

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

გიორგი ჟორჟოლიანი

ადვოკატი, საქართველოს ადვოკატთა ასოციაციის ინტელექტუალური საკუთრების სამართლის კომიტეტის წევრი

I. შესავალი

ინტერნეტ სივრცეში განვითარებული ურთიერთობები ძირითად შემთხვევაში აღიქმება როგორც მხოლოდ ტექნოლოგიური ინოვაციის ნაწილი და ექსკლუზიურად მასთან ასოცირებული მოვლენა, რაც, რაღა თქმა უნდა, არ შეესაბამება ობიექტურ რეალობას, ინტერნეტი მჭიდროდ არის დაკავშირებული სხვადასხვა სამართალურ თიერთობასთან. წინამდებარე სტატია ისეთ უმნიშვნელოვანეს საკითხს შეეხება, როგორცაა ინტერნეტსივრცეში წარმოშობილი ზიანი და მასზე გავრცელებული სამოქალაქო სამართლებრივი პასუხისმგებლობა, უფრო ზუსტად კი იგი ინტერნეტ დელიქტების სამართლებრივ ანალიზს მოიცავს.

ინტერნეტსივრცე ციფრული რეკლუციის უდიდეს და უმნიშვნელოვანეს ნაწილს იკავებს და იგი თანამედროვე ადამიანის ყოფიერების განუყოფელ ნაწილადაა ქცეული. შესაბამისად, ინტერნეტსივრცეში განხორციელებული ზიანის მომტანი ქმედება აქტუალურ სამართლებრივ საკითხად გადაიქცა მთელი მსოფლიოსთვის. ინტერნეტში განხორციელებული ნებისმიერი ქმედება, დაწყებული სოციალურ ქსელში გაკეთებული განცხადებით, დამთავრებული პროგრამული უზრუნველყოფის წარმოებით შესაძლოა სამოქალაქო პასუხისმგებლობის დაკისრების წყარო იყოს. სწორედ ამიტომ ინტერნეტის ბუნება ხშირად საშიშ და უკონტროლო მოვლენად გვევლინება. შესაბამისად, განსახილველი თემა უაღრესად საინტერესოა როგორც ტექნოლო-

გიური, ისე სამართლებრივი კუთხით, განსაკუთრებით კი საქართველოსთვის, სადაც აღნიშნულ საკითხს იურიდიულ ლიტერატურა არ მოიცავს.

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.² 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 კონკურენციასა და კიბერუსაფრთხოებაზე.³ ინტერნეტ დელიქტი მჭიდროდ არის დაკავშირებული თანამედროვე ტექნოლოგიურ ინდუსტრია-სთან, გამომდინარე იქიდან, რომ ის დროთა განმავლობაში უფრო მეტად ინტერნეტ სივრცეზე არის ორიენტირებული, ასევე, მნიშვნელოვანი ურთიერთკავშირი აქვს ინტერნეტ დელიქტებსა და ელექტრონულ კომერციას, ზოგადად ნებისმიერ ინტერნეტ ტრანზაქციას. შესაბამისად ელექტრონუ-

¹ 2019 წლისთვის ინტერნეტ მომხმარებლების საერთო რაოდენობა 4 მილიარდზე მეტს შეადგენს, პერსონალური კომპიუტერების გარდა ინტერნეტთან დაკავშირებული მოწყობილობების რაოდენობა 13 მილიარდს აღწერს, ხოლო, რეგისტრირებული ინტერნეტ დომენების რაოდენობა 350 მილიონამდეა. დეტალური სტატისტიკა იხ. ბმულზე <https://datareportal.com/reports/digital-2019-global-digital-overview/>; <https://techjury.net/blog/how-many-iot-devices-are-there/>; <https://domainnamestat.com/statistics/overview>.

² 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.
³ Rustad M. L., Global Internet Law, West Academic Publishing, St. Paul 2014, 112.

ლი კომერციის მასშტაბების ზრდა იწვევს ინტერნეტ დელიქტების რიცხვის მატებასაც.⁴

სახელდებასთან დაკავშირებით უნდა აღინიშნოს, რომ ინტერნეტ დელიქტი საქართველოსთვის უფრო მეტად გასაზიარებელია, ავსტრია⁵ და გერმანიის⁶ მსგავსად (Internetdelikt), ვიდრე კიბერ დელიქტი (Cyber Tort),⁷ რომელიც ხშირად მოიცავს ციფრულ დელიქტებსაც, რისთვისაც ინტერნეტის არსებობა სავალდებულო ელემენტს არ წარმოადგენს.

სტატიაში საკითხთან დაკავშირებით წარმოდგენილია სამი სამართლებრივი სივრცე. ამერიკის შეერთებული შტატებისთვის უშუალოდ ინტერნეტ დელიქტების სამართლებრივი ანალიზი განხილული. ევროპის კავშირის მიხედვით ინტერნეტ დელიქტებთან დაკავშირებული განსჯადობისა და გამოსაყენებელი სამართლის პრობლემატიკა, ხოლო საქართველოს, როგორც ბოლო სამართლებრივი სივრცის ანალიზისთვის შედარებით—სამართლებრივი დისკურსის ფარგლებშია მოცემული სასამართლო პრაქტიკა.

II. ინტერნეტ დელიქტების რეგულაცია ამერიკის შეერთებულ შტატებში

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 ჩნდება 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)⁸ და ის შესაძლოა დელიქტური ქმედების წყაროს წარმოადგენდეს. აღსანიშნა-

ვია, რომ ნივთების ინტერნეტის ერთიანი ცნება თუ კონცეფცია არ არსებობს,⁹ მიუხედავად ამისა, ნივთების ინტერნეტის კატეგორიზაცია შემდეგი მიმართულებებით არის შესაძლებელი: ჯანმრთელობისა და ფიტნესის სენსორები, ავტომობილის თვითმართვადი სისტემები, ჭკვიანი სახლის სისტემები, დასაქმებულთა მონიტორინგის სისტემები და პროგრამული უზრუნველყოფა, რომელიც იძლევა ნივთების ინტერნეტის მართვის საშუალებას სმარტფონებისა და კომპიუტერების საშუალებით.¹⁰ მიუხედავად ამისა, უშუალოდ კომპიუტერები და სმარტფონები არ არის მოაზრებული, როგორც ნივთების ინტერნეტის ნაწილი.¹¹

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.¹² რთულია იმის თქმა თუ IoT და პროგრამული უზრუნველყოფა რამდენად აყენებს ზიანს სოციალურ კეთილდღეობას, თუმცა ორივე უდავოდ შეიძლება მოვიაზროთ, როგორც დელიქტური ვალდებულების ახალი წყარო პროდუქტის მწარმოებლისთვის, რიგ შემთხვევაში გამყიდვლისთვისა და მიმწოდებლისთვის, რადგანაც სწორედ მათი წარმოებული გემოგანხილული 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.¹³ ინტერნეტ დელიქტთან მიმართებაში წუნდებული პროდუქტის ობიექტებად განხილული უნდა იქნეს პროგრამული უზრუნველყოფა (software) და ნივთების ინტერნეტი (Internet of Things, IoT).

⁴ 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.

⁵ OGH 10.7.2012, 4 Ob 82/12f.MR 2012, 343.

⁶ Rauscher T., Internationales Privatrecht: Mit internationalem Verfahrensrecht, C.F. Müller, Heidelberg 2017, 368.

⁷ 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.

⁸ 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).

⁹ Paez M./La Marca M., The Internet of Things: Emerging Legal Issues for Businesses, Northern Kentucky Law Review, Vol. 43, Number 1, 2016, 31.

¹⁰ Peppet S. R., Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Texas Law Review, Vol. 93, 2014, 98.

¹¹ Paez M./La Marca M., The Internet of Things: Emerging Legal Issues for Businesses, Northern Kentucky Law Review, Vol. 43, Number 1, 2016, 31.

¹² Citron D. K., Cyber Civil Rights, Boston University Law Review, Vol. 89:61, 2009, 62.

¹³ Sales N. A., Regulating Cyber-Security, Northwestern University Law Review, Vol.107, No. 4, 2013, 1533.

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

მწარმოებელი, გამყიდველი ან მიმწოდებელი, რომელიც წუნდებულ პროდუქტს ყიდის ან მისი დისტრიბუციითა დაკავებული, პასუხისმგებელია მიყენებული ზიანისთვის, რომელიც ასეთმა პროდუქტმა გამოიწვია.¹⁴ კომერციული ჯაჭვის მონაწილეებს პასუხისმგებლობა უშუალოდ საკუთარი წუნდებული კონტრიბუციისთვის ეკისრებათ. ამასთან ამერიკული დელიქტური სამართალი, წუნდებული პროდუქტისთვის ავითარებს სამ შესაძლო შეთხვევას. პირველი ესაა საწარმოო წუნი (manufacturing defect),¹⁵ მეორე კონსტრუქციული წუნი (design defect),¹⁶ ხოლო, მესამე კი არგაფრთხილების შემთხვევაა (failure to warn).¹⁷

პროგრამული უზრუნველყოფისთვის და ნივთების ინტერნეტისთვის, როგორც წუნდებული პროდუქტისთვის განხილული უნდა იქნეს მათი კიბერუსაფრთხოების საკითხი, რადგანაც ინტერნეტთან დაკავშირებული მოწყობილობები კიბერშეტევების მიმართ ხშირად უძლურნი არიან.¹⁸

პროგრამული უზრუნველყოფა წარმოებისას გადის რამდენიმე ეტაპს, ესენია, კონსტრუქციის, იგივე საერთო კოდის შერჩევისა და პროექტირების, პროგრამული კოდის შექმნის, გამოცდისა და ბოლოს, გამრავლებისა და დისტრიბუციის ეტაპი. ნათელია, რომ კოდის შექმნის ეტაპზე ხარვეზი ჩაითვლება კონსტრუქციის წუნად, ხოლო, გამრავლების

ეტაპზე ინდივიდუალური გაუმართაობა კი საწარმოო წუნად. შესაბამისად კოდირების ეტაპზე პროგრამული უზრუნველყოფისთვის ნაკლოვანი კიბერუსაფრთხოების შერჩევა კონსტრუქციის წუნად უნდა იქნეს მიჩნეული.¹⁹ თუმცაღა მომხმარებელთა პოზიციიდან, კოდის შექმნის ეტაპზე დეფექტი შეიძლება მოიპოვებოდეს როგორც საწარმოო წუნი, რაც თავის მხრივ, მკაცრი პასუხისმგებლობის დელიქტთანაა დაკავშირებული.²⁰ ეს უკანასკნელი მოსაზრება არ უნდა იქნეს გაზიარებული, რადგანაც მკაცრი პასუხისმგებლობიდან გამოწვეული ზიანის ანაზღაურების მოცულობა, მწარმოებლების წარმადობას აწარმოონ ახალი პროდუქტი მნიშვნელოვნად შეამცირებს, შესაბამისად, პროდუქტის წარმოების სოციალური სიკეთე გადაწონის მკაცრი პასუხისმგებლობის გამოყენების აუცილებლობას.²¹

ნივთების ინტერნეტისთვისაც გაზიარებული უნდა იქნეს კონსტრუქციის წუნი, გამომდინარე იქიდან, რომ ნივთების ინტერნეტის მთავარი ბირთვი პროგრამული უზრუნველყოფა და დელიქტური პასუხისმგებლობის წყარო სწორედ მისი დაუცველობაა.²² თავის მხრივ, აღნიშნული შესაძლოა ტექნიკური ნაწილების (hardware) მიზეზითაც იყოს გამოწვეული, ხშირად პროდუქტის შემადგენლობა იმდენად პატარაა, რომ მათ მწარმოებლებს უბრალოდ არ ჰყოფნით სიმძლავრე მოწყობილობაში განათავსონ ისეთი უსაფრთხოების ზომები, როგორცაა მონაცემთა დაშიფრვა,²³ ასევე, IoT მოწყობილობები, განსხვავებით სმარტფონებისა და კომპიუტერებისა, არ ექვემდებარებიან დისტანციურ განახლებასა და გაუმჯობესებას,²⁴ თუმცაღა ეს უკანასკნელი

¹⁴ American Law Institute, Restatement of the Law Third, Torts: Products Liability, 1998, §1.

¹⁵ საწარმოო წუნის დროს 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, აღნიშნულს უკავშირდება მკაცრი პასუხისმგებლობის (strict liability) დოქტრინა, რომლის დროსაც მოსარჩელე არაა ვალდებული მოთხოვნის დასაკმაყოფილებლად დაამტკიცოს მოპასუხის ბრალეულობა ან ნებისმიერი არაგონივრული ქმედება, რომელიც მიზეზობრივ კავშირშია ზიანთან. იხ. American Law Institute, Restatement of the Law Third, Torts: Products Liability, 1998, §2(a); *Hylton K.*, Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 340.

¹⁶ ასეთ დროს პროდუქტის საწარმოო კონსტრუქცია წუნდებულია, თუმცაღა თავად მწარმოებელს, გამყიდველს ან კომერციული ჯაჭვის ყოველ წინამორბედს შეეძლო შეემცირებინა პროდუქტით გამოწვეული ზიანი, ალტერნატიული უსაფრთხო კონსტრუქციის შერჩევით. აღნიშნულს უკავშირდება მომხმარებლის მოლოდინის ტესტი (consumer expectation test), რომლის მიხედვითაც მოსარჩელე უნდა დაამტკიცოს, რომ პროდუქტი არ შეესაბამება საშუალო მომხმარებლის მოლოდინს პროდუქტის უსაფრთხოებასთან დაკავშირებით. იხ. American Law Institute, Restatement of the Law Third, Torts: Products Liability, 1998, §2(b); *Hylton K.*, Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 340.

¹⁷ ასეთ შემთხვევაში პროდუქტისთვის განსაზღვრულია შეუსაბამო გამოყენების წესები ან გაფრთხილებები, როდესაც შესაძლებელი იყო მწარმოებლის ან გამყიდველის მიერ შესაბამისი გონივრული გამოყენების წესებისა და გაფრთხილებების შეთვავება მომხმარებლისთვის, რაც გამოიწვევდა ზიანის შემცირებას ან აცილებას. იხ. American Law Institute, Restatement of the Law Third, Torts: Products Liability, 1998, §2(c); *Hylton K.*, Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 341.

¹⁸ *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.

¹⁹ *Scott M. D.*, Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, Maryland Law Review, Vol. 67, Issue 2, 2008, 459.

²⁰ იქვე, 459-460.

²¹ *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. მიითებულია 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).

²² *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.

²³ Encryption — დაშიფრვა, ხშირად გამოყენებადი მექანიზმი კიბერ უსაფრთხოებისთვის. ასეთ დროს ინფორაცია დაშიფრულია ისე, რომ მისი წაკითხვა მხოლოდ ავტორიზებულ პირს შეუძლია, რაც არ გამოორიცხავს თავის მხრივ ასეთ შიფრზე სხვათა ხელმისაწვდომობას, თუმცაღა მისი აღქმა/წაკითხვა მხოლოდ დაშიფრული ინფორაციის გასაღების მქონეს შეუძლია. კიბერ შიფრისთვის გამოიყენება ეგრეთ 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.

²⁴ *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.

მოსაზრება ბოლო დროს სულ უფრო მეტად გაქარწყლებადია პროდუქტის მწარმოებელი კომპანიების მიერ.²⁵

სამოქალაქო სამართლებრივი პასუხისმგებლობა პროგრამული უზრუნველყოფის ან ნივთების ინტერნეტის მოწყობილობის კონსტრუქციული წუნის გამო შესაძლებელია დადგეს მწარმოებლისთვის, თუმცა ისეთ შემთხვევებში, სადაც დისტანციური ჩარევა კიბერშეტევით 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 გააგრძელა სამუხრუჭე სისტემაზე.²⁶

პრობლემურ საკითხს წარმოადგენს შემთხვევა, როდესაც დელიქტი კიბერშეტევის განმახორციელებლის მიერ, სხვისი საკუთრების, კონკრეტულად IoT მოწყობილობების ან პროგრამული უზრუნველყოფის გამოყენებით ხდება, რასაც მესამე პირების ზიანი მოსდევს შედეგად, რაც გემოსენებული პროდუქტის ჰაკერთათვის მარტივად ხელმისაწვდომობით არის განპირობებული. ნაკლოვანი კიბერუსაფრთხოება, როგორც წინ ასეთ შემთხვევაში არ გვევლინება მწარმოებლების სამოქალაქო პასუხისმგებლობის საფუძვლად, რაც უმთავრესად განპირობებულია ეკონომიკური დანაკარგის დოქტრინით (economic loss doctrine).²⁷ რასაც ისიც ემატება, რომ სხვის მოწყობილობაში შეღწევა DDoS შეტევის განმახორციელებლის მიერ სისხლისსამართლებრივი პასუხისმგებლობის გამოწვევად ქმედებად ითვლება,²⁸ რაც სწორად პროდუქტის მწარმოებლისთვის, პასუხისმგებლობის გამომრიცხველია კაუზაციის გამო, თუმცა არა მაშინ, როდესაც პირის სისხლისსამართლებრივი მნიშვნელობის ქმედება მისთვის მოსალოდნელი და განჭვრეტადი იყო.²⁹ პროგრამული უზრუნველყოფისა და IoT მოწყობილობების მწარმოებლები თანამედროვე ტექნოლოგიების ბაზარზე დამკვიდრებული კომპანიები არიან, შესაბამისად, მათთვის ნათელია, რომ მათი პროდუქტი შესა-

ძლოა კიბერთავდასხმის ობიექტი გახდეს. გამომდინარე აქედან, თუ ისინი უსაფრთხოების გონივრულ მექანიზმებს არ შეიმუშავენ, რისი არარსებობაც წუნის საფუძველია, ისინი დაცვის ღირსნიც არ უნდა იყვნენ.³⁰

1.1.2. ეკონომიკური დანაკარგის დოქტრინის ჩანაცვლება

წუნდებული პროდუქტით გამოწვეული ზიანის ანაზღაურების მოთხოვნის შემზღუდველი ერთ-ერთი მთავარი ფაქტორი ეკონომიკური დანაკარგის დოქტრინაა,³¹ რომლის მიხედვითაც მოპასუხისგან ზიანის ანაზღაურება მხოლოდ მაშინაა შესაძლებელი, როდესაც ზიანი ფიზიკურად არის გამოხატული პირის ან საკუთრების მიმართ,³² ასევე, შესაძლოა ანაზღაურდეს ყველა სხვა თანმდევი ეკონომიკური დანაკარგი, რომელიც განპირობებულია ფიზიკური ზიანით, მაგრამ არ ანაზღაურდება ფიზიკური ზიანის გარეშე არსებული ეკონომიკური დანაკარგი. სწორედ ეს უკანასკნელი შემთხვევა უმეტესად სახეზე კიბერთავდასხმის დროს, პირს თუმცა ადგება ზიანი, მაგრამ იგი სრულიად ეკონომიკური ხასიათისაა და მას უშუალო ფიზიკური ზიანი პირისა თუ საკუთრების მიმართ არ ახლავს.³³ შეზღუდვის უმთავრესი გამართლება ბაზრის რეგულაციისთვის თავისუფალი სივრცის არსებობაა, უფრო კონკრეტულად კი პროდუქტზე ნდობის საკითხს საერთო სამართალი სრულიად ეკონომიკურ ბაზარს ანდობს.³⁴ თუმცა, გამართლება სრულიად გარეშე მესამე პირებთან მიმართებაში არ გამოდგება. ისინი წუნდებული პროდუქტის შექენაში საერთოდ არ მონაწილეობენ და შესაბამისად, ვერ აკეთებენ არჩევანს ხარისხიან პროდუქტზე, რასაც ისიც ემატება, რომ მათ არც რაიმე სახელშეკრულებო ბერკეტი არ აქვთ მოთხოვნის საფუძვლად.³⁵

უსამართლობა იქნებოდა მესამე პირების წუნდებული პროდუქტით გამოწვეული ზიანის ანაზღაურების მოთხოვნის ეკონომიკური დანაკარგის დოქტრინით სრულიად შეზღუდვა, განსაკუთრებით კი მაშინ, როდესაც მწარმოებელი არ ზრუნავს მისი პროდუქტის კიბერუსაფრთხოებაზე. 2018 წლის მონაცემებით DDOS შეტევებში,³⁶ სადაც წუნდებული

²⁵ 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/?sh=3b646f0a487a> (ვიზიტის დრო: 24.06.2019).

²⁶ იქვე, 1578-1579.

²⁷ *Sales N. A.*, Regulating Cyber-Security, Northwestern University Law Review, Vol. 107, No. 4, 2013, 1535.

²⁸ *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.

²⁹ *Rustad M. L./ Koenig T. H.*, The Tort of Negligent Enablement of Cybercrime, Berkeley Technology Law Journal, Vol. 20, Issue 4, 2005, 1570.

³⁰ იქვე, 1570.

³¹ *Hylton, K.*, Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 344.

³² იქვე.

³³ *Sales N. A.*, Regulating Cyber-Security, Northwestern University Law Review, Vol. 107, No. 4, 2013, 1535.

³⁴ *Hylton K.*, Tort Law: A Modern Perspective, Cambridge University Press, Cambridge 2016, 345.

³⁵ *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.

³⁶ 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) მიწოდება დიდი რაოდენობით მონაცემები, რომელსაც სერვისი 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-

პროგრამული უზრუნველყოფა და ნივთების ინტერნეტის მოწყობილობებია ჩართული ზიანმა მესამე პირებისთვის საშუალოდ 120 000 დოლარიდან ორ მილიონ დოლარდე შეადგინა, ყოველი ასეთი შეტევისთვის.³⁷ მაგალითისთვის, კიბერშეტევებში შესაძლოა ჩართული იყოს ისეთი მოწყობილობები როგორცაა, საბავშვო უსაფრთხოების მონიტორები³⁸ და ჭკვიანი კამერები, ერთ-ერთი ასეთი შეტევის დროს IoT მოწყობილობების წყალობით შეერთებული შტატების ადმოსავლეთ სანაპირო თითქმის უინტერნეტოდ დარჩა, ხოლო საიტები Twitter, Amazon და Netflix აღარ იყო ხელმისაწვდომი.³⁹ აღნიშნული გარემოების შემთხვევაშიც კი მესამე პირების ზიანის ანაზღაურების მოთხოვნა, მიმართული უშუალოდ იმ მწარმოებლისადმი, რომელმაც აწარმოა წუნდებული კიბერუსაფრთხოების მქონე პროდუქტი, ფაქტობრივად შეუძლებელია წუნდებული პროდუქტის პასუხისმგებლობის მოთხოვნით ეკონომიკური დანაკარგის დოქტრინის გამო.

ეკონომიკური დოქტრინის ჩანაცვლება ინტერნეტამდე პირველად საქმეზე People Express Airlines, Inc. v. Consol. Rail⁴⁰ მოხდა უშუალო მიზეზობრივი კავშირისა (proximate cause) და განჭვრეტადობის დოქტრინით (foreseeability).⁴¹

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 ისეთებზე, სადაც მიზეზობრივი კავშირი ზიანთან ძალიან დაშორებულია მწარმოებლისგან.⁴² ანალოგიურ შინაარსს იზიარებს შორეული კაუზის დოქტრინაც (remoteness doctrine).⁴³

პროგრამულ უზრუნველყოფასთან და ნივთების ინტერნეტთან მიმართებაში უშუალო მიზეზობრივი კავშირი, პირიქით, აფართოებს მწარმოებლის პასუხისმგებლობას რაც

საფუძველია მესამე პირებისთვის მოითხოვონ ეკონომიკური დანაკარგები, ფიზიკური ზიანის გარეშე, რადგანაც მწარმოებლების არაგულისხმიერი მიდგომა კიბერუსაფრთხოების მიმართ არის ერთგვარი კატალიზატორი მესამე პირების ზიანისთვის.⁴⁴ 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.⁴⁵ ამრიგად ნათელია, რომ მწარმოებლების ქმედების მიზეზობრივი კავშირი მესამე პირების ზიანთან სახეზეა მაშინ როდესაც ისინი კიბერ უსაფრთხოებაზე არ ბრუნავენ და ამით ერთგვარად ხელს უწყობენ კიბერშეტევების განხორციელებას, ხოლო, ეს უკანასკნელი კი მათთვის სრულიად განჭვრეტადია და 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, უნდა გაეცეს დადებითი პასუხი, ხოლო ლიტერატურაში გამოთქმულ მოსაზრებას თუ როგორ,⁴⁶ უშუალო მიზეზობრივი კავშირი და განჭვრეტადობის დოქტრინა ესადაგება.

1.2. ინტერნეტ საშუალებებით ვირტუალური საკუთრების ხელყოფა

Trespass, როგორც ხელყოფის ან ზიანის მიყენების,⁴⁷ ტრანსფორმაცია ინტერნეტ სივრცეში ამერიკის შეერთებული შტატების სასამართლოების დამსახურებაა. თუმცადა აღსანიშნავია, რომ სანამ ხელყოფიდან (trespass) გამომდინარე დოქტრინის კიბერ/ინტერნეტხელყოფის (cybertrespass) დამკვიდრება მოხდებოდა, რომელიც Compuserve v. Cyber Promotions⁴⁸ და eBay, Inc. v. Bidder's Edge⁴⁹ საქმეებს უკავშირდება, მისი უმნიშვნელოვანესი პროვოცირება არა კიბერ დავაზე, არამედ ტელეკომუნიკაციებთან დაკავშირებულ საქმეზე მოხდა Thrifty-Tel

Defense and Deterrence in Cyberspace, Harvard Journal of Law & Technology, Vol. 25, Number 2, 2012, 444-445.
³⁷ 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).
³⁸ ვრცლად იხ. Owllet Baby Wi-Fi Monitor "Worst IoT Security Of 2016", <https://www.informationsecuritybuzz.com/expert-comments/owllet-baby-wi-fi-monitor-worst-iot-security-2016>.
³⁹ Mirai-ის შეტევის შესახებ ვრცლად იხ. <https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet>.
⁴⁰ People Express Airlines, Inc. v. Consolidated Rail Corp., 495 A.2d 107 (N.J. 1985).
⁴¹ 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.
⁴² Rustad M. L. / Koenig T. H., The Tort of Negligent Enablement of Cybercrime, Berkeley Technology Law Journal, Vol. 20, Issue 4, 2005. 1601-1602.
⁴³ Schwartz E. V., Remoteness Doctrine: A Rational Limit on Tort Law, Cornell Journal of Law and Public Policy, Vol. 8, Issue 3, 1999, 429.

⁴⁴ 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.
⁴⁵ Owen G. D., Bending Nature, Bending Law, Florida Law Review, Vol. 62, Number 3, 2010, 609
⁴⁶ 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.
⁴⁷ ცვაივერტი ვ./ კოტცი პ., შედარებითი სამართალმცოდნეობის შესავალი კურსი სამართლის სფეროში, ტ. 2, რედაქტორი ნინიძე თ., ვისიაი, თბილისი 2001, 297-298.
⁴⁸ Compuserve Inc. v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997)
⁴⁹ eBay, Inc. v. Bidder's Edge LLC, 100 F. Supp. 2d 1058 (N.D. Cal. 2000)

v. Bezenek,⁵⁰ სადაც სასურველი შედეგის მისაღწევად მოსარჩელე მხარემ, რომლის სატელეფონო სერვისი არამართლმომიერად 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 არამატერიალური ნივთებისადმი.⁵¹ სწორედ აქედან მოყოლებული კიბერხელყოფა განიხილება როგორც მოძრავი ნივთის ხელყოფის დერივაცია.

მოძრავი ნივთის ხელყოფა, როგორც საფუძველი კიბერხელყოფისთვის (cybertrespass), დოქტრინის არსებობისა და მისი სასამართლო პრაქტიკის ადრეულ ეტაპზე სრულიად მისაღები იყო, როგორც სასამართლოებისთვის, ასევე, სამართლის აკადემიური სივრცისთვის.⁵² თუმცა, დროთა განმავლობაში დამკვიდრებულ კიბერხელყოფის დოქტრინას მრავალი საკამათო ასპექტი გამოუჩნდა.

1.2.1. ინტერნეტ სივრცის ბუნება კიბერხელყოფასთან 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.⁵³ რაც სრულიად მისაღები და გამართლებულია, გამომდინარე იქიდან, რომ როგორც სამართლებრივად, ასევე, ფიზიკური სამყაროს ბუნებიდან რთულად წარმოსადგენია მოძრავი ნივთისადმი საზღვრის/სივრცის რღვევა.

ნათელია, რომ კიბერხელყოფის ჩამოყალიბებისას, როგორც მოძრავი ნივთის ხელყოფიდან გამომდინარე დოქტრინა, არ იყო გათვალისწინებული უშუალოდ ინტერნეტისა და ონლაინ სივრცის ბუნება, შესაბამისად, მისი დაცვის ქვეშ მოექცა მხოლოდ მოწყობილობა, რომლითაც ინტერნეტზე წვდომა ხდება,⁵⁴ და არა უშუალოდ ინტერნეტსივრცეში არსებული სერვისები თუ მისი კომპონენტები. აღნი-

შნული შეზღუდვიდან გამომდინარე, მხარე, რომელიც დოქტრინისგან დაცვას ელოდებოდა ან მნიშვნელოვნად გაფართოებულად იღებდა მას ან კონტრასტულად დაუცველი რჩებოდა.⁵⁵

ინტერნეტსივრცის შემადგენელი კომპონენტების გათვალისწინებით, იქნება ეს ვებსაიტი, ელექტრონული ფოსტა თუ სხვა რესურსი,⁵⁶ ერთი მოსაზრების თანახმად უფრო მეტად გასაზიარებელია მათთვის რომ ისინი არა მოძრავ ნივთებს (personal property) წარმოადგენენ, არამედ მეტი ფიქსაციის გამო ემსგავსებიან უძრავ ნივთებს (real property).⁵⁷ თუმცა, აღნიშნული მოსაზრება სასამართლოს არასდროს გაუზიარებია.

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 მესაკუთრეს მის ფლობაში.⁵⁸ თუმცა, 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.⁵⁹ თუმცა, საქმეზე Compuserve v. Cyber Promotions სასამართლომ განსხვავებული სტანდარტი დაამკვიდრა მოძრავი ნივთების ხელყოფისთვის, მან დოქტრინას გვერდი აუარა და მოძრავი ნივთების ხელყოფის ტრანსფორმაცია კიბერხელყოფისთვის დაამკვიდრა, პირდაპირი ფიზიკური ზიანის არსებობის არასავალდებულო ხასიათით,⁶⁰ რაც კიბერხელყოფის კრიტიკის მთავარი საფუძველი გახდა.

დოქტრინის გვერდის ავლის კრიტიკა საბოლოოდ გამართლდა და პრაქტიკა შეიცვალა საქმეზე Intel Corp. v. Hamidi⁶¹ კალიფორნიის შტატის უზენაესი სასამართლოს მიერ. მან განმარტა რომ წინამორბედი პრაქტიკა⁶² არ იყო

⁵⁵ Fairfield J., Virtual Property, Boston University Law Review, Volume 85, 2005, 1075.

⁵⁶ იქვე, 1052–1053

⁵⁷ Epstein R. A., Cybertrespass, University of Chicago Law Review: Vol. 70, Iss. 1, Article 6, 2003, 83.

⁵⁸ American Law Institute, Restatement of the Law, Second, Torts, Volume 1, 1965, § 217.

⁵⁹ იქვე, § 218.

⁶⁰ ანალოგიური გადაწყვეტილება იქნა მიღებული საქმეზე eBay, Inc. v. Bidder's Edge, სადაც მოსარჩელე eBay-მ მიიღო მოპასუხის საწინააღმდეგოდ მოქმედების შესრულების აკრძალვა. 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.

⁶¹ Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003)

⁶² იგულისხმება Thrifty-Tel v. Bezenek, eBay, Inc. v. Bidder's Edge.

⁵⁰ Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559 (4th Dist. 1996)

⁵¹ Balganes 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.

⁵² Hedley S., Cybertrespass — A Solution in Search of a Problem?, Journal of European Tort Law, Vol. 5, Issue 2, 2014, 171–172.

⁵³ Lastowka G., Decoding Cyberproperty, Indiana Law Review, Vol. 40, No. 1, 2007, 27.

⁵⁴ მაგალითად კომპიუტერები, მათი შემადგენელი ნაწილები, ასევე, სერვერები სადაც შესაძლოა ელექტრონული ფოსტის მონაცემთა ბაზები იყოს განთავსებული ან ვებ-ჰოსტინგის სერვერები, სადაც საიტი თავის კონტენტს ტვირთავს.

მართებული, არამხოლოდ კალიფორნიის შტატის სამართლისთვის, არამედ მთლიანად ამერიკული სამართლისთვის — მოძრავი ნივთების ხელყოფის დოქტრინისთვის დაუშვებელია ზიანის არსებობის გამორიცხვა, რომლის არსებობაც მოსარჩელემ უნდა ამტკიცოს.⁶³ უნდა ჩაითვალოს, რომ მაშინდელი სასამართლო პრაქტიკის განვითარების ტენდენციიდან გამომდინარე გადაწყვეტილება მართებულია და უნდა იქნეს გაზიარებული, შესაბამისად 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 ზიანის⁶⁴ არსებობის აღმოფხვრას.

გემოგანხილული მსჯელობის მიხედვით, ნათელია თუ როგორი წარუმატებელი შეიძლება იყოს ინტერნეტთან მიმართებაში სამართლებრივი ტრანსფორმაცია. Intel Corp. v. Hamidi საქმის შემდეგ იშვიათად თუ მომხდარა ინტერნეტ ხელყოფის დელიქტის გამოყენება სასამართლო დავისას, რამაც თავის მხრივ თავისუფლება მისცა სხვა სამართლებრივ მექანიზმებს მოეგვარებინათ მსგავსი დელიქტური შემთხვევები.⁶⁵

1.3. ონლაინ დეფამაცია

პასუხისმგებლობა დეფამაციისთვის საერთო სამართლისთვის სიხალეს არ წარმოადგენს.⁶⁶ მიუხედავად იმისა რომ ინტერნეტ დეფამაცია მნიშვნელოვნად ემსგავსება ტრადიციულ დეფამატორულ დელიქტს, მას მაინც გააჩნია თავისი სპეციფიკური მახასიათებლები.⁶⁷

ციფრული სამყაროს ფართო ხელისაწვდომობამდე დეფამატორული განცხადებებიდან გამომდინარე სარჩელები ძირითადად მასმედიის წინააღმდეგ იყო მიმართული, თუმცა და ინტერნეტის განვითარებასთან ერთად მოპასუხეებად ძირითადად ბლოგერები, სოციალური მედიისა და სხვადასხვა ონლაინ ფორუმის მომხმარებლები გვევლინებიან.⁶⁸ აღნიშნულმა მთელი რიგი ისეთი ახალი პრობლემური საკითხებისა წარმოშვა, როგორცაა ვებსაიტზე გამოქვეყნებული ცნობა, როგორც ზიანის წყარო, არაადეკვატური სამა-

რთლებრივი დაცვის საშუალებები⁶⁹ და ვებგვერდების პასუხისმგებლობის საკითხი.

ზოგადი განმარტების მიხედვით, ონლაინ დეფამაცია განხორციელებულია მაშინ, როდესაც პირის შესახებ ცრუ ცნობები ან ცილისწამება ქვეყნდება ინტერნეტის საშუალებით, რასაც მოჰყვება ზიანი ან აღნიშნული ცნობები იმდენად პროვოკაციულია, რომ ზიანის დადგომა საგარაუდოა.⁷⁰ აღსანიშნავია, რომ ტრადიციული დეფამაციის მსგავსად ინტერნეტში გავრცელებული ცნობისთვის, მოპასუხე სრულ დაცვას იძენს თუ აღნიშნული ცნობა სიმართლეს წარმოადგენს.⁷¹

1.3.1. ვებგვერდზე გამოქვეყნებული მატერიალი, როგორც ზიანის წყარო

ინტერნეტის ბუნებიდან გამომდინარე ნებისმიერ პირს სხვადასხვა პლატფორმაზე/ვებგვერდზე მხოლოდ რეგისტრაციის შემდეგაც მარტივად შეუძლია ყოველგვარი მოდერაციის გარეშე ნებისმიერი ცნობის განთავსება (დაბო-სტვა),⁷² ნათელია, რომ ცნობის შემცველი მატერიალი, იქნება ვიდეო თუ ფოტო მასალა განსაკუთრებულ შემთხვევებში შესაძლოა წაიშალოს,⁷³ თუმცა აღნიშნული არ ხდება ავტომატურად, შესაბამისად ყოველი ასეთი მატერიალი პირისთვის, როგორც დეფამაცია ან ცრუ ინფორმაცია, შესაძლოა ზიანის მომტანი იყოს, მიუხედავად იმისა, თუ რა ხანგრძლივობითა და მასშტაბით ხდება მისი გავრცელება. სწორედ გემოგანხილული წარმოადგენს ზიანის მომტან ერთ-ერთ მატერიალს, რომლის შექმნაც ნებისმიერ პირს შეუძლია, ინტერნეტის ფართო ხელმისაწვდომობის გამო, სადაც უმთავრესი მნიშვნელობა არა ცნობის გამოხატულებას, არამედ მისი გავრცელების სიმართლეს აქვს.

მეორე და მნიშვნელოვნად გავრცელებულ შემთხვევას წარმოადგენს, ეგრეთ წოდებული ინტერნეტ საინფორმაციო სააგენტოები და მათ მიერ შექმნილი მატერიალი, რაც ერთი შეხედვით ტრადიციული ბეჭდვითი გამოცემების ანალოგს წარმოადგენს,⁷⁴ აღნიშნულთან მიმართებაში მნიშვნელოვანია, რომ საინფორმაციო სააგენტოს ვებგვერდზე ხშირად არა ჟურნალისტები არამედ ინფორმაციის მიმწოდებლები

⁶⁹ იქვე, 16.

⁷⁰ Rustad M. L., *Global Internet Law in a Nutshell*, 3rd edition, West Academic, St. Paul 2016, 187.

⁷¹ იქვე, 188.

⁷² მაგალითისთვის, Facebook, YouTube მხოლოდ რეგისტრაციის საჭიროებენ, რომლის შემდეგაც მომხმარებელს ნებისმიერი კონტენტის განთავსება შეუძლია საიტზე, წინასწარი მოდერაციის გარეშე. ასევე, არსებობს საიტები მაგალითად Tumblr.com და WordPress.com, სადაც ინტერნეტ მომხმარებელს შეუძლია საკუთარი ქვე-დომენი დაარეგისტრიროს და ჰქონდეს დამოუკიდებელი ბლოგი.

⁷³ მაგალითად YouTube-ის პოლიტიკა საკითხთან მიმართებაში იხ. ბმულზე <https://www.youtube.com/intl/en-GB/yt/about/policies/> (ვიზიტის დრო: 24.06.2019)

⁷⁴ 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.

⁶³ Lastowka G., *Decoding Cyberproperty*, *Indiana Law Review*, Vol. 40, No. 1, 2007, 37–38.

⁶⁴ Sharkey M. C., *Trespass Torts and Self-Help for an Electronic Age*, *Tulsa Law Review*, Vol. 45, 2010, 115.

⁶⁵ Hedley S., *Cybertrespass — A Solution in Search of a Problem?*, *Journal of European Tort Law*, Vol. 5, Issue 2, 2014, 175–178.

⁶⁶ 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.

⁶⁷ იქვე.

⁶⁸ Ardia S. D., *Freedom of Speech, Defamation, and Injunctions*, *William & Mary Law Review*, Vol. 55, 2013, 5.

დებენ სიახლეებს. საქმეზე O'Grady v. Superior Court⁷⁵ და Mortg. Specialists, Inc. v. Implode-Explode Heavy Indus.⁷⁶ სასამართლომ აღნიშნა, რომ მიუხედავად მატერიალის მიწოდებლებისა, რომლებიც არ არიან ჟურნალისტები, ვებგვერდები, რომლებიც იზიარებენ საინფორმაციო გამოცემლობის მახასიათებლებს, ითვლებიან საინფორმაციო სააგენტოებად. სწორედ აღნიშნულ შემთხვევაში ინფორმაციის წარმდგენელი დეფამაციურ ცნობას შესაძლოა ასეთი ვებგვერდის, საშუალებით ახორციელებდეს, რომელიც მედია საშუალებად არის მიჩნეული.⁷⁷ შესაბამისად ზიანის წყაროდ გვევლინება კომბინირებული ელემენტი, ჩვეულებრივი მომხმარებლის მიწოდებული სიახლე, რომელსაც ინტერნეტ სააგენტო ავრცელებს, როგორც საინფორმაციო სიახლეს.

1.3.2. კომუნიკაციურ ქსელში ეთიკურობის შესახებ კანონი და მეორადი პასუხისმგებლობა

ონლაინ დეფამაციას უკავშირდება, 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 ცილისმწამებლურ მატერიალს. შესაბამისად ინტერნეტ სერვისების პროვაიდერებზე არ ვრცელდება დეფამაციისგან წარმოშობილი დელიქტური პასუხისმგებლობა.⁷⁸

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.⁷⁹

⁷⁵ O'Grady v. Superior Court, 139 Cal. App. 4th1423, 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.

⁷⁶ 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.

⁷⁷ იქვე, 583.

⁷⁸ *Miller L. R.*, Business Law Today, Standard: Text & Summarized Cases, 11th Edition, Cengage Learning, Boston 2015, 176.

⁷⁹ *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227 (US District Court for the Northern District of Illinois, 1996).

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 შემოფარგვლა. კიბერსქვათინგი ხშირად არა დომენის ან ინტერნეტ გვერდის უკან მიყიდვას ისახავს რეგისტრირებული ნიშნის მფლობელისთვის, არამედ ინტერნეტ მომხმარებლების შეცდომაში შეყვანას და მათ მიზიდვას ისეთ რესურსზე, რომელიც სასაქონლო ნიშნის მფლობელის რეპუტაციას უქმნის საფრთხეს, ავრცელებს მის მიმართ დამამცირებელ ცნობებს ან გამოიჩინებს ირონიული მატერიალით.⁸⁰ უფრო ზოგადად კი კიბერსქვათინგის მიზანს წარმოადგენს სახელით⁸¹ დაგროვებული სიკეთის ხელყოფა, ამავე სახელის დომენად არამართლზომიერი გამოყენებისას.⁸²

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

მომხმარებელთა დაცვის კანონი ანტი-კიბერსქვათინგის შესახებ (Anticybersquatting Consumer Protection Act, ACPA),⁸³ 1999 წელს იქნა მიღებული შეერთებული შტატების კონგრესის მიერ. მისი მთავარი მიზანია მომხმარებლები და ბიზნესი დაიცვას კიბერსქვათინგისგან და აღკვეთოს პრობლემური შემთხვევები, ასევე, ხელი შეუწყოს ელექტრონული კომერციის განვითარებას.⁸⁴ ACPA-ს მიღების კიდევ ერთი მიზეზი მისი წინამორბედის სასაქონლო ნიშნითა აღრევის შესახებ ფედერალური კანონის (Federal Trademark Dilution Act, FTDA),⁸⁵ წარუმატებლობა გამოდგა, როგორც სასარჩელო მოთხოვნის სამართლებრივი საფუძველი, გამომდინარე იქიდან, რომ მისი დაცვის სფერო იმდენად ვიწრო და სასაქონლო ნიშნისთვის

⁸⁰ *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.

⁸¹ კიბერსქვათინგისთვის სავალდებულო არ არის რეგისტრირებული სასაქონლო ნიშნის არსებობა. კიბერსქვათინგი ხორციელდება მაშინაც როდესაც სქვათერი პირის პროფესიულ სახელწოდებას ან სახელს იყენებს. მაგალითად იხ. *Madonna Ciccone, p/k/a Madonna v. Dan Parisi and "Madonna.com"* Case No. D2000-0847

⁸² *Barbantonis F. N.*, Should Contributory Cybersquatting be Actionable?, North Carolina Journal of Law & Technology, Vol. 17, Issue 1, 2015, 85.

⁸³ 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)

⁸⁴ *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.

⁸⁵ 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)

ტრადიციული იყო, დომენების მფლობელთა დიდი ნაწილი დაცვის გარეშე რჩებოდა, უფრო კონკრეტულად კი კანონი ითხოვდა ნიშანი ყოფილიყო, როგორც ცნობილი, ასევე, გამასხვავებელუნარიანი, კუმულატიურად.⁸⁶

გემოსხენებულთან მიმართებაში გასამართლებელია მოსაზრება,⁸⁷ რომლის მიხედვითაც მხოლოდ სასაქონლო ნიშნების საკანონმდებლო დამცავი მექანიზმები არ გამოდგება იმ შემთხვევაში, როდესაც დავა დომენს ეხება. მოსაზრების თანახმად სასაქონლო ნიშნის მფლობელს მასზე გააჩნია კვაზი-საკუთრებასთან დაკავშირებული უფლებები, რაც ნიშნავს იმას რომ ნიშანია საკუთრება და არა უშუალოდ პროდუქტი რომელზეც ისაა განთავსებული.⁸⁸ დომენის შეთხვევაში კი საკმარისია გაუქმდეს სასაქონლო ნიშნის შემცველი დომენი, მას ნიშნის მფლობელი თავიდან დაარეგისტრირებს და ფაქტობრივად შეიძენს მასზე საკუთრებას, რაც კონტრაფაქციული საქონლის შემთხვევაში შეუძლებელია. შესაბამისად, სასაქონლო ნიშნებთან დაკავშირებული ნორმატიული მოწესრიგება უშუალოდ სასაქონლო ნიშნებს მიესადაგება და მხოლოდ მათი გამოყენებით, შესაძლოა ინტერნეტში დელიქტური ვალდებულება ატიპურად იქნეს მოწესრიგებული.

რაც შეეხება უშუალოდ მოთხოვნას, მოსარჩელეს შეუძლია ACPA-ს მიხედვით, მოითხოვოს მოპასუხისგან მოქმედების შესრულების აკრძალვა,⁸⁹ ზიანის ანაზღაურება,⁹⁰ ან კანონის მიერ დაწესებული ზიანის ანაზღაურება (statutory damages), რომელიც განისაზღვრება 1000–100 000 დოლარამდე თითოეული დომენისთვის, რაც თავისთავად გამორიცხავს ფაქტობრივად მიყენებული ზიანის მოთხოვნის საშუალებას.⁹¹ მიუხედავად იმისა, რომ ეს უკანასკნელი საკმაოდ მკაცრად გამოიყურება კიბერსქვათერების პასუხისმგებლობისთვის, ხშირად ფაქტობრივი ზიანის ანაზღაურების მოთხოვნა გაცილებით აჭარბებს კანონისმიერი ზიანის მოცულობის ფარგლებს. მაგალითად, საქმეზე *Pinterest, Inc. v. Qian Jin*⁹² კიბერსქვათერ მოპასუხეს დაეკისრა 7.2 მილიონის ანაზღაურება მოსარჩელის სასარგებლოდ.

2.1.2. დომენურ სახელებთან დაკავშირებული დავების გადაწყვეტის ერთიანი პოლიტიკა (UDRP)

კიბერსქვათინგისთვის მნიშვნელოვან მოვლენას წარმოადგენს დომენურ სახელებთან დაკავშირებული დავების გადაწყვეტის ერთიანი პოლიტიკის არსებობა (Uniform Domain Name Dispute Resolution Policy), რომელიც 1999 წელს მიწვებული სახელებისა და ნომრების ინტერნეტკორპორაციის (ICANN) მიერ შემუშავდა.⁹³

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.⁹⁴ აღსანიშნავია, რომ ICANN-მა დავის გადაწყვეტის პირველ პროვაიდერად უფლებამოსილება ინტელექტუალური საკუთრების მსოფლიო ორგანიზაციას მიანიჭა (WIPO),⁹⁵ რომელმაც 44 000-ზე მეტი საქმე მიიღო განსახილველად დომენურ დავებთან დაკავშირებით.⁹⁶

2.2. ინტერნეტ მეკობრეობა და საავტორო უფლებები

მართებულად უნდა მივიჩნიოთ, რომ ინტერნეტ მეკობრეობის დროს საქმე ძირითადად საავტორო უფლებების დარღვევას შეეხება და შესაბამისად ყოველი ასეთი დავა უნდა გადაწყდეს საავტორო უფლებებთან დაკავშირებული ნორმატიული მოწესრიგების შესაბამისად. დელიქტის მახასიათებელი თითქმის ყოველთვის საავტორო უფლებით დაცული მატერიალის ინტერნეტში განთავსებაა შესაბამისი უფლების გარეშე, რასაც გაცილებით დიდი ეკონომიკური ზიანი ახლავს, ვიდრე ტრადიციულად მატერიალის რეალურ სამყაროში გავრცელებით.

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

მართლზომიერი გამოყენება (Fair Use) მნიშვნელოვან დოქტრინას წარმოადგენდა საავტორო უფლებების გაციფრულებაში. მისი მიხედვით საზოგადოებისთვის ხელმი-

⁸⁶ *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.
⁸⁷ *Mercer D. J.*, Cybersquatting: Blackmail on the Information Superhighway, *Journal of Science & Technology Law*, Vol. 6, Notes, 2000, 3–4.
⁸⁸ იქვე, 3–4.
⁸⁹ Anticybersquatting Consumer Protection Act, (15 U.S.C. § 1125(d)). Section 3(a)(1).
⁹⁰ იქვე, Section 3(a)(2).
⁹¹ იქვე, Section 3(b)(d).
⁹² *Pinterest, Inc. v. Qian Jin*, No. C 12-04586 RS (N.D. Cal. Sep. 30, 2013)

⁹³ *Schulte J. C.*, The New Anticybersquatting Law and uniform Dispute Resolution Policy for Domain Names, *Tort & Insurance Law Journal*, Vol. 36, 2000, 107.
⁹⁴ *Singh H.*, Domain Name Disputes and Their Resolution under UDRP Route: A Review, *Archives of Business Research*, Vol. 6, No.12, 2018, 150.
⁹⁵ *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.
⁹⁶ სტატისტიკა წლების მიხედვით იხ. ბმულზე <https://www.wipo.int/amc/en/domains/statistics/cases.jsp> (ვიზიტის დრო: 24.06.2019).

საწვდომი და გამოყენებადი უნდა იყოს საავტორო უფლებებით დაცული მატერიალი ისეთი მიზნებისთვის როგორც კრიტიკა, კომენტარება, რეპორტაჟი, სწავლება, განათლება და კვლევა, ყოველგვარი პასუხისმგებლობის გარეშე.⁹⁷ დოქტრინის მნიშვნელობიდან გამომდინარე იგი კოდიფიცირებულია.⁹⁸ რაც შეეხება კანონს საავტორო უფლებების შესახებ ციფრულ ეპოქაში (Digital Millennium Copyright Act, DMCA),⁹⁹ იგი მიმართულია ტექნოლოგიური ინოვაციებიდან გამომდინარე დამატებითი მექანიზმის შექმნისკენ საავტორო უფლებების დასაცავად, თუმცა ის საკამათო ნორმატიულ მოწესრიგებად ხასიათდება და ხშირად მოიხსენიება როგორც ინტერნეტ სივრცის გადამრჩენელი ან, სრულიად საპირისპიროდ, ონლაინში გამოხატვის თავისუფლების შემზღვეველი აქტი.¹⁰⁰

გემოხსენებული კანონის მიღებისას ორი მნიშვნელოვანი აზრი გამოითქვა. პირველი ის, რომ კანონისა და შესაბამისი დაცვის არარსებობის შემთხვევაში საავტორო უფლების მფლობელები ნაწარმოებს არ განათავსებდნენ ინტერნეტში.¹⁰¹ ხოლო, მეორე, კი იყო ის რომ ჩვეულებრივი მომხმარებლები შესაძლოა არასახარბიელო სიტუაციაში აღმოჩენილიყვნენ უფლების მფლობელთა მხრიდან მექანიზმების არასწორი გამოყენების გამო.¹⁰²

გემოხსენებული ორივე მოსაზრება მართებული აღმოჩნდა. ასევე, ნაწილობრივ გასაზიარებელია მოსაზრება რომ DMCA-იმ მნიშვნელოვნად შეზღუდა მართლმომიერი გამოყენების უფლება.¹⁰³ რაც დაუკავშირდა სიტყვისა და გამოხატვის თავისუფლების შეზღუდვას,¹⁰⁴ გამომდინარე იქიდან, რომ DMCA-ის მიერ დადგენილი შეტყობინებისა და წაშლის (notice and takedown) პროცესის განხორციელებისას საავტორო უფლების მფლობელის შეტყობინების შემდეგ საიტი ვალდებულია წაშალოს მითითებული მატერია-

ლი,¹⁰⁵ თუმცა პროცესის ფარგლებში საიტის ადმინისტრაციისთვის შეუძლებელია იმაზე მსჯელობა მომხმარებლის მიერ ატვირთული მატერიალი მართლმომიერი თუ არა, აღნიშნული საკითხი მნიშვნელოვნად პრობლემურად რჩება დღემდე, რადგანაც არ არსებობს დამატებით მაკონტროლებელი რეგულაცია შეტყობინებისა და წაშლის სისტემებისთვის რაც მათი არაკეთილსინდისიერი გამოყენების პრობლემას გადაჭრიდა.¹⁰⁶

2.2.2. უსაფრთხო ნავსადგომის წესი

DMCA-ის ერთ-ერთ უდიდეს დამსახურებად ითვლება, უსაფრთხო ნავსადგომის (safe harbor) შექმნა ინტერნეტ სერვისის პროვაიდერებისთვისა და საიტებისთვის. შეერთებული შტატების კოდექსის მე-17 თავის 512-ე მუხლი ოთხ სხვადასხვა წინაპირობას ადგენს იმისთვის რომ გემოხსენებულ სუბიექტებს მათი მომხმარებლის გამო არ დაეკისროთ პასუხისმგებლობა საავტორო უფლების ინტერნეტში დარღვევისთვის. თუმცა ყველაზე მეტად საკამათოდ ითვლება უსაფრთხო ნავსადგომის წესი, რომელიც სერვისის პროვაიდერებს იცავს მაშინაც კი როდესაც უფლების დამრღვევი მატერიალი მათ სერვერებზე ან ქსელში ინახება.¹⁰⁷ ასეთ შემთხვევაში სერვისის პროვაიდერს პასუხისმგებლობა არ დაეკისრება მაშინ, თუ ის არ ფლობს ინფორმაციას უფლების დამრღვევი მატერიალის შესახებ.¹⁰⁸ არ იღებს პირდაპირ ეკონომიკურ მოგებას მატერიალიდან და პირდაპირ არ აკონტროლებს ამ პროცესს¹⁰⁹ და ბოლოს, სერვისის მიმწოდებელი უფლების დამრღვევი მატერიალის შეტყობისთანავე შლის ან ზღუდავს წვდომას მასზე.¹¹⁰ ეს უკანასკნელი კი გემოხსენებულ შეტყობინებისა და წაშლის რეჟიმთანაა დაკავშირებული.

III. 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.

⁹⁷ 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.

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

⁹⁹ 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).

¹⁰⁰ 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.

¹⁰¹ 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.

¹⁰² იქვე, 761.

¹⁰³ Laos J. T., Fair Use and the Digital Millennium Copyright Act, Michigan Telecommunications and Technology Law Review, Vol. 13, Issue 2, 2007, 603.

¹⁰⁴ 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.

¹⁰⁵ Matthew S., Internet Safe Harbors and the Transformation of Copyright Law, Notre Dame Law Review, Vol. 93, Issue 2, 2018, 503–504.

¹⁰⁶ მაგალითისთვის YouTube-ზე შეტყობინებისა და წაშლის რეჟიმის პროცესის განხორციელების შემდეგ მითითებული მატერიალი საიტიდან უპირობოდ წაიშლება თუნდაც ის სამართლიანი გამოყენების მოქმედების ფარგლებში ექველდეს. საიტი უბრალოდ მითითებს რომ უფლების მფლობელმა უნდა გაითვალისწინოს სამართლიანი გამოყენების დოქტრინა, თუმცა რაიმე მზოჯავი ვალდებულება ამისთვის მას არ აქვს. დამატებით იხ. <https://support.google.com/youtube/answer/2807622> (ვიზიტის დრო: 24.06.2019).

¹⁰⁷ Matthew S., Internet Safe Harbors and the Transformation of Copyright Law, Notre Dame Law Review, Vol. 93, Issue 2, 2018, 511.

¹⁰⁸ 17 U.S.C. § 512(c)(A).

¹⁰⁹ იქვე, § 512(c)(1)(B).

¹¹⁰ იქვე, § 512(c)(1)(C).

ინტერნეტის უსაზღვრო ბუნებიდან გამომდინარე ხშირია შემთხვევა როდესაც ინტერნეტში განხორციელებული დელიქტური ქმედება რამდენიმე ქვეყანას მოიცავს, შესაბამისად კი მასზე შესაძლოა სხვადასხვა ქვეყნის სამართლის სისტემის მოწესრიგება გავრცელდეს,¹¹¹ სწორედ ასეთი შემთხვევებით ხასიათდება ინტერნეტ დელიქტები ევროპის კავშირში, რაც თავისთავად წინ წევს განსჯადობისა და გამოსაყენებელი სამართლის პრობლემატიკას.

გემოსხენებულის მიუხედავად ევროპის კავშირის საერთაშორისო კერძო სამართლისთვის ცალკეულად ინტერნეტში წარმოშობილი ზიანისთვის სპეციალური მოწესრიგება არასდროს არ ყოფილა რეგულირებული, შესაბამისად არ არსებობს მკაფიოდ განსაზღვრული გამიჯვნა ინტერნეტსა და რეალურ სამყაროს ზიანზე გასავრცელებელ ნორმებს შორის.¹¹² გამომდინარე აქედან ორივე შემთხვევაზე ვრცელდება ერთი და იგივე მოწესრიგება, კონკრეტულად კი განსჯადობისთვის რეგულაცია ბრიუსელი I,¹¹³ ხოლო, გამოსაყენებელი სამართლისთვის კი რეგულაცია რომი II.¹¹⁴

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.¹¹⁵ შესაბამისად არც მოსარჩელის მოქალაქეობას აქვს მნიშვნელობა. გამომდინარე აქედან რეზიდენტ პირებზე იგივე რეჟიმი ვრცელდება რაც წევრი ქვეყნის მოქალაქე პირებზე.¹¹⁶

სპეციალური წესის თანახმად, მოსარჩელეს შეუძლია სარჩელის წარდგენა დელიქტთან ან კვაზი-დელიქტთან დაკავშირებულ დავაზე იმ ადგილის მიხედვით, სადაც ზიანის

მომტანი ქმედება განხორციელდა ან შეიძლება განხორციელდეს (აქვე აღსანიშნავია, რომ მოცემული მუხლი დელიქტისთვის იყენებს ტერმინებს, როგორც tort, ასევე, delict).¹¹⁷

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.¹¹⁸

პრობლემის გადასაჭრელად, განსაკუთრებით კი მაშინ როცა საქმე ონლაინ დეფამაციას ეხება, გამოიყენება ევროპული კავშირის მართლმსაჯულების სასამართლოს მიერ დამკვიდრებული შევილის დოქტრინა (Shevill doctrine),¹¹⁹ მიუხედავად იმისა რომ საქმე, რომელსაც დოქტრინა ეყრდნობა ინტერნეტის განვითარების პირველ ეტაპებზე იყო მიღებული და არ მსჯელობს უშუალოდ ინტერნეტში მიყენებულ ზიანზე, იგი სპეციალური განსჯადობის განმარტების მთავარ საშუალებად არის გამოყენებული სასამართლოების მიერ.¹²⁰

1.1. შევილის დოქტრინა (საქმე C-68/93)

შევილის საქმეზე, რომელიც ბეჭდური გამოცემის მიერ გავრცელებული ცილისმწამებლური ცნობების შედეგად მიყენებულ ზიანს ეხებოდა სასამართლომ დაადგინა, რომ მოსარჩელეს სრული ზიანი მხოლოდ მოპასუხის ტერიტორიულობის მიხედვით შეეძლო მოეთხოვა, ხოლო წევრ სახელმწიფოებში კი მხოლოდ ის ზიანი, რაც უშუალოდ მათ ტერიტორიაზე დადგა.¹²¹ სწორედ აღნიშნულის შემდეგ დამკვიდრდა მოზაიკის პრინციპი.¹²²

მოზაიკის პრინციპი, მიესადაგება სპეციალურ განსჯადობას, რომელიც თავის მხრივ გადახვევაა ზოგადი წესისგან, ეს უკანასკნელი კი წარმოადგენს ძალთა თანაფარდობის ბერკეტს მოსარჩელესა და მოპასუხეს შორის, გამომდინარე იქიდან რომ, თუ მოსარჩელეს აქვს საშუალება ამირჩიოს საქმის განმხილველი სასამართლო, მოპასუხეს უნდა ჰქონდეს გონივრული შესაძლებლობა მოემზადოს მი-

¹¹¹ 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,
¹¹² Lutz T., Internet Cases in EU Private International Law Developing a Coherent Approach, International & Comparative Law Quarterly, Vol. 66, Issue, 2017, 688.
¹¹³ 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>.
¹¹⁴ 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>.
¹¹⁵ Regulation (EU) No 1215/2012, Article 4; ანალოგიურად ძველი რეგულაციის Regulation (EC) No 44/2001, Article 2.
¹¹⁶ 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.

¹¹⁷ Regulation (EU) No 1215/2012, Article 7(2); ანალოგიურად ძველი რეგულაციის Regulation (EC) No 44/2001, Article 5(3)
¹¹⁸ Lutz T., Internet Cases in EU Private International Law Developing a Coherent Approach, International & Comparative Law Quarterly, Vol. 66, Issue, 2017, 690—691.
¹¹⁹ C-68/93 Shevill and Others v Presse Alliance ECLI:EU:C:1995:61 (1995).
¹²⁰ 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.
¹²¹ 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.
¹²² იქვე.

სთვის დაყენებულ მოთხოვნაზე საპასუხოდ,¹²³ თუმცა ზოგადი წესიდან გადახვევა შესაძლებელია მხოლოდ მკარად საგამონაკლისო და განჭვრეტად შემთხვევებში.¹²⁴

1.2. სპეციალური განსჯადობის ახალი სასამართლო ჭრილი

შევილის დოქტორის ჩანაცვლებად შესაძლოა მოვიზომოთ მოსარჩელის ინტერესთა ცენტრის კრიტერიუმი, რომელიც განვითარდა ონლაინ დეფამაციის ერთ-ერთ საქმეზე.¹²⁵ აღნიშნული საქმის მიხედვით, სასამართლოს წინაშე დაისვა საკითხი, ბრიუსელი I რეგულაციის 7(2) მუხლის მიხედვით ალტერნატიულად ხომ არ უნდა დადგინდეს განსჯადობა ინტერნეტ დელიქტთან სპეციალურ კავშირში,¹²⁶ რაც განსჯადი ქვეყნის დადგენის უფრო მეტად პროგნოზირებად ფორმულას შექმნიდა.

ინტერესთა ცენტრი ახალ საშუალებას ქმნის განსჯადობის პრობლემის გადასაჭრელად ინტერნეტ დელიქტთან მიმართებაში, რომლის მიხედვითაც, მოსარჩელეს ზიანის მთლიანი მოცულობის მოთხოვნა შეუძლია იმ წევრ სახელმწიფოში, სადაც კი ზიანი დადგა.¹²⁷ გემოსხენებულ საქმეში სასამართლომ განმარტა რომ ინტერესთა ცენტრი მოსარჩელისთვის ძირითადად ის ადგილია სადაც ის რეზიდენტი პირია, მიუხედავად ამისა ინტერესთა ცენტრის ადგილი შესაძლოა სხვაც იყოს, მაგალითად, მოსარჩელის სამსახური, რომელიც სხვა წევრ სახელმწიფოში მდებარეობს.¹²⁸

1.3. ინტერნეტ დელიქტის თანმდევი ფორუმ შოპინგი

ინტერნეტის უსაზღვრო ბუნებიდან გამომდინარე, ვირტუალურ სამყაროში განხორციელებულმა დელიქტმა შესაძლოა რამდენიმე ქვეყნის ფარგლები მოიცვას, რაც განსაკუთრებით წინ წევს ეგრეთ წოდებული ფორუმ შოპინგის საკითხს ინტერნეტ დელიქტებისთვის.¹²⁹

თავისთავად, მოსარჩელე ყოველთვის ეცდება მისთვის სასურველი სასამართლო ამოარჩიოს იმ ქვეყნის მიხედვით, რომელშიც მისი მოთხოვნის დაკმაყოფილებას ყველაზე მეტი ალბათობა ექნება. შევილის დოქტორისა და ინტერესთა

ცენტრის მიხედვით, მოსარჩელეს ევროპის კავშირის ყველა წევრ ქვეყანაში აქვს შესაძლებლობა მოითხოვოს ზიანი, რაღა თქმა უნდა, ისეთი საგამონაკლისო შემთხვევების გარდა, სადაც ზიანი არ დამდგარა ან ინტერნეტის საშუალებით ზიანის მომტანი მატერიალი არ არის ხელმისაწვდომი.

პრობლემის გადაჭრა ევროპის კავშირის საერთაშორისო კერძო სამართლის დამატებითი ნორმატიული მოწესრიგებით ფაქტობრივად შეუძლებელია, რადგანაც ინტერნეტ სამართლისთვის ცალკეული განსჯადობის ნორმები უნდა შემუშავდეს, რაც უაღრესად რთულია ისეთი მოვლენისთვის, როგორც ინტერნეტში წარმოშობილი ურთიერთობებია. აღნიშნული პრობლემის გადასაჭრელად ერთადერთ გზას ტოვებს, დამკვიდრდეს ისეთი სასამართლო ინტერპრეტაცია სპეციალური განსჯადობისთვის, რომლის მიხედვითაც მოდავე მხარეების საპროცესო ბალანსი მაქსიმალურად თანაბარი იქნება.

2. გამოსაყენებელი სამართალი

გამოსაყენებელი სამართლის დასადგენად, ანუ იმ ნორმებისა თუ რომელი უნდა იყოს სახელმძღვანელო უშუალოდ საქმის განხილვისას არასახელმწიფოებო ვალდებულებებისთვის, ევროპის კავშირში გამოიყენება რეგულაცია რომი II, რომლის მე-4 მუხლის მიხედვით დელიქტური ვალდებულება უნდა მოწესრიგდეს იმ ქვეყნის სამართლის მიხედვით, რომელშიც ზიანი წარმოიშვა, იმისდა მიუხედავად თუ სად განხორციელდა ზიანის მაპროვოცირებელი მოვლენა და სად დადგა ირიბი ზიანი. მოცემული მუხლის მიხედვით რეგულაცია დაზარალებულს არ აძლევს საშუალებას ამოირჩიოს იმ ქვეყნების სამართალს შორის ერთ-ერთი, სადაც ზიანის წარმოშობი მოვლენა განხორციელდა და სადაც ზიანი დადგა, რაც არსებითად განსხვავდება რეგულაცია ბრიუსელი I-ის 7(2) მუხლისგან, სადაც მხარეს ამ ორს შორის არჩევანის ვაკეთება შეუძლია.¹³⁰ მიუხედავად ამისა, თუ ზიანი დამდგარა 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).¹³¹ თუმცაღა, მოცემული მოსაზრების მისაღებას საეჭვოს ხდის ინტერნეტის ფართოდ ხელმისაწვდომი ბუნება, გამომდინარე აქედან ინტერნეტ დელიქტის დროს სავარაუდოა, რომ ზიანი სხვადასხვა სახელმწიფოებში დადგება, შესაბამისად გამოყენებული უნდა იქნეს არა ყველა ქვეყნის სამართალი, არამედ იმ სახელმწიფოსი, რომელიც

¹²³ 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.

¹²⁴ იქვე.
¹²⁵ 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).

¹²⁶ 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.

¹²⁷ Hartley C. T., Jurisdiction in tort claims for non-physical harm under Brussels 2012, Article 7(2), Vol. 67, 2018, 1001.

¹²⁸ Joined Cases C-509/09 and C-161/10, Paragraph 52 of the judgment, მითითებულია Hartley C. T., Jurisdiction in tort claims for non-physical harm under Brussels 2012, International and Comparative Law Quarterly, Vol. 67, 2018, 1001, მიხედვით.

¹²⁹ Smith G., Internet Law and Regulation, Sweet & Maxwell, 2007, 459.

¹³⁰ 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

¹³¹ 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.

ყველაზე მეტად არის დაკავშირებული დელიქტურ ქმედება-სთან.¹³²

IV. ინტერნეტ დელიქტები საქართველოში

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

1. სასამართლო პრაქტიკა

1.1. ინტერნეტ დავების საწყისი წერტილი

რაოდენ გასაკვირიც არ უნდა იყოს, საქართველოს უზენაესმა სასამართლო ინტერნეტ დელიქტთან მიხლოებული დავა ვერ კიდევ 2000 წელს განიხილა.¹³³ საქმე შეეხებოდა დომენის, როგორც სასაქონლო ნიშნის გამოყენების აკრძალვას.

საქმე თავის მხრივ, ატიპურ 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 აკრძალა 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,¹³⁴ თუმცადა, 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.“¹³⁵ რაც მართებულ მსჯელობას წარმოადგენს და თავის მხრივ, ირიბად ამყარებს იმ არგუმენტს რომ მსგავსი ტიპის დავებისთვის მხოლოდ საკანონმდებლო ბაზაზე დაყრდნობა არ არის გამართლებული.¹³⁶ სასამართლო ქვემდგომი ინსტანციის გადაწყვეტილების გასაუქმებლად მიუთითებს: „დომენური სახელისა და სასაქონლო ნიშნის გამოყენების მართლზომიერება შეფასებულ უნდა იქნეს საქმიანი ბრუნვის ტრადიციებისა და უფლების განხორციელების მართლზომიერი საზღვრების გათვალისწინებით. აღნიშნული თვალსაზრისით, არამართლზომიერად უნდა იქნეს მიჩნეული, რომ არაკეთილსინდისიერი კონკურენციის მიზნით ინტერნეტში დომენად დარეგისტრირდეს ნიშანი, რომელიც უკვე არსებული გარკვეული რეპუტაციის მქონე სასაქონლო ნიშნის იდენტური ან მსგავსია.“, ასევე, იმ დროისთვის ინოვაციური საკითხსაც ამიტებს დავიდან გამომდინარე: „არამართლზომიერად უნდა იქნეს მიჩნეული უკვე დარეგისტრირებული დომენური სახელის სხვა პირის მიერ სასაქონლო ნიშნად რეგისტრაცია და შემდეგში სასაქონლო ნიშანზე განსაკუთრებული უფლების საფუძველზე დომენის გამოყენების აკრძალვა.“¹³⁷ აქვე უნდა აღინიშნოს რომ მოცემული განმარტება ფაქტობრივად ნორმატიულ მოწესრიგებამდე ამკვიდრებს სასაქონლო ნიშნის არაკეთილსინდისიერი განზრახვით რეგისტრაციის დაუშვებლობას.¹³⁸ საყურადღებოა ისიც, რომ ამერიკის შეერთებული შტატების მომხმარებელთა დაცვის კანონი ანტი-კიბერსექსთინგის შესახებ, მოქმედების საფუძველად მნიშვნელოვნად ითვალისწინებს არაკეთილსინდისიერ განზრახვას.¹³⁹

აღსანიშნავია, რომ პირველი მსგავსი ტიპის დავა ინტელექტუალური საკუთრების მსოფლიო ორგანიზაციის მიერ სწორედ 2000 წელს იქნა გადაწყვეტილი.¹⁴⁰

1.2. ინტერნეტსივრცე როგორც მეწარმეთა არაკეთილსინდისიერი კონკურენციის ასპარეზი

ინტერნეტ სივრცეში მიყენებული ზიანისთვის უმნიშვნელოვანესი გადაწყვეტილება საქმეზე No2/30577-16¹⁴¹ ერთი მხრივ, წინ გადადგმული ნაბიჯია პრაქტიკისთვის, ხოლო,

¹³² 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.

¹³³ საქართველოს უზენაესი სასამართლოს 2000 წლის 11 ოქტომბრის განჩინება საქმეზე №: 3კ/589.

¹³⁴ 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.

¹³⁵ საქართველოს უზენაესი სასამართლოს 2000 წლის 11 ოქტომბრის განჩინება საქმეზე №: 3კ/589.

¹³⁶ Mercer D. J., Cybersquatting: Blackmail on the Information Superhighway, Journal of Science & Technology Law, Vol. 6, Notes, 2000, 3-4.

¹³⁷ საქართველოს უზენაესი სასამართლოს 2000 წლის 11 ოქტომბრის განჩინება საქმეზე №: 3კ/589.

¹³⁸ 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.

¹³⁹ Anticybersquatting Consumer Protection Act, (15 U.S.C. § 1125(d)). Section 2.

¹⁴⁰ World Wrestling Federation Entertainment, Inc. v. Michael Bosman, WIPO, No. D99-. 0001 (Jan. 14, 2000)

¹⁴¹ თბილისის საქალაქო სასამართლოს 2017 წლის 8 მაისის გადაწყვეტილება საქმეზე No2/30577-16.

მორე მხრივ, ნათლად გვიჩვენებს თუ რაოდენ მოუძაღბელი შეიძლება აღმოჩნდეს სასამართლო ტექნიკურად ახალი სამართლებრივი საკითხის წინაშე.

მოსარჩელეც და მოპასუხეც მოცემულ საქმეში წარმოდგენდნენ ერთი და იმავე კომპანიის Apple Inc.—ის პროდუქტის დისტრიბუტორებს საქართველოში. მოსარჩელის განცხადებების მიხედვით ირკვევა, რომ მოპასუხემ გადაწყვიტა ინტერნეტის მეშვეობით არაკეთილსინდისიერი კონკურენცია გაეწია მოსარჩელისთვის, კონკრეტულად კი შექმნა მოსარჩელის სახელწოდებით საიტი, რომლის დომენური სახელი მხოლოდ ერთი ასოთი განსხვავდებოდა მოსარჩელის სახელისგან, სადაც ათავსებდა მოსარჩელისთვის რეპუტაციის შემლახველ მატერიალს, ასევე, მოსარჩელის განმარტებით, მოპასუხემ იგივე ქმედება განახორციელა სოციალურ ქსელ Facebook.com-ზე, სადაც მოსარჩელის ბუსტი სახელის შემცველობით 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.

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,¹⁴² რომელიც სისხლისსამართლებრივ დანაშაულზეა მიღებული. მოცემულ გადაწყვეტილებაზე მიუთითება არასწორია, შემდეგი სავარაუდო ფაქტობრივი უზუსტობების გამო. სისხლისსამართლებრივი დანაშაულის¹⁴³ საქმეზე United States v. John Zuccarini, 2003 წლის არცერთი თვის 29 რიცხვში გადაწყვეტილება არ ყოფილა მიღებული, მოცემულ საქმეზე ბრალდებულმა დანაშაული 2003 წლის 10 დეკემბერს აღიარა, ხოლო, სასჯელი მას 2004 წლის 26 თებერვალს შეეფარდა.¹⁴⁴ სასამართლო სავარაუდოდ გულისხმობს არა გადაწყვეტილებას, არამედ 2003 წლის 29 აგვისტოს გაცემულ დაკავების ბრძანებას, რომე-

¹⁴² თბილისის საქალაქო სასამართლოს 2017 წლის 8 მაისის გადაწყვეტილება საქმეზე No2/30577-16. სამოტივაციო ნაწილი, სამართლებრივი შეფასება პუნქტი 6.1.

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

¹⁴⁴ 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. ბმულზე <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.

ლსაც თავის მხრივ საფუძვლად უდევს ამერიკის შეერთებული შტატების საფოსტო ინსპექციის ოფიცრის საგამოძიებო მასალების მიმომხილველი ჩვენება.¹⁴⁵

პრაქტიკის საწყის ეტაპზე და ზოგადად არ უნდა იყოს რეკომენდებული მოსამართლემ გადაწყვეტილების გასამყარებლად გამოიყენოს სხვა ქვეყნის არა გადაწყვეტილება, არამედ ინსპექტორის საგამოძიებო მასალები და შემოგვთავაზოს იგი, როგორც გადაწყვეტილება.

სასურველი იქნებოდა სასამართლოს კიბერსქვათინგის განმარტება შემოეთავაზებინა, რადგანაც საქმის შემადგენლობა ძალიან მიახლოებულია კიბერსქვათინგთან, რაც არ მომხდარა, აღნიშნული შესაძლოა გამოწვეული ყოფილიყო იმით რომ კიბერსქვათინგი უშუალოდ სასაქონლო ნიშანთან არის დაკავშირებული,¹⁴⁶ კონკრეტულ შემთხვევაში კი მოსარჩელეს მოპასუხის დომენში გამოყენებული დასახელება რეგისტრირებული, როგორც სასაქონლო ნიშანი არ ჰქონია, მოპასუხის დომენის რეგისტრაციის მომენტისთვის, თუმცა 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.“¹⁴⁷

ყოველივე ზემოგანხილულიდან ნათელია რომ სასამართლო არა შეგნებულად არ ამახვილებს გარკვეულ სამართლებრივ მოცემულობებზე ყურადღებას, არამედ იგი უბრალოდ მზად არ აღმოჩნდა ინტერნეტსივრცეში წარმოშობილი ზიანისთვის შესაბამისი მკაფიო და ნათელი დეფინიციები ჩამოეყალიბებინა. მნიშვნელოვანია მოსარჩელე მხარის სწორი სამართლებრივი განმარტებების მიწოდება სასამართლოსთვის, რაც პრაქტიკის განვითარებას ხელს უწყობს.

სასურველი იქნებოდა, სასამართლოს განმარტებისთვის გამოეყენებინა ერთადერთი ნორმატიული აქტი, რომელიც დომენებსა და ვებსაიტებს შეეხება, მიუხედავად იმისა, რომ იგი აღმინისტრაციული მოწესრიგებისთვის გამოიყენება. საუბარია საქართველოს კომუნიკაციების ეროვნული კომისიის დადგენილება №3-ზე.¹⁴⁸ მოცემული ნორმატიული

¹⁴⁵ 2003 წლის 29 აგვისტოს საგამოძიებო ჩვენება და დაკავების ბრძანება იხ. ბმულზე <http://dnattorney.com/United%20States%20of%20America%20v.%20John%20Zuccarini.pdf> (ვიზიტის დრო: 24.06.2019).

¹⁴⁶ Uniform Domain Name Dispute Resolution Policy, Paragraph 4.; 15 U.S. Code §1125(d).

¹⁴⁷ თბილისის საქალაქო სასამართლოს 2017 წლის 8 მაისის გადაწყვეტილება საქმეზე No2/30577-16. ფაქტობრივი გარემოებები პუნქტი 3.19.

¹⁴⁸ 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,

აქტი იძლევა დომენის განმარტებას, რომლის მიხედვითაც ის არის „ინტერნეტ—სახელი, რომელიც ეკუთვნის ერთადერთ იურიდიულ ან ფიზიკურ პირს და ახდენს მის იდენტიფიცირებას და განსხვავებას სხვათაგან“.¹⁴⁹ ხოლო შინაარსობრივი დეფინიციის მიხედვით “ინტერნეტ—გვერდის დომენი არ უნდა იყოს დამაბნეველი, არ უნდა ემსახურობდეს სხვა ინტერნეტ—გვერდის გადაფარვას და უნდა შეესაბამებოდეს მის შინაარსს“.¹⁵⁰ 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 ისინი შეცდომაში არ შევიდნენ და არ მიადგეთ ზიანი. მოცემული დავა, თავის მხრივ განხილული აქტის ორივე კომპონენტს შეიცავს, მოპასუხე არევისტორებს დომენს რომლითაც ახორციელებს არაკეთილსინდისიერ კონკურენციასა და მეორე მხრივ, შეჰყავს მომხმარებელი შეცდომაში.

თუმცა, 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 თეორიის¹⁵¹ 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 სირთულეებთან არის აღნიშნული ტიპის დავები დაკავშირებული

1.3. საავტორო უფლებები ინტერნეტში

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

რომელმაც მოიცვა დომენი და ვებ გვერდის რეგულაცია. იხ. ბმულზე <https://matsne.gov.ge/ka/document/view/74110>.
¹⁴⁹ იქვე, მუხლი 2. ნაწილი 3. პ9 ქვეპუნქტი.
¹⁵⁰ იქვე, მუხლი 10. ნაწილი 1.
¹⁵¹ *ქონაშეილი ქ.*, ბრალი, როგორც სამოქალაქო სამართლებრივი პასუხისმგებლობის პირობა, სამართლის ჟურნალი, №1, თბილისი 2009, 83.

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 მატერიალს ქმნის, რაც თავისთავად დაცულია საავტორო უფლებით და იგი ათავსებს აღნიშნულ მატერიალს საკუთარ ვებგვერდზე სტატიებისა და სიახლეების სახით, მოპასუხესაც გააჩნია ვებგვერდი, სადაც იგი მოსარჩელის მიერ შექმნილ მატერიალს ნებართვისა და შეთანხმების გარეშე ათავსებდა, სისტემატურად და დიდი მოცულობით.¹⁵² ასევე, აღსანიშნავია, რომ სასარჩელო მოთხოვნამ 259 908.25 ლარი შეადგინა.

მოცემული საქმე წინ წამოწევს უკვე განხილულ ეგრეთ წოდებული უსაფრთხო ნავსადგომის (safe harbor) წესის არარსებობის პრობლემას ქართული სამართლებრივი სივრცისთვის, მიუხედავად იმისა, რომ მოპასუხემ ვერ დაამტკიცა, რომ იგი არ ათავსებდა მის ვებგვერდზე მოსარჩელის მიერ შექმნილ სტატიებსა და სიახლეებს, მნიშვნელოვან სამართლებრივ პრობლემას წააწყდებოდა სასამართლო თუ მოპასუხე შეძლებდა დაემტკიცებინა, რომ საიტზე საავტორო უფლებით დაცულ მატერიალს გარეშე პირები ანუ მომხმარებლები აქვეყნებდნენ. ასეთი შემთხვევისთვისაც კი სასამართლო აღნიშნავს, რომ ეკონომიკურ შემოსავალს სწორედ მოპასუხე იღებს და მნიშვნელობა არ აქვს თუ ვინ განათავსებს დაცულ მატერიალს მის საიტზე უფლების დარღვევით,¹⁵³ რაც ნიშნავს იმას, რომ მხოლოდ ეკონომიკური სარგებლის მიღება პასუხისმგებლობის დაკისრების საკმარისი პირობაა, რაც ცალსახად არასწორია. სასამართლომ სულ მცირე უნდა გაითვალისწინოს, რამდენად ინფორმირებულია ადმინისტრაცია ვებსაიტზე განთავსებული უფლების დამრღვევი მატერიალის შესახებ¹⁵⁴ და უშუალოდ აკონტროლებს თუ არა იგი ეკონომიკურ შემოსავალს ასეთი მატერიალიდან.¹⁵⁵ 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, შეერთებულ შტატებში უკვე დამკვიდრებულ ნორმატიულ მოწესრიგებას ეყრდნობა.

მნიშვნელოვანია ასევე მხარეთა წინდახედულობის როლი აღნიშნულ დავაში. მოსარჩელეს წინასწარ ჰქონდა მი-

¹⁵² თბილისის საქალაქო სასამართლოს 2019 წლის 7 თებერვლის გადაწყვეტილება საქმეზე N2/26484-15. ფაქტობრივი გარემოებები, პუნქტი 3.1.3.
¹⁵³ იქვე. ფაქტობრივი გარემოებები, პუნქტი 3.2.1.
¹⁵⁴ 17 U.S.C. § 512(c)(A).
¹⁵⁵ იქვე, § 512(c)(1)(B).

თითებული თითოეული მასალის ღირებულება საკუთარ ვებგვერდზე,¹⁵⁶ რამაც მას გაუმარტივა, როგორც მტკიცების ტვირთი სასარჩელო მოთხოვნის მოცულობასთან დაკავშირებით, ასევე, ააცილა დამატებითი ხარჯი, რომელიც ექსპერტიზასა და სხვა მოქმედებებს დასჭირდებოდა მიყენებული ზიანის შესაფასებლად. მეორადი პასუხისმგებლობის აცილების მცდელობას წარმოადგენს მოპასუხის ქმედება, რომელიც იხსნიდა პასუხისმგებლობას მომხმარებელთა გამოქვეყნებულ მასალაზე.¹⁵⁷

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 ერთჯერადი კომპენსაციაა, რომელიც მისაღები ფულადი ანაზღაურების ათმაგ ოდენობაზე ნაკლები არ უნდა იყოს, რაც თავის მხრივ ერთგვარ არასტანდარტულ სადამსჯელო კომპენსაციას¹⁵⁸ (punitive damages) წარმოადგენს, რაც ქართული ნორმატიული ბაზისთვის უიშვიათესი მოვლენაა და ემსახურება პირთა ანალოგიური ქმედების პრევენციას. ასევე, საყურადღებოა რომ სასამართლო აღნიშნული დავისთვისაც სამოქალაქო კოდექსით გათვალისწინებულ დელიქტურ ნორმებს უსადაგებს დავის გარემოებებს.

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

1.4. ონლაინ ცილისწამება

1.4.1. ნორმატიული საფუძვლების მისადაგება

საქართველოს სამოქალაქო კოდექსის მე-18 მუხლის მე-2 ნაწილის მიხედვით პირს უფლება აქვს დაიცვას საკუთარი პატივი, ღირსება, პირადი ცხოვრების საიდუმლოება, პირადი ხელშეუხებლობა ან საქმიანი რეპუტაცია სასამართლოს საშუალებით. სწორედ ამ ნორმატიულ დანაწესს უნდა შევესაბამოთ ონლაინ დეფამაცია ქართულ სამართლებრივ რეალობაში. მნიშვნელოვანია ისიც, რომ კანონმდებელი მე-18 მუხლით მოაზრებულ დეფამაციურ ქმედებას უკავშირებს დელიქტურ საფუძვლებს, შესაბამისად სა-

¹⁵⁶ თბილისის საქალაქო სასამართლოს 2019 წლის 7 თებერვლის გადაწყვეტილება საქმეზე N2/26484-15. ფაქტობრივი გარემოებები, პუნქტი 3.1.3.

¹⁵⁷ თბილისის საქალაქო სასამართლოს 2019 წლის 7 თებერვლის გადაწყვეტილება საქმეზე N2/26484-15. ფაქტობრივი გარემოებები, პუნქტი 3.1.6.

¹⁵⁸ *Visscher T. L., Tort Damages, Rotterdam Institute of Law and Economics (RILE) Working Paper Series No. 2008/02, 2008, 17-18.*

მოქალაქო კოდექსის 993-ე მუხლი პირს, რომელმაც განახორციელა ზიანის მომტანი ცნობების გავრცელება ან განმარტება, აკისრებს წარმოშობილი ზიანის ანაზღაურებას. ერთი შეხედვით შესაძლოა ქართული სამართლებრივი სივრცისთვის ჩაითვალოს რომ ონლაინ დეფამაციის ტრანსფორმაცია იგივე გზით ხდება, როგორც ეს შეერთებული შტატების შემთხვევაშია.

1.4.2. მტკიცების ტვირთი

პრობლემურია ინტერნეტ სივრცეში ცილისმწამებლური განცხადებების გავრცელებაზე პასუხისმგებელი პირის განსაზღვრის მტკიცების ტვირთი,¹⁵⁹ 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 ფაქტობრივად მოსარჩელისთვის დაუძლეველ მტკიცების ტვირთს ქმნის.

განსხვავებულ პრაქტიკას ამკვიდრებს უზენაესი სასამართლო ისეთი შემთხვევისთვის როდესაც ინტერნეტში გავრცელებული ცნობების ავტორის იდენტიფიცირება შესაძლებელია. საქართველოს უზენაესი სასამართლოს 2012 წლის 3 აგვისტოს გადაწყვეტილებით საქმეზე Nას-208-201-2012, დამკვიდრდა ერთგვარი პრეზუმფიცია, რომ თუ ვებგვერდის მომხმარებლის ანგარიში იძლევა ვარაუდს რომ ის მოპასუხეს ეკუთვნის იგი უნდა ჩაითვალოს მის პირად ანგარიშად. ხოლო, მტკიცების ტვირთი კი სწორედ მოპასუხეზე გადავა, ანგარიშის მისდამი კუთვნილების ნაწილში.

2. არასასამართლო პრაქტიკა კიბერსექვათინგი ქართულად

საქართველოს კომუნიკაციების ეროვნული კომისიის 2017 წლის 30 ნოემბრის გადაწყვეტილება N 793 / 16-ის¹⁶⁰

¹⁵⁹ *ჯორბენაძე ს.*, სამოქალაქო კოდექსის ონლაინ კომენტარი, civil-code.ge, 2017, მუხლი 18 55-ე ველი.

¹⁶⁰ საქართველოს კომუნიკაციების ეროვნული კომისიის 2017 წლის 30 ნოემბრის გადაწყვეტილება N 793 / 16 შპს „კავკასუს ონლაინის“ მიმართ სს „თბილისი ბანკის“ საჩივრის განხილვის თაობაზე, იხ. ბმულზე

მიხედვით ფიზიკურმა პირმა 4 დომენი 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 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 ეროვნულ კომისიას დომენებზე წვდომის შესაზღუდად, რაც უშუალოდ რეგისტრატორის მიმართ პრეტენზიაა და არა ფიზიკური პირის, რეგისტრანტის მიმართ.

მოცემულობის მიხედვით სახეზეა კიბერსქვათინგის ნათელი მაგალითი. ფიზიკურმა პირმა დაარეგისტრირა დომენები საქართველოში ერთ-ერთი ყველაზე დიდი კომერციული ორგანიზაციის, როგორც საფირმო, ისე სასაქონლო ნიშნის შემცველობით, რაც ერთ-ერთი კომპონენტია კიბერსქვათინგისთვის, ხოლო, ბოლო დომენის რეგისტრაციიდან მომდევნო დღეს კი უკვე სთავაზობს ნიშნის მფლობელს მათ შექენას. აღნიშნული ფაქტია რომ ფიზიკური პირის არაკეთილსინდისიერებაზე მიუთითებს, რაც კიდევ ერთ მახასიათებელს წარმოადგენს კიბერსქვათინგისთვის.¹⁶¹

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.¹⁶² ეგრეთ წოდებული მეორადი პასუხისმგებლობა რეგისტრატორებისთვის შეერთებული შტატების სასამართლოების მიერ შემოთავაზებული ცნებაა¹⁶³ 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.¹⁶⁴ პირველი კომპონენტი მოცემულ შემთხვევაში შესაძლოა სადავო გახდეს, თუმცადა დანარჩენი ორი რეგისტრატორისთვის უნდა გამოირიცხოს. ხოლო უმთავრესად უნდა აღინიშნოს რომ მსგავსი კომპონენტების გამოყენება და დამკვიდრება შესაბამის ნორმატიულ აქტებში ქართული კანონმდებლობისთვის უადრესად რეკომე-

ნდებულია, რათა მკაფიოდ გაიმიჯნოს რა შემთხვევაში შეიძლება მოთხოვნა მიესადაგებოდეს დომენის რეგისტრატორს და რა შემთხვევაში უნდა დაეკისროს მას პასუხისმგებლობა.

უდავოდ საინტერესოა მეორადი პასუხისმგებლობის საკითხი ქართული რეგისტრატორისთვის, თუმცადა 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.

კრიტიკისთვის უნდა ითქვას, რომ იურიდიულ ლიტერატურაში გამოთქმული მართებული მოსაზრება, რომ სასამართლოს მიერ მსგავსი ტიპის დავების განხილვა, სადაც საქმე ინტელექტუალურ საკუთრებასა და დომენს შეეხება, უფრო მეტად მიზანშეწონილია, რომ მოხდეს სპეციალური არბიტრის მიერ,¹⁶⁵ მიუთითებს იმაზე, რომ საქართველოს კომუნიკაციების ეროვნული კომისია, როგორც ადმინისტრაციული ორგანო მითუმეტეს ვერ იქნება კომპეტენტური მსგავსი შინაარსის დავა განიხილოს. რაც შეეხება უშუალოდ პირს რომელმაც სადავო დომენები დაარეგისტრირა ადმინისტრაციული წარმოების ფარგლებში ვერ იქნება საშუალება ადეკვატური შეპასუხება განახორციელოს მისი ქმედების მართლზომიერების დასადასტურებლად.

V. შეჯამება

ინტერნეტსივრცეში მიყენებული ზიანი, როგორც სამართლებრივი მოვლენა შესაძლოა მოწესრიგებული იყოს უკვე არსებული ტრადიციული დელიქტური სამართლის მიხედვით, თუმცადა აღნიშნული ტრანსფორმაცია ყოველთვის წარმატებული არ არის, როგორც ეს კიბერხელყოფის შემთხვევაში აღმოჩნდა, ხოლო რიგ შემთხვევებში წარმატებული ტრანსფორმაცია მხოლოდ შესაბამისი ცვლილებებით არის შესაძლებელი, რისი ნათელი მაგალითიც შეერთებულ შტატებში წუნდებული პროდუქტით გამოწვეული ზიანისთვის ეკონომიკური დანაკარგის დოქტორის დოგმატური მიდგომის ჩანაცვლებაა.

ევროპის კავშირისთვის ნორმატიული მოწესრიგების შემავსებლად პრაქტიკის განვითარება უნდა იყოს მოაზრებული. მიუხედავად იმისა, რომ უკვე არსებობს სახელმძღვანელო პრაქტიკა, იგი მაინც ნაკლოვანია.

საქართველოში განხილული საკითხის პრაქტიკული მნიშვნელობა, განპირობებულია, როგორც ტექნოლოგიური და სამართლებრივი სიახლით, ასევე, საზოგადოების დამოკიდებულებით ინტერნეტის მიმართ. გარდა პოზიტიური ასპექტებისა, რაც კომუნიკაციისა და სხვადასხვა ტრანზა-

<http://www.gncc.ge/ge/legal-acts/solutions/2017-793-16.page> (ვიზიტის დრო: 24.06.2019).
¹⁶¹ Uniform Domain Name Dispute Resolution Policy, Paragraph 4.; 15 U.S. Code §1125(d).
¹⁶² *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.
¹⁶³ იქვე.
¹⁶⁴ *Barbantonis F. N.*, Should Contributory Cybersquatting be Actionable?, North Carolina Journal of Law & Technology, Vol. 17, Issue 1, 2015, 97.

¹⁶⁵ *Singh H.*, Domain Name Disputes and Their Resolution under UDRP Route: A Review, Archives of Business Research, Vol.6, No.12, 2018, 150.

ქცის სიმარტივეს უკავშირდება, ინტერნეტი, მის მომხმარებლებს ნეგატიური ქმედების სიმარტივისა და შესაბამისი პასუხისმგებლობის არდაკისრების ვარაუდს უქმნის, რაც ნათლად გამოჩნდა განხილული ქართული სასამართლო პრაქტიკის მიხედვით, სადაც ორი კომპანიისთვის ინტერნეტ სივრცე არაკეთილსინდისიერი კონკურენციის პლატფორმად და ასპარეზად გადაიქცა. ხოლო, ინტერნეტში უფლების დარღვევის სიმარტივის თვალსაჩინო მაგალითად კი საავტორო უფლებებით დაცული მატერიალის საინფორმაციო ვებგვერდზე „გადაკოპირება“ გამოდგება.

ინტერნეტ სივრცეში განვითარებული ურთიერთობების კიდევ უფრო აქტუალურად და მნიშვნელოვნად გადაქცევა გარდაუვალია, როგორც მსოფლიოსთვის, ასევე, საქართველოსთვის, გამომდინარე იქიდან, რომ ინტერნეტსივრცე 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.