

ინტერნეტ-სივრცის რეგულირება და უსაფრთხოება

რატი აბულაძე

ეკონომიკის დოქტორი

თსუ პროფესორი

ცენზურის ფენომენი ისეთივე ძველია, როგორც ცივილიზაცია და წარმოადგენს დიქტატურის დამახასიათებელ მოვლენას. ინტერნეტი, როგორც ყველაზე დინამიურად განვითარებადი ინფორმაციულ-კომუნიკაციური ტექნოლოგია გახდა ცენზურის იმპულსი და რეგულირების ხელშეწყობი, როგორც საზოგადოების იდეების გამოხატვის, გენერირებისა და ინფორმაციის კონტროლის რესურსი. ინტერნეტ-ცენზურის მოტივი არ განსხვავდება სხვა მასობრივი ინფორმაციის საშუალებების ცენზურის მოტივისაგან.

ცენზურის თემა მრავალფეროვანია, რომელიც შეიძლება მოიცავდეს პოლიტიკურ, ეთნიკურ, შეიარაღებულ კონფლიქტს, სხვადასხვა მიმდინარეობებს, მორალურ მიზეზებს (როგორც ამორალური), მუსულმანურ ქვეყნებში აზარტული თამაშებს, ნარკომანიას, რწმენის საკითხების განხილვას, ქალთა უფლებების დაცვას (ირანში), ავტორთა უფლებების დაცვას, დისკრიმინაციას და სხვა საკითხებს.¹

რეპრესიული რეჟიმების მიერ მომხმარებლებისათვის ინტერნეტში ინფორმაციასთან თავისუფალი წვდომის შემზღუდავი ტექნიკური და არატექნიკური ღონისძიებებია: ინტერნეტ-მომხმარებლის საქმიანობის მონიტორინგი, განსაზღვრულ web-საიტებთან მომხმარებლის დაშვების უარყოფა (ბლოკირება), ინტერნეტ-მომხმარებლის თვალყურის დევნება და მონაცემთა ნაკადის ფილტრაცია, საიტის ოპერატორებისათვის ცენზურის წესების დაცვით კონტენტის ადაპტირების სწავლება, ინტერნეტ-ბლოკირება და ჩახშობა.²

კიბერსივრცეში ცენზურისა და ინტერნეტ-მომხმარებლების კონტროლირებისათვის სახელმწიფოები იყენებენ IP-მისამართების ბლოკირებას, ვირუსებით ბლოკირებას, პროგრამების ინფექციით დაზიანებას, DNS გატაცება/გადამისამართებას, TCP კონტენტურ ფილტრაციას, პერსონალური ინფორმაციის შეგროვებას, წვდომის სიჩქარის შემცირებას, სოციალურ ზემოქმედებას, განსაზღვრული web-გვერდების გადამისამართებას სამთავრობო პროპაგანდის ტრანსლირებისათვის, ე-ფოსტაზე შეღწევისა და გასუფთავებას, ყალ-

ბი ინტერნეტ-საიტების შექმნას და სხვა მეთოდებს.

ინტერნეტ-ცენზურა ზღუდავს საზოგადოების ფუნდამენტალურ უფლებას. ამ უფლების სრულ განხორციელებას გადამწყვეტი მნიშვნელობა აქვს პირადი თავისუფლებისა და დემოკრატიის განვითარებისათვის. ის არა მხოლოდ გადამწყვეტ როლს თამაშობს სიღარიბის მიზეზებთან ბრძოლაში, ასევე ყველაზე მძლავრი ძალაა მშვიდობის განმტკიცებისა და კონფლიქტის გადაჭრისთვის,³ ეკონომიკური წინსვლისა და ზრდისთვის.

ცენზურის იდეა შენიღბულია სამი ძირითადი სოციალური ინსტიტუტის - ოჯახის, ეკლესიისა და სახელმწიფოს დაცვის სახით.⁴

ცენზურის კონტექსტში ძირითადია პოლიტიკური მოტივი, რომლის კონტექსტშიც სხვადასხვა ქვეყნის რეჟიმის მიერ მკაცრად კონტროლირდება ან იბლოკება ოპოზიციური ჯგუფების, რისკ ჯგუფებისა და კრიტიკული იდეების საზოგადო წარმოდგენა, ინტერნეტ-ტრაფიკი, ქვეყნის საზღვრებს გარეთ მომუშავე „არასასურველი“ საიტების მუშაობა.¹ მსოფლიოს მრავალ ქვეყანაში ინტერნეტის სახელმწიფო შეზღუდვა გამოიყენება ყოვლისმომცველი და შეუთავსებელი წესებით, რომელიც ხალხს იჭერს ავტონომიურ რეჟიმში და გაქრობით აშინებს პოლიტიკურ ოპოზიციას. ინტერნეტის რეგულირება დიქტატურის მსგავსია, რომლითაც რეჟიმი ახშობს, გმობს ან აშინებს თავისუფალ სიტყვას.⁵ ამიტომ ინტერნეტის რეგულირების პოლიტიკასთან კავშირში დღის წესრიგში ძირითადად დგას სიტყვის თავისუფლების საკითხი, როცა სიტყვის თავისუფლება იკარგება, ყველა დანარჩენის თავისუფლებაც ეცემა.

სახელმწიფოს პოლიტიკა ინტერნეტ-ცენზურის მიმართ შეიძლება დაჯგუფდეს 4 კატეგორიაში:⁶

- ინტერნეტ-ინდუსტრიის თვითრეგულაციასა და საბოლოო მომხმარებლის მიერ ფილტრაციის/ბლოკირების ტექნოლოგიის ნებაყოფლობითი გამოყენების პოლიტიკური ხელშეწყობა (კანადა, დასავლეთ ევროპის ქვეყნები);

- სისხლის სამართლებრივი სასჯელები (ჯარიმები ან პატიმრობა), გამოყენებული კონტენტის პროვაიდერების მიმართ, რომლებიც ონლაინში ქმნიან და გენერირებენ „არასრულწლოვნებისათვის შეუფერებელ“ კონტენტს (აშშ);

- კონტენტთან წვდომის ბლოკირების სამთავრობო მანდატი (სინგაპური);

■ ინტერნეტთან საჯარო წვდომის სახელისუფლებო აკრძალვა (ან რეგისტრაცია/ნებართვა). ასეთი ქვეყნების რაოდენობა ოფიციალურად სამ ათეულზე მეტია.

ცენზურა ხელს უშლის ვაჭრობას, მნიშვნელოვან ბარიერს წარმოადგენს ინტერაქტიული მომსახურების წარდგენისათვის და ძლიერ ზეგავლენას ახდენს ბიზნესის განვითარებაზე (რადგან შეიძლება მონოპოლიურ მდგომარეობაში აღმოჩნდეს. მაგალითად, Baidu).⁷

ინტერნეტ-ესკალაცია, ინტერნეტ-ფილტრაცია და სანქციები ანელებს კომერციის მუშაობას, ინტერნეტ-მომხმარებელთა აქტივობასა და ჩართულობას, ინტერნეტ-მომხმარებელს უკარგავს ქსელში ყოფნის სურვილს და არ ქმნის ხელსაყრელ ბიზნეს კლიმატს.

დღეისათვის საჯარო ფაქტს წარმოადგენს კორპორატიული სექტორის მიერ საძიებო შესაძლებლობებისა და ინფორმაციის მართვა, მომხმარებლის პირადი ინფორმაციის ნახვა და შეგროვება, დაშვების კონტროლი და მონიტორინგი.

Google, Yahoo, AOL, Microsoft აგროვებს კონფიდენციალურ ინფორმაციას, ახდენს მათ კლასიფიცირებას, სეგმენტირებას და ამ ინფორმაციას იყენებს მიზნობრივი რეკლამის დემონსტრირებისთვის.⁸ თუმცა, როგორც ამერიკელი პროფესორი ნისენბაუმი (Helen F. Nissenbaum) აღნიშნავს, ყველაფერი, რაც კეთდება, შემთხვევები რომელიც ხდება, ოპერაციები რომელსაც აქვს ადგილი, ხდება არა მხოლოდ განსაზღვრულ კონტექსტში, არამედ პოლიტიკის, კულტურისა და საერთო თანხმობის მოლოდინისაგან, ხოლო ტექნოლოგიების გამოყენების საკვანძო პრინციპს წარმოადგენს სოციალური გაგების დინამიკა და შეთანწყობისთვის მორგებული პოლიტიკა.⁹

ინტერნეტ-ცენზურა შეიძლება განვიხილოთ როგორც არასასაქირო, ხელისუფლების არაკანონიერი, ირაციონალური მცდელობა აკონტროლოს, სამოქალაქო და კერძო სექტორის ინფორმაციის ნაკადი ინტერნეტში. რომელიც მორალურად დასაძრახისია, ქმნის დიდ შესაძლებლობებს შიდა სამთავრობო კორუფციისათვის,¹⁰ იწვევს ქვეყნის ჰერმეტიულობას, ქსელურ ვაკუუმსა და „დახურულ პროტექციონიზმს“.

საზოგადოება აღარ კონტროლირდება ექსკლუზიურად ცენტრალური დაზვერვის მიერ, არამედ მაკონტროლებელი მოწყობილობების გავრცელება და დაზვერვა ნაწილდება მრავალფეროვან ერთეულ ქმედებებში (პროცესებში). ამ ქმედებების კოორდინირება ჩართულია

ინფორმაციის გაცვლისა და სხვა შესაბამისი რესურსების პარალელურ მოქმედებებში.¹¹

ინფორმაციის ნაკადის რეგულირებითა და მიდგომებით გამოყოფენ 4 ტიპის ქვეყანას:¹²

- ლიბერალური ქვეყნები, რომლებიც გამოდიან მონაცემების თვითრეგულირებისა და ნებაყოფლობითი ფილტრაციით. ამ ჯგუფის ქვეყნებში საბავშვო პორნოგრაფიის, მასალების, ძალადობის პროპაგანდის, ნაციზმის და ა.შ. პუბლიკაცია, წარმოადგენს უკანონოს, თუმცა ინფორმაციასთან წვდომა ნებაყოფლობითი ხასიათის მატარებელია და ცენზურით არ იზღუდება (კანადა, დიდი ბრიტანეთი, დასავლეთ ევროპის ქვეყნები);

- ქვეყნები, რომლებიც გამოდიან ონლაინ რეჟიმში ინფორმაციასთან თავისუფალი დაშვების წინააღმდეგ „მხოლოდ არასრულწლოვნებისათვის“ (ახალი ზელანდია, აშშ-ი, იაპონია, ტაივანი, ინდონეზია);

- ქვეყნები, რომლებსაც ქსელში ინფორმაციასთან შეზღუდული წვდომა აქვთ. აკრძალულია უხამსი ხასიათის, პოლიტიკური, ახალი ამბების, „საფრთხის შემცველ“ ინფორმაციასთან და სხვა საინფორმაციო საიტებთან წვდომა (მაღაიზია, ტაილანდი, თურქეთი, არაბთა გაერთიანებული ემირატები, ინდოეთი, ყაზახეთი, ტუნისი, ავსტრალია, შრილანკა, ბაჰრეინი და სხვა).¹³

- ქვეყნები, სადაც ინფორმაციასთან თავისუფალი წვდომა აკრძალულია. ასეთი „ინტერნეტის მტერი და რეპრესიული რეჟიმის ქვეყნებია“:¹³ მიანმარი, ჩინეთი, ირანი, კუბა, ჩრდილოეთ კორეა, საუდის არაბეთი, სირია, თურქმენეთი, უზბეკეთი, ვიეტნამი, ბელარუსია, ბაჰრეინი.

ქვეყნების უმრავლესობა აშკარად (მაგალითად, ვენესუელას ეროვნული კანონმდებლობით აქვთ დამტკიცებული) თუ ფარულად (ინფორმაციული დაბლოკვით) მიზანშეწონილად იყენებს ინტერნეტ-ცენზურას, როგორც სახელმწიფოს მართვის შემადგენელ კომპონენტს, სადაც რეგულირების სახელი და მექანიზმი რაციონალიზებულია.

საერთაშორისო ორგანიზაციის „Reporters Without Borders“-ის ანგარიშით „ინტერნეტ-რეგულირების პრობლემების“ მქონე ქვეყნების 44%-ზე მეტი აზიის რეგიონიდანაა, 22% - შუა აღმოსავლეთის რეგიონის ქვეყნებია, აფრიკისა და ევროპის რეგიონის ქვეყნების წილი შეადგენს 13%-ს (თითოეული), ხოლო ლათინური ამერიკის და ოკეანისპირა რეგიონების ქვეყნების წილი 4%-ს (თითოეული).¹³

The open net-ის ანგარიშით გარკვეული ხარისხის ინტერნეტ-ფილტრა-

ციას ანარმოებს 59 ქვეყანა.¹⁴ თავისუფალი პრესის ხელშეწყობი ორგანიზაციის (CPJ-Committee to Protect Journalists) კვლევით ცენზურის მქონე ქვეყნების ტოპ ათეულში ლიდერობს ერიტრია, მეორე და მესამე ადგილებს ინანილებს ჩრდილოეთ კორეა და სირია, ხუთეულში შედის ირანი და ეკვატორული გვინეა, მე-6 ადგილს იკავებს უზბეკეთი, მას მოსდევს ბირმა, საუდის არაბეთი, კუბა და ათეულს აბოლოებს ბელარუსი.¹⁵

აღსანიშნავია, რომ ცენზორი სახელმწიფოების საერთო რაოდენობა არაოფიციალურად გაცილებით მეტია, რადგან ინტერნეტ-ცენზურა და კონტენტის ფილტრაცია არ აფიშირდება და გასაიდუმლოებულია, ამიტომ ცენზორი სახელმწიფოების სტატისტიკის სრული სურათის ასახვა რთულია.

თუმცა ცენზურას უარყოფითი კონტექსტის გარდა აქვს პოზიტიური მხარეც, კერძოდ: ინტერნეტ-რეგულირებას საჭიროებს არასრულწლოვნების უფლებების დაცვა, ექსტრემიზმის, ნაციზმის, რასიზმის, სიონიზმის და რელიგიის პროპაგანდა, ასევე სხვა ფორმის შეუწყნარებლობა, ძალადობა, სისასტიკე, ანტისემიტიზმისა და ტერორიზმის პროპაგანდა, „ჩრდილოვანი სერვერის ეკონომიკის“ სტიმულირება და სხვა.

ინტერნეტ-რეგულირებისა და კონტროლის „ჯანსაღ“ საკანონმდებლო მოდელს იყენებს აშშ, რომლის „არასრულწლოვანთა კერძო ცხოვრების დაცვის აქტი“ ინტერნეტში ბავშვების (13 წლამდე) მუშაობის რეგულირებისა და ეფექტური კონტროლის უზრუნველყოფისათვის ახდენს web-რესურსების აუცილებელ კლასიფიკაციასა და ფილტრაციას.²⁰

სპეციალური ფილტრებს იყენებს ევროპის საზოგადოება მანერე კონტენტის (საბავშო პორნოგრაფიის, რასიზმის, ტერორიზმის, სიძულვილის გაღვივების მიმართულებით) ცენტრალიზებული გაცხრილვის სახით. ფილტრაცია ხდება დიფამაციის კანონის საფუძველზეც. იფილტრება ისეთი სფეროები, როგორიცაა საავტორო უფლებების დაცვა, აზარტული თამაშები. ინტერნეტ-მომსახურების პროვაიდერების (ISP), საძიებო სისტემების და კონტენტ-პროვაიდერების ფილტრაცია, წარმოადგენს „ნებაყოფლობით“ და ხორციელდება იმ შეგნებით, რომ სახელმწიფო ორგანოებთან თანამშრომლობის უგულვებლყოფა გამოიწვევს იძულებით საკანონმდებლო რეგულირების ღონისძიებებს.¹⁶

ევროპაში არსებული ინტერნეტ-რეგულირების კანონმდებლობა

პიზნატი, მენეჯმენტი, მარკეტინგი

არეგულირებს ინტერნეტის უსაფრთხო გამოყენებას სკოლებში და სტიმულირებს მომხმარებელთა ინფორმირებასა და თავდაცვის სწავლების პროგრამებს.¹⁷

თუმცა, ინტერნეტის სტრუქტურა განაპირობებს როგორც ინტერნეტ-ცენზურის, კონტროლისა და ბლოკადის, ისე მისი თავიდან აცილების შესაძლებლობას. ინტერნეტ-ცენზურის გვერდის ავლის პოპულარული ტექნოლოგიებია: Freenet, Freerate, GPass, FirePhoenix, Triangle Boy, Hotspot Shield Tor (The Onion Router), Garden, UltraSurf, DynaWeb, Psiphon, UltraReach და სხვა (იხ. ცხრილი 1).

ცხრილი 1 ინტერნეტ-ცენზურის გვერდის ავლის გავლენიანი ტექნოლოგიები*

ტექნოლოგია	მწარმოებელი	მახასიათებელი
Freenet	შემუშავებულია იან კლარკის (Ian Clarke) მიერ 1991 წელს.	ტექნოლოგია მხარს უჭერს ანონ-იმური მასალების შენახვასა და ძიებას;
Triangle Boy	შემუშავებულია SafeWeb-ის (www.safeweb.com) მიერ (2000 წელს).	ტექნოლოგია უზურუნველყოფს სერვერებიდან web-გვერდების შეუფერხებლად მიღებას, IP ბლოკირებისა და ინტერნეტ-ფილტრაციის თავიდან აცილებას. გავრცელებულია საუდის არაბეთ-სადა ჩინეთში.
Garden	შემუშავებულია Garden-ქსელის მიერ (www.gardennetworks.com) (2001 წელს).	ანტი-ცენზურის სისტემა, როგორც პირველ ინტელექტუალური პროექსი სისტემა, რომელიც პოპულარულია ჩინეთში, რადგან გაიმარჯვა GFW ცენზურაზე. ტექნოლოგია მუდმივად ახლდება და იხვეწება მოხალისთა სპეციალური ჯგუფის მიერ.

UltraSurf	შემუშავებულია კომპანია UltraSurf-ის www.ultrareach.com მიერ. (2002 წლიდან)	ანტი-ცენზურის ფლაგმანი web-საიტის თავისუფლად დაათვალიერების, ე-ფოსტის (UltraMail) უსაფრთხოების მომსახურების, დატვირთვის ბალანსირებისა და დეფექტების შემთხვევაში მუშაობის შესაძლებლობას იძლევა.
DynaWeb	შემუშავებულია Dynamic Internet Technology Inc. (DIT) მიერ (2001 წელს).	ანტი-ცენზურის მომსახურების ნაკრები. 2002 წელს DIT-მა წარმოადგინა მომსახურება ცენზურის წინააღმდეგ DynaWeb-ის ჩარჩოებში. DynaWeb-ი წარმოადგენს web-ზე დაფუძნებულ ანტი-ცენზურის პორტალს. DIT-ს გამოქვეყნებული აქვს ინტერნეტ-ცენზურის ოპერაციების ტექნიკური ანალიზი და რეკომენდაციები (http://www.dit-inc.us/press.php);
Tor (The Onion Router)	შემუშავებულია აშშ-ის Naval Research Laboratory-ის ხელშეწყობით. 2004 წელს მემკვიდრეობით გადაეცა Electronic Frontier Foundation-ს (EFF)	ანტი-ცენზურისადმი ბრძოლის არსენალის ტექნოლოგია;
GPass და Fire-Phoenix	შემუშავებულია World's Gate Inc. (WG) მიერ. (2006 წლის ზაფხული)	ტექნოლოგია, მსხვილი და საიმიედო ინტერნეტ-პლატფორმების აგებით საიმიედო მომსახურებას სთავაზობს მომხმარებლებს. ძირითადად ფოკუსირებულია განსაკუთრებით რეპრესიული რეჟიმში მყოფ მომხმარებლებზე.
Freegate	შემუშავებულია აშშ-ის The Global Internet Freedom Consortium-ის მიერ.	ირანში პოპულარულია ანტი-ცენზურის პროგრამა UltraReach და Freegate.

პიონერები, მენეჯერები, მარკეტინგები

Hotspot Shield	შემუშავებულია ინტერნეტ-კომპანია AnchorFree-ის მიერ.	უფასო და რეკლამის მხარდაჭერით ინტერნეტ-მომხმარებლების მონაცემების დაშიფვრისა და მათი იდენტურობის დამალვის შესაძლებლობას იძლევა (ამჟამად 7.5 მლნ მომხმარებელი ჰყავს მსოფლიოში).
Psiphon	შემუშავებულია ტორენტის უნივერსიტეტის სამოქალაქო ლაბორატორიის მიერ.	ინტერნეტ-ცენზურასთან ბრძოლის ინსტრუმენტი, რომელიც ბლოკირებული საიტების აღდგენისა და ელექტრონული მოსმენის გაშიფვრის საშუალებას იძლევა.

***ცხრილი აგებულია სხვადასხვა წყაროს საფუძველზე**

ასევე ცენზურის გვერდის ავლა შესაძლებელია ისეთი ტექნოლოგიური ინოვაციებით, როგორიცაა: პროქსი სერვერები, ვირტუალური კერძო ქსელები (VPNs), iPhones, BlackBerry და სხვა, რომელიც არ იძლევა ინტერნეტ-კონტროლის, მოსმენისა და ელექტრონულ რეჟიმში არსებული ინფორმაციის, პორტფელის მონიტორინგის, მიმოწერის გაკონტროლების შესაძლებლობას.¹⁸

დაბოლოს, ინტერნეტ-სივრცეში არსებული ცენზურიდან გამომდინარე შეიძლება დავასკვნათ, რომ:

- ცალკეულ ქვეყნებში ადგილი აქვს პრივატიზებულ ცენზურასა და ციფრულ მკარტიზმს;¹⁹
- ინტერნეტ-კონტროლის უზრუნველყოფისთვის ცენზორების სამართლებრივი ვარიანტები ფართოა;
- დღეისათვის ავტორიტარული რეჟიმები ახორციელებენ ამბიციურ, კარგად დაგეგმილ სტრატეგიას საინფორმაციო საკომუნიკაციო ტექნოლოგიების სფეროში, რისთვისაც იყენებენ სამართლებრივ, ტექნიკურ და სოციალურ ღონისძიებებს ინტერნეტის მოხმარების განვითარების მოდელში (მაგალითად, სინგაპური);^{20; 21}
- ცალკეული ქვეყნის რეჟიმი „სტაბილურობის შენარჩუნებისთვის“ ატარებს მკაცრ ინტერნეტ-კონტენტის კონტროლსა და პრევენციას „გამანადგურებელი“ ინფორმაციის გავრცელების წინააღმდეგ;
- ინტერნეტ-ცენზურის შედეგად დემოკრატიზაციის პროცესი

კარგავს იმპულსს, რომელიც ნეგატიურ ზემოქმედებას ახდენს ინტერნეტში საკუთარი შეხედულების თავისუფალ გამოხატვაზე;

- ზოგადად ცენზურის სრული სურათის ასახვა და მისი დეტალიზების მონაცემის მოპოვება რთულია, რადგან კვლევის ნებისმიერი მონაცემი ეყრდნობა ადმინისტრაციულ, გაფილტრულ ინტერნეტ-მონაცემს.

ამრიგად, ინტერნეტ სივრცეში არსებული ცენზურის ტენდენციების საფუძველზე საზოგადოებრივი ხასიათის გასატარებელი ღონისძიებებია:

- ინტერნეტის კულტურული გამოყენების, ინტერნეტ-საზოგადოების სიფხიზლისა და აგრესიული ინტერნეტ-კონტენტის პრობლემის გათვითცნობიერების დონის ამაღლებისათვის უნდა გატარდეს საგანმანათლებლო და სოციალური აქტივობა;

- ფილტრაცია უნდა მოხდეს დიფამაციის კანონის საფუძველზე. უნდა შეიქმნას ინტერნეტის რეგულირების კანონპროექტები და მოხდეს მისი საერთაშორისო ექსპერტიზა;

- ეროვნული და საერთაშორისო კანონმდებლობით უნდა დარეგულირდეს ბუნდოვანი განსხვავება ნებაყოფლობით და სავალდებულო ფილტრაციას შორის;

- სახელმწიფოსთვის ეროვნული კანონმდებლობით უნდა განისაზღვროს ინტერნეტ-კონტენტის რეგულირების წესები, თვითრეგულირება და ერთობლივი რეგულირება, ინტერნეტ-მომხმარებლის ანონიმურობა, ინტერნეტის მეშვეობით მომსახურების წარდგენის თავისუფლება, ინფორმაციული კონტენტის სერვისის პროვაიდერებისათვის პასუხისმგებლობა, სახელმწიფო კონტროლის უქონლობა, მოქალაქეების ინფორმაციულ საზოგადოებაში ჩართვისათვის ბარიერების მოშორება და სხვა;¹⁹

- კორპორაციული სექტორის მიერ ინტერნეტ-მომხმარებლებთან შეთანხმების გარეშე დაგროვილი ინფორმაციის გამოუყენებლობა უნდა გაკონტროლდეს კანონმდებლობით;

- ინტერნეტ-გარემოს ცენზურისათვის უნდა შეიქმნას საერთაშორისო შეზღუდვის წესები, არსებული რეგულირების დასაშვები ფორმები, შესაბამისობაში უნდა იყოს როგორც ეროვნულ კანონებთან ისე საერთაშორისო სამართლის ნორმებთან, რაც საბოლოოდ უნდა გაკონტროლდეს საერთაშორისო მონიტორინგის სისტემით. ის რაც ერთ ქვეყანაში არალეგალურს წარმოადგენს და მიიჩნევა არასწორად,

პიზნატი, მენეჯმენტი, მარკეტინგი

მეორე ქვეყანაში საესეებით კანონიერია. რაც წინააღმდეგობაში მოდის სახელმწიფოების კანონმდებლობასთან;

- მსოფლიო ქსელი არ უნდა განიცდიდეს ძალიან მკაცრ შეზღუდვას, სადაც ნებისმიერი ინტერნეტ-რეგულირება ქსელში შეიძლება იყოს მხოლოდ ნებაყოფლობითი, საზოგადოების მიერ შერჩეული კონტენტის ფილტრაციის სისტემის არჩევით. საზოგადოება ინფორმირებული უნდა იყოს ცენზორის ცენტრის/ცენტრებისა და მათ მიერ განსაზღვრული რეგულირების წესების შესახებ, რაც საზოგადოების ნდობას ანმტკიცებს და მართველობის პროცესის ეფექტურობას ზრდის;

- სახელმწიფო ინტერნეტ-წვდომას უნდა უდგებოდეს როგორც მოსახლეობის „ფუნდამენტალურ უფლებას“, ხოლო „ინტერნეტი უნდა იყოს ნდობის სივრცე. წინააღმდეგ შემთხვევაში, ინტერნეტი მოქმედი ძალით გახდება შხამიანი და სახიფათო ვიდრე სასარგებლო;

- ცენზურით ადამიანს ვერ გარდაქმნი, ის მხოლოდ გაჩუმდება. ამიტომ ცენზურა უნდა ეფუძნებოდეს კონსესუსს, ინტერნეტ-რეგულირებაში სამოქალაქო სექტორის ჩართულობას, წინააღმდეგ შემთხვევაში ინტერნეტ-მომხმარებლები გაბედული თვითორგანიზებით მოახდენენ ცენზურის გვერდის ავლას;

- რასაკვირველია ყველა სახის ინტერნეტ-საიტის „კონტროლირება“ შეუძლებელია იგივე გზით, როგორც ტრადიციული მედიის, რადგან სამოქალაქო და კორპორაციული სექტორის შესაძლებლობები, რესურსები და განფენილობა ცვლის ურთიერთდამოკიდებულებას, კონტროლსა და რეგულირებას.

გამოყენებული ლიტერატურა

1. Hindley B., Lee-Makiyama H. Protectionism Online: Internet Censorship and International Trade Law.

ECIPE Working Paper. No. 12/2009. <http://www.ecipe.org/publications/ecipe-working-papers/protectionism-online-internet-censorship-and-international-trade-law/PDF>

2. Global Internet Freedom Consortium (GIFC). Defeat Internet Censorship: Overview of Advanced Technologies and Products. November 21, 2007. http://www.internetfreedom.org/archive/Defeat_Internet_Censorship_White_Paper.pdf

3. <http://www.article19.org/data/files/pdfs/publications/iran-art-censorship.pdf>
4. <http://gilc.org/speech/osistudy/censorship/>
5. <http://www.reuters.com/article/idUSL2774335120070727>
6. <http://www.efa.org.au/Issues/Censor/cens3.html>
7. <http://www.newsland.ru/news/detail/id/432229/cat/69/>
8. http://www.nytimes.com/2008/03/20/business/media/20adco.html?_r=1
9. The Office of the Commissioner of Canada. Social Network Site Privacy, A Comparative Analysis of Six Sites. February, 2009. http://www.priv.gc.ca/information/pub/sub_comp_200901_e.pdf
10. <http://www.mannkal.org/downloads/scholars/internet-censorship-in-australia.pdf>
11. Messner D., Meyer-Stamer J. Governance and Networks. Tools to Study the Dynamics of Clusters and Global Value Chains. IDS/INEF Project “The Impact of Global and Local Governance on Industrial Upgrading” Duisburg, February 2000. http://home.furb.br/wilhelm/COMPETIV/JMS_governance_tools.pdf
12. <http://ouin.ru/usa1/>
13. www.rsf.org
14. <http://www.gtnoise.net/papers/2010/burnett:usenixsec2010.pdf>
15. <http://cpj.org/reports/CPI.Ten.Most.Censored.5.2.12.pdf>
16. Лоскутов И. Сравнительный анализ международных норм законодательного регулирования Интернета в различных странах (2008 г.). **International Foundation of speech Freedom Protection** “Adilsoz”. <http://www.adilsoz.kz/site.php?lan=russian&id=785>
17. www.netpolice.ru/article/regul/regul_3.html
18. <http://www.voanews.com/georgian/news/-----100687384.html>
19. www.wikileaks.org
20. Rodan G. “The Internet and Political Control in Singapore”, Political Science Quarterly, volume 113, number 1 (Spring), 1998. pp. 63-89.
21. Hwa Ang P. “How Countries Are Regulating Internet Content”, paper presented at the 1997 Annual Meeting of the Internet Society, Kuala Lumpur, Malaysia, 25-27 June 1997.