალი“, 2000, № 2.
3. საქართველოს ეროვნული უსაფრთხოების კონცეფცია, საქართველოს მთავრობა, 2008.
4. გოცირიძე, ანდრია, სვანაძე, ვლადიმერ, “კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები,” სსიპ კიბერუსაფრთხოების ბიურო, საქართველოს თავდაცვის სამინისტრო, 2015.

5. მშვიდობაძე ხ. საქართველოს კიბერბარომეტრი, საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი, ანგარიში, 2015.
6. პირველი, გ. „კიბერდანაშაულის შესახებ“ ევროპულ კონვენციასთან საქართველოს სისხლის სამართლის კანონმდებლობის შეუსაბამობით გამოწვეული პრობლემები, სამეცნიერო ჟურნ. „პოლიცია და უსაფრთხოება“, თბ., 2018, №1.
7. პირველი, გ., საინფორმაციო ტექნოლოგიების გამოყენებით ჩადენილ დანაშაულთა კრიმინოლოგიური ანალიზი, თბ., 2017.
8. ლეკვეიშვილი, მ., თოდუა, ნ., მამულაშვილი, გ., სისხლის სამართლის კერძო ნაწილი, ნაწილი II, თბ., 2019.
9. მამულაშვილი გ., კიბერდანაშაული - 286-ე მუხლის კომენტარი, სისხლის სამართლის კერძო ნაწილი II - ავტორთა კოლექტივი, 2020.

IV. უცხოური წყაროები:

1. Lucky L. and Eisenberg J., Renewing U.S. Telecommunications Research, Washington, DC: The National Academies Press, 2006 (https://doi.org/10.17226/11711)
2. Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, (www.securityfocus.com/infocus/1527)
3. Kigerl A., Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories, Social Science Computer Review, 20(10), 2017.
4. Gecko, The criminalization of Phishing and Identity Theft, Computer und Resht, 2005.
5. Gercke M., Understanding cybercrime: Phenomena, challenges and legal response, International Telecommunication Union, 2012.
6. Nogguchi, Search engines lift cover of privacy, The Washington Post, 2004 (www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/)
7. Mitnick K, Simon W., The Art of Deception: Controlling the Human Element of Security, Chapter 4 “Building Trust”, 2002.
8. Yetter, R. B., Darknets, cybercrime & the onion router: Anonymity & security in cyberspace, 2015.
9. Nomokonov V.A., Tropina T.L., Cybercrime as a New Criminal Threat, Journ. Criminology: Yesterday, Today, Tomorrow, №24, 2012.
10. Sieber, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime.
11. Masuda, The Information Society as Post-Industrial Society
12. Andrews, The Legal Challenge Posed by the new Technology, Jurismetrics Journal, 1983.
13. Decker, Ch., Cyber crime: an Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008.
14. Schjolberg, Computers and Penal Legislation, A study of the legal politics and a new technology, 1983.
15. Richard W. Aldrich, Cyberterrorism and computer crimes: issues surrounding the establishmentof an international legal regime, 2000.

16. Ditzion, R., Geddes, E., Computer Crimes, American Criminal Law Review, 2003, L. Rev. 285.
17. Adams, J., Comment, Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet
18. Hatcher, M., McDannell, J., Ostfeld, S.,Computer Crimes, Amrican Criminal Law Review, 1999, Rev. 397
19. Rutrell Y., Sniffers Overhauled For E-Biz, 2000.
20. Goodman M., Why the Police Don't Care About Computer Crime, 10 HARV. J. LAW & TEC., 1997
21. Gordon/Ford, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, № 1, 2006.
22. Sieber, Council of Europe Organised Crime Report, 2004.
23. Walden, I., Computer Crime and Digital Investigations, Oxford: OUP, 2007.
24. Clarke, J., The Awareness and Perception of Spyware amongst Home PC Computer Users, 2006
25. Reich, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security.
26. Tsakalidi G. Vergidis K., A systematic approach toward description and classification of cybercrime incidents Department of Applied Informatics, University of Macedonia.
27. Brenner, Susan W. Cybercrime and the law: Challenges, issues, and outcomes. UPNE, 2012.
28. The Counterfeit Access Device and Computer Fraud and Abuse Law of 1984,
29. Glenn D. Baker, Note, Trespassers Will Be Prosecuted: Computer Crime in the 1990s, 1993.
30. Abrams N., Beale S.S., Klein R., Federal Criminal Law and its Enforcement, 5th ed. , 2010, 205.
31. Ashworth A. J. United Kingdom // The Handbook of Comparative Criminal Law / eds. by K. J. Heller, M. D. Dubber. Stanford; California, 2011.
32. Brenner, Susan W. Cybercrime and the law: Challenges, issues, and outcomes. UPNE, 2012.
33. Kryshevych O., Andrushchenko I., Striltsiv O., Pyvovar Y., Rivchachenko O., Modern methods of computer-related fraud: legal characteristics and qualification, jour. Cuestiones Politicas, Vol. 39 № 68, 2021.
34. Rachavelias, M. G., Online financial crimes and fraud committed with electronic means of payment—a general approach and case studies in Greece, ERA-Forum, Vol.19 (3), 2018.
35. Sepec, M., Slovenian criminal code and modern criminal law approach to computer-related fraud: A comparative legal analysis., International Journal of Cyber Criminology, 6(2), 2012.
36. Dr. Roberto Flor, “Fraud, Computer-related fraud and Identity-related fraud”, Faculty of Law – University of Verona, March 2009.
37. Moise, A.C., Some Remarks Regarding the Criminalization and the Forensic Investigation of the Crime of Computer Forgery in the Romanian Legislation, Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law, Vol. 14(63) Special Issue, 2021

38. Bucur, A. Legal provisions Regarding the Judical Analysis of computer Forgery and Computer Fraud, Union of Jurists of Romanian, Law Review, vol. VII (2), 2017.
39. Schjolberg, S., Computer-related Offences - A presentation at the Octopus Interface - Conference on the Challenge of Cybercrime, Council of Europe, Strasbourg, France, 2004, 12
40. Zlati, G. 2020. Tratat de criminalitate informatică - Cybercrime Treaty, Volume I, Bucharest: Solomon, 2020
41. Alazab, M., Broadhurst, R., An Analysis of the Nature of Spam as Cybercrime. Cyber-Physical Security. Protecting Critical Infrastructure, vol 3. Springer, 2017.
42. Gupta, C. M.,Kumar, D., Identity theft: A small step towards big financial crimes. Journal of Financial Crime, 27 (3), 2020.
43. Arnell, P., Faturoti, B., The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. International Review of Law, Computers & Technology , 2022.
44. Darius Sauliūnas, D., "Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convenction on Cybercrime, 11.
45. Трофимова Д. Н., Базавлуцкая С. В., Киберпреступность, жур. Молодой ученый, 2020, № 15 (30).
46. Простосердов М.А., Экономические преступления, совершаемые в киберпространстве, и меры противодействия, Дис., 2016.
47. Чернякова А. В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации, Юридическая наука и правоохранительная практика, № 4 (46), 2018.
48. Зигмунт О.А., Петровский А.В., Кибер и интернет-преступность в Германии и России: возможности сравнительного исследования, Юридическая наука и правоохранительная практика, №4 (34), 2015.
49. Semykina O.I., Combating Cyber Crimes in Foreign Contries, Журнал зарубежного законодательства и сравнительного правоведения, 2016.
50. Уголовный кодекс Франции / науч. ред. Л.В. Головко, Н.Е. Крыловой; пер. с фр. Н.Е. Крыловой. СПб.: Юрид. центр Пресс, 2002.
51. Маймеску С. Информационные преступления и преступления в области электросвязи, Комментарий к Уголовному кодексу Республики Молдова. Общая и Особенная части. Кишинэу, 2010.
52. Дмитришен М, Гончаров И. Мошенничество в информационных технологиях.
53. Wiesbaden, S., Cybercrime: Bundeslagebild, 2013.
54. Odenthal R. Korruption und Mitarbeiterkriminalitat: Wirtschaftskriminalitat vorbeugen, erkennen und aufdecken. 2., vollstandig Qberarbeitete und erweiterte Auflage. Gabler I GWV Fachverlage GmbH, Wiesbaden, 2009.

55. Küpper, G., Strafrecht Besonderer Teil 1 Delikte gegen Rechtsgüter der Person und Gemeinschaft by, René Börner, 2017.
56. Heinrich, B., Aktuelle Probleme des Internetstrafrechts, Humbolt Forum Recht, 2006.
57. ISTAG's Report on Revising Europe's ICT Strategy, 2009, 4
58. UN General Assembly, Crime prevention and criminal justice. Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, resolution, adopted at the 68th plenary meeting, 14 Dec. 1990.
59. ITU Toolkit for Cybercrime legislation, American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law, 2010.
60. Georgia ranks 9th in Europe for cyber security," Agenda.ge, April 2, 2019,
61. "Global Cybersecurity Index (GCI)," International Telecomincation Union (ITU) 2018.

V. ელექტრონული წყაროები:

1. https://doi.org/10.17226/11711 [18.04.2022].
2. www.securityfocus.com/infocus/1527 [18.04.2022].
3. www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/ [18.04.2022]
4. https://www.investopedia.com/terms/m/mooreslaw.asp [06.05.2022]
5. https://www.insidehook.com/article/history/melissa-virus-changed-internet [07.05.2022]
6. https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/itu-toolkit-for-cybercrime-legislation-%28draft%29.pdf [07.05.2022]
7. https://cybercrime.org.za/worm/#:~:text=A%20computer%20worm%20is%20a,features%20found%20on%20many%20computers [07.05.2022].
8. https://dspace.nplg.gov.ge/bitstream/1234/144787/1/Kibertavdacva.pdf [07.05.2022]
9. https://mod.gov.ge/uploads/2018/pdf/TAD-ENG.pdf [08.05.2022]
10. https://www.gov.ge/files/469_59439_212523_14.pdf [08.05.2022]
11. https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150 [08.05.2022]
12. https://www.un.org/press/en/2003/pi1550.doc.htm [08.05.2022]
13. https://www.coe.int/en/web/cybercrime/parties-observers [08.05.2022]
14. https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan2022-p/1680a564bb [08.05.2022]
15. https://ccdcoe.org/organisations/au/ [08.05.2022]
16. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093 [08.05.2022]
17. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040 [08.05.2022]
18. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en [08.05.2022]
19. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [08.05.2022]
20. https://www.ejn-crimjust.europa.eu
21. http://www.chebucto.ns.ca/Current/HalifaxSummitG7/ [08.05.2022]

22. https://www.congress.gov/bill/98th-congress/house-bill/5112 [10.05.2022]
23. https://www.legislation.gov.uk/ukpga/1990/18/contents [10.05.2022]
24. https://www.lewik.org/term/15792/computer-fraud-section-263a-german-criminal-code/ [10.05.2022].
25. https://info.parliament.ge/file/1/BillReviewContent/268580 [02.06.2022].
26. https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf [31.05.2022]