საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის რეფორმირებისთვის – შედარებითი და ევროპულ სამართლებრივი მოსაზრებები (ნაწილი 2*)**

გერმანიის უზენაესი ფედერალური სასამართლოს მოსამართლე, იენის ფრიდრიხ შილერის უნივერსიტეტის ლექტორი დოქ. ***ვოლფგანგ ბერი*** / იენის ფრიდრიხ შილერის უნივერსიტეტის პროფესორი დოქ. ***ედვარდ შრამი***

IV. ინფრასტრუქტურული სუბიექტების მონაცემებზე წვდომის შეფასება ევროპული სამართლის ჭრილში

1. პრობლემის არსი

საკითხის განხილვისას, უპირველეს ყოვლისა, შესაფასებელია, არის თუ არა ევროპული კანონმდებლობით გამართლებული დაცვის მხარისთვის კრიტიკული ინფრასტრუქტურის სუბიექტებთან არსებული ვიდეო ჩანაწერებზე ან სხვა კომპიუტერულ მონაცემებზე წვდომის პირდაპირი აკრძალვა. ამ შემთხვევაში ალტერნატივა შეიძლება იყოს ისეთი რეგულაციის შექმნა, რომელიც დაცვის მხარეს მისცემდა მონაცემების გამოთხოვის უფლებას, თუმცა აღნიშნული უფლებამოსილების განხორციელებაზე (დაცვის მხარის შუამდგომლობის საფუძველზე) კონტროლი ექნებოდა სასამართლოს. ამის შემდეგ სასამართლომ შეიძლება ყოველ კონკრეტულ შემთხვევაში გადაწყვიტოს, თუ რამდენად მიზანშეწონილი იქნება ამ კრიტიკული ინფრასტრუქტურის სუბიექტებიდან ვიდეოჩანაწერების ან სხვა კომპიუტერული მონაცემების გადაცემა დაცვის მხარისთვის.

„კრიტიკული ინფრასტრუქტურის სუბიექტები“, საქართველოს კანონის პროექტის თანახმად, შედგება ობიექტების ორი ჯგუფისაგან. პირველი ჯგუფი მოიცავს სათვალთვალო შენობას ე. ი., უპირველეს ყოვლისა, საჯარო დაწესებულებას, რომელიც შექმნილია სისხლისსამართლებრივი დევნისა ან სხვა სპეციალური მიზნებისთვის, შენიღბული ობიექტების ჩათვლით (მაგალითად, შენიღბულ საცხოვრებელ შენობას) და ასევე ისეთ შენობებს, რომლებიც გამოიყენება ამ ორგანოების ოპერატიულ-ტექნიკური აპარატურისა და აღჭურვილობის შესანახად. ეს ობიექტები წარმოადგენენ სახელმწიფო საიდუმლოებას, შესაბამისად, მათ შესახებ ინფორმაციას დიდი მნიშვნელობა აქვს საჯარო წესრიგისთვის.

მეორე ჯგუფი მოიცავს აეროპორტებსა და ნებისმიერ ობიექტს, რომელიც დაკავშირებულია ნავთობისა და გაზის, ელექტროენერგიის ან ქიმიური, ბიოლოგიური, რადიოაქტიური და ბირთვული პროდუქტების შეძენასთან. მათ შეუზღუდავ ფუნქციონირებას განსაკუთრებული მნიშვნელობა აქვს სახელმწიფოებრივი ან საზოგადოებრივი წესრიგისთვის ან მთავრობის შეუზღუდავი ფუნქციონირებისთვის, ან, ზოგადად, საზოგადოებისთვის.

საკანონმდებლო ინიციატივა არ აძლევს დაცვის მხარეს უფლებას, გამოითხოვოს ინფორმაცია ამ ობიექტებზე დამონტაჟებული სათვალთვალო კამერებიდან. ამასთან, არ აქვს მნიშვნელობა, ეს კამერები დამონტაჟებულია შიგნით თუ მის ფარგლებს გარეთ. ანალოგიურად, დაცვის მხარეს არ აქვს უფლება, გამოითხოვოს ელექტრონულად არსებული კომუნიკაციის მონაცემები კრიტიკულ ინფრასტრუქტურულ სუბიექტებზე. იგივე ეხება სამინისტროს თანამშრომელთა პირად ფაილებზე ინფორმაციის შეგროვებასა და დამუშავებას, რომლებიც უკავშირდება მათ სამსახურებრივ საქმიანობას ან/და სამინისტროში მიმდინარე ელექტრონულ თვალთვალსა და კონტროლს.

ქვემოთ ნავარაუდებია, რომ პროკურატურას ან სხვა სამართალდამცავ ორგანოებს წვდომა ექნებათ ზემოთ დასახელებულ მონაცემებზე. კითხვაზე, შეიძლება თუ არა, კანონმდებლის ნებით მათზე დაწესდეს შეზღუდვები წინასწარი ან შემდგომი სასამართლო კონტროლის გზით, წარმოდგენილი

---

* მოცემული სტატია წარმოადგენს DGStZ-ის 2019 წლის პირველი გამოცემის პირველ და მომდევნო გვერდებზე გამოქვეყნებული სტატიის გაგრძელებას.

** სტატია ქართულად თარგმნა *ხათუნა ბაგრატიონმა*.

ინფორმაციის შეზღუდული მოცულობის გამო, ამ ეტაპზე პასუხის გაცემა შეუძლებელია.

2. გამოყენების ფარგლები

კრიტიკული ინფრასტრუქტურის სუბიექტების შესახებ შემოთავაზებული ახალი რეგულაცია შედარებით დიდი მასშტაბით ითვალისწინებს დაცვის მხარის გამორიცხვის შემთხვევებს. ის ვრცელდება, ერთი მხრივ, ვიდეო ჩანაწერებზე, რომლებიც გადაღებულია ინფრასტრუქტურის სუბიექტების ფარგლებს გარეთ ან შიგნით. მეორე მხრივ, ის ასევე მოიცავს ინფორმაციას თანამშრომლების შესახებ, რომელიც მოცემულია მათ პირად საქმეებში და დაკავშირებულია მათ სამსახურებრივ საქმიანობასთან ან სამინისტროში მიმდინარე ელექტრონულ თვალთვალთან და კონტროლთან. გარდა ამისა, დაცვის მხარისთვის არ უნდა იყოს ხელმისაწვდომი ელექტრონულ საშუალებებში შენახული ინფორმაცია, რომელიც ეხება ინფრასტრუქტურის სუბიექტებს.

2.1. აეროპორტი

აეროპორტის შენობაში სათვალთვალო კამერის ვიდეოჩანაწერების სრული გამორიცხვა შესაძლოა არ იყოს გამართლებული. იმდენად, რამდენადაც, აეროპორტების დიდი ნაწილი – ისევე, როგორც, მაგალითად, მატარებლის სადგურები ან ნავსადგურები – საჯაროდ ხელმისაწვდომი არიან. თვითმფრინავისა და აეროპორტის ტერიტორიის სივრცის დიდი ნაწილი არ წარმოადგენს უსაფრთხოების დაცვის მომეტებულ საჭიროებასთან დაკავშირებულ საიდუმლო ტერიტორიას და ყველასთვის საჯაროდ ხელმისაწვდომია. ე. ი. ისინი არ ექვემდებარება პირთა შეზღუდულ დაშვებას (მაგ., ბილეთების გასაყიდი დარბაზები და იქ არსებული მაღაზიები, კაფეები და ა. შ.). ვინაიდან ტერმინი „აეროპორტი“ კანონპროექტში არამხოლოდ პირად სფეროსთან დაკავშირებული ადგილების გაგებით გამოიყენება (მაგ., გასახდელები, საპირფარეშოები და ა. შ.), არამედ ასევე მოიცავს აეროპორტის საჯაროდ ხელმისაწვდომ არეებს, ასეთი ფართო გამორიცხვა არ უნდა იყოს მიზანშეწონილი. უცნაურია, რომ აეროპორტში, სათვალთვალო კამერის ჩანაწერები არ შეიძლება იყოს ხელმისაწვდომი დაცვის მხარისთვის, თუმცა აეროპორტში სმარტფონის ან ციფრული კამერის გამოყენებით მგზავრების ან სტუმრების მიერ გადაღებული კადრები (და შესაძლებელია, რომ ისინი ზუსტად იმავეს გამოსახავდნენ, რასაც სათვალთვალო კამერები) არ ექვემდებარება შეზღუდვებს და, ალბათ, განიხილება, როგორც ჩვეულებრივი, დაცვის მხარისთვის ხელმისაწვდომი მტკიცებულებები. ეს შეუსაბამობა საკანონმდებლო ორგანოს მიერ გამოსწორებულ უნდა იქნას.

2.2. სახელმწიფო სათვალთვალო შენობა, სახელმწიფო მოხელეები

სახელმწიფო სათვალთვალო შენობები და აღჭურვილობა, კანონპროექტის თანახმად, შეიძლება მოექცეს „კრიტიკული ინფრასტრუქტურის სუბიექტის“ განმარტებაში.

რამდენადაც არ ხდება უსაფრთხოების სუბიექტებში დასაქმებული პერსონალის ვინაობის გამჟღავნება, პრობლემაც არ არსებობს. თუ რომელი თანამშრომელი რომელი ტექნოლოგიით ახორციელებს თვალთვალს, არის ისეთი საკითხი, რომელსაც თავისთავად არ აქვს მნიშვნელობა სისხლის სამართლის საქმეზე დაცვისთვის. გარდა ამისა, უსაფრთხოებასთან დაკავშირებული საიდუმლოების დაცვა მნიშვნელოვანია კრიმინალური და ტერორისტული ორგანიზაციების მიერ მუქარის არიდების კონტექსტში – თვალთვალზე პასუხისმგებელი სუბიექტები არ უნდა გახდნენ საბოტაჟისკენ მიმართული ქმედებების ან სულაც ტერორისტული თავდასხმების სამიზნე. გარდა ამისა, საზედამხედველო დაწესებულებებში დასაქმებულთა მიმართ მესამე პირების მხრიდან მომდინარე ყველანაირი საფრთხე გამორიცხული უნდა იყოს. ამდენად, სისხლისსამართლებრივი წარმოებისასაც უნდა იქნეს გათვალისწინებული საიდუმლოების დაცვის როგორც სახელმწიფო და საზოგადოებრივი ინტერესები, აგრეთვე პერსონალის დაცვის ინტერესები.

3. ევროპული სამართლის ნორმები

3.1. ევროპის უსაფრთხოების დაცვის სამართალი

„კრიტიკული ინფრასტრუქტურის“ ევროპულ-სამართლებრივი განმარტება, უპირველეს ყოვლისა, მოცემულია 2008 წლის 8 დეკემბრის ევროკავშირის 2008/114/EG დირექტივის მე-2 მუხლის ა) ქვეპუნქტში[1], რომლის თანახმადაც, კრიტიკული ინფრასტრუქტურა არის –

- წევრ სახელმწიფოში განთავსებული მოწყობილობა, სისტემა ან მისი ნაწილი,

- რომელიც აუცილებელია მოსახლეობის მნიშვნელოვანი სოციალური ფუნქციების, ჯანმრთელობის, უსაფრთხოების და ეკონომიკური ან სოციალური კეთილდღეობის შესანარჩუნებლად[2]

- და მათი შეფერხება ან განადგურება მნიშვნელოვან გავლენას მოახდენს წევრ სახელმწიფოზე, იმდენად, რამდენადაც ამ ფუნქციების შენარჩუნება შეუძლებელი იქნება.

ევროპულ დონეზე ევროპული კრიტიკული ინფრასტრუქტურა მოიცავს ორივე სექტორს – ენერგიასა (ელექტროენერგია, ნავთობი, გაზი) და ტრანსპორტს (საგზაო, სარკინიგზო, საავიაციო, მოძრაობა, შიდა წყლებში ნაოსნობა, ოკეანისა და სანაპირო გადაზიდვები და პორტები). ამ დირექტივაში, საქართველოს კანონის პროექტისგან განსხვავებით, სახელმწიფო სათვალთვალო შენობები არ შედის კრიტიკულ ინფრასტრუქტურულ სუბიექტებში. ასეთი სათვალთვალო შენობები დირექტივაში არ არის ნახსენები.

მეორე მხრივ, გერმანიის უსაფრთხოების შესახებ კანონმდებლობაში სექტორების წრე კიდევ უფრო მეტად ფართოვდება. ისინი მოიცავენ სახელმწიფოსა და ადმინისტრაციას, მათ შორის სასამართლო ხელისუფლების თანამშრომლებს.[3]

ევროპული სამართლის მოთხოვნა კრიტიკული ინფრასტრუქტურის სუბიექტის შესახებ ინფორმაციის ან კრიტიკული ინფრასტრუქტურის სუბიექტიდან მოპოვებული ინფორმაციების სისხლის სამართლის პროცესში განსაკუთრებული საიდუმლო დაცვისთვის დაქვემდებარების შესახებ – როგორც ჩანს – არ არსებობს. ზემოხსენებული დირექტივაც ამის თაობაზე არაფერს ამბობს. თუმცა დირექტივა, ზოგადად, რამდენიმე ადგილას ხაზს უსვამს, რომ მხედველობაში უნდა იქნას მიღებული სახელმწიფოს ეროვნული საიდუმლოების ინტერესები, რაც ნიშნავს, რომ – განსაკუთრებით კრიტიკული ინფრასტრუქტურის სუბიექტების შემთხვევაში – დებულებები საიდუმლოს დაცვის შესახებ დაცულ უნდა იქნას.[4]

3.2. მონაცემთა დაცვის ევროპული სამართალი

ხშირ შემთხვევაში, ინფრასტრუქტურის სუბიექტიდან მონაცემის ამოღებისას საქმე გვაქვს პერსონალურ მონაცემებთან. პერსონალური მონაცემები არის ისეთი მონაცემები, რომლებიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირებს.[5] ასეთი შემთხვევაა, მაგალითად, თუ პირები, რომლებიც ჩანან კამერის ჩანაწერზე, უკვე ცნობილი არიან სახელით ან, სულ მცირე, შესაძლებელია მათი იდენტიფიცირება. ეს ამავდროულად ხსნის მონაცემთა დაცვის შესახებ კანონის მოქმედების არეალს. ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია (DGSVO),[6] რომელიც ძალაში შევიდა 2018 წლის მაისში, განზრახ არ შეიცავს უსაფრთხოების და სისხლის სამართლის სფეროს შესახებ დებულებებს: ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის მე-2 მუხლის მე-2

[1] იხ. ევროპული კრიტიკული ინფრასტრუქტურის იდენტიფიკაციისა და მონაცემების წარმოდგენის და მათი დაცვის გაუმჯობესების აუცილებლობის შესახებ შეფასების დირექტივა (ევროკავშირის ოფიციალური საუწყებო მაცნე 23. 12. 2008, L 345/75).

[2] 2013 წლის 12 აგვისტოს 2013/40/EU დირექტივის თანახმად, მათ რიგს განეკუთვნება ენერგოსადგურები, სატრანსპორტო და სახელმწიფო ქსელები.

[3] ასე, მაგალითად, მოსახლეობის დაცვისა და კატასტროფებისას დახმარების გერმანიის ფედერალური ოფისი: იხ. ვებ-გვერდი: www.bbk.bund.de.

[4] დირექტივის მე-7 და მე-18 დეკლარაციული ნაწილი 2013/40/EU.

[5] შეად. განმარტება მონაცემთა დაცვის შესახებ ძირითადი დებულების მე-4 მუხლის პირველ პუნქტში.

[6] 2016 წლის 27 აპრილის ევროპარლამენტისა და ევროსაბჭოს რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, მონაცემთა თავისუფალი მიმოცვლისა და 95/46/EG დირექტივის (მონაცემთა დაცვა-ზოგადი რეგულაცია) გაუქმების შესახებ.

პუნქტის დ) ქვეპუნქტი ითვალისწინებს, რომ ეს რეგულაცია არ ვრცელდება უფლებამოსილი ორგანოების მიერ პერსონალური მონაცემების დამუშავებაზე სისხლის სამართლის დანაშაულის თავიდან აცილების, გამოძიების, გამოვლენის ან დევნის, ან სასჯელის აღსრულების მიზნით, მათ შორის, საზოგადოებრივი უსაფრთხოების დაცვისა და საფრთხეების თავიდან აცილებისას.

სისხლის სამართლის პროცესში გამოიყენება პოლიციასა და მართლმსაჯულების ორგანოებში მონაცემთა დაცვის დირექტივა 2016/680,[7] რომელიც უნდა იქნეს იმპლემენტირებული შესაბამის ეროვნულ სამართალში. დირექტივა (EU) 2016/680, განსხვავებით მანამდე მოქმედი მონაცემთა დაცვის RB 2008/977 / JHA ჩარჩო გადაწყვეტილებისაგან, ეხება არა მხოლოდ ტრანსნაციონალურ, არამედ წმინდა შიდასახელმწიფოებრივ საკითხებსაც. ამავდროულად, გერმანიაში იმპლემენტაცია განხორციელდა სხვადასხვა საკანონმდებლო ცვლილების გზით, მათ შორის სისხლის სამართლის საპროცესო კოდექსში[8]. დირექტივა იძლევა კომპეტენტური ორგანოების მიერ მონაცემთა დამუშავებას შესაძლებლობას (პირველი მუხლი) რეპრესიული და პროფილაქტიკური მიზნით, იმ პირობით, რომ ეს არის პროპორციული და შეესაბამება მონაცემთა დაცვის სხვა რეგულაციებს, როგორც ეს განსაზღვრულია დირექტივის მე–4 მუხლში. აგრეთვე, პერსონალურ მონაცემთა დაცვის ფარგლებში დასაშვებია, რომ პერსონალური მონაცემები გადაცემულ იქნას დაცვის მხარისთვის. 72-ე დირექტივის წინასიტყვაობაში ასევე მკაფიოდაა მითითებული პერსონალურ მონაცემთა გადაცემის შესაძლებლობაზე, თუმცა ეს მოითხოვს აუცილებლობის კრიტერიუმის მკაცრ დაცვას. თუ ეჭვმიტანილის დასაცავად აუცილებელია ამ ინფორმაციის გადაცემა მისი დამცველისთვის, მაშინ ეს ნებადართულია მონაცემთა დაცვის შესახებ კანონის შესაბამისად. დირექტივა შეიცავს აგრეთვე პერსონალურ მონაცემების მესამე ქვეყნებსა თუ საერთაშორისო ორგანიზაციებზე გადაცემის წესებს (35-ე და მომდევნო მუხლი)

3.3. ადამიანის უფლებათა ევროპული კონვენცია

თუ სისხლის სამართლის საქმეზე დაცვის მხარემ ვერ მოიპოვა ინფრასტრუქტურული კრიტიკული სუბიექტებისგან ინფორმაციაზე წვდომის უფლება, მაშინ აღნიშნული ექცევა ადამიანის უფლებათა ევროპული კონვენციის მე-6 მუხლის პირველი პუნქტის პირველი წინადადების – სამართლიანი სასამართლოს უფლების – მოქმედების ფარგლებში.

ა) მხარეთა შეჯიბრობითობა და თანასწორობა

მტკიცებულებათა მოპოვებაზე არსებითად შეუზღუდავი წვდომა სამართლიანი სისხლის სამართლის პროცესის ძირითადი პრინციპია.[9] ძირითადად, ბრალდებულს ან მის დამცველს უფლება აქვს ქონდეს წვდომა ყველა იმ მტკიცებულებაზე, რომელიც აქვს ბრალდების მხარეს.[10] ამის უკან დგას მხარეთა შეჯიბრობითობისა და თანასწორობის იდეა სისხლის სამართლის პროცესებში მონაწილე პირთათვის.[11] თუმცა, შეიძლება საჭირო გახდეს გარკვეული მტკიცებულებების წვდომაზე ბრალდებულისა და მისი დამცველის შეზღუდვა, თუ ეს წარმოადგენს საჯარო ინტერესს. ამრიგად, თუ კრიტიკული ინფრასტრუქტურის სუბიექტების, მათ შორის სახელმწიფო სამეთვალყურეო სტრუქტურების, შესახებ გარკვეული ინფორმაცია არ არის ხელმისაწვდომი დაცვის მხარისთვის, ეს შეიძლება იყოს საჭირო ზემოხსენებული საიდუმლოებისა და უსაფრთხოების საფუძვლებიდან გამომდინა-

[7] 27.04.2016 წლის ევროპარლამენტისა და ევროსაბჭოს დირექტივა (EU) 2016/680 უფლებამოსილი ორგანოების მიერ სისხლის სამართლის დანაშაულის თავიდან აცილების, გამოძიების, გამოვლენის ან დევნის მიზნით ან სასჯელის აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის და საბჭოს 2008/977/JI ჩარჩო გადაწყვეტილების გაუქმების შესახებ.

[8] პერსონალურ მონაცემთა დაცვის VO (EU) 2016/679-სთან შესაბამისობისა და (EU) 2016/680 დირექტივის იმპლემენტაციის შესახებ კანონი v. 30.07.2017, BGBl I 2017, 2097 და მომდევნო.

[9] *Jähnke/Schramm*, Europäisches Strafrecht (EuStR), 2017, Kap. 9 Rn. 55.

[10] *Meyer-Ladewig/Harrendorf/König*, in: *Mayer-Ladewig/Nettesheim/von Raumer*, EMRK, 4. Aufl. 2017, Art. 6 Rn. 140.

[11] ბულუტი ავსტრიის წინააღმდეგ, EGMR 22. 2. 1996 – 17358/90, 47: თითოეულ მხარეს უნდა მიეცეს გონივრული შესაძლებლობა, წარმოადგინოს მისი დასაბუთება ისეთ პირობებში, რომ არ აღმოჩნდეს მეორე მხარესთან შედარებით უარეს მდგომარეობაში.“

რე (მაგალითად, ტერორისტული ან დივერსიული რისკების გამო).

თუ პროკურატურა ან სასამართლო არსებით სხდომაზე კვლავ აგრძელებს ამ მტკიცებულების გამოყენებას, მაშინ ასეთ შემთხვევაში დადგებოდა პროცესში მონაწილე მხარების მხრიდან კომპენსაციის ვალდებულება: მტკიცებულების მიღებაზე უარის თქმით გამოწვეული უარყოფითი შედეგები შეიძლება და უნდა ანაზღაურდეს სხვა ღონისძიებებით. ეს შეიძლება გაკეთდეს, უპირველეს ყოვლისა, სხვა მტკიცებულებების გამოყენებით, ასევე იმ მტკიცებულებების განსაკუთრებით ფრთხილად შეფასებით, რომლებიც არ არის ხელმისაწვდომი დაცვის მხარისთვის.[12] ადამიანის უფლებათა ევროპული სასამართლოს დადგენილი პრეცედენტული სამართლის თანახმად, გადამწყვეტი მნიშვნელობა აქვს, რომ, საერთო ჯამში, ეს პროცესი იყოს ზოგადად სამართლიანი.[13]

ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტული სამართლის თანახმად, მტკიცებულება, რომელიც გამოძიების პროცესში მხოლოდ ბრალდების მხარისთვის ან სასამართლოსთვის იყო ხელმისაწვდომი და არა დაცვის მხარისთვის, აბსოლუტურად შეჯიბრებით სისხლის სამართლის პროცესში (მაგ., როგორც საქართველოში) არ შეიძლება გამოყენებულ იქნას სასამართლოს მთავარ სხდომაზე როგორც ერთადერთი ან გადამწყვეტი მტკიცებულება.[14] მტკიცებულებათა სამართლიანად მოპოვების პრინციპი, რომელიც ადამიანის უფლებათა ევროპული სასამართლოს მიერ ანონიმური მოწმის დაკითხვისთვის, დაცვის მხარის მიერ კითხვების დასმის ან შეპასუხების შესაძლებლობის არარსებობის შემთხვევებში იქნა შემუშავებული, შეიძლება მარტივად გავრცელდეს აქ განხილულ საქმეთა კონსტალაციებზე.[15]

ბ) ერთადერთი გამამართლებელი მტკიცებულება

განსაკუთრებით პრობლემურია ბრალდებულის გამორიცხვის საკითხი, როცა ის ვიდეოჩანაწერი, რომლითაც მას შეუძლია დაამტკიცოს თავისი უდანაშაულობა, არის ერთადერთი და გადამწყვეტი მტკიცებულება. ეს ნიშნავს „in dubio pro reo“ პრინციპის და, შესაბამისად, „სამართლიანი სასამართლოს“ პრინციპის დარღვევას, როცა ბრალდებულს ეკისრება მტკიცების ძალზედ მაღალი ტვირთი და ბრალდებულის სასარგებლო ნებისმიერი მტკიცებულება გამორიცხულია.[16] წარმოიდგინეთ მაგალითი, რომ ბრალდებულს შეცდომით ედავებიან აეროპორტში პოლიციელის ცემას. თუ პოლიციელები სასამართლოს მისცემენ ცრუ ჩვენებას, ბრალდებულს – თუ მას არ გააჩნია სხვა მტკიცებულებები – აღნიშნულის გაბათილების საშუალება ექნება მხოლოდ ვიდეოსათვალთვალო კამერის ჩანაწერის მიწოდებით. მხოლოდ ამის შემდეგ შეიძლება ამ ვიდეო ჩანაწერიდან დადასტურდეს, რომ იგი თავად სცემეს. მას უარს ეტყვიან ამ ჩანაწერზე წვდომაზე, თუ თავად პროკურატურა არ წარუდგენს ამ მტკიცებულებას.

გ) კვალიფიციური სასამართლო კონტროლი

ყოველივე ზემოაღნიშნულიდან გამომდინარე, სასურველი იქნება, რომ, სამართლიანი სასამართლო განხილვის თვალსაზრისით, დაცვის მხარეს კრიტიკული ინფრასტრუქტურის სუბიექტებიდან ვიდეოჩანაწერებზე ან სხვა კომპიუტერულ ფაილებზე წვდომა არ შეეზღუდოს. ცხადია, სამართალდამცავი ორგანოებისადმი მარტივი განცხადებით მიმართვა არ იქნებოდა საკმარისი. კრიტიკული ინფრასტრუქტურული სუბიექტების უსაფრთხოების მაღალი მნიშვნელობის გამო იგი უნდა ექვემდებარებოდეს სასამართლო კონტროლს (მას ასევე მოსამართლის პრივილეგიას უწოდებენ). ამასთან შესაძლებელია არამარტო მარტივი, არამედ კვალიფიციური სასამართლო კონტროლის შემოღება. დასაფიქრებელია, შუამდგომლობაზე გადაწყვეტილება უნდა მიიღოს თუ არა მხოლოდ იმ სისხლის სამართლის სასამართლომ, რომელსაც სახელმწიფო დაცვის სპეციალური კომპეტენცია გააჩნია (მიწის სასამართლოებთან არსებული გერმანიის სახელმწიფო დაცვის პალატის მსგავსად,

[12] შეად. ასევე გერმანიის უმაღლესი ფედერალური სასამართლოს გადაწყვეტილება BGHSt 55, 70 Rn. 29, განხილულია: *Schramm*, HRRS 2011, 156.

[13] EGMR NStZ 2007, 103 (Haas v. Deutschland); BVerfG NJW 2010, 925; *Meyer-Goßner/Schmitt*, Art. 6 EMRK Rn. 22a; *Schramm*, Internationales Strafrecht, 2. Aufl. 2018, Kap. 3 Rn. 49.

[14] EGMR NJOZ 2010, 1903 Rn. 207. Vgl. auch *Jähnke/Schramm*, EuStR, Kap. 9 Rn. 26: „Was dem Gericht vorliegt, muss auch der Verteidiger kennen.“

[15] *Meyer-Goßner/Schmitt*, 61. Aufl. 2018, Art. 6 EMRK Rn. 22a m. w. N.

[16] *Meyer-Ladewig/Harrendorf/König*, in: *Mayer-Ladewig/Nettesheim/von Raumer,* EMRK, Art. 6 EMRK Rn. 140.

სასამართლოების შესახებ კონსტიტუციური კანონის 74-ე მუხლის შესაბამისად). გარდა ამისა, შესაძლებელია, რომ ბრალდებულისთვის ინფორმაციის გაცემის შესახებ გადაწყვეტილების მიღება არა მხოლოდ ერთი მოსამართლის, არამედ რამდენიმე მოსამართლის (დაახლოებით 3 მოსამართლე) ხელში იყოს.[17] ასევე უნდა არსებობდეს ამ სასამართლო გადაწყვეტილების სხვა სასამართლოს მიერ გადასინჯვის შესაძლებლობა (მაგალითად, გასაჩივრების ფორმით).

4. გერმანიის სისხლის სამართლის საპროცესო კოდექსის დებულებები

ტერმინი „კრიტიკული ინფრასტრუქტურის სუბიექტი“ არ გვხვდება გერმანიის სისხლის სამართლის საპროცესო კოდექსში. ასევე არ მოიპოვება კრიტიკული ინფრასტრუქტურის შესახებ რაიმე დებულება გერმანიის სისხლის სამართლის სხვა საპროცესო კანონმდებლობაში. მხოლოდ მატერიალური სისხლის სამართლის კანონმდებლობაშია მოხსენიებული „ინფრასტრუქტურა“ და სარგებლობს გაძლიერებული სისხლის სამართლებრივი დაცვით, კერძოდ, ის გვხვდება კომპიუტერული საბოტაჟის დანაშაულის შემადგენლობაში (სისხლის სამართლის კოდექსის[18] 303-ე მუხლის მე-4 ნაწილის მე-3 ქვეპუნქტი)[19] ან საჯარო დაწესებულებების ფუნქციონირებისთვის ხელის შეშლის შესახებ მუხლში (სსკ-ის 316b მუხლის პირველი ნაწილი).

4.1. კონფიდენციალურობის ინტერესების დაცვა, გაუთქმელობის განცხადება

პროცედურული თვალსაზრისით, გერმანიის სისხლის სამართლის საპროცესო კოდექსი იცავს სახელმწიფო საიდუმლოების ინტერესებს და კონფიდენციალურობას მოხელეების მიერ ჩვენების მიცემაზე ნებართვის და გაუთქმელობის ხელწერილის ზოგადი სამართლებრივი ინსტიტუტებით.

მაგალითად, პოლიციელების, პროკურორების, მოსამართლეების ან სხვა საჯარო მოსამსახურეების დაკითხვა მხოლოდ მას შემდეგ არის შესაძლებელი, თუ მანამდე მოპოვებულ იქნა შესაბამისი ზემდგომი ორგანოს მხრიდან ჩვენების მიცემაზე ნებართვა (სისხლის სამართლის საპროცესო კოდექსის[20] § 54). თუ ეს ნებართვა არ არის მოპოვებული, მაშინ საჯარო მოხელეები ვალდებულნი არიან, უარი თქვან ჩვენების მიცემაზე.[21] ანალოგიურად, როცა სახელმწიფო ორგანოებს სხვა ფორმით სთხოვენ ინფორმაციას, ან თუ სახელისუფლებო სტრუქტურა მოითხოვს აქტების გაცემას ან სხვა სახელისუფლებო ორგანოს ზედამხედველობის ქვეშ არსებული ნივთების გადაცემას (მაგ., კომპიუტერული ფაილები, ვიდეოჩანაწერები[22]) – აღნიშნულზე უარის თქმა ასევე შეუძლია ზემდგომ ორგანოს (სსსკ § 96). ეს უარი (ე. წ. „გაუთქმელობის განცხადება“) გამართლებულია მხოლოდ იმ შემთხვევაში, თუ ფაილების გამჟღავნება და ა. შ. საზიანო იქნება ფედერალური რესპუბლიკის ან მიწის კეთილდღეობისთვის. ინფორმაციის ამგვარი გაცემა ან კრიტიკული ინფრასტრუქტურის სუბიექტების თანამშრომლების დაკითხვა მხოლოდ ზემდგომი ორგანოს მიერ დამტკიცების შემდეგ შესაძლოა იყოს საკანონმდებლო მექანიზმი, რომელიც ემსახურება სახელმწიფო საიდუმლოების დაცვას სისხლის სამართლის პროცესის ფარგლებში.

[17] დაახლოებით მსგავსი პროცედურებია გასავლელი გერმანიაში შენობის აუდიო კონტროლის ბრძანების გაცემისას (ე. წ. დიდი უკანონო ფარული მიყურადება სსსკ § 100c) ან ონლაინ-ჩხრეკა (სსსკ § 100b) სსსკ § 100e მუხლის მე-2 ნაწილისა და სასამართლოების შესახებ კონსტიტუციური კანონის 74a მუხლის მე-5 ნაწილისა და 76-ე მუხლის მე-2 ნაწილის ერთობლიობით გათვალისწინებული საპროცესო საფუძვლებით; შეად. SK-StPO-*Frister*, § 74a GVG Rn. 32.

[18] შემდეგში შემოკლებულია, როგორც სსკ.

[19] შეად. *Schramm*, Strafrecht Besonderer Teil 1, 2017, § 6 Rn. 59.

[20] შემდეგში შემოკლებულია, როგორც სსსკ.

[21] *Eschelbach*, in: *Satzger/Schluckebier/Widmaier*, StPO, 3. Aufl. 2018, § 54 Rn. 2; *Percic*, Münchener Kommentar zur StPO, 2014, § 54 Rn. 1.

[22] *Eschelbach*, in: *Satzger/Schluckebier/Widmaier*, § 96 Rn. 2.

4.2. სასამართლო კონტროლი ზედამხედველობის ღონისძიებებზე; მე-10 მუხლის კანონი

ხაზგასმით უნდა აღინიშნოს, რომ სასამართლოს განჩინება კრიტიკული ინფრასტრუქტურის სუბიექტებთან დაკავშირებული ინფორმაციის გაცემის თაობაზე საქართველოშიც იქნება კანონიერი ისეთ შემთხვევებში, თუ პროკურატურას და პოლიციას სურს გამოიყენოს ეს ინფორმაცია. გერმანიაში პოლიციისა და პროკურატურის წვდომა ტელეკომუნიკაციების შინაარსზე (სსსკ § 100a), ონლაინ-ჩხრეკაზე (სსსკ § 100b), ტელეკომუნიკაციის ტრაფიკის მონაცემებზე (სსსკ § 100j) ან ისეთ ვიდეო ფილმებზე, რომლებიც ინახება კომპიუტერში ან სმარტფონში (ამოღება სსსკ §§ 94, 98 მუხლების შესაბამისად), მხოლოდ სასამართლოს განჩინების საფუძველზე არის შესაძლებელი (სსსკ § 98 პირველი ნაწილი, § 100e პირველი ნაწილის პირველი წინადადება). წინააღმდეგ შემთხვევაში არსებობს რისკი, რომ დანაშაულების გასახსნელად შეიძლება სასამართლო ნებართვის გარეშე განხორციელდეს ფარული მიყურადების ღონისძიებები. მაშინ შესაძლებელია ვერავინ დაადგინოს, საერთოდ მოხდა თუ არა ასეთი ფარული მიყურადება. თუმცა სამართალდამცავი ორგანოებისთვის არსებობს შესაძლებლობა, გადაუდებელი აუცილებლობის შემთხვევაში სასამართლო განჩინების გარეშე განახორციელონ ფარული მიყურადება ან ამოღება. მაგრამ ეს ღონისძიება სასამართლოს მიერ სამი დღის განმავლობაში უნდა იქნეს დამტკიცებული (სსსკ § 98, მე-2 ნაწილის პირველი წინადადება, § 100e, პირველი ნაწილის მე-2 და მე-3 წინადადებები).

აქვე უნდა აღინიშნოს აგრეთვე საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის ზემოხსენებული (იხ. თავი II) გადაწყვეტილება, რომლის თანახმად, „პროცესის დამაჯერებელი გამჭვირვალობა და საკანონმდებლო დონეზე კონტროლის მექანიზმები“ იქნა მოთხოვნილი, რათა მომხდარიყო ეროვნული უსაფრთხოების სამსახურების მიერ საკომუნიკაციო არხებზე პირდაპირი ჩარევის თავიდან აცილება.[23]

ეს გავლენას მოახდენს კიდევ ერთ ევროპულ სამართლებრივ განზომილებაზე: სათვალთვალო ღონისძიების დაწყებასა და – საჭიროების შემთხვევაში – განხორციელებაზე სასამართლო კონტროლი ინსტიტუციურად განამტკიცებდა ბრალდებულის პერსონალური მონაცემების დაცვას, რომელიც ადამიანის უფლებათა ევროპული სასამართლოს მიერ კონვენციის მე-8 მუხლის ფარგლებში განიხილება როგორც პირადი ცხოვრების ნაწილი[24]. სახელმწიფოს მიერ კომუნიკაციების ზედამხედველობისას უფლების ბოროტად გამოყენების რისკი ძალიან მაღალია და ევროსასამართლოს პრეცედენტული გადაწყვეტილების მითითებების შესაბამისად, შიდასახელმწიფოებრივმა სამართალმა ხელი უნდა შეუშალოს ხელისუფლების ორგანოების მხრიდან თვითნებურ ჩარევას: პირი ან დაწესებულება, რომელიც პასუხისმგებელია მიყურადების ღონისძიებებზე ნებართვის გაცემაზე, უნდა იყოს დამოუკიდებელი და ექვემდებარებოდეს სასამართლო ან დამოუკიდებელი კონტროლის სხვაგვარ მექანიზმს. მიყურადების ღონისძიება უნდა იყოს დროში შეზღუდული. ასევე უნდა შეიქმნას რეგულაციები, რომლებიც საშუალებას მისცემს დაცვის მხარეს, გაუწიოს კონტროლი მოსმენის ოქმების ცვლილებების გარეშე გადაცემას.[25]

თუმცა, გერმანიაში სხვაგვარად ხდება. მაგალითად, მაშინ, როდესაც გერმანიის უსაფრთხოების ორგანოები მოქმედებენ არა რეპრესიულად, ე. ი. დანაშაულს კი არ იძიებენ, არამედ მოქმედებენ პრევენციულ-პოლიციურად ან კონკრეტული სამართლებრივი სიკეთის დაზიანების თავიდან აცილების მიზნით[26]: გერმანიის კონსტიტუციური დაცვის ორგანოებსა და გერმანიის ფედერალურ სადაზვერვო სამსახურს შეუძლია ტელეკომუნიკაციების მონიტორინგი და ჩაწერა სასამართლო

[23] შეად. გეგეშიძე, ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება – ქართული სამართალი და საერთაშორისო სტანდარტები, გერმანულ-ქართული სისხლის სამართლის ჟურნალი, მეორე გამოცემა – აგვისტო, 2017 წელი, გვ. 44.

[24] EGMR NJW 2007, 1433 Rn, 76 ff (Weber/Saravia v. Deutschland).; *Meyer-Ladewig/Nettesheim*, in: *Mayer-Ladewig/Nettesheim/von Raumer*, EMRK, Art. 8 EMRK Rn. 32.

[25] *Meyer-Ladewig/Nettesheim*, in: *Mayer-Ladewig/Nettesheim/von Raumer*, EMRK, Art. 8 EMRK Rn. 39 unter Verweis auf EGMR NJW 2007, 1433 (Weber/Saravia v. Deutschland).

[26] *Roggan*, in: G-10-Gesetz, Kommentar, 2012, G 10 § 1 Rn. 3 – 5.

ბრძანების გარეშე, თუკი აუცილებელია თავიდან იქნას აცილებული საფრთხე, რომელიც ემუქრება თავისუფალ, დემოკრატიულ საზოგადოებრივ წყობილებას (მიმოწერის, საფოსტო და სატელეკომუნიკაციო საიდუმლოს შეზღუდვის შესახებ კანონის პირველი მუხლი, ე. წ. მე-10 მუხლის კანონი).[27] ნებისმიერ შემთხვევაში, საქმიანობა ექვემდებარება კონტროლს საპარლამენტო ზედამხედველობის ორგანოს მიერ მე-10 მუხლის კანონის მე-16 მუხლის თანახმად და ასევე მე-10 მუხლის კომისიის[28] ან, ფედერალური სადაზვერვო სამსახურის შესახებ კანონის მე-16 მუხლის თანახმად, დამოუკიდებელი კომიტეტის მიერ, რომელიც შედგება სამი ფედერალური მოსამართლისაგან და მოხსენებებს წარუდგენს პარლამენტის საკონტროლო კომიტეტს.

5. შეფასება

კრიტიკული ინფრასტრუქტურის სუბიექტებიდან ვიდეოჩანაწერები ან სხვა კომპიუტერული ფაილები, როგორც წესი, ეხება სახელმწიფო საიდუმლოების დაცვის ინტერესებს. ამ ინფრასტრუქტურისა და მათი პერსონალის საბოტაჟის, ტერორისტული აქტის, დაშინების ან მუქარის გზით ნებისმიერი საფრთხის გათვალისწინებით, ლეგიტიმურია, რომ ეს ფაილები არ უნდა იყოს მარტივად ხელმისაწვდომი დაცვის მხარისთვის. თუმცა იმის გამო, რომ ასეთ ფაილებს, რა თქმა უნდა, შეიძლება გადამწყვეტი მნიშვნელობა ჰქონდეს დაცვისა და ბრალდებულისათვის, განსაკუთრებით იმ შემთხვევაში, თუ ისინი ბრალდებულს საბოლოოდ ათავისუფლებს, ამგვარ მტკიცებულებებზე წვდომაზე უპირობო დაუშვებლობა, სამართლიანი განხილვის უფლების თვალსაზრისით (ევროკონვენციის მე-6 მუხლი), ევროპული კანონმდებლობით გაუმართლებელია. მაშინ, შემოღებულ უნდა იქნეს დათქმა სასამართლო კონტროლის შესახებ, ე. ი. სასამართლომ უნდა გადაწყვიტოს, უნდა მიენიჭოს თუ არა ბრალდებულის დაცვის ინტერესებს უფრო მეტი მნიშვნელობა, ვიდრე სახელმწიფოსა და ზოგადად საზოგადოების საიდუმლოებისა და დაცვის ინტერესებს. აქ შეიძლება კანონი ისე იქნეს შემუშავებული, რომ, პრინციპში, მან დაუშვას გაცემის უფლება და სპეციალური დათქმის ფარგლებში ეს გაცემა აიკრძალოს მხოლოდ გამონაკლის შემთხვევაში, საზოგადოებრივი უსაფრთხოებისა და წესრიგისთვის მნიშვნელოვანი საფრთხის არსებობისას. მხარეთა თანასწორუფლებიანობის თვალსაზრისით, სისხლის სამართლის შეჯიბრებით პროცესში თანმიმდევრული იქნებოდა ასევე, თუ სახელმწიფო უსაფრთხოებისა და სამართალდამცავი ორგანოების სამეთვალყურეო საქმიანობა – გერმანული მოდელის (სსსკ §§ 98, 100) მსგავსად – დაექვემდებარება სამოსამართლო კონტროლს: სისხლის სამართლის პროცესში მათ ასეთი მონაცემების შეგროვება ან მოპოვება უნდა შეძლონ მხოლოდ სასამართლოს მიერ ნებართვის გაცემის შემდეგ.

[27] 2001 წლის 26.ივნისის კანონი (მიმოწერის, საფოსტო და სატელეკომუნიკაციო საიდუმლოს შეზღუდვის შესახებ (მე-10 მუხლის კანონი – G10) v (BGBl. I, 1254), უკანასკნელი ცვლილებები განხორციელდა 2011 წლის 7 დეკემბრის კანონით (BGBl. I S. 2576, 2580).

[28] Zur Konformität dieses Gesetzes mit Art. 8 EMRK vgl. EGMR 2007, 1433 (Weber/Saravia v. Deutschland).