ივანე ჯავახიშვილის სახელობის
თბილისის სახელმწიფო უნივერსიტეტი
იურიდიული ფაკულტეტი

სამართლის ჟურნალი

№1, 2019

უნივერსიტეტის
გამომცემლობა

UDC (უაკ) 34(051.2)
ს-216

გამოცემულია ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის საუნივერსიტეტო საგამომცემლო საბჭოს გადაწყვეტილებით

ISSN 1987-7668

თამარ გეგეშიძე*

ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში

წინამდებარე ნაშრომში განხილულია ინტერნეტკომუნიკაციის მოპოვების ფარულ საგამოძიებო მოქმედებასთან დაკავშირებული ქართული კანონმდებლობა და საერთაშორისო სტანდარტები. თანამედროვე ტექნოლოგიების სწრაფი განვითარების პირობებში ფარული მეთვალყურეობის სფეროში პირადი ცხოვრების დაცვის საკითხი მნიშვნელოვან გამოწვევად იქცა. მას შემდეგ, რაც საქართველოს საკონსტიტუციო სასამართლომ 2016 წლის 14 აპრილის გადაწყვეტილებით არაკონსტიტუციურად ცნო კომუნიკაციის რეალურ დროში მოპოვების ფარული საგამოძიებო მოქმედებების მარეგულირებელი გარკვეული დებულებები, მოცემული საკითხი განსაკუთრებით აქტუალური გახდა ქართულ რეალობაში. აღნიშნულის გათვალისწინებით, ნაშრომის მიზანია საქართველოს საკონსტიტუციო სასამართლოს მიერ დადგენილი კონსტიტუციურსამართლებრივი სტანდარტებისა და კანონმდებლობაში განხორციელებული ცვლილებების განხილვა, ინტერნეტკომუნიკაციის მონიტორინგის ღონისძიებასთან დაკავშირებული ცალკეული პრობლემატური საკითხების გაანალიზება და ამ სფეროში შემუშავებული საუკეთესო უცხოური პრაქტიკის წარმოჩენა.

საკვანძო სიტყვები: ინტერნეტკომუნიკაციის მონიტორინგი, პირადი ცხოვრების უფლება, ფარული მეთვალყურეობის ღონისძიებები, კომუნიკაციის რეალურ დროში მოპოვება, ფარული საგამოძიებო მოქმედებები.

1. შესავალი

საინფორმაციო ტექნოლოგიებმა, განსაკუთრებით კი ინტერნეტმა, ფუნდამენტური ცვლილებები შეიტანა საზოგადოების ცხოვრების წესში.[1] დიდი მოცულობის ინფორმაციის მთელი მსოფლიოს მასშტაბით სწრაფად და ნაკლები ხარჯებით გავრცელების გზით ინტერნეტმა გარდაქმნა კომუნიკაციის არსებული შესაძლებლობები.[2] ინტერნეტკომუნიკაცია გამოყენების თვალსაზრისით არ ჩამოუვარდება კომუნიკაციის ტრადიციულ მეთოდებს, როგორიცაა, მაგალითად, სატელეფონო კომუნიკაცია. „პირებს შორის გაცვლადი ინფორმაციის ოდენობის, შინაარსის, თვისებრიობის, სახეობის თვალსაზრისით, ფაქტობრივად, არ არსებობს სხვაობა ტელეფონითა და ინტერნეტით ინფორმაციის გაცვლისას. მეტიც, გამოყენების ინტენსივობის თვალსაზრისით და, შესაბამისად, ინფორმაციულობის ხარისხის, მოცულობის მიხედვით, დღევანდელ დღეს ინტერნეტკომუნიკაცია ბევრად უფრო ინფორმაციული შეიძლება იყოს. შესაბამისად, ამ სივრცეში უკონტროლო შეღწევა ბევრად უფრო ინტენსიურ ჩარევას შეიძლება იწვევდეს პრივატულ სფეროში და, შედეგად, არღვევდეს ადამიანების ფუნდამენტურ უფლებებს.“[3]

თანამედროვე ტექნოლოგიური პროგრესის ფონზე თანდათან იზრდება სახელმწიფოს ტექნიკური შესაძლებლობები ელექტრონული მეთვალყურეობის სფეროში. ელექტრონულ კომუნიკაციას შეუძლია გამოავლინოს ყველაზე ინტიმური და სენსიტიური დეტალები პიროვნების შესახებ, მათ შორის, მისი წარსული და სამომავლო საქმიანობა. შესაბამისად, კომუნიკაციებს დიდი მტკიცებულებითი ღირებულება გააჩნია.[4]

---

* ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი.

1 *Wright J.,* Necessary and Inherent Limits to Internet Surveillance, Internet Policy Review, Vol. 2, Issue 3, 2013, 1.

2 *Clough J.,* Principles of Cybercrime, New York, 2010, 135.

3 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, 55-56.

4 Report of the Special Rapporteur “On the Promotion and Protection of the Right to Freedom of Opinion and Expression”, 17.04.2013, 4, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>, [02.04.2019].

ინტერნეტკომუნიკაციის საშუალებებით გადაცემული ინფორმაციის მოპოვება და სისხლის სამართლის პროცესში გამოყენება საქართველოს კონსტიტუციის მე-15 მუხლით, ადამიანის უფლებათა და ძირითად თავისუფლებათა ევროპული კონვენციის (შემდგომში – კონვენცია) მე-8 მუხლით, ადამიანის უფლებათა საყოველთაო დეკლარაციის მე-12 მუხლითა და სხვა არაერთი საერთაშორისო სამართლებრივი აქტით უზრუნველყოფილი პირადი ცხოვრების უფლების განსაკუთრებით ინტენსიურ შეზღუდვას წარმოადგენს. ინტერნეტსივრცეში საზღვრების არარსებობისა და თანამედროვე ტექნოლოგიების მზარდი განვითარების პირობებში, კომუნიკაციის მონიტორინგის პროცესში პირადი ცხოვრების დაცვა უკვე აღარ არის მხოლოდ ერთი სახელმწიფოს გამოწვევა და გლობალურ ხასიათს ატარებს. აღსანიშნავია ისიც, რომ რამდენიმე წლის წინ ე.წ. „უკანონო მოსმენების“ საკითხი საქართველოში მთელი სიმძაფრით წამოიჭრა. 2014 წლის აგვისტოდან მოყოლებული, როდესაც საქართველოს პარლამენტმა მიიღო ახალი საკანონმდებლო პაკეტი ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით, ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების პროცესში პირადი ცხოვრების დაცვის საკითხი აქტუალურობას არ კარგავს. ამასთან, საქართველოს საკონსტიტუციო სასამართლომ 2016 წლის 14 აპრილის გადაწყვეტილებით ინტერნეტურთიერთობის მონიტორინგის[5] (ასევე სატელეფონო მოსმენის) ღონისძიებასთან დაკავშირებული გარკვეული დებულებები კონსტიტუციურსამართლებრივ სტანდარტთან შეუსაბამოდ მიიჩნია.[6] აღნიშნული გადაწყვეტილების შესრულების მიზნით, ქართულ კანონმდებლობაში 2017 წლის 22 მარტს გარკვეული ცვლილებები განხორციელდა, თუმცა დღევანდელი მდგომარეობით კვლავ მიმდინარეობს დავა საკონსტიტუციო სასამართლოში. მითითებული დავის ფარგლებში მოსარჩელეები მიიჩნევენ, რომ კანონმდებლობაში განხორციელებული ცვლილებები ვერ პასუხობს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით დადგენილ მოთხოვნებს.[7]

აღნიშნულის გათვალისწინებით, წინამდებარე ნაშრომში განხილული იქნება ფარული მეთვალყურეობის სფეროში შემუშავებული პირადი ცხოვრების უფლების დაცვის ძირითადი გარანტიები, ინტერნეტკომუნიკაციის მოპოვების შესაძლებლობები, საკონსტიტუციო სასამართლოს მიერ დადგენილი კონსტიტუციურსამართლებრივი სტანდარტები და ქართულ კანონმდებლობაში განხორციელებული ცვლილებები, აგრეთვე – ინტერნეტკომუნიკაციის მონიტორინგთან დაკავშირებული ცალკეული პრობლემატური საკითხები და საერთაშორისო პრაქტიკა.

2. პირადი ცხოვრების უფლება და მასთან დაკავშირებული ძირითადი გარანტიები ფარულ საგამოძიებო მოქმედებებთან მიმართებით

როგორც უკვე აღინიშნა, ინტერნეტი მსოფლიოს ნებისმიერი წერტილიდან ინფორმაციის გაცვლის უპრეცედენტო შესაძლებლობებს გვთავაზობს. ინტერნეტკომუნიკაციის საშუალებებს მიეკუთვნება თანამედროვე ტექნოლოგიებზე დაფუძნებული და ყველასთვის ხელმისაწვდომი აპ-

[5] 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილებაში საკონსტიტუციო სასამართლომ იმსჯელა საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით (სატელეფონო მოსმენა) და ამავე მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებებზე. გადაწყვეტილებაში 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ინტერკომუნიკაციის რეალურ დროში მოპოვების ღონისძიება მოხსენებულია, როგორც „ინტერნეტკომუნიკაციის მონიტორინგი“, იგივე „ინტერნეტურთიერთობის მონიტორინგი“.

[6] იქვე.

[7] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი.

ლიკაციები თუ ვებგვერდები, როგორებიცაა, მაგალითად, Facebook, Messenger, Skype, Whatsapp, Viber, Gmail და სხვა მრავალი. აღნიშნული პროდუქტები თავდაპირველ ეტაპზე განსხვავდებოდა ერთმანეთისგან ფუნქციურად და ტექნოლოგიურად, თუმცა თანამედროვე ტექნოლოგიების ხელმისაწვდომობამ საშუალება მისცა შემქმნელებს, იმ დონემდე განევითარებინათ პროდუქცია, რომ ზემოთ ჩამოთვლილ და კიდევ სხვა მრავალ პროდუქტს თითქმის მსგავსი სერვისების შეთავაზება შეუძლია მომხმარებლებისთვის. ესენია ინტერნეტტელეფონი (VoIP), ვიდეოზარი, ტექსტური და ხმოვანი შეტყობინებები, ფოტო/ვიდეომონაცემების გაზიარება და ა.შ.

აღსანიშნავია, რომ საქართველოს კონსტიტუციის მე-15 მუხლით დაცულია კომუნიკაციის თავისუფლება, რაც გულისხმობს კომუნიკაციის დაცვას გარეშე პირთა არასასურველი მონაწილეობისგან.[8] კონსტიტუციით დაცულია როგორც სადენიანი, ისე უსადენო ელექტრონული საკომუნიკაციო სისტემებით დამყარებული კომუნიკაცია.[9] ამასთან, პირადი ცხოვრების უფლების დაცვის ქვეშ ექცევა როგორც უშუალოდ კომუნიკაციის შინაარსი, ასევე კომუნიკაციის მაიდენტიფიცირებელი მონაცემები.[10] შინაარსობრივ მონაცემებს მიეკუთვნება, მაგალითად, ელექტრონული ფოსტით გაგზავნილი და მიღებული შეტყობინებები, ინტერნეტტელეფონის საუბრის შინაარსი, ინტერნეტაპლიკაციების და სოციალური ქსელების მეშვეობით გაცვლილი ტექსტური, ხმოვანი და სხვა ციფრული ფორმატის შეტყობინებები, გაგზავნილი და მიღებული ფაილები და სხვ. მაიდენტიფიცირებელ მონაცემებს – იმავე მეტადატას – განეკუთვნება ინფორმაცია, რომელიც წარმოშობილი ან დამუშავებულია კომუნიკაციის განხორციელების შედეგად.[11] აღნიშნული ინფორმაცია შესაძლოა გამოყენებულ იქნეს იმ პირის დასადგენად, რომელთანაც მომხმარებელმა დაამყარა კომუნიკაცია, ასევე შესაძლებელია გამოვლინდეს საშუალება, რომლითაც განხორციელდა კომუნიკაცია, განისაზღვროს კომუნიკაციის დრო და ადგილი. გარდა ამისა, ეს მონაცემები ითვალისწინებს შესაძლებლობას, დადგინდეს, მოცემული დროის მონაკვეთში რა ინტენსივობით განახორციელა მომხმარებელმა კომუნიკაცია კონკრეტულ პირებთან (საქმე Tele2 Sverige AB and Watson).[12] ინტერნეტკომუნიკაციების შემთხვევაში მეტადატას განეკუთვნება, მაგალითად, ინტერნეტპროტოკოლის მისამართი (IP მისამართი), რომელსაც განსაკუთრებული მტკიცებულებითი ღირებულება აქვს გამოძიებისათვის. აღნიშნული მონაცემი შესაძლოა გამოყენებულ იქნეს მისი მფლობელის ვინაობის და ადგილმდებარეობის დასადგენად და მის მიერ ინტერნეტსივრცეში განხორციელებული ქმედებების თვალთვალის მიზნებისათვის.[13] ასევე, ამგვარ მონაცემს წარმოადგენს ელექტრონული ფოსტის გამგზავნა-მიღებასთან დაკავშირებული მონაცემები, ინტერნეტთან წვდომის შესახებ ინფორმაცია, ადგილმდებარეობის შესახებ მონაცემები[14] და სხვ.

---

[8] საქართველოს კონსტიტუციის კომენტარი, თავი მეორე, საქართველოს მოქალაქეობა, ადამიანის უფლებანი და თავისუფლებანი, თბილისი, 2013, 181. წიგნში მოხსენიებულია საქართველოს კონსტიტუციის ძველი რედაქციის მე-20 მუხლი.

[9] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, 28.

[10] იქვე, 61-62. იხ. ასევე Case NC-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and others, [2014], Court of Justice, 34. Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 98-100.

[11] *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, No. 2, 2015, 54.

[12] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 98.

[13] Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 18, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.>, [02.04.2019] .

[14] *Kerr O.S.,* The Next Generation Communications Privacy Act, University of Pennsylvania Law Review, Vol. 162, No. 2, 2014, 384.

როგორც უკვე აღინიშნა, ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვება და სისხლის სამართლის პროცესში გამოყენება პირადი ცხოვრების უფლების განსაკუთრებით სერიოზულ შეზღუდვას წარმოადგენს. ამავდროულად, პირადი ცხოვრების უფლება არ არის აბსოლუტური ხასიათის და სახელმწიფოს შეუძლია მასში გამონაკლის შემთხვევებში მნიშვნელოვანი საზოგადოებრივი ინტერესების გათვალისწინებით ჩაერიოს. ბუნებრივია, სახელმწიფოს უნდა გააჩნდეს ბერკეტი, ტერორიზმიდან და სხვა სერიოზული დანაშაულებიდან მომდინარე საფრთხეების გასანეიტრალებლად გამოიყენოს ფარული მეთვალყურეობის ღონისძიებები, მაგრამ მათი გამოყენება მხოლოდ საგამონაკლისო შემთხვევებში დაიშვება, იმ პირობით, რომ აღნიშნული ღონისძიება ლეგიტიმური მიზნის (სახელმწიფო უსაფრთხოების დაცვის, დანაშაულის ან უწესრიგობის თავიდან აცილების) მიღწევის პროპორციული და აუცილებელი საშუალება იქნება (საქმე კლასი და სხვები გერმანიის წინააღმდეგ).[15]

კონვენციის მე-8 მუხლით გათვალისწინებულ უფლებასთან დაკავშირებულ საქმეებში ევროპული სასამართლო კანონიერების, ლეგიტიმური მიზნისა და პროპორციულობის პრინციპებით ხელმძღვანელობს. კანონიერების პრინციპი აერთიანებს კანონმდებლობაში სამართლებრივი საფუძვლის არსებობისა და ასეთი საფუძვლის „ხარისხის“ მოთხოვნებს. ეს უკანასკნელი კი თავის თავში მოიცავს „კანონის ხელმისაწვდომობისა“ და „განჭვრეტადობის“ კრიტერიუმებს. ევროპულ სასამართლოს არაერთ საქმეზე აღუნიშნავს, რომ „კანონის განჭვრეტადობა“ ფარული მეთვალყურეობის ღონისძიებების კონტექსტში არ არის ანალოგიური შინაარსის, როგორც სხვა მრავალ სფეროში. ამ კონკრეტულ საკითხთან მიმართებით „კანონის განჭვრეტადობა“ არ გულისხმობს პირის შესაძლებლობას, წინასწარ განსაზღვროს, როდის შეიძლება დაექვემდებაროს სამართალდამცავი ორგანოების მხრიდან თვალთვალს და თავისი ქმედებაც აღნიშნულის შესაბამისად წარმართოს. მიუხედავად ამისა, აღმასრულებელი ხელისუფლების საქმიანობის საიდუმლო რეჟიმში განხორციელების გამო თვითნებობის რისკი თვალსაჩინოა. შესაბამისად, აუცილებელია „ნათელი, დეტალური ნორმების“ არსებობა, განსაკუთრებით იმ პირობებში, როდესაც ტექნოლოგია, რომელიც ფარული მეთვალყურეობის ღონისძიების განხორციელების შესაძლებლობას იძლევა, მუდმივად იხვეწება (საქმე მელოუინი გაერთიანებული სამეფოს წინააღმდეგ, ლეანდერი შვედეთის წინააღმდეგ, ვალენზუელა კონტრერასი ესპანეთის წინააღმდეგ, ჰუვიგი საფრანგეთის წინააღმდეგ, ევროპული ინტეგრაციისა და ადამიანის უფლებათა ასოციაცია და ეკიმჯიევი ბულგარეთის წინააღმდეგ, კრუსლინი საფრანგეთის წინააღმდეგ).[16] „ეროვნული კანონმდებლობა უნდა იყოს საკმარისად მკაფიო, რათა მოქალაქეებს მიეცეთ ადეკვატური მითითება იმ გარემოებებისა და პირობების შესახებ, რომელთა არსებობისას სახელმწიფო ხელისუფლების ორგანოები უფლებამოსილნი არიან, გამოიყენონ აღნიშნული ღონისძიებები (საქმე მელოუინი გაერთიანებული სამეფოს წინააღმდეგ, ზახაროვი რუსეთის წინააღმდეგ)“.[17] ევროპული სასამართლოს განმარტებით, ვინაიდან ამ ღონისძიებების პრაქტიკაში აღსრულება არ არის მისი ადრესატებისა და მთლიანად საზოგადოებისთვის საჯარო, კანონის უზენაესობის პრინციპის საწინააღმდეგო იქნებოდა აღმასრულებელი ხელისუფლებისთვის ან თუნდაც სასამართლოსთვის შეუზღუდავი დისკრეციის მინიჭება. შესაბამისად, თვითნებობის საწინააღმდეგო გარანტიების უზრუნველსაყოფად კანონმდებლობით „საკმარისი სიცხადით“

[15] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 49.

[16] Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67; Leander v. Sweden, [1987], ECtHR, (Ser. A.), 51; Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V, 46; Huvig v. France, [1990], ECtHR, (Ser. A.), 32. Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 75; Kruslin v. France, [1990], ECtHR, (Ser. A.), 33.

[17] Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67; Roman Zakharov v. Russia, [2015] ECtHR, 229.

უნდა დარეგულირდეს აღნიშნული დისკრეციის ფარგლები და მისი განხორციელების წესი (საქმე ზახაროვი რუსეთის წინააღმდეგ).[18] კანონმდებლობამ, რომელიც კერძო კომუნიკაციის ხელშეუხებლობის უფლებაში ჩარევის შესაძლებლობას იძლევა, „დეტალურად უნდა განსაზღვროს გარემოებები, რომელთა შემთხვევაშიც დასაშვებია ამგვარი ჩარევა.“[19]

კონვენციის მე-8 მუხლით უზრუნველყოფილი პირადი ცხოვრების უფლების შეზღუდვა ასევე უნდა წარმოადგენდეს „აუცილებლობას დემოკრატიულ საზოგადოებაში (საქმე კენედი გაერთიანებული სამეფოს წინააღმდეგ, ზახაროვი რუსეთის წინააღმდეგ)“.[20] ფარული მეთვალყურეობის კონტექსტში ევროპულ სასამართლოს არაერთ საქმეზე აღუნიშნავს, რომ საჯარო და კერძო ინტერესების დაბალანსების პროცესში სახელმწიფოები სარგებლობენ მიხედულების გარკვეული ფარგლებით, ეროვნული ინტერესების დაცვის მიზნით აირჩიონ გარკვეული ღონისძიება. თუმცა იქიდან გამომდინარე, რომ ფარული მეთვალყურეობის სისტემას დემოკრატიის დაცვის მოტივით შეუძლია თავადვე გაანადგუროს დემოკრატიული საფუძვლები, აუცილებელია, კანონმდებლობამ უზრუნველყოს თვითნებობისგან დაცვის საკმარისი და ეფექტიანი გარანტიები. ამ თვალსაზრისით, შეფასების დროს მხედველობაში მიიღება საქმის ყველა გარემოება, როგორებიცაა, მაგალითად, „სავარაუდო ღონისძიების ხასიათი, ხანგრძლივობა და ფარგლები, მისი ჩატარების საფუძვლები, მის ჩატარებაზე ნებართვის გამცემი, განმახორციელებელი და ზედამხედველობაზე კომპეტენტური ორგანოები და გასაჩივრების საშუალებები (საქმე კლასი და სხვები გერმანიის წინააღმდეგ, კენედი გაერთიანებული სამეფოს წინააღმდეგ, ზახაროვი რუსეთის წინააღმდეგ, ვებერი და სარავია გერმანიის წინააღმდეგ).“[21] „დემოკრატიულ საზოგადოებაში აუცილებლობის“ მოთხოვნა გულისხმობს, რომ ფარული მეთვალყურეობის ღონისძიება უნდა აკმაყოფილებდეს „მკაცრი აუცილებლობის“ ტესტს, რაც ნიშნავს, რომ „მკაცრად აუცილებელი“ უნდა იყოს, ერთი მხრივ, ზოგადად, დემოკრატიული საფუძვლების უზრუნველსაყოფად, ხოლო მეორე მხრივ, კონკრეტულ სიტუაციაში სასიცოცხლო მნიშვნელობის ინფორმაციის მოპოვების მიზნით (საქმე საბო და ვისი უნგრეთის წინააღმდეგ).[22] პროპორციულობის პრინციპი ასევე მოითხოვს, რომ უფლებაში ჩარევის არჩეული ზომა მიუკუთვნებოდეს შედეგის მისაღწევად გამოსადეგ საშუალებათა შორის ყველაზე ნაკლებად ინტენსიურს.[23]

აღსანიშნავია, რომ საქართველოს კონსტიტუციის მე-15 მუხლი ადგენს კომუნიკაციის ხელშეუხებლობის უფლებაში ჩარევის სამართლებრივ საფუძვლებს. აღნიშნული მუხლის მე-2 პუნქტიდან გამომდინარე, ამ მუხლში ჩამოთვლილ უფლებათა შეზღუდვა დასაშვებია მხოლოდ კანონის შესაბამისად, დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით, სასამართლოს გადაწყვეტი-

---

18 Roman Zakharov v. Russia, [2015] ECtHR, 230.

19 General Comment No. 16 Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation), Human Rights Committee, 1988.

20 Kennedy v. United Kingdom, [2010] ECtHR, 130, Roman Zakharov v. Russia, [2015] ECtHR, 227.

21 Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 49-50; Kennedy v. United Kingdom, [2010] ECtHR, 153; Roman Zakharov v. Russia, [2015] ECtHR, 232. Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI, 106.

22 Szabo and Vissy v. Hungary, [2016] ECtHR, 73.

23 CCPR General Comment No. 27: Article 12 (Freedom of Movement), UN Human Rights Committee, 02.11.1999, 11-16, მითითებული: Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 9, <https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc>, [02.04.2019]; იხ. ასევე International Principles on the Application of Human Rights to Communications Surveillance, <https://en.necessaryandproportionate.org/text>, [02.04.2019].

ლებით ან მის გარეშეც კანონით გათვალისწინებული გადაუდებელი აუცილებლობისას.[24] დანაშაულის გამოძიების მიზნებისათვის ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების წესი და პროცედურა განსაზღვრულია საქართველოს სისხლის სამართლის საპროცესო კოდექსით (შემდგომში სსსკ). სსსკ-ის XVI[1] თავი განსაზღვრავს ფარული საგამოძიებო მოქმედებების განხორციელებასა და მოპოვებული ინფორმაციის გამოყენებასთან დაკავშირებულ სტანდარტებს. ინტერნეტთან მიმართებით ინფორმაციის მიმდინარე რეჟიმში მოპოვების საპროცესო ღონისძიება განსაზღვრულია სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით, კერძოდ, აღნიშნული ნორმის მიხედვით, ფარული საგამოძიებო მოქმედების ერთ-ერთ სახეს მიეკუთვნება ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან (კავშირგაბმულობის საშუალებებთან, კომპიუტერულ ქსელებთან, სახაზო კომუნიკაციებთან და სასადგურე აპარატურასთან მიერთებით), კომპიუტერული სისტემიდან (როგორც უშუალოდ, ისე დისტანციურად) და ამ მიზნით კომპიუტერულ სისტემაში შესაბამისი პროგრამული უზრუნველყოფის საშუალებების ინსტალაცია.[25]

3. ინტერნეტკომუნიკაციის მოპოვების შესაძლებლობები

ფარული მეთვალყურეობის ღონისძიებების ხასიათიდან და საიდუმლო რეჟიმში განხორციელების თავისებურებიდან გამომდინარე, დეტალური ინფორმაცია იმის შესახებ, თუ რომელ ტექნიკურ საშუალებებს იყენებენ სახელმწიფოები ინტერნეტით გადაცემული ინფორმაციის მოპოვების მიზნით, ხშირად არ არის საზოგადოებისათვის ხელმისაწვდომი. თუმცა საერთაშორისო დონეზე არსებულ სხვადასხვა წყაროებში განხილულია სამართალდამცავი ორგანოების მიერ გამოყენებული ძირითადი მეთოდები. მაგალითად, გაეროს სპეციალური მომხსენებლის 2013 წლის 17 აპრილის ანგარიშში გამოყოფილია კერძო კომუნიკაციის მოპოვების რამდენიმე ტექნიკური შესაძლებლობა. აღნიშნული ანგარიშის მიხედვით, სახელმწიფოებს კერძო კომუნიკაციის მონიტორინგის სხვადასხვა ტექნიკურ საშუალებაზე მიუწვდებათ ხელი, მაგალითად, „კონკრეტულ ლოკაციასთან ან პიროვნებასთან მიმართებით ინტერნეტკაბელზე სპეციალური მოწყობილობის დამაგრების გზით შესაძლებელია პიროვნების ონლაინ აქტივობების თვალთვალი, მათ შორის, ინფორმაციის მოპოვება იმასთან დაკავშირებით, თუ რომელ ვებგვერდებს სტუმრობს მომხმარებელი“.[26] კონკრეტული ადრესატების მიმართ გამიზნული ფარული მეთვალყურეობის პარალელურად, ზოგიერთი სახელმწიფო ინტერნეტ და სატელეფონო კომუნიკაციის მასობრივი/ტოტალური მონიტორინგის ტექნიკურ შესაძლებლობებს ფლობს, „ელექტრონული კომუნიკაციის გამტარ ოპტიკურ-ბოჭკოვან კაბელებზე სპეციალური მოწყობილობების დამონტაჟებით შესაძლებელია სატელეფონო და ონლაინ კომუნიკაციის თითქმის სრული კონტროლის მოპოვება“.[27]

გარდა აღნიშნულისა, საერთაშორისო დონეზე არსებულ დოკუმენტებსა თუ სამეცნიერო წრეებში მწვავე დისკუსიისა და განხილვის ქვეშ მოექცა სამართალდამცავი ორგანოების მიერ „კომპიუტერულ სისტემაში ფარული შეღწევის“ მეთოდის (hacking) გამოყენებით ინფორმაციის მო-

---

[24] საქართველოს კონსტიტუციის მე-15 მუხლი, პარლამენტის უწყებანი, 31-33, 24/08/1995.

[25] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, 1431 მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტი, <www.matsne.gov.ge>, [02.04.2019].

[26] Report of the Special Rapporteur “On the Promotion and Protection of the Right to Freedom of Opinion and Expression”, 17.04.2013, 10, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>, [02.04.2019].

[27] ქვე, 11.

პოვების პრაქტიკა. როგორც ცნობილია, აღნიშნული ღონისძიება არაერთი ქვეყნის სამართალდამცავი ორგანოს მიერ გამოიყენება დანაშაულის გამოძიების მიზნებისათვის.[28] თავის მხრივ, „კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიების განმარტება საკმაოდ რთულია, ვინაიდან ეს ტერმინი ღონისძიებათა ფართო სპექტრს მოიცავს".[29] მაგალითად, ერთ-ერთი წამყვანი უფლებათა დამცველი ორგანიზაციის განმარტებით, ამ მეთოდით შესაძლებელია კომპიუტერულ სისტემაზე დისტანციურად წვდომა და პოტენციურად ხელმისაწვდომია სისტემაში შენახული ნებისმიერი მონაცემი.[30] ასევე შესაძლებელია კომუნიკაციის მონიტორინგი რეალურ დროში.[31] გერმანიის საკონსტიტუციო სასამართლო 2008 წლის 27 თებერვლის გადაწყვეტილებაში, რომელიც ეხებოდა კომპიუტერულ სისტემაში ფარულად შეღწევის ღონისძიების კონსტიტუციურობას, განმარტავს, რომ ინფორმაციულ სისტემაში ფარული შეღწევის გზით შესაძლებელია სისტემის გამოყენების კონტროლი, შენახულ მონაცემებზე წვდომა ან სისტემაზე კონტროლის მოპოვება დისტანციურად.[32] ამასთან, კომპიუტერულ სისტემაში ფარული შეღწევა შესაძლებელია სხვადასხვა გზით განხორციელდეს.[33]

აღნიშნული ტექნიკური შესაძლებლობის გამოყენების პრაქტიკას მნიშვნელოვანი ყურადღება დაეთმო გაეროს სპეციალური მომხსენებლის ზემოაღნიშნულ ანგარიშში, რომელშიც ხაზგასმულია, რომ, პირადი ცხოვრების მსგავსად, ინტენსიური მეთოდების გამოყენება, როგორიცაა, მაგალითად, „ე.წ. ტროიანი (ჯაშუში პროგრამა)", წარმოადგენს სერიოზულ გამოწვევას ელექტრონულ კომუნიკაციებზე ფარული თვალთვალის ტრადიციული ფორმებისთვის, სცდება აქამდე არსებული სამართლებრივი რეგულირების ფარგლებს და, ადამიანის უფლებების დაცვის თვალსაზრისით, განსაკუთრებით შემზღუდველ ხასიათს ატარებს.[34]

აღსანიშნავია, რომ დღესდღეობით ინტერნეტსივრცეში სულ უფრო იზრდება კომუნიკაციის დაშიფვრის გამოყენების პრაქტიკა. დაშიფვრა სტანდარტული და აუცილებელი საშუალებაც კი გახდა, რომელიც უზრუნველყოფს, ერთი მხრივ, მონაცემთა უსაფრთხოებას, მეორე მხრივ კი, კერძო პირებს შორის კომუნიკაციის დაცვას გარეშე პირთა ხელმისაწვდომობისგან. ინტერნეტსივრცეში დაშიფვრის ფართო მასშტაბებით გავრცელება არსებით ზეგაგავლენას ახდენს სახელმწიფოს

---

28 *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices (Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs), Policy Department for Citizens' Rights and Constitutional Affairs, 2017, 42-43, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019]. იხ. ასევე *Winter L.B.,* Remote Computer Searches under Spanish Law: The Proportionality Principle and the Protection of Privacy, Zeitschrift für die Gesamte Strafrechtswissenschaft, Vol. 129, No 1, 2017, 211-212.

29 Encryption and Anonymity Follow-up Report, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2018, 7, <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>, [02.04.2019].

30 Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 8, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>, [03.04.2019].

31 იქვე.

32 BVerfG, Judgment of the First Senate of 27th February 2008 - 1 BvR 370/07.

33 *Vaciago G., Ramalho D.S.,* Online Searches and Online Surveillance: The Use of Trojans and other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, Vol.13, 2016, 88-89, <http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252>, [03.04.2019].

34 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 17.04.2013, 10, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>, [02.04.2019].

მიერ ინფორმაციის მოპოვების შესაძლებლობებზე.[35] იქიდან გამომდინარე, რომ ძირითადი აპლიკაციების და სოციალური ქსელების მეშვეობით წარმოებული კომუნიკაცია ინტერნეტსივრცეში დაშიფრული სახით გადაიცემა, ადგილობრივი ოპერატორები (ინტერნეტსერვისის მიმწოდებლები) მოკლებული არიან აღნიშნული ინფორმაციის წაკითხვის შესაძლებლობას.[36] შესაბამისად, ამ ინფორმაციაზე წვდომის აპრობირებულ მეთოდს წარმოადგენს მისი გამოთხოვა უშუალოდ ვებსერვისების ან აპლიკაციების მწარმოებელი კომპანიებისგან (Facebook, Instagram და სხვ.). ამასთან, დაშიფვრის სხვადასხვა სახეები არსებობს, ზოგიერთი სერვისის მიმწოდებელი, როგორიცაა, მაგალითად, Google ან Dropbox, ახორციელებს მონაცემების შენახვას დაშიფრული სახით და განშიფვრის ტექნიკურ შესაძლებლობას თვითონ ფლობს. ასეთი ინფორმაციის მოპოვება შესაძლებელია აღნიშნული სერვისის მიმწოდებლის მეშვეობით.[37] სხვა ტიპის დაშიფვრის შემთხვევაში (End-to-End დაშიფვრა) კომუნიკაციის განშიფვრის ტექნიკური შესაძლებლობა (დაშიფვრის „გასაღები“) გააჩნიათ მხოლოდ კომუნიკაციის მხარეებს თავიანთ კომპიუტერებში ან სმარტფონებში და, შესაბამისად, კომუნიკაციის შინაარსი სერვისის მიმწოდებლისთვისაც არ არის ხელმისაწვდომი.[38] აქედან გამომდინარე, ამ მეთოდით დაშიფრული ინფორმაციის მოპოვება სამართალდამცავი ორგანოებისთვის საკმაოდ პრობლემურია.[39] აღსანიშნავია, რომ, როგორც წესი, დაშიფვრა იცავს მხოლოდ კომუნიკაციის შინაარსს და არა მის მაიდენტიფიცირებელ მონაცემებს, როგორიცაა, მაგალითად, ინტერნეტპროტოკოლის მისამართი (IP მისამართი).[40] ასევე დაუშიფრავი სახით შეიძლება იყოს ხელმისაწვდომი ინფორმაცია იმის შესახებ, თუ რა ვებგვერდებს ეწვია მომხმარებელი.[41]

როგორც უკვე აღინიშნა, კერძო კომპანიების მფლობელობაში განუზომელი რაოდენობის ინფორმაცია გროვდება. ამასთან, ვინაიდან ელექტრონული ინფორმაციის გადინება არ არის შეზღუდული სახელმწიფოს ეროვნული საზღვრებით, მონაცემები შეიძლება ინახებოდეს ტრანსნაციონალურ დონეზე და არა იმ ქვეყანაში, სადაც მოხდა მისი შეგროვება ან სადაც იმყოფება მონაცემთა სუბიექტი.[42] სერვისმიმწოდებელთან შენახული ინფორმაციის გამოთხოვა შესაძლოა განხორციელდეს სერვისის მიმწოდებლისადმი პირდაპირი მიმართვის გზით ან იმ სახელმწიფოს სამართალდამცავ ორგანოებთან თანამშრომლობის მეშვეობით, რომლის იურისდიქციაშიც იმყოფება შესაბამისი სერვისის მიმწოდებელი.[43] ტრანსნაციონალური მოთხოვნები მონაცემთა „ნებაყოფლობით“ გადაცემის მიზნით – საერთაშორისო დონეზე სტანდარტული პროცედურაა. ამ გზით სახელმწიფოს შე-

---

35 *Swire P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 203.

36 *Swire P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 202.

37 *Corn G.S., Brenner-Beck D.,* "Going Dark": Encryption, Privacy, Liberty and Security in the "Golden Age of Surveillance", The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E.,* (eds), New York, 2017, 334.

38 იქვე, 335.

39 იქვე, 334-335, იხ. ასევე *Swire. P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 202.

40 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 22.05.2015, 4, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement>, [27.03.2019].

41 Encryption and Anonymity Follow-up Report, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2018, 18, <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>, [02.04.2019].

42 *Haase A., Peters E.,* Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance, International Data Privacy Law, Vol. 7, No. 2, 2017, 126.

43 იქვე.

უძლია თავი დააღწიოს საერთაშორისო თანამშრომლობის ფორმალიზებულ პროცესს.[44] თუმცა ინფორმაციის გამოთხოვა პირდაპირ სერვისის მიმწოდებლისგან შესაძლოა მრავალ პრაქტიკულ სირთულესთან იყოს დაკავშირებული, როდესაც სერვისის მიმწოდებელი იმყოფება უცხო სახელმწიფოს იურისდიქციის ქვეშ. მოთხოვნის გამგზავნი სახელმწიფო, ბუნებრივია, არ ფლობს სამართლებრივ ბერკეტს, აიძულოს უცხო იურისდიქციაში დაფუძნებული კომპანია, მასთან ითანამშრომლოს და მიაწოდოს სასურველი ინფორმაცია. შესაბამისად, ეს თანამშრომლობა პრაქტიკაში, როგორც წესი, ნებაყოფლობით საწყისებზე ხორციელდება.[45]

როგორც ვხედავთ, გამოძიების მიზნებისათვის ინტერნეტკომუნიკაციის მოპოვების სხვადასხვა გზა არსებობს. სისხლის სამართლის პროცესში ინტერნეტით განხორციელებული კომუნიკაციის მოპოვების ძირითადი შესაძლებლობების უკეთ გააზრების მიზნით, ინფორმაციის რეალურ დროში მოპოვების შესაძლებლობების პარალელურად, ასევე განხილულ იქნა ვებსერვისებისა და აპლიკაციების მწარმოებელი კომპანიებისგან მათთან შენახული ინფორმაციის გამოთხოვის საკითხებიც.

4. საქართველოს საკონსტიტუციო სასამართლოს მიერ დადგენილი სტანდარტები და კანონმდებლობაში განხორციელებული ცვლილებები

2016 წლის 14 აპრილის გადაწყვეტილებით საქართველოს საკონსტიტუციო სასამართლომ არაკონსტიტუციურად ცნო „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის ის ნორმა, რომელიც ფარული საგამოძიებო მოქმედებების განსახორციელებლად შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს – სახელმწიფო უსაფრთხოების სამსახურს – ანიჭებდა უფლებამოსილებას, „ჰქონოდა კავშირგაბმულობისა და კომუნიკაციის ფიზიკური ხაზებიდან და მათი შემაერთებლებიდან, მეილსერვერებიდან, ბაზებიდან, სასადგურე აპარატურიდან, კავშირგაბმულობის ქსელებიდან და კავშირგაბმულობის სხვა შემაერთებლებიდან ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობა და ამ მიზნით კომუნიკაციის აღნიშნულ საშუალებებთან, საჭიროების შემთხვევაში, უსასყიდლოდ განეთავსებინა მართლზომიერი გადაჭერის მენეჯმენტის სისტემა, სხვა სათანადო აპარატურა და პროგრამული უზრუნველყოფის საშუალებები“. არაკონსტიტუციურად იქნა მიჩნეული არა ზოგადად კომუნიკაციის რეალურ დროში მოპოვების ინსტიტუტი, არამედ ამ უფლებამოსილებით „გამოძიებაზე პასუხისმგებელი“ და „პროფესიულად დაინტერესებული“ ორგანოს – სახელმწიფო უსაფრთხოების სამსახურის აღჭურვა.[46]

გადაწყვეტილებაში ნორმების არაკონსტიტუციურობის ერთ-ერთ არგუმენტად მითითებულია ის გარემოება, რომ კანონმდებლობა არ ითვალისწინებდა პერსონალურ მონაცემთა დაცვის ინსპექტორის[47] უფლებას, განეხორციელებინა ინფორმაციის რეალურ დროში მოპოვების ტექნიკუ-

---

44 იქვე, 130.

45 *Haase A., Peters E.,* Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance, International Data Privacy Law, Vol. 7, No. 2, 2017, 130-131.

46 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება.

47 კანონმდებლობაში განხორციელებული ცვლილებების შედეგად, 2019 წლის 10 მაისიდან გაუქმდა პერსონალურ მონაცემთა დაცვის ინსპექტორის თანამდებობა და მის უფლებამონაცვლედ ჩაითვალა სახელმწიფო ინსპექტორი და სახელმწიფო ინსპექტორის სამსახური. საკონსტიტუციო სასამართლოს გადაწყვეტილებაში იმ დროს მოქმედი კანონმდებლობის შესაბამისად, მოხსენიებულია „პერსონალურ მონაცემთა დაცვის ინსპექტორი“.

რი ინფრასტრუქტურის „სრული და ყოვლისმომცველი შემოწმება“, რის გამოც ამ პროცესში არ გამოირიცხებოდა მონაცემთა დამმუშავებლების თვითნებობა და უკანონო ქმედება[48].

საკონსტიტუციო სასამართლოში სამართალწარმოების შედეგად დადასტურდა, რომ სახელმწიფოს უფლებამოსილ ორგანოს გააჩნდა შესაძლებლობა, ჰქონოდა „ე.წ. მუდმივი მიერთების სისტემა ინტერნეტპროვაიდერებთანაც“. ასევე დადასტურდა, რომ „დიდ კომპანიებში აქვთ კიდეც განთავსებული ეს აპარატურა“. თუმცა, როგორც გაირკვა, ეს სისტემა გამოუსადეგარია და პრაქტიკაში მიმართავენ ე.წ. „დავირუსების“ ტექნიკას. „კერძოდ, მოწმის სიტყვებით: „მიუხედავად იმისა, რომ ჩვენ რიგ დიდ კომპანიებში გვაქვს ეს აპარატურა განთავსებული რეალურ დროში ინფორმაციის მოპოვებისთვის, ეს სისტემა თავისი არსით არ არის ეფექტური, სწორედ ამიტომაც არ მოხდა ინტერნეტთან მიმართებაში რეალურ დროში ამ არქიტექტურის აწყობა...“.[49]

საკონსტიტუციო სასამართლომ მიიჩნია, რომ „სადავო ნორმები არ მიჯნავს ერთმანეთისგან, რომელი ტექნიკური საშუალება რომელი საგამოძიებო მოქმედებისთვის უნდა გამოიყენოს უფლებამოსილმა ორგანომ“. სასამართლოს შეფასებით, აღნიშნული ნორმებიდან რჩება შთაბეჭდილება, რომ ინტერნეტურთიერთობის მონიტორინგისთვის გამოყენებადია როგორც მართლზომიერი გადაჭერის მენეჯმენტის სისტემა, ასევე „სხვა სათანადო აპარატურა და პროგრამული უზრუნველყოფის საშუალებები“. თუმცა სასამართლო სხდომაზე სახელმწიფო უსაფრთხოების სამსახურის წარმომადგენლის განმარტებით დადგინდა, რომ ინტერნეტთან მიმართებით პრაქტიკაში გამოიყენებოდა მხოლოდ სადავო ნორმებით გათვალისწინებული „სხვა სათანადო აპარატურა და პროგრამული უზრუნველყოფის საშუალებები“. სასამართლოს შეფასებით, ვინაიდან „ინფორმაცია გასაიდუმლოებულია“ და „მინიმალურ დონეზეც კი გამოირიცხება“ იმ „ტექნიკური საშუალებების აუდიტი“, რომელიც გამოიყენება ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების მიზნებისათვის, „აბსოლუტურად არაგანჭვრეტადია ინფორმაცია, თუ როდის, რომელ აპარატურასა და პროგრამული უზრუნველყოფის საშუალებას იყენებს სახელმწიფო. ეს კი გულისხმობს ამ პროცესზე კონტროლის აბსოლუტურ შეუძლებლობას და, შედეგად, უფლების დარღვევის თავისთავად რისკებს.“[50] სასამართლოს განმარტებით, სახელმწიფო არ უნდა იყოს აღჭურვილი „აბსოლუტურად უკონტროლო სივრცით, სადაც არავის არასდროს ეცოდინება, დროის რა პერიოდში, რომელი შემთხვევებისთვის, რა ტიპის/შინაარსის ტექნიკური საშუალებები გამოიყენება და, რაც მთავარია, გამოიყენება თუ არა მხოლოდ კონსტიტუციური მოთხოვნების უპირობო დაცვით.“[51] ასეთ პირობებში აღნიშნული ფარული საგამოძიებო მოქმედების კანონიერებაზე „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით[52] გათვალისწინებული კონტროლის ერთადერთი ბერკეტი – ინსპექტირების შესაძლებლობა, არაეფექტიანად იქნა მიჩნეული.[53]

აღნიშნული გადაწყვეტილების შესრულების მიზნით, საქართველოს კანონმდებლობაში 2017 წლის 22 მარტის საკანონმდებლო პაკეტით რიგი ცვლილებები განხორციელდა ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და სისხლის სამართლის პროცესში

---

48 საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, 59.

49 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, 54.

50 იქვე, 55.

51 იქვე.

52 კანონმდებლობაში განხორციელებული ცვლილებების შედეგად, ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით ინსპექტირების უფლებამოსილება დღეს გათვალისწინებულია „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონში.

53 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, 55.

გამოყენების მიმართულებით. ერთ-ერთ ნოვაციას ამ თვალსაზრისით წარმოადგენს ახალი ორგანოს – ოპერატიულ-ტექნიკური სააგენტოს შექმნა, რომელიც სახელმწიფო უსაფრთხოების სამსახურის მმართველობის ქვეშ მოქმედი საჯარო სამართლის იურიდიული პირის სახით ჩამოყალიბდა და აღიჭურვა ფარული მეთვალყურეობის ღონისძიებების ტექნიკური აღსრულების უფლებამოსილებით.

ცვლილებების შედეგად, ფარული მეთვალყურეობის ღონისძიებებთან დაკავშირებით დადგინდა კომუნიკაციის რეალურ დროში მოპოვების შემდეგი გზები: სტაციონარული, ნახევრად სტაციონარული და არასტაციონარული ტექნიკური შესაძლებლობა. ამასთან, განისაზღვრა, რომ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედება ხორციელდება კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული, ნახევრად სტაციონარული ან არასტაციონარული ტექნიკური შესაძლებლობით.[54]

როგორც უკვე აღინიშნა, დღეს არსებული მდგომარეობით საკონსტიტუციო სასამართლოში ისევ სადავოდ არის გამხდარი ფარული საგამოძიებო მოქმედებების განხორციელებისას სატელეფონო და ინტერნეტკომუნიკაციაზე პირდაპირი წვდომის, ისევე როგორც მაიდენტიფიცირებელი მონაცემების კოპირებისა და შენახვის შესაძლებლობის ოპერატიულ-ტექნიკური სააგენტოსათვის მინიჭების საკითხი. აღნიშნული დავის ფარგლებში, მოსარჩელეებმა მოითხოვეს ინფორმაციის რეალურ დროში მოპოვების ტექნიკურ შესაძლებლობასთან, ასევე კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კოპირებისა და შენახვის უფლებამოსილებასთან დაკავშირებული ნორმების ძალადაკარგულად ცნობა არსებითი განხილვის გარეშე, თუმცა 2017 წლის 29 დეკემბრის საოქმო ჩანაწერით საკონსტიტუციო სასამართლომ მოსარჩელეებს უარი უთხრა სადავო ნორმების არსებითი განხილვის გარეშე ძალადაკარგულად გამოცხადებაზე, ვინაიდან მიიჩნია, რომ ინტერნეტკომუნიკაციებთან, ისევე როგორც ზემოაღნიშნულ სხვა საკითხებთან მიმართებით, სადავო ნორმები არ არის საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით ცნობილი ნორმების იდენტური შინაარსის და კანონმდებლობაში განხორციელებული ცვლილებებით არსებითად შეიცვალა მარეგულირებელი კანონმდებლობა. ამდენად, ინფორმაციის რეალურ დროში მოპოვებასთან, მათ შორის, ინტერნეტკომუნიკაციებთან დაკავშირებული (ასევე, კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კოპირებისა და შენახვის მარეგულირებელი) კანონმდებლობის კონსტიტუციურობას საკონსტიტუციო სასამართლო შეაფასებს არსებითი განხილვის ფორმატში.[55]

აღსანიშნავია, რომ 2016 წლის 14 აპრილის გადაწყვეტილებით ინტერნეტკომუნიკაციის მონიტორინგთან დაკავშირებული ნორმების არაკონსტიტუციურობა საკმარისი გარე კონტროლის მექანიზმების არარსებობამ განაპირობა. ამ თვალსაზრისით, სასამართლომ ხაზი გაუსვა პერსონალურ მონაცემთა დაცვის ინსპექტორის[56] მიერ მოცემული ღონისძიების განსახორციელებლად გამოყენებული ტექნიკური საშუალებების შემოწმების უფლების კანონმდებლობაში რეგლამენტაციის აუცილებლობას. ამ კონტექსტში, 2017 წლის 29 დეკემბრის საოქმო ჩანაწერში საკონსტიტუციო სასა-

---

54 სსსკ-ის 143[3] მუხლის მე-4 ნაწილის „ბ“ ქვეპუნქტი.

55 საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი. აღნიშნული საოქმო ჩანაწერის მიხედვით, ინტერნეტკომუნიკაციებთან, ისევე როგორც განსახილველ სხვა საკითხებთან მიმართებით, სასამართლოს შემადგენლობაში აზრები ორად გაიყო – სამმა მოსამართლემ განსხვავებული მოსაზრება გამოხატა და მიიჩნია, რომ „ინტერნეტკომუნიკაციებთან მიმართებით კანონმდებლობას არ განუცდია იმგვარი არსებითი ცვლილება, რაც აუცილებელს გახდიდა მასზე დამატებით, არსებითად მსჯელობას“.

56 იმ დროს მოქმედი კანონმდებლობის შესაბამისად, საკონსტიტუციო სასამართლოს გადაწყვეტილებაში მოხსენიებულია „პერსონალურ მონაცემთა დაცვის ინსპექტორი“.

მართლომ ინტერნეტთან მიმართებით სადავო ნორმების არსებითად განსახილველად მიღების შესახებ გადაწყვეტილებას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში 2017 წლის 22 მარტს განხორციელებული ცვლილებები დაუდო საფუძვლად, კერძოდ, აქცენტი გაკეთდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 35^1 მუხლის 4^1 პუნქტზე[57], რომელშიც 2017 წლის 22 მარტის ცვლილებებით ხაზგასმით აღინიშნა, რომ „ინსპექტორი უფლებამოსილია შევიდეს სააგენტოს შეზღუდული დაშვების არეალებში და მიმდინარე რეჟიმში დააკვირდეს უფლებამოსილი ორგანოების მიერ საქმიანობის განხორციელებას..., მიიღოს ინფორმაცია ფარული საგამოძიებო მოქმედებების მიზნებისათვის გამოყენებული ტექნიკური ინფრასტრუქტურის შესახებ და შეამოწმოს ეს ინფრასტრუქტურა“.[58] ნიშანდობლივია, რომ, სასამართლო სხდომაზე ინსპექტორის მიერ გაკეთებული განმარტებით, მას ისედაც ჰქონდა ეს უფლებამოსილებები, თუმცა გაწერილი იყო მის ბრძანებაში და არა კანონში.[59]

კვლევის ფარგლებში პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატიდან[60] გამოთხოვილი საჯარო ინფორმაციის თანახმად, „2017-2018 წლებში განხორციელდა სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს 02 (ორი) არაგეგმური შემოწმება ფარული საგამოძიებო მოქმედების განხორციელების შედეგად მონაცემთა დამუშავების კანონიერების შესწავლის მიზნით“.[61] ინსპექტორის აპარატის წერილში მითითებულია, რომ აღნიშნული ინსპექტირების ფარგლებში, მათ შორის, ჩატარდა იმ ტექნიკური ინფრასტრუქტურის შემოწმება, რომელიც განკუთვნილია სსსკ-ის 143^1 მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების განსახორციელებლად. გარდა ამისა, სსსკ-ის 143^1 მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით განსაზღვრული საგამოძიებო მოქმედების განხორციელებისათვის განკუთვნილი ტექნიკური ინფრასტრუქტურის შემოწმება ასევე ჩატარდა 2016 წელს საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ოპერატიულ-ტექნიკური დეპარტამენტის ინსპექტირების ფარგლებშიც.[62]

ყოველივე აღნიშნულიდან გამომდინარე, აშკარაა, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორი (2019 წლის 10 მაისამდე მოქმედი კანონმდებლობის მიხედვით) და მისი უფლებამონაცვლე - სახელმწიფო ინსპექტორის სამსახური, 2016 წლიდან ახორციელებს ინტერნეტურთიერთობის მონიტორინგის ჩასატარებლად გამოყენებული ტექნიკური საშუალებების შემოწმებას. ეს უფლებამოსილება ცხადად იქნა რეგლამენტირებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში 2017 წლის მარტის ცვლილებებით (კანონმდებლობაში შემდგომში განხორციელებული ცვლილებებით, რომელიც ამოქმედდა 2019 წლის 10 მაისიდან, დღეს იგივე უფლებამოსილება გათვალისწინებულია „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კა-

---

57 აღსანიშნავია, რომ, კანონმდებლობაში განხორციელებული ცვლილებების თანახმად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 35^1 მუხლი შემდგომში ამოღებულ იქნა და ინსპექტირებასთან დაკავშირებულ ამ მუხლში გათვალისწინებული უფლებამოსილებები ანალოგიური შინაარსით აისახა „სახელმწიფოს ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-18 მუხლის მე-7 პუნქტში, რომელიც ამოქმედდა 2019 წლის 10 მაისიდან.

58 საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, 58, 65-66.

59 იქვე, 58-59.

60 საჯარო ინფორმაციის გამოთხოვის დროს მოქმედი კანონმდებლობით, დღეს არსებული „სახელმწიფო ინსპექტორის სამსახურის“ ნაცვლად ფუნქციონირებდა „პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი“.

61 პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის საჯარო ინფორმაციაზე პასუხისმგებელი პირის 2019 წლის 21 იანვრის წერილი (№: PDP 7 19 00000216).

62 იქვე.

ნონის მე-18 მუხლის მე-7 პუნქტში), თუმცა როგორც პერსონალურ მონაცემთა დაცვის ინსპექტორმა[63] საკონსტიტუციო სასამართლოში თავადვე დაადასტურა, კანონქვემდებარე აქტით მანამდეც იყო აღჭურვილი ამ შესაძლებლობით. მოცემულ ვითარებაში, შეიძლება ითქვას, რომ საეჭვოა, რეალურად რამდენად განიცადა ინსპექტირების ფუნქციამ ისეთი არსებითი სახეცვლილება, რომლითაც ინსპექტორი მანამდე არარსებული უფლებამოსილებით აღიჭურვა. საბოლოო ჯამში, უნდა აღინიშნოს, რომ ვინაიდან საკონსტიტუციო სასამართლომ არსებითად განსახილველად მიიღო ინტერნეტკომუნიკაციის რეალურ დროში მოპოვებასთან დაკავშირებული ნორმები, არსებული დავის ფარგლებში გადაწყდება, თუ რამდენად საკმარისია „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-18 მუხლის მე-7 პუნქტით გაწერილი ფუნქციები იმისთვის, რათა 2016 წლის 14 აპრილის გადაწყვეტილებაში აღნიშნული „ტექნიკური ინფრასტრუქტურის სრული და ყოვლისმომცველი შემოწმების“ აუცილებლობის მოთხოვნა დაკმაყოფილდეს.

5. ცალკეული პრობლემური ასპექტი და საერთაშორისო პრაქტიკა

საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის საოქმო ჩანაწერში საუბარია იმაზე, რომ ინტერნეტთან მიმართებით სტაციონარული ტექნიკური შესაძლებლობით კომუნიკაციის რეალურ დროში მოპოვება არ ხდება, ვინაიდან ამისათვის აუცილებელია ძვირადღირებული სისტემა და, ამასთან, ნაკლებად ეფექტურია. სისტემის არაეფექტიანობა განპირობებულია ინტერნეტსივრცეში ინფორმაციის დაშიფრული სახით გადაცემის გარემოებით.[64] ამავდროულად, როგორც უკვე აღინიშნა, საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებიდან იკვეთება, რომ ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების მიზნით „პრაქტიკაში მიმართავენ ე.წ. „დავირუსების ტექნიკას“. სამართლებრივ ენაზე, მოქმედი კანონმდებლობის მიხედვით, „დავირუსების ტექნიკა“, სავარაუდოდ, უნდა მოვიაზროთ კომუნიკაციის რეალურ დროში მოპოვების „არასტაციონარული ტექნიკური შესაძლებლობის“ ქვეშ, ვინაიდან „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის თანახმად, არასტაციონარული ტექნიკური შესაძლებლობა განმარტებულია სწორედ, როგორც მონაცემების გადაჭერა „კომუნიკაციის მიმდინარეობისას ან მისი დასრულებისთანავე, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურე ინფრასტრუქტურაზე მიერთების გარეშე, სპეციალური ტექნიკური ან/და პროგრამული საშუალებების გამოყენებით“.[65] რაც შეეხება ნახევრად სტაციონარულ ტექნიკურ შესაძლებლობას, აღნიშნული საშუალების ეფექტიანობასა და პრაქტიკაში გამოყენებადობასთან დაკავშირებით ინფორმაცია ხელმისაწვდომი არ არის.

ნიშანდობლივია, რომ საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებიდან არ ჩანს, თუ რა იგულისხმება „დავირუსების ტექნიკის“ ქვეშ, გადაწყვეტილებაში არ არის განვითარებული მსჯელობა იმასთან დაკავშირებით, თუ რა ტექნიკურ შესაძლებლობაზე არის ამ

---

[63] აღნიშნული საკონსტიტუციო დავის მიმდინარეობის დროს კანონმდებლობა ითვალისწინებდა „პერსონალურ მონაცემთა დაცვის ინსპექტორის“ თანამდებობას.

[64] საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე, 131.

[65] „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-2 მუხლის „ზ“ პუნქტი.

შემთხვევაში საუბარი. როგორც ზემოთ აღინიშნა, საერთაშორისო დონეზე არსებულ დოკუმენტებში, უფლებადამცველი ორგანიზაციების ანგარიშებსა თუ უცხოურ სამეცნიერო ლიტერატურაში აქტიურად განიხილება და მნიშვნელოვანი ყურადღების ქვეშაა მოქცეული კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიება (რომელიც მოიცავს, მათ შორის, „დავირუსების ტექნიკას“[66]) და მასთან დაკავშირებული ტექნიკური შესაძლებლობები, რასაც განაპირობებს, ზოგადი თვალსაზრისით, ამ მეთოდის უაღრესად ინტენსიური ხასიათი და ინფორმაციის ფართო რესურსზე წვდომის შეუზღუდავი პოტენციალი. როგორც ცნობილია, კომპიუტერულ სისტემაში ფარულად შეღწევის შემდგომ შესაძლებელია სხვადასხვა ტიპის ინფორმაციის მოპოვება, ამრიგად, გამოყოფენ ამ მეთოდის სხვადასხვა ფუნქციურ შესაძლებლობებს.[67] აღნიშნულის გათვალისწინებით, გაუგებარია, თუ რა შინაარსის ღონისძიებას მოიაზრებს გადაწყვეტილებაში არსებული ჩანაწერი „ე.წ. დავირუსების ტექნიკასთან“ დაკავშირებით.

ზოგადი თვალსაზრისით, კომპიუტერულ სისტემაში ფარული შეღწევის მეთოდთან მიმართებით უნდა აღინიშნოს, რომ თანამედროვე ინტერნეტსივრცეში ინფორმაციის დაშიფრულ ფორმატში მიმოცვლის პირობებში ეს ღონისძიება შესაძლოა ერთ-ერთი ყველაზე ეფექტიანი და ზოგიერთ შემთხვევაში უალტერნატივო საშუალებაც კი იყოს დანაშაულის გამოძიების მიზნებისათვის, მეორე მხრივ, გასათვალისწინებელია მისი უაღრესად ინტენსიური ხასიათი. ზოგიერთი ევროპული სახელმწიფო პირდაპირ არეგულირებს ამ მეთოდის გამოყენების შესაძლებლობას კანონმდებლობაში, თუმცა, როგორც წესი, ასეთ შემთხვევაში გაცილებით მკაცრი მიდგომა და უფლების დაცვის მნიშვნელოვანი გარანტიებია გათვალისწინებული.[68] კომპიუტერულ სისტემაში ფარულ შეღწევასთან დაკავშირებით კრიტიკის ერთ-ერთ მთავარ ობიექტს სწორედ სპეციალური საკანონმდებლო რეგულაციების არარსებობის პირობებში მისი გამოყენება წარმოადგენს.[69] ამ ღონისძიების განხორციელება დასაშვები შეიძლება იყოს მხოლოდ მკაცრად აუცილებელ შემთხვევებში, „კონკრეტული სამართლებრივი რეგლამენტაციისა“ და ადეკვატური გარანტიების პირობებში.[70] „კონკრეტული ნორმატიული მოწესრიგების მოთხოვნა“ ასევე გულისხმობს, რომ ეს მეთოდი დარეგულირდეს დებულებებით, რომლებიც „მორგებული იქნება მათთვის დამახასიათებელ სპეციფიკას“.[71] ნორმები, რომლებიც განკუთვნილია ფარული მეთვალყურეობის ტრადიციული ფორმებისთვის, მაგალითად,

---

66 BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07.

67 *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 58-59, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019]. იხ. ასევე *Sagers G.,* The Role of Security in Wireless Privacy, წიგნში: Privacy in the Digital Age, 21st-Century Challenges to the Fourth Amendment, (eds.), *Lind N.S., Rankin E.,* Vol.2, California, 2015, 508. Access Now, A Human Rights Response to Government Hacking, 2016, 11, <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf >, [03.04.2019].

68 BVerfG, Judgment of the First Senate of 27th February 2008 - 1 BvR 370/07; *Vaciago G., Ramalho D.S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, 13, 2016, 92, 94-95, <http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252>, [03.04.2019]. იხ. ასევე *Gutheil M., Liger Q., Heetman A., Eager J*. (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 51-54, 58-61, 79-80, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

69 *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 67, <http://www.europarl.europa.eu-/RegData/etudes/-STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

70 Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 18, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>, [03.04.2019].

71 იქვე.

სატელეფონო მოსმენისთვის, არ არის საკმარისი ამ ღონისძიებასთან მიმართებით ადეკვატური გარანტიების უზრუნველსაყოფად. ანალოგიურად, კომპიუტერულ სისტემაში ფარული შეღწევის მეთოდის მარეგულირებელი კანონმდებლობა, რომელიც იმეორებს ელექტრონული მეთვალყურეობის სხვა ღონისძიებების მარეგულირებელ წესებს, მოკლებულია სათანადო დაცვის მექანიზმებს.[72]

როგორც აღინიშნა, „კანონის განჭვრეტადობის“ კონტექსტში აუცილებელია, ფარული მეთვალყურეობის ღონისძიებები დარეგულირდეს ნათელი, მკაფიო სამართლებრივი დებულებებით. მკაფიო და დეტალური ნორმები აუცილებელია ელექტრონული მეთვალყურეობის კონტექსტში კანონიერებისა და პროპორციულობის უზრუნველსაყოფად.[73] ამ საგამოძიებო მოქმედებების ფარული ხასიათიდან და უფლებაში ჩარევის ინტენსივობიდან გამომდინარე, კანონის განსაზღვრულობა ამ კონტექსტში განსაკუთრებით მნიშვნელოვანია.

აღნიშნულ საკითხთან დაკავშირებით ხაზი უნდა გაესვას იმ გარემოებას, რომ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტი, რომელიც არეგულირებს ინტერნეტთან მიმართებით ინფორმაციის მოპოვების საგამოძიებო მოქმედებას, იმდენად ზოგადი სახით არის ჩამოყალიბებული, რომ პრაქტიკულად მოიაზრებს ინფორმაციის მოპოვებას ნებისმიერი საშუალების გამოყენებით. აღნიშნული ნორმა ჯერ კიდევ „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონში იყო განსაზღვრული ფარული საგამოძიებო მოქმედების სახით სსსკ-ში გათვალისწინებამდე და 2014 წელს განხორციელებული ცვლილებების შედეგად უცვლელი სახით იქნა გადმოტანილი საპროცესო კოდექსში. თანამედროვე ტექნიკური პროგრესის პირობებში განსაკუთრებით მნიშვნელოვანია, კანონმდებლობამ ფეხი აუწყოს ინფორმაციული ტექნოლოგიების მოდერნიზების ტემპს. ინფორმაციულ რესურსზე წვდომის დღეს არსებული მრავალმხრივი და ფუნქციურად განსხვავებული შესაძლებლობების ფონზე აშკარაა, რომ აღნიშნული ნორმა ვეღარ პასუხობს სამართლებრივი სიცხადის მოთხოვნებს. საკონსტიტუციო სასამართლო 2016 წლის 14 აპრილის გადაწყვეტილებაში მიუთითებს, რომ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიება მოიაზრებს „სახელმწიფოს მიერ ნებისმიერი ინფორმაციის მოხსნას და ფიქსაციას ყველა კავშირგაბმულობის საშუალებებიდან, კომპიუტერული ქსელებიდან, კომპიუტერული სისტემიდან, რაც, ფაქტობრივად, გულისხმობს როგორც ინტერნეტურთიერთობის მონიტორინგს, ისე კომპიუტერულ სისტემებში არსებულ, შექმნილ/შენახულ ინფორმაციაზე ხელმისაწვდომობის უზრუნველყოფას“.[74] სასამართლოს მიერ გამოყოფილი ეს ორი შესაძლებლობა თავისი შინაარსით აბსოლუტურად განსხვავებულ ღონისძიებებს წარმოადგენს.

საერთაშორისო დონეზე არსებული სხვადასხვა წყაროებისა თუ ევროპული ქვეყნების გამოცდილების გათვალისწინებით, ინტერნეტკომუნიკაციის მოპოვების ღონისძიების მკაფიოდ რეგლამენტაციის საკითხის მნიშვნელობა ასევე ხაზგასმულია „დავირუსების ტექნიკასთან“ მიმართებითაც, კერძოდ, იმ შემთხვევაში, როდესაც დღის წესრიგში დგას კომპიუტერულ სისტემაში ფარულად შეღწევის ღონისძიების განსხვავებული ფუნქციური შესაძლებლობების გამოყენების საკითხი, რეკომენდებულია, რომ ტექნიკური თვალსაზრისით ძირითადი შესაძლებლობები საკანონმდებლო

---

72 Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 18, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>, [03.04.2019].

73 Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23.09.2014, 14-15, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement>, [02.04.2019].

74 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, 38.

დონეზე გაიმიჯნოს და მათი ჩატარება ცალ-ცალკე ნებართვის პროცედურას დაექვემდებაროს,[75] რაც განპირობებულია იმით, რომ პირადი ცხოვრების უფლებაზე გავლენა და ჩარევის ხარისხი განსხვავდება „დავირუსების“ სხვადასხვა ტიპების შემთხვევაში, რაც მოითხოვს „პროპორციულობის“ პრინციპთან შესაბამისობის განსხვავებულ შეფასებას.[76] აღნიშნული ასევე აუცილებელია ამ ღონისძიების მრავალმხრივი ტექნიკური პოტენციალის გადამეტებულად ან თვითნებურად გამოყენების პრევენციის მიზნებისათვის.[77] კომპიუტერული სისტემიდან ინფორმაციის მოპოვების ღონისძიებების ამგვარ საკანონმდებლო დიფერენციაციას ითვალისწინებს, მაგალითად, გერმანიის სისხლის სამართლის საპროცესო კოდექსი, რომელშიც დამოუკიდებელი ღონისძიებების სახით არის ჩამოყალიბებული ე.წ. „ონლაინ ჩხრეკა“ და „კომუნიკაციის მონიტორინგი“ (ე.წ. Source-TKÜ). „ონლაინ ჩხრეკა“ გულისხმობს ღონისძიების ადრესატის ინფორმირების გარეშე ტექნიკური საშუალებებით ინფორმაციულ სისტემაში შეღწევას და ამ სისტემიდან ინფორმაციის მოპოვებას, ხოლო „კომუნიკაციების მონიტორინგის“ ქვეშ მოიაზრება ღონისძიების ადრესატის ინფორმირების გარეშე ტექნიკური საშუალებებით ინფორმაციულ სისტემაში შეღწევის გზით კომუნიკაციის მონიტორინგი და ჩაწერა.[78] ეს ღონისძიება შესაძლებელს ხდის კომუნიკაციის წაკითხვას მის დაშიფვრამდე ან განშიფვრის შემდგომ.[79] მოცემული საგამოძიებო მოქმედებების საკანონმდებლო მოთხოვნათა შესაბამისად წარმართვის უზრუნველსაყოფად, მათ განსახორციელებლად განკუთვნილი კომპიუტერული პროგრამის გამოყენება შესაძლებელია მხოლოდ შესაბამისი ტესტირების გავლისა და სპეციალურად დადგენილ მინიმალურ სტანდარტებთან შესაბამისობის დადგენის შემდეგ.[80] ეს მექანიზმი მოცემული საგამოძიებო მოქმედებებისთვის დამახასიათებელი ფართო ტექნიკური შესაძლებლობების გადამეტებულად, უკანონოდ გამოყენების საწინააღმდეგო მნიშვნელოვან გარანტიას წარმოადგენს.

ყოველივე აღნიშნულის გათვალისწინებით, მიზანშეწონილია, სამართლებრივად დაკონკრეტდეს სსსკ-ის 143^1 მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ელექტრონული მეთვალყურეობის ტიპები, რათა ერთმანეთისგან გაიმიჯნოს კომუნიკაციის რეალურ დროში მოპოვებისა და კომპიუტერულ სისტემაში შენახულ ინფორმაციაზე წვდომის უფლებამოსილებები.

---

75 *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 51, 89, <http://www.europarl.europa.eu/RegData/etudes/STUD/-2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

76 Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 25, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>, [03.04.2019]. დოკუმენტში საუბარია კომპიუტერულ სისტემაში შენახული ინფორმაციის მოპოვებისა და მიმდინარე რეჟიმში თვალთვალის შესაძლებლობების დამოუკიდებელი ნებართვის პროცედურის გზით დიფერენცირებაზე.

77 *Gutheil M., Liger Q., Heetman A., Eager J*. (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 12, 58, <http://www.europarl.europa.eu/-RegData/etudes/-STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

78 Strafprozeßordnung (StPO), §100a Abs.1 S.2, §100b, <https://www.gesetze-im-internet.de/stpo/index.html>, [03.04.2019]. კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიების ძირითადი ფუნქციონალური შესაძლებლობების დიფერენცირების მოთხოვნა ფიქსირდება ასევე იტალიის საკასაციო სასამართლოს 2016 წლის პირველი ივლისის გადაწყვეტილებაში. აღნიშნულ საკითხთან დაკავშირებით იხ. *Gutheil M., Liger Q., Heetman A., Eager J*. (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 85, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

79 <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html>, [03.04.2019].

80 იქვე.

სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიების მეტი სამართლებრივი სიცხადით რეგულირების პარალელურად, მნიშვნელოვანია, რომ მოცემული ფარული საგამოძიებო მოქმედების ჩატარების ყოველ კონკრეტულ შემთხვევაში მოსამართლე ინფორმირებული იყოს მოთხოვნილი კონკრეტული ღონისძიების განსახორციელებლად გამოსაყენებელი ტექნიკური საშუალებების შესახებ. ფარული მეთვალყურეობის ღონისძიების პროპორციულობის შეფასებისას ერთ-ერთ მნიშვნელოვან საზომს წარმოადგენს გამოყენებული ტექნიკური საშუალებების პოტენციალი უფლებაში ჩარევის ინტენსივობის თვალსაზრისით. პროპორციულობა ღონისძიებისა, რომელიც ზღუდავს პირადი ცხოვრების უფლებას და კონკრეტული ტექნიკური საშუალების გამოყენებით ფარული მეთვალყურეობის შესაძლებლობას ითვალისწინებს, დამოკიდებულია იმაზე, თუ რა ცოდნა აქვთ შესაბამის ორგანოებს ღონისძიების მასშტაბსა და გამოსაყენებელ ტექნიკურ შესაძლებლობებზე. აღნიშნული გულისხმობს, რომ ფარული საგამოძიებო მოქმედების გამოყენებამდე წინასწარ უნდა შეფასდეს კონკრეტული ღონისძიების თანმდევი პრივატულ სფეროში ჩარევის ინტენსივობა.[81] ამ კონტექსტში, მხედველობაშია მისაღები ის გარემოება, რომ, სსსკ-ის მიხედვით, არც პროკურორის შუამდგომლობის და არც ფარული საგამოძიებო მოქმედების ჩატარებაზე ნებართვის გაცემის თაობაზე სასამართლოს განჩინების სავალდებულო რეკვიზიტად არ არის განსაზღვრული იმ ტექნიკური საშუალებების შესახებ ინფორმაცია, რომელთა გამოყენებითაც უნდა განხორციელდეს სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული კონკრეტული ღონისძიება.[82] გამოყენებული ტექნიკური საშუალებების თაობაზე ინფორმაციის აღნიშვნა სავალდებულოა მხოლოდ ფარული საგამოძიებო მოქმედების ოქმში, რომელიც ღონისძიების დასრულების შემდეგ დგება.[83] რაც შეეხება სასამართლოს განჩინებას და პროკურორის შუამდგომლობას, სსსკ-ით ამ დოკუმენტების სავალდებულო რეკვიზიტებად განსაზღვრული მონაცემები საკმარისი არ არის იმისთვის, რათა მოსამართლეს შეექმნას მკაფიო წარმოდგენა იმის შესახებ, თუ როგორ უნდა განხორციელდეს კონკრეტული საგამოძიებო მოქმედება პრაქტიკული თვალსაზრისით. შესაბამისად, რთული წარმოსადგენია სათანადოდ შეფასდეს, რამდენად წარმოადგენს კონკრეტული ფარული საგამოძიებო მოქმედება პირად ცხოვრებაში ჩარევის პროპორციულ, ყველაზე ნაკლებად შემზღუდველ, თანაზომიერ საშუალებას.

6. დასკვნა

ამრიგად, წინამდებარე ნაშრომში განხილულ იქნა ინტერნეტკომუნიკაციის მონიტორინგის ღონისძიებასთან დაკავშირებული რამდენიმე პრობლემატური საკითხი. ხაზი გაესვა სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტის არასაკმარისად მკაფიო, ზოგად ფორმულირებას, რაც განაპირობებს ამ ნორმის ქვეშ ინტერნეტთან მიმართებაში ნებისმიერი მეთოდით ინფორმაციის მოპოვების შესაძლებლობების გაერთიანებას. თანამედროვე ეპოქაში პირადი ხასიათის ინფორმაციის ელექტრონული საშუალებებით მოპოვების შესაძლებლობები – მრავალფეროვანი, ხოლო პირადი ცხოვრების უფლებაზე მათი შესაძლო გავლენა და ჩარევის ხარისხი, ხშირ შემთხვევაში, განსხვავებულია, რაც კონკრეტულ ვითარებაში პროპორციულობის ტესტის განსხვავებულ შეფასებას

---

81 *Milaj J.,* Privacy, Surveillance and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol. 30, No. 3, 2016, 115.

82 იხ. სსსკ-ის 143[3] მუხლის მე-10 ნაწილი.

83 იხ. სსსკ-ის 143[6] მუხლის მე-14 ნაწილი.

შეიძლება მოითხოვდეს. შესაბამისად, ინტერნეტთან მიმართებაში ფარული მეთვალყურეობის ღონისძიებების მკაფიო საკანონმდებლო რეგლამენტაცია განსაკუთრებით მნიშვნელოვანია. აღნიშნულის საილუსტრაციოდ შეიძლება მოყვანილ იქნეს გერმანიის კანონმდებლობით გათვალისწინებული მაგალითი კომპიუტერული სისტემის „ონლაინ ჩხრეკისა“ და კომუნიკაციის მიმდინარე რეჟიმში მონიტორინგის ღონისძიებების დამოუკიდებელ საგამოძიებო მოქმედებებად ჩამოყალიბებასთან დაკავშირებით. გარდა აღნიშნულისა, კონკრეტულ ვითარებაში ღონისძიების პროპორციულობასთან დაკავშირებული ასპექტების სრულფასოვანი ანალიზისთვის აუცილებელია, რომ პროკურორის შუამდგომლობა და სასამართლოს განჩინება განსაზღვრავდეს ფარული საგამოძიებო მოქმედების ჩატარების გზების თაობაზე ამომწურავ ინფორმაციას – ადგენდეს იმ ტექნიკურ საშუალებებს, რომელთა მეშვეობითაც უნდა შეიზღუდოს კონკრეტულ შემთხვევაში კერძო კომუნიკაციის ხელშეუხებლობა.

ნაშრომში ასევე მნიშვნელოვანი ყურადღება დაეთმო საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებაში არსებულ ჩანაწერს იმასთან დაკავშირებით, რომ ინტერნეტკომუნიკაციებთან მიმართებით პრაქტიკაში გამოიყენება „ე.წ. დავირუსების ტექნიკა“. ამ თვალსაზრისით ბუნდოვანია, თუ რა ტექნიკური შესაძლებლობა მოიაზრება მითითებული ტერმინის ქვეშ. გადაწყვეტილებაში არ არის ყურადღება გამახვილებული ამ მეთოდის შინაარსსა და ინტენსივობაზე. ამასთან, როგორც უკვე აღინიშნა, არსებობს ამ ღონისძიების განსხვავებული ტიპები. ზოგიერთი ევროპული სახელმწიფო პირდაპირ არეგულირებს კანონმდებლობაში კომპიუტერულ სისტემაში ფარული შეღწევის კონკრეტული ფუნქციური შესაძლებლობების განხორციელების საკითხს და შესაბამის გარანტიებს. მიიჩნევა, რომ ამ საგამოძიებო მოქმედებასთან მიმართებით არასაკმარისია სხვა ფარული მეთვალყურეობის ღონისძიებებთან, მაგალითად, სატელეფონო მოსმენასთან დაკავშირებული რეგულაციები და, მისი ინტენსიური ხასიათის გათვალისწინებით, უფრო მკაცრი მიდგომა უნდა იქნეს შემუშავებული. აქედან გამომდინარე, იმ შემთხვევაში, თუკი საქართველოს რეალობაშიც დგას დღის წესრიგში „დავირუსების“ ტექნიკის პრაქტიკაში გამოყენების საკითხი, აღნიშნული უნდა დაექვემდებაროს კონკრეტულ, სპეციალურ ნორმატიულ მოწესრიგებას, განსხვავებულ, მკაცრ მიდგომასა და უფლების დაცვის საიმედო გარანტიებს.

ბიბლიოგრაფია:

1. საქართველოს კონსტიტუცია, 24/08/1995.
2. საქართველოს სისხლის სამართლის საპროცესო კოდექსი, 09/10/2009.
3. „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ” საქართველოს კანონი, 22/03/2017.
4. საქართველოს კონსტიტუციის კომენტარი, თავი მეორე, საქართველოს მოქალაქეობა, ადამიანის უფლებანი და თავისუფლებანი, თბილისი, 2013, 181.
5. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის საჯარო ინფორმაციაზე პასუხისმგებელი პირის 2019 წლის 21 იანვრის წერილი (№: PDP 7 19 00000216).
6. საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, 58, 59, 65-66.
7. საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე, 131.

8. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, 28, 38, 54, 55-56, 57-58.
9. Strafprozeßordnung (StPO) Deutschlands, 07/04/1987.
10. CCPR General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence and Protection of Honor and Reputation), UN Human Rights Committee, 08. 04. 1988.
11. CCPR General Comment No. 27: Article 12 (Freedom of Movement), UN Human Rights Committee, 02.11.1999.
12. *Clough J.,* Principles of Cybercrime, New York, 2010, 135, 136, 153-154.
13. *Corn G.S., Brenner-Beck D.,* "Going Dark": Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance", The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E.,* (eds.), New York, 2017, 334-335.
14. *Haase A., Peters E.,* Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance, International Data Privacy Law, Vol. 7, No. 2, 2017, 126, 130-131.
15. *Kerr O.S.,* The Next Generation Communications Privacy Act, University of Pennsylvania Law Review, Vol. 162, No. 2, 2014, 384.
16. *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, No. 2, 2015, 54.
17. *Milaj J.,* Privacy, Surveillance and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol. 30, No. 3, 2016, 115.
18. *Sagers G.,* The Role of Security in Wireless Privacy, წიგნში: Privacy in the Digital Age, 21st-Century Challenges to the Fourth Amendment, *Lind N.S., Rankin E.,* (eds.), (eds.), Vol.2, California, 2015, 508.
19. *Swire P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 202-203.
20. *Vaciago G., Ramalho D.S.,*Online Searches and Online Surveillance: The Use of Trojans and other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, Vol.13, 2016, 88-89, 92, 94-95, <http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252>, [03.04.2019].
21. *Winter L.B.,* Remote Computer Searches under Spanish Law: The Proportionality Principle and the Protection of Privacy, Zeitschrift für die Gesamte Strafrechtswissenschaft, Vol.129, No. 1, 2017, 211-212.
22. *Wright J.,* Necessary and Inherent Limits to Internet Surveillance, Internet Policy Review, Vol. 2, No. 3, 2013, 1.
23. Access Now, A Human Rights Response to Government Hacking, 2016, 11, <https://www.accessnow.-org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>, [03.04.2019].
24. Encryption and Anonymity Follow-up Report, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2018, 7, 18, <https://www.ohchr.org/Documents/Issues/-Opinion/EncryptionAnonymityFollowUpReport.pdf, [02.04.2019].
25. *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices (Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs), Policy Department for Citizens' Rights and Constitutional Affairs, 2017, 12, 42-43, 51-54, 58-61, 67, 79-80, 85, 89, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].
26. International Principles on the Application of Human Rights to Communications Surveillance, <https://en.necessaryandproportionate.org/text>, [03.04.2019].
27. Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 8, 18, 25, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>, [02.04.2019].

28. Report of the Office of the United Nations High Commissioner for Human Rights, The right to Privacy in the Digital Age, 30.06.2014, 9, <https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc>, [02.04.2019].
29. Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23.09.2014, 14-15, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement>, [02.04.2019].
30. Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 4, 10, 11, 18, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>,[02.04.2019].
31. Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 98-100.
32. Szabo and Vissy v. Hungary, [2016] ECtHR, 73.
33. Roman Zakharov v. Russia, [2015] ECtHR, 227, 229, 230, 232.
34. Case NC-293/12 and C-594/12, Digital Rights Ireland ltd and Seitlinger and others, [2014], Court of Justice, 34.
35. Kennedy v. United Kingdom, [2010] ECtHR, 130, 153.
36. BVerfG, Judgment of the First Senate of 27th February 2008 - 1 BvR 370/07.
37. Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 75.
38. Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI, 106.
39. Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V, 46.
40. Huvig v. France, [1990], ECtHR, (Ser. A.), 32.
41. Kruslin v. France, [1990], ECtHR, (Ser. A.), 33.
42. Leander v. Sweden, [1987] ECtHR, (Ser. A.), 51.
43. Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67.
44. Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 49-50.
45. <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html>, [03.04.2019].