P-ISSN 1987-7668 / E-ISSN 2720-782X
https://doi.org/10.60131/jlaw.2.2024.8331

ქეთევანი კუკავა*

პირადი ცხოვრების ხელშეუხებლობა და პერსონალურ მონაცემთა დაცვა v. ეროვნული უსაფრთხოების დაცვა და დანაშაულის წინააღმდეგ ბრძოლა: ევროკავშირის სამართლისა და სასამართლო პრაქტიკის ანალიზი

ტექნოლოგიური პროგრესის თანმდევი რისკების გათვალისწინებით, თანამედროვე მსოფლიოში პერსონალურ მონაცემთა დაცვის აუცილებლობა მნიშვნელოვნად გაიზარდა. ციფრულმა ტექნოლოგიამ, არაერთ სარგებელთან ერთად, მეთვალყურეობის უპრეცედენტო შესაძლებლობაც შექმნა, რაც საფრთხეს უქმნის ადამიანის უფლებებსა და დემოკრატიულ ღირებულებებს.

დანაშაულის წინააღმდეგ ბრძოლა და ეროვნული უსაფრთხოების დაცვა მნიშვნელოვანი ლეგიტიმური მიზნებია, რომელთა მიღწევის ერთ-ერთი საშუალება ელექტრონულ კომუნიკაციებთან დაკავშირებული მონაცემების დამუშავებაა. ამავე დროს, სახელმწიფოს ფართო უფლებამოსილება ადამიანებს მუდმივი მეთვალყურეობის განცდას უჩენს და მსუსხავ ეფექტს წარმოშობს. სახელმწიფო ორგანოების ფართო დისკრეცია და გატარებული ღონისძიებების ფარული ხასიათი ადამიანის უფლებების დარღვევის მომეტებულ რისკს ქმნის. შესაბამისად, ადამიანის უფლებათა სამართალში ერთ-ერთი მთავარი გამოწვევაა ბალანსის დაცვა ერთი მხრივ, დანაშაულის წინააღმდეგ ბრძოლის და ეროვნული უსაფრთხოების დაცვის მიზანსა და მეორე მხრივ, ადამიანის ძირითად უფლებებს შორის.

ბოლო პერიოდში ევროკავშირის მართლმსაჯულების სასამართლომ მნიშვნელოვანი გადაწყვეტილებები მიიღო ელექტრონულ კომუნიკაციებთან დაკავშირებული მონაცემების შენახვისა და გადაცემის რეჟიმების ევროკავშირის სამართალთან შესაბამისობის თაობაზე. სხვადასხვა სამართლებრივ სიკეთეს შორის სამართლიანი ბალანსის უზრუნველყოფის პროცესში სასამართლო სათანადოდ იაზრებს როგორც თანამედროვე მსოფლიოში არსებულ საფრთხეებს, ისე ადამიანის ძირითადი უფლებების დაცვის მნიშვნელობას.

წინამდებარე სტატია განიხილავს ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავების საკითხს ევროკავშირის სამართლის მიხედვით და აანალიზებს ამ კუთხით ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკის განვითარებას.

საკვანძო სიტყვები: *ელექტრონული კომუნიკაციები, მონაცემთა შენახვა, ეროვნული უსაფრთხოება, ევროკავშირის მართლმსაჯულების სასამართლო*

1. შესავალი

პირადი ცხოვრების ხელშეუხებლობის უფლება ადამიანებს თავიანთი პიროვნების, შეხედულებებისა და ურთიერთობების თავისუფლად განვითარების შესაძლებლობას ანიჭებს. ამავე დროს, ეს უფლება სხვა ძირითადი უფლებებით სარგებლობის წინაპირობა და დემოკრატიული საზოგადოების ერთ-ერთი მნიშვნელოვანი ღირებულებაა.

ციფრულმა ტექნოლოგიამ მეთვალყურეობის უპრეცედენტო შესაძლებლობა შექმნა, რაც მნიშვნელოვან საფრთხეს უქმნის პირადი ცხოვრების ხელშეუხებლობას და პერსონალურ მონაცემთა დაცვის უფლებას. თანამედროვე მსოფლიოში გროვდება დიდი მოცულობის პერსონალური ინფორმაცია, რომელიც სულ უფრო კომპლექსური გზებით მუშავდება.

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი.

თანამედროვე ტექნოლოგიები ადამიანების ყოველდღიური ცხოვრების განუყოფელი ნაწილია. მართალია, ფიზიკური პირები ნებაყოფლობით გასცემენ პირად ინფორმაციას მომსახურებასა და ინფორმაციაზე ელექტრონული წვდომის სანაცვლოდ, მაგრამ ტექნოლოგიებზე დამოკიდებულების გათვალისწინებით, კომუნიკაციების ელექტრონული საშუალებების გამოყენებაზე უარი ფაქტობრივად სოციალური ურთიერთკავშირისგან იმ დონემდე თავშეკავებას გულისხმობს, რომ შეუძლებელია ამგვარი უარი რეალურ არჩევანად ჩაითვალოს.[1] ციფრულად ურთიერთდაკავშირებულ საზოგადოებაში ტექნოლოგიების გამოყენებაზე უარი და საზოგადოებაში სრულფასოვნად მონაწილეობა ფაქტობრივად ერთმანეთთან შეუთავსებელია.[2]

ტექნოლოგიური პროგრესის თანმდევი რისკების გათვალისწინებით, პერსონალურ მონაცემთა დაცვის აუცილებლობა მნიშვნელოვნად გაიზარდა. ევროკავშირის ძირითად უფლებათა ქარტია (შემდგომში – „ქარტია“) ერთმანეთისგან მიჯნავს ერთი მხრივ, პერსონალურ მონაცემთა დაცვის უფლებას[3] და მეორე მხრივ, პირადი და ოჯახური ცხოვრების პატივისცემის უფლებას.[4] ამასთან, ქარტიით გარანტირებული უფლებებისა და თავისუფლებების ნებისმიერი შეზღუდვა გათვალისწინებული უნდა იყოს კანონით, პატივს სცემდეს ამ უფლებების და თავისუფლებების არსს და უნდა შეესაბამებოდეს პროპორციულობის პრინციპს.[5]

დანაშაულის წინააღმდეგ ბრძოლა და ეროვნული უსაფრთხოების დაცვა მნიშვნელოვანი ლეგიტიმური მიზნებია, რომელთა მიღწევის ერთ-ერთი საშუალება ელექტრონულ კომუნიკაციებთან დაკავშირებული მონაცემების დამუშავებაა. ამავე დროს, სახელმწიფოს მხრიდან თვითნებობის და უფლებამოსილების ბოროტად გამოყენების საწინააღმდეგო მყარი გარანტიების არსებობას გადამწყვეტი მნიშვნელობა აქვს დემოკრატიული ღირებულებების დასაცავად.

ელექტრონულ კომუნიკაციებთან დაკავშირებული მონაცემების შენახვისა და მათზე სახელმწიფო ორგანოების წვდომის სამართლებრივი რეჟიმი არაერთხელ გამხდარა ფართო დისკუსიისა და მსჯელობის საგანი. ამ თვალსაზრისით განსაკუთრებით მნიშვნელოვანია ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკით დადგენილი სტანდარტი, რაც ემსახურება ბალანსის დაცვას ერთი მხრივ, დანაშაულის წინააღმდეგ ბრძოლისა და ეროვნული უსაფრთხოების დაცვის მიზანსა და მეორე მხრივ, ადამიანის ძირითად უფლებებს შორის.

წინამდებარე სტატიის მიზანია, განიხილოს ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავების საკითხი ევროკავშირის სამართლის მიხედვით და გააანალიზოს ამ კუთხით ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკის განვითარება.

2. პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ 2002/58/EC დირექტივა

ელექტრონული კომუნიკაციების სექტორში პერსონალური მონაცემების დამუშავებისა და პირადი ცხოვრების ხელშეუხებლობის დაცვის შესახებ ევროპული პარლამენტისა და საბ-

---

1 *Ronen Y.,* Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers, Utrecht Journal of International and European Law, Vol. 31, N 80, 2015, 73.

2 *Karaboga M., Matzner T., Obersteller H., Ochs C.,* Is there a Right to Offline Alternatives in a Digital World? in Data Protection and Privacy: (In)visibilities and Infrastructures, *Leenes R., Brakel R.v., Gutwirth S., Hert P.D.,* (eds), Springer International Publishing AG, 2017, 54.

3 Charter of Fundamental Rights of the European Union, 07/12/2000, მუხლი 8.

4 იქვე, მუხლი 7.

5 იქვე, მუხლი 52 (1).

ჭოს 2002/58/EC დირექტივის (შემდგომში – „2002/58 დირექტივა“ ან „პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ დირექტივა“) მიზანია ელექტრონული კომუნიკაციების სექტორში მონაცემთა დამუშავებისას ადამიანის ძირითადი უფლებების და თავისუფლებების, განსაკუთრებით კი პირადი ცხოვრების ხელშეუხებლობისა და კონფიდენციალურობის დაცვის უზრუნველყოფა, ასევე ამგვარი მონაცემების და ელექტრონული კომუნიკაციის მოწყობილობისა და მომსახურების თავისუფალი მიმოცვლის უზრუნველყოფა ევროკავშირში.[6]

2002/58 დირექტივა ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ შემდეგი სამი კატეგორიის მონაცემების დამუშავებას არეგულირებს: ტრაფიკის მონაცემები,[7] ადგილმდებარეობის მონაცემები[8] და კომუნიკაციის შინაარსი. დირექტივა ითვალისწინებს როგორც ელექტრონული კომუნიკაციის შინაარსის, ისე მასთან დაკავშირებული ტრაფიკის მონაცემების კონფიდენციალურობის პრინციპს.[9] ამ დირექტივის მიღებით, ევროკავშირის კანონმდებელმა პირადი და ოჯახური ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის მნიშვნელოვანი გარანტიები შექმნა.

დირექტივის მე-15 მუხლი წევრ სახელმწიფოებს გამონაკლისის დადგენის უფლებამოსილებას ანიჭებს, როდესაც ეს აუცილებელი, შესაბამისი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში ეროვნული უსაფრთხოების, თავდაცვის და საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, ასევე დანაშაულის თავიდან აცილების, გამოძიების, გამოვლენის და სისხლისსამართლებრივი დევნის მიზნით.[10] ამ მიზნების მისაღწევად წევრ სახელმწიფოებს შეუძლიათ, მიიღონ კანონმდებლობა მონაცემების შეზღუდული ვადით შენახვის თაობაზე.[11] ამავე დროს, დირექტივით გათვალისწინებული უფლებებიდან და ვალდებულებებიდან გადახვევის შესაძლებლობა არ გულისხმობს იმას, რომ გამონაკლისი შესაძლოა წესად იქცეს.[12]

მნიშვნელოვანია აღინიშნოს, რომ 2002/58 დირექტივა არ ვრცელდება საზოგადოებრივი უსაფრთხოების, თავდაცვის, სახელმწიფო უსაფრთხოებისა და სისხლის სამართლის სფე-

---

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), მუხლი 1 (1).
უნდა აღინიშნოს ისიც, რომ განხილვის პროცესშია ელექტრონული კომუნიკაციების სექტორში პირადი ცხოვრების პატივისცემის და პერსონალური მონაცემების დაცვის შესახებ ევროპარლამენტისა და საბჭოს რეგულაცია, რომელმაც 2002/58 დირექტივა უნდა ჩაანაცვლოს. დღეის მდგომარეობით, ეს რეგულაცია მიღებული არ არის. დამატებითი ინფორმაცია ხელმისაწვდომია: <https://eur-lex.europa.eu/procedure/EN/2017_3> [10.08.2024].

[7] „ტრაფიკის მონაცემები“ გულისხმობს ნებისმიერ მონაცემს, რომელიც მუშავდება ელექტრონული საკომუნიკაციო ქსელით კომუნიკაციის გადაცემის ან გადასახადის დარიცხვის მიზნით. 2002/58 დირექტივის მე-2 მუხლის „ბ“ ქვეპუნქტი.

[8] „ადგილმდებარეობის მონაცემები“ ნიშნავს ნებისმიერ მონაცემს, რომელიც მუშავდება ელექტრონულ საკომუნიკაციო ქსელში ან ელექტრონული საკომუნიკაციო მომსახურების მიერ და მიუთითებს საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მომხმარებლის საბოლოო მოწყობილობის გეოგრაფიულ ადგილმდებარეობას. 2002/58 დირექტივის მე-2 მუხლის „გ“ ქვეპუნქტი.

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), მუხლი 5.

[10] იქვე, მუხლი 15 (1).

[11] იქვე.

[12] C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU, § 59.

როში სახელმწიფოს საქმიანობაზე.[13] ამასთან, ევროკავშირის შესახებ ხელშეკრულების თანახმად, ეროვნული უსაფრთხოების საკითხი თითოეული წევრი სახელმწიფოს პასუხისმგებლობაა.[14] მიუხედავად ამისა, ევროკავშირის მართლმსაჯულების სასამართლოს განმარტებით, ეროვნული კანონმდებლობა, რომელიც სახელმწიფო ორგანოს ანიჭებს უფლებამოსილებას, ეროვნული უსაფრთხოების დაცვის მიზნით ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს მოსთხოვოს ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვა და უსაფრთხოებისა და დაზვერვის სამსახურებისთვის გადაცემა, 2002/58 დირექტივის ფარგლებში ექცევა.[15]

3. მონაცემთა შენახვის შესახებ 2006/24/EC დირექტივის გაუქმება

ევროპული პარლამენტისა და საბჭოს 2006 წლის 15 მარტის 2006/24/EC დირექტივა (შემდგომში – „მონაცემთა შენახვის შესახებ დირექტივა“ ან „2006/24 დირექტივა“) საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებსა და საჯარო საკომუნიკაციო ქსელების ოპერატორებს ავალდებულებდა, შეენახათ მონაცემები და უზრუნველეყოთ უფლებამოსილი ორგანოებისთვის ამ მონაცემების ხელმისაწვდომობა მძიმე დანაშაულის გამოძიების, გამოვლენის და სისხლისსამართლებრივი დევნის მიზნით. დირექტივა განზოგადებულად ფარავდა ყველა პირს და ელექტრონული კომუნიკაციის საშუალებას, ასევე ტრაფიკის მონაცემებს ყოველგვარი დიფერენციაციის, შეზღუდვის ან გამონაკლისის გარეშე.[16] მიუხედავად იმისა, რომ დირექტივა არ უშვებდა კომუნიკაციის შინაარსის შენახვის შესაძლებლობას, მთლიანობაში, შენახული მონაცემების მეშვეობით შეიძლებოდა ზუსტი დასკვნების გამოტანა ადამიანების პირად ცხოვრებასთან დაკავშირებით, მათ შორის, ყოველდღიური ჩვევების, მუდმივი ან დროებითი საცხოვრებლის, ყოველდღიური ან სხვა გადაადგილების, სოციალური კავშირებისა და იმ გარემოს შესახებ, სადაც ხშირად იმყოფებიან.[17]

2014 წელს ევროკავშირის მართლმსაჯულების სასამართლოს დიდმა პალატამ მონაცემთა შენახვის შესახებ დირექტივა გააუქმა. სასამართლოს თანახმად, მძიმე დანაშაულის, განსაკუთრებით, ორგანიზებული დანაშაულისა და ტერორიზმის წინააღმდეგ ბრძოლას საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად უდიდესი მნიშვნელობა აქვს და მისი ეფექტურობა შეიძლება დიდწილად დამოკიდებული იყოს თანამედროვე საგამოძიებო მეთოდებზე.[18] თუმცა, ამგვარი მიზნის არსებობა თავისთავად არ ამართლებს 2006/24 დირექტივით გათვალისწინებულ შენახვის წესს.[19]

---

13 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), მუხლი 1 (3).

14 Treaty on European Union, 07/02/1992, მუხლი 4 (2).

15 Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU, § 104. C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU, § 49.

16 C-293/12, C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, [2014], CJEU, §§ 57-59.

17 იქვე, § 27.

18 იქვე, § 51.

19 იქვე.

მონაცემთა შენახვის შესახებ დირექტივა ვრცელდებოდა ყველა იმ ადამიანზე, ვინც ელექტრონული საკომუნიკაციო მომსახურებით სარგებლობდა. ის ეხებოდა იმ პირებსაც, ვისთან მიმართებითაც არ არსებობდა მტკიცებულება, რაც მძიმე დანაშაულთან მათ თუნდაც არაპირდაპირ ან დისტანციურ კავშირზე მიუთითებდა.[20] გარდა ამისა, ის არ ითვალისწინებდა ობიექტურ კრიტერიუმს, რომლის მიხედვითაც შენახულ ინფორმაციაზე წვდომის და მათი გამოყენების უფლებამოსილების მქონე პირების რაოდენობა მკაცრი აუცილებლობით იქნებოდა შემოსაზღვრული.[21] შენახულ მონაცემებზე უფლებამოსილი ორგანოების წვდომა არ იყო დამოკიდებული სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს წინასწარ განხილვაზე.[22] 2006/24 დირექტივა ადგენდა მინიმუმ 6 და მაქსიმუმ 24 თვიან შენახვის ვადას, თუმცა არაფერს ამბობდა იმის თაობაზე, რომ შენახვის ვადის განსაზღვრა ობიექტურ კრიტერიუმებს უნდა ეფუძნებოდეს.[23] საბოლოო ჯამში, ევროკავშირის მართლმსაჯულების სასამართლოს თანახმად, მონაცემთა შენახვის შესახებ დირექტივა პროპორციულობის პრინციპთან შეუსაბამო იყო.

4. ელექტრონულ კომუნიკაციებთან დაკავშირებული მონაცემების შენახვისა და გადაცემის წესი ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკის მიხედვით

2006/24 დირექტივის გაუქმების შემდეგ, ეროვნულ დონეზე მონაცემთა შენახვის რეჟიმების იურიდიული ძალა ეჭვქვეშ დადგა. შედეგად, ევროკავშირის მართლმსაჯულების სასამართლოს წინასწარი გადაწყვეტილების მისაღებად ორი მიმართვა წარედგინა, რომლის ფარგლებში შვედეთისა და გაერთიანებული სამეფოს კანონმდებლობის 2002/58 დირექტივასა და ქარტიასთან შესაბამისობა შეფასდა. 2016 წელს მიღებულ გადაწყვეტილებაში სასამართლომ აღნიშნა, რომ ეროვნული კანონმდებლობა, რომელიც ხელისუფლებას ანიჭებს უფლებამოსილებას, დანაშაულთან ბრძოლის მიზნით საკომუნიკაციო მომსახურების მიმწოდებლებს მოსთხოვოს ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტური და განურჩეველი შენახვა, ქარტიის მოთხოვნების გათვალისწინებით, 2002/58 დირექტივას არ შეესაბამება.[24]

ამავე დროს, ევროკავშირის მართლმსაჯულების სასამართლოს თანახმად, წევრ სახელმწიფოებს შეუძლიათ, კანონმდებლობით დაარეგულირონ მძიმე დანაშაულის წინააღმდეგ ბრძოლის მიზნით მონაცემების მიზნობრივი შენახვა, თუკი გათვალისწინებული იქნება სათანადო გარანტიები პერსონალური მონაცემების ბოროტად გამოყენების რისკის თავიდან ასაცილებლად.[25] გადაუდებელი აუცილებლობის შემთხვევების გარდა, შენახულ მონაცემებზე უფლებამოსილი სახელმწიფო ორგანოების წვდომა უნდა დაექვემდებაროს სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს წინასწარ განხილვას[26] და კანონიერად შეგროვებული მონაცემები შენახულ უნდა იქნეს ევროკავშირის ფარგლებში.[27]

---

[20] იქვე, § 58.
[21] იქვე, § 62.
[22] იქვე.
[23] იქვე, § 64.
[24] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, [2016], CJEU.
[25] იქვე, §§ 108-109.
[26] იქვე, § 120.
[27] იქვე, § 122.

მონაცემთა შენახვისა და გადაცემის რეჟიმთან დაკავშირებით სამართლებრივი მსჯელობა 2016 წლის გადაწყვეტილების შემდეგაც გაგრძელდა. ამ კუთხით მნიშვნელოვანია ევროკავშირის მართლმსაჯულების სასამართლოს 2020 წლის 6 ოქტომბრის გადაწყვეტილება, რომელიც ეროვნული უსაფრთხოების დაცვის მიზნით მონაცემთა დამუშავებას შეეხება. სასამართლომ იმსჯელა გაერთიანებული სამეფოს კანონმდებლობაზე, რომელიც სახელმწიფო მდივანს ანიჭებდა უფლებამოსილებას, ეროვნული უსაფრთხოების ინტერესებიდან გამომდინარე, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისთვის მოეთხოვა ტრაფიკისა და ადგილმდებარეობის მონაცემების უსაფრთხოებისა და დაზვერვის სამსახურებისთვის გადაცემა. ევროკავშირის მართლმსაჯულების სასამართლოს შეფასებით, ამგვარი რეგულირება კონფიდენციალურობის პრინციპიდან გამონაკლისს წესად აქცევს[28] და ადამიანებს მუდმივი მეთვალყურეობის განცდას უჩენს.[29] უსაფრთხოებისა და დაზვერვის სამსახურებისთვის მონაცემების გადაცემა სასამართლომ პირადი ცხოვრების ხელშეუხებლობის უფლებაში განსაკუთრებით სერიოზულ ჩარევად მიიჩნია.[30]

ტრაფიკისა და ადგილმდებარეობის მონაცემების გადაცემის რეჟიმი ელექტრონული საკომუნიკაციო მომსახურების ყველა მომხმარებელზე ახდენდა გავლენას, მიუხედავად იმისა, ჰქონდათ თუ არა მათ საფრთხესთან თუნდაც არაპირდაპირი კავშირი.[31] სასამართლოს განმარტებით, ევროკავშირის სამართალი კრძალავს იმგვარ ეროვნულ კანონმდებლობას, რომელიც სახელმწიფო ორგანოს ანიჭებს უფლებამოსილებას, ეროვნული უსაფრთხოების დაცვის მიზნით, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს მოსთხოვოს ტრაფიკისა და ადგილმდებარეობის მონაცემების უსაფრთხოებისა და დაზვერვის სამსახურებისთვის ბლანკეტური გადაცემა.[32]

2020 წლის 6 ოქტომბერს ევროკავშირის მართლმსაჯულების სასამართლომ მეორე მნიშვნელოვანი გადაწყვეტილებაც მიიღო, რომლითაც ელექტრონული კომუნიკაციების სექტორში ტრაფიკისა და ადგილმდებარეობის მონაცემების, ასევე ინტერნეტ პროტოკოლის მისამართებისა და ვინაობასთან დაკავშირებული მონაცემების შენახვის წესები განსაზღვრა.[33] ამ საქმეში სასამართლომ ქარტიის შუქზე, საფრანგეთისა და ბელგიის კანონმდებლობის 2002/58 დირექტივის მე-15 (1) მუხლთან შესაბამისობა შეაფასა. მიღებული გადაწყვეტილებით დადგენილი სტანდარტები შეიძლება შემდეგნაირად შეჯამდეს:

1) ევროკავშირის სამართალი არ გამორიცხავს ეროვნული უსაფრთხოების დაცვის მიზნით ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტურ შენახვას შემდეგი დათქმებით: ა) ეს ღონისძიება გამოყენებულ უნდა იქნეს იმ შემთხვევაში, როდესაც სახელმწიფოს ეროვნული უსაფრთხოება რეალური და მიმდინარე ან განჭვრეტადი მნიშვნელოვანი საფრთხის წინაშეა;[34] ბ) ყველა მომხმარებლის მონაცემების პრევენციული შენახვის შესა-

[28] C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU, § 69.
[29] იქვე, § 71
[30] იქვე.
[31] იქვე, § 80.
[32] იქვე, § 82.
[33] Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU.
[34] იქვე, § 137.

ხებ ამგვარი მითითება მკაცრი აუცილებლობით დროში შეზღუდული უნდა იყოს და პერსონალური მონაცემების ბოროტად გამოყენებისგან ეფექტურად დასაცავად მყარ გარანტიებს უნდა დაექვემდებაროს. შესაბამისად, მონაცემთა შენახვას სისტემატური ხასიათი არ უნდა ჰქონდეს.[35] მითითება მონაცემების შენახვის შესახებ შესაძლოა განახლდეს, თუკი საფრთხე განაგრძობს არსებობას.[36] გ) მონაცემების შენახვის შესახებ ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისადმი გაცემული მითითება სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ ეფექტურ განხილვას უნდა დაექვემდებაროს, რომლის გადაწყვეტილება სავალდებულოა.[37] ამგვარი განხილვის მიზანი მნიშვნელოვანი საფრთხის არსებობის და სათანადო გარანტიების უზრუნველყოფის დადასტურებაა.[38]

2) ევროკავშირის სამართალი გამორიცხავს დანაშაულთან ბრძოლის და საზოგადოებრივი უსაფრთხოების უზრუნველყოფის მიზნით ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტურ შენახვას.[39]

3) ევროკავშირის სამართალი არ გამორიცხავს მძიმე დანაშაულთან ბრძოლის, საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული მნიშვნელოვანი საფრთხეების თავიდან აცილების და ეროვნული უსაფრთხოების დაცვის მიზნით ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ ტრაფიკისა და ადგილმდებარეობის მონაცემების მიზნობრივ შენახვას, თუკი მონაცემების კატეგორიების, კომუნიკაციის საშუალებების, სამიზნე ჯგუფის და შენახვის პერიოდის თვალსაზრისით ამგვარი შენახვა მკაცრი აუცილებლობით არის შეზღუდული.[40]

4) ევროკავშირის სამართალი არ გამორიცხავს მძიმე დანაშაულთან ბრძოლის, საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული მნიშვნელოვანი საფრთხეების თავიდან აცილების და ეროვნული უსაფრთხოების დაცვის მიზნით ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ ინტერნეტ პროტოკოლის მისამართების შეზღუდული ვადით ბლანკეტურ შენახვას, თუკი ამგვარი შენახვა ამ მონაცემთა გამოყენების მარეგულირებელ სათანადო მატერიალურ და პროცედურულ დათქმებს დაექვემდებარება.[41]

5) ევროკავშირის სამართალი არ გამორიცხავს ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ ელექტრონული საკომუნიკაციო სისტემების ყველა მომხმარებლის ვინაობასთან დაკავშირებული მონაცემების შენახვას დანაშაულის პრევენციის, გამოძიების, გამოვლენისა და სისხლისსამართლებრივი დევნის დაწყების, ასევე ეროვნული და საზოგადოებრივი უსაფრთხოების დაცვის მიზნით.[42]

6) ევროკავშირის სამართალი არ გამორიცხავს მძიმე დანაშაულთან ბრძოლის და ეროვნული უსაფრთხოების დაცვის მიზნით ელექტრონული საკომუნიკაციო მომსახურების

[35] იქვე, § 138.
[36] იქვე, § 138.
[37] იქვე, § 139.
[38] იქვე.
[39] იქვე, §§ 141-143.
[40] იქვე, §§ 146-147.
[41] იქვე, §§ 155-156.
[42] იქვე, § 159.

მიმწოდებლების მიერ ტრაფიკისა და ადგილმდებარეობის მონაცემების შეზღუდული ვადით გადაუდებელი წესით შენახვას.[43] უფლებამოსილი სახელმწიფო ორგანოს ამგვარი გადაწყვეტილება ეფექტურ სასამართლო კონტროლს უნდა დაექვემდებაროს.[44]

7) ევროკავშირის სამართალი უშვებს ეროვნული უსაფრთხოების დაცვის მიზნით ელექტრონული საკომუნიკაციო სისტემების ყველა მომხმარებლის ტრაფიკისა და ადგილმდებარეობის მონაცემების შეზღუდული ვადით ავტომატურ ანალიზს.[45] ამ შემთხვევაზე ვრცელდება ეროვნული უსაფრთხოების დაცვის მიზნით მონაცემთა ბლანკეტურ შენახვასთან დაკავშირებული პირობები.[46]

8) ევროკავშირის სამართალი უშვებს ეროვნული უსაფრთხოების დაცვის მიზნით ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების დავალდებულებას, რეალურ დროში მიზნობრივად შეაგროვონ ტრაფიკისა და ადგილმდებარეობის მონაცემები.[47] მონაცემების რეალურ დროში შეგროვების შესახებ გადაწყვეტილება ეროვნული კანონმდებლობით გათვალისწინებულ ობიექტურ და არადისკრიმინაციულ კრიტერიუმებს უნდა დაეფუძნოს, უნდა დაექვემდებაროს სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ წინასწარ განხილვას, ხოლო გადაუდებელი აუცილებლობისას მისი კანონიერება უნდა შემოწმდეს უმოკლეს ვადაში.[48]

ევროკავშირის მართლმსაჯულების სასამართლოს ეს გადაწყვეტილებები მნიშვნელოვანი გზამკვლევია ერთი მხრივ, პირადი ცხოვრების ხელშეუხებლობის და პერსონალურ მონაცემთა დაცვის უფლებას და მეორე მხრივ, ეროვნული უსაფრთხოების ინტერესს შორის ბალანსის დაცვის თვალსაზრისით. სასამართლოს მსჯელობა ეფუძნება თანამედროვე მსოფლიოში არსებული საფრთხეების მხედველობაში მიღებას და ადამიანის ძირითად უფლებათა დაცვის მნიშვნელობის სათანადო გააზრებას. ამასთან, მიზანშეწონილია 2020 წელს მიღებული გადაწყვეტილებების განხილვა წინამორბედი გადაწყვეტილებებით დადგენილ სტანდარტებთან მიმართებით.

2014 და 2016 წელს მიღებული გადაწყვეტილებებისგან განსხვავებით, რომლებიც დანაშაულის წინააღმდეგ ბრძოლის მიზნით მონაცემთა შენახვის შედარებით მარტივ რეჟიმს შეეხებოდა,[49] 2020 წლის გადაწყვეტილებაში პერსონალურ მონაცემთა დაცვის საპირწონედ განხილულ იქნა ეროვნული უსაფრთხოების დაცვის ინტერესი.[50] გარდა ამისა, სასამართლომ იმსჯელა მონაცემთა უფრო ფართო კატეგორიაზე: ტრაფიკისა და ადგილმდებარეობის მონაცემებთან ერთად განხილვის საგანი გახდა ინტერნეტ პროტოკოლის მისამართები და პირის ვინაობასთან დაკავშირებული მონაცემებიც. მონაცემთა კატეგორიები, მათი დამუშავების ოპერაციები და მიზნები 2020 წლის გადაწყვეტილებას უფრო კომპლექსურს ხდის წინამორბედ გადაწყვეტილებებთან შედარებით.[51]

---

[43] იქვე, §§ 163-164.
[44] იქვე, § 163.
[45] იქვე, § 178.
[46] იქვე, §§ 176-179.
[47] იქვე, § 188.
[48] იქვე, § 189.
[49] *Eskens S.,* The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-depth Review of La Quadrature du Net and Others and Privacy International, Vol. 8, Issue 1, 2022, 143.
[50] Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU.
[51] *Eskens S.,* The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-depth Review of La Quadrature du Net and Others and Privacy International, Vol. 8, Issue 1, 2022, 143.

თუკი 2014 წელს მიღებული გადაწყვეტილებით ევროკავშირის მართლმსაჯულების სასამართლომ მონაცემთა შენახვის დირექტივა გააუქმა, ხოლო 2016 წელს დანაშაულის წინააღმდეგ ბრძოლის მიზნით მონაცემთა ბლანკეტური და განურჩეველი შენახვა აკრძალა, 2020 წელს მიღებულ გადაწყვეტილებაში სასამართლომ განიხილა ის გამონაკლისი შემთხვევები, როდესაც ევროკავშირის სამართალი მონაცემთა ბლანკეტურ შენახვას უშვებს. ამავე დროს, სასამართლომ ამგვარი ზომების მისაღებად მკაცრი პირობები განსაზღვრა.[52]

უნდა აღინიშნოს ისიც, რომ 2020 წლის გადაწყვეტილებაში ევროკავშირის მართლმსაჯულების სასამართლო უმეტესად ყურადღებას ამახვილებს სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მხრიდან კონტროლის განხორციელების მნიშვნელობაზე, თუმცა ამგვარი კონტროლი ნახსენები არ არის მონაცემთა მიზნობრივ შენახვასთან, ასევე ინტერნეტ პროტოკოლის მისამართებისა და ვინაობასთან დაკავშირებული მონაცემების შენახვასთან მიმართებით.[53] შესაძლოა, ეს განპირობებულია იმით, რომ ევროკავშირის მართლმსაჯულების სასამართლომ მონაცემთა შენახვის ეს ფორმები ძირითად უფლებებში შედარებით მსუბუქ ჩარევად მიიჩნია, თუმცა გამოთქმულია მოსაზრება, რომ ამან მომავალში შეიძლება დამატებითი კითხვები წარმოშვას.[54]

ზემოთ განხილული გადაწყვეტილებები ხაზს უსვამს ტრაფიკისა და ადგილმდებარეობის მონაცემების დაცვის მნიშვნელობას. ევროკავშირის მართლმსაჯულების სასამართლოს შეფასებით, ამგვარი მონაცემები შესაძლოა პირის პირადი ცხოვრების შესახებ დიდი ოდენობით ინფორმაციას ამჟღავნებდეს, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს.[55] ეს მონაცემები ადამიანების ცხოვრების შესახებ ზუსტი დასკვნების გამოტანისა და პირთა პროფილების შექმნის შესაძლებლობას იძლევა, რაც პირადი ცხოვრების ხელშეუხებლობის თვალსაზრისით, კომუნიკაციების შინაარსზე ნაკლებად სენსიტიური არ არის.[56] სასამართლოს ამგვარი მსჯელობა ციფრულ ეპოქაში არსებული მნიშვნელოვანი გამოწვევების სათანადო გააზრებას ეფუძნება. თანამედროვე ტექნოლოგიების მზარდი შესაძლებლობების გათვალისწინებით, ადვილია მონაცემთა ურთიერთდაკავშირება და სრულიად ახალი ინფორმაციის მოპოვება.[57] შესაბამისად, ნებისმიერი სახის პერსონალური მონაცემის დაცვა განსაკუთრებულ მნიშვნელობას იძენს.

აღსანიშნავია ისიც, რომ კომუნიკაციებთან დაკავშირებული მონაცემების შენახვა გავლენას ახდენს არა მხოლოდ პირადი ცხოვრების ხელშეუხებლობასა და პერსონალურ მონაცემთა დაცვის უფლებაზე, არამედ ქარტიის მე-11 მუხლით გათვალისწინებულ გამოხატვის თავისუფლებაზეც. ამგვარი მონაცემების მასობრივ შეგროვებას შესაძლოა მსუსხავი ეფექტი

---

52 იქვე.

53 იქვე, 154.

54 იქვე.

55 Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU, § 117.

56 იქვე.
Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, [2016], CJEU, § 99.
C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU, § 71.

57 *Karaboga M., Matzner T., Obersteller H., Ochs C.,* Is there a Right to Offline Alternatives in a Digital World? in Data Protection and Privacy: (In)visibilities and Infrastructures, *Leenes R., Brakel R.v., Gutwirth S., Hert P.D.,* (eds), Springer International Publishing AG, 2017, 45.

ჰქონდეს, რადგან განცდა იმისა, რომ მეთვალყურეობა ხორციელდება, ადამიანებს საკუთარი გამოხატვის თავისუფლების შეზღუდვისკენ უბიძგებს.[58] სასამართლოც პირდაპირ აღნიშნავს, რომ ტრაფიკის და ადგილმდებარეობის მონაცემების შენახვამ შესაძლებელია უარყოფითი გავლენა მოახდინოს მომხმარებელთა მიერ ელექტრონული საკომუნიკაციო საშუალებების გამოყენებაზე და შედეგად, მათ გამოხატვის თავისუფლებაზე, რადგან ამგვარმა ღონისძიებამ შესაძლოა ადამიანებს აფიქრებინოს, რომ მათ პირად ცხოვრებაზე მუდმივი მეთვალყურეობა ხორციელდება.[59]

ევროკავშირის მართლმსაჯულების სასამართლო შემწყნარებლურ დამოკიდებულებას ამჟღავნებს მონაცემების ბლანკეტური შენახვის მიმართ, როდესაც საქმე ეროვნული უსაფრთხოების დაცვას ეხება, განსხვავებით მძიმე დანაშაულთან ბრძოლის და საზოგადოებრივი უსაფრთხოების დაცვის შემთხვევებისა. ეროვნული უსაფრთხოების დაცვის გაძლიერებული რეჟიმის უზრუნველსაყოფად სახელმწიფოები მოწინავე ტექნოლოგიებს იყენებენ და მნიშვნელოვან ღონისძიებებს ახორციელებენ და სასამართლოც გარკვეულწილად ამ მიდგომას იზიარებს. ზემოთ განხილული გადაწყვეტილებები ცხადყოფს, რომ სხვადასხვა სამართლებრივ სიკეთეს შორის სამართლიანი ბალანსის უზრუნველყოფის პროცესში სასამართლო პრაგმატულ მიდგომას ამჟღავნებს.

ამავე დროს, ევროკავშირის მართლმსაჯულების სასამართლოს მსჯელობა კრიტიკის საგანიც გახდა განსხვავებული მიზეზებით. რამდენიმე სახელმწიფომ მონაცემთა შენახვასთან დაკავშირებული პროპორციულობის ტესტი ზედმეტად მკაცრად მიიჩნია, ხოლო შემოთავაზებული გადაწყვეტა, მაგალითად, მონაცემთა მიზნობრივი შენახვა, უსარგებლოდ ან არაპრაქტიკულად.[60] მეორე მხრივ, ადამიანის უფლებათა დამცველები, რომლებიც მხარს უჭერენ მასობრივი მეთვალყურეობის ინსტრუმენტების სრულ აკრძალვას, ევროკავშირის მართლმსაჯულების სასამართლოს ბოლო დროინდელ გადაწყვეტილებებს ეროვნული უსაფრთხოების დასაცავად შეუზღუდავი მეთვალყურეობის მეთოდების დაკანონების ფორმად მიიჩნევენ.[61]

5. დასკვნა

თანამედროვე მსოფლიოში არსებული საფრთხეების გათვალისწინებით, მძიმე დანაშაულების თავიდან ასაცილებლად და ეროვნული უსაფრთხოების დასაცავად სახელმწიფოები ელექტრონულ კომუნიკაციებთან დაკავშირებულ მონაცემებს ამუშავებენ, რაც პირადი ცხოვრების ხელშეუხებლობის და პერსონალურ მონაცემთა დაცვის უფლების ხელყოფის რისკს წარმოშობს. შესაბამისად, ადამიანის უფლებათა სამართალში ერთ-ერთი მთავარი გამოწვევაა სამართლიანი ბალანსის უზრუნველყოფა ერთი მხრივ, დანაშაულის წინააღმდეგ ბრძოლის და ეროვნული უსაფრთხოების დაცვის მიზანსა და მეორე მხრივ, ადამიანის ძირითად უფლებებს შორის.

---

58 *Buono I., & Taylor A.,* Mass Surveillance in the CJEU: Forging European Consensus, Cambridge Law Journal, Vol. 76, No. 2, 2017, 251.

59 Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, [2016], CJEU, §§ 100-101.

60 *Celeste E., Formici G.,* Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia, German Law Journal, 2024, 18.

61 იქვე.

ევროკავშირის შესახებ ხელშეკრულების თანახმად, ეროვნული უსაფრთხოების საკითხი თითოეული წევრი სახელმწიფოს პასუხისმგებლობაა.[62] მიუხედავად ამისა, ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილებები ცხადყოფს, რომ ეროვნული კანონმდებლობა, რომელიც ეროვნული უსაფრთხოების დაცვის მიზნით ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს მონაცემების შენახვას და გადაცემას ავალდებულებს, 2002/58 დირექტივის ფარგლებში ექცევა.

მნიშვნელოვანია, რომ ევროკავშირის სამართალი გამორიცხავს ეროვნული უსაფრთხოების დაცვის მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტურ გადაცემას უსაფრთხოებისა და დაზვერვის სამსახურებისთვის, რადგან ამგვარი პრაქტიკა ადამიანებს მუდმივი მეთვალყურეობის განცდას უჩენს და კონფიდენციალურობის პრინციპიდან გამონაკლისს წესად აქცევს.

ევროკავშირის მართლმსაჯულების სასამართლომ მკაფიოდ განსაზღვრა ელექტრონულ კომუნიკაციებთან დაკავშირებული მონაცემების შენახვის წესიც. მონაცემთა მიზნობრივი შენახვისგან განსხვავებით, ბლანკეტური შენახვა თითოეულ ადამიანს ეხება, მიუხედავად იმისა, აქვს თუ არა მას კავშირი კონკრეტულ საფრთხესთან ან დანაშაულთან. სასამართლომ დაადგინა, რომ მონაცემთა მასობრივ შენახვას მძიმე დანაშაულის წინააღმდეგ ბრძოლის ინტერესი ვერ ამართლებს, თუმცა ამ ღონისძიების გამოყენება დასაშვებია ეროვნული უსაფრთხოების დასაცავად. ამავე დროს, ამ შემთხვევაშიც კი მონაცემთა შენახვას სისტემატური ხასიათი არ უნდა ჰქონდეს და ეს ღონისძიება გამოყენებულ უნდა იქნეს მხოლოდ იმ შემთხვევაში, როდესაც სახელმწიფოს ეროვნული უსაფრთხოება რეალური და მიმდინარე ან განჭვრეტადი მნიშვნელოვანი საფრთხის წინაშეა. გარდა ამისა, ადამიანის უფლებების დაცვის ერთ-ერთი მნიშვნელოვანი გარანტია სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მხრიდან კონტროლის განხორციელებაა. შესაბამისად, ბლანკეტური შენახვის რეჟიმის სრულად აკრძალვის ნაცვლად, მოსამართლეებმა მკაფიო საზღვრების და მკაცრი პროპორციულობის ტესტის დადგენის გზა აირჩიეს.

საბოლოო ჯამში, ევროკავშირის სამართალი და სასამართლო პრაქტიკა ეფუძნება როგორც თანამედროვე მსოფლიოში არსებული საფრთხეების, ისე ადამიანის უფლებების დაცვის მნიშვნელობის სათანადო გააზრებას. ამავე დროს, ეროვნულ დონეზე უფლებამოსილების ბოროტად გამოყენების საწინააღმდეგო გარანტიების არსებობას და მათ ეფექტურობას გადამწყვეტი მნიშვნელობა აქვს დემოკრატიული ღირებულებების დასაცავად.

ბიბლიოგრაფია:

1. Charter of Fundamental Rights of the European Union, 2000.
2. Treaty on European Union, 1992.
3. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
4. *Buono I., Taylor A.,* Mass Surveillance in the CJEU: Forging European Consensus, Cambridge Law Journal, Vol. 76, No. 2, 2017, 251-253.
5. *Celeste E., Formici G.,* Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia, German Law Journal, 2024, 13, 18.

[62] Treaty on European Union, 07/02/1992, მუხლი 4 (2).

6. *Eskens S.,* The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-depth Review of La Quadrature du Net and Others and Privacy International, European Data Protection Law Review (EDPL), Vol. 8, No. 1, 143.
7. *Karaboga M., Matzner T., Obersteller H., Ochs C.,* Is there a Right to Offline Alternatives in a Digital World? in Data Protection and Privacy: (In)visibilities and Infrastructures, *Leenes R., Brakel R.v., Gutwirth S., Hert P.D.,* (eds), Springer International Publishing AG, 2017, 45, 54.
8. *Ronen Y.,* Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers, Utrecht Journal of International and European Law, Vol. 31, N 80, 2015, 73.
9. Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU.
10. C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU.
11. Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, [2016], CJEU.
12. C-293/12, C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, [2014], CJEU.