

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

სამართლის სამაგისტრო პროგრამა

სამაგისტრო ნაშრომი თემაზე

ინტერნეტ დელიქტების სამართლებრივი ანალიზი ამერიკის შეერთებული
შტატების, ევროპის კავშირისა და ქართული სამართლის მიხედვით

წარდგენილია სამართლის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ავტორი: გიორგი ჟორჯოლიანი

Email: zhorzholianigigi@yahoo.com

ტელ.: 557 90 57 11

ხელმძღვანელი: გიორგი რუსიაშვილი, სამართლის დოქტორი, ასისტენტ-
პროფესორი.



თბილისი
2019

სარჩევი

შემოკლებათა განმარტება	4
I. შესავალი	5
II. ინტერნეტ დელიქტის ცნება.....	8
III. ინტერნეტ დელიქტების რეგულაცია ამერიკის შეერთებულ შტატებში.....	9
1. ტრადიციული დელიქტების ტრანსფორმაცია ინტერნეტ დელიქტთან მიმართებაში	10
1.1. პროგრამული უზრუნველყოფა და ნივთების ინტერნეტი, როგორც პასუხისმგებლობის ახალი წყარო პროდუქტის მწარმოებლებისთვის.....	10
1.1.1. წუნის კატეგორიზაცია და პასუხისმგებლობა წუნდებული პროდუქტისთვის.....	12
1.1.2. ნივთების ინტერნეტი და პროგრამული უზრუნველყოფა, როგორც პლატფორმა ინტერნეტ დელიქტისთვის.....	13
1.1.3. ეკონომიკური დანაკარგის დოქტრინის ჩანაცვლება.....	17
1.2. ინტერნეტ საშუალებებით ვირტუალური საკუთრების ხელყოფა	20
1.2.1. ინტერნეტ სივრცის ბუნება კიბერ ხელყოფასთან მიმართებაში ...	21
1.2.2. ინტერნეტ ხელყოფის კრიტიკა	22
1.2.3. თვითდახმარება, ხსნა თუ კრიტიკის კიდევ ერთი საფუძველი? ..	25
1.3. ონლაინ დეფამაცია.....	29
1.3.1. ვებგვერდზე გამოქვეყნებული კონტენტი, როგორც ზიანის წყარო	30
1.3.2. კონსტიტუციის პირველი შესწორება, როგორც ფარი კონტენტის გამავრცელებლისთვის.....	31
1.3.3. კომუნიკაციურ ქსელში ეთიკურობის შესახებ კანონი და ვებგვერდების მეორადი პასუხისმგებლობა	32
2. დელიქტური ვალდებულების ახალი ინტერნეტ სახეობები	32
2.1. კიბერსქვათინგი.....	32
2.1.1. მიდგომა ინტელექტუალური საკუთრებისადმი და მომხმარებელთა დაცვის კანონი ანტი-კიბერსქვათინგის შესახებ.	33
2.1.2. დომენური დავების გადაწყვეტის ერთიანი პოლიტიკა (UDRP) ..	35

2.2. ინტერნეტ მეკობრეობა და საავტორო უფლებები.....	36
2.2.1. კანონი საავტორო უფლებების შესახებ ციფრულ ეპოქაში და მართლზომიერი გამოყენების პრობლემური ურთიერთმიმართება	36
2.2.2. უსაფრთხო ნავსადგომის წესი.....	38
IV. ინტერნეტ დელიქტების რეგულატორული მოწესრიგება ევროპის კავშირში	39
1. ინტერნეტ დელიქტების განსჯადობის საკითხი რეგულაცია ბრიუსელი I მიხედვით.....	40
1.1. შევილის დოქტრინა (საქმე C-68/93).....	41
1.2. სპეციალური განსჯადობის ახალი სასამართლო ქრილი	43
1.3. განსხვავებული მიდგომა სასაქონლო ნიშნების მიმართ.....	44
1.4. ინტერნეტ დელიქტის თანმდევი ფორუმ შოპინგი	45
2. გამოსაყენებელი სამართალი.....	46
V. ინტერნეტ დელიქტები საქართველოში	49
1. სასამართლო და არასამართლო პრაქტიკა	49
1.1. ინტერნეტ დავების საწყისი წერტილი	49
1.2. ინტერნეტ სივრცე როგორც მეწარმეთა არაკეთილსინდისიერი კონკურენციის ასპარეზი.....	51
1.3. კიბერსექვათინგი ქართულად	55
1.3.1. ადმინისტრაციული ორგანოს ჩარევის კრიტიკა და დავის გადაწყვეტის სხვა მექანიზმებთან შედარება	57
1.4. საავტორო უფლებები ინტერნეტში.....	59
1.5. ონლაინ ცილისწამება.....	61
1.5.1. ნორმატიული საფუძვლების მისადაგება	61
1.5.2. მტკიცების ტვირთი.....	62
VI. დასკვნა	63
ბიბლიოგრაფია.....	66

შემოკლებათა განმარტება

სსკ – საქართველოს სამოქალაქო კოდექსი

იხ. – იხილეთ

რედ. – რედაქტორი

ACPA – Anticybersquatting Consumer Protection Act

FTDA – Federal Trademark Dilution Act

ICANN – Internet Corporation for Assigned Names and Numbers

UDRP – Uniform Domain Name Dispute Resolution Policy

WIPO – World Intellectual Property Organization

DMCA – Digital Millennium Copyright Act

CJEU – Court of Justice of the European Union

IoT – Internet of Things

ინტერნეტ დელიქტების სამართლებრივი ანალიზი ამერიკის შეერთებული შტატების, ევროპის კავშირისა და ქართული სამართლის მიხედვით

I. შესავალი

ინტერნეტ სივრცეში განვითარებული ურთიერთობები ძირითად შემთხვევაში აღიქმება როგორც მხოლოდ ტექნოლოგიური ინოვაციის ნაწილი და მხოლოდ ინფორმაციულ მეცნიერებასთან დაკავშირებული მოვლენა, რაც, რაღა თქმა უნდა, არ შეესაბამება ობიექტურ რეალობას, ინტერნეტი მჭიდროდ არის დაკავშირებული სხვადასხვა სამართალურთიერთობასთან. წინამდებარე ნაშრომი სწორედ ასეთ უმნიშვნელოვანეს საკითხს ინტერნეტ სივრცეში წარმოშობილ ზიანსა და მის სამოქალაქო-სამართლებრივ პასუხისმგებლობას, უფრო ზუსტად კი ინტერნეტ დელიქტების სამართლებრივ ანალიზს შეეხება.

2019 წლისთვის ინტერნეტ მომხმარებლების საერთო რაოდენობა 4 მილიარდზე მეტს შეადგენს,¹ პერსონალური კომპიუტერების გარდა ინტერნეტთან დაკავშირებული მოწყობილობების რაოდენობა 13 მილიარდს აჭარბებს,² ხოლო, რეგისტრირებული ინტერნეტ დომენების³ რაოდენობა 350 მილიონამდეა.⁴ მოცემული ინფორმაცია ხაზს უსვამს იმას რომ ინტერნეტ სივრცე ციფრული რევოლუციის უდიდეს და უმნიშვნელოვანეს ნაწილს იკავებს და იგი თანამედროვე ადამიანის ყოფიერების განუყოფელ ნაწილადაა ქცეული.

ინტერნეტ დელიქტი ინტერნეტის განვითარებასთან ერთად აქტუალურ სამართლებრივ საკითხად გადაიქცა, მთელი მსოფლიოსთვის. ინტერნეტში განხორციელებული ნებისმიერი ქმედება, დაწყებული სოციალურ ქსელში

¹ დეტალური სტატისტიკა იხ. ბმულზე <https://datareportal.com/reports/digital-2019-global-digital-overview> (ვიზიტის დრო: 24.06.2019).

² დეტალური სტატისტიკა იხ. ბმულზე <https://datareportal.com/reports/digital-2019-global-digital-overview>; <https://techjury.net/blog/how-many-iot-devices-are-there/> (ვიზიტის დრო: 24.06.2019).

³ ინტერნეტ დომენი არის ასოებისაგან და ციფრებისგან შემდგარი დასახელება, რომელიც ებმება ინტერნეტ პროტოკოლის მისამართს (IP Address), რომელიც კომპიუტერის ბრაუზერს უთითებს თუ საიტის რომელი გვერდი გახსნას. კონკრეტული დომენის მიზმა მხოლოდ ერთი IP მისამართზეა შესაძლებელი, რასაც ისიც ემატება რომ მისილირებულება არამხოლოდ ეკონომიკურია, შესაბამისად იურიდიულ ლიტერატურაში არსებობს მოსაზრება, რომ დომენი არა ინტელექტუალური საკუთრებაა, არამედ კვაზი-საკუთრებას წარმოადგენს. საკითხთან დაკავშირებით იხ. *Lipton D. J., Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy, Wake Forest Law Review, Vol. 40, 2005, 1366–1367.*

⁴ დეტალური სტატისტიკა იხ. ბმულზე <https://domainnamestat.com/statistics/overview> (ვიზიტის დრო: 24.06.2019).

გაკეთებული განცხადებით, დამთავრებული პერსონალურ კომპიუტერში არსებული პროგრამული უზრუნველყოფით შესაძლოა სამოქალაქო პასუხისმგებლობის დაკისრების წყარო იყოს. სწორედ ამიტომ ინტერნეტის ბუნება ხშირად საშიშ და უკონტროლო მოვლენად გვევლინება. შესაბამისად განსახილველი თემა უადრესად საინტერესოა როგორც ტექნოლოგიური, ისე სამართლებრივი კუთხით.

ნაშრომი თემის აქტუალობას სამართლებრივი ჩარჩოს ფარგლებში წარმოაჩენს. იგი მკითხველს სთავაზობს როგორც მსოფლიოში ინტერნეტამდე არსებული ნორმატიული თუ სასამართლო პრაქტიკის ტრანსფორმაციას ინტერნეტ სივრცეში მიყენებული ზიანისთვის, ასევე, დელიქტური ქმედების ახალ კატეგორიებს ინტერნეტ დელიქტის სახით, ამასთან ერთად, ნაშრომი ნათლად აჩვენებს ტრანსფორმაციის პრობლემურობასა და ახალი დეფინიციების ნაკლოვანებებს.

კვლევის საკითხი შეიძლება ითქვას, რომ არასდროს ყოფილა ქართულ იურიდიულ ლიტერატურაში შესწავლილი და მოცემული სამართლებრივი კვლევა პირველია ქართული სამართლებრივი სივრცისთვის. ნაშრომი მაქსიმალურად ცდილობს მკითხველისთვის იყოს ამომწურავი და ანალიზის სახით აწვდიდეს მას თემის უმნიშვნელოვანეს ასპექტებს. სწორედ ამიტომ მასში განხილულია სამი სამართლებრივი სივრცე. ამერიკის შეერთებული შტატები, ევროპის კავშირი და საქართველო. თავის მხრივ ნაშრომი მიზნად არ ისახავს სამივე სივრცისთვის ერთი და იგივე კონკრეტული შემთხვევები განიხილოს, არამედ შეერთებული შტატებისა და ევროპის კავშირის შემთხვევებში განიხილოს მათი ინდივიდუალური პრობლემატიკა და მოიცვას სამართლებრივი ანალიზი რომელიც ურთიერთშემავსებელია ამ ორი სივრცისთვის, ხოლო, საქართველოსთვის განიხილოს სასამართლო პრაქტიკა და შესთავაზოს მკითხველს თანმდევი მოწესრიგება.

სამართლებრივი ანალიზი გამოირჩევა მისი კრიტიკულობით სამივე სამართლებრივი სივრცის მიმართ და სამივე მათგანისთვის რიგ შემთხვევებში მკითხველს სთავაზობს დოქტრინალური თუ სასამართლო პრაქტიკის რაციონალური ჩანაცვლების გზებს განსხვავებული მიდგომებით.

ნაშრომში, განსაკუთრებით საქართველოს სამართლებრივი სივრცისთვის გამოყენებულია შედარებით–სამართლებრივი კვლევა უპირატესად ამერიკის შეერთებულ შტატებთან მიმართებაში, ხოლო, ზოგიერთი ინტერნეტ პლატფორმისთვის შემოთავაზებულია პრაქტიკული კვლევა.

წინამდებარე კვლევის მთავარი მიზანია ინტერნეტ სივრცეში მიყენებული ზიანის, როგორც ტექნოლოგიის განვითარების თანმდევი მახასიათებლისა და სამართლებრივი სიახლის მნიშვნელობის წარმოჩენა. მნიშვნელოვანი სასამართლო გადაწყვეტილებებისა და მათი როლის გაანალიზება დოქტრინასთან მიმართებით, ასევე, დამკვიდრებული სამართლებრივი მდგომარეობის ზომიერი კრიტიკა საკითხზე შექმნილი იურიდიული ლიტერატურის თითქმის ყველა მნიშვნელოვან ნაშრომზე დაყრდნობით. ხოლო საქართველოსთვის კი ნორმატიული საფუძვლების არარსებობისა და სასამართლო პრაქტიკის ანალიზი.

ნაშრომის ძირითადი ნაწილი სამი თავისგან შედგება. იგი იწყება ამერიკის შეერთებული შტატების სამართლით, რაც განპირობებულია იმ ფაქტით, რომ სწორედ იგი ამკვიდრებს პირველად ინტერნეტ სივრცეში წარმოშობილი ზიანისთვის სამართლებრივ რეგულაციებს და საერთო სამართალში არსებულ დოქტრინებს უსადაგებს მას, არამხოლოდ თეორიულად, არამედ სასამართლო პრაქტიკაშიც. ინტერნეტ დელიქტების რეგულაცია ამერიკის შეერთებულ შტატებში თავის მხრივ იყოფა ორ ნაწილიდან, პირველ ნაწილში მკითხველი გაეცნობა ისეთი ტრადიციული დელიქტების ტრანსფორმაციასა და მათ პრობლემურ ხასიათს ტექნოლოგიურ ინოვაციასთან, როგორცაა დეფამაცია, საკუთრების ხელყოფა და წუნდებული პროდუქტიდან გამოწვეული პასუხისმგებლობა. ხოლო, მეორე ნაწილში მოცემული იქნება დელიქტური ვალდებულების ახალი სახეობები კიბერსქვათინგი და ინტერნეტ მეკობრეობა.

ნაშრომის ძირითადი ნაწილი გრძელდება ევროპის კავშირის რეგულატორული მოწესრიგებით, რაც არა უშუალოდ ინტერნეტ დელიქტების სხვადასხვა კატეგორიასა და იმავე საკითხების განხილვას უკავშირდება რაც შეერთებული შტატებისთვის იყო მოცემული, არამედ ისეთი შემთხვევების სამართლებრივ ანალიზს სადაც დელიქტურ ქმედებაში რამდენიმე წევრი ქვეყნის მასშტაბი არის მოცული, რითიც ნაშრომი ინტერნეტ დელიქტების უსაზღვრო ბუნებას, ასევე, ზიანის მომტანი ქმედების განხორციელებისა და უშუალოდ ზიანის დადგომის ადგილის აცდენას უსვამს ხაზს.

ძირითადი ნაწილის დასასრულს კი მოცემულია ქართული სასამართლო პრაქტიკა, რომელიც სპეციალურად არის ბოლოსთვის გადააზრებული, რადგანაც მკითხველისთვის უკვე ნაცნობი იყოს თუ რას მოიცავს ინტერნეტში განხორციელებული დელიქტური ქმედება და როგორი მიდგომა უნდა არსებობდეს მის მიმართ ქართულ სამართლებრივ სივრცეში. მოცემულ ნაწილში მხოლოდ სასამართლო პრაქტიკის ანალიზი განპირობებულია

იმით, რომ სპეციალური ნორმატიული მოწესრიგება ინტერნეტში წარმოშობილი ურთიერთობებისთვის საქართველოში ნაშრომის მომზადების პერიოდში არ არსებობს, ხოლო კვლევისთვის ნორმატიული მოწესრიგების რეკომენდაციები თვალსაჩინოებისთვის პრაქტიკასთან ერთად არის მოცემული და არა განცალკევებით სხვა ქვეყნის სამართლის მაგალითზე, რაც კიდევ უფრო მეტად ადაპტირებულს ხდის მსგავს რეკომენდაციებს ქართული სამართლისთვის.

II. ინტერნეტ დელიქტის ცნება

ინტერნეტ დელიქტის დეფინიცია და ცნება არცერთ რეგულაციასა და ნორმატიულ აქტში არ არის მოცემული, გამომდინარე აქედან მისი ერთიანი განმარტების ქვეშ მოქცევა შეუძლებელია. ინტერნეტ დელიქტთა კლასიფიკაცია და განმარტება უნდა მოხდეს მათი შემადგენლობის მიხედვით და ყოველი კონკრეტული შემთხვევა განხილული უნდა იქნეს ინდივიდუალურად.⁵ განსხვავებით მატერიალურ სამყაროში წარმოქმნილი დელიქტებისა, რომლებიც ხშირად უშუალოდ მიმართულია პირების სამართლებრივი სიკეთის ფიზიკური ზიანისკენ, რა თქმა უნდა, გარდა ზიანის მომტანი ცნობების გავრცელებისა, ინტერნეტ დელიქტებისთვის დამახასიათებელია მათი წარმოშობა ინტერნეტ სივრცეში ელექტრონული კომუნიკაციების საშუალებებით და მათი ორიენტაცია ფინანსურ დანაკარგებზე, რეპუტაციის შელახვაზე, არაკეთილსინდისიერ კონკურენციაზე და კიბერ უსაფრთხოებაზე.⁶ ინტერნეტ დელიქტებისთვის, ასევე, ერთ-ერთი მთავარი მახასიათებელია შეუზღუდავი ექსტერიტორიულობა და უსაზღვრო ბუნებაა, რაც ინტერნეტის ფართო გავრცელების და მარტივად ხელმისაწვდომობის შედეგია.

ინტერნეტ დელიქტი მჭიდროდ არის დაკავშირებული თანამედროვე ინდუსტრიულ და ტექნოლოგიურ სფეროებთან, გამომდინარე იქიდან, რომ ისინი დროთა განმავლობაში უფრო მეტად ინტერნეტ სივრცეზე არიან ორიენტირებულნი, ასევე, მნიშვნელოვანი ურთიერთკავშირი აქვს ინტერნეტ დელიქტებსა და ელექტრონულ კომერციას და ზოგადად ნებისმიერ

⁵ Świerczyński M., Electronic torts/delicts in the Rome II regulation, Tort Law in Poland, Germany and Europe, eds. Heiderhoff B./Zmij G., sellier. european law publishers, Munich 2009, 174.

⁶ Rustad M. L., Global Internet Law, West Academic Publishing, St. Paul 2014, 112.

ინტერნეტ ტრანზაქციას. შესაბამისად ელექტრონული კომერციის მასშტაბების ზრდა იწვევს ინტერნეტ დელიქტების რიცხვის მატებასაც.⁷

ინტერნეტ დელიქტისთვის, ასევე, არ არის დამკვიდრებული ერთიანი ტერმინი, რომელიც იურიდიულ ლიტერატურაში გამოყენებული იქნებოდა ინტერნეტ სივრცეში მიყენებული ზიანის აღსანიშნავად. მაგალითისთვის ამერიკის შეერთებულ შტატებში დამკვიდრებული ტერმინია კიბერ დელიქტი (Cyber Tort),⁸ რომელიც ხშირად მოიცავს ციფრულ და კომპიუტერულ დელიქტებსაც, ასევე, სისხლისსამართლებრივ დანაშაულსაც, ტერმინი თავის მხრივ გაზიარებულია ევროპის კავშირის ერთიან სამართლებრივ რეგულაციაზე საუბრისას იურიდიულ ლიტერატურაში, მაგრამ მხოლოდ სამოქალაქო ინტერნეტ დავებთან მიმართებაში, ამისგან განსხვავებით ევროპის კავშირის წევრ ქვეყნებში კონკრეტულად კი, ავსტრიაში⁹ და გერმანიაში¹⁰ იყენებენ განსხვავებულ ტერმინს ინტერნეტ დელიქტს (Internetdelikt).

ამრიგად მართებული იქნება ინტერნეტ დელიქტების დეფინიციის არა ცალკე არამედ თითოეულ ინდივიდუალურ შემთხვევაში განხილვა კონკრეტული სამართლებრივი სივრცის ანალიზთან პარალელურად, რაც უფრო თვალსაჩინოდ წარმოადგენს მათ სამართლებრივ ბუნებასა და განმარტებას.

III. ინტერნეტ დელიქტების რეგულაცია ამერიკის შეერთებულ შტატებში

ინტერნეტ სივრცეში მიყენებული ზიანისთვის სამოქალაქო სამართლებრივი პასუხისმგებლობის საკითხის განვითარებაში ერთ–ერთი პირველი, უპირველესი თუ არა სწორედ შეერთებული შტატები იყო. მნიშვნელოვანია, რომ ერთი მხრივ, ინტერნეტში განხორციელებული ზოგიერთი დელიქტისთვის, როგორც იურიდიული ლიტერატურა, ასევე, სასამართლო პრაქტიკა ტრადიციული დელიქტების ტრანსფორმაციას გვთავაზობს. ხოლო, სრულიად ახალი ინტერნეტ დელიქტებისთვის კი ჩნდება შესაბამისი ნორმატიული მოწესრიგება. შესაბამისად შეერთებული შტატებისთვის სწორედ აღნიშნული ორი მიმართულებით უნდა იქნეს განხილული ინტერნეტ დელიქტები.

⁷ *Savin A.*, Jurisdiction Over Cybertorts in the EU–A Coherent Picture?, *Liber amicorum: Gašo Knežević*, ed. *Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016, 212–213.

⁸ *Mosier G./Fitzgerald T.*, Cyber Torts: Common Law and Statutory Restraints in the United States, *Journal of International Commercial Law and Technology*, Vol.2, Issue 1, 2007, 17.

⁹ OGH 10.7.2012, 4 Ob 82/12f, MR 2012, 343.

¹⁰ *Rauscher T.*, *Internationales Privatrecht: Mit internationalem Verfahrensrecht*, C.F. Müller, Heidelberg 2017, 368.

1. ტრადიციული დელიქტების ტრანსფორმაცია ინტერნეტ დელიქტთან მიმართებაში

1.1. პროგრამული უზრუნველყოფა და ნივთების ინტერნეტი, როგორც პასუხისმგებლობის ახალი წყარო პროდუქტის მწარმოებლებისთვის

ინტერნეტ დელიქტებზე საუბრისას თავისთავად პირველადი ასოციაცია გვიჩნდება კომუნიკაციაზე, რომელიც კომპიუტერების საშუალებით ხორციელდება და მართულია ადამიანის მიერ, თუმცა ინტერნეტის საშუალებით კომუნიკაცია არამხოლოდ კომპიუტერებს შესაძლოა ჰქონდეთ, არამედ ჩვენ მიერ გამოყენებად ყოველდღიურ ნივთებს, სწორედ ასეთი ნივთების ერთობლიობას ეწოდება ნივთების ინტერნეტი (Internet of Things, IoT)¹¹ და ის შესაძლოა დელიქტური ქმედების წყაროს წარმოადგენდეს. აღსანიშნავია, რომ ნივთების ინტერნეტის ერთიანი ცნება თუ კონცეფცია არ არსებობს,¹² მიუხედავად ამისა ნივთების ინტერნეტის კატეგორიზაცია შემდეგი მიმართულებებით არის შესაძლებელი: ჯანმრთელობისა და ფიტნესის სენსორები, ავტომობილის თვითმართვადი სისტემები, ჰკვიანი სახლის სისტემები, დასაქმებულთა მონიტორინგის სისტემები და პროგრამული უზრუნველყოფა, რომელიც იძლევა ნივთების ინტერნეტის მართვის საშუალებას სმარტფონებისა და კომპიუტერების საშუალებით.¹³ მიუხედავად ამისა უშუალოდ კომპიუტერები და სმარტფონები არ არის მოაზრებული, როგორც ნივთების ინტერნეტის ნაწილი.¹⁴

IoT გარიგებები¹⁵ ჰიბრიდული მახასიათებელით გამოირჩევა. პროდუქტის ნასყიდობამ შეიძლება მოიცვას არა მხოლოდ ნივთის გადაცემისა და მისი ინსტალაციის სერვისის ხელშეკრულება, არამედ სხვადასხვა პროგრამული

¹¹ თვალსაჩინოებისთვის ერთ-ერთი ასეთი მოწყობილობაა Google Home, რომელსაც შეუძლია ჩვენი ხმოვანი მითითებით აკონტროლოს სხვა IoT მოწყობილობები, შეგვირჩიოს მუსიკა ონლაინ ბაზებიდან, ავტომატურად შეასრულოს სხვადასხვა დავალება, მათ შორის პერიოდულად იყიდოს პროდუქტი ინტერნეტის საშუალებით. Google Home-ის შესახებ ვრცლად იხ. https://store.google.com/product/google_home (ვიზიტის დრო: 24.06.2019).

¹² *Paez M./ La Marca M.*, The Internet of Things: Emerging Legal Issues for Businesses, Northern Kentucky Law Review, Vol. 43, Number 1, 2016, 31.

¹³ *Peppet S. R.*, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Texas Law Review, Vol. 93, 2014, 98.

¹⁴ *Paez M./ La Marca M.*, The Internet of Things: Emerging Legal Issues for Businesses, Northern Kentucky Law Review, Vol. 43, Number 1, 2016, 31.

¹⁵ იგულისხმება IoT პროდუქტის მწარმოებელსა და მომხმარებელს შორის დადებული გარიგება IoT პროდუქტის შეძენასთან დაკავშირებით და არა ისეთი გარიგებები, რომლებიც უშუალოდ IoT-ის საშუალებით შეიძლება დაიდოს, ამ უკანასკნელისთვის იხილეთ *Elvy S.*, Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond, Hofstra Law Review, Vol. 44, 2016, 869-873.

უზრუნველყოფის სერვისები, რომლებიც დროში განგრძობადია და მართულია ერთმანეთთან ინტერნეტის საშუალებით დაკავშირებული მოწყობილობებით.¹⁶ ამრიგად მომხმარებელი შესაძლოა IoT მოწყობილობის შექმნის დროს დაეხმოს სამი განსხვავებული სახის გარიგებას. პირველი შეეხება უშუალოდ პროგრამულ უზრუნველყოფას, იგივე პროგრამის სამომხმარებლო ხელშეკრულებას (End-user license agreement, EULA), რომელიც შესაძლოა ექცეოდეს ინტელექტუალური საკუთრების სამართლისა და ზოგადად საერთო სამართლის რეგულირების სფეროში. მეორე შეთანხმება მოიცავს უშუალოდ IoT მოწყობილობის, როგორც ნივთის ნასყიდობის ხელშეკრულებას და ბოლოს სალიცენზიო შეთანხმება პროდუქტის მწარმოებლის სერვისებით სარგებლობის შესახებ.¹⁷

ნათელია, რომ ნივთების ინტერნეტი, მანამდე კი პროგრამული უზრუნველყოფა, როგორც ტექნიკური ინოვაცია მიმართულია სოციალური და ეკონომიკური პროგრესისკენ, თუმცა ეს უკანასკნელი ზოგადად შესაძლოა სოციალური კეთილდღეობისთვის პროდუქტიული აქტივობების ხარჯზე მოხდეს, ან სულაც ზიანის მომტანი იყოს მისთვის.¹⁸ რთულია იმის თქმა თუ IoT რამდენად აყენებს ზიანს სოციალურ კეთილდღეობას, თუმცა იგი უდავოდ შეიძლება მოვიაზროთ როგორც დელიქტური ვალდებულების ახალი წყარო პროდუქტის მწარმოებლისთვის, რიგ შემთხვევაში გამყიდველისთვისა და მიმწოდებლისთვის, რადგანაც სწორედ მათი წარმოებული ზემოგანხილული პროდუქტი შესაძლოა იყოს წუნდებული და არამდგრადი კიბერ უსაფრთხოებასთან მიმართებაში.

წუნდებულ პროდუქტზე პასუხისმგებლობას გააჩნია ორი ურთიერთ შემავსებელი მიზანი. პირველი ეს არის მომხმარებელთა კომპენსაცია, რომელთაც მიადგათ ზიანი წუნდებული პროდუქტიდან გამომდინარე და მეორე, მონეტარული დანაკარგების რისკის გამოყენება იმისთვის, რომ მოხდეს კომპანიების ინიცირება მიიღონ გონივრული უსაფრთხოების ზომები პროდუქტის შექმნისას.¹⁹ ინტერნეტ დელიქტთან მიმართებაში წუნდებული პროდუქტის ობიექტებად განხილული უნდა იქნეს პროგრამული უზრუნველყოფა (software) და ნივთების ინტერნეტი (Internet of Things, IoT).

¹⁶ *Elvy S.*, The Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?, Washington and Lee Law Review, Vol. 74:1, 2017, 91.

¹⁷ იქვე, 94.

¹⁸ *Citron D. K.*, Cyber Civil Rights, Boston University Law Review, Vol. 89:61, 2009, 62.

¹⁹ *Sales N. A.*, Regulating Cyber-Security, Northwestern University Law Review, Vol.107, No. 4, 2013, 1533.

1.1.1. წუნის კატეგორიზაცია და პასუხისმგებლობა წუნდებული პროდუქტისთვის

მწარმოებელი, გამყიდველი ან მიმწოდებელი, რომელიც წუნდებულ პროდუქტს ყიდის ან მისი დისტრიბუციითაა დაკავებული, პასუხისმგებელია მიყენებული ზიანისთვის, რომელიც ასეთმა პროდუქტმა გამოიწვია.²⁰ ამასთან ამერიკული დელიქტური სამართალი, წუნდებული პროდუქტისთვის ავითარებს სამ შესაძლო შეთხვევას. პირველი, როდესაც პროდუქტი გაყიდვის ან დისტრიბუციის მომენტისთვის წუნდებულია ისე, რომ მას გააჩნია საწარმოო წუნი და ის მისი პირველადი დანიშნულებისთვის გამოუსადეგარია, მიუხედავად იმისა რომ მისი წარმოების პროცესში პროდუქტი ყველა ნორმის დაცვით დამზადდა.²¹ აღნიშნულიდან გამომდინარეობს საწარმოო წუნის თეორია (manufacturing defect),²² რომლის მიხედვითაც წუნიდან გამოწვეული ზიანის შემთხვევაში მოსარჩელეს შეუძლია მკაცრი პასუხისმგებლობის (strict liability) დოქტრინიდან გამომდინარე პროდუქტის მწარმოებლის ან გამყიდველის წინააღმდეგ წარადგინოს სარჩელი, რომლის მიხედვითაც მოსარჩელეს არ აქვს ვალდებულება მოთხოვნის დასაკმაყოფილებლად დაამტკიცოს მოპასუხის ბრალეულობა ან ნებისმიერი არაგონივრული ქმედება, რომელიც მიზეზობრივ კავშირშია ზიანთან. საკმარისია მოსარჩელემ წარმოადგინოს მტკიცებულება, რომ პროდუქტი წუნდებული იყო გადაცემის მომენტში, მისი მოთხოვნა დაკმაყოფილდება.²³

მეორე პასუხისმგებლობის შემთხვევაა, როდესაც პროდუქტის საწარმოო კონსტრუქცია წუნდებულია, თუმცაღა თავად მწარმოებელს, გამყიდველს ან კომერციული ჯაჭვის ყოველ წინამორბედს შეეძლო შეემცირებინა პროდუქტით გამოწვეული ზიანი, ალტერნატიული უსაფრთხო კონსტრუქციის შერჩევით.²⁴ აღნიშნულ მოცემულობას შეესაბამება კონსტრუქციული წუნის თეორია (design defect),²⁵ რასაც უკავშირდება მომხმარებლის მოლოდინის ტესტი (consumer expectation test), რომლის მიხედვითაც მოსარჩელემ უნდა დაამტკიცოს, რომ პროდუქტი არ შეესაბამება საშუალო მომხმარებლის მოლოდინს პროდუქტის უსაფრთხოებასთან დაკავშირებით.²⁶ ასევე, აღნიშნულ თეორიას უკავშირდება, სარგებლიანობის

²⁰ American Law Institute, Restatement of the Law Third, Torts: Products Liability, 1998, §1.

²¹ იქვე, §2(a).

²² Hylton, K., Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 340.

²³ იქვე.

²⁴ American Law Institute, Restatement of the Law Third, Torts: Products Liability, 1998, §2(b).

²⁵ Hylton, K., Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 340.

²⁶ იქვე.

რისკის ტესტი (risk-utility test), რის მიხედვითაც მოსარჩელეს ეკისრება მტკიცების ტვირთი, რომ მოპასუხის შერჩეული პროდუქტის კონსტრუქცია არაგონივრული საფრთხის მატარებელია და აჭარბებს მისი სარგებლიანობის ხარისხს, როდესაც მისი შედარება ალტერნატიულ უსაფრთხო კონსტრუქციასთან ხდება.²⁷

ბოლოს, მესამე პასუხისმგებლობის წყაროა, შემთხვევა როდესაც პროდუქტისთვის განსაზღვრულია შეუსაბამო გამოყენების წესები ან გაფრთხილებები, როდესაც შესაძლებელი იყო მწარმოებლის ან გამყიდველის მიერ შესაბამისი გონივრული გამოყენების წესებისა და გაფრთხილებების შეთქვაზება მომხმარებლისთვის, რაც გამოიწვევდა ზიანის შემცირებას ან აცილებას.²⁸ ზემოგანხილულს შეესაბამება არგაფრთხილების თეორია (failure to warn). ასეთ დროს თუმცა იცის მწარმოებელმა პროდუქტის წუნის შესახებ იგი ვერ აფრთხილებს მომხმარებელს ადეკვატურად, აღნიშნული მოიაზრება როგორც გაუფრთხილებლობა (negligence), შესაბამისად თუ მწარმოებელი გონივრულ გაფრთხილებას მისცემდა მომხმარებელს და იგი ეფექტური იქნებოდა, ასეთის არარსებობისას მან, როგორც მოპასუხემ დავაში პასუხი უნდა აგოს ასეთი წუნის გამო მიყენებული ზიანისთვის.²⁹

1.1.2. ნივთების ინტერნეტი და პროგრამული უზრუნველყოფა, როგორც პლატფორმა ინტერნეტ დელიქტისთვის.

პროგრამული უზრუნველყოფის წუნი, მიიჩნევა სტრუქტურის წუნად, რასაც განაპირობებს შემდეგი ფაქტორები. პროგრამული უზრუნველყოფა წარმოებისას გადის რამდენიმე ეტაპს. ესენია, კონსტრუქციის შერჩევის, პროგრამული კოდის შექმნის, გამოცდისა და ბოლოს, გამრავლებისა და დისტრიბუციის ეტაპი. ნათელია, რომ სტრუქტურის შერჩევის ეტაპზე, ხარვეზი, ჩათვლება სტრუქტურის წუნად, ხოლო, გამრავლების ეტაპზე ინდივიდუალური გაუმართაობა კი საწარმოო წუნად.³⁰ სადავოა კოდის შექმნის ეტაპზე გამოვლენილი წუნის ბუნება. მწარმოებელთა პერსპექტივიდან ის მიეკუთვნება კონსტრუქციის წუნს, ხოლო, პროგრამული უზრუნველყოფის შემძენთა პოზიციიდან, კოდის შექმნის ეტაპზე დეფექტი უნდა მოიაზრებოდეს როგორც საწარმოო წუნი, რაც თავის მხრივ მკაცრი პასუხისმგებლობის დელიქტთანაა დაკავშირებული.³¹ ეს უკანასკნელი

²⁷ იქვე.

²⁸ American Law Institute, Restatement of the Law Third, Torts: Products Liability, 1998, §2(c).

²⁹ Hylton, K., Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 341.

³⁰ Scott M. D., Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, Maryland Law Review, Vol. 67, Issue 2, 2008, 459.

³¹ იქვე, 459–460.

მოსაზრება არ უნდა იქნეს გაზიარებული, რადგანაც მკაცრი პასუხისმგებლობიდან გამოწვეული ზიანის ანაზღაურების მოცულობა, მწარმოებლების წარმადობას აწარმოონ ახალი პროდუქტი მნიშვნელოვნად შეამცირებს, ასევე, შეუძლებელია პროგრამული უზრუნველყოფის ყოველი ხარვეზი მისი წარმოების ეტაპზე იქნეს აღმოფხვრილი.³² შესაბამისად პროდუქტის წარმოების სოციალური სიკეთე გადაწონის მკაცრი პასუხისმგებლობის გამოყენების აუცილებლობას.³³

იმის გასარკვევად თუ წუნდებული პროდუქტიდან გამომდინარე, ზემოგანხილული დელიქტური შემთხვევებიდან, რომელი მოიცავს ნივთების ინტერნეტიდან გამოწვეულ ზიანს, განსაზღვრული უნდა იყოს მისი წუნის პრობლემურობის საკითხი. იურიდიულ ლიტერატურაში გამოთქმული მოსაზრების თანახმად, რასაც თავის მხრივ საფუძვლად შესაბამისი ტექნიკური ასპექტები აქვს, ნივთების ინტერნეტის მთავარი პრობლემა მისი დაუცველობაა, რაც ეხება, როგორც ტექნიკურ ნაწილებს (hardware), ასევე, პროგრამულ უზრუნველყოფას (software).³⁴ ორივე შემადგენლობის წუნდებულობას ნივთების ინტერნეტის მოწყობილობებისთვის შესაძლოა განაპირობებდეს შემდეგი წინაპირობები: IoT მოწყობილობები ყველაზე ხშირად არა ინფორაციული ტექნოლოგიების მწარმოებელი კომპანიების მიერ არის შექნილი. პროდუქტის სენსორები იმდენად პატარაა, რომ მათ მწარმოებლებს უბრალოდ არ ყოფნით სიმძლავრე მოწყობილობაში განათავსონ ისეთი უსაფრთხოების ზომები როგორცაა მონაცემთა დაშიფრვა³⁵ და ბოლოს IoT მოწყობილობები, განსხვავებით სმარტფონებისა და კომპიუტერებისა, არ ექვემდებარებიან დისტანციურ განახლებასა და გაუმჯობესებას.³⁶ თუმცადა ეს უკანასკნელი მოსაზრება ბოლო დროს სულ უფრო მეტად გაქარწყლებადია პროდუქტის მწარმოებელი კომპანიების

³² იქვე, 469.

³³ Childers S. J., Don't Stop the Music: No Strict Products Liability for Embedded Software, University of Florida Journal of Law and Public Policy, Vol. 19, 2008, 166. მითითებულია *Vihul L.*, The Liability of Software Manufacturers for Defective Products, Tallinn Paper No. 2, NATO Cooperative Cyber Defence Centre of Excellence, 2014, 8. მიხედვით იხ. ბმულზე: <https://ccdcoe.org/library/publications/> (ვიზიტის დრო: 24.06.2019).

³⁴ Peppet S. R., Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Texas Law Review, Vol. 93, 2014, 133–134.

³⁵ Encryption – დაშიფრვა, ხშირად გამოყენებადი მექანიზმია კიბერ უსაფრთხოებისთვის. ასეთ დროს ინფორაცია დაშიფრულია ისე, რომ მისი წაკითხვა მხოლოდ ავტორიზებულ პირს შეუძლია, რაც არ გამორიცხავს თავის მხრივ ასეთ შიფრზე სხვათა ხელმისაწვდომობას, თუმცადა მისი აღქმა/წაკითხვა მხოლოდ დაშიფრული ინფორაციის გასაღების მქონდეს შეუძლია. კიბერ შიფრისთვის გამოიყენება ეგრედ წოდებული „ბიტების“ (bits) გრძელი რიგი, რომელიც შედგება ერთიანებისა და ნულიანებისგან. ვრცლად იხ. *Kerr O. S. / Schneier B.*, Encryption Workarounds, Georgetown Law Journal, Vol. 106, Issue 4, 2018, 993–994.

³⁶ Peppet S. R., Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Texas Law Review, Vol. 93, 2014, 133–134.

მიერ.³⁷ IoT მოწყობილობების ტექნიკური კომპლექსურობის მიუხედავად, მათთვის გაზიარებული უნდა იქნეს კონსტრუქციის წუნის თეორია, გამომდინარე იქიდან, რომ ნივთების ინტერნეტის მთავარი ბირთვი პროგრამული უზრუნველყოფაა და დელიქტური პასუხისმგებლობის წყარო სწორედ მისი დაუცველობაა.³⁸

სწორედ პროგრამული უზრუნველყოფისა და ნივთების ინტერნეტის კიბერ დაუცველობის გამო, რომელსაც თავის მხრივ კონსტრუქციის წუნის განაპირობებს, ინტერნეტთან დაკავშირებული მოწყობილობები კიბერ შეტევების მიმართ უძლურნი არიან.³⁹ თავის მხრივ დელიქტური ქმედება სწორედ კიბერ შეტევაში გამოიხატება, რომელიც ყველაზე ხშირად DDoS-ით⁴⁰ არის განხორციელებული. ამავდროულად სხვის მოწყობილობაში შეღწევა DDoS შეტევის განმახორციელებლის მიერ სისხლის სამართლებრივი პასუხისმგებლობის ქმედებად ითვლება,⁴¹ რაც ხშირად მხარისთვის, რომელიც გაუფრთხილებელი ქმედების უკან დგას, ანუ პროდუქტის მწარმოებლისთვის, პასუხისმგებლობის გამომრიცხველია, თუმცა არა მაშინ როდესაც, პირის სისხლის სამართლებრივი ქმედება მისთვის მოსალოდნელი და განჭვრეტადი იყო.⁴² პროგრამული უზრუნველყოფისა და IoT მოწყობილობების მწარმოებლები თანამედროვე ტექნოლოგიების ბაზარზე

³⁷ მაგალითისთვის ელექტრო და თვითმართვადი ავტომობილების მწარმოებელმა კომპანიამ Tesla 2018 წელს 29 000-ზე მეტ ავტომობილს შესთავაზა პროგრამული უზრუნველყოფის განახლება, რითიც გადაჭრა ავტომობილებში ტექნიკური პრობლემა, რაც თავის მხრივ ნივთების ინტერნეტის გარეშე შეუძლებელი იქნებოდა. ვრცლად იხ. *Plant R./ Topham C., How Tesla, Nest And Medtronic Are Using IoT-Derived Data To Move Their Businesses Forward*, Forbes. იხ. ბმულზე <https://www.forbes.com/sites/insights-hitachi/2018/06/12/how-tesla-nest-and-medtronic-are-using-iot-derived-data-to-move-their-businesses-forward/#3b646f0a487a> (ვიზიტის დრო: 24.06.2019).

³⁸ *Butler A., Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, University of Michigan Journal of Law Reform, Vol. 50, Issue 4, 2017, 926-927.

³⁹ *Lichtman D. G./ Posner E., Holding Internet Service Providers Accountable*, The Law and Economics of Cyber security, ed. *Grady M./ Parisi F.*, 2006, 254-255.

⁴⁰ DDoS – distributed denial-of-service, მოცემული შეტევა არის კიბერ ოპერაცია, რომელიც ხორციელდება მართული კომპიუტერული ან ინტერნეტთან დაკავშირებული მოწყობილობებიდან, რომლის მეშვეობითაც სერვისის (საიტის, აპლიკაციას, ოპერაციულ სისტემას) მიეწოდება დიდი რაოდენობით მონაცემები, რომელსაც სერვისის ვერ უმკლავდება, რაც საბოლოოდ მისი ფუნქციონირების შეწყვეტას იწვევს, რაც თავის მხრივ მილიონობით დოლარის ზიანს აყენებს კომპანიას. ვრცლად იხ. *Kesan P. J./ Hayes M. C., Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, Harvard Journal of Law & Technology, Vol. 25, Number 2, 2012, 444-445.

⁴¹ *Butler A., Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, University of Michigan Journal of Law Reform, Vol. 50, Issue 4, 2017, 915.

⁴² *Rustad M. L./ Koenig T. H., The Tort of Negligent Enablement of Cybercrime*, Berkeley Technology Law Journal, Vol. 20, Issue 4, 2005, 1570.

დამკვიდრებული კომპანიები არიან, შესაბამისად მათთვის ნათელია, რომ მათი პროდუქტი შესაძლოა კიბერ თავდასხმის ობიექტი გახდეს, გამომდინარე აქედან თუ ისინი უსაფრთხოების გონივრულ მექანიზმებს არ შეიმუშავენ რისი არარსებობაც წუნის საფუძველია, ისინი დაცვის ღირსნიც არ უნდა იყვნენ.⁴³

როგორც უკვე განვიხილეთ, მწარმოებლის სამოქალაქო სამართლებრივი პასუხისმგებლობა პროგრამული უზრუნველყოფის ან ნივთების ინტერნეტის მოწყობილობის სტრუქტურული წუნის გამო შესაძლებელია დადგეს, თუმცა ისეთ შემთხვევებში სადაც დისტანციური ჩარევა მესამე პირისგან არ ხდება და ზიანი მატერიალური ფორმით არის გამოხატული, მაგალითისთვის, მძიმე ტექნიკის სამუხრუჭე სისტემის გაუმართაობა პროგრამული უზრუნველყოფის წუნის გამო მოხდა, რამაც ფიზიკური ზიანი გამოიწვია, სასამართლომ აღნიშნულ შემთხვევაზე წუნდებული პროდუქტის პასუხისმგებლობა გაავრცელა.⁴⁴ ხოლო IoT-ისთვის ერთ-ერთ საქმეზე მოსარჩელემ მოპასუხის ავტომობილის ნაუცბადევი აჩქარების გამო სასამართლოს შესთავაზა დავის გადაწყვეთა წუნდებული პროდუქტიდან გამომდინარე წესებით გადაეწყვიტა.⁴⁵

თუმცა პრობლემურ საკითხს წარმოადგენს შემთხვევა, როდესაც დელიქტი კიბერ შეტევის განმახორციელებლის მიერ, სხვისი საკუთრების, კონკრეტულად IoT მოწყობილობების ან პროგრამული უზრუნველყოფის გამოყენებით ხდება, რასაც მესამე პირებისთვის ზიანის მიყენება მოსდევს შედეგად, რაც თავის მხრივ ზემოხსენებული პროდუქტის კიბერ უსაფრთხოების წუნით არის გამოწვეული და შესაბამისად საფრთხის მატარებელი და ინტერნეტთან კავშირის დროს მარტივად ხელმისაწვდომია. ნაკლოვანი კიბერ უსაფრთხოება, როგორც წუნი სამოქალაქო პასუხისმგებლობის საფუძველს მწარმოებლების მიმართ ძირითად შემთხვევაში არ წარმოადგენს. რაც უმთავრესად განპირობებულია ეკონომიკური დანაკარგის დოქტრინით (economic loss doctrine).⁴⁶

⁴³ იქვე, 1570.

⁴⁴ იქვე, 1578-1579.

⁴⁵ Ji Chang Son v. Tesla Motors, Inc., მითითებულია *Dean B. C.*, An Exploration of Strict Products Liability and the Internet of Things, Center for Democracy & Technology, 2018, 15.

⁴⁶ *Sales N. A.*, Regulating Cyber-Security, Northwestern University Law Review, Vol. 107, No. 4, 2013, 1535.

1.1.3. ეკონომიკური დანაკარგის დოქტრინის ჩანაცვლება

წუნდებული პროდუქტიდან გამოწვეული ზიანის ანაზღაურების მოთხოვნის შემზღვევლი ერთ–ერთი მთავარი ფაქტორი ეკონომიკური დანაკარგის დოქტრინაა,⁴⁷ რომლის მიხედვითაც მოპასუხისგან ზიანის ანაზღაურება მხოლოდ მაშინ არის შესაძლებელი როდესაც ზიანი ფიზიკურად არის გამოხატული პირის ან საკუთრების მიმართ,⁴⁸ ასევე, შესაძლოა ანაზღაურდეს ყველა სხვა თანმდევი ეკონომიკური დანაკარგი, რომელიც განპირობებულია ფიზიკური ზიანით, მაგრამ არ ანაზღაურდება ფიზიკური ზიანის გარეშე არსებული ეკონომიკური დანაკარგი. სწორედ ეს უკანასკნელი შემთხვევაა უმეტესად სახეზე კიბერ თავდასხმის დროს, პირს თუმცადა ადგება ზიანი, მაგრამ იგი სრულიად ეკონომიკური ხასიათისაა და მას უშუალო ფიზიკური ზიანი პირისა თუ საკუთრების მიმართ არ ახლავს.⁴⁹ თავის მხრივ სტატიკურ შემთხვევაში, სრულიად ნათელია ეკონომიკური დანაკარგის დოქტრინის შემზღვეველობა. მაგალითად როდესაც წუნდებული პროგრამული უზრუნველყოფა ინტერნეტის გარეშე ჩარევისგან დამოუკიდებლად წყვეტს მუშაობას, რასაც მოჰყვება ოპერაციული სისტემის გათიშვა, წარმოების შეჩერება და ისეთი დანაკარგები რაც უშუალოდ პროგრამული უზრუნველყოფიდან არის გამომდინარე.⁵⁰ შეზღუდვის უმთავრესი გამართლება ბაზრის რეგულაციისთვის თავისუფალი სივრცის არსებობაა, უფრო კონკრეტულად კი პროდუქტზე ნდობის საკითხს საერთო სამართალი სრულიად ეკონომიკურ ბაზარს ანდობს.⁵¹ აღნიშნული ტრანსფორმირებულია მომხარებლის სამოქალაქო რისკის არჩევანში, თავად შეარჩიოს პროდუქტი არსებულ ბაზარზე. იყიდოს დაბალ ფასიანი რისკის მატარებელი პროგრამული უზრუნველყოფა და მოწყობილობა, თუ იყოს უფრო დაცული და გაიღოს მეტი რესურსი ძვირადღირებული პროდუქტისთვის. თავის მხრივ ეკონომიკური დანაკარგის დოქტრინა სწორედ პირველ მომხმარებელს ზღუდავს, რომელიც დაბალ ფასიან პროდუქტს ყიდულობს და დანაკარგზე რისკის მატარებელიც თავადვეა.⁵²

განსხვავებული სიტუაციაა, როდესაც დაუცველი პროგრამული უზრუნველყოფისა და ნივთების ინტერნეტის გამო ზიანი ადგებათ

⁴⁷ *Hylton, K.*, Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 344.

⁴⁸ იქვე.

⁴⁹ *Sales N. A.*, Regulating Cyber-Security, Northwestern University Law Review, Vol. 107, No. 4, 2013, 1535.

⁵⁰ *Butler A.*, Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, University of Michigan Journal of Law Reform, Vol. 50, Issue 4, 2017, 920.

⁵¹ *Hylton K.*, Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 345.

⁵² იქვე, 345–346.

ზემოგანხილული ურთიერთობიდან სრულიად გარეშე მესამე პირებს.⁵³ რომლებიც არ არიან პროდუქტის შემძენნი, არამედ ის პირები, რომლებსაც აღნიშნული პროდუქტების წუნდებული კიბერ უსაფრთხოების გამო ადგებათ ზიანი. 2018 წლის მონაცემებით DDoS შეტევებში სადაც წუნდებული პროგრამული უზრუნველყოფა და ნივთების ინტერნეტის მოწყობილობებია ჩართული ზიანმა მესამე პირებისთვის საშუალოდ 120 000 დოლარიდან ორ მილიონ დოლარდე შეადგინა, ყოველი ასეთი შეტევისთვის.⁵⁴ აღნიშნული გარემოების შემთხვევაშიც კი უშუალოდ იმ მწარმოებლისთვის, რომლის მიერაც იქნა წარმოებული წუნდებული კიბერ უსაფრთხოების მქონე პროდუქტი, ზიანის ანაზღაურების მოთხოვნა მესამე პირების მიერ ფაქტიურად შეუძლებელია წუნდებული პროდუქტის პასუხისმგებლობის მოთხოვნით, ეკონომიკური დანაკარგის დოქტრინის შეზღუდვის გამო, თავისთავად ეს უკანასკნელი არ ართმევს მოსარჩელებს უფლებას ზიანის ანაზღაურება სხვა საფუძვლით მოითხოვონ,⁵⁵ ასევე ისეთ შემთხვევაში როდესაც წმინდა ეკონომიკურ დანაკარგს (pure economic loss) ემატება კიბერ შეტევიდან მიყენებული სხვადასხვა მოწყობილობების ფიზიკური დაზიანებაც, ზიანმიყენებულ მესამე პირებს თავისთავად უჩნდებათ წუნდებული პროდუქტიდან გამოწვეული ზიანის მოთხოვნის უფლება.⁵⁶ მაგრამ მიუხედავად ფიზიკური ზიანისა წუნდებული პროდუქტიდან გამომდინარე მოთხოვნა მაინც შეიძლება გამოირიცხოს ინტეგრირებული სისტემის წესის გამო.⁵⁷ ამრიგად დაზარებული მესამე პირები ეკონომიკური დანაკარგის დოქტრინის გამო განხილული ინტერნეტ დელიქტის დროს, წუნდებული პროდუქტის მწარმოებლისგან ანაზღაურებას უმეტეს შემთხვევაში ვერ იღებენ, რასაც ისიც ემატება რომ მათ არც სახელშეკრულებო ბერკეტი არ აქვთ მოთხოვნის საფუძვლად.⁵⁸

⁵³ *Butler A.*, Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, University of Michigan Journal of Law Reform, Vol. 50, Issue 4, 2017, 920.

⁵⁴ ვრცლად იხ. Kaspersky Lab research, https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report (ვიზიტის დრო: 24.06.2019).

⁵⁵ *Scott M. D.*, Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, Maryland Law Review, Vol. 67, Issue 2, 2008, 471.

⁵⁶ *Butler A.*, Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, University of Michigan Journal of Law Reform, Vol. 50, Issue 4, 2017, 921.

⁵⁷ *Wausau Tile, Inc. v. County Concrete Corp.* N.W.2d, 452 (1999). მოთითებულია *Anzivino A. R.*, The False Dilemma of the Economic Loss Doctrine, Marquette Law Review, Vol. 93, 2010, 1122.

⁵⁸ *Butler A.*, Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, University of Michigan Journal of Law Reform, Vol. 50, Issue 4, 2017, 921.

ზემოგანხილულის მიხედვით უსამართლობა იქნებოდა მესამე პირების წუნდებული პროდუქტიდან გამომდინარე ზიანის ანაზღაურების მოთხოვნის ეკონომიკური დანაკარგის დოქტრინით სრულიად შეზღუდვა, განსაკუთრებით კი მაშინ როდესაც მწარმოებელი არ ზრუნავს მისი პროდუქტის კიბერ უსაფრთხოებაზე, ხოლო, მესამე პირები საერთოდ არჩევანს არიან მოკლებულნი პროდუქტის შერჩევას.⁵⁹ ეკონომიკური დოქტრინის ჩანაცვლება ინტერნეტამდე პირველად საქმეზე *People Express Airlines, Inc. v. Consol. Rail*⁶⁰ მოხდა უშუალო მიზეზობრივი კავშირისა (proximate cause) და განჭვრეტადობის დოქტრინით (foreseeability).⁶¹

უშუალო მიზეზობრივი კავშირი და განჭვრეტადობაც იგივე ფუნქციას ემსახურება, რასაც ეკონომიკური დანაკარგის დოქტრინა, მოაქციოს დელიქტური ვალდებულება გონივრულ ჩარჩოში პროდუქტის მწარმოებლისთვის, რათა აღნიშნული ვალდებულება არ გავრცელდეს მის თითოეულ ქმედებაზე, მათ შორის ისეთზეც, სადაც მიზეზობრივი კავშირი ზიანთან ძალიან დაშორებულია მწარმოებლისგან.⁶² ანალოგიურ შინაარსს იზიარებს შორეული კაუზის დოქტრინაც (remoteness doctrine).⁶³

პროგრამულ უზრუნველყოფასთან და ნივთების ინტერნეტთან მიმართებაში უშუალო მიზეზობრივი კავშირი პირიქით აფართოებს მწარმოებლის პასუხისგებლობას რაც საფუძველია მესამე პირებისთვის მოითხოვონ ეკონომიკური დანაკარგები, ფიზიკური ზიანის გარეშე, რადგანაც მწარმოებლების არაგულისხმიერი მიდგომა კიბერ უსაფრთხოების მიმართ არის ერთგვარი კატალიზატორი მესამე პირების ზიანისთვის.⁶⁴ რაც შეეხება განჭვრეტადობას, ის უშუალო მიზეზობრივ კავშირთან ერთად შესაძლოა ერთადერთი საშუალება იყოს განყენებული მესამე პირების მოთხოვნის საფუძვლისთვის, გამომდინარე იქიდან რომ ტექნოლოგიების განვითარებასთან თანმდევი მოულოდნელი შედეგები და ზიანის საფრთხე უფრო და უფრო განჭვრეტადი ხდება მწარმოებლებისთვის და არა პირიქით.⁶⁵ ამრიგად ნათელია, რომ მწარმოებლების მიზეზობრივი კავშირი მესამე

⁵⁹ *Smith W. B.*, Proximity-Driven Liability, *Georgetown Law Journal*, Vol. 102, 2014, 1797.

⁶⁰ *People Express Airlines, Inc. v. Consolidated Rail Corp.*, 495 A.2d 107 (N.J. 1985).

⁶¹ *Sharkey M. C.*, In Search of the Cheapest Cost Avoider: Another View of the Economic Loss Rule, *University of Cincinnati Law Review*, Vol. 85, 2018, 1020.

⁶² *Rustad M. L. / Koenig T. H.*, The Tort of Negligent Enablement of Cybercrime, *Berkeley Technology Law Journal*, Vol. 20, Issue 4, 2005. 1601–1602.

⁶³ *Schwartz E. V.*, Remoteness Doctrine: A Rational Limit on Tort Law, *Cornell Journal of Law and Public Policy*, Vol. 8, Issue 3, 1999, 429.

⁶⁴ *Scott D. M.*, Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, *Maryland Law Review*, Vol. 67, Issue 2, 2008, 448-450.

⁶⁵ *Owen G. D.*, Bending Nature, Bending Law, *Florida Law Review*, Vol. 62, Number 3, 2010, 609

პირების ზიანთან სახეზეა მაშინ როდესაც ისინი კიბერ უსაფრთხოებაზე არ ზრუნავენ და ამით ერთგვარად ხელს უწყობენ კიბერ შეტევების განხორციელებას, ხოლო, ეს უკანასკნელი კი მათთვის სრულიად განჭვრეტადია და მათთვის თავიდანვე სავარაუდოა, რომ მათი წუნდებული პროდუქტი მესამე პირების ზიანს გამოიწვევს.

საბოლოოდ უნდა აღინიშნოს, რომ განხილული მსჯელობიდან კითხვას უნდა დაეკისროს თუ არა პროგრამული უზრუნველყოფისა და IoT მოწყობილობათა მწარმოებლებს პასუხისმგებლობა მათი წუნდებული პროდუქტისთვის, რომლითაც ზიანი მესამე პირებს ადგებათ ნათელია, რომ პასუხი პოზიტიურია, ხოლო ლიტერატურაში გამოთქმულ მოსაზრებას თუ როგორ,⁶⁶ უშუალო მიზეზობრივი კავშირი და განჭვრეტადობის დოქტრინა ესადაგება.

1.2. ინტერნეტ საშუალებებით ვირტუალური საკუთრების ხელყოფა

Trespass, როგორც ხელყოფის ან ზიანის მიყენების,⁶⁷ ტრანსფორაცია ინტერნეტ სივრცეში ამერიკის შეერთებული შტატების სასამართლოების დამსახურებაა. თუმცადა აღსანიშნავია, რომ სანამ ხელყოფიდან (trespass) გამომდინარე დოქტრინის კიბერ/ინტერნეტ ხელყოფის (cybertrespass) დამკვიდრება მოხდებოდა, რომელიც *Compuserve v. Cyber Promotions*⁶⁸ და *eBay, Inc. v. Bidder's Edge*⁶⁹ საქმეებს უკავშირდება, მისი უმნიშვნელოვანესი პროვოცირება არა კიბერ დავაზე, არამედ ტელეკომუნიკაციებთან დაკავშირებულ საქმეზე მოხდა *Thrifty-Tel v. Bezenek*⁷⁰, სადაც სასურველი შედეგის მისაღწევად მოსარჩელე მხარემ, რომლის სატელეფონო სერვისი არამართლზომიერად იქნა გამოყენებული მოპასუხე მხარის მიერ, რათა ამ უკანასკნელს განეხორციელებინა ფასიანი ზარები უფასოდ, სასამართლოს შესთავაზა უკანონო მითვისების (conversion) დოქტრინის გამოყენება, რაც თავის მხრივ სასამართლომ უარყო იმ მიზეზით, რომ უკანონო მითვისება, გამოიყენება მხოლოდ განსხეულებული ნივთებისადმი, სასამართლომ მოცემული დელიქტური ქმედება მოაწესრიგა, როგორც მოძრავი ნივთის ხელყოფა (trespass to chattels), რაც ასევე, არასდროს ყოფილა გამოყენებული

⁶⁶ *Butler A.*, Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, *University of Michigan Journal of Law Reform*, Vol. 50, Issue 4, 2017, 919.

⁶⁷ *ცვაიგერტი ვ./ კოტცი ჰ.*, შედარებითი სამართალმცოდნეობის შესავალი კერძო სამართლის სფეროში, ტ. 2, რედაქტორი *ნინიძე თ.*, ჯისიაი, თბილისი 2001, 297–298.

⁶⁸ *Compuserve Inc. v. Cyber Promotions*, 962 F. Supp. 1015 (S.D. Ohio 1997)

⁶⁹ *eBay, Inc. v. Bidder's Edge LLC*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000)

⁷⁰ *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559 (4th Dist. 1996)

არამატერიალური ნივთებისადი.⁷¹ სწორედ აქედან მოყოლებული კიბერ ხელყოფა განიხილება როგორც მოძრავი ნივთის ხელყოფის დერივაცია.

მოძრავი ნივთის ხელყოფა, როგორც საფუძველი კიბერ ხელყოფისთვის (cybertrespass), დოქტრინის არსებობისა და მისი სასამართლო პრაქტიკის ადრეულ ეტაპზე სრულიად მისაღები იყო, როგორც სასამართლოებისთვის, ასევე, სამართლის აკადემიური სივრცისთვის.⁷² თუმცაღა დროთა განმავლობაში დამკვიდრებულ კიბერ ხელყოფის დოქტრინას მრავალი კონტროვერსიული ასპექტი გამოუჩნდა, რომელთაც შემდგომ ქვეთავებში განვიხილავთ.

1.2.1. ინტერნეტ სივრცის ბუნება კიბერ ხელყოფასთან მიმართებაში

ტერმინი trespass არამხოლოდ ინტერნეტ ხელყოფისთვის, არამედ ზოგადად trespass to chattels–თან მიმართებაში გაგებული უნდა იქნეს როგორც მოძრავი ნივთის ხელყოფა ან მფლობელობაში ხელშეშლა და არა როგორც სივრცის დარღვევა მოძრავ ნივთთან მიმართებაში, როგორც trespass–ის დამკვიდრებული დეფინიცია.⁷³ რაც სრულიად მისაღები და გამართლებულია, გამოდინარე იქიდან, რომ როგორც სამართლებრივად, ასევე, ფიზიკური სამყაროს ბუნებიდან რთულად წარმოსადგენია მოძრავი ნივთისადმი საზღვრის/სივრცის რღვევა.

ნათელია, რომ კიბერ ხელყოფის ჩამოყალიბებისას, როგორც მოძრავი ნივთის ხელყოფიდან გამომდინარე დოქტრინა, არ იყო გათვალისწინებული უშუალოდ ინტერნეტისა და ონლაინ სივრცის ბუნება, შესაბამისად მისი დაცვის ქვეშ უნდა მოქცეულიყო მხოლოდ ის მატარებელი რომლითაც ინტერნეტზე წვდომა ხდება,⁷⁴ გამომდინარე აქედან, მხარე რომელიც დოქტრინისგან დაცვას ელოდებოდა ან მნიშვნელოვნად გაფართოებულად იღებდა მას ან კონტრასტულად დაუცველი რჩებოდა.⁷⁵

⁷¹ *Balganesh S.*, Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass, Michigan Telecommunications and Technology Law Review, Vol. 12, 2006, 279.

⁷² *Hedley S.*, Cybertrespass – A Solution in Search of a Problem?, Journal of European Tort Law, Vol. 5, Issue 2, 2014, 171-172.

⁷³ *Lastowka G.*, Decoding Cyberproperty, Indiana Law Review, Vol. 40, No. 1, 2007, 27.

⁷⁴ მაგალითად კომპიუტერები, მათი შემადგენელი ნაწილები, ასევე, სერვერები სადაც შესაძლოა ელექტრონული ფოსტის მონაცემთა ბაზები იყოს განთავსებული ან ვებ-ჰოსტინგის სერვერები, სადაც საიტი თავის კონტენტს ტვირთავს.

⁷⁵ *Fairfield J.*, Virtual Property, Boston University Law Review, Volume 85, 2005, 1075.

ინტერნეტ სივრცის შემადგენელი კომპონენტების გათვალისწინებით, იქნება ეს ვებ-საიტი, ელექტრონული ფოსტა თუ სხვა რესურსი,⁷⁶ ერთი მოსაზრების თანახმად უფრო მეტად გასაზიარებელია მათთვის რომ ისინი არა მოძრავ ნივთებს (personal property) წარმოადგენენ, არამედ მეტი ფიქსაციის გამო ემსგავსებიან უძრავ ნივთებს (real property).⁷⁷ გამომდინარე აქედან სწორედ მოცემული ასპექტის გამო ამერიკული სამართლის დელიქტური და სანივთო სამართალი მნიშვნელოვან როლს თამაშობდა ინტერნეტ ხელყოფისთვის, რაც თავის მხრივ წარმოშობს კონკურენციას trespass to chattels-სა და trespass to land-ს შორის განსახილველ საკითხთან დაკავშირებით.⁷⁸ თუმცაღა აღნიშნული კონკურენცია ზოგადად trespass-ისთვის, როგორც ხელყოფა, ამერიკული სამართლისთვის დამახასიათებელია, კომენტატორთა ერთი მოსაზრების თანახმად აღნიშნული განპირობებულია ინგლისური საერთო სამართლიდან შეგნებული გადახვევით, ხოლო, მეორე მოსაზრების მიხედვით ისეთი ნომინალური ხელყოფა სადაც ზიანი არ არსებობს, მხარე სასამართლო დაცვას არ საჭიროებს.⁷⁹ ყოველივე განხილულიდან გამომდინარე კიბერ ხელყოფა, როგორც მოძრავი ნივთის ხელყოფა პრობლემურ დოქტრინად გვევლინებოდა და შეიძლება ითქვას მისი ჩანაცვლება ადრეულ ეტაპზე უძრავი ნივთების ხელყოფით (trespass to land) გაცილებით რაციონალურ სახეს მისცემდა მას.

1.2.2. ინტერნეტ ხელყოფის კრიტიკა

მოძრავი ნივთების ხელყოფა შესაძლოა განხორციელდეს მაშინ როდესაც პირი განზრახი მოქმედებით სხვა პირს ჩამოართმევს მფლობელობას ნივთზე ან იყენებს სხვის მოძრავ ნივთს ან ხელს უშლის მოძრავი ნივთის მფლობელს მის ფლობაში.⁸⁰ თუმცაღა დელიქტის მიმყენებლის პასუხისმგებლობა მფლობელის წინაშე დადგება მხოლოდ მაშინ როდესაც, მან მფლობელს ჩამოართვა ნივთი, ნივთი კარგავს მის მახასიათებელს, ხარისხს ან ღირებულებას, მფლობელი არსებითი დროის მანძილზე ვერ ახდენს ნივთის გამოყენებას ან ზიანი ადგება მფლობელს, სხვა პირს ან ნივთს, რომლის მიმართაც მფლობელს გააჩნია სამართლებრივი ინტერესი.⁸¹ სწორედ მოცემული განმარტება უნდა გამხდარიყო ინტერნეტ ხელყოფის დოქტრინის საფუძველი, თუმცაღა საქმეზე *Compuserve v. Cyber Promotions* სასამართლომ

⁷⁶ იქვე, 1052–1053

⁷⁷ *Epstein R. A.*, *Cybertrespass*, *University of Chicago Law Review*: Vol. 70, Iss. 1, Article 6, 2003, 83.

⁷⁸ იქვე, 78.

⁷⁹ *Lastowka G.*, *Decoding Cyberproperty*, *Indiana Law Review*, Vol. 40, No. 1, 2007, 28.

⁸⁰ *American Law Institute*, *Restatement of the Law, Second, Torts, Volume 1*, 1965, § 217.

⁸¹ იქვე, § 218.

განსხვავებული სტანდარტი დაამკვიდრა მოძრავი ნივთების ხელყოფისთვის, როგორც ინტერნეტ ხელყოფა. საქმეში სადაც მოსარჩელე ონლაინ სერვისების პროვაიდერი იყო სადავოდ ხდიდა მოპასუხის ქმედებას, რომლითაც იგი მოსარჩელის სერვერების გამოყენებით Compuserve მომხმარებლებისთვის გზავნიდა არასასურველ რეკლამებს ელექტრონული ფოსტით. სასამართლომ დავის მოწესრიგება, თავისთავად მოძრავი ნივთების ხელყოფის დოქტრინით სცადა და თუმცაღა მან გაითვალისწინა დოქტრინის შეზღუდვა რომ აუცილებელია რეალური ფიზიკური ზიანის არსებობა, რომელიც თავის მხრივ მოსარჩელემ უნდა ამტკიცოს, როგორც უკვე აღვნიშნეთ გარემოებით რომ ნივთმა დაკარგავა მისი მახასიათებელი, ხარისხი ან ღირებულება,⁸² სასამართლომ მსგავსად Thrifty-Tel v. Bezenek-სა არ გაითვალისწინა ქმედების prima facie მახასიათებელი და ზედაპირულად მიმოიხილა იგი.⁸³ რასაც ნათლად ხაზს უსვამს შემდეგი გარემოებები, მოცემულ საქმეზე ორი სახის ზიანი დადგინდა. პირველი, ეს იყო დიდი რაოდენობით ელექტრონული წერილები, რომლებიც მნიშვნელოვან ადგილს იკავებდა მოსარჩელის მყარ დისკზე და აფერხებდა მათი კომპიუტერების წარმადობას, რამაც სასამართლოს აზრით შეამცირა მოსარჩელის ნივთის ღირებულება, მიუხედავად იმისა რომ განსხვავებული ზიანი არ წარმოშობილა და მეორე, სერვისის მომხმარებლებს ელექტრონული ფოსტა უშუალოდ მოსარჩელისგან მისდიოდათ, რაც მათ უკმაყოფილებას იწვევდა და საბოლოო ჯამში რეპუტაციას, როგორც იურიდიულ ინტერესს უქმნიდა საფრთხეს. მიუხედავად იმისა რო ერთი შეხედვით ორივე ზიანი მოძრავი ნივთების ხელყოფას აკმაყოფილებს, დოქტრინა მოიცავს მხოლოდ პირდაპირ ფიზიკურ ზიანს, რაც როგორც პირველ შეთხვევაში არ იყო სახეზე, და იგი მხოლოდ არასასურველი ელექტრონული შეტყობინებებით იყო გამოწვეული, ასევე, მეორე შეთხვევაც, სამართლებრივი ინტერესის ხელყოფაც არ იყო გამოწვეული პირდაპირი ზიანით, არამედ ისევ და ისევ არასასურველი ელექტრონული წერილებით, რომლებზეც მომხმარებლები პრეტენზიას გამოთქვამდნენ.⁸⁴ ამრიგად სასამართლომ დოქტრინას გვერდი აუარა და მოძრავი ნივთების ხელყოფის ტრანსფორაცია კიბერ ხელყოფისთვის დაამკვიდრა, პირდაპირი ფიზიკური ზიანის არსებობის არასავალდებულო ხასიათით.⁸⁵

⁸² *Balganesh S.*, Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass, *Michigan Telecommunications and Technology Law Review*, Vol. 12, 2006, 281.

⁸³ იქვე, 280.

⁸⁴ იქვე, 281–282.

⁸⁵ ანალოგიური გადაწყვეტილება იქნა მიღებული საქმეზე *eBay, Inc. v. Bidder's Edge*, სადაც მოსარჩელე eBay-მ მიიღო მოპასუხის საწინააღმდეგოდ მოქმედების შესრულების აკრძალვა.

ზემოგანხილულმა სასამართლო პრაქტიკამ საფუძველი ჩაუყარა კიბერ ხელყოფისთვის მოძრავი ნივთების ხელყოფის სარჩელის აღძვრას უფრო ფართო საფუძველებით ვიდრე დოქტრინა იძლევა ამის საშუალებას. კონკრეტულად კი სასამართლოს შეეძლო სარჩელი დაეკმაყოფილებინა ნივთის რეალური ზიანის ან ასეთი ზიანის საფრთხის არსებობისას, ან თუ ზიანი მის მფლობელს ან სხვა ნივთს მიადგებოდა და არა სავალდებულოდ ხელყოფის ობიექტს, ასევე, შემთხვევაში როდესაც ზიანი კომპიუტერულ სისტემაში ჩარევამ გამოიწვია და ბოლოს მხარემ შეიძლება მიიღოს მოპასუხის წინააღმდეგ მოქმედების შესრულების აკრძალვა იმ შემთხვევაშიც კი როდესაც არანაირი ზიანი არ იარსებებს და საქმე მხოლოდ მოპასუხის ნივთის გამოყენებასთან გვექნება ინტერნეტის საშუალებით.⁸⁶ გამომდინარე აქედან, მიუხედავად გაფართოებული შესაძლებლობისა, კიდევ უფრო ბუნდოვანი გახდა თუ რა სახის ზიანი უნდა ამტკიცოს მოსარჩელემ ყოველი კონკრეტული შემთხვევისთვის, რაც კრიტიკის ერთ-ერთი მთავარი საფუძველია. აღნიშნულთან დაკავშირებით გასაზიარებელია მოსაზრება, რომ მოძრავი ნივთების ხელყოფის დოქტრინა უშუალოდ მფლობელობით ინტერესს უკავშირდება მოძრავი ნივთისადმი და მისი ფიზიკური დაცვისკენ არის მიმართული, შესაბამისად მფლობელობითი ინტერესი ქარწყლდება მაშინ, როდესაც ნივთისადმი დაცვას ანაცვლებს სხვა გარეშე ინტერესი, მაგალითად ეკონომიკური სარგებელი, რომელიც მან შეიძლება მოიტანოს.⁸⁷

დოქტრინის გვერდის ავლის კრიტიკის საბოლოო გამართლება და პრაქტიკის შეცვლა მოხდა საქმეზე Intel Corp. v. Hamidi⁸⁸ კალიფორნიის შტატის უზენაესი სასამართლოს მიერ. საქმეში მოპასუხე მოსარჩელის ყოფილ თანამშრომელს წარმოადგენდა, რომელიც თავის ყოფილ კოლეგებს სამუშაო ელექტრონულ ფოსტაზე უგზავნიდა კონკრეტული შინაარსის წერილებს მოსარჩელის, როგორც დამსაქმებლის წინააღმდეგ, ჯამში ასეთი წერილების ოდენობა 30 000-ზე მეტი იყო. თუმცა კომპანიას წერილებით არანაირი ზიანი არ მიადგა და როგორც სასამართლომ აღნიშნა დავის მთავარი საფუძველი წერილების შინაარსი იყო და არა ზიანი.⁸⁹ მოსარჩელის მოთხოვნა თავისთავად არა ზიანის ანაზღაურება, არამედ მოქმედების შესრულების

მოცემულ საქმეზე დავა არა ელექტრონული ფოსტით ხელყოფას, არამედ ვებ საიტიდან დიდი რაოდენობით ინფორმაციის მოთხოვნას ეხებოდა, რაც მნიშვნელოვნად აფერხებდა მოპასუხის სერვერის მუშაობას, სადაც საიტი იყო განთავსებული.

⁸⁶ *Bellia L. P.*, *Defending Cyberproperty*, *New York University Law Review*, Vol. 79, 2004, 2178-2179.

⁸⁷ იქვე, 2181.

⁸⁸ *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003)

⁸⁹ *Wong M.*, *Cyber-trespass and 'Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience* *International Journal of Law and Information Technology*, Vol. 15, Issue 1, 2007, 107.

აკრძალვა იყო, რაც დაკავშირებულია არა მხოლოდ არასასურველი მოქმედების აღმოფხვრასთან, არამედ იმასთანაც, რომ სადაც ზიანის ფულადი სახის ანაზღაურებაა შესაძლებელი იქ მოქმედების შესრულების აკრძალვა ვერ იქნება გამოყენებული.⁹⁰ უზენაეს სასამართლომდე, ორივე ქვემდგომმა სასამართლო ინსტანციებმა მოსარჩელის მოთხოვნა დააკმაყოფილა და მოძრავი ნივთების ხელყოფაზე დამკვიდრებული გაფართოებული პრაქტიკით გაამყარა გადაწყვეტილება. თუმცადა უზენაესმა სასამართლომ აღნიშნული გადაწყვეტილებები შეცვალა და განმარტა რომ წინამორბედი პრაქტიკა⁹¹ არ იყო მართებული, არამხოლოდ კალიფორნიის შტატის სამართლისთვის, არამედ მთლიანად ამერიკული სამართლისთვის – მოძრავი ნივთების ხელყოფის დოქტრინისთვის დაუშვებელია ზიანის არსებობის გამორიცხვა, რომლის არსებობაც მოსარჩელემ უნდა ამტკიცოს.⁹² უნდა ჩაითვალოს, რომ მაშინდელი სასამართლო პრაქტიკის განვითარების ტენდენციიდან გამომდინარე გადაწყვეტილება მართებულია და უნდა იქნეს გაზიარებული, რომ მოძრავი ნივთის ხელყოფისთვის ინტერნეტ ხელყოფასთან მიმართებაში, დოქტრინამ უნდა შეინარჩუნოს მისი ტრადიციული სახე, რომელიც უშუალო ზიანის არსებობას უკავშირდება, წინააღმდეგ შემთხვევაში მოსარჩელე სარჩელის წარდგენის ისეთ ფართო შესაძლებლობას მიიღებდა, რომელიც თავის თავში მოიცავდა როგორც ჩვეულებრივი ინტერნეტ კომუნიკაციის აღკვეთას, ასევე, პოტენციური სამომავლო ზიანის⁹³ არსებობას.

Intel Corp. v. Hamidi საქმის შემდეგ იშვიათად თუ მომხდარა ინტერნეტ ხელყოფის დელიქტის გამოყენება წარმატებით სასამართლო დავისას, რამაც თავის მხრივ თავისუფლება მისცა სხვა სამართლებრივ მექანიზმებს მოეგვარებინათ მსგავსი დელიქტური შეთხვევები.⁹⁴

1.2.3. თვითდახმარება, ხსნა თუ კრიტიკის კიდევ ერთი საფუძველი?

თვითდახმარება (self-help) სამართლებრივ ჭრილში შესაძლოა მოვიაზროთ არა როგორც რაიმე კონკრეტული, არამედ რიგი ქმედებებისა,⁹⁵ რომელთაც

⁹⁰ *Sharkey M. C.*, *Trespass Torts and Self-Help for an Electronic Age*, *Tulsa Law Review*, Vol. 45, 2010, 104.

⁹¹ იგულისხმება *Thrifty-Tel v. Bezenek*, *eBay, Inc. v. Bidder's Edge*.

⁹² *Lastowka G.*, *Decoding Cyberproperty*, *Indiana Law Review*, Vol. 40, No. 1, 2007, 37–38.

⁹³ *Sharkey M. C.*, *Trespass Torts and Self-Help for an Electronic Age*, *Tulsa Law Review*, Vol. 45, 2010, 115.

⁹⁴ *Hedley S.*, *Cybertrespass – A Solution in Search of a Problem?*, *Journal of European Tort Law*, Vol. 5, Issue 2, 2014, 175-178.

⁹⁵ მაგალითისთვის ღია მიწის ნაკვეთისთვის, რომელიც ხშირად მეზობლების სასაქონლო მოედანს წარადგენს, რაც ჩვენთვის შესაძლოა უსიამოვნო იყოს, ღობის მოწყობით.

პირი ახორციელებს სახელმწიფო/სასამართლო დახმარების გარეშე რათა დაიცვას საკუთარი იურიდიული ინტერესი და უფლება.⁹⁶ მიუხედავად იმისა, რომ თვითდახმარება შესაძლოა გამოყენებულ იქნეს სხვადასხვა სამართლებრივი სივრცისთვის, გადამეტებული მცდელობა შესაძლოა გადაიზარდოს სისხლის სამართლებრივ დანაშაულში, გამომდინარე აქედან თვითდახმარება სამართლებრივად შეზღუდული მექანიზმია.⁹⁷

ინტერნეტ საკუთრების (cyberproperty) დეფინიციის საფუძველი ტრადიციული საკუთრებაა და შესაბამისად იგი იმეორებს მის ისეთ მახასიათებლებს, როგორცაა მფლობელობითი ინტერესი და სხვათა ზემოქედების გამორიცხვის უფლება (right to exclude).⁹⁸ გამომდინარე იქიდან რომ სასამართლო პრაქტიკა ინტერნეტ სივრცის შემადგენლობას, სერვერებს, ბაზებს და სხვა ელემენტებს აღიქვამს როგორც მოძრავ ნივთებს თვითდახმარება სწორედ მის ფარგლებში უნდა იყოს მოაზრებული, უფრო კონკრეტულად კი, როგორც უკვე აღვნიშნეთ უმნიშვნელო ზიანის ან ზიანის გარეშე ხელყოფის დროს პირი მოკლებულია მიმართოს სარჩელს მოძრავი ნივთის ხელყოფის გამო, მაგრამ იგი იღებს საკმარის სამართლებრივ დაცვას მისი მოძრავი ნივთისადმი, რომელიც ერთგვარი პრივილეგიაა რომ დაცული იყოს საკუთრება ნებისმიერ ჩარევისგან საკუთარი ძალებით.⁹⁹

მნიშვნელოვანია გარემოება, რომლის მიხედვითაც, მოსარჩელეს სასამართლოში სარჩელის წარდგენა მხოლოდ მას შემდეგ შეუძლია რაც იგი თვითდახმარების ზომებს მიმართავს და ისინი მისთვის უშედეგო გამოდგება, უფრო ზუსტად კი ამოწურავს თვითდახმარების ბარიერებს. აღნიშნულს სასამართლომ საქმეზე *CompuServe v. Cyber Promotions* ნიშნელოვნად გაუსვა ხაზი.¹⁰⁰ თუმცადა სადავოა რა უნდა ჩაითვალოს თვითდახმარების საშუალებების ამოწურვად. ერთი მოსაზრების თანახმად, ინტერნეტ ხელყოფისთვის, თვითდახმარების ლიმიტის ამოწურვად უნდა ჩაითვალოს მნიშვნელოვანი ტექნიკური საშუალებების გამოყენება, რომელიც დაბლოკავდა არასასურველ წვდომას, ხოლო, მეორე მოსაზრების თანახმად საკმარისია მინიმალური შეტყობინების სტანდარტი, რომლის მიხედვითაც

⁹⁶ *Chandler A. J.*, Technological Self-Help and Equality in Cyberspace, McGill Law Journal, Vol. 56, Number 1, 2010, 42.

⁹⁷ იქვე, 42–43.

⁹⁸ *Carrier A. M./Lastowka G.*, Against Cyberproperty. Berkeley Technology Law Journal, Vol. 22, 2007, 1485.

⁹⁹ *Epstein R. A.*, Cybertrespass, University of Chicago Law Review: Volume 70 Iss. 1, Article 6, 2003, 77.

¹⁰⁰ *Sharkey M. C.*, Trespass Torts and Self-Help for an Electronic Age, Tulsa Law Review, Vol. 45, 2010, 110.

ლიმიტის ამოწურვად უნდა ჩაითვალოს ჩვეულებრივი ტექსტი არასასურველი მოქმედების აკრძალვის შესახებ.¹⁰¹

თვითდახმარება ინტერნეტ ხელყოფისთვის მრავალი საშუალებით შეიძლება იქნეს მიღწეული, მაგალითისთვის ინტერნეტ რესურსის ადმინისტრატორს შეუძლია არასასურველი მომხმარებლის IP მისამართი დაბლოკოს ან სულაც კომპანიამ დახურული (არასაჯარო) საიტი შექმნას, სადაც ინფორმაცია ხელმისაწვდომი მხოლოდ გამომწერებისთვის იქნება.¹⁰² თუმცა ინტერნეტ სივრცის და ზოგადად ინფორმაციული ტექნოლოგიების ბუნებიდან გამომდინარე ასეთი თვითდახმარების მექანიზმები დიდ რესურსს მოითხოვს და ხშირად არაეფექტურიცაა, ყოველ დაბლოკილ IP მისამართს შეიძლება მოჰყვეს შეცვლილი ან სულაც proxy სერვერის საშუალებით შენიღბული მისამართი, რომელიც გვერდს ბლოკს აუვლის. რაც თავისმხრივ ერთგვარ დაუსრულებელ თამაშს დაემსგავსება.¹⁰³

ინტერნეტ საკუთრების მოაზრება, როგორც ჩვეულებრივ რეალურ სივრცეში არსებული საკუთრება, უკავშირდება ინტერნეტ საკუთრებისთვის ყველა იმ უფლებით სარგებლობას, რომელიც ზოგადად საკუთრებას გააჩნია.¹⁰⁴ სწორედ ასეთი ერთ–ერთი უმთავრესი უფლებაა სხვათა ზემოქედების გამორიცხვის უფლება, რომელიც მესაკუთრეს უფლებას აძლევს, სხვებს საკუთარი შეხედულებიდან გამომდინარე აუკრძალოს საკუთრებით სარგებლობა, არსებობს მოსაზრება, რომ მოცემული უფლების არ არსებობის შეთხვევაში ზედმეტი იქნებოდა საკუთრების უფლებაზე საუბარი, რადგანაც ფაქტიურად მოისპობოდა კერძო საკუთრების არსი, გამომდინარე იქიდან რომ ნებისმიერი პირი შეძლებდა სხვისი საკუთრებით სარგებლობას.¹⁰⁵ თვითდახმარებასა და სხვათა ზემოქედების გამორიცხვის უფლების ურთიერთმიმართებასთან დაკავშირებით მნიშვნელოვანია, რომ თვითდახმარების ნებისმიერი მოქმედება ემსახურება სხვათა ზემოქმედების გამორიცხვის უფლების რეალიზებას, შესაბამის იგი ერთ–ერთი ინსტრუმენტია ამ უფლების განსახორციელებლად.

¹⁰¹ იქვე, 109.

¹⁰² აღნიშნულ მეთოდს მრავალი კომპანია თუ ბიბლიოთეკა იყენებს, ასევე, საგულისხმოა რომ მეთოდის გამოყენება კონტრასტულად, დახურული ტორენტ ტრეკერების მიერაც ხდება.

¹⁰³ *Keamey D.*, Network Effects and the Emerging Doctrine of Cybertrespass, *Yale Law & Policy Review*, Vol. 23, Issue 1, 2005, 318.

¹⁰⁴ *Balganesh S.*, Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass, *Michigan Telecommunications and Technology Law Review*, Vol. 12, 2006, 294.

¹⁰⁵ იქვე.

მოდრავი ნივთის ხელყოფისთვის სხვათა ზემოქმედების გამორიცხვის უფლება, შესაძლოა მოვიაზროთ, როგორც არა უფლება არამედ პრივილეგია მესაკუთრისთვის, რასაც ორი საფუძველი აქვს, პირველი ეს არის ზემოქმედების გამორიცხვის საშუალების არჩევანი, ხოლო, მეორე პირი რომლისთვისაც გამოირიცხა ზემოქმედების საშუალება ვერ მოახდენს აპელირებას სხვა უფლებაზე ან მოთხოვნაზე, რომლითაც აუკრძალავს ნივთის მესაკუთრეს გამორიცხვის უფლების გამოყენებას.¹⁰⁶ თვალსაჩინოებისთვის, მართალია საიტის მესაკუთრე ვერ აუკრძალავს მომხმარებელს, რომ არ შემოვიდნენ საიტზე, თუმცა იგი ჩაკეტავს საიტს და ხელმისაწვდომს გახდის მხოლოდ წინასწარ განსაზღვრული პირთა წრისთვის, ხოლო, სხვა ყველასთვის ვინც ვერ იღებს საიტზე წვდომას ეს ვერ გახდება სასამართლოში სარჩელის წარდგენის მიზეზი, იმ საფუძველით, რომ მათ აუკრძალონ საიტის მესაკუთრეს მსგავსი მოქმედების განხორციელება.

თუმცა ზემოგანხილულ სხვათა ზემოქმედების გამორიცხვის უფლებასაც გამოუჩნდა კრიტიკა, არა კონკრეტულად მოდრავი ნივთის ხელყოფასთან მიმართებაში, არამედ ზოგადად ინტერნეტ საკუთრებასთან დაკავშირებით, უფრო კონკრეტულად კი აღნიშნული უფლების მინიჭება ინტერნეტ რესურსის მესაკუთრეთათვის ინტერნეტის განვითარებისთვის კატასტროფული შედეგების მომტანი იქნებოდა.¹⁰⁷ მოცემული მოსაზრების მთავარი არგუმენტი ისაა, რომ ინტერნეტ მესაკუთრეები ხშირად გამოიყენებდნენ უფლებას, რითიც დაბლოკავდნენ პოზიტიურ მოქმედებებსაც კი მომხმარებელთა მხრიდან,¹⁰⁸ ხოლო, ამ უკანასკნელთა პოზიციიდან კი ყოველთვის საიტზე თუ სხვა რესურსზე წვდომა მხოლოდ მესაკუთრესთან მოლაპარაკებების შემდეგ იქნებოდა შესაძლებელი, რაც ნათელია რომ ინტერნეტის პროდუქტიულობას მნიშვნელოვნად შეამცირებდა.¹⁰⁹ მიუხედავად რაციონალური არგუმენტისა, ინტერნეტ საკუთრებამ დროთა განმავლობაში მაინც აითვისა სხვათა ზემოქმედების გამორიცხვის უფლება და ინტერნეტში ვხვდებით, როგორც ღიად ხელმისაწვდომ რესურსებს, ასევე, დახურულ რესურსებსაც.

ამრიგად რთულია იმის თქმა რომ თვითდახმარება გვევლინება, როგორც დოქტრინალური status quo, რომელიც მოდრავი ნივთის ხელყოფის იმ ნაკლს ავსებს კიბერ ხელყოფისთვის, რომელიც მას უნდა გააჩნდეს უმრავი ნივთის

¹⁰⁶ იქვე, 295.

¹⁰⁷ *Bellia L. P.*, *Defending Cyberproperty*, *New York University Law Review*, Vol. 79, 2004, 2170.

¹⁰⁸ იქვე, 2171.

¹⁰⁹ იქვე, 2202.

ხელყოფის დოქტრინიდან.¹¹⁰ მიუხედავად ამისა უდავოა რომ იგი მნიშვნელოვან ელემენტად გვევლინება ინტერნეტ რესურსის დასაცავად, შესაბამისად კრიტიკა მისი არაეფექტურობის შესახებ უსაფუძვლოდ უნდა მივიჩნიოთ. რაც შეეხება ზემოქედების გამორიცხვის უფლებას, როგორც უკვე აღვნიშნეთ იგი სხვადასხვა ინტერნეტ რესურსის მიერ განსხვავებულად გამოიყენება.

1.3. ონლაინ დეფამაცია

პასუხისმგებლობა დეფამაციისთვის საერთო სამართლისთვის სიახლეს არ წარადგენს.¹¹¹ მიუხედავად იმისა რომ ინტერნეტ დეფამაცია მნიშვნელოვნად ემსგავსება ტრადიციულ დეფამატორულ დელიქტს, მას მაინც გააჩნია თავისი სპეციფიკური მახასიათებლები.¹¹²

ციფრული სამყაროს ფართო ხელისაწვდომობამდე დეფამატორული განცხადებებიდან გამომდინარე სარჩელები ძირითადად მასმედიის წინააღმდეგ იყო მიმართული, თუმცაღა ინტერნეტის განვითარებასთან ერთად მოპასუხეებად ძირითადად ბლოგერები, სოციალური მედიისა და სხვადასხვა ონლაინ ფორუმის მომხმარებლები გვევლინებიან.¹¹³ აღნიშნულმა მთელი რიგი ისეთი ახალი პრობლემური საკითხებისა წარმოშვა, როგორიცაა ვებ-საიტზე გამოქვეყნებული ცნობა, როგორც ზიანის წყარო, არაადეკვატური სამართლებრივი დაცვის საშუალებები,¹¹⁴ ვის უნდა დაეკისროს პასუხისმგებლობა ანონიმური ინტერნეტ დეფამაციისთვის¹¹⁵ და ბოლოს ინტერნეტ შუამავლების პასუხისმგებლობის საკითხი.

ზოგადი განმარტების მიხედვით ონლაინ დეფამაცია განხორციელებულია მაშინ, როდესაც პირის შესახებ ცრუ ცნობების ან ცილისწამების შეტყობინება (გამოქვეყნება) ხდება მესამე მხარისთვის. რასაც მოჰყვება ზიანი ან აღნიშნული ცნობები იმდენად მაპროვოცირებელია, რომ ზიანის დადგომა სავარაუდოა.¹¹⁶ აღსანიშნავია, რომ ტრადიციული დეფამაციის მსგავსად

¹¹⁰ *Sharkey M. C.*, *Trespass Torts and Self-Help for an Electronic Age*, *Tulsa Law Review*, Vol. 45, 2010, 120–121.

¹¹¹ *Garon M. J.*, *Tidying up the Internet: Take Down of Unauthorized Content under Copyright, Trademark and Defamation Law*, *Capital University Law Review*, Vol. 41, 2013, 529.

¹¹² იქვე.

¹¹³ *Ardia S. D.*, *Freedom of Speech, Defamation, and Injunctions*, *William & Mary Law Review*, Vol. 55, 2013, 5.

¹¹⁴ იქვე, 16.

¹¹⁵ *Perry R./ Zarsky R.*, *Who Should Be Liable for Online Anonymous Defamation?*, *University of Chicago Law Review Dialogue*, Vol. 82, 162.

¹¹⁶ *Rustad M. L.*, *Global Internet Law in a Nutshell*, 3rd edition, West Academic, St. Paul 2016, 187.

ინტერნეტში გავრცელებული ცნობისთვის, მოპასუხე სრულ დაცვას იძენს თუ აღნიშნული ცნობა სიმართლეს წარმოადგენს.¹¹⁷

1.3.1. ვებგვერდზე გამოქვეყნებული კონტენტი, როგორც ზიანის წყარო

ინტერნეტის ბუნებიდან გამომდინარე ნებისმიერ პირს სხვადასხვა პლატფორმაზე მხოლოდ რეგისტრაციის შემდეგაც მარტივად შეუძლია ყოველგვარი მოდერაციის გარეშე ნებისმიერი ცნობის განთავსება (დაპოსტვა),¹¹⁸ ნათელია, რომ ცნობის შემცველი კონტენტი, იქნება ვიდეო თუ ფოტო მასალა განსაკუთრებულ შემთხვევებში შესაძლოა წაიშალოს,¹¹⁹ თუმცადა ყოველი ასეთი მატერიალი პირისთვის როგორც დეფამაცია ან ცრუ ინფორმაცია შესაძლოა ზიანის მომტანი იყოს, მიუხედავად იმისა თუ რა მასშტაბით ხდება მისი გავრცელება. სწორედ ზემოგანხილული წარმოადგენს ზიანის მომტან ერთ-ერთ კონტენტს, რომლის განხორციელებაც ნებისმიერ პირს შეუძლია, ინტერნეტის ფართო ხელმისაწვდომობის გამო, სადაც უმთავრესი მნიშვნელობა არა ცნობის გამოხატულებას, არამედ მისი გავრცელების სიმარტივეს აქვს.

მეორე და მნიშვნელოვნად გავრცელებულ შემთხვევას წარმოადგენს, ეგრეთ წოდებული ინტერნეტ საინფორმაციო სააგენტოები, რომლებიც ერთი შეხედვით ტრადიციული ბეჭდვითი გამოცემების ანალოგებს წარმოადგენენ,¹²⁰ აღნიშნულთან მიმართებაში მნიშვნელოვანია, რომ საინფორმაციო სააგენტოს ვებგვერდზე ხშირად არა ჟურნალისტები არამედ ინფორმაციის მიმწოდებლები დებენ სიახლეებს. საქმეზე *O'Grady v. Superior Court*¹²¹ და *Mortg. Specialists, Inc. v. Implode-Explode Heavy Indus.*¹²²

¹¹⁷ იქვე, 188.

¹¹⁸ მაგალითისთვის, FaceBook, YouTube მხოლოდ რეგისტრაციას საჭიროებენ, რომლის შემდეგაც მომხარებელს ნებისმიერი კონტენტის განთავსება შეუძლია საიტზე, წინასწარი მოდერაციის გარეშე. ასევე, არსებობს საიტები მაგალითად Tumblr.com და WordPress.com, სადაც ინტერნეტ მომხარებელს შეუძლია საკუთარი ქვე-დომენი დაარეგისტროს და ჰქონდეს დამოუკიდებელი ბლოგი.

¹¹⁹ მაგალითად YouTube-ის პოლიტიკა საკითხთან მიმართებაში იხ. ბმულზე <https://www.youtube.com/intl/en-GB/yt/about/policies/> (ვიზიტის დრო: 24.06.2019)

¹²⁰ *Guicheteau L.*, What Is the Media in the Age of the Internet? Defamation Law and the Blogosphere, Washington Journal of Law, Technology & Arts, Vol. 8, Issue 5, 2013, 581.

¹²¹ *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 44 Cal. Rptr. 3d 72 (Cal. App. 6 Dist. 2006), მითითებულია *Guicheteau L.*, What Is the Media in the Age of the Internet? Defamation Law and the Blogosphere, Washington Journal of Law, Technology & Arts, Vol. 8, Issue 5, 2013, 582 მიხედვით.

¹²² *Mortg. Specialists, Inc. v. Implode-Explode Heavy Indus., Inc.*, 160 N.H.227, 999 A.2d 184 (N.H. 2010). მითითებულია *Guicheteau L.*, What Is the Media in the Age of the Internet? Defamation Law and the Blogosphere, Washington Journal of Law, Technology & Arts, Vol. 8, Issue 5, 2013, 582 მიხედვით.

სასამართლომ ნათლად აღნიშნა, რომ მიუხედავად კონტენტის მიმწოდებლისა ვებგვერდები, რომლებიც იზიარებენ საინფორმაციო გამომცემლობის მახასიათებლებს, ითვლებიან საინფორმაციო სააგენტოებად. სწორედ აღნიშნულ შემთხვევაში ინფორმაციის წარმდგენელი დეფამაციურ ცნობას შესაძლოა ასეთი ვებგვერდის, ბლოგის საშუალებით ახორციელებდეს, რომელიც მედია საშუალებად არის მიჩნეული.¹²³ შესაბამისად ზიანის წყაროდ გვევლინება კომბინირებული ელემენტი, ჩვეულებრივი მომხმარებლის მიწოდებული სიახლე, რომელსაც ინტერნეტ სააგენტო ავრცელებს, როგორც საინფორმაციო სიახლეს.

1.3.2. კონსტიტუციის პირველი შესწორება, როგორც ფარი კონტენტის გამავრცელებლისთვის

ამერიკის კონსტიტუციის პირველი შესწორების მიხედვით, კონგრესმა არ უნდა მიიღოს ისეთი კანონი, რომელიც შეზღუდავს სიტყვის ან პრესის თავისუფლებას.¹²⁴ მიუხედავად ამისა უზენაესი სასამართლო საწყისი პერიოდი მაინც არ იყენებდა პირველი შესწორებით დაცული უფლებების პრივილეგიას, განსაკუთრებით მედია საშუალებებზე.¹²⁵ თუმცაღა საქმეზე *New York Times Co. v. Sullivan*¹²⁶ უზენაესმა სასამართლომ პირველი შესწორება გაავრცელა მედიის წინააღმდეგ მიმართულ სარჩელზე დეფამაციის შესახებ, რამაც საფუძველი დაუდო მთელ რიგ შეზღუდვებსა და დაცვის მექანიზმებს.

ონლაინ ბლოგინგი ნათელი მაგალითია დელიქტური ქმედებისა და პირველი შესწორების დაპირისპირებისა, სადაც ეს უკანასკნელი იმარჯვებს იმ შემთხვევაში თუ ბლოგის ავტორს გააჩნია რწმენა რომ მის მიერ გამოქვეყნებული ინფორმაცია ნეგატიური შინაარსის მიუხედავად სარწმუნოა. დეფამაციისთვის სამოქალაქო პასუხისმგებლობის დასაკისრებლად საკითხი ხშირად გავრცელებული ინფორმაციის მიზნებამდე დაიყვანება, მაგალითისთვის შემთხვევაში თუ დეფამაცია ემსახურება სიტყვის გამოხატვის ისეთ გზებს, როგორცაა პაროდია ან ხელოვნების ნიმუში, კონსტიტუციის პირველი ცვლილების დაცვის

¹²³ იქვე, 583.

¹²⁴ First Amendment to the United States Constitution, იხ. ბმულზე https://www.law.cornell.edu/constitution/first_amendment/ (ვიზიტის დრო: 24.06.2019).

¹²⁵ *Horton E. A.*, Beyond Control?: The Rise and Fall of Defamation Regulation on the Internet, *Valparaiso University Law Review*, Vol. 43, Number 3, 2009, 1290.

¹²⁶ *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), მითითებულია *Horton E. A.*, Beyond Control?: The Rise and Fall of Defamation Regulation on the Internet, *Valparaiso University Law Review*, Vol. 43, Number 3, 2009, 1291 მიხედვით.

წარმადობა უფრო მეტად იზრდება, ხოლო, ისეთ შემთხვევებში როდესაც დეფამაცია ფინანსური მდგომარეობის გაუმჯობესებას ან პირიქით, სხვა პირისთვის გაუარესებას ეხება, ასეთ შემთხვევაში დაცვის შანსები იკლებს.¹²⁷

1.3.3. კომუნიკაციურ ქსელში ეთიკურობის შესახებ კანონი და ვებგვერდების მეორადი პასუხისმგებლობა

ონლაინ დეფამაციას უკავშირდება ასევე ინტერნეტ პროვაიდერებისა და სერვისების მომწოდებლების მეორადი პასუხისმგებლობის საკითხიც. კომუნიკაციურ ქსელში ეთიკურობის შესახებ კანონის (Communications Decency Act) მიხედვით, არ შეიძლება ზემოხსენებულნი აღქმულნი იყვნენ როგორც გამომცემლები ან მედია საშუალებები, რომლებიც წინასწარ გაცნობილნი არიან დეფამაციურ მატერიალს. შესაბამისად ინტერნეტ სერვისების პროვაიდერებზე არ ვრცელდება დეფამაციისგან წარმოშობილი დელიქტური პასუხისმგებლობა.¹²⁸

2. დელიქტური ვალდებულების ახალი ინტერნეტ სახეობები

2.1. კიბერსქვათინგი

კიბერსქვათინგი, სასამართლოს მიერ, დამკვიდრებული განმარტების მიხედვით, ესაა პროცესი, როდესაც პირი ცდილობს მიიღოს ეკონომიკური სარგებელი ინტერნეტის საშუალებით, მაშინ როდესაც არეგისტრირებს ინტერნეტ დომენს ცნობილი კომპანიის სასაქონლო ნიშნის მიხედვით, რომლის ცნობადობისთვის და კეთილდღეობისთვის დახარჯულია მილიონობით დოლარი და შემდეგ ცდილობს ამავე დომენის მიყიდვას სასაქონლო ნიშნის მფლობელისთვის.¹²⁹ აღნიშნული დეფინიცია, იმისდა მიუხედავად, რომ საკმაოდ მოცულობითი და განმარტებითი ხასიათისაა, სასამართლო გადაწყვეტილების მიღების მომენტისათვისაც უკვე ნაკლები იყო. არასწორია კიბერსქვათინგის განმარტების, როგორც დელიქტური ქმედების, მხოლოდ არამართლზომიერი განზრახვით დარეგისტრირებული დომენის სასაქონლო ნიშნის მფლობელისთვის მიყიდვით შემოიფარგლოს.

¹²⁷ *Mullen M.*, The Internet and Public Policy: Cybertorts and Online Property Rights, Minnesota House Research Department, 2018, 3, იხ. ბმულზე: https://www.house.leg.state.mn.us/hrd/pubs/int_cybertort.pdf. (ვიზიტის დრო: 24.06.2019).

¹²⁸ *Miller L. R.*, Business Law Today, Standard: Text & Summarized Cases, 11th Edition, Cengage Learning, Boston 2015, 176.

¹²⁹ *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227 (US District Court for the Northern District of Illinois, 1996).

კიბერსკვათინგი ხშირად არა დომენის ან ინტერნეტ გვერდის უკან მიყიდვას ისახავს რეგისტრირებული ნიშნის მფლობელისთვის, არამედ ინტერნეტ მომხმარებლების შეცდომაში შეყვანას და მათ მიზიდვას ისეთ რესურსზე, რომელიც ხშირად სასაქონლო ნიშნის მფლობელის რეპუტაციას უქმნის საფრთხეს, ავრცელებს მის მიმართ დამამცირებელ ცნობებს ან გამოიჩინებს ირონიული მატერიალით.¹³⁰ უფრო ზოგადად კი კიბერსკვათინგის მიზანს წარმოადგენს სახელით¹³¹ დაგროვებული სიკეთის ხელყოფა, ამავე სახელის დომენად არამარლზომიერი გამოყენებისას.¹³²

კიბერსკვათინგი, ფართოდ და მნიშვნელოვნად, კალიფორნიის ცენტრალური ოლქის საოლქო სასამართლოს მიერ იქნა დამკვიდრებული, 1998 წელს. საქმის გადაწყვეტილებაში მოსამართლემ მოპასუხე მხარეს პირდაპირ უწოდა კიბერსკვათინგები, გამომდინარე იქიდან რომ მათ 12 000-ზე მეტი დომენური სახელწოდება ჰქონდათ დაკავებული, არა პირადი მიზნებისთვის, არამედ იმისთვის რომ სხვებისთვის შეეშალათ ხელი ესარგებლად სადავო დომენებით.¹³³ აღნიშნულ საქმეში ნათლად გამოჩნდა თუ რა მასშტაბის შესაძლოა იყოს კიბერსკვათინგი.

2.1.1. მიდგომა ინტელექტუალური საკუთრებისადმი და მომხმარებელთა დაცვის კანონი ანტი-კიბერსკვათინგის შესახებ.

მომხმარებელთა დაცვის კანონი ანტი-კიბერსკვათინგის შესახებ (Anticybersquatting Consumer Protection Act, ACPA),¹³⁴ 1999 წელს იქნა მიღებული შეერთებული შტატების კონგრესის მიერ. მისი მთავარი მიზანია მომხმარებლები და ბიზნესი დაიცვას კიბერსკვათინგის შემთხვევებისგან და აღკვეთოს იგი, ასევე, ხელი შეუწყოს ელექტრონული კომერციის

¹³⁰ Curtin J. T., The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites, Journal of Law and Policy Vol. 19, Issue 1, 2010, 354-359.

¹³¹ კიბერსკვათინგისთვის სავალდებულო არ არის რეგისტრირებული სასაქონლო ნიშნის არსებობა. კიბერსკვათინგი ხორციელდება მაშინაც როდესაც სკვათერი პირის პროფესიულ სახელწოდებას ან სახელს იყენებს. მაგალითად იხ. Madonna Ciccone, p/k/a Madonna v. Dan Parisi and "Madonna.com" Case No. D2000-0847

¹³² *Barbantonis F. N.*, Should Contributory Cybersquatting be Actionable?, North Carolina Journal of Law & Technology, Vol. 17, Issue 1, 2015, 85.

¹³³ AVERY DENNISON CORPORATION v. Jerry SUMPTON, No. CV 97-407 JSL. United States District Court, C.D. California

¹³⁴ Anticybersquatting Consumer Protection Act, (15 U.S.C. § 1125(d)). იხ. ბმულზე <https://www.congress.gov/bill/106th-congress/senate-bill/1255/text/is>; <https://www.govtrack.us/congress/bills/106/s1255/text>. (ვიზიტის დრო: 24.06.2019)

განვითარებას.¹³⁵ ACPA–ს მიღების კიდევ ერთი მიზეზი მისი წინამორბედის სასაქონლო ნიშანთა აღრევის შესახებ ფედერალური კანონის (Federal Trademark Dilution Act, FTDA),¹³⁶ წარუმატებლობა გამოდგა, როგორც სასარჩელო მოთხოვნის სამართლებრივი საფუძველი, გამომდინარე იქიდან, რომ მისი დაცვის სფერო იმდენად ვიწრო და სასაქონლო ნიშნისთვის ტრადიციული იყო, დომენების მფლობელთა დიდი ნაწილი დაცვის გარეშე რჩებოდა, უფრო კონკრეტულად კი კანონი ითხოვდა ნიშანი ყოფილიყო, როგორც ცნობილი, ასევე, განმასხვავებელუნარიანი კუმულატიურად.¹³⁷

ზემოხსენებულთან მიმართებაში გასაზიარებელია მოსაზრება,¹³⁸ რომლის მიხედვითაც სასაქონლო ნიშნების საკანონმდებლო დამცავი მექანიზმები არ გამოდგება შემთხვევაში, როდესაც დავა დომენს ეხება. მოსაზრების თანახმად სასაქონლო ნიშნის მფლობელს მასზე გააჩნია კვაზი–საკუთრებასთან დაკავშირებული უფლებები, რაც მოაზრებული უნდა იქნეს ისე, რომ სასაქონლო ნიშანი, რომელიც დატანებულია პროდუქტზე წარმოადგენს განცალკევებად ნიშანს უშუალოდ პროდუქტისგან, გამომდინარე აქედან სასაქონლო ნიშნის მფლობელი არ იძენს საკუთრებას უშუალოდ პროდუქტის მიმართ, არამედ ნიშანთან დაკავშირებული უფლებები ეხმარება მას გაყიდოს საკუთარი პროდუქცია.¹³⁹ შესაბამისად, სასაქონლო ნიშნებთან დაკავშირებული ნორმატიული მოწესრიგება უშუალოდ სასაქონლო ნიშნებს მიესადაგება და მხოლოდ მათი გამოყენებით, შესაძლოა ინტერნეტში დელიქტური ვალდებულება პათოლოგიურად იქნეს მოწესრიგებული, განსაკუთრებით კი მაშინ როდესაც დავა არაუშუალოდ კონტრაფაქციულ პროდუქტს ეხება, არამედ არამატერიალურ ინტერნეტ დომენსა და საიტს.

აღსანიშნავია, რომ ერთ–ერთ კიბერსქვათინგ დავაში,¹⁴⁰ სადაც მოპასუხე ცნობილი დომენების რეგისტრატორი GoDaddy.com იყო, ამერიკის შეერთებული შტატების სააპელაციო სასამართლომ Anticybersquatting Consumer Protection Act–ზე დაყრდნობით გააკეთა განმარტება, რომ

¹³⁵ *Nguyen X.*, Blame It On the Cybersquatters: How Congress Partially Ends the Circus Among the Circuits with the Anticybersquatting Consumer Protection Act, *Loyola University Chicago Law Journal*, Vol. 32, 2001, 777.

¹³⁶ Federal Trademark Dilution Act (15 U.S.C. § 1125 et seq), იხ. ბმულზე <https://www.govtrack.us/congress/bills/104/hr1295/text/enr>. (ვიზიტის დრო: 24.06.2019)

¹³⁷ *Nguyen X.*, Blame It On the Cybersquatters: How Congress Partially Ends the Circus Among the Circuits with the Anticybersquatting Consumer Protection Act, *Loyola University Chicago Law Journal*, Vol. 32, 2001, 781–782.

¹³⁸ *Mercer D. J.*, Cybersquatting: Blackmail on the Information Superhighway, *Journal of Science & Technology Law*, Vol. 6, Notes, 2000, 3–4.

¹³⁹ იქვე, 3–4.

¹⁴⁰ *Petroliam Nasional Berhad v. GoDaddy.com, Inc.*, U.S., No. 13-1255, United States Court of Appeals, Ninth Circuit.

დომენების მარეგისტრირებლებს არ ეკისრებათ მეორადი პასუხისმგებლობა მათთან დარეგისტრირებული დომენების გამო.

რაც შეეხება უშუალოდ მოთხოვნას, მოსარჩელეს შეუძლია ACPA-ს მიხედვით, მოითხოვოს მოპასუხისგან მოქმედების შესრულების აკრძალვა,¹⁴¹ ზიანის ანაზღაურება,¹⁴² ან კანონის მიერ დაწესებული ზიანის ანაზღაურება (statutory damages), რომელიც განისაზღვრება 1000–100 000 დოლარამდე თითოეული დომენისთვის, რაც თავისთავად გამორიცხავს ფაქტიურად მიყენებული ზიანის მოთხოვნის საშუალებას.¹⁴³ მიუხედავად იმისა, რომ ეს უკანასკნელი საკმაოდ მკაცრად გამოიყურება კიბერსექვათერების პასუხისმგებლობისთვის, ხშირად ფაქტიური ზიანის ანაზღაურების მოთხოვნა გაცილებით აჭარბებს კანონისმიერი ზიანის მოცულობის ფარგლებს. მაგალითად საქმეზე *Pinterest, Inc. v. Qian Jin*¹⁴⁴ კიბერსექვათერ მოპასუხეს დაეკისრა 7.2 მილიონის ანაზღაურება მოპასუხის სასარგებლოდ.

2.1.2. დომენური დავების გადაწყვეტის ერთიანი პოლიტიკა (UDRP)

კიბერსექვათინგისთვის მნიშვნელოვან მოვლენას წარმოადგენს დომენური დავების გადაწყვეტის ერთიანი პოლიტიკის არსებობა (Uniform Domain Name Dispute Resolution Policy), რომელიც 1999 წელს ინტერნეტ კორპორაცია მინიჭებულ სახელებსა და რიცხვებზე და ინტერნეტში დომენების განაწილების მაკონტროლებელი საერთაშორისო ორგანიზაციის (ICANN) მიერ იქნა შემუშავებული.¹⁴⁵

აღნიშნული პოლიტიკა წარმოადგენს არასასამართლო პროცესს, რომელიც ამ უკანასკნელზე სწრაფი და ეკონომიურია. ასევე, მნიშვნელოვან გარემოებას წარმოადგენს ის ფაქტი რომ UDRP-ს დავის განხილვაში არბიტრის როლს ასრულებს უშუალოდ ექსპერტი, რაც სასამართლოს შემთხვევაში შესაძლოა საერთოდ გამორიცხული იყოს, გამომდინარე იქიდან რომ მოსამართლეს არ გააჩნდეს შესაბამისი საექსპერტო ცოდნა და განათლება.¹⁴⁶ აღსანიშნავია, რომ

¹⁴¹ Anticybersquatting Consumer Protection Act, (15 U.S.C. § 1125(d)). Section 3(a)(1).

¹⁴² იქვე, Section 3(a)(2).

¹⁴³ იქვე, Section 3(b)(d).

¹⁴⁴ *Pinterest, Inc. v. Qian Jin*, No. C 12-04586 RS (N.D. Cal. Sep. 30, 2013)

¹⁴⁵ *Schulte J. C.*, The New Anticybersquatting Law and uniform Dispute Resolution Policy for Domain Names, *Tort & Insurance Law Journal*, Vol. 36, 2000, 107.

¹⁴⁶ *Singh H.*, Domain Name Disputes and Their Resolution under UDRP Route: A Review, *Archives of Business Research*, Vol. 6, No.12, 2018, 150,

ICANN-მა დავის გადაწყვეტის პირველ პროვაიდერად უფლებამოსილება ინტელექტუალური საკუთრების მსოფლიო ორგანიზაციას მიანიჭა (WIPO).¹⁴⁷

ამრიგად UDRP მისი არსებობის დღიდან უნიკალურ მოვლენად იქცა არამხოლოდ დომენური დავების გადაწყვეტისთვის, არამედ როგორც მოვლენა, საერთაშორისო დავის გადაწყვეტის მექანიზმი.¹⁴⁸ UDRP-სთან მიმართვიანობა ყოველ წელს უფრო მეტად და მეტად მატულობს, წინააღმდეგარე ნაშრომის წერის პროცესისთვის კი WIPO-ში ერთობლივად 44 000-ზე მეტი საქმეა მიღებული დომენურ დავებთან დაკავშირებით.¹⁴⁹

2.2. ინტერნეტ მეკობრეობა და საავტორო უფლებები

მართებულად უნდა მივიჩნიოთ, რომ ინტერნეტ მეკობრეობის დროს საქმე ძირითადად საავტორო უფლებების დარღვევასთან გვაქვს და შესაბამისად ყოველი ასეთი დავა უნდა გადაწყდეს საავტორო უფლებებთან დაკავშირებული ნორმატიული აქტების შესაბამისად. მიუხედავად ამისა, იურიდიულ ლიტერატურაში არსებობს მოსაზრება, რომ ინტერნეტ მეკობრეობის დროსაც კი ინტერნეტ სამართალი გამოსაყენებლად „ყვავის“,¹⁵⁰ შესაბამისად იგი ირიბად მაგრამ მაინც მოაზრებული შეიძლება იყოს ინტერნეტ დელიქტად. დელიქტის მახასიათებელი თითქმის ყოველთვის საავტორო უფლებით დაცული მატერიალის ინტერნეტში განთავსებაა შესაბამისი უფლების გარეშე, რასაც გაცილებით დიდი ეკონომიკური ზიანი მოყვება, ვიდრე ტრადიციულად მატერიალის რეალურ სამყაროში გავრცელებით. უფრო მეტად მართებულაა განვიხილოთ არა უშუალოდ სტანდარტული შემთხვევები, არამედ თანმდევი პრობლემური საკითხები.

2.2.1. კანონი საავტორო უფლებების შესახებ ციფრულ ეპოქაში და მართლზომიერი გამოყენების პრობლემური ურთიერთმიმართება

მართლზომიერი გამოყენება (Fair Use) მნიშვნელოვან დოქტრინას წარმოადგენდა საავტორო უფლებების დიგიტალიზაციამდეც. მისი მიხედვით საზოგადოებისთვის ხელმისაწვდომი და გამოყენებადი უნდა იყოს საავტორო უფლებებით დაცული მატერიალი ისეთი მიზნებისთვის

¹⁴⁷ *Helper R. L./ Dinwoodie B. G.*, Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy, *William & Mary Law Review*, Vol. 43, 2001, 186.

¹⁴⁸ იქვე, 187.

¹⁴⁹ სტატისტიკა წლების მიხედვით იხ. ბმულზე <https://www.wipo.int/amc/en/domains/statistics/cases.jsp> (ვიზიტის დრო: 24.06.2019).

¹⁵⁰ *Rustad L. M/ Koenig H. T.*, Rebooting Cybertort Law, *Washington Law Review*, Vol. 80, 2005, 346-347,

როგორცაა, კრიტიკა, კომენტირება, რეპორტაჟი, სწავლება, განათლება და კვლევა, ყოველგვარი პასუხისმგებლობის გარეშე.¹⁵¹ დოქტრინის მნიშვნელობიდან გამომდინარე იგი, ასევე, კოდიფიცირებულია.¹⁵² რაც შეეხება კანონს საავტორო უფლებების შესახებ ციფრულ ეპოქაში (Digital Millennium Copyright Act, DMCA),¹⁵³ იგი მიმართულია ტექნოლოგიური ინოვაციებიდან გამომდინარე დამატებითი მექანიზმის შექმნისკენ საავტორო უფლებების დასაცავად, თუმცა ის კონტროლერსიალურად ხასიათდება და ხშირად მოიხსენიება როგორც ინტერნეტ სივრცის გადამრჩენელი ან სრულიად საპირისპიროდ ონლაინში გამოხატვის თავისუფლების შემზღვეველი აქტი.¹⁵⁴

თავის მხრივ სენატის წარმომადგენლებმა კანონის მიღებისას ორი მნიშვნელოვანი აზრი გამოთქვეს. პირველი ეს იყო, რომ კანონისა და შესაბამისი დაცვის არარსებობის შემთხვევაში საავტორო უფლების მფლობელები ნაწარმოებს არ განათავსებდნენ ინტერნეტში.¹⁵⁵ ხოლო, მეორე, კი იყო ის რომ ჩვეულებრივი მომხმარებლები შესაძლოა არასახარბიელო სიტუაციაში აღმოჩენილიყვნენ უფლების მფლობელთა მხრიდან მექანიზმების არასწორი გამოყენების გამო.¹⁵⁶

ზემოხსენებული ორივე მოსაზრება მართებული აღმოჩნდა. ასევე, ნაწილობრივ გასაზიარებელია მოსაზრება რომ DMCA-იმ მნიშვნელოვნად შეზღუდა მართლზომიერი გამოყენების უფლება.¹⁵⁷ რაც დაკავშირებულ იქნა სიტყვისა და გამოხატვის თავისუფლების შეზღუდვასთან,¹⁵⁸ გამომდინარე იქიდან რომ DMCA-ის მიერ დადგენილი შეტყობინებისა და წაშლის პროცესის განხორციელებისას, რომლის დროსაც საავტორო უფლების მფლობელის შეტყობინების შემდეგ საიტი ვალდებულია წაშალოს

¹⁵¹ *Calandrillo P. S./ Davison M. E.*, The Dangers of the Digital Millennium Copyright Act: Much ado About Nothing?, *William & Mary Law Review*, Vol. 50, Issue 2, 2008, 364.

¹⁵² 17 U.S. Code, § 107. იხ. ბმულზე <https://www.law.cornell.edu/uscode/text/17/107> (ვიზიტის დრო: 24.06.2019).

¹⁵³ 17 U.S.C. § 512, § 1201–1205, § 1301–1332; 28 U.S.C. § 4001. იხ. ბმულზე <https://www.law.cornell.edu/uscode/text/17/512>; <https://www.law.cornell.edu/uscode/text/17/chapter-12>. (ვიზიტის დრო: 24.06.2019).

¹⁵⁴ *Asp M. E.*, Section 512 of the Digital Millennium Copyright Act: User Experience and User Frustration, *Iowa Law Review*, Edition 103, Issue 2, 2018, 752.

¹⁵⁵ 44 CONG.REC. 9234 (1998) (statement of Sen. Hatch). მითითებულია *Asp M. E.*, Section 512 of the Digital Millennium Copyright Act: User Experience and User Frustration, *Iowa Law Review*, Edition 103, Issue 2, 2018, 760.

¹⁵⁶ იქვე, 761.

¹⁵⁷ *Loos J. T.*, Fair Use and the Digital Millennium Copyright Act, *Michigan Telecommunications and Technology Law Review*, Vol. 13, Issue 2, 2007, 603.

¹⁵⁸ *Asp M. E.*, Section 512 of the Digital Millennium Copyright Act: User Experience and User Frustration, *Iowa Law Review*, Edition 103, Issue 2, 2018, 753.

მითითებული მატერიალი.¹⁵⁹ თუმცა პროცესის ფარგლებში საიტის ადმინისტრაციის მიერ შეუძლებელია იმაზე მსჯელობა მომხმარებლის მიერ ატვირთული კონტენტი მართლზომიერია თუ არა, აღნიშნული საკითხი მნიშვნელოვნად პრობლემურად რჩება დღემდე, რადგანაც არ არსებობს დამატებით მაკონტროლებელი რეგულაცია შეტყობინებისა და წაშლის სისტემებისთვის რაც მის არაკეთილსინდისიერი გამოყენების პრობლემას გადაჭრიდა.¹⁶⁰

2.2.2. უსაფრთხო ნავსადგომის წესი.

DMCA-ის ერთ-ერთ უდიდეს დამსახურებად ითვლება, უსაფრთხო ნავსადგომების (safe harbor) შექმნა ინტერნეტ სერვისის პროვაიდერებისთვის და საიტებისთვის. შეერთებული შტატების კოდექსის მე-17 თავის 512-ე მუხლი ოთხ სხვადასხვა წინაპირობას იძლევა იმისთვის რომ ზემოხსენებულ სუბიექტებს მათი მომხმარებლის გამო არ დაეკისროთ პასუხისმგებლობა საავტორო უფლების ინტერნეტში დარღვევისთვის. თუმცა ყველაზე მეტად კონტროლერსიალურად ითვლება უსაფრთხო ნავსადგომის წესი, რომელიც სერვისის პროვაიდერებს იცავს მაშინაც კი როდესაც უფლების დამრღვევი მატერიალი მათ სერვერებზე ან ქსელში ინახება.¹⁶¹ ასეთ შემთხვევაში სერვისის პროვაიდერს პასუხისმგებლობა არ დაეკისრება მაშინ, თუ ის არ ფლობს ინფორმაციას უფლებების დამრღვევი მატერიალის შესახებ.¹⁶² არ იღებს პირდაპირ ეკონომიკურ მოგებას მატერიალიდან და პირდაპირ აკონტროლებს ამ პროცესს¹⁶³ და ბოლოს, სერვისის მიმწოდებელი უფლების დამრღვევი მატერიალის შეტყობისთანავე შლის მას ან ზღუდავს წვდომას მასზე.¹⁶⁴ ეს უკანასკნელი კი ზემოხსენებულ შეტყობინებისა და წაშლის რეჟიმთანაა დაკავშირებული.

გამომდინარე იქიდან, რომ ინტერნეტში საავტორო უფლების დარღვევა, როგორც ინტერნეტ დელიქტი სწორედ ჩვეულებრივი მომხმარებლის მიერ

¹⁵⁹ *Matthew S.*, Internet Safe Harbors and the Transformation of Copyright Law, *Notre Dame Law Review*, Vol. 93, Issue 2, 2018, 503-504.

¹⁶⁰ მაგალითისთვის YouTube-ზე შეტყობინებისა და წაშლის რეჟიმის პროცესის განხორციელების შემდეგ მითითებული მატერიალი საიტიდან უპირობოდ წაიშლება თუნდაც ის სამართლიანი გამოყენების მოქმედების ფარგლებში ექცეოდეს. საიტი უბრალოდ მიუთითებს რომ უფლების მფლობელმა უნდა გაითვალისწინოს სამართლიანი გამოყენების დოქტრინა, თუმცა რაიმე მბოჭავი ვალდებულება ამისთვის მას არ აქვს. დამატებით იხ. <https://support.google.com/youtube/answer/2807622> (ვიზიტის დრო: 24.06.2019).

¹⁶¹ *Matthew S.*, Internet Safe Harbors and the Transformation of Copyright Law, *Notre Dame Law Review*, Vol. 93, Issue 2, 2018, 511.

¹⁶² 17 U.S.C. § 512(c)(A).

¹⁶³ იქვე, § 512(c)(1)(B).

¹⁶⁴ იქვე, § 512(c)(1)(C).

არის განხორციელებული სხვადასხვა საიტზე, ეს უკანასკნელი უსაფრთხო ნავსადგომის წესის დასაკმაყოფილებლად ქმნიან წინასწარ დანიშნულ აგენტს,¹⁶⁵ რომელიც თავის მხრივ ზრუნავს შეტყობინებისა და წაშლის რეჟიმის უზრუნველყოფაზე. აღნიშნულთან დაკავშირებით მნიშვნელოვან პრაქტიკას წარმოადგენს YouTube-ს წინააღმდეგ დავა, როდესაც 2007 წელს Viacom International-მა 1 მილიარდიანი (აშშ დოლარი) მოთხოვნა წააყენა მის წინააღმდეგ ინტერნეტში საავტორო უფლებების დარღვევებთან დაკავშირებით. გამომდინარე იქიდან რომ იმ დროს YouTube არ სარგებლობა DMCA-ით რეგულირებული წესებით და მას არ გააჩნდა ამავე აქტით განსაზღვრული აგენტი, რომელიც იზრუნებდა შეტყობინების შემთხვევაში საავტორო უფლების გარეშე ატვირთული კონტენტის წაშლაზე.¹⁶⁶ თუმცა დავა მორიგებით დასრულდა, სწორედ მის შემდეგ დაიწყო საიტებმა წინასწარ დანიშნული აგენტების პოლიტიკაზე მუშაობა.

IV. ინტერნეტ დელიქტების რეგულატორული მოწესრიგება ევროპის კავშირში

ამერიკის შეერთებული შტატებისგან განსხვავებით ევროპის კავშირის სამართალზე საუბრისას შეუძლებელია კონკრეტული წევრი ქვეყნის სამართლის განხილვა ისეთ ტექნიკურად და სამართლებრივად ახალ საკითხზე, როგორცაა ინტერნეტ დელიქტი და ზოგადად ინტერნეტ სივრცეში მიყენებული ზიანი. სწორედ ამიტომ მართებულია განხილულ იქნეს ევროპის კავშირის რეგულატორული მოწესრიგება და მართლმსაჯულების ევროპული სასამართლოს (CJEU) მნიშვნელოვანი პრაქტიკა აღნიშნულ საკითხთან მიმართებით.

ინტერნეტის უსაზღვრო ბუნებიდან გამომდინარე ხშირია შემთხვევა როდესაც ინტერნეტში განხორციელებული დელიქტური ქმედება რამდენიმე ქვეყანას მოიცავს, შესაბამისად კი მასზე შესაძლოა სხვადასხვა ქვეყნის სამართლის სისტემა გავრცელდეს,¹⁶⁷ სწორედ ასეთი შემთხვევებით ხასიათდება ინტერნეტ დელიქტები ევროპის კავშირში, რაც თავისთავად წინ წევს განსჯადობისა და გამოსაყენებელი სამართლის პრობლემატიკას.

ზემოხსენებულის მიუხედავად ევროპის კავშირის საერთაშორისო კერძო სამართლისთვის ცალკეულად ინტერნეტში წარმოშობილი ზიანისთვის სპეციალური მოწესრიგება არასდროს არ ყოფილა რეგულირებული,

¹⁶⁵ იქვე, § 512(c)(2).

¹⁶⁶ Viacom International, Inc. v. YouTube, Inc., No. 07 Civ. 2103, U.S. District Court for the Southern District of New York

¹⁶⁷ *Mierina A.*, Some reflections on non-contractual obligations in cyberspace considering the Rome II regulation, SHS Web of Conferences Vol. 10. Article 00023, 2014, 1,

შესაბამისად არ არსებობს მკაფიოდ განსაზღვრული გამიჯვნა ინტერნეტსა და რეალურ სამყაროს ზიანზე გასავრცელებელ ნორმებს შორის.¹⁶⁸ გამომდინარე აქედან ორივე შემთხვევაზე ვრცელდება ერთი და იგივე მოწესრიგება, კონკრეტულად კი განსჯადობისთვის რეგულაცია ბრიუსელი I,¹⁶⁹ ხოლო, გამოსაყენებელი სამართლისთვის კი რეგულაცია რომი II.¹⁷⁰ ასევე, მნიშვნელოვანია რომ ხსენებული რეგულაციები მაქსიმალურად შეესაბამება ერთმანეთს და არცერთი მანთვანი არ შეიცავს კოლიზიურ ნორმებს, რომელიც მიესადაგება ინტერნეტში განხორციელებულ ქმედებებს.¹⁷¹

1. ინტერნეტ დელიქტების განსჯადობის საკითხი რეგულაცია ბრიუსელი I მიხედვით.

რეგულაცია ბრიუსელი I მოიცავს განსჯადობის ორ წესს, ზოგადსა და სპეციალურს.

ზოგადი წესის თანახმად მოსარჩელემ მოპასუხის წინააღმდეგ სარჩელი უნდა აღძრას იმ ქვეყანაში სადაც მოპასუხე წარმოადგენს რეზიდენტ პირს, იმისდა მიუხედავად თუ რომელი ქვეყნის მოქალაქეა იგი.¹⁷² შესაბამისად არც მოსარჩელის მოქალაქეობას აქვს მნიშვნელობა. გამომდინარე აქედან რეზიდენტ პირებზე იგივე რეჟიმი ვრცელდება რაც წევრი ქვეყნის მოქალაქე პირებზე.¹⁷³

სპეციალური წესის თანახმად, მოსარჩელეს შეუძლია სარჩელის წარდგენა მაშინ როდესაც საქმე გვაქვს დელიქტთან ან კვაზი–დელიქტთან იმ ადგილის მიხედვით სადაც ზიანის მომტანი ქმედება განხორციელდა ან შეიძლება

¹⁶⁸ *Lutzi T.*, Internet Cases in EU Private International Law Developing a Coherent Approach, *International & Comparative Law Quarterly*, Vol. 66, Issue, 2017, 688.

¹⁶⁹ Brussels I, Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, რომელმაც 2015 წელს Council Regulation (EC) No 44/2001 ჩაანაცვლა. იხ. ბმულზე <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001R0044>.

¹⁷⁰ Rome II, Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations. იხ. ბმულზე <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32007R0864>.

¹⁷¹ *Mierina A.*, Some reflections on non-contractual obligations in cyberspace considering the Rome II regulation, *SHS Web of Conferences* Vol. 10. Article 00023, 2014, 4.

¹⁷² Regulation (EU) No 1215/2012, Article 4; ანალოგიურად ძველი რეგულაციისა Regulation (EC) No 44/2001, Article 2.

¹⁷³ *Savin A.*, Jurisdiction Over Cybertorts in the EU—A Coherent Picture?, *Liber amicorum: Gašo Knežević, ed. Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016, 214.

განხორციელდეს (აქვე აღსანიშნავია რომ მოცემული მუხლი დელიქტისთვის იყენებს ტერმინებს, როგორც tort, ასევე, delict).¹⁷⁴

მიუხედავად იმისა, რომ სპეციალური განსჯადობის ნორმატიული საფუძვლის ტექსტი ნათლად აღსაქმელია, პრობლემას წარმოადგენს ზიანის მომტანი კაუზალური ქმედებისა და ზიანის წარმოქმნის ადგილის აცდენა. უფრო კონკრეტულად კი ზიანის მომტან ქმედებას შესაძლოა ზიანი მოჰყვეს ყოველ იმ ადგილას სადაც ზიანის მომტანი რესურსი ინტერნეტის საშუალებით ხელისაწვდომია.¹⁷⁵ აღნიშნულიდან გამომდინარე კი სპეციალური წესი იმდენად ფართო ექსტერიტორიულობის იქნებოდა, საბოლოო ჯამში დავის განსჯადი ქვეყნის არჩევა ყოველგვარ გონივრულობას გასცდებოდა. გამომდინარე აქედან პრობლემის გადასაჭრელად აუცილებლად უდნა დაისვას კითხვა, საკმარისია მხოლოდ რესურსის ხელმისაწვდომობა წევრ ქვეყანაში თუ საჭიროა უფრო მეტად ახლო კავშირის დადგენა წევრი ქვეყნის განსჯადობისთვის.¹⁷⁶

პრობლემის გადასაჭრელად, განსაკუთრებით კი მაშინ როცა საქმე ონლაინ დეფამაციას ეხება, გამოიყენება ევროპული კავშირის მართლმსაჯულების სასამართლოს მიერ დამკვიდრებული შევილის დოქტრინა (Shevill doctrine),¹⁷⁷ მიუხედავად იმისა რომ საქმე, რომელსაც დოქტრინა ეყრდნობა ინტერნეტის განვითარების პირველ ეტაპებზე იქნა მიღებული და არ მსჯელობს უშუალოდ ინტერნეტში მიყენებულ ზიანზე, იგი სპეციალური განსჯადობის განმარტების მთავარ საშუალებად არის გამოყენებული სასამართლოების მიერ.¹⁷⁸

1.1. შევილის დოქტრინა (საქმე C-68/93)

შევილის საქმე შეეხებოდა არამატერიალურ ზიანს, რომელიც გამოწვეული იყო ერთ–ერთი ბეჭდური გამოცემის მიერ გავრცელებული დეფამატორული ცნონების შედეგად. აღნიშნული გამოცემა თავისუფალ მიმოქცევაში იყო ევროპის კავშირის რამდენიმე წევრი ქვეყნის მასშტაბით. მოსარჩელემ, რომელიც ბრიტანეთის მოქალაქე იყო და ცხოვრობდა ინგლისში, მოთხოვნა

¹⁷⁴ Regulation (EU) No 1215/2012, Article 7(2); ანალოგიურად ძველი რეგულაციის Regulation (EC) No 44/2001, Article 5(3)

¹⁷⁵ *Lutzi T.*, Internet Cases in EU Private International Law Developing a Coherent Approach, *International & Comparative Law Quarterly*, Vol. 66, Issue, 2017, 690–691.

¹⁷⁶ *Joubert N.*, Cyber-Torts and Personal Jurisdiction: The Paris Court of Appeal Makes a Stand, *The International and Comparative Law Quarterly*, Vol. 58, No. 2, 2009, 477.

¹⁷⁷ C-68/93 *Shevill and Others v Presse Alliance* ECLI:EU:C:1995:61 (1995).

¹⁷⁸ *Savin A.*, Jurisdiction Over Cybertorts in the EU—A Coherent Picture?, *Liber amicorum: Gašo Knežević*, ed. *Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016, 217.

ინგლისის უმაღლესი სასამართლოს წინაშე წარადგინა, იურიდიული პირის მიმართ, რომელიც ოპერირებდა ფრანგული სამართლის ქვეშ და რეგისტრირებული მისამართი გააჩნდა პარიზში. მოპასუხემ განახორციელა შედაგება განსჯადობასთან დაკავშირებით და მიუთითა, რომ მის მიხედვით სახეზე არ იყო ინგლისში მიყენებული ზიანი. სასამართლომ ამასთან დაკავშირებით კი ზიანის მიყენების ადგილზე განმარტა, რომ მოცემული შემთხვევისთვის ზიანი დგებოდა ყველა იმ ადგილას სადაც გაზეთი ბრუნვაში იყო გაშვებული, ერთ–ერთი ასეთი ქვეყანა კი სწორედ ინგლისი იყო, გამომდინარე აქედან მოსარჩელეს ეძლეოდა საშუალება თავადვე ამოერჩია დანაწევრებული ადგილმდებარეობის მიხედვით თუ რომელი სასამართლოსთვის უნდა მიემართა. თუმცა სასამართლომ ზიანის მოთხოვნა შეზღუდა განსჯადობის მიხედვით. კონკრეტულად კი მოსარჩელეს სრული ზიანი მხოლოდ მოპასუხის ტერიტორიულობის მიხედვით შეეძლო მოეთხოვა, ხოლო წევრ სახელმწიფოებში კი მხოლოდ ის ზიანი მოეთხოვა, რაც უშუალოდ მათ ტერიტორიაზე დადგა.¹⁷⁹ სწორედ აღნიშნულის შემდეგ დამკვიდრდა მოზაიკის თეორია პრაქტიკაში,¹⁸⁰ ხოლო, ინტერნეტში ზიანის მიყენების შემთხვევები მოაზრებულ იქნა, როგორ მრავალ–სახელმწიფოიანი დელიქტები.¹⁸¹

ზემოგანხილული პრაქტიკაცა და მოზაიკის თეორიაც, მიესადაგება სპეციალურ განსჯადობას, რომელიც თავის მხრივ ზოგადი წესისგან გადახვევაა, ეს უკანასკნელი წარმოადგენს ძალთა თანაფარდობის ბერკეტს მოსარჩელესა და მოპასუხეს შორის, გამომდინარე იქიდან რომ რადგანაც მოსარჩელეს აქვს საშუალება ამოირჩიოს საქმის განმხილველი სასამართლო, მოპასუხეს უნდა ჰქონდეს გონივრული შესაძლებლობა რომ მოემზადოს მისთვის დაყენებულ მოთხოვნაზე საპასუხოდ,¹⁸² თუმცა ზოგადი წესიდან გადახვევა შესაძლებელია მხოლოდ მკაცრად საგამონაკლისო და განჭვრეტად შემთხვევებში.¹⁸³

მოზაიკის თეორიაც ერთი შეხედვით საგამონაკლისო გადახვევას წარმოადგენს და სპეციალური განსჯადობის ნორმატიულ საფუძველს მიესადაგება, თუმცა იგი კრიტიკის საფუძველია შემდეგი გარეობების გამო. მოსარჩელისთვის არასდროს არ არის შესაძლებელია სრული ზიანი

¹⁷⁹ *Oster J.*, Rethinking Shevill. Conceptualising the EU private international law of Internet torts against personality rights, *International Review of Law, Computers & Technology*, 6:2-3, 115.

¹⁸⁰ იქვე.

¹⁸¹ *Savin A.*, Jurisdiction Over Cybertorts in the EU—A Coherent Picture?, *Liber amicorum: Gašo Knežević*, ed. *Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016, 217.

¹⁸² *Šrámek M.*, Brussels I: Recent Developments in the Interpretation of Special Jurisdiction Provisions for Internet Torts, *Masaryk University Journal of Law and Technology*, Vol. 9, 2015, 167.

¹⁸³ იქვე.

მოითხოვოს იმ ქვეყნის სასამართლოს წინაშე, რომელშიც დადგა ზიანი, გარდა იმ სასამართლოსი სადაც მოპასუხე რეზიდენტია.¹⁸⁴ ხოლო, მოპასუხისთვის კი არსებობს საშიშროება იმისა რომ მის წინააღმდეგ დავა წარმოებულ იქნეს ევროპის კავშირის ყველა წევრ სახელწიფოში, რაც მცირე მოცულობის დავასაც კი სერიოზულ ხარჯად გადააქცევს.¹⁸⁵

1.2. სპეციალური განსჯადობის ახალი სასამართლო ჭრილი

შევილის დოქტორის ჩანაცვლებად შესაძლოა მოვიაზროთ მოსარჩელის ინტერესთა ცენტრის კრიტერიუმი, განვითარებული ონლაინ დეფამაციის საქმეზე.¹⁸⁶ აღნიშნული საქმის მიხედვით სასამართლოს წინაშე დაისვა საკითხი, ბრიუსელი I რეგულაციის 7(2) მუხლის მიხედვით ალტერნატიულად ხომ არ უნდა იქნეს დადგენილი განსჯადობა ინტერნეტ დელიქტთან სპეციალურ კავშირში,¹⁸⁷ რაც გამოიწვევდა განსჯადი ქვეყნის დადგენის უფრო მეტად პროგნოზირებად ფორმულას, შესაბამისად მოიაზრება, რომ შეიძლება ინტერნეტ დელიქტების დროს, განსაკუთრებით კი დეფამაციის გამოყენებულ იქნეს მინიმალური კავშირების ტესტი, რომლის მიხედვითაც სასამართლომ საკუთარი განსჯადობის დროს ჯერ უნდა დაადგინოს მოპასუხისა და განხორციელებული დელიქტური ქმედების კავშირი სარჩელის შეტანის ადგილთან.

ინტერესთა ცენტრი ახალ საშუალებას იძლევა განსჯადობის პრობლემის გადასაჭრელად ინტერნეტ დელიქტთან მიმართებაში, რომლის მიხედვითაც მოსარჩელეს ზიანის მთლიანი მოცულობის მოთხოვნა შეუძლია იმ წევრ სახელმწიფოში სადაც კი ზიანი დადგა.¹⁸⁸ ზემოხსენებულ საქმეში სასამართლომ განმარტა რომ ინტერესთა ცენტრი მოსარჩელისთვის ძირითადად ის ადგილია სადაც ის რეზიდენტი პირია, მიუხედავად ამისა

¹⁸⁴ *Lutzi T.*, Internet Cases in EU Private International Law Developing a Coherent Approach, *International & Comparative Law Quarterly*, Vol. 66, Issue, 2017, 692.

¹⁸⁵ იქვე.

¹⁸⁶ *Joined Cases C-509/09 and C-161/10. eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited ECLI:EU:C:2011:192 (2011).*

¹⁸⁷ *Savin A.*, Jurisdiction Over Cybertorts in the EU—A Coherent Picture?, *Liber amicorum: Gašo Knežević*, ed. *Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016, 218.

¹⁸⁸ *Hartley C. T.*, Jurisdiction in tort claims for non-physical harm under Brussels 2012, Article 7(2), *Vol. 67*, 2018, 1001.

ინტერესთა ცენტრის ადგილი შესაძლოა სხვაც იყოს, მაგალითად მოსარჩელის სამსახური რომელიც სხვა წევრ სახელმწიფოში მდებარეობს.¹⁸⁹

1.3. განსხვავებული მიდგომა სასაქონლო ნიშნების მიმართ

საქმეზე Wintersteiger AG v Products 4U Sondermaschinenbau GmbH¹⁹⁰, მოსარჩელეს წარმოადგენდა კომპანია Wintersteiger–ი რომელიც აწარმოებს სათხილამურო ინვენტარს, მოპასუხე Products 4U Sondermaschinenbau, ასევე, წარმოადგენს სათხილამურო ინვენტარის მწარმოებელ კომპანიას, რომელიც მოსარჩელისთვის ამზადებდა სხვადასხვა სათხილამურო აქსესუარს. 2008 წელს მოპასუხემ გუგლის სარეკლამო დივიზიას AdWord–ს დაუკვეთა რეკლამა Wintersteiger–ის სასაქონლო ნიშნის გამოყენებით, რამაც გამოიწვია ის რომ Wintersteiger–ის პროდუქტის მოძებნისას გუგლის გერმანულ საიტზე, ორიგინალურ პროდუქტთან ერთად ყოველითვის იძებნებოდა Products 4U–ის პროდუქტიც. იმისდა მიუხედავად რომ მოთხოვნა ავსტრიის სასამართლოების წინაშე იქნა წარდგენილი საბოლოო გადაწყვეტილება ევროპული კავშირის მართლმსაჯულების სასამართლოს მიერ იქნა მიღებული, რომლის მიხედვითაც საბოლოო ჯამში უნდა ითქვას, რომ სასაქონლო ნიშნებთან დაკავშირებული ინტერნეტ დელიქტის დროს განსჯადობა უნდა გამოირკვეს ან სასაქონლო ნიშნის რეგისტრაციის ადგილის მიხედვით ან რეკლამის დამკვეთის ადგილსამყოფელის მიხედვით.¹⁹¹

ამრიგად ჩვენ მიერ განხილულ შემთხვევებში ნათელია ინტერესთა ცენტრის მიდგომა მოსარჩელეს უხსნის პრობლემას სრული ზიანის მოთხოვნისთვის, თუმცა იგი უფრო მეტად პრობლემური ხდება მოსარჩელისთვის, ფაქტიურად მისთვის ყოვლად განუჭვრეტელი რჩება ინტერესთა ცენტრის მიხედვით თუ რომელი წევრი სახელმწიფოს სასამართლო განიხილავს დავას. ამრიგად შევილის დოქტრინაც და ინტერესთა კონფლიქტის მიდგომაც ბოლომდე არ მიესადაგება ინტერნეტ დელიქტს, კონკრეტულად კი ონლაინ დეფამაციას. ასევე, მნიშვნელოვანია, რომ ორივე შემთხვევაში შესაძლო ფორუმ შოპინგის პრობლემა გადაწყვეტილი არ არის.

¹⁸⁹ Joined Cases C-509/09 and C-161/10, Paragraph 52 of the judgment, მიითითებულია *Hartley C. T.*, Jurisdiction in tort claims for non-physical harm under Brussels 2012, *International and Comparative Law Quarterly*, Vol. 67, 2018, 1001, მიხედვით.

¹⁹⁰ Case C-523/10 Wintersteiger AG v Products 4U Sondermaschinenbau GmbH ECLI:EU:C:2012:220 (2012).

¹⁹¹ *Savin A.*, Jurisdiction Over Cybertorts in the EU–A Coherent Picture?, *Liber amicorum: Gašo Knežević*, ed. *Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016, 221-223.

1.4. ინტერნეტ დელიქტის თანმდევი ფორუმ შოპინგი

ინტერნეტის უსაზღვრო ბუნებიდან გამომდინარე, ვირტუალურ სამყაროში განხორციელებული დელიქტი შესაძლოა მოცული იყოს რამდენიმე ქვეყნის ფარგლებით, რაც განსაკუთრებით წინ წევს ეგრედ წოდებული ფორუმ შოპინგის საკითხს ინტერნეტ დელიქტებისთვის.¹⁹² თავისთავად მოსარჩელე ყოველთვის ეცდება მისთვის სასურველი სასამართლო ამოარჩიოს იმ ქვეყნის მიხედვით, რომელშიც მისი მოთხოვნის დაკმაყოფილებას ყველაზე მეტი ალბათობა ექნება. შვეილის დოქტრინისა და ინტერესთა ცენტრის მიხედვით მოსარჩელეს ევროპის კავშირის ყველა წევრ ქვეყანაში აქვს შესაძლებლობა მოითხოვოს ზიანი, რაღა თქმა უნდა ისეთი საგამონაკლისო შემთხვევებისა, სადაც ზიანი არ დამდგარა ან ინტერნეტის საშუალებით ზიანის მომტანი მატერიალი არ არის ხელმისაწვდომი.

აღნიშნული პრობლემა CJEU–ს მიერ გადაუჭრელი და პასუხგაუცემელია შვეილის მოდიფიცირებული ვერსიისთვისაც კი, რომელსაც თითქოსდა უნდა ამოეწურა პრობლემა.¹⁹³ თუმცაღა მოხდა პირიქით, შეცვლილი შვეილის დოქტრინა უფრო მეტად აფართოვდა ფორუმ შოპინგის შესაძლებლობას ინტელექტუალური საკუთრებისთვის იმ დონემდე, რომ საკმარისი ხდებოდა მხოლოდ ზიანის მომტანი მატერიალი პოტენციურად მაინც ხელმისაწვდომი ყოფილიყო წევრ ქვეყანაში, საქმე ამ ქვეყნის განსჯადობასაც დაექვემდებარებოდა. აღნიშნულთან დაკავშირებით გამოთქმული მოსაზრება რომ ასეთი მოცემულობა ხელს შეუწყობდა ფორუმ შოპინგის კიდევ უფრო ფართოდ დამკვიდრებას სასამართლოს მიერ არ იქნა გათვალისწინებული.¹⁹⁴

პრობლემის გადაჭრა ევროპის კავშირის საერთაშორისო კერძო სამართლის დამატებითი ნორმატიული მოწესრიგებით ფაქტიურად შეუძლებელია, რადგანაც შემუშავებული უნდა იქნეს ინტერნეტ სამართლისთვის ცალკეული განსჯადობის ნორმები, რაც უაღრესად რთულია ისეთი მოვლენისთვის, როგორც ინტერნეტში წარმოშობილი ურთიერთობებია. რაც თავისთავად პრობლემის გადასაჭრელად ერთადერთ გზას ტოვებს, დამკვიდრდეს ისეთი სასამართლო ინტერპრეტაცია სპეციალური განსჯადობისთვის, რომლის

¹⁹² *Smith G.*, *Internet Law and Regulation*, Sweet & Maxwell, 2007, 459.

¹⁹³ *Husovec M.*, Comment on “Pinckney”, *International Review of Intellectual Property and Competition Law*, 45(3), 2014, 372.

¹⁹⁴ *Savin A.*, *Jurisdiction Over Cybertorts in the EU—A Coherent Picture?*, *Liber amicorum: Gašo Knežević, ed. Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016, 224–225.

მიხედვითაც მოდავე მხარეების საპროცესო ბალანსი მაქსიმალურად თანაბარი იქნება.

2. გამოსაყენებელი სამართალი

გამოსაყენებელი სამართლის დასადგენად, ანუ იმ ნორმებისა თუ რომელი უნდა იყოს სახელმძღვანელო უშუალოდ საქმის განხილვის დროს, ევროპის კავშირში გამოიყენება რეგულაცია რომი II, აქვე უნდა აღინიშნოს რომ ხსენებული არ შეიცავს არანაირ სამართლის კოლიზიურ ნორმებს ინტერნეტ დელიქტებთან დაკავშირებით, აღნიშნულთან მიმართებაში გასათვალისწინებელია, რომ მსგავსი კოლიზიური ნორმების ფორმულირებისას ტექნოლოგიური ინოვაციებიდან გამომდინარე მაქსიმალურად თავიდან აცილებული უნდა იქნეს „საშიში“ ჩანაწერების არსებობა.¹⁹⁵

რეგულაცია რომის II მე-4 მუხლის მიხედვით დელიქტური ვალდებულება უნდა მოწესრიგდეს იმ ქვეყნის სამართლის მიხედვით, რომელშიც ზიანი წარმოიშვა, იმისდა მიუხედავად თუ სად განხორციელდა ზიანის მაპროვოცირებელი მოვლენა და იმისდა მიუხედავად თუ სად დადგა ირიბი ზიანი. მოცემული მუხლის მიხედვით რეგულაცია ზიან მიყენებულ პირს არ აძლევს საშუალებას ამოირჩიოს იმ ქვეყნების სამართალს შორის ერთ-ერთი, სადაც ზიანის წარმომშობი მოვლენა განხორციელდა და სადაც ზიანი დადგა, რაც არსებითად განსხვავდება რეგულაცია ბრიუსელი I-ის 7(2) მუხლისგან, სადაც მხარეს ამ ორს შორის არჩევანის გაკეთება შეუძლია.¹⁹⁶ მიუხედავად ამისა, თუ ზიანი დამდგარია რამდენიმე ქვეყანაში თანადროულად, ინტერნეტ დელიქტზე შესაძლებელია გავრცელდეს სხვადასხვა ქვეყნის კანონმდებლობა მხოლოდ იმ ნაწილებში, რა მოცულობითაც დადგა ზიანი განსხვავებულ სახელმწიფოებში (საუბარია მხოლოდ და მხოლოდ ევროპის კავშირის ქვეყნებზე).¹⁹⁷ თუმცადა, მოცემული მოსაზრების მისაღებობას საეჭვოს ხდის ინტერნეტის ფართოდ ხელმისაწვდომი ბუნება, გამომდინარე აქედან ინტერნეტ დელიქტის დროს სავარაუდოა, რომ ზიანი სხვადასხვა სახელმწიფოებში დადგება, შესაბამისად გამოყენებული უნდა იქნეს არა

¹⁹⁵ Świerczyński M., Electronic torts/delicts in the Rome II regulation, Tort Law in Poland, Germany and Europe, eds. Heiderhoff B./Zmij G., sellier. european law publishers, Munich 2009, 174.

¹⁹⁶ Bogdan M., Torts in Cyberspace - The Impact of the New Regulation “Rome II”, Masaryk University Journal of Law and Technology, Vol. 2, No 1, 2008, 4-5

¹⁹⁷ Mierina A., Some reflections on non-contractual obligations in cyberspace considering the Rome II regulation, SHS Web of Conferences Vol. 10. Article 00023, 2014, 5-6.

ყველა ქვეყნის სამართალი, არამედ იმ სახელმწიფოსი, რომელიც ყველაზე მეტად არის დაკავშირებული დელიქტურ ქმედებასთან.¹⁹⁸

აღსანიშნავია, რომ დელიქტური ქმედება როგორცაა დეფამაცია, ვერ მოხვდა რომი II ფარგლებში, მიუხედავად იმისა რომ რეგულაციის თავდაპირველ ვერსიაში პირადი უფლებების შესახებ ჩანაწერი არსებობდა,¹⁹⁹ გამომდინარე იქიდან რომ ევროპის კავშირის წევრი ქვეყნების მიერ ვერ იქნა კონსესუსი მიღწეული, რომელიც ყველა მათგანს დააკმაყოფილებდა. ზოგი ქვეყანა შემფოთებას გამოთქვამდა საკითხთან დაკავშირებით, როდესაც ადგილობრივი გამომცემლების წინააღმდეგ წარდგენილი სარჩელები აუცილებლად სხვა ქვეყნის სამართლის შესაბამისად უნდა განხილულიყო, მაშინაც კი, როდესაც ადგილობრივი საკანონმდებლო ბაზა სრულიად შეესაბამებოდა დავას.²⁰⁰

ზემოხსენებულს ემატება ისიც, რომ ევროპის კავშირში არ არის უნიფიცირებული დეფამაციასთან დაკავშირებული კოლიზიური ნორმები, შესაბამისად ასეთი ინტერნეტ დელიქტის დროს მოსარჩელეს აქვს მანიპულაციის საშუალება, რათა ამოირჩიოს ერთ–ერთი გამოსაყენებელი სამართალი სამი შესაძლო შემთხვევიდან, რასაც რეგულაცია ბრიუსელი I უწყობს ხელს. პირველ შემთხვევაში მოსარჩელეს სარჩელის წარდგენა შეუძლია იმ ადგილის მიხედვით სადაც დეფამაციის განმახორციელებელი არის რეგისტრირებული/რეზიდენტი. მეორე შემთხვევაში მოსარჩელეს შეუძლია სარჩელის შეტანა იმ ქვეყნის მასშტაბით სადაც დეფამაციური ცნობები გავრცელდა, ხოლო, მესამე და ყველაზე საინტერესო გზაა სარჩელის იმ ადგილის მიხედვით წარდგენა სადაც, იურიდიულ ლიტერატურაში მოაზრებული ცნება ინტერნეტ დელიქტებთან დაკავშირებით, ინტერესთა ცენტრი იყრის თავს.²⁰¹

ზემოგანხილული მსჯელობიდან, ნათლად ჩანს, ინტერნეტ დელიქტის მიერ წარმოშობილი ზიანის ტერიტორიულობის დადგენის პრობლემატიკა. იმისდა მიუხედავად, რომ რეგულაცია რომი II მე–4 მუხლით პირდაპირ გვეუბნება გამოსაყენებელი სამართლის დადგენის შესაძლებლობას, იმ ქვეყნის სამართლის მიხედვით, რომელშიც დელიქტურმა ქმედებამ გამოიწვია ზიანი, მოცემული მუხლი არ აკონკრეტებს თუ რა ითვლება

¹⁹⁸ *Bogdan M.*, Torts in Cyberspace - The Impact of the New Regulation “Rome II”, Masaryk University Journal of Law and Technology, Vol 2, No 1, 2008, 5.

¹⁹⁹ *Savin A.*, EU Internet Law, Edward Elgar Publishing, Cheltenham/Northampton 2013, 67-68.

²⁰⁰ *Mierina A.*, Some reflections on non-contractual obligations in cyberspace considering the Rome II regulation, SHS Web of Conferences Vol. 10. Article 00023, 2014, 6.

²⁰¹ იქვე, 6-7.

ზიანის წარმოშობის უშუალო ადგილად, რაც პრობლემურს ხდის მის განსაზღვრას, შესაბამისად არ არსებობს ერთიანი ნორმატიულ საფუძველზე დამყარებული მოსაზრება მოცემულ საკითხთან დაკავშირებით. საქმეზე Peter Pinckney vs KDG Mediatech AG²⁰² სადაც მოსარჩელე პიტერ ფინქნი, მუსიკოსი, სარჩელით წარსდგა საფრანგეთის სასამართლოს წინაშე, მისი დარღვეული საავტორო უფლებიდან გამომდინარე მოთხოვნით ავსტრიული კომპანიის წინააღმდეგ, რომელიც თავის მხრივ ფინქნის მუსიკალურ მატერიალს ინტერნეტის საშუალებით ყიდდა ბრიტანული საიტის საშუალებით, ეს უკანასკნელი თავისმხრივ ხელმისაწვდომი იყო, ევროპის კავშირის ქვეყნებში მათ შორის საფრანგეთშიც. შესაბამისად პრობლემას წარმოადენდა საქმის განხილველი სასამართლოს განსჯადობის საკითხი, რადგანაც ზუსტად შეუძლებელი იყო იმ კონკრეტული ტერიტორიის დადგენა, სადაც მოსარჩელეს ზიანი ადგებოდა. ევროპული კავშირის მართლმსაჯულების სასამართლომ განმარტა, რომ რადგანაც ზოგადად საავტორო უფლებები ევროპის კავშირის მასშტაბით დაცულია, არსებობდა საშიშროება, რომ დარღვევას უშუალოდ საფრანგეთშიც ჰქონოდა ადგილი, რადგანაც მის ტერიტორიაზეც საავტორო უფლებები დაცულია.²⁰³ მოცემული საქმიდან გამომდინარე უნდა ვივარაუდოთ, თუ დაცული სიკეთის დარღვევის საშიშროება არსებობს უშუალო უფლების დარღვევასთან ერთად პარალელურად, მაშინ ევროპის კავშირის იმ წევრი სახელმწიფოს სასამართლოს ექნება საქმის განხილვის უფლება, რომელშიც შესაძლოა უფლება დაირღვეს ხოლო გამოსაყენებელი სამართალი კი იმის მიხედვით განისაზღვროს სადაც საართლებრივი სიკეთე დაცულია.²⁰⁴ აღნიშნული განმარტება არ უნდა იქნეს ზოგადი წესის სახით მიღებული და მისი გამოყენება სასურველია მხოლოდ საავტორო უფლებებთან დაკავშირებით მოხდეს, თუმცადა სასამართლოს განმარტება მაინც ღიას ტოვებს პრობლემურ საკითხს განსჯადობასთან დაკავშირებით და არ არის ბოლომდე დამაკმაყოფილებელი, გამომდინარე იქიდან რომ საავტორო უფლებების საკითხი სპეციფიკური ხასიათისაა და მნიშვნელოვნად არის დაკავშირებული წარმოშობის ტერიტორიულობის პრინციპთან.

²⁰² Case C-170/12 Peter Pinckney v KDG Mediatech AG

²⁰³ *Gonçalves A.*, The Application of the General Rule of the Rome II Regulation to Internet Torts, Masaryk University Journal of Law and Technology, Vol 8, No 1, 2014, 64.

²⁰⁴ მიუხედავად იმისა რომ რომი II რეგულაციის მე-8 მუხლის მიხედვით ინტელექტუალურ საკუთრებასთან მიმართებაში გამოსაყენებელი სამართალი უნდა იყოს იმ ქვეყნის სამართალი სადაც უფლება დაცულია, მოაზრებულია იმ წევრი სახელმწიფოს სამართალი რომელშიც უშუალოდ დარღვევა განხორციელდა და არა ყველა ის წევრი სახელმწიფო სადაც ინტელექტუალური საკუთრებაა ზოგადად დაცული.

ამრიგად რომი II რეგულაცია უფრო მეტად „მოუხეშავია“, ინტერნეტ დელიქტებთან მიმართებაში, ვიდრე ბრიუსელი I რეგულაცია, იმისდამიუხედავად, რომ ისინი სხვადასხვა რეგულატორულ საკითხს მოიცავენ. რეგულაცია რომი II ყოველი განხილული საქმის შემდეგ უფრო მეტად კონტროვერსიულ კითხვებს ბადებს მისი და ინტერნეტ სივრცეში მიყენებული ზიანის ურთიერთმიმართებასთან დაკავშირებით, განსაკუთრებით კი ზიანის ადგილის განსაზღვრის და დაცული სივრცის ბუნების კორელაციურობის საკითხების შესახებ.

V. ინტერნეტ დელიქტები საქართველოში

ქართულ იურიდიულ ლიტერატურაში ინტერნეტ დელიქტებზე მსჯელობა ფაქტიურად არ მიმდინარეობს. თუმცადა პრაქტიკული პრობლემა ქართული სამართლისთვის რეალურია, როგორც სასამართლო დავებისთვის, ასევე, ნორმატიული მოწესრიგებისთვის, აქვე უნდა აღინიშნოს რომ ორივე მოცემულობა არამხოლოდ ისეთ კონკრეტულ საკითხს როგორცაა ინტერნეტ სივრცეში მიყენებულ ზიანი, არამედ ზოგადად ინტერნეტში წარმოშობილ ურთიერთობებს ეხება.

წინამდებარე თავის მიზანია განიხილოს მოცემულ საკითხთან დაკავშირებით ქართული სასამართლო პრაქტიკა და მოახდინოს მისი პრობლემატიკის სწორად წარმოჩენა, ასევე, არსებული ნორმატიული საფუძვლების ინტერნეტ დელიქტთან მიმართება და კვლევის ფარგლებში შესთავაზოს მათი ინტერპრეტაციის ან/და ჩამოყალიბების შესაძლო რეკომენდაციები.

1. სასამართლო და არასამართლო პრაქტიკა

1.1. ინტერნეტ დავების საწყისი წერტილი

რაოდენ გასაკვირიც არ უნდა იყოს საქართველოს უზენაესი სასამართლოს მიერ ინტერნეტ დელიქტთან მიახლოებული დავა ჯერ კიდევ 2000 წელს იქნა განხილული.²⁰⁵ საქმე შეეხებოდა დომენის, როგორც სასაქონლო ნიშნის გამოყენების აკრძალვას. თავის მხრივ სადავო დომენი მოპასუხეს 1997 წელს ჰქონდა რეგისტრირებული, ხოლო, სასაქონლო ნიშანი, რომელიც მოსარჩელეს ეკუთვნოდა, დარეგისტრირდა 1998 წელს. იმისდა მიუხედავად

²⁰⁵ საქართველოს უზენაესი სასამართლოს 2000 წლის 11 ოქტომბრის განჩინება საქმეზე №: 3კ/589.

რომ ქვემდგომი ინსტანციის მიერ, მოსარჩელის მოთხოვნა დომენის გამოყენების აკრძალვაზე დაკმაყოფილებულ იქნა, საკასაციო სასამართლომ მნიშვნელოვნად იმსჯელა საკითხთან მიმართებაში, და გააუქმა მოთხოვნის დამაკმაყოფილებელი ქვემდგომი სასამართლოს გადაწყვეტილება. საქმე თავის მხრივ, ატიპიურ მოვლენას წარმოადგენს, მისი არა დომენის, არამედ უშუალოდ ნიშნის რეგისტრაციის პერსპექტივით. მოცემულ შემთხვევაში დავის მხარეებს შორის არ შედგა კონკრეტული სახელშეკრულებო ურთიერთობა, რომლის შემდეგაც მოსარჩელემ არაკეთილსინდისიერი განზრახვით გადაწყვიტა მოპასუხის დომენური სახელი, დაერეგისტრირებინა, როგორც მისი სასაქონლო ნიშანი და ამის შემდეგ აეკრძალა მოპასუხისთვის დომენის გამოყენება. თავის მხრივ თუ დავეყრდნობით სასაქონლო ნიშნების მომწესრიგებელ ნორმატიულ ბაზას, მოსარჩელის მოთხოვნა მაშინაც და ახლაც სამართლებრივად დასაბუთებულია, რადგანაც სახელზე როგორც სასაქონლო ნიშანზე უფლება მხოლოდ მისი რეგისტრაციის შემდეგ წარმოიშობა,²⁰⁶ თუმცა სასამართლო მიუთითებს „ის, რომ არ არსებობს კანონმდებლობა, რომელიც არეგულირებს ინტერნეტთან დაკავშირებულ ურთიერთობებს, არ შეიძლება გახდეს ინტერნეტში გამოყენებული პირის ინდივიდუალიზაციის საშუალებების სახელისა და მისამართის დაცვაზე უარის თქმის საფუძველი.“²⁰⁷ რაც მართებულ მსჯელობას წარმოადგენს და თავის მხრივ, ირიბად ამყარებს იმ არგუმენტს რომ მსგავსი ტიპის დავებისთვის მხოლოდ საკანონმდებლო ბაზაზე დაყრდნობა არ არის გამართლებული.²⁰⁸ სასამართლო ქვემდგომი ინსტანციის გადაწყვეტილების გასაუქმებლად მიუთითებს: „დომენური სახელისა და სასაქონლო ნიშნის გამოყენების მართლობიერება შეფასებულ უნდა იქნეს საქმიანი ბრუნვის ტრადიციებისა და უფლების განხორციელების მართლობიერი საზღვრების გათვალისწინებით. აღნიშნული თვალსაზრისით, არამართლობიერად უნდა იქნეს მიჩნეული, რომ არაკეთილსინდისიერი კონკურენციის მიზნით ინტერნეტში დომენად დარეგისტრირდეს ნიშანი, რომელიც უკვე არსებული გარკვეული რეპუტაციის მქონე სასაქონლო ნიშნის იდენტური ან მსგავსია.“, რაც სრულიად მიესადაგება კიბერსქვათინგის აკრძალვის საფუძვლებს,

²⁰⁶ დავის დაწყებისთვის მოქმედებდა საქართველოს სამოქალაქო კოდექსის 1997 წლის 24 ივლისის პუბლიკაცია, რომლის 1102 მუხლიც სასაქონლო ნიშნის რეგისტრაციის დაცვას მხოლოდ მისი რეგისტრაციის შემდეგ ითვალისწინებდა. 2018 წლის 5 ივლისის საქართველოს კანონის პუბლიკაციაც სასაქონლო ნიშნების შესახებ მე-3 მუხლის მე-3 ნაწილით ნიშნის დაცვას რეგისტრაციის შემდეგ ითვალისწინებს.

²⁰⁷ საქართველოს უზენაესი სასამართლოს 2000 წლის 11 ოქტომბრის განჩინება საქმეზე №: 3კ/589.

²⁰⁸ *Mercer D. J.*, Cybersquatting: Blackmail on the Information Superhighway, *Journal of Science & Technology Law*, Vol. 6, Notes, 2000, 3-4.

სასამართლო, ასევე, იმ დროისთვის ინოვაციური საკითხსაც ამატებს დავიდან გამომდინარე: „არამართლობიერად უნდა იქნეს მიჩნეული უკვე დარეგისტრირებული დომენური სახელის სხვა პირის მიერ სასაქონლო ნიშნად რეგისტრაცია და შემდეგში სასაქონლო ნიშანზე განსაკუთრებული უფლების საფუძველზე დომენის გამოყენების აკრძალვა.“²⁰⁹ აქვე უნდა აღინიშნოს რომ მოცემული განმარტება ფაქტიურად პირველად ამკვიდრებს სასაქონლო ნიშნის არაკეთილსინდისიერი განზრახვით რეგისტრაციის დაუშვებლობას.²¹⁰ თავის მხრივ საყურადღებოა ისიც, რომ ამერიკის შეერთებული შტატების მომხმარებელთა დაცვის კანონი ანტი-კიბერსქვათინგის შესახებ, მოქმედების საფუძველად მნიშვნელოვნად ითვალისწინებს არაკეთილსინდისიერ განზრახვას.²¹¹

ასევე აღსანიშნავია, რომ პირველი მსგავსი ტიპის დავა ინტელექტუალური საკუთრების მსოფლიო ორგანიზაციის მიერ სწორედ 2000 წელს იქნა გადაწყვეტილი.²¹²

ამრიგად უზენაესი სასამართლოს განჩინება სრულიად შესაბამისობაში იყო იმდროინდელი ინტერნეტ დავების გადაწყვეტის მსოფლიო ტენდენციებთან, მიუხედავად იმისა რომ პალატა არ იშველიებს უცხოურ პრაქტიკასა და თეორიულ ასპექტებს საკითხთან დაკავშირებით. განჩინება, ასევე, ამკვიდრებს მნიშვნელოვან პრაქტიკას ისეთი დომენური სახელის დაცვისთვის რომელიც არ წარმოადგენს რეგისტრირებულ სასაქონლო ნიშანს თუმცა დაკავშირებულია მისი მფლობელის საფირმო სახელწოდებასთან და გააჩნია გარკვეული რეპუტაცია.

1.2. ინტერნეტ სივრცე როგორც მეწარმეთა არაკეთილსინდისიერი კონკურენციის ასპარეზი

ინტერნეტ სივრცეში მიყენებული ზიანისთვის უმნიშვნელოვანესი გადაწყვეტილება საქმეზე No2/30577-16²¹³ ერთი მხრივ წინ გადადგმული

²⁰⁹ საქართველოს უზენაესი სასამართლოს 2000 წლის 11 ოქტომბრის განჩინება საქმეზე №: 3კ/589.

²¹⁰ საქმის განხილვის მომენტში დათქმა ნიშნის არაკეთილსინდისიერი რეგისტრაციის აკრძალვის შესახებ არ არსებობდა. მსგავსი ჩანაწერი სასაქონლო ნიშნების შესახებ საქართველოს კანონში 2005 წელს შევიდა; საქართველოს 2005 წლის 20 დეკემბრის კანონი №2380 - სსმ I, №1, 04.01.2006 წ., მუხ. 3.

²¹¹ Anticybersquatting Consumer Protection Act, (15 U.S.C. § 1125(d)). Section 2.

²¹² World Wrestling Federation Entertainment, Inc. v. Michael Bosman, WIPO, No. D99-. 0001 (Jan. 14, 2000)

²¹³ თბილისის საქალაქო სასამართლოს 2017 წლის 8 მაისის გადაწყვეტილება საქმეზე No2/30577-16.

ნაბიჯია პრაქტიკისთვის, ხოლო, მეორე მხრივ ნათლად გვიჩვენებს თუ როდენ მოუმზადებელი შეიძლება აღმოჩნდეს სასამართლო ტექნიკურად ახალი სამართლებრივი საკითხის წინაშე.

მოსარჩელეც და მოპასუხეც მოცემულ საქმეში წარმოადგენენ ერთი და იმავე კომპანიის Apple Inc.–ის პროდუქტის დისტრიბუტორებს საქართველოში. გამომდინარე იქიდან, რომ ლოკალური ბაზარი მიმართულებით ძირითადად მოდავე მხარეებს ჰქონდათ ათვისებული, მოპასუხემ გადაწყვიტა ინტერნეტის მეშვეობით არაკეთილსინდისიერი კონკურენცია გაეწია მოსარჩელისთვის, კონკრეტულად კი შექმნა მოსარჩელის სახელწოდებით საიტი, რომლის დომენური სახელი მხოლოდ ერთი ასოთი განსხვავდებოდა მოსარჩელის სახელისგან, სადაც ანთავსებდა მოსარჩელისთვის რეკლამის შემლახველ მატერიალს, ასევე, მოსარჩელის განმარტებით მოპასუხემ იგივე ქმედება განახორციელა სოციალურ ქსელ Facebook.com-ზე, სადაც მოსარჩელის ზუსტი სახელით შექმნა გვერდი. მოსარჩელის მოთხოვნამ 1 553 851,56 ლარი შეადგინა, რაც არამხოლოდ ინტერნეტ დავისთვის, არამედ ზოგადად ქართული სასამართლო პრაქტიკისთვის მნიშვნელოვან მოცულობას წარმოადგენს, რაც კიდევ ერთხელ ხაზს უსვამს თუ რა მასშტაბის შეიძლება იყოს ინტერნეტში წარმოშობილი ზიანი.

სასარჩელო მოთხოვნა ნაწილობრივ, 856 163 ლარის ოდენობით დაკმაყოფილდა. უპირველეს ყოვლისა ყურადღება უნდა გამახვილდეს სამოტივაციო ნაწილის სამართლებრივი შეფასების პრობლემატიკაზე და მის სავარაუდო ხარვეზზე. სასამართლო ქართული პრაქტიკის არარსებობის გამო სადავო საკითხთან მიმართებაში მიუთითებს უცხოურ პრაქტიკაზე. კონკრეტულად 2003 წლის გაურკვეველი თვის 29 რიცხვის გადაწყვეტილებაზე,²¹⁴ რომელიც სისხლის სამართლებრივ დანაშაულზეა მიღებული. მოცემულ გადაწყვეტილებაზე მიუთითება არასწორია, შემდეგი სავარაუდო ფაქტობრივი უზუსტობების გამო. სისხლისსამართლებრივი დანაშაულის²¹⁵ საქმეზე United States v. John Zuccarini, 2003 წლის არცერთი თვის 29 რიცხვში გადაწყვეტილება არ ყოფილა მიღებული, მოცემულ საქმეზე დაცვის მხარემ დანაშაული 2003 წლის 10 დეკემბერს აღიარა, ხოლო, სასჯელი

²¹⁴ თბილისის საქალაქო სასამართლოს 2017 წლის 8 მაისის გადაწყვეტილება საქმეზე No2/30577-16. სამოტივაციო ნაწილი, სამართლებრივი შეფასება პუნქტი 6.1.

²¹⁵ 18 U.S. Code §2252B. Misleading domain names on the Internet. აღნიშნული მუხლი შეერთებული შტატების კოდექსის სისხლის სამართლებრივი დანაშაულისა და საპროცედურო ნორმების თავშია მოქცეული (18 U.S. Code Title 18— CRIMES AND CRIMINAL PROCEDURE) იხ. ბმულზე <https://www.law.cornell.edu/uscode/text/18/2252B#>.

მას 2004 წლის 26 თებერვალს შეეფარდა.²¹⁶ სასამართლო სავარაუდოდ გულისხმობს არა გადაწყვეტილებას, არამედ 2003 წლის 29 აგვისტოს გაცემულ დაკავების ბრძანებას, რომელსაც თავის მხრივ საფუძვლად უდევს ამერიკის შეერთებული შტატების საფოსტო ინსპექციის ოფიცრის საგამომიებო მასალების მიმომხილველი ჩვენება.²¹⁷

პრაქტიკის საწყის ეტაპზე და ზოგადადაც არ უნდა იყოს რეკომენდებული მოსამართლემ გადაწყვეტილების გასამყარებლად გამოიყენოს სხვა ქვეყნის არა გადაწყვეტილება, არამედ ინსპექტორის საგამომიებო მასალები, რომელიც არა სამოქალაქო დავას, არამედ ინტერნეტში კრიმინალურ საქმიანობას ეხება.

აღნიშნულ დავაში სასამართლოს ყურადღება უნდა გაემახვილებინა კიბერსქვათინგის მოვლენაზე, განსაკუთრებით ისეთ პირობებში, როდესაც ნორმატიული რეგულაცია არ არსებობს საქართველოსთვის მსგავსი საკითხისადმი და მოცემულ საქმეზე სასამართლო პრაქტიკა სამომავლო დავებისთვის სახელმძღვანელო უნდა იყოს. მაგალითისთვის იგივე John Zuccarini ერთ–ერთი ყველაზე ცნობილი კიბერსქვათერია²¹⁸ და მის წინააღმდეგ ათეულობით კიბერსქვათინგთან დაკავშირებული დავა ნაწარმოები,²¹⁹ სწორედ ამ უკანასკნელთა გამოყენება იქნებოდა რელევანტური, რომლებიც პირდაპირ მიუთითებენ რომ სასაქონლო ნიშნის თუ სახელის გამოყენება არაკეთილსინდისიერი განზრახვით ყოველად დაუშვებელია.

სასამართლო არ იყენებს ტერმინს კიბერსქვათინგს და არ განმარტავს მას რელევანტურად, მიუხედავად იმისა, რომ მისი შემადგენლობა ძალიან მიახლოებულია დავის მოცემულობასთან, რაც შესაძლოა გამოწვეული ყოფილიყო იმით რომ კიბერსქვათინგი უშუალოდ სასაქონლო ნიშანთან არის

²¹⁶ United States Attorney, Southern District of New York, 'Cyber scammer' Sentenced to 30 Months for Using Deceptive Internet Names to Mislead Minors to X-Rated Sites, February 26, 2004, *იხ. ბულზე* <https://www.justice.gov/archive/criminal/cybercrime/press-releases/2004/zuccariniSent.htm>; (ვიზიტის დრო: 24.06.2019). ასევე, *იხ. Clark G. C., The Truth in Domain Names Act of 2003 and a Preventative Measure to Combat Typosquatting, Cornell Law Review, Vol. 89, Issue 6, 2004, 1513.*

²¹⁷ 2003 წლის 29 აგვისტოს საგამომიებო ჩვენება და დაკავების ბრძანება *იხ. ბულზე* <http://dnattorney.com/United%20States%20of%20America%20v.%20John%20Zuccarini.pdf> (ვიზიტის დრო: 24.06.2019).

²¹⁸ *იხ. 2003 წლის ელექტრონული სტატია World's most notorious cybersquatter arrested* https://www.theregister.co.uk/2003/09/04/worlds_most_notorious_cybersquatter_arrested/.

²¹⁹ *Dow Jones & Company, Inc. and Dow Jones LP v. John Zuccarini, WIPO, No. D2000-0578 (Aug. 28, 2000); Diageo plc v. John Zuccarini, Individually and t/a Cupcake Patrol, WIPO, No. D2000 – 0996 (Oct. 22, 2000); Federal Trade Commission v. John Zuccarini, Civil Action No.01-CV-4854, United States District Court for the Eastern District of Pennsylvania.; Kevin Spacey v John Zuccarini, National Arbitration Forum, Claim Number: FA0103000096937, 2001.*

დაკავშირებული,²²⁰ კონკრეტულ შემთხვევაში კი მოსარჩელეს მოპასუხის დომენში გამოყენებული დასახელება რეგისტრირებული, როგორც სასაქონლო ნიშანი არ ჰქონია, თუმცადა სასამართლო არ ერიდება გადაწყვეტილებაში სასაქონლო ნიშნებზე საუბარს და იგი კიბერსქვათინგის ნორმატიულ საფუძველსაც კი იყენებს „იდენტური ან მსგავსი დომენის გამოყენებას ზღუდავს იმ პირების მიერ, რომლებსაც არ ეკუთვნით შესაბამის სახელწოდებაზე სასაქონლო ნიშანი.“²²¹ რაც თავის მხრივ უზუსტობაა რადგანაც დომენის სახელში სასაქონლო ნიშნის მართლზომიერ გამოყენებას სასამართლოს მიერ მოხმობილი ნორმატიული დანაწესი არ ზღუდავს.²²²

ყოველივე ზემოგანხილულიდან ნათელია რომ სასამართლო არა შეგნებულად არ ამხვილებს გარკვეულ სამართლებრივ მოცემულობებზე ყურადღებას, არამედ იგი უბრალოდ მზად არ აღმოჩნდა ინტერნეტ სივრცეში წარმოშობილი ზიანისთვის შესაბამისი მკაფიო და ნათელი დეფინიციები ჩამოეყალიბებინა. მნიშვნელოვანია, რომ მოსარჩელე მხარის წარმომადგენლები ხელს უწყობდნენ სასამართლო გადაწყვეტილების თანამედროვე სტანდარტებში მოქცევას და სასამართლოს აწვდიდნენ შესაბამის ცნობებს მოცემულ ინტერნეტ დელიქტთან დაკავშირებით, რაც თავისთავად დადებითი მოვლენაა.

სასამართლო, ასევე, არ იყენებს დამატებით, თუნდაც განმარტებისთვის საქართველოსთვის ერთადერთ ნორმატიულ აქტს რომელიც დომენებსა და ვებ საიტებს შეეხება, საუბარია საქართველოს კომუნიკაციების ეროვნული კომისიის დადგენილება №3–ზე.²²³ მოცემული ნორმატიული აქტი იძლევა დომენის განმარტებას, რომლის მიხედვითაც ის არის „ინტერნეტ–სახელი, რომელიც ეკუთვნის ერთადერთ იურიდიულ ან ფიზიკურ პირს და ახდენს მის იდენტიფიცირებას და განსხვავებას სხვათაგან“.²²⁴ ხოლო შინაარსობრივი დეფინიციის მიხედვით “ინტერნეტ–გვერდის დომენი არ უნდა იყოს დამახვეელი, არ უნდა ემსახუროდეს სხვა ინტერნეტ–გვერდის

²²⁰ Uniform Domain Name Dispute Resolution Policy, Paragraph 4.; 15 U.S. Code §1125(d).

²²¹ თბილისის საქალაქო სასამართლოს 2017 წლის 8 მაისის გადაწყვეტილება საქმეზე No2/30577-16. ფაქტობრივი გარემოებები პუნქტი 3.19.

²²² 15 U.S. Code §1125(c)(3).

²²³ საქართველოს კომუნიკაციების ეროვნული კომისიის 2006 წლის 17 მარტის დადგენილება №3, ელექტრონული კომუნიკაციების სფეროში მომსახურების მიწოდების წესებისა და მომხმარებელთა უფლებების დაცვის შესახებ, იხ. ბმულზე <https://matsne.gov.ge/ka/document/view/63556>. აღნიშნულ ნორმატიულ აქტში ცვლილება 2007 წლის 9 ნოემბერს შევიდა, რომელმაც მოიცვა დომენი და ვებ გვერდის რეგულაცია. იხ. ბმულზე <https://matsne.gov.ge/ka/document/view/74110>.

²²⁴ იქვე, მუხლი 2. ნაწილი 3. 3^o ქვეპუნქტი.

გადაფარვას და უნდა შეესაბამებოდეს მის შინაარსს²²⁵ ამრიგად დომენი უნდა აკმაყოფილებდეს ორ კომპონენტს. პირველი ეს არის არაკეთილსინდისიერი კონკურენციის აღმოფხვრა, რაც გამოიხატება იმაში რომ დომენი უნდა იძლეოდეს იდენტიფიცირების საშუალებას მისი მფლობელისა, ასევე, არ უნდა იძლეოდეს სხვა უკვე დამკვიდრებულ დომენთან აღრევის საშუალებას და არ უნდა ცდილობდეს მის ჩანაცვლებას. ხოლო, მეორე კომპონენტი კი მომხმარებელთა დაცვაა, რათა არ მოხდეს მათი შეცდომაში შეყვანა და ზიანის მიყენება. მოცემული დავა, თავის მხრივ განხილული აქტის ორივე კომპონენტს შეიცავს, მოპასუხე არეგისტრირებს დომენს რომლითაც ახორციელებს არაკეთილსინდისიერ კონკურენციას და მეორე მხრივ, შეჰყავს მომხმარებელი შეცდომაში.

თუმცაღა აღსანიშნავია, რომ სასამართლო თავს ართმევს სამოქალაქო კოდექსის დელიქტური ნორმების (სსკ 992–ე და შემდგომი მუხლები) ზუსტად მისადაგებას მოცემულობისთვის, კონკრეტულად კი მისი ტრანსფორმაცია წარმოდგენილი მტკიცებულებების დელიქტურ დანაწესებთან ზედმიწევნითია, ისეთ შეთხვევაში როდესაც გასათვალისწინებელია ინტერნეტის ბუნება და მასში წარმოშობილი ურთიერთობები. ასევე, საგულისხმოა ადეკვატური მიზეზობრიობის თეორიის²²⁶ მიმართება მოცემულ დავასთან და მისი გამოყენების მართებულობა, გამომდინარე იქიდან რომ ინტერნეტ სივრცეში რთულია ზიანის გამომწვევი ყოველი ქმედების მიდევნება.

ამრიგად აღნიშნული დავა გვაჩვენებს თუ ინტერნეტ სივრცეში მიყენებული ზიანი როგორი ფართო მოცულობის შეიძლება იყოს და როგორ შეიძლება გადაიქცეს ინტერნეტი ორი კომპანიის კონკურენციის ცენტრად, ხოლო, მეორე მხრივ კი რა სამართლებრივ სირთულებებთან არის აღნიშნული ტიპის დავები დაკავშირებული.

1.3. კიბერსექსუალური ქართულად

საქართველოს კომუნიკაციების ეროვნული კომისიის 2017 წლის 30 ნოემბრის გადაწყვეტილება N 793 / 16–ის²²⁷ მიხედვით ფიზიკურმა პირმა 4 დომენი

²²⁵ იქვე, მუხლი 10. ნაწილი 1.

²²⁶ *ქობაშვილი ქ.*, ბრალი, როგორც სამოქალაქო სამართლებრივი პასუხისმგებლობის პირობა, სამართლის ჟურნალი, #1, თბილისი 2009, 83.

²²⁷ საქართველოს კომუნიკაციების ეროვნული კომისიის 2017 წლის 30 ნოემბრის გადაწყვეტილება N 793 / 16 შპს „კავკასუს ონლაინის“ მიმართ სს „თიბისი ბანკის“ საჩივრის განხილვის თაობაზე, იხ. ბმულზე <http://www.gncc.ge/ge/legal-acts/solutions/2017-793-16.page> (ვიზიტის დრო: 24.06.2019).

დაარეგისტრირა სს „თიბისი ბანკის“ სასაქონლო ნიშნის TBC Bank და TBC შემცველობით. აღნიშნული პირი დომენების რეგისტრაციის შემდეგ შეეცადა ისინი სს „თიბისი ბანკისთვის“ მიეყიდა, ამ უკანასკნელმა კი თავის მხრივ უარი თქვა დომენების შექენაზე და მიმართა რეგისტრატორს შპს „კავკასუს ონლაინს“ დომენების გაუქმების მოთხოვნით, რაზეც რეგისტრატორმა უარი განაცხადა, სწორედ ამის შემდეგ სს „თიბისი ბანკმა“ მიმართა კომუნიკაციების ეროვნული კომისიას დომენებზე წვდომის შესაზღუდად, რაც უშუალოდ რეგისტრატორის მიმართ პრეტენზიაა და არა ფიზიკური პირის რეგისტრანტის მიმართ.

მოცემულობის მიხედვით სახეზე ნათელი მაგალითია კიბერსქვათინგისა. ფიზიკური პირი არეგისტრირებს დომენებს ერთ–ერთი ყველაზე დიდი კომერციული ორგანიზაციის, როგორც საფირმო, ისე სასაქონლო ნიშნის შემცველობით დროის მცირე მონაკვეთში, რაც პირველი კომპონენტი კიბერსქვათინგისთვის, ხოლო, ბოლო დომენის რეგისტრაციიდან მომდევნო დღეს კი უკვე სთავაზობს ნიშნის მფლობელს მათ შექენას. აღნიშნული ფაქტია რომ ფიზიკური პირის არაკეთილსინდისიერებაზე მიუთითებს, რაც მეორე მახასიათებელს წარადგენს კიბერსქვათინგისთვის.²²⁸

თუმცადა მოცემული საქმე არა კიბერსქვათინგის სტანდარტული მახასიათებლით არამედ რეგისტრატორის ბრალეულობაზე მითითებით გამოირჩევა, რაც ხელშემწყობი კიბერსქვათინგის (contributory cybersquatting) სახელითაა ცნობილი, რა დროსაც პირი აქტიური ან პასიური ქმედებით ხელს უწყობს კიბერსქვათინგს, აღნიშნულში ძირითადად დომენების რეგისტრატორები ექცევიან.²²⁹ ეგრედ წოდებული მეორადი პასუხისმგებლობა რეგისტრატორებისთვის შეერთებული შტატების სასამართლოების მიერ შემოთავაზებული ცნებაა²³⁰ და იგი შემდეგი კომპონენტებისგან შედგება: მნიშვნელოვნად კონტროლდება თუ არა დომენის რეგისტრაციის სერვისი რეგისტრატორის მიერ, იცის თუ არა რეგისტრატორმა მომხმარებლის კიბერსქვათინგის შესახებ და იცის თუ არა მომხმარებლის არაკეთილსინდისიერი განზრახვის შესახებ, რომელიც ეკონომიკურ მოგებასთანაა კავშირში.²³¹ ერთი მხრივ პირველი კომპონენტი მოცემულ შემთხვევაში შესაძლოა სადავო გახდეს, თუმცადა დანარჩენი ორი რეგისტრატორისთვის უნდა გამოირიცხოს. ხოლო უმთავრესად უნდა

²²⁸ Uniform Domain Name Dispute Resolution Policy, Paragraph 4.; 15 U.S. Code §1125(d).

²²⁹ *Walczak A. C.*, The New and Evolving Tort of Contributory Cybersquatting: Did the Courts Get it Right?, *University of Illinois Journal of Law, Technology & Policy*, Vol. 2012, 2012, 535–536.

²³⁰ იქვე.

²³¹ *Barbantonis F. N.*, Should Contributory Cybersquatting be Actionable?, *North Carolina Journal of Law & Technology*, Vol. 17, Issue 1, 2015, 97.

აღინიშნოს რომ მსგავსი კომპონენტების გამოყენება და დამკვიდრება შესაბამის ნორმატიულ აქტებში ქართული კანონმდებლობისთვის უაღრესად რეკომენდებულია, რათა მკაფიოდ გაიმიჯნოს რა შემთხვევაში შეიძლება მოთხოვნა მიესადაგებოდეს დომენის რეგისტრატორს და რა შემთხვევაში უნდა დაეკისროს მას პასუხისმგებლობა.

უდავოდ საინტერესოა მეორადი პასუხისმგებლობის საკითხი ქართული რეგისტრატორისთვის, თუმცა ზემოგანხილული შემთხვევა მხოლოდ სამოქალაქო დავის ფარგლებშია შესაძლებელია, რაც თავისთავად ნათელია, რომ საქართველოს კომუნიკაციების ეროვნული კომისიის კომპეტენციას სცდება. აქვე უნდა აღინიშნოს რომ იგი ვერც საარბიტრაჟო ტრიბუნალად მოგვევლინება.

კრიტიკის მხრივ კი უნდა ითქვას, რომ იურიდიულ ლიტერატურაში გამოთქმული მოსაზრება, რომ სასამართლოს მიერ მსგავსი ტიპის დავების განხილვა, სადაც საქმე ინტელექტუალურ საკუთრებას შეეხება, უფრო მეტად მიზანშეწონილია რომ მოხდეს სპეციალური არბიტრის მიერ,²³² მაშინ საქართველოს კომუნიკაციების ეროვნული კომისია, როგორც ადმინისტრაციული ორგანო მითუმეტეს ვერ იქნება კომპეტენტური მსგავსი შინაარსის დავა განიხილოს. რაც შეეხება უშუალოდ პირს რომელმაც სადავო დომენები დაარეგისტრირა ადმინისტრაციულ წარმოებაში როგორც არამოპასუხე მხარეს ვერ ექნება საშუალება ადეკვატური შეპასუხება განახორციელოს მისი ქმედების მართლზომიერების დასადასტურებლად.

1.3.1. ადმინისტრაციული ორგანოს ჩარევის კრიტიკა და დავის გადაწყვეტის სხვა მექანიზმებთან შედარება

ზემოგანხილული კრიტიკის უფრო ღრმა სამართლებრივი ანალიზისთვის, საჭიროა ადმინისტრაციული ორგანოს მიერ ადმინისტრაციული წარმოების ფარგლების როგორც დავის გადაწყვეტის საშუალების შედარება სხვა სამართლებრივ სივრცეში არსებულ დავის გადაწყვეტის მექანიზმებთან.

უპირველესად უნდა აღინიშნოს რომ განხილული ადმინისტრაციული საჩივრის განხილვის პროცესში შეუძლებელია იმ ზიანის ანაზღაურების მოთხოვნა, რომელიც სასაქონლო ნიშნის მფლობელს შეიძლებოდა მიდგომოდა, გამომდინარე იქიდან, რომ უშუალოდ დელიქტური ქმედების განმახორციელებელი ფიზიკური პირი, რომელმაც დაარეგისტრირა

²³² *Singh H.*, Domain Name Disputes and Their Resolution under UDRP Route: A Review, Archives of Business Research, Vol.6, No.12, 2018, 150.

დომენები არაკეთილსინდისიერი განზრახვით არ ექცევა საქართველოს კომუნიკაციების ეროვნული კომისიის სამართლებრივი რეგულირების სფეროში. შესაბამისად პირმა, რომელსაც ზიანი ადგება მისი სასაქონლო ნიშნის თუ სახელის არამართლზომიერად დომენის დასახელებაში გამოყენებისას ცალკე დავა უნდა აწარმოოს სამოქალაქო წესით და მიუთითოს სსკ-ს ტრადიციულ დელიქტურ საფუძვლებზე, რაც ნათელია რომ არასწორია, რადგანაც მხარე ებმევა ორმაგად ხანგრძლივ პროცესში და იგი საპროცესო თუ სხვა ხარჯებს წევს დამატებითი დავისთვის. სრულიად განსხვავებულ, მაგრამ სწორ მიდგომას გვთავაზობს შეერთებული შტატების მომხმარებელთა დაცვის კანონი ანტი-კიბერსქვათინგის შესახებ. ნიშნის მფლობელს შეუძლია როგორც დომენის გაუქმების, ასევე, დომენის მისთვის გადაცემის მოთხოვნის დაყენება სამოქალაქო დავის ფარგლებში,²³³ ხოლო, პარალელურად ასევე შეუძლია მოითხოვოს ზიანის ანაზღაურება,²³⁴ ან კანონის მიერ დაწესებული ზიანის ანაზღაურება (statutory damages), რომელიც განისაზღვრება 1000–100 000 დოლარამდე თითოეული დომენისთვის, რაც თავისთავად გამორიცხავს ფაქტიურად მიყენებული ზიანის მოთხოვნის საშუალებას.²³⁵ შეერთებული შტატების მოწესრიგება ყველა შესაძლო შემთხვევას ითვალისწინებს და ამოწურავს მას, შესაბამისად ქართულ სამართლებრივ სივრცეში სასურველია არსებობდეს ანალოგიური მიდგომა საკითხისადმი და მექანიზმი, რაც ადმინისტრაციული ორგანოს როლს სრულიად გამორიცხავდა მსგავსი ტიპის დავაში.

ალტერნატიულ მექანიზმებთან მიმართებაში საგულისხმოა, რომ საქართველოს ქვეყნის კოდის ზედა დონის დომენისთვის²³⁶ 2018 წელს მიღებული იქნა WIPO-ს დომენურ სახელებთან დაკავშირებული დავების მოგვარების პოლიტიკის ვარიაცია.²³⁷ რაც საშუალებას იძლევა დომენური დავების განსახილველად მოსარჩელემ მიმართოს WIPO-ს და დავა ერთიანი პოლიტიკის მიხედვით გადაწყდეს .GE დომენისთვის. აღნიშნულის უმთავრეს უპირატესობას წარმოადგენს დავის განხილვა კვალიფიციური სპეციალისტის მიერ, რომელსაც შესაბამისი მიმართულებით გააჩნია სპეციფიკური ცოდნა. ასევე, მნიშვნელოვანია, რომ ზემოგანხილული ადმინისტრაციული საჩივრის ფარგლებში დომენების რეგისტრანტი

²³³ Anticybersquatting Consumer Protection Act, (15 U.S.C. § 1125(d)). Section 2(a)(d)(1)(D)

²³⁴ იქვე, Section 3(a)(2).

²³⁵ იქვე, Section 3(b)(d).

²³⁶ ქვეყნის კოდის ზედა დონის დომენი იგივე country code top-level domain (ccTLD), საქართველოსთვის ასეთ აღმნიშვნელად გამოიყენება .GE.

²³⁷ .GE დომენურ სახელებთან დაკავშირებული დავების მოგვარების პოლიტიკა იხ. ბმულზე https://nic.ge/cdn/f/11/21/TqdWTM568E6syHk5mIF05g/GE_Domain_Name_Dispute_Resolution_Policy_GEO.pdf (ვიზიტის დრო: 07.07.2019)

უშუალოდ საჩივრის მხარე ვერ იქნებოდა, WIPO–ს შემთხვევაში საჩივრის უშუალო მოპასუხე რეგისტრანტად გვევალება, რაც კვალიფიციური არგუმენტაციისა და პასუხის/შესაგებლის წარდგენის შესაძლებლობას იძლევა რეგისტრანტისთვის. თუმცა UDRP-ს შემთხვევაშიც ზიანის მოთხოვნა ACPA-სგან განსხვავებით შეუძლებელია.²³⁸

აღსანიშნავია, რომ WIPO–ს მიერ განხილულ იქნა დავა²³⁹ .GE დომენურ სახელებთან დაკავშირებული დავების მოგვარების პოლიტიკის მიხედვით საქართველოს რეზიდენტი ფიზიკური პირის წინააღმდეგ, რომელმაც ცნობილი საკურიერო კომპანიის Glovo-ს სასაქონლო ნიშნის შემცველი დასახელებით დაარეგისტრირა ორი დომენი glovoapp.ge და glovo.ge. რომლების მიყიდვასაც იგი მოსარჩელე კომპანია Glovo–სთვის 10 000 ევროდ ცდილობდა, რაც ნათელია, რომ არაკეთილსინდისიერი განზრახვის უმთავრესი ელემენტია, რამაც მოპასუხის შეპასუხება, რომ დომენები საოჯახო ბიზნესისთვის უნდა გამოეყენებინა და მან Glovo–ს შესახებ საერთოდ არ იცოდა, გადაწონა. დავა მოსარჩელის სასარგებლოდ დასრულდა და მას ორივე დომენი გადაეცა.

ამრიგად უნდა ითქვას, რომ ზემოგანხილული შედარება ნათლად გვაჩვენებს მსგავსი ტიპის დავებისთვის მათი გადაწყვეტის სხვა მექანიზმების უპირატესობებს, ვიდრე ეს ადმინისტრაციული ორგანოს შემთხვევაში შეიძლება იყოს.

1.4. საავტორო უფლებები ინტერნეტში

მიუხედავად იმისა, რომ ქართული რეალობისთვის ინტერნეტი სიახლეს აღარ წარმოადგენს და შესაბამისად ინტერნეტ მეკობრეობაც მნიშვნელოვანი პრობლემაა, სამოქალაქო დავების პრაქტიკა აღნიშნული მიმართულებით ძალიან მცირეა.

მნიშვნელოვანია თბილისის საქალაქო სასამართლოს 2019 წლის 7 თებერვლის გადაწყვეტილება საქმეზე N2/26484-15, რომელიც საავტორო უფლებების ინტერნეტ სივრცეში დარღვევას ეხება.

დავის მიხედვით მოსარჩელე ელექტრონულ/ინტერნეტ მედია საშუალებას წარმოადგენს, რომელიც უნიკალურ კონტენტს ქმნის, რაც თავისთავად დაცულია საავტორო უფლებით და იგი ათავსებს აღნიშნულ მატერიალს

²³⁸ Singh H., Domain Name Disputes and Their Resolution under UDRP Route: A Review, Archives of Business Research, Vol.6, No.12, 2018, 154.

²³⁹ Glovoapp23, S.L. v. Ketevan Vadachkoria, WIPO, No. DGE2018-0001 (Nov. 8, 2018)

საკუთარ ვებ გვერდზე სტატიებისა და სიახლეების სახით, მოპასუხესაც თავის მხრივ გააჩნია ვებ გვერდი სადაც იგი მოსარჩელის მიერ შექმნილ კონტენტს ნებართვისა და შეთანხმების გარეშე ათავსებდა, სისტემატურად და დიდი მოცულობით.²⁴⁰ ასევე, აღსანიშნავია, რომ სასარჩელო მოთხოვნამ 259 908.25 ლარი შეადგინა.

მოცემული საქმე წინ წამოწევს ჩვენ მიერ უკვე განხილული ეგრეთ წოდებული უსაფრთხო ნავსადგომის (safe harbor) წესის არარსებობას ქართული სამართლებრივი სივრცისთვის, მიუხედავად იმისა რომ მოპასუხემ ვერ დაამტკიცა, რომ იგი არ ანთავსებდა მის გვერდზე მოსარჩელის მიერ შექმნილ სტატიებსა და სიახლეებს, არამედ მათ სრულიად გარეშე მესამე პირები აქვეყნებდნენ მოპასუხის საიტზე. მნიშვნელოვან სამართლებრივ პრობლემას წააწყდებოდა სასამართლო თუ მოპასუხე შეძლებდა დაემტკიცებინა, რომ საიტზე საავტორო უფლებით დაცულ მატერიალს გარეშე პირები ანუ მომხმარებლები აქვეყნებენ. ასეთი შემთხვევისთვისაც კი სასამართლო აღნიშნავს, რომ ეკონომიკურ შემოსავალს სწორედ მოპასუხე იღებს და მნიშვნელობა არ აქვს თუ ვინ განათავსებს დაცულ მატერიალს მის საიტზე უფლების დარღვევით,²⁴¹ რაც ნიშნავს იმას, რომ მხოლოდ ეკონომიკური სარგებლის მიღება პასუხისმგებლობის დაკისრების ერთადერთი პირობაა, რაც ცალსახად არასწორია. სასამართლომ სულ მცირე უნდა გაითვალისწინოს რამდენად ინფორმირებულია ადმინისტრაცია ვებ საიტზე განთავსებული უფლების დამრღვევი მატერიალის შესახებ²⁴² და უშუალოდ აკონტროლებს თუ არა იგი ეკონომიკურ შემოსავალს უფლება დამრღვევი მატერიალიდან.²⁴³ შესაბამისად აუცილებლად უნდა არსებობდეს ნორმატიული დანაწესი რომლის მიხედვითაც მკაფიოდ გამოირიცხება ინტერნეტ სერვისის პროვაიდერებისა და ვებგვერდების პასუხისმგებლობა მათი მომხმარებლების განხორციელებული ქმედებების გამო. რეკომენდაციის სახით კი შესაძლოა ზემოგანხილული ასპექტების გათვალისწინება კანონდებლობისთვის, რომელიც თავის მხრივ უცხო ქვეყნის უკვე დამკვიდრებულ ნორმატიულ მოწესრიგებას ეყრდნობა.

მნიშვნელოვანია ასევე თვითდახმარების (self-help) როლი აღნიშნულ დავაში. მოსარჩელეს წინასწარ ჰქონდა მითითებული თითოეული მასალის

²⁴⁰ თბილისის საქალაქო სასამართლოს 2019 წლის 7 თებერვლის გადაწყვეტილება საქმეზე N2/26484-15. ფაქტობრივი გარემოებები, პუნქტი 3.1.3.

²⁴¹ იქვე. ფაქტობრივი გარემოებები, პუნქტი 3.2.1.

²⁴² 17 U.S.C. § 512(c)(A).

²⁴³ იქვე, § 512(c)(1)(B).

ღირებულება საკუთარ ვებგვერდზე,²⁴⁴ რამაც მას გაუმარტივა, როგორც მტკიცების ტვირთი სასარჩელო მოთხოვნის მოცულობასთან დაკავშირებით, ასევე, ააცილა დამატებითი ხარჯი, რომელიც ექსპერტიზასა და სხვა მოქმედებებს დასჭირდებოდა მიყენებული ზიანის შესაფასებლად. ასევე, თვითდახმარებისა და მეორადი პასუხისმგებლობის აცილების მცდელობას წარმოადგენს მოპასუხის ქმედებაც, რომელიც იხსნიდა პასუხისმგებლობას მომხარებელთა გამოქვეყნებულ მასალაზე.²⁴⁵

აღნიშნულ დავაში სასარჩელო მოთხოვნა საერთო ჯამში 120 000 ლარით დაკმაყოფილდა, რისი ნორმატიული საფუძველიც საავტორო და მომიჯნავე უფლებების შესახებ 59-ე მუხლის 1 ნაწილის ვ-ქვეპუნქტით გათვალისწინებული ერთგვარი კომპენსაციაა, რომელიც მისაღები ფულადი ანაზღაურების ათმაგ ოდენობაზე ნაკლები არ უნდა იყოს, რაც თავის მხრივ ერთგვარ არასტანდარტულ სადამსჯელო კომპენსაციას²⁴⁶ (punitive damages) წარმოადგენს, რაც ქართული ნორმატიული ბაზისთვის უიშვიათეს მოვლენაა და ემსახურება პირთა ანალოგიური ქმედების პრევენციას. ასევე, საყურადღებოა რომ სასამართლო აღნიშნული დავისთვისაც სამოქალაქო კოდექსით გათვალისწინებულ დელიქტურ ნორმებს უსადაგებს დავის გარემოებებს.

დასკვნის სახით კი უნდა ითქვას, რომ აღნიშნული საქმე კიდევ ერთი ნათელი მაგალითია იმისა, თუ ინტერნეტ სივრცეში მიყენებული ზიანი, როგორი მასშტაბური შეიძლება იყოს, რასაც ისიც ემატება, რომ ისეთი უფლებების როგორცაა საავტორო უფლება, ინტერნეტ სივრცეში ხელყოფა გაცილებით მარტივია, რადგანაც დაცული მატერიალი ყველასთვის ხელმისაწვდომია ინტერნეტის ბუნებიდან გამომდინარე და იგი ნებისმიერი მომხმარებლისა თუ კონკურენტის მიერ შეიძლება იყოს გამოყენებული.

1.5. ონლაინ ცილისწამება

1.5.1. ნორმატიული საფუძვლების მისადაგება

საქართველოს სამოქალაქო კოდექსის მე-18 მუხლის მე-2 ნაწილის მიხედვით პირს უფლება აქვს დაიცვას საკუთარი პატივი, ღირსება, პირადი ცხოვრების

²⁴⁴ თბილისის საქალაქო სასამართლოს 2019 წლის 7 თებერვლის გადაწყვეტილება საქმეზე N2/26484-15. ფაქტობრივი გარემოებები, პუნქტი 3.1.3.

²⁴⁵ თბილისის საქალაქო სასამართლოს 2019 წლის 7 თებერვლის გადაწყვეტილება საქმეზე N2/26484-15. ფაქტობრივი გარემოებები, პუნქტი 3.1.6.

²⁴⁶ *Vijscher T. L.*, Tort Damages, Rotterdam Institute of Law and Economics (RILE) Working Paper Series No. 2008/02, 2008, 17-18.

საიდუმლოება, პირადი ხელშეუხებლობა ან საქმიანი რეპუტაცია სასამართლოს საშუალებით. სწორედ ამ ნორმატიულ დანაწესს უნდა შევუსაბამოთ ონლაინ დეფამაცია ქართულ სამართლებრივ რეალობაში. მნიშვნელოვანია ისიც, რომ კანონმდებელი მე-18 მუხლით მოაზრებულ დეფამაციურ ქმედებას უკავშირებს დელიქტურ საფუძვლებს, შესაბამისად სამოქალაქო კოდექსის 993-ე მუხლი პირს, რომელმაც განახორციელა ზიანის მომტანი ცნობების გავრცელება ან გახმაურება, აკისრებს წარმოშობილი ზიანის ანაზღაურებას. ერთი შეხედვით შესაძლოა ქართული სამართლებრივი სივრცისთვის ჩაითვალოს რომ ონლაინ დეფამაციის ტრანსფორმაცია იგივე გზით ხდება, როგორც ეს შეერთებული შტატების შემთხვევაშია, თუმცადა განსხვავებით მისგან საქართველოში სპეციფიკური განცალკევებული მოწესრიგება მსგავსად Communications Decency Act-ისა არ არის შემუშავებული.

1.5.2. მტკიცების ტვირთი

პრობლემურია ინტერნეტ სივრცეში ცილისმწამებლური განცხადებების გავრცელებაზე პასუხისმგებელი პირის განსაზღვრის მტკიცების ტვირთი,²⁴⁷ სიზუსტისთვის კი უნდა დაკონკრეტდეს, რომ აღნიშნული განსაკუთრებით ეხება ანონიმურად გავრცელებულ ცნობებს.

საქართველოს უზენაესი სასამართლოს 2013 წლის 10 ოქტომბრის გადაწყვეტილების მიხედვით საქმეზე Nას-1378-1300-2012, სასამართლო მკაფიოდ მიუთითებს რომ მოსარჩელემ მოპასუხის მიერ ინტერნეტში ცნობის გავრცელება უშუალოდ უნდა დაამტკიცოს და ამისთვის მხოლოდ იმაზე მითითება რომ დავის მხარეებს შორის დაძაბული ურთიერთობა არსებობს არ კმარა. სასამართლო, ასევე, ზოგადად ინტერნეტისა და ვებ გვერდების ბუნებაზე ამახვილებს ყურადღებას: „ინტერნეტში სადავო განცხადების განთავსების შესაძლებლობა გააჩნდა არა მხოლოდ მოპასუხეს, არამედ შესაბამის ვებ-გვერდზე დარეგისტრირებულ ნებისმიერ პირს“. რაც, ნამდვილად ანონიმურად ცნობების გავრცელების პრობლემურობას უსვამს ხაზს და ფაქტიურად მოსარჩელისთვის დაუძლეველ მტკიცების ტვირთს ქმნის.

განსხვავებულ პრაქტიკას ამკვიდრებს უზენაესი სასამართლო ისეთი შემთხვევისთვის როდესაც ინტერნეტში გავრცელებული ცნობების ავტორის იდენტიფიცირება შესაძლებელია. საქართველოს უზენაესი სასამართლოს

²⁴⁷ *ჯორბენაძე ს.*, სამოქალაქო კოდექსის ონლაინ კომენტარი, civilcode.ge, 2017, მუხლი 18 55-ე ველი.

2012 წლის 3 აგვისტოს გადაწყვეტილებით საქმეზე Nას-208-201-2012, დამკვიდრდა ერთგვარი პრეზუმფცია, რომ თუ ვებ გვერდის მომხმარებლის ანგარიში იძლევა ვარაუდს რომ იგი მოპასუხეს ეკუთვნის იგი უნდა ჩაითვალოს მის პირად ანგარიშად. ხოლო, მტკიცების ტვირთი კი სწორედ მასზე გადავა, ანგარიშის მისდამი კუთვნილების ნაწილში.

VI. დასკვნა

ნაშრომი მკითხველს ნათლად წარმოუდგენს იმ სამართლებრივ ტენდენციებსა და პრობლემატიკას, რომელიც განსახილველ საკითხს ახასიათებს და თანსდევს. იგი კონსტრუქციულად ცდილობს მისი მიზნის ამოწურვას, შესთავაზოს მკითხველს ინტერნეტ დელიქტის, როგორც სამართლებრივი მოვლენის შესაძლო დეფინიციები, რომელიც შესაძლოა უკვე არსებულ დელიქტურ ქმედებას უკავშირდებოდეს ან სულაც დელიქტური ქმედების ახალ სახეობას წარმოადგენდეს.

ნაშრომში შეგნებულად არის დათმობილი ძირითადი ნაწილის ორი საწყისი თავი შეერთებული შტატებისა და ევროპის კავშირის სამართლისთვის, რადგანაც მკითხველისთვის ისეთი ახალი საკითხი, რომელიც აქამდე არასდროს ყოფილა ქართულ იურიდიულ ლიტერატურაში განხილული, მნიშვნელოვნად წარმოჩენილი და აღქმადი იყოს. არასწორი იქნებოდა საკითხის პირდაპირ ქართული სამართლის არსებული მდგომარეობით განხილვა, რადგანაც სასამართლო და არასასამართლო პრაქტიკის გარდა მისდამი არც ნორმატიული და არც დოქტრინალური მიდგომა არ არსებობს, რაც ნაშრომში წარმოდგენილ მრავალ კითხვას პასუხგაუცემელს დატოვებდა.

ზემოგანხილულის მიუხედავად ნაშრომი უცხო სამართლისთვისაც კი მკითხველს საჭირო შემთხვევებში კრიტიკულ მიდგომას სთავაზობს. რისი თვალსაჩინო მაგალითიც შეიძლება იყოს შეერთებული შტატებისთვის, სამოქალაქო პასუხისმგებლობის გამომრიცხველი ეკონომიკური დანაკარგების დოქტრინის ჩანაცვლება განჭვრეტადობის დოქტრინით. ხოლო, ევროპის კავშირისთვის კი ე.წ. ფორუმ შოპინგის კრიტიკა.

ქართული სამართლებრივი სივრცისთვის კი კვლევა მკითხველს, სთავაზობს როგორც უმნიშვნელოვანეს სასამართლო და არასასამართლო პრაქტიკას, ასევე, მათ პარალელურად განიხილავს შესაძლო სამომავლო ნორმატიული მოწესრიგების რეკომენდაციასაც. ასევე, შეიძლება ითქვას, რომ ნაშრომი

საკითხით დაინტერესებული იურისტებისთვის ერთგვარ საორიენტაციო კვლევას წარმოადგენს, რომელიც, როგორც გზამკვლევი ეყრდნობა უცხოენოვანი იურიდიული ლიტერატურის უმნიშვნელოვანეს ნაშრომებს მოცემულ საკითხთან მიმართებაში და სასამართლო პრაქტიკას.

ნორმატიულ მოწესრიგებასთან დაკავშირებით აუცილებლად გათვალისწინებული უნდა იქნეს ნაშრომში შემოთავაზებული რეკომენდაციები, რომელიც თავის მხრივ უმეტესად შეერთებული შტატების საკანონმდებლო ბაზას ეყრდნობა, ასევე, ავტორისეულ პრაქტიკულ სამართლებრივ კვლევას სხვადასხვა ინტერნეტ გვერდის სამართლებრივ პოლიტიკაზე.

მართალია, ქართული იურიდიული ლიტერატურა არ მსჯელობას ინტერნეტ სირცემი წარმოშობილ ზიანსა და მასთან დაკავშირებულ სამოქალაქო პასუხისმგებლობაზე, სასამართლო პრაქტიკა განსახილველი მიმართულებით უკვე არსებობს და აღსანიშნავია, რომ დავის მოცულობა ზოგ შემთხვევაში რამდენიმე ასეულ ლარსაც კი შეადგენს, რაც თემის აქტუალობას კიდევ ერთხელ უსვამს ხაზს. თუმცადა იურიდიული ლიტერატურის არ არსებობა, თავისთავად დროთა განმავლობაში გამოიწვევს იმას, რომ სასამართლო გადაწყვეტილებებსა თუ განჩინებებში თეორიული საყრდენის მნიშვნელოვანი პრობლემურობა წარმოიშობა.

განხილული საკითხის კიდევ ერთი პრაქტიკული მნიშვნელობა საქართველოსთვის საზოგადოების დამოკიდებულებაა ინტერნეტის მიმართ, გარდა პოზიტიური ასპექტებისა, რაც კომუნიკაციისა და სხვადასხვა ტრანზაქციის სიმარტივეს უკავშირდება, მის მომხარებლებს ნეგატიური ქმედების სიმარტივისა და შესაბამისი პასუხისმგებლობის არდაკისრების ვარაუდს უქმნის, რაც ნათლად გამოჩნდა ჩვენ მიერ განხილული ქართულ სასამართლო პრაქტიკის მიხედვით, სადაც ორი კომპანიისთვის ინტერნეტ სივრცე არაკეთილსინდისიერი კონკურენციის პლატფორმად და ასპარეზად გადაიქცა.

ნაშრომში, ასევე, ნათლად ჩანს ფიზიკური სამყაროსა და ვირტუალური სამყაროს კვეთა, მიუხედავად იმისა რომ სამართლებრივი ანალიზი მხოლოდ ინტერნეტ სივრცეში მიყენებულ ზიანს ეხება. რისი ნათელი მაგალითიცაა ინტერნეტის ბუნების მოძრავი და უძრავი ნივთების მახასიათებლებთან ტრანსფორმაცია. უფრო კონკრეტულად კი შეერთებული შტატების იურიდიულ ლიტერატურაში განვითარებული მოსაზრება, რომ ინტერნეტისთვის იგივე სამართლებრივი მოწესრიგება უნდა იქნეს ხელყოფისგან დაცვის ნაწილში, როგორც ეს უძრავი ნივთებისთვისაა.

ამრიგად საბოლოო დასკვნის სახით უნდა ითქვას, რომ განსახილველი საკითხის კიდევ უფრო აქტუალურად და მნიშვნელოვნად გადაქცევა გარდაუვალია, როგორც მსოფლიოსთვის, ასევე, საქართველოსთვის, გამომდინარე იქიდან, რომ ინტერნეტ სივრცე სულ უფრო და უფრო იზრდება. მისი როლი როგორც სოციუმის განვითარებაში, ასევე, ბიზნესისთვისა და ელექტრონული კომერციისთვის შეუცვლელია, რაც ნათელია, ზიანის მომტან ქმედებებთან მჭიდროდ არის დაკავშირებული და სპეციალურ სამართლებრივ ჩარჩოში მოქცევას საჭიროებს.

ბიბლიოგრაფია

ლიტერატურა

ქოჩაშვილი ქეთევან, ბრალი, როგორც სამოქალაქო სამართლებრივი პასუხისმგებლობის პირობა, სამართლის ჟურნალი, #1, თბილისი 2009.

ცვაიგერტი კონრად/ კოტცი ჰაინ/ ნინიძე თედო (რედ), შედარებითი სამართალმცოდნეობის შესავალი კერძო სამართლის სფეროში, ტ. 2, ჯისიაი, თბილისი 2001.

ჯორბენაძე სერგი, სამოქალაქო კოდექსის ონლაინ კომენტარი, 2017, მუხლი 18.

American Law Institute, Restatement of the Law Third, Torts: Products Liability, 1998.

American Law Institute, Restatement of the Law Second, Torts, Volume 1, 1965.

Anzivino Ralph A., The False Dilemma of the Economic Loss Doctrine, Marquette Law Review, Vol. 93, 2010.

Ardia David S., Freedom of Speech, Defamation, and Injunctions, William & Mary Law Review, Vol. 55, 2013.

Asp Emily M., Section 512 of the Digital Millennium Copyright Act: User Experience and User Frustration, Iowa Law Review, Edition 103, Issue 2, 2018.

Balganesh Shyamkrishna, Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass, Michigan Telecommunications and Technology Law Review, Vol. 12, 2006.

Barbantonis Nicholas Foss, Should Contributory Cybersquatting be Actionable?, North Carolina Journal of Law & Technology, Vol. 17, Issue 1, 2015.

Bellia Patricia L., Defending Cyberproperty, New York University Law Review, Vol. 79, 2004.

Bogdan Michael, Torts in Cyberspace - The Impact of the New Regulation "Rome II", Masaryk University Journal of Law and Technology, Vol. 2, No 1, 2008.

Butler Alan, Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, University of Michigan Journal of Law Reform, Vol. 50, Issue 4, 2017.

Calandrillo Steve P. / Davison Ewa M., The Dangers of the Digital Millennium Copyright Act: Much ado About Nothing?, William & Mary Law Review, Vol. 50, Issue 2, 2008.

Carrier Michael A. /Lastowka Greg, Against Cyberproperty. Berkeley Technology Law Journal, Vol. 22, 2007.

Chandler A. Jennifer, Technological Self-Help and Equality in Cyberspace, McGill Law Journal, Vol. 56, Number 1, 2010.

Childers Seldon J., Don't Stop the Music: No Strict Products Liability for Embedded Software, University of Florida Journal of Law and Public Policy, Vol. 19, 2008.

Citron Danielle Keats., Cyber Civil Rights, Boston University Law Review, Vol. 89:61, 2009.

Curtin Thomas J., The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites, Journal of Law and Policy Vol. 19, Issue 1, 2010.

Elvy Stacy-Ann, The Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?, Washington and Lee Law Review, Vol. 74:1, 2017.

Elvy Stacy-Ann, Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond, Hofstra Law Review, Vol. 44, 2016.

Epstein Richard, Cybertrespass, University of Chicago Law Review: Vol. 70, Iss. 1, Article 6, 2003.

Fairfield Joshua, Virtual Property, Boston University Law Review, Volume 85, 2005.

Garon Jon M., Tidying up the Internet: Take Down of Unauthorized Content under Copyright, Trademark and Defamation Law, Capital University Law Review, Vol. 41, 2013.

Gonçalves Anabela Susana De Sousa, The Application of the General Rule of the Rome II Regulation to Internet Torts, Masaryk University Journal of Law and Technology, Vol 8, No 1, 2014.

Guicheteau Lauren, What Is the Media in the Age of the Internet? Defamation Law and the Blogosphere, Washington Journal of Law, Technology & Arts, Vol. 8, Issue 5, 2013.

Hartley Trevor C., Jurisdiction in tort claims for non-physical harm under Brussels 2012, International and Comparative Law Quarterly, Vol. 67, 2018.

Hedley Steve, Cybertrespass – A Solution in Search of a Problem?, *Journal of European Tort Law*, Vol. 5, Issue 2, 2014.

Helper Laurence R. / Dinwoodie Graeme B., Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy, *William & Mary Law Review*, Vol. 43, 2001.

Horton Allison E., Beyond Control?: The Rise and Fall of Defamation Regulation on the Internet, *Valparaiso University Law Review*, Vol. 43, Number 3, 2009.

Hylton Keith N., *Tort Law: A Modern Perspective*, Cambridge University Press, Cambridge 2016.

Hylton Keith N., Property Rules, Liability Rules, and Immunity: An Application to Cyberspace, *Boston University Law Review*, Vol. 87:1, 2007.

Joubert Natalie, Cyber-Torts and Personal Jurisdiction: The Paris Court of Appeal Makes a Stand, *The International and Comparative Law Quarterly*, Vol. 58, No. 2, 2009.

Keamey Daniel, Network Effects and the Emerging Doctrine of Cybertrespass, *Yale Law & Policy Review*, Vol. 23, Issue 1, 2005.

Kerr Orin S. / Schneier Bruce, Encryption Workarounds, *Georgetown Law Journal*, Vol. 106, Issue 4, 2018.

Kesan Jay P. / Hayes Carol M., Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, *Harvard Journal of Law & Technology*, Vol. 25, Number 2, 2012.

Lastowka Greg, Decoding Cyberproperty, *Indiana Law Review*, Vol. 40, No. 1, 2007.

Lichtman Douglas Gary/ Posner Eric, Holding Internet Service Providers Accountable, *The Law and Economics of Cybersecurity*, ed. *Grady M./ Parisi F.*, 2006.

Lipton Jacqueline D., Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy, *Wake Forest Law Review*, Vol. 40, 2005.

Loos Thomas J., Fair Use and the Digital Millennium Copyright Act, *Michigan Telecommunications and Technology Law Review*, Vol. 13, Issue 2, 2007.

Lutzi Tobias, Internet Cases in EU Private International Law Developing a Coherent Approach, *International & Comparative Law Quarterly*, Vol. 66, Issue, 2017.

Mercer John D., Cybersquatting: Blackmail on the Information Superhighway, Journal of Science & Technology Law, Vol. 6, Notes, 2000.

Mierina A., Some reflections on non-contractual obligations in cyberspace considering the Rome II regulation, SHS Web of Conferences Vol. 10. Article 00023, 2014.

Miller Roger LeRoy, Business Law Today, Standard: Text & Summarized Cases, 11th Edition, Cengage Learning, Boston 2015.

Mosier Gregory/Fitzgerald Tara, Cyber Torts: Common Law and Statutory Restraints in the United States, Journal of International Commercial Law and Technology, Vol.2, Issue 1, 2007.

Nguyen Xuan-Thao, Blame It On the Cybersquatters: How Congress Partially Ends the Circus Among the Circuits with the Anticybersquatting Consumer Protection Act, Loyola University Chicago Law Journal, Vol. 32, 2001.

Oster Jan, Rethinking Shevill. Conceptualising the EU private international law of Internet torts against personality rights, International Review of Law, Computers & Technology, 6:2-3, 2012.

Owen David G., Bending Nature, Bending Law, Florida Law Review, Vol. 62, Number 3, 2010.

Paez Mauricio/La Marca Mike, The Internet of Things: Emerging Legal Issues for Businesses, Northern Kentucky Law Review, Vol. 43, Number 1, 2016.

Peppet Scott R., Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Texas Law Review, Vol. 93, 2014.

Perry Ronen/ Zarsky Tal, Who Should Be Liable for Online Anonymous Defamation?, University of Chicago Law Review Dialogue, Vol. 82, 2015.

Rauscher Thomas, Internationales Privatrecht: Mit internationalem Verfahrensrecht, C.F. Müller, Heidelberg 2017.

Rustad Michael L., Global Internet Law in a Nutshell, 3rd edition, West Academic, St. Paul 2016.

Rustad Michael L., Global Internet Law, West Academic Publishing, St. Paul 2014.

Rustad Michael L. / Koenig Thomas H., The Tort of Negligent Enablement of Cybercrime, Berkeley Technology Law Journal, Vol. 20, Issue 4, 2005.

Sag Matthew, Internet Safe Harbors and the Transformation of Copyright Law, Notre Dame Law Review, Vol. 93, Issue 2, 2018.

Sales Nathan Alexander, Regulating Cyber-Security, Northwestern University Law Review, Vol.107, No. 4, 2013.

Savin Andrej, EU Internet Law, Edward Elgar Publishing, Cheltenham/Northampton 2013.

Savin Andrej, Jurisdiction Over Cybertorts in the EU–A Coherent Picture?, Liber amicorum: Gašo Knežević, ed. *Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016.

Savin Andrej, Jurisdiction Over Cybertorts in the EU–A Coherent Picture?, Liber amicorum: Gašo Knežević, ed. *Varandy T.*, Faculty of Law, University of Belgrade, Belgrade 2016.

Schulte Christopher J., The New Anticybersquatting Law and uniform Dispute Resolution Policy for Domain Names, Tort & Insurance Law Journal, Vol. 36, 2000.

Schwartz Victor E., Remoteness Doctrine: A Rational Limit on Tort Law, Cornell Journal of Law and Public Policy, Vol. 8, Issue 3, 1999.

Scott Michael D., Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, Maryland Law Review, Vol. 67, Issue 2, 2008.

Sharkey Catherine M., Trespass Torts and Self-Help for an Electronic Age, Tulsa Law Review, Vol. 45, 2010.

Sharkey Catherine M., In Search of the Cheapest Cost Avoider: Another View of the Economic Loss Rule, University of Cincinnati Law Review, Vol. 85, 2018.

Singh Harman Preet, Domain Name Disputes and Their Resolution under UDRP Route: A Review, Archives of Business Research, Vol.6, No.12, 2018.

Smith Bryant Walker, Proximity-Driven Liability, Georgetown Law Journal, Vol. 102, 2014.

Smith Graham, Internet Law and Regulation, Sweet & Maxwell, London 2007.

Štárek Martin, Brussels I: Recent Developments in the Interpretation of Special Jurisdiction Provisions for Internet Torts, Masaryk University Journal of Law and Technology, Vol. 9, 2015.

Świerczyński Marek, Electronic torts/delicts in the Rome II regulation, Tort Law in Poland, Germany and Europe, eds. *Heiderhoff B./ Zmij G.*, sellier. European law publishers, Munich 2009.

Vihul Liis, The Liability of Software Manufacturers for Defective Products, Tallinn Paper No. 2, NATO Cooperative Cyber Defence Centre of Excellence, 2014.

Visscher Louis T., Tort Damages, Rotterdam Institute of Law and Economics (RILE) Working Paper Series No. 2008/02, 2008.

Walczak Christine A., The New and Evolving Tort of Contributory Cybersquatting: Did the Courts Get it Right?, University of Illinois Journal of Law, Technology & Policy, Vol. 2012, 2012.

Wong Mary, Cyber-trespass and 'Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience, International Journal of Law and Information Technology, Vol. 15, Issue 1, 2007.

სასამართლო პრაქტიკა

საქართველო

საქართველოს უზენაესი სასამართლოს 2000 წლის 11 ოქტომბრის განჩინება საქმეზე №: 3კ/589.

საქართველოს უზენაესი სასამართლოს 2012 წლის 3 აგვისტოს გადაწყვეტილება საქმეზე Nას-208-201-2012.

საქართველოს უზენაესი სასამართლოს 2013 წლის 10 ოქტომბრის გადაწყვეტილება საქმეზე Nას-1378-1300-2012.

თბილისის საქალაქო სასამართლოს 2017 წლის 8 მაისის გადაწყვეტილება საქმეზე No2/30577-16.

თბილისის საქალაქო სასამართლოს 2019 წლის 7 თებერვლის გადაწყვეტილება საქმეზე N2/26484-15.

ამერიკის შეერთებული შტატები

Ji Chang Son v. Tesla Motors, Inc (8:16-cv-02282), California Central District Court. (Filed 2016).

Wausau Tile, Inc. v. County Concrete Corp. N.W.2d, 452 (1999).

Express Airlines, Inc. v. Consolidated Rail Corp., 495 A.2d 107 (N.J. 1985).

Compuserve Inc. v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997).

eBay, Inc. v. Bidder's Edge LLC, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559 (4th Dist. 1996).

O'Grady v. Superior Court, 139 Cal. App. 4th 1423, 44 Cal. Rptr. 3d 72 (Cal. App. 6 Dist. 2006).

Mortg. Specialists, Inc. v. Implode-Explode Heavy Indus., Inc., 160 N.H.227, 999 A.2d 184 (N.H. 2010).

New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

Intermatic Inc. v. Toepfen, 947 F. Supp. 1227 (N.D. Ill. 1996).

Petroliam. Nasional Berhad v. GoDaddy.com, Inc., 737 F.3d 546, 548 (9th Cir. 2013).

ევროპის კავშირი

C-68/93 Shevill and Others v Presse Alliance ECLI:EU:C:1995:61 (1995).

Joined Cases C-509/09 and C-161/10. eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited ECLI:EU:C:2011:192 (2011).

Case C-523/10 Wintersteiger AG v Products 4U Sondermaschinenbau GmbH ECLI:EU:C:2012:220 (2012).

Case C-170/12 Peter Pinckney v KDG Mediatech AG ECLI:EU:C:2013:635 (2013).

არასასამართლო პრაქტიკა

საქართველოს კომუნიკაციების ეროვნული კომისიის 2017 წლის 30 ნოემბრის გადაწყვეტილება N 793 / 16

Dow Jones & Company, Inc. and Dow Jones LP v. John Zuccarini, WIPO, No. D2000-0578 (Aug. 28, 2000)

Diageo plc v. John Zuccarini, Individually and t/a Cupcake Patrol, WIPO, No. D2000 – 0996 (Oct. 22, 2000)

Glovoapp23, S.L. v. Ketevan Vadachkoria, WIPO, No. DGE2018-0001 (Nov. 8, 2018)

სამართლებრივი აქტები

საქართველო

საქართველოს კანონი. საავტორო და მომიჯნავე უფლებების შესახებ

საქართველოს სამოქალაქო კოდექსი

საქართველოს კომუნიკაციების ეროვნული კომისიის 2006 წლის 17 მარტის დადგენილება №3

ამერიკის შეერთებული შტატები

Communications Decency Act – კომუნიკაციურ კავშირში ეთიკურობის შესახებ კანონი

Anticybersquatting Consumer Protection Act – მომხმარებელთა დაცვის კანონი ანტი-კიბერსკვათინგის შესახებ

Digital Millennium Copyright Act – კანონი საავტორო უფლებების შესახებ ციფრულ ეპოქაში

ევროპის კავშირი

Regulation (EU) No 1215/2012 (Brussels I Regulation (recast) – რეგულაცია ბრიუსელი I

Regulation (EC) No 864/2007 (Rome II Regulation) - რეგულაცია რომი II

ინტერნეტ რესურსები

სტატისტიკა ინტერნეტ მომხმარებლების რაოდენობის შესახებ – <https://datareportal.com/reports/digital-2019-global-digital-overview> (ვიზიტის დრო: 24.06.2019)

სტატისტიკა ინტერნეტთან დაკავშირებული მოწყობილობების შესახებ – <https://techjury.net/blog/how-many-iot-devices-are-there/> (ვიზიტის დრო: 24.06.2019)

სტატისტიკა ინტერნეტ დომენების რაოდენობის შესახებ – <https://domainnamestat.com/statistics/overview> (ვიზიტის დრო: 24.06.2019)

Google Home-ის შესახებ – https://store.google.com/product/google_home (ვიზიტის დრო: 24.06.2019)

Plant R./ Topham C., How Tesla, Nest And Medtronic Are Using IoT-Derived Data To Move Their Businesses Forward, Forbes. – <https://www.forbes.com/sites/insights-hitachi/2018/06/12/how-tesla-nest-and-medtronic-are-using-iot-derived-data-to-move-their-businesses-forward/#3b646f0a487a> (ვიზიტის დრო: 24.06.2019)

Kaspersky Lab research, https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report (ვიზიტის დრო: 24.06.2019)

YouTube-ის პოლიტიკა – <https://www.youtube.com/intl/en-GB/yt/about/policies/> (ვიზიტის დრო: 24.06.2019)

WIPO UDRP სტატისტიკა წლების მიხედვით – <https://www.wipo.int/amc/en/domains/statistics/cases.jsp> (ვიზიტის დრო: 24.06.2019)

YouTube-ზე შეტყობინებისა და წაშლის რეჟიმის შესახებ – <https://support.google.com/youtube/answer/2807622> (ვიზიტის დრო: 24.06.2019)

United States Attorney, Southern District of New York, 'Cyber scammer' Sentenced to 30 Months for Using Deceptive Internet Names to Mislead Minors to X-Rated Sites, February 26, 2004, – <https://www.justice.gov/archive/criminal/cybercrime/press-releases/2004/zuccariniSent.htm>

2003 წლის 29 აგვისტოს საგაომიებო ჩვენება და დაკავების ბრძანება საქმეზე United States v. John Zuccarini – <http://dnattorney.com/United%20States%20of%20America%20v.%20John%20Zuccarini.pdf>

GE დომენურ სახელებთან დაკავშირებული დავების მოგვარების პოლიტიკა – https://nic.ge/cdn/f/11/21/TqdWtM568E6syHk5mIF05g/GE_Domain_Name_Dispute_Resolution_Policy_GEO.pdf (ვიზიტის დრო: 07.07.2019)