ადამიანის უფლებათა ევროპული სასამართლოს და ევროკავშირის მართლმსაჯულების სასამართლოს მიერ მიღებული გადაწყვეტილებების კრებული

პირადი და ოჯახური ცხოვრების პატივისცემის უფლება

პერსონალურ მონაცემთა დაცვა

თბილისი
2022

ადამიანის უფლებათა ევროპული სასამართლოს და ევროკავშირის მართლმსაჯულების სასამართლოს მიერ მიღებული გადაწყვეტილებების კრებული

პირადი და ოჯახური ცხოვრების პატივისცემის უფლება

პერსონალურ მონაცემთა დაცვა

თბილისი
2022

კრებულზე მუშაობდნენ:

ქეთევან კუკავა
კანონის უზენაესობისა და ადამიანის უფლებების მიმართულების ხელმძღვანელი, IDFI

ნატა ახალაძე
იურისტი, IDFI

სალომე ჩხაიძე
იურისტი/მკვლევარი, IDFI

Kingdom of the Netherlands

IDFI ინფორმაციის თავისუფლების განვითარების ინსტიტუტი

საელჩო ინსპექტორის სამსახური

კრებული მომზადდა პროექტის „პერსონალური მონაცემების დაცვის მხარდაჭერა საქართველოში“ ფარგლებში, რომელიც მხარდაჭერილია საქართველოში ნიდერლანდების საელჩოს მიერ. კრებულში გამოხატული მოსაზრებები შეიძლება არ ასახავდეს ნიდერლანდების საელჩოს პოზიციას.

ISBN 978-9941-8-4066-1

სარჩევი

წინასიტყვაობა

ტექნოლოგიების განვითარება პოტენციურად ზრდის პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევის რისკებს. პერსონალურ მონაცემთა დამუშავება სულ უფრო ფართომასშტაბიან სახეს იძენს როგორც საჯარო, ისე კერძო სექტორში. მონაცემების უკანონო დამუშავების შემთხვევაში კი ზიანი ადგება მონაცემთა სუბიექტის ინტერესებს. შესაბამისად, სამართლებრივი ჩარჩოსა და პრაქტიკის ადაპტირება ახალ გამოწვევებსა და რისკებთან განსაკუთრებულ მნიშვნელობას იძენს.

ტექნოლოგიური პროგრესის პარალელურად, აუცილებელია, მიდგომების განახლება და გარანტიების გაუმჯობესება, რათა ადამიანის უფლებათა ევროპული კონვენციითა და ევროპის კავშირის ძირითად უფლებათა ქარტიით გარანტირებული უფლებები პრაქტიკული და ეფექტური დარჩეს.

წინამდებარე კრებული ადამიანის უფლებათა ევროპული სასამართლოს და ევროკავშირის მართლმსაჯულების სასამართლოს მიერ მიღებულ 10 მნიშვნელოვან გადაწყვეტილებას აერთიანებს. მისი მიზანია მკითხველს გააცნოს პრეცედენტული სამართალი, არსებული რეალობისა და გამოწვევების შესაბამისად განვითარებული ახალი მიდგომები.

ევროკავშირთან ასოცირების შეთანხმება და მისი დღის წესრიგი ითვალისწინებს საქართველოში პერსონალური მონაცემების მაღალ დონეზე დაცვის უზრუნველყოფას, ევროპული სტანდარტების შესაბამისად. ჩვენი მიზანია, ხელი შევუწყოთ ევროპულ სტანდარტებთან დაახლოებას სასამართლოების უახლესი პრაქტიკის შესახებ ცნობიერების ამაღლების გზით.

კრებულში განხილულ საქმეებში სასამართლოებმა შემდეგ მნიშვნელოვან საკითხებზე იმსჯელეს: პოლიციის მიერ პერსონალური მონაცემების დამუშავება; ფარული მეთვალყურეობა; მასობრივი მიყურადება; საკომუნიკაციო მომსახურების მიმწოდებლებისგან და უცხოური დაზვერვის სამსახურებიდან მონაცემების მიღება; დამსაქმებლის მიერ დასაქმებულის კომუნიკაციების მონიტორინგი; ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავება; დამსაქმებლის მიერ ვიდეო მონიტორინგის განხორციელება.

კრებულში შესული გადაწყვეტილებები საინტერესო იქნება იურისტებისთვის, აკადემიური სფეროს წარმომადგენლებისთვის, სტუდენტებისთვის და ზოგადად, პერსონალურ მონაცემთა დაცვით დაინტერესებული პირებისთვის.

დიდი მადლობა მინდა გადავუხადო საქართველოში ნიდერლანდების სამეფოს საელჩოს ამ პროექტის მხარდაჭერისთვის, ასევე სახელმწიფო ინსპექტორის სამსახურს ნაყოფიერი თანამშრომლობისთვის.

ქეთევან კუკავა
კანონის უზენაესობისა და ადამიანის უფლებების მიმართულების ხელმძღვანელი
ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, IDFI

ევროპა მსოფლიოში პერსონალური მონაცემების დაცვის მოწინავე ხაზშია. ევროპის საბჭოსა და ევროკავშირის მონაცემთა დაცვის სტანდარტები ემყარება გამოცდილებას და კულტურას, რომელიც ათწლეულების განმავლობაში ყალიბდებოდა ევროპის ქვეყნებში.

ბოლო წლებში, საქართველოში პერსონალურ მონაცემთა დაცვის კანონმდებლობამ მნიშვნელოვანი პროგრესი განიცადა, თუმცა მონაცემების დაცვის თანამედროვე, მაღალი სტანდარტის დასამკვიდრებლად ჯერ კიდევ ბევრი ნაბიჯია გადასადგმელი.

კრებულში წარმოდგენილი ადამიანის უფლებათა ევროპული სასამართლოს და ევროკავშირის მართლმსაჯულების სასამართლოს ბოლოდროინდელი პრეცედენტული გადაწყვეტილებები ხელს შეუწყობს როგორც იურიდიული პროფესიების წარმომადგენლების ცოდნის გაღრმავებას, ასევე, ნებისმიერი დაინტერესებული პირის ინფორმირებულობას. საერთაშორისო პრაქტიკის ქართულ ენაზე ხელმისაწვდომობა ხელს შეუწყობს საკანონმდებლო დებულებების ინტერპრეტაციას და მათ პრაქტიკულ გამოყენებას საუკეთესო ევროპული სტანდარტების შესაბამისად, რაც პერსონალურ მონაცემთა დაცვის მიზნით გამოყენებულ ღონისძიებებს მეტად ეფექტურს გახდის.

მადლობას ვუხდით საქართველოში ნიდერლანდების სამეფოს საელჩოსა და ინფორმაციის თავისუფლების განვითარების ინსტიტუტს (IDFI), რომელთა მხარდაჭერითა და თანამშრომლობით გახდა შესაძლებელი ამ პროექტის განხორციელება.

სალომე ბახსოლიანი
სახელმწიფო ინსპექტორის მოადგილე

ადამიანის უფლებათა ევროპული სასამართლოს მიერ მიღებული გადაწყვეტილებები

BĂRBULESCU V. ROMANIA

05/09/2017

ფაქტობრივი გარემოებები

ადამიანის უფლებათა ევროპული კონვენციის (შემდგომ „კონვენცია'') მე-8 მუხლზე (პირადი და ოჯახური ცხოვრების პატივისცემის უფლება) დაყრდნობით, ბოგდან მიჰაი ბარბულესკუმ (შემდგომ „მომჩივანი") საჩივრით მიმართა ადამიანის უფლებათა ევროპულ სასამართლოს (შემდგომ „სასამართლო") და მიუთითა, რომ დამსაქმებლის მიერ ელექტრონული კომუნიკაციების მონიტორინგის საფუძველზე, მასთან შრომითი ხელშეკრულების შეწყვეტა არღვევდა მისი პირადი ცხოვრებისა და მიმოწერის პატივისცემის უფლებას. მომჩივანი მიიჩნევდა, რომ ეროვნულმა სასამართლოებმა ვერ შეასრულეს ამ უფლების დაცვის ვალდებულება.

მომჩივანი წარმოშობით რუმინელი, ბუქარესტის მკვიდრი გახლდათ. 2004 წლის 1-ლი აგვისტოდან 2007 წლის 6 აგვისტომდე ის კერძო კომპანიაში იყო დასაქმებული ინჟინრის პოზიციაზე, გაყიდვების მიმართულებით. კლიენტებისთვის პასუხის გაცემის მიზნით, დამსაქმებლის მოთხოვნით, მან შექმნა ''Yahoo Messenger''-ის ანგარიში. ამ პერიოდისთვის, მას უკვე ჰქონდა პერსონალური Yahoo Messenger-ის ანგარიში.

2007 წლის 3 ივლისს კომპანიამ თანამშრომლებს შორის გაავრცელა ინფორმაცია, რომ პირადი მიზნებისთვის ინტერნეტის, ტელეფონისა და ასლის გადამღები აპარატის გამოყენებისთვის, ერთი თანამშრომელი გათავისუფლდა სამსახურიდან დისციპლინური გადაცდომის საფუძველზე. კომპანიის შინაგანაწესი კრძალავდა პირადი მიზნით კომპანიის რესურსების გამოყენებას, თუმცა რეგულაციები არ შეიცავდა მითითებას იმის შესახებ, რომ დამსაქმებელს შეეძლო თანამშრომლების კომუნიკაციის მონიტორინგი. მომჩივანს ეცნობა, რომ განხორციელდა მისი Yahoo Messenger-ის ანგარიშის მონიტორინგი და არსებობდა მტკიცებულება, რომ მან ინტერნეტი პირადი მიზნებისთვის გამოიყენა. 2007 წლის 13 ივლისს მომჩივანი დამსაქმებელმა ახსნა-განმარტებისთვის დაიბარა, თუმცა მას არ ჰქონდა ინფორმაცია, რომ ზედამხედველობა მისი კომუნიკაციის შინაარსზეც გავრცელდა.

მომჩივანმა უარყო ინტერნეტის არასამსახურებრივი მიზნით გამოყენების ფაქტი, საპასუხოდ კი დამსაქმებელმა მას წარუდგინა 45 გვერდიანი ჩანაწერი 2007 წლის 5-12 ივლისის კომუნიკაციებიდან, რომელიც შეიცავდა პირადი ხასიათის მიმოწერას ძმასთან და საცოლესთან. პირადი კომუნიკაციის ზოგიერთი შეტყობინება ინტიმური ხასიათის იყო. შინაგანაწესის დარღვევისათვის, რომელიც კრძალავდა კომპანიის რესურსების პირადი მიზნებისთვის გამოყენებას, 2007 წლის 1-ელ აგვისტოს კომპანიამ მომჩივანთან შრომითი ხელშეკრულება შეწყვიტა.

მომჩივანმა სასამართლოს მიმართა და დამსაქმებლის მიერ შრომითი ხელშეკრულების შეწყვეტის გადაწყვეტილება გაასაჩივრა იმ საფუძველით, რომ დამსაქმებლის ქმედება იყო კონსტიტუციისა და სისხლის სამართლის კოდექსის საწინააღმდეგო, არაკანონიერი და კომპანიამ მისი კომუნიკაციების მონიტორინგით მიმოწერის დაცულობის უფლება დაარღვია.

ბუქარესტის რაიონულმა სასამართლომ საჩივარი არ დააკმაყოფილა იმ საფუძვლით, რომ დამსაქმებლები უფლებამოსილნი იყვნენ დაედგინათ ინტერნეტის მოხმარების წესები, რადგან ინტერნეტი იყო დასაქმებულთათვის სამსახურებრივი მოვალეობის შესასრულებლად მინიჭებული ინსტრუმენტი.

მომჩივანმა ეს გადაწყვეტილება გაასაჩივრა და მიუთითა, რომ სასამართლომ შეპირის-პირებულ ინტერესებს შორის სამართლიანი ბალანსი არ დაიცვა. ის ასევე ამტკიცებდა, რომ არც შინაგანაწესი და არც შეტყობინების ფურცელი მიუთითებდა იმაზე, რომ დამსაქმებელს შეეძლო დასაქმებულის კომუნიკაციის მონიტორინგი. 2008 წლის 17 ივნისის სააპელაციო სასამართლოს გადაწყვეტილებით, მისი საჩივარი არ დაკმაყოფილდა. მეორე ინსტანციის სასამართლომ გაიზიარა რაიონული სასამართლოს ძირითადი შეფასება. მონაცემთა დაცვის შესახებ ევროკავშირის 95/46/EC დირექტივაზე დაყრდნობით, სააპელაციო სასამართლომ დაადგინა, რომ კომპანიის რესურსების პირადი მიზნებისთვის გამოყენების აკრძალვის შესახებ კომპანიის თანამშრომლების გაფრთხილების შემდეგ, დამსაქმებლის ქცევა გონივრულად უნდა ჩაითვალოს. სასამართლომ აღნიშნა, რომ მომჩივნის კომუნიკაციების კონტროლი იყო ერთადერთი საშუალება დისციპლინური დარღვევის არსებობის დასადგენად, ე.ი. დამსაქმებლის ლეგიტიმური მიზნის მისაღწევად.

ამავდროულად, მომჩივანმა კომპანიის წინააღმდეგ წარადგინა სისხლის სამართლის საჩივარი მიმოწერის საიდუმლოების დარღვევის თაობაზე. შესაბამისმა უწყებამ საქმე არ განიხილა იმ საფუძვლით, რომ კომპანია იყო კომპიუტერული სისტემისა და ინტერნეტ კავშირის მესაკუთრე და მას ჰქონდა უფლებამოსილება, შეემოწმებინა დასაქმებულთა ინტერნეტ აქტივობები და სერვერებზე შენახული ინფორმაცია. ამასთან, პერსონალური მიზნებისთვის IT სისტემების გამოყენების აკრძალვის გათვალისწინებით, მონიტორინგი წინასწარ განჭვრეტადი იყო. ეს გადაწყვეტილება მომჩივანს არ გაუსაჩივრებია.

ადამიანის უფლებათა ევროპული სასამართლოს პალატამ, 2016 წლის 12 იანვრის გადაწყვეტილებით, ექვსი ხმით ერთის წინააღმდეგ დაადგინა, რომ კონვენციის მე-8 მუხლით გათვალისწინებული უფლება არ დარღვეულა. სასამართლომ დაასკვნა, რომ ეროვნულმა სასამართლოებმა დაიცვეს სამართლიანი ბალანსი მომჩივნის პირადი ცხოვრებისა და მიმოწერის პატივისცემის უფლებასა და დამსაქმებლის ინტერესებს შორის. პალატის მიერ მიღებულ გადაწყვეტილებაში აღნიშნულია, რომ პირად ცხოვრებასა და კორესპონდენციაში ჩარევა სახეზე იყო, თუმცა დისციპლინური სამართალწარმოების კონტექსტში დამსაქმებლის მიერ მომჩივნის კომუნიკაციების მონიტორინგი გონივრული იყო. ამასთან, სასამართლომ აღნიშნა, რომ დამსაქმებელს მომჩივნის კომუნიკაციის შინაარსზე წვდომა მხოლოდ მას შემდეგ ჰქონდა, რაც მომჩივანმა განაცხადა, რომ მან გამოიყენა Yahoo Messenger სამუშაოსთან დაკავშირებული მიზნებისთვის. პალატამ ასევე აღნიშნა, რომ ეროვნულ სასამართლოებს არ დაუფუძნებიათ გადაწყვეტილებები მომჩივნის კომუნიკაციების შინაარსზე და დამსაქმებლის მონიტორინგის საქმიანობა შემოიფარგლებოდა მხოლოდ დასაქმებულის მიერ Yahoo Messenger-ის გამოყენებით.

მომჩივნის არგუმენტაცია

მომჩივნის შეხედულებით, პალატამ არ გაითვალისწინა საქმის ფაქტობრივი გარემოებების გარკვეული ასპექტები. Yahoo Messenger-ის დიზაინი მიუთითებს, რომ ის შექმნილია პირადი მოხმარებისთვის. დამსაქმებლის მიერ ამ ინსტრუმენტის სამუშაო კონტექსტში გამოყენების გადაწყვეტილება არ ცვლის იმ ფაქტს, რომ პლატფორმა ძირითადად განკუთვნილია პირადი მოხმარებისათვის. მომჩივანი აღნიშნავდა, რომ ის არ იყო წინასწარ გაფრთხილებული იმის შესახებ, რომ კომპანიის წარმომადგენლებს, შესაძლოა, მისი პირადი კომუნიკაცია შეემოწმებინათ ან წაეკითხათ. ამასთან, კომპანიას არ ჰქონდა შემუშავებული ინტერნეტის გამოყენების პოლიტიკა.

მომჩივნის პოზიციით, სასამართლოს უნდა განესხვავებინა მოგების მიღების მიზნით განხორციელებული კომუნიკაცია და პირადი ხასიათის კომუნიკაცია, რომელსაც კომპანიისთვის არანაირი ზიანი არ მიუყენებია და არც დასაქმებულს მიუღია ამით რამე სარგებელი. მან განაცხადა, რომ თანამედროვე სამუშაო პირობები შეუძლებელს ხდიდა პირად და პროფესიულ ცხოვრებას შორის მკაფიო გამყოფი ხაზის გავლებას, აღნიშნული კი ეჭვქვეშ აყენებდა ყველა იმ პოლიტიკის ლეგიტიმურობას, რომელიც კრძალავდა ინტერნეტთან დაკავშირებული მოწყობილობის პირადი მიზნებისთვის გამოყენებას.

მომჩივანი მიუთითებდა, რომ დამსაქმებელმა ჯერ ფარულად შეამოწმა და მხოლოდ შემდეგ მისცა შესაძლებლობა, დაეზუსტებინა, ეს კომუნიკაცია იყო პირადი თუ სამსახურებრივი ხასიათის. მისი მტკიცებით, ეროვნულმა სასამართლოებმა საქმის ფაქტობრივი გარემოებები არასწორად გააანალიზეს და ვერ გაითვალისწინეს კიბერ სივრცეში კომუნიკაციის სპეციფიკური მახასიათებლები.

მომჩივნის თქმით, თანამშრომლებისთვის ხელმისაწვდომი იყო მხოლოდ ერთი პრინტერი, შესაბამისად, სხვა დასაქმებულებსაც შეეძლოთ ენახათ Yahoo Messenger-ის 45 გვერდიანი კომუნიკაციის ჩანაწერი.

მომჩივანი არწმუნებდა დიდ პალატას, დაედასტურებინა, რომ თანამშრომელთა მიმოწერის მონიტორინგი შეიძლება განხორციელდეს მხოლოდ მოქმედი კანონმდებლობის შესაბამისად, გამჭვირვალედ და დამსაქმებლებს არ უნდა ჰქონდეთ დისკრეცია, აკონტროლონ თავიანთი თანამშრომლების მიმოწერა.

მთავრობის არგუმენტაცია

მთავრობის პოზიციით, მომჩივნის მიერ კონვენციის მე-8 მუხლის საფუძველზე წარდგენილი საჩივარი დაუსაბუთებელი იყო. 2007 წლის 5 ივლისიდან 13 ივლისამდე მომჩივნის კომუნიკაციის ჩაწერა იმიტომ განხორციელდა, რომ დამსაქმებელს მისთვის მიეცა შესაძლებლობა, გაემართლებინა ინტერნეტის გამოყენება, რომელიც უფრო შესამჩნევი იყო, ვიდრე სხვა კოლეგების.

მთავრობის პოზიციით, მას შემდეგ, რაც მომჩივანმა განმარტა, რომ კომუნიკაცია დაკავშირებული იყო სამსახურებრივ საქმიანობასთან, დამსაქმებელმა გამოიკვლია მისი ახსნა-განმარტების მართებულობა.

მთავრობამ გაიზიარა პალატის გადაწყვეტილება და აღნიშნა, რომ რუმინეთმა დაიცვა ბალანსი მომჩივნისა და დამსაქმებლის ინტერესებს შორის, შესაბამისად, სახელმწიფომ შეასრულა მე-8 მუხლით გათვალისწინებული პოზიტიური ვალდებულება.

მთავრობა მიუთითებდა, რომ მომჩივანს ეროვნული სასამართლოების დონეზე უნდა ედავა შრომითი სამართლის კონტექსტში. ამ შემთხვევაში კი განხილვის მთავარი აქცენტი გახლდათ, შეესაბამებოდა თუ არა მომჩივნის წინააღმდეგ ჩატარებული დისციპლინური სამართალწარმოება შიდა კანონმდებლობას. მას ასევე შეეძლო, სპეციალური საჩივარი შეეტანა პირადი და ოჯახური ცხოვრების პატივისცემის უფლების დარღვევის თაობაზე, მაგრამ არც ეს გააკეთა. მართალია, მომჩივანმა კომპანიის წინააღმდეგ სისხლის სამართლის საჩივარი წარადგინა, თუმცა შესაბამისმა უწყებებმა შემდგომი მოქმედებების განხორციელება საჭიროდ არ ჩათვალეს იმ საფუძვლით, რომ მონიტორინგი უკანონო არ იყო.

მთავრობის განმარტებით, ევროპის საბჭოს წევრ სახელმწიფოებში დამსაქმებლის მიერ დასაქმებულის მონიტორინგის შესახებ ერთგვაროვანი მიდგომა არ არის. მთავრობამ ასევე აღნიშნა, რომ შიდა სასამართლოებმა განიხილეს დამსაქმებლის გადაწყვეტილების კანონიერება და აუცილებლობა და დაასკვნეს, რომ დისციპლინური სამართალწარმოება მოქმედი კანონმდებლობის შესაბამისად ჩატარდა. მომჩივანს რომ დამსაქმებლის მიერ მიცემული შესაძლებლობა გამოეყენებინა, სასამართლოები შეპირისპირებულ ინტერესებს სხვაგვარად შეაფასებდნენ.

მომჩივნის ბრალდებაზე, რომ 45 გვერდიანი კომუნიკაციის ჩანაწერები კომპანიის სხვა თანამშრომლებმა ნახეს, მთავრობამ დასძინა, რომ მონიტორინგის მასალაზე წვდომა ჰქონდა მხოლოდ სამწევრიან დისციპლინურ საბჭოს, მაშინ როდესაც თავად მომჩივანმა, ეროვნული სასამართლოების ეტაპზე საქმის განხილვისას, სრულად წარადგინა კომუნიკაციის ჩანაწერი, ინტიმური დეტალების დაუფარავად.

მთავრობის განცხადებით, მომჩივნის კომუნიკაციის მონიტორინგი იყო აუცილებელი, რადგან შინაგანაწესის დარღვევის ფაქტის დასადგენად, დისციპლინურ საბჭოს უნდა გამოეკვლია დასაქმებულის მიერ მოყვანილი არგუმენტები. ამასთან, მსგავსად პალატის გადაწყვეტილებისა, მხედველობაში უნდა იქნას მიღებული ის ფაქტიც, რომ კომუნიკაციის შინაარსი ეროვნულ სასამართლოებს მხედველობაში არ მიუღიათ, ჩანაწერების გამოყენებით დადგინდა მხოლოდ კომუნიკაციის პირადი ხასიათი.

მესამე მხარეთა მოსაზრებები

ა. *საფრანგეთის მთავრობის მოსაზრებები*

საფრანგეთის მთავრობამ აქცენტი გააკეთა პირადი ცხოვრებისა და მიმოწერის პატივისცემის უზრუნველყოფის ჭრილში ეროვნული ხელისუფლების პოზიტიური ვალდებულების ფარგლებზე. საფრანგეთის მთავრობამ წარადგინა საფრანგეთის სამოქალაქო კოდექსის, შრომის სამართლისა და სისხლის სამართლის კანონმდებლობის შესაბამისი ნორმების დეტალური მიმოხილვა. მთავრობის შეხედულებით, კონვენციის მე-8 მუხლი ვრცელდება მხოლოდ მკაცრი გაგებით პერსონალურ მონაცემებზე, მიმოწერასა და ელექტრონულ აქტივობებზე. ამასთან დაკავშირებით, მთავრობამ მოიხმო საფრანგეთის საკასაციო სასამართლოს პრეცედენტული სამართალი და მიუთითა, რომ ნებისმიერი მონაცემი, რომლის დამუშავება, გაგზავნა ან მიღება ხორციელდება დამსაქმებლის ელექტრონული მოწყობილობით, ივარაუდება, რომ არის პროფესიული ხასიათის მანამ, სანამ დასაქმებული ნათლად აღნიშნავს, რომ მონაცემები არის ნამდვილად პერსონალური.

საფრანგეთის მთავრობამ განაცხადა, რომ ამ სფეროში სახელმწიფოებს უნდა ჰქონდეთ მიხედულების ფართო ფარგლები, რამდენადაც მიზანს წარმოადგენს კონკურენტულ კერძო ინტერესებს შორის ბალანსის დაცვა. დამსაქმებელს შეეძლო, გონივრული მოცულობით გაეკონტროლებინა დასაქმებულთა პროფესიული მონაცემები და მიმოწერა ლეგიტიმური მიზნის განსახორციელებლად.

ბ. *ევროპის პროფესიული კავშირების კონფედერაციის მოსაზრებები*

ევროპის პროფესიული კავშირების კონფედერაციის (ETUC) მოსაზრებით, სამუშაო გარემოში კონფიდენციალურობის დაცვას გადამწყვეტი მნიშვნელობა ჰქონდა, განსაკუთრებით იმ ფაქტის გათვალისწინებით, რომ ამ კონტექსტში თანამშრომლები სტრუქტურულად იყვნენ დამოკიდებული დამსაქმებლებზე. შესაბამისი საერთაშორისო და ევროპული სამართლის პრინციპების ანალიზის საფუძველზე, ინტერნეტზე წვდომა უნდა ჩაითვალოს ადამიანის უფლებად, ხოლო მიმოწერის დაცულობის უფლება უნდა გაძლიერდეს. ევროპის პროფესიული კავშირების კონფედერაციის შეხედულებით, თანამშრომლების თანხმობა ან სულ მცირე წინასწარი შეტყობინება სავალდებულო იყო. დასაქმებულები ინფორმირებულები უნდა ყოფილიყვნენ იქამდე, ვიდრე დამსაქმებელი თანამშრომლების პერსონალური მონაცემების დამუშავებას დაიწყებდა.

სასამართლოს შეფასება

ადამიანის უფლებათა ევროპული სასამართლოს დიდმა პალატამ განმარტა, რომ ,,პირადი ცხოვრებისა" და ,,მიმოწერის" ცნებები მოიცავს სამუშაო სივრცეში განხორციელებულ კომუნიკაციასაც. პირადი ცხოვრებისა და მიმოწერის პატივისცემის უფლება განაგრძობს არსებობას, მიუხედავად იმისა, რომ ეს უფლება საჭიროების ფარგლებში შეიძლება შეზღუდული იყოს. მართალია, მომჩივნის მიმოწერის მონიტორინგი არ ყოფილა სახელმწიფო ორგანოების პირდაპირი ჩარევის შედეგი, თუმცა მათი პასუხისმგებლობაა, უზრუნველყონ კონვენციის მე-8 მუხლით გათვალისწინებული უფლებით სარგებლობის გარანტიები.

სასამართლომ საქმე განიხილა სახელმწიფოს პოზიტიური ვალდებულების ჭრილში, რამდენადაც კერძო კომპანიის მიერ განხორციელებული ღონისძიება ეროვნულმა სასამართლოებმა გაიზიარეს. სასამართლოს პოზიციით, ეროვნულ ხელისუფლებას მოეთხოვებოდა, დაეცვა ბალანსი პირადი ცხოვრების პატივისცემის უფლებასა და დამსაქმებლის უფლებას შორის - გაატაროს ღონისძიებები კომპანიის შეუფერხებელი მართვის უზრუნველსაყოფად.

წინამდებარე საქმეში, სასამართლოს უნდა განემარტა დასაქმების კონტექსტში მომჩივნის პირადი ცხოვრების და მიმოწერის პატივისცემის უფლების დაცვის მიმართ მოპასუხე სახელმწიფოს პოზიტიური ვალდებულების ბუნება და ფარგლები. სასამართლოს შეფასებით, რამდენადაც ამ საქმესთან კავშირშია შრომის სამართალი, სახელმწიფო ვალდებული იყო დაედგინა საკანონმდებლო ჩარჩო მომჩივნის პირადი ცხოვრებისა და მიმოწერის დასაცავად კერძო დამსაქმებელთან მისი პროფესიული ურთიერთობის კონტექსტში. სასამართლო მიიჩნევს, რომ სახელმწიფოებს აქვთ ფართო მიხედულების ფარგლები დამსაქმებლის მიერ დასაქმებულთათვის არა-პროფესიული ხასიათის ელექტრონული კომუნიკაციის გამოყენების მარეგულირებელი პირობების დამდგენი კანონმდებლობის საჭიროებების შეფასებისას. თუმცა, ეს დისკრეცია არ შეიძლება შეუზღუდავი ხასიათის იყოს. სახელმწიფომ უნდა უზრუნველყოს ის, რომ კომუნიკაციის საშუალებებზე მონიტორინგის ზომებს, მათი მოცულობისა და ხანგრძლივობის მიუხედავად, თვითნებობის თავიდან ასაცილებლად, თან ახლდეს ადეკვატური და საკმარისი დაცვის გარანტიები.

ამ კონტექსტში, ეროვნულმა ორგანოებმა ყურადღება უნდა გაამახვილონ შემდეგ ფაქტორებზე:

01 იყო თუ არა დასაქმებული გაფრთხილებული იმის შესახებ, რომ დამსაქმებელს შეეძლო განეხორციელებინა კომუნიკაციის მონიტორინგი და ჰქონდა თუ არა მას ინფორმაცია შესაბამისი ზომების გატარების შესახებ. როგორც წესი, კონვენციის მე-8 მუხლთან შესაბამისობისათვის, მონიტორინგის ხასიათთან დაკავშირებული შეტყობინება უნდა იყო მკაფიო და წინასწარ გადაცემული;

02 დამსაქმებლის მხრიდან მონიტორინგის მოცულობა და დასაქმებულის პირად ცხოვრებაში ჩარევის ხარისხი. ერთმანეთისგან უნდა განსხვავდეს კომუნიკაციის ნაკადის და კომუნიკაციის შინაარსის მონიტორინგი. ასევე, უნდა დადგინდეს, განხორციელდა მთელი მიმოწერის თუ მხოლოდ მისი ნაწილის მონიტორინგი, იყო თუ არა ჩარევა დროით შეზღუდული და ადამიანთა რაოდენობა, რომელთაც ხელი მიუწვდებოდათ მის შედეგებზე, ლიმიტირებული. იგივე ვრცელდება მონიტორინგის სივრცეში შეზღუდვებზე;

03 წარმოადგინა თუ არა დამსაქმებელმა ლეგიტიმური მიზნები მიმოწერის და მისი შინაარსის მონიტორინგის გასამართლებლად. ვინაიდან კომუნიკაციების შინაარსის მონიტორინგი აშკარად უფრო ინვაზიური ხასიათის მეთოდია, ის უფრო წონად გამართლებას საჭიროებს;

04 იყო თუ არა შესაძლებელი კომუნიკაციის შინაარსზე უშუალო წვდომაზე უფრო ნაკლებად მზღუდავი ხასიათის საშუალების გამოყენება. ამასთან, საქმის გარემოებების გათვალისწინებით, უნდა შეფასდეს, თუ რამდენად შეიძლებოდა დამსაქმებლის მიზნის მიღწევა დასაქმებულის მიმოწერის მთელ შინაარსზე წვდომის გარეშე;

05 რა შედეგი იქონია მონიტორინგმა დასაქმებულზე და დამსაქმებლის მხრიდან იყო თუ არა შედეგები გამოყენებული გაცხადებული მიზნის მისაღწევად;

06 იყო თუ არა დასაქმებული უზრუნველყოფილი დაცვის სათანადო გარანტიებით, განსაკუთრებით მაშინ, როდესაც მონიტორინგის ღონისძიებები იყო მზღუდავი ხასიათის. დაცვის ზომებით უზრუნველყოფილი უნდა იყოს, რომ დასაქმებულის წინასწარი გაფრთხილების გარეშე დამსაქმებელს ხელი არ მიუწვდებოდეს შესაბამისი მიმოწერის შინაარსზე.

სახელმწიფომ უნდა უზრუნველყოს, რომ დასაქმებულს, რომლის მიმოწერაზეც მონიტორინგი განხორციელდა, ხელი მიუწვდებოდეს სასამართლო ორგანოზე, რომელიც უფლებამოსილია დაადგინოს, რამდენად იყო ზემოაღნიშნული კრიტერიუმები დაცული და მიღებული სადავო ზომები - კანონიერი. მოცემულ საქმეში გასარკვევია, რამდენად დაიცვეს ეროვნულმა სასამართლოებმა კონვენციის მოთხოვნები საქმის განხილვისას. სასამართლომ შეამოწმა ფორმა, რომლითაც ეროვნულმა სასამართლოებმა რელევანტური ფაქტები დაადგინეს.

გადაწყვეტილების თანახმად, არ იკვეთება, რომ მომჩივანი წინასწარ იყო ინფორმირებული დამსაქმებლის მიერ კომუნიკაციის მონიტორინგის მოცულობისა და შინაარსის ან იმ შესაძლებლობის შესახებ, რომ დამსაქმებლისთვის შესაძლოა ხელმისაწვდომი გამხდარიყო მისი მოკლე ტექსტური შეტყობინებების შინაარსი. ეროვნულმა სასამართლოებმა არაფერი გააკეთეს იმის დასადგენად, შეატყობინეს თუ არა წინასწარ მომჩივანს მონიტორინგის ზომების გამოყენების შესაძლებლობისა და ასეთი ზომების ფარგლების და ხასიათის შესახებ. სასამართლოს შეხედულებით, წინასწარ შეტყობინებად დაკვალიფიცირებისათვის, დამსაქმებლისგან შეტყობინება უნდა გაიცეს მანამ, სანამ მონიტორინგი დაიწყება, განსაკუთრებით მაშინ, როდესაც დასაქმებულის კომუნიკაციის შინაარსზე წვდომა ხორციელდება.

ევროპულმა სასამართლომ აღნიშნა, რომ უფლებაში ჩარევის გასამართლებლად, ეროვნულმა სასამართლოებმა ასევე არ გამოიკვლიეს დამსაქმებლის ლეგიტიმური მიზნები. სააპელაციო სასამართლოს საერთოდ არ უმსჯელია, თუ რა განსაკუთრებულ მიზანს შეიძლებოდა გაემართლებინა ასეთი მკაცრი მონიტორინგი. რაიონულმა სასამართლომ ამ საკითხთან დაკავშირებით, მიუთითა კომპანიის IT სისტემის დაზიანების თავიდან აცილების აუცილებლობაზე, პასუხისმგებლობაზე, რაც შეიძლებოდა კომპანიას დაკისრებოდა კიბერსივრცეში უკანონო ქმედებებისთვის და დამსაქმებლის კომერციული საიდუმლოების გამჟღავნების რისკებზე. თუმცა, სასამართლოს მოსაზრებით, ეს მიზეზები მხოლოდ თეორიულია, რამდენადაც რეალურ საფრთხეზე არაფერი მიუთითებდა. სასამართლოებმა სათანადოდ არ იმსჯელეს, მიზნის მიღწევა შეიძლებოდა თუ არა სხვა ნაკლებად მზღუდავი

საშუალების გამოყენებით. ეროვნულ მართლმსაჯულების ორგანოებს ასევე არ განუხილავთ მონიტორინგის შედეგების გამოყენებისა და მომჩივნის მიმართ წარმოებული დისციპლინური სამართალწარმოების საკითხები, მითუმეტეს, რომ კომპანიამ ყველაზე მკაცრი სანქცია - სამსახურიდან გათავისუფლება გამოიყენა.

გადაწყვეტილების მიხედვით, ეროვნულმა სასამართლოებმა ასევე არ დაადგინეს, დისციპლინური წარმოების რა ეტაპიდან მიუწვდებოდა ხელი დამსაქმებელს კომუნიკაციის შინაარსზე. სასამართლოს მოსაზრებით, იმის დაშვება, რომ მიმოწერის შინაარსი, შესაძლოა, დისციპლინური წარმოების ნებისმიერ ეტაპზე გამხდარიყო ხელმისაწვდომი, გამჭვირვალობის პრინციპს ეწინააღმდეგებოდა.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, ევროპული სასამართლოს დიდმა პალატამ მიიჩნია, რომ ეროვნულმა სასამართლოებმა ვერ უზრუნველყვეს მომჩივნის კონვენციის მე-8 მუხლით გათვალისწინებული უფლების ადეკვატური დაცვა.

საქმის შედეგი

ადამიანის უფლებათა ევროპული სასამართლოს დიდმა პალატამ, 2017 წლის 5 სექტემბრის გადაწყვეტილებით, თერთმეტი ხმით ექვსის წინააღმდეგ, დაადგინა, რომ დაირღვა ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის მე-8 მუხლი - პირადი და ოჯახური ცხოვრების პატივისცემის უფლება.

თექვსმეტი ხმით ერთის წინააღმდეგ, სასამართლომ მიიჩნია, რომ უფლების დარღვევის დადგენა წარმოადგენდა მოთხოვნის საკმარის და სამართლიან დაკმაყოფილებას და მომჩივნისთვის ზიანის ანაზღაურება საჭიროდ არ ჩათვალა, ხოლო 14 ხმით 3-ის წინააღმდეგ მთავრობას მომჩივნის სასარგებლოდ გაწეული ხარჯების გადახდა დააკისრა 1,365 ევროს ოდენობით.

მოსამართლე კარაკასის ნაწილობრივ განსხვავებული აზრი

მოსამართლე აღნიშნავს, რომ ის ეთანხმება უმრავლესობის პოზიციას კონვენციის მე-8 მუხლის დარღვევის დადგენასთან დაკავშირებით, თუმცა არ მიაჩნია, რომ მომჩივნის მორალური ზიანის ასანაზღაურებლად მხოლოდ უფლების დარღვევის დადგენა იყო საკმარისი. მსგავს გადაწყვეტილებას სასამართლო იღებს მხოლოდ გამონაკლისის სახით.

მოცემულ საქმეში, ეროვნულმა სასამართლოებმა არ დაიცვეს მომჩივნის კონვენციით გარანტირებული უფლება, მის წინააღმდეგ გამართულმა დისციპლინურმა სამართალწარმოების პროცედურებმა მნიშვნელოვნად დააზარალა მომჩივანი - მან დაკარგა სამსახური. მე-8 მუხლის დარღვევამ მას მიაყენა მორალური ზიანი, რომელიც ვერ ანაზღაურდება უბრალოდ იმის აღიარებით, რომ დარღვევას ჰქონდა ადგილი.

მოსამართლეების რაიმონდის, დედოვის, კიოლბროს, მიტსის, მარუ-ვიკსტრომის და ეიქის საერთო განსხვავებული აზრი

მოსამართლეები ეთანხმებიან უმრავლესობის პოზიციას, რომ მოცემული შემთხვევა სასამართლომ უნდა განიხილოს სახელმწიფოს პოზიტიური ვალდებულების ჭრილში, თუმცა ისინი არ იზიარებენ დიდი პალატის გადაწყვეტილებას კონვენციის მე-8 მუხლის დარღვევის თაობაზე.

განსხვავებული მოსაზრების თანახმად, სახელმწიფოს პოზიტიური ვალდებულების კონტექსტში, მომჩივნის ფიზიკური და ფსიქოლოგიური ხელშეუხებლობის დაცვის შესაბამისი პრინციპები დიდი პალატის მიერ არის ჩამოყალიბებული სასამართლოს პრეცედენტული სამართლის სახით. პირველ რიგში, უნდა აღინიშნოს, რომ პირადი ცხოვრების პატივისცემის უზრუნველსაყოფად შესაბამისი ღონისძიებების შერჩევის უფლებამოსილება ევროპის საბჭოს წევრ ქვეყნებს აქვთ მინიჭებული, თუნდაც ეს ინდივიდების ურთიერთობების სფეროს ეხებოდეს. მეორე, სახელმწიფოს მიერ მიღებული ზომები უნდა არსებობდეს ადეკვატური საკანონმდებლო ჩარჩოს ფორმით, რომელიც დაზარალებულის სათანადო დაცვას უზრუნველყოფს. მე-8 მუხლი არ მოითხოვს, რომ არსებობდეს სისხლის სამართლის დებულება, რომელიც კონკრეტულ ქმედებაზე ვრცელდება. საკანონმდებლო ბაზა ასევე შეიძლება შედგებოდეს სამოქალაქო სამართლებრივი დაცვის საშუალებებისგან, რომელთაც დაცვის საკმარისი გარანტიების უზრუნველყოფა შეუძლიათ.

მოსამართლეთა შეხედულებით, დიდმა პალატამ დაავიწროვა საქმის გარემოებების გამოკვლევის ფოკუსი. უმრავლესობამ ფაქტობრივად გვერდი აუარა და თავი აარიდა რეალურ კითხვას - დაამტკიცა და გამოიყენა თუ არა ხელშემკვრელმა სახელმწიფომ ადეკვატური „სამართლებრივი ჩარჩო“, რომელიც, სულ მცირე, ითვალისწინებდა სამოქალაქო სამართლის საშუალებებს, რომლებიც მომჩივნის საკმარის დაცვას უზრუნველყოფდა?

განსხვავებული მოსაზრების თანახმად, კომპანიის წინააღმდეგ შეტანილ სისხლის სამართლებრივ საჩივარს მომჩივანი ბოლომდე არ მიჰყვა. ამასთან, მან მხოლოდ შრომითი დავების განმხილველ სასამართლოს მიმართა მისი სამსახურიდან გათავისუფლების შესახებ გადაწყვეტილების კანონიერების განხილვის მიზნით და არა დამსაქმებლის მიერ მისი პირადი ცხოვრების/მიმოწერის პატივისცემის დარღვევის შესაფასებლად. სასამართლომ სათანადოდ არ შეაფასა, ეროვნული სამართლებრივი ჩარჩო ითვალისწინებდა თუ არა მომჩივნის უფლების დაცვის ადეკვატურ საშუალებებს. სასამართლომ უგულებელყო სახელმწიფოს მიხედულების ფარგლებიც, რომელიც რუმინეთს უფლებამოსილებას ანიჭებდა, თავად

განესაზღვრა დაცვის საშუალებები. მოსამართლეთა შეფასებით, საქმეში არ არსებობს მტკიცებულება, რომელიც მიუთითებს, რომ არსებული დაცვის საშუალებები არ იყო საკმარისად ხელმისაწვდომი ან ეფექტური მე-8 მუხლით გათვალისწინებული უფლების დაცვის უზრუნველსაყოფად.

უმრავლესობამ აქცენტი გააკეთა შრომითი დავების განმხილველი ეროვნული სასამართლოების მიერ განვითარებულ მსჯელობაზე, რაც მართებული მიდგომა არ იყო. თუმცა, ამ შემთხვევაშიც, განსხვავებული აზრის ავტორი მოსამართლეების შეხედულებით, ამ ანალიზს მე-8 მუხლის დარღვევამდე არ მივყავართ.

ეროვნულმა სასამართლოებმა დაასკვნეს, რომ დამსაქმებლისგან მომჩივანმა მიიღო სათანადო შეტყობინება იმის თაობაზე, რომ მის მიერ კომპიუტერით სარგებლობა, შესაძლოა, მონიტორინგის საგანი გამხდარიყო. მოსამართლეები იზიარებენ ამ შეფასებას და აღნიშნავენ, რომ მომჩივანს უნდა ჰქონოდა მისი ქმედებების მონიტორინგის მოლოდინი. მოსამართლეების მოსაზრებით, კონტროლის ლეგიტიმური მიზანი გახლდათ კომპანიის შეუფერხებელი ფუნქციონირება და დამსაქმებლის მხრიდან თანამშრომლების სამსახურებრივი მოვალეობების განხორციელების მონიტორინგი ვერ ჩაითვლება არაგონივრულად. შესაბამისად, ეროვნულმა სასამართლოებმა ორ კერძო ინტერესს შორის სათანადო ბალანსი დაიცვეს. ამასთან, გასათვალისწინებელია, რომ კონტროლი იყო დროში შეზღუდული და ის ეხებოდა მხოლოდ მომჩივნის ელექტრონულ კომუნიკაციასა და ინტერნეტ აქტივობებს, ხოლო მონიტორინგის შედეგი მხოლოდ დისციპლინური სამართალწარმოების მიზნებისთვის გამოიყენეს და მასზე წვდომა ჰქონდა ამ პროცესში ჩართულ პირებს.

ზემოაღნიშნულიდან გამომდინარე, მოსამართლეები მიიჩნევენ, რომ ეროვნული სასამართლოები მოქმედებდნენ მიხედულების ფარგლებში და მოცემულ საქმეში არ დარღვეულა მომჩივნის პირადი ცხოვრებისა და მიმოწერის პატივისცემის უფლება.

BENEDIK V. SLOVENIA

24/04/2018

ფაქტობრივი გარემოებები

იგორ ბენედიკმა (შემდგომ „მომჩივანი“) ადამიანის უფლებათა ევროპულ სასამართლოს (შემდგომ „სასამართლო“) მიმართა და მის მიმართ ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის (შემდგომ „კონვენცია“) მე-8 მუხლის დარღვევის დადგენა მოითხოვა, რადგან პოლიციამ ინტერნეტ პროვაიდერისგან არაკანონიერად მოიპოვა მისი მონაცემები, რასაც შედეგად მისი ვინაობის იდენტიფიცირება მოჰყვა.

2006 წელს, შვეიცარიის სამართალდამცავი ორგანოს წარმომადგენლებმა ქსელის, „Razorback”-ის მომხმარებლების მონიტორინგი განახორციელეს, რის შედეგადაც აღმოჩნდა, რომ არსებობდნენ მომხმარებლები, რომლებიც ფლობდნენ და ერთმანეთში ცვლიდნენ ბავშვთა პორნოგრაფიის ამსახველ ფოტოსურათებსა და ვიდეოებს. აკრძალული შინაარსის მქონე ფაილები იგზავნებოდა ერთრანგიანი ე.წ. P2P (Pear-to-Peer) ქსელის მეშვეობით, სადაც თითოეული დაკავშირებული კომპიუტერი ერთდროულად მოქმედებდა როგორც სერვისის მიმღებიც და მიმწოდებელიც (server). აქედან გამომდინარე, თითოეულ მომხმარებელს ჰქონდა წვდომა ყველა იმ ფაილზე, რომელსაც სხვა მომხმარებელი გასაზიარებლად ხელმისაწვდომს გახდიდა. მათ ასევე შეეძლოთ ფაილების ჩამოტვირთვა და გამოყენება. შვეიცარიის პოლიციის მიერ ჩაწერილ დინამიური ინტერნეტ პროტოკოლის[1] (ე.წ. "IP") მისამართებს შორის, ერთ-ერთი IP მისამართი მოგვიანებით მომჩივანს დაუკავშირეს.

შვეიცარიის პოლიციის მიერ მოპოვებულ მასალებზე დაყრდნობით, სლოვენიის პოლიციამ, სასამართლო განჩინების (ორდერის) გარეშე, სლოვენიის ინტერნეტ პროვაიდერს (ISP) მომჩივნის შესახებ ინფორმაციის გადაცემა მოსთხოვა. პროვაიდერმა პოლიციას მიაწოდა მომჩივნის მამის სახელი და მისამართი. შემდგომ, სასამართლო განჩინების საფუძველზე, პროკურორმა მოიპოვა აბონენტის პერსონალური მონაცემები და ინტერნეტ ტრაფიკის შესახებ ინფორმაცია. 2007 წელს, ასევე განჩინების საფუძველზე, მომჩივნის საცხოვრებელი სახლიდან ამოიღეს 4 ერთეული კომპიუტერი და გააკეთეს კომპიუტერის მყარი დისკების ასლები. თავდაპირველად, ეჭვმიტანილი გახლდათ მომჩივნის მამა, ხოლო შემდგომ - მომჩივანი.

მყარ დისკებზე არსებული ფაილების შესწავლისას დადგინდა, რომ მათი მცირე ნაწილი შეიცავდა ბავშვთა პორნოგრაფიას. ასევე, მომჩივანს დაყენებული ჰქონდა eMule პროგრამა, რომელიც როგორც სხვა მომხმარებლის ფაილების გადმოწერის, ისე - საკუთარის სხვებისთვის გაზიარების შესაძლებლობას იძლეოდა. ზემოაღნიშნულის გათვალისწინებით, მომჩივნის მიმართ აღიძრა სისხლის სამართლის საქმე პორნოგრაფიის შემცველი მასალის ჩვენების, წარმოების, ფლობისა და გავრცელების მუხლით.

[1] ავტორის შენიშვნა: განსხვავებით სტატიკური IP მისამართისაგან, დინამიური IP მისამართი დროთა განმავლობაში იცვლება, რაც უფრო რთულს ხდის მესამე პირის მიერ მომხმარებლის იდენტიფიცირებას.

მომჩივანი მიუთითებდა, რომ მან არ იცოდა საეჭვო ფაილების შინაარსი და ინტერნეტ პროვაიდერმა უკანონოდ, სასამართლო განჩინების გარეშე, გადასცა პოლიციას მის შესახებ ინფორმაცია. მომჩივანმა გამოძიების დაწყების შესახებ გადაწყვეტილება გაასაჩივრა იმ საფუძვლით, რომ მისი ვინაობის შესახებ ინფორმაცია პოლიციამ არაკანონიერად მოიპოვა. საქმის განხილვისას მომჩივანმა მოითხოვა უკანონოდ მოპოვებული მტკიცებულებების (მათ შორის, სასამართლოს განჩინების გარეშე მოპოვებული ინფორმაცია IP მისამართის შესახებ) დაუშვებლად ცნობა, რაც სასამართლომ არ დააკმაყოფილა.

2008 წელს, სასამართლომ ის დამნაშავედ ცნო და აღნიშნა, რომ მას უნდა სცოდნოდა არასრულწლოვნის გამოსახულების შემცველი ჩამოტვირთული 630 პორნოგრაფიული ფოტოსა და 199 ვიდეოს შესახებ, რომელიც მან სხვა მომხმარებლებისთვისაც გახადა ხელმისაწვდომი. მომჩივანს მიესაჯა 8 თვიანი პირობითი მსჯავრი 2 წლიანი გამოსაცდელი ვადით.

გადაწყვეტილება გაასაჩივრა როგორც პროკურატურამ, ისე მომჩივანმა. ლუბლიანას ზემდგომი სასამართლოს გადაწყვეტილებით, პირობითი სასჯელი შეიცვალა 6 თვიანი პატიმრობით, ხოლო მომჩივნის საჩივარი არ დაკმაყოფილდა უსაფუძვლობის გამო.

მომჩივანმა უზენაეს სასამართლოშიც შეიტანა საჩივარი და მიუთითა, რომ დინამიური IP მისამართი პოლიციას ინტერნეტ პროვაიდერისგან სასამართლო განჩინების გარეშე არ უნდა მიეღო. უზენაესმა სასამართლომ არ დააკმაყოფილა საჩივარი იმ საფუძვლით, რომ შვეიცარიის პოლიციას მარტივად შეეძლო P2P ქსელის მონიტორინგისას ამ ინფორმაციის მიღება მომხმარებლების მიერ გარკვეული შინაარსის მქონე ფაილების გაზიარებისას და ეს არ წარმოადგენდა ინტერნეტ ტრაფიკში ჩარევას. სასამართლოს განმარტებით, მსგავსი კომუნიკაცია ვერ იქნებოდა პირადი სახის და შესაბამისად, დაცული - კონსტიტუციის 37-ე მუხლით.

მომჩივანმა ასევე შეიტანა კონსტიტუციური სარჩელი საკონსტიტუციო სასამართლოში. სასამართლომ მოსაზრების წარდგენის მიზნით, ინფორმაციის კომისარს მიმართა. კომისრის შეხედულების თანახმად, ელექტრონული კომუნიკაციის ინდივიდუალური მომხმარებლის იდენტობის მოპოვების მიზეზი გახლდათ ის, რომ მომხმარებელი კომუნიკაციისთვის საზოგადოებისთვის მეტნაკლებად ხელმისაწვდომ ვებგვერდს იყენებდა. ინფორმაციის კომისრის მოსაზრებით, შეუძლებელი იყო ტრაფიკისა და აბონენტის მონაცემების ერთმანეთისაგან განცალკევება, რამდენადაც თავად ტრაფიკს არ აქვს არანაირი მნიშვნელობა, თუ ის კონკრეტულ პირს არ განსაზღვრავს. კომისარმა ასევე განმარტა, რომ მოქმედი კანონმდებლობით, ელექტრონულ კომუნიკაციასთან დაკავშირებული ნებისმიერი ინფორმაციის მისაღებად, იქნება ეს ტრაფიკის თუ იდენტიფიკაციის მონაცემები, საჭიროა სასამართლო განჩინება.

საკონსტიტუციო სასამართლომ 7 ხმით 2-ის წინააღმდეგ არ დააკმაყოფილა სარჩელი და დაასკვნა, რომ მომჩივნის კონსტიტუციური უფლებები არ დარღვეულა. გადაწყვეტილების მიხედვით, თუ პოლიციას დანაშაულის ეჭვი აქვს, მას უნდა შეეძლოს იმ პირთა იდენტიფიცირება, ვინც ამ დანაშაულებრივი სახის კომუნიკაციაში მონაწილეობს, რადგან ინტერნეტის მომხმარებლების ანონიმურობის პრინციპიდან გამომდინარე, რთულია მათი მიკვლევა. სასამართლო განჩინების აღების საჭიროება კი დამოკიდებულია პირად კომუნიკაციაში ჩარევაზე.

საკონსტიტუციო სასამართლომ განმარტა, რომ ტრაფიკის მონაცემები ნიშნავს ნებისმიერ მონაცემს, რომელიც დამუშავებულია ელექტრონულ საკომუნიკაციო ქსელში კომუნიკაციის გადასაცემად ან გადასახადის დარიცხვის მიზნებისათვის. შესაბამისად, IP მისამართი ტრაფიკის მონაცემს წარმოადგენს. საკონსტიტუციო სასამართლომ იმსჯელა, ჰქონდა თუ არა მომჩივანს კომუნიკაციის ამ პლატფორმაზე პრივატულობის ლეგიტიმური მოლოდინი.

გადაწყვეტილების თანახმად, ტრაფიკის მონაცემები კონსტიტუციის 37-ე მუხლის დაცვის ქვეშ ექცეოდა. თუმცა, გამომდინარე იქედან, რომ მომჩივანმა არ დაფარა IP მისამართი, რომლითაც მას ინტერნეტზე ჰქონდა წვდომა, მან შეგნებულად გახადა ის საჯაროდ ხელმისაწვდომი. შესაბამისად, მას ვერ ექნებოდა პრივატულობის მოლოდინი. საკონსტიტუციო სასამართლოს ამ გადაწყვეტილებას თან ახლდა ორი მოსამართლის განსხვავებული აზრი.

მომჩივნის არგუმენტაცია

მომჩივანი ეყრდნობოდა პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ 108-ე კონვენციაში არსებულ პერსონალური მონაცემების განმარტებას და მიუთითებდა, რომ მისი იდენტიფიცირება სასამართლოს განჩინების გარეშე მოპოვებული მონაცემებით მოხდა.

მომჩივანი აღნიშნავდა, რომ მართალია, მან გააზიარა კომუნიკაციის შინაარსი განუსაზღვრელი პირებისთვის, თუმცა ტრაფიკის მონაცემების ჭრილში, მას უარი არ უთქვამს პირადი ცხოვრების პატივისცემის უფლებაზე. მომჩივნის მოსაზრებით, მონაცემები, როგორიც არის ინტერნეტით სარგებლობის ხანგრძლივობა, მომხმარებლის ვინაობა და იმ ვებგვერდების შესახებ ინფორმაცია, რომელსაც ამ პერიოდში მომხმარებელი ესტუმრა, სარგებლობს კომუნიკაციისა და ინფორმაციის კონფიდენციალურობის განსაკუთრებული დაცვით.

მომჩივანმა მიუთითა, რომ აუცილებელია სტატიკური და დინამიური IP მისამართების ერთმანეთისაგან განსხვავება. პირველი მუდმივად იგივეა, ხოლო დინამიური IP მისამართი ინტერნეტთან დაკავშირების ყოველ ჯერზე იცვლება. შესაბამისად, დინამიური IP მისამართის არჩევით, მომჩივანი ამტკიცებს, რომ მან იდენტობის დაფარვა აირჩია, რამდენადაც მისი ვინაობის გასარკვევად, დამატებით სხვა მონაცემების ცოდნაა საჭირო.

არგუმენტაციაში ნათქვამია, რომ კომუნიკაციის შინაარსის შესახებ მონაცემები მოპოვებული იყო სლოვენიის შესაბამისი უწყებების ჩართულობის გარეშე, ხოლო მათ ამ მონაცემების მისაღებად სასამართლო განჩინება დასჭირდებოდათ. როდესაც სლოვენიის პოლიციამ მისი IP მისამართი მოიპოვა, კანონმდებლობა არ იყო მკაფიო. მეტიც, ეროვნული კანონმდებლობის დებულებები ერთმანეთთან წინააღმდეგობაში მოდიოდა. კონსტიტუციის 37-ე მუხლი მხოლოდ სასამართლო განჩინების საფუძველზე უშვებდა კომუნიკაციის კონფიდენციალურობის უფლებაში ჩარევას. ასევე, ელექტრონული კომუნიკაციების კანონის თანახმად, ტრაფიკის მონაცემები დაცული უნდა ყოფილიყო და პირად კომუნიკაციაში ჩარევა მხოლოდ კომპეტენტური უწყებების მიერ გაცემული ორდერის საფუძველზე შეიძლებოდა. ასევე,

ინტერნეტ პროვაიდერები ვალდებული იყვნენ, წაეშალათ ტრაფიკის მონაცემები, თუ ის გადასახადის დარიცხვის მიზნებისთვის საჭირო აღარ იყო. მეორე მხრივ, სისხლის სამართლის საპროცესო აქტი ინფორმაციაზე ხელმისაწვდომობის სხვა პირობებს ითვალისწინებდა, რაც მიუთითებდა, რომ შესაბამისი უწყებების თვითნებობისგან სათანადო დაცვა უზრუნველყოფილი არ იყო. მომჩივნის პოზიციით, მოცემულ შემთხვევაზე უნდა გავრცელებულიყო კონსტიტუციის 37-ე მუხლი, რომელიც პირად ცხოვრებაში ჩარევას მხოლოდ სასამართლო განჩინების საფუძველზე უშვებდა.

მთავრობის არგუმენტაცია

მთავრობის შეხედულებით, სტატიკური და დინამიური IP მისამართები პერსონალურ მონაცემებს წარმოადგენდა, თუმცა არა - ტრაფიკის მონაცემებს. გამოძიება მხოლოდ მას შემდეგ ფოკუსირდა მომჩივანზე, რაც მისი საცხოვრებელი ბინიდან კომპიუტერები ამოიღეს და მისი ოჯახის წევრები დაკითხეს. შესაბამისად, კავშირი აბონენტსა და მომჩივანს შორის მხოლოდ სახლის ჩხრეკის შემდეგ გამოვლინდა, რაც სათანადო სასამართლო განჩინების საფუძველზე განხორციელდა.

მთავრობის პოზიციით, IP მისამართი პერსონალური მონაცემი იყო, რამდენადაც ის პირის იდენტიფიცირების შესაძლებლობას იძლეოდა. მომჩივანმა თავად აირჩია იმგვარი ვებგვერდით სარგებლობა, რომელიც მის პერსონალურ მონაცემებსა თუ კომუნიკაციის შინაარსს პირთა განუსაზღვრელი წრისთვის ხელმისაწვდომს ხდიდა. მთავრობა მიუთითებდა, რომ მომჩივანი სადავოდ არ ხდიდა იმ გარემოებას, რომ მან არ დაფარა IP მისამართი, რომლითაც ის ოპერირებდა. რადგან IP მისამართის გამჟღავნება აბონენტის მონაცემების გამჟღავნებას გულისხმობდა, მას არ ჰქონია განზრახვა, მისი ვინაობის საიდუმლოება დაეცვა.

მთავრობამ აღნიშნა, რომ ბავშვების უფლებების დასაცავად გატარებული ზომები კანონიერი და პროპორციული იყო. ბავშვები განსაკუთრებით დაუცველ/მოწყვლად ჯგუფს მიეკუთვნებიან და სწორედ ამიტომ არის კონვენციით მათი სპეციალური დაცვა უზრუნველყოფილი.

სასამართლოს შეფასება

სასამართლომ იმსჯელა, პოლიციის მოთხოვნის საფუძველზე ინტერნეტ პროვაიდერის მიერ სამართალდამცავი ორგანოსთვის აბონენტის შესახებ ინფორმაციის გადაცემა, რომელმაც მომჩივნის ვინაობის იდენტიფიცირება გამოიწვია, წარმოადგენდა თუ არა კონვენციის მე-8 მუხლით გათვალისწინებული პირადი ცხოვრების პატივისცემის უფლების დარღვევას. კონვენციის მე-8 მუხლის მე-2 პუნქტის თანახმად, პირადი ცხოვრების პატივისცემის უფლებაში ჩარევა უნდა განხორციელდეს კანონის შესაბამისად, ემსახურებოდეს ერთ ან მეტ ლეგიტიმურ მიზანს და აუცილებელი იყოს დემოკრატიულ საზოგადოებაში ამ მიზნის მისაღწევად.

სასამართლომ განმარტა, რომ IP მისამართი არის ქსელის თითოეული მოწყობილობისთვის მინიჭებული უნიკალური ნომერი, რომელიც მათ კავშირის დამყარების საშუალებას აძლევს. განსხვავებით სტატიკური IP მისამართისაგან, რომელიც მუდმივად არის დაკავშირებული კონკრეტული მოწყობილობის ინტერფეისთან, დინამიური IP მისამართი დროებითია და ინტერნეტთან დაკავშირების ყოველ ჯერზე იცვლება.

კანონთან შესაბამისობის კრიტერიუმზე მსჯელობისას, სასამართლომ აღნიშნა, რომ ეროვნულ კანონმდებლობაში იყო გარკვეული საფუძველი იმისათვის, რომ პოლიციას აბონენტის დინამიურ IP მისამართთან დაკავშირებული ინფორმაცია მოეპოვებინა. თუმცა, გასარკვევია, იყო თუ არა კანონი ხელმისაწვდომი, განჭვრეტადი და კანონის უზენაესობის პრინციპთან თავსებადი. გადაწყვეტილების თანახმად, ხელმისაწვდომობისა და განჭვრეტადობის კუთხით პრობლემა არ იკვეთება. რაც შეეხება კანონის უზენაესობის პრინციპთან თავსებადობას, აქ საჭიროა ეროვნული კანონმდებლობა თვითნებური ჩარევისგან ადეკვატურ დაცვის მექანიზმებს ითვალისწინებდეს. დაცვის ეს გარანტიები ქმედითი და ეფექტური უნდა იყოს.

სლოვენიის სისხლის სამართლის საპროცესო აქტის 149ბ(3) მუხლი, რომელსაც შიდა უწყებები ეყრდნობოდნენ, გარკვეული ელექტრონული კომუნიკაციის საშუალების მომხმარებლის შესახებ ინფორმაციის გამოთხოვას შეეხება. ის არ შეიცავს კონკრეტულ წესებს, რომლებიც დინამიურ IP მისამართებს ან აბონენტის ინფორმაციას მიემართება. სასამართლომ განმარტა, რომ კონსტიტუციის 37-ე მუხლის მიხედვით, კომუნიკაციის კონფიდენციალურობაში ჩარევა დასაშვებია მხოლოდ სასამართლო განჩინების საფუძველზე.

ამასთან, ელექტრონული კომუნიკაციების კანონი, რომელიც უშუალოდ არეგულირებს ელექტრონული კომუნიკაციის უსაფრთხოებასა და კონფიდენციალურობას, მაშინ არ ითვალისწინებდა აბონენტის ან/და ტრაფიკის მონაცემების გადაცემას სისხლის სამართლის სამართალწარმოების მიზნებისთვის. პირიქით, ის მიუთითებდა, რომ ინტერნეტ პროვაიდერმა უნდა დაიცვას ელექტრონული კომუნიკაციის, მათ შორის ტრაფიკის მონაცემების, კონფიდენციალურობა. ამ კანონის თანახმად, მესამე პირისათვის ტრაფიკის მონაცემების გადაცემა შეიძლება მხოლოდ მაშინ, თუ ეს საჭიროა მომსახურების გასაწევად, გარდა იმ შემთხვევისა, როდესაც უფლებამოსილი უწყება კანონის შესაბამისად კომუნიკაციის ამოღების ორდერს გასცემს. შესაბამისად, სასამართლომ აღნიშნა, რომ შიდა კანონმდებლობა, სულ მცირე, თანმიმდევრული არ იყო.

გადაწყვეტილებაში ნათქვამია, რომ საკონსტიტუციო სასამართლოს ერთადერთი არგუმენტი, რის საფუძველზეც მან არ დააკმაყოფილა მომჩივნის მოთხოვნა და დაეთანხმა განჩინების გარეშე აბონენტის ინფორმაციის გაცემას, გახლდათ მომჩივნის მიერ პრივატულობის ლეგიტიმურ მოლოდინზე უარის თქმის პრეზუმფცია.

ყურადსაღებია ის ფაქტი, რომ ეროვნულმა კანონმდებლობამ პოლიციას ვერ შეუშალა ხელი, ინტერნეტ პროვაიდერისგან ინფორმაცია მიეღო, ხოლო თვეების შემდეგ, როდესაც საგამოძიებო მოქმედებები ჯერ კიდევ დაწყებული არ იყო, სასამართლოსთვის მიემართა და მიეღო სრულად თუ არა ნაწილობრივ მაინც იგივე ინფორმაცია, რაც მათ უკვე გააჩნდათ, ამჯერად სასამართლო განჩინების საფუძველზე. სასამართლოს განმარტებით, ეს გარემოება აჩვენებს,

რომ სისხლის სამართლის საპროცესო აქტის 149ბ(3) მუხლი, რომელსაც პოლიცია ეყრდნობოდა, არ ითვალისწინებდა თვითნებური ჩარევისაგან დაცვის გარანტიებს. კანონმდებლობა ასევე არ არეგულირებდა მოპოვებული ინფორმაციის შენახვის პირობებს და არ ითვალისწინებდა უფლებამოსილების ბოროტად გამოყენებისგან დაცვის გარანტიებს ამ მონაცემებზე წვდომის ან მათი გადაცემის პროცესში. აღნიშნული კი პოლიციას შესაძლებლობას აძლევდა, ინტერნეტ პროვაიდერთან მიმართვის საფუძველზე ონლაინ აქტივობის ავტორი გამოევლინა. ამასთან, არ არსებობდა პოლიციის ამ უფლებამოსილების განხორციელებაზე დამოუკიდებელი ზედამხედველობის მექანიზმი.

აღნიშნულიდან გამომდინარე, სასამართლომ დაასკვნა, რომ დინამიურ IP მისამართთან დაკავშირებული ინფორმაცია პოლიციამ იმ კანონმდებლობაზე დაყრდნობით მოიპოვა, რომელიც საკმარისად ცხადი არ იყო და დაცვის სათანადო გარანტიებს არ ითვალისწინებდა. მომჩივნის პირად ცხოვრებაში ჩარევა არ მომხდარა „კანონის შესაბამისად“, როგორც ამას კონვენციის მე-8 მუხლის მეორე პუნქტი მოითხოვს. შესაბამისად, გატარებული ზომების ლეგიტიმური მიზნისა და პროპორციულობის შემოწმების გარეშე, სასამართლომ კონვენციის მე-8 მუხლის დარღვევა დაადგინა.

საქმის შედეგი

ადამიანის უფლებათა ევროპულმა სასამართლომ ექვსი ხმით ერთის წინააღმდეგ დაადგინა კონვენციის მე-8 მუხლის - პირადი ცხოვრების პატივისცემის უფლების დარღვევა.

სასამართლომ ერთხმად მიიჩნია, რომ უფლების დარღვევის დადგენა მოთხოვნის საკმარის და სამართლიან დაკმაყოფილებას წარმოადგენდა და მომჩივნისთვის ზიანის ანაზღაურება საჭიროდ არ ჩათვალა, ხოლო 6 ხმით ერთის წინააღმდეგ მთავრობას მომჩივნის სასარგებლოდ დააკისრა გაწეული ხარჯების - 3,522 ევროს გადახდა.

მოსამართლე იუდკივსკას თანმხვედრი აზრი, რომელსაც მოსამართლე ბოშნიაკი შეუერთდა

მოსამართლე ეთანხმება საქმის შედეგსა და უმრავლესობის მიერ გამოყენებულ მეთოდოლოგიას, თუმცა აღნიშნავს, რომ გასაკვირია უფლებაში ჩარევის დადგენამდე სასამართლოს გართულებული მისვლა და პრივატულობის გონივრულ მოლოდინთან დაკავშირებით ძალიან ფრთხილი მიდგომა. მოცემული საქმე წარმოადგენს უნიკალურ შესაძლებლობას, განიმარტოს ციფრულ ეპოქაში პრივატულობის გონივრული მოლოდინის ფარგლები, სადაც, ჩვენს კონტროლს მიღმა, თითოეული ადამიანის პირადი ცხოვრების შესახებ დიდი ოდენობის ინფორმაცია ცირკულირებს.

დღევანდელ რეალობაში, პირადი ცხოვრების შესახებ ინფორმაციის დაცვა განსაკუთრებით ფასეული ხდება, რაც დღითიდღე უფრო მეტ დაცვას საჭიროებს. იუდკივსკა მიუთითებს, რომ მათ, როგორც მოსამართლეებს, ევალებათ გადახედონ პირადი ცხოვრების პატივისცემის პარადიგმას ისეთი დავების ჭრილში, როგორიც მოცემული საქმეა.

საქმეზე *Katz v. United States* მოსამართლე ჰარლენის თანმხვედრი მოსაზრების თანახმად, პრივატულობის გონივრული მოლოდინის დასადგენად საჭიროა ორმაგი წინაპირობის არსებობა: 1) პირმა გამოხატა პრივატულობის რეალური (სუბიექტური) მოლოდინი და 2) საზოგადოება თანხმდება, რომ ეს მოლოდინი არის გონივრული (ობიექტური). მაგალითად, საქმეში *Bărbulescu v. Romania* სასამართლომ ღიად დატოვა საკითხი, მომჩივანს გააჩნდა თუ არა სამუშაო დროს მიმოწერისას პრივატულობის გონივრული მოლოდინი. წინამდებარე საქმეშიც, ეს საკითხი წამოიჭრა და დასანანია, რომ სასამართლომ ხელიდან გაუშვა მკაფიო პოზიციის დაფიქსირების შესაძლებლობა.

ნიუ ჯერსის სასამართლომ საქმეზე *State v. Reid* განმარტა, რომ ინდივიდებს ISP მისამართები ინტერნეტზე წვდომის მოსაპოვებლად სჭირდებათ. როდესაც ინდივიდი სახლიდან პრივატულად შედის ვებგვერდზე, მას აქვს მოლოდინი, რომ მისი მოქმედებები კონფიდენციალურია. ბევრმა არ იცის, რომ ვებგვერდები, რომლებსაც ისინი სტუმრობენ, IP მისამართებს არეგისტრირებენ. სხვა უფრო გათვითცნობიერებულმა მომხმარებელმა კი იცის, რომ ციფრთა ეს წყობა (იგულისხმება IP მისამართი) დანარჩენი მსოფლიოსთვის არაფერს ნიშნავს, მხოლოდ ინტერნეტ პროვაიდერს შეუძლია IP მისამართი მომხმარებლის სახელად „გადათარგმნოს“.

ნიუ ჯერსის სასამართლომ ასევე თქვა, რომ კოდირებული IP მისამართი არაფერს ამბობს ინტერნეტ კომუნიკაციის შინაარსზე, ხოლო აბონენტის მონაცემებს პიროვნებაზე ბევრი რამის თქმა შეუძლია. IP მისამართების მთელი ჩამონათვალით, შესაძლებელია, პირის ინტერნეტ მოხმარების მიკვლევა. ამ ინფორმაციას შეუძლია გამოავლინოს პირის პირადი ცხოვრების ინტიმური დეტალები. მიუხედავად იმისა, რომ შესაძლოა უშუალოდ ინტერნეტ კომუნიკაციის შინაარსი უფრო მეტ ინფორმაციას ამჟღავნებდეს პირის შესახებ, ორივე ტიპის ინფორმაცია მოიცავს კონფიდენციალურობის ინტერესებს.

მოსამართლის შეხედულებით, ტრაფიკის მონაცემები თუ მეტამონაცემები დღეს უფრო ფართოდ მოიპოვება, ვიდრე კომუნიკაციის შინაარსი. ამგვარი ჩარევა კანონით წინასწარ დადგენილი, მკაფიოდ გამოხატული, ამომწურავი, ზუსტი და ნათელი უნდა იყოს, როგორც მატერიალურ-სამართლებრივად, ისე პროცედურულად. უნდა განისაზღვროს ინდივიდთა კომუნიკაციაში სახელმწიფოს ჩარევის, მეტამონაცემების ან კომუნიკაციის მონაცემების შეგროვების, იმ სფეროების მონიტორინგისა და თვალთვალის საფუძვლები და პირობები, სადაც პირებს პრივატულობის გონივრული მოლოდინი აქვთ.

შეხედულება, რომ მეტამონაცემები შინაარსზე ნაკლები ხარისხის დაცვას იმსახურებს, დღევანდელ რეალობას ეწინააღმდეგება. ამ კატეგორიის მონაცემთა მრავალი ფორმა არსებობს - სატელეფონო ზარები, ელ-ფოსტები, ვებგვერდზე შესვლის ისტორიები, Google Maps-ის მიერ ნაჩვენები ადგილმდებარეობა და ა. შ. თუ პირთან დაკავშირებული ეს

მონაცემები შეგროვდება, გამოიკვეთება პირის პორტრეტი, რომელიც ამჟღავნებს მის ეთნიკურ წარმომავლობას, რწმენას, რელიგიურ შეხედულებებს, ფინანსურ მდგომარეობას, ჯგუფის წევრობას, შენაძენების ისტორიას და სხვა.

მრავალი განსხვავებული წყაროდან მიღებული სხვადასხვა კატეგორიის მონაცემების დამუშავება ახალ რისკებს ქმნის ადამიანის უფლებების მიმართულებით, რაზეც სასამართლოს თვალის დახუჭვა არ შეუძლია, იმ მოცემულობის გათვალისწინებით, რომ ყველაფერი რასაც ჩვენ დღეს ვაკეთებთ, ციფრულ კვალს ტოვებს.

მოცემულ შემთხვევაში, მომჩივანს პრივატულობის გონივრული მოლოდინი ჰქონდა, რამდენადაც IP მისამართის პირთან დაკავშირება მხოლოდ ინტერნეტ პროვაიდერის მიერ მოწოდებული ინფორმაციით არის შესაძლებელი. სასამართლოს ერთმნიშვნელოვნად უნდა განემარტა, რომ IP მისამართების ტექნიკური ანონიმურობიდან გამომდინარე, ინტერნეტ მომხმარებლებს ვებგვერდებზე გადასვლისას პრივატულობის მოლოდინი აქვთ და ამ მონაცემთა დამუშავება იმ კანონის შესაბამისად უნდა ხდებოდეს, რომელიც ზემოთ ჩამოთვლილ კრიტერიუმებს აკმაყოფილებს.

მოსამართლე აღნიშნავს, რომ ჩვენი ძირითადი უფლება, თავადვე გადავწყვიტოთ, თუ როგორ წარვადგენთ საკუთარ თავს გარე სამყაროსთან, არის არსებითი და სასამართლოს ეს პოზიცია უნდა გაემყარებინა.

მოსამართლე ვეჰაბოვიჩის განსხვავებული აზრი

გადაწყვეტილებაზე დართულ განსხვავებულ მოსაზრებაში მოსამართლე მიუთითებს, რომ მან არ დაუჭირა მხარი უმრავლესობის პოზიციას, რომლის მიხედვით, კონვენციის მე-8 მუხლით გათვალისწინებული პირადი და ოჯახური ცხოვრების პატივისცემის უფლების დარღვევა დადგინდა.

2006 წელს სახელმწიფო უწყებებისათვის მიწოდებული ინფორმაცია მომჩივნის არც ტრაფიკის მონაცემს შეიცავდა და არც პერსონალურ მონაცემებს. ეს იყო მომჩივნის მამის მისამართი, სახელი და გვარი, ვინც უშუალოდ გახლდათ ინტერნეტ სერვისის აბონენტი. აქედან გამომდინარე, მომჩივანს არ შეუძლია თავი დაზარალებულად გამოაცხადოს.

ბავშვთა პორნოგრაფიის შემცველი ფაილების გადაცემა დანაშაულებრივი ქმედებაა და ამ დასჯადი ქმედების გონივრული ეჭვი სახელმწიფო უწყებებს ავალდებულებს, დამატებით გამოიკვლიონ გარემოებები. ინფორმაცია, რომელიც მომჩივნის ტრაფიკის მონაცემებს შეიცავდა, მოპოვებული იყო სასამართლოს განჩინების საფუძველზე. 2007 წელს საცხოვრებელი სახლიდან კომპიუტერების ამოღების შემდეგ, მომჩივანს შეუძლია, საკუთარ თავს დაზარალებული უწოდოს.

მოსამართლის შეხედულებით, მამის შესახებ გადაცემული ინფორმაცია არ არის მომჩივანთან საკმარისად დაკავშირებული და ის ვერ ჩაითვლება თავად მომჩივნის პერსონალური მონაცემების გამჟღავნებად. შიდა უწყებებს არ მიუღიათ მომჩივნის შესახებ ინფორმაცია. სასამართლო განჩინების მიღებამდე ის არ ყოფილა არც „იდენტიფიცირებული“ და არც „იდენტიფიცირებადი პირი“, სწორედ ამიტომ, მოსამართლე ვეჰაბოვიჩი არ ეთანხმება უმრავლესობის გადაწყვეტას.

პრივატულობის გონივრულ მოლოდინთან დაკავშირებით, მოსამართლეს მიაჩნია, რომ მომჩივნის სუბიექტური მოლოდინი სასამართლოს არ უნდა მიეღო მხედველობაში, რადგან საქმე დანაშაულებრივ ქმედებას ეხებოდა. ძირითადად ყველა შემთხვევაში, დამნაშავეებს არ სურთ, რომ სხვებმა მათი საქმიანობის შესახებ შეიტყონ. ეს მოლოდინი ვერ იქნება გონივრული, როცა ის არაკანონიერ, კრიმინალურ მოტივს ეფუძნება. დანაშაულებრივი ქმედების დაფარვის მოლოდინი არ უნდა ჩაითვალოს გონივრულად. ამასთან, მომჩივანმა პორნოგრაფიის შემცველი ფაილები გააზიარა საჯაროდ ხელმისაწვდომი ქსელის მეშვეობით. შესაბამისად, მან იცოდა ან უნდა სცოდნოდა, რომ მისი ქმედებები ანონიმური არ იყო.

განსხვავებულ აზრში ნათქვამია, რომ ევროპულმა სასამართლომ არაერთ საქმეში მიიჩნია დანაშაულის აღკვეთა უფლებაში ჩარევის ლეგიტიმურ მიზნად (მაგალითად, Nada v. Switzerland და S. and Marper v. the United Kingdom). მოყვანილ მიზეზთა გამო, მოსამართლე არ დაეთანხმა უმრავლესობის გადაწყვეტილებას, რომლითაც მომჩივნის მიმართ კონვენციის მე-8 მუხლის დარღვევა დადგინდა.

BIG BROTHER WATCH AND OTHERS V. THE UNITED KINGDOM

25/05/2021

ფაქტობრივი გარემოებები

2013, 2014 და 2015 წლებში ადამიანის უფლებების დაცვის სფეროში მომუშავე ორგანიზაციებმა და პირებმა (შემდგომ „მომჩივნები“) ადამიანის უფლებათა ევროპულ სასამართლოს (შემდგომ „სასამართლო“) მიმართეს იმ საფუძვლით, რომ გაერთიანებული სამეფოს ელექტრონული მეთვალყურეობის შემდეგი სამი რეჟიმი კონვენციის მოთხოვნებს არ შეესაბამებოდა: 1. მასობრივი მიყურადების TEMPORA პროგრამა, რომელიც დიდი ოდენობით მონაცემებს ინახავდა და მართავდა. 2. უცხო სახელმწიფოებთან დაზვერვის მონაცემების მიმოცვლის რეჟიმი ამერიკის შეერთებული შტატების PRISM და Upstream პროგრამების მეშვეობით. 3. კომუნიკაციების მონაცემების მიღება საკომუნიკაციო მომსახურების მიმწოდებლებისგან.

სასამართლოში სამი საჩივარი მას შემდეგ შევიდა, რაც ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სააგენტოს ყოფილმა კონტრაქტორმა, ედუარდ სნოუდენმა ფარული მეთვალყურეობისა და დაზვერვის მონაცემების გაცვლის იმ პროგრამების შესახებ გაამჟღავნა ინფორმაცია, რასაც აშშ-სა და გაერთიანებული სამეფოს დაზვერვის სამსახურები იყენებდნენ. მომჩივნები მიიჩნევდნენ, რომ მათი საქმიანობიდან გამომდინარე, გაერთიანებული სამეფოს დაზვერვის სამსახურებს, შესაძლოა, მათ მიმართ მიყურადება განეხორციელებინათ ან ელექტრონული კომუნიკაციების შესახებ მონაცემები მოეპოვებინათ საკომუნიკაციო მომსახურების მიმწოდებლების ან უცხოური დაზვერვის სამსახურებიდან.

გაერთიანებული სამეფო კომუნიკაციების მასობრივი მიყურადებისთვის ორ სისტემას იყენებდა. პირველი სისტემა ტრაფიკს ადარებდა სელექტორების[2] სიას და გროვდებოდა ის კომუნიკაცია, რომელიც სელექტორს შეესაბამებოდა, ხოლო დანარჩენი ავტომატურად ჩამოწერას ექვემდებარებოდა. „გადარჩევის პროცესის“ შედეგად ანალიტიკოსები წყვეტდნენ, რომელი კომუნიკაცია იყო დაზვერვისთვის ღირებული, რაც უნდა გაეხსნათ და წაეკითხათ.

მეორე სისტემა ორ ეტაპიანი იყო. პირველ ეტაპზე „დამუშავების წესების“ გამოყენების შედეგად გამოირიცხებოდა ის მასალა, რომელიც არ იყო მნიშვნელოვანი, ხოლო მეორე ეტაპზე კომპლექსური კითხვარის შედეგად დაზვერვისთვის ღირებული მასალა შეირჩეოდა. ანალიტიკოსები მხოლოდ ამ პროცესის შედეგად შერჩეულ კომუნიკაციას ამოწმებდნენ, ხოლო დანარჩენი მასალა ჩამოწერას ექვემდებარებოდა.

2 კონკრეტული იდენტიფიკატორი, მაგალითად, სახელი, ელექტრონული მისამართი და აშ.

გარდა ამისა, გაერთიანებული სამეფო ამერიკის შეერთებული შტატებიდან ითხოვდა და ღებულობდა ორი პროგრამის მეშვეობით მოპოვებულ ინფორმაციას. PRISM პროგრამა ინტერნეტ მომსახურების მიმწოდებლებისგან დაზვერვის მასალებს (როგორიც არის, კომუნიკაციები) მიზნობრივად მოიპოვებდა, ხოლო Upstream პროგრამა საკომუნიკაციო მომსახურების მიმწოდებლების ოპტიკურ-ბოჭკოვანი სადენებიდან და ინფრასტრუქტურიდან შინაარსსა და კომუნიკაციებთან დაკავშირებულ მონაცემებს აგროვებდა. Upstream პროგრამას ფართო წვდომა ჰქონდა გლობალურ მონაცემებზე, რომლებიც გროვდებოდა, ინახებოდა და საკვანძო სიტყვების გამოყენებით იძებნებოდა.

რაც შეეხება საკომუნიკაციო მომსახურების მიმწოდებლებისგან მონაცემების მიღებას, გაერთიანებული სამეფოს სახელმწიფო მდივანი განსაზღვრავდა „უფლებამოსილ პირს," რომელსაც შეეძლო საკომუნიკაციო მომსახურების მიმწოდებლებისგან მონაცემების გამჟღავნება მოეთხოვა, თუკი არსებობდა კანონმდებლობით გათვალისწინებული საფუძველი, როგორიც არის ეროვნული უსაფრთხოების ინტერესი, დანაშაულის თავიდან აცილების ან გამოვლენის ან უწესრიგობის თავიდან აცილების მიზანი, გაერთიანებული სამეფოს ეკონომიკური კეთილდღეობის ინტერესი, საზოგადოებრივი უსაფრთხოების ინტერესი, საზოგადოებრივი ჯანმრთელობის დაცვის მიზანი და სხვა.

მომჩივნები ზემოაღნიშნულ სამ რეჟიმს ასაჩივრებდნენ ადამიანის უფლებათა ევროპული კონვენციის (შემდგომ „კონვენცია") მე-8 (პირადი და ოჯახური ცხოვრების პატივისცემის უფლება) და მე-10 (გამოხატვის თავისუფლება) მუხლებთან მიმართებით.

მომჩივნების არგუმენტაცია

მომჩივნები მიიჩნევდნენ, რომ კომუნიკაციების მასობრივი მიყურადების რეჟიმი არ შეესაბამებოდა კონვენციის მე-8 მუხლს, რადგან არ იყო აუცილებელი და პროპორციული, შესაბამისად, არ ექცეოდა სახელმწიფოს მიხედულების ფარგლებში. საქმეში *Szabó and Vissy v. Hungary* სასამართლომ აღნიშნა, რომ ფარული მეთვალყურეობის ღონისძიება უნდა იყოს „მკაცრად აუცილებელი" დემოკრატიული ინსტიტუტების დასაცავად და მნიშვნელოვანი დაზვერვის მონაცემების მოსაპოვებლად, მოცემულ შემთხვევაში კი მასობრივი მიყურადება ამ ტესტს ვერ აკმაყოფილებდა.

მომჩივნების თანახმად, მე-8 მუხლით გარანტირებულ უფლებაში ცალ-ცალკე ჩარევა ხორციელდებოდა კომუნიკაციების მიყურადებისას (შინაარსი ან/და კომუნიკაციებთან დაკავშირებული მონაცემები); მონაცემების შენახვისას; მათი ავტომატური დამუშავებისას და შემოწმებისას.

მომჩივნები თანხმდებოდნენ, რომ „არსებითი“ ჩარევა ხორციელდებოდა კომუნიკაციების შემოწმებისას, თუმცა ამავე დროს მიიჩნევდნენ, რომ არასწორი იქნებოდა მტკიცება იმისა, რომ ამ ეტაპამდე არავითარ „მნიშვნელოვან“ ჩარევას ადგილი არ ჰქონდა. პირიქით, სასამართლოს პრაქტიკა ცხადყოფდა, რომ სახელმწიფოს მიერ პერსონალური ინფორმაციის თუნდაც მხოლოდ შენახვა მე-8 მუხლით გათვალისწინებულ უფლებაში მნიშვნელოვანი ჩარევაა. იმის გათვალისწინებით, რომ დამუშავების საშუალებები სწრაფად განვითარდა, მონაცემების მხოლოდ შენახვა და ელექტრონული დამუშავება, უშუალოდ შინაარსის ან კომუნიკაციასთან დაკავშირებული მონაცემების ნახვის გარეშე, თავისთავად, შესაძლოა, მნიშვნელოვნად ინვაზიური იყოს.

მომჩივნები მიიჩნევდნენ, რომ მიყურადების რეჟიმი კანონს არ შეესაბამებოდა, რადგან ამ საკითხის მარეგულირებელი აქტი იყო ზედმეტად რთული, ხოლო მეთვალყურეობის ნამდვილი ბუნება და ფარგლები ფაქტობრივად ცხადი გახდა მხოლოდ მას შემდეგ, რაც ედუარდ სნოუდენმა ამის შესახებ საიდუმლო ინფორმაცია გაამჟღავნა.

საზოგადოებისა და ტექნოლოგიების ცვლილების შედეგად, აუცილებელი გახდა სასამართლოს მიერ მიდგომების განახლება და გარანტიების გაუმჯობესება, რათა კონვენციით გარანტირებული უფლებები პრაქტიკული და ეფექტური დარჩეს. მომჩივანთა აზრით, გაუმჯობესებულმა გარანტიებმა უნდა მოიცვას წინასწარი დამოუკიდებელი სასამართლო ნებართვა ორდერებზე, ასევე სელექტორებისა და შესამოწმებელი მონაცემების შერჩევაზე. გარდა ამისა, როდესაც სელექტორი ან საძიებო ტერმინი კონკრეტულ პირს ეხება, მის მიმართ გონივრული ეჭვის თაობაზე ობიექტური მტკიცებულება უნდა არსებობდეს. საბოლოოდ, მეთვალყურეობის სამიზნეს უნდა ეცნობოს მის მიმართ გატარებული ღონისძიების შესახებ მას შემდეგ, რაც ამგვარი შეტყობინება საჯარო ინტერესს არსებით ზიანს არ მოუტანს.

მომჩივნები გაერთიანებულ სამეფოში არსებული მიყურადების რეჟიმის რამდენიმე პრობლემურ ასპექტზე ამახვილებდნენ ყურადღებას:

01 პირველ რიგში, არ არსებობდა დამოუკიდებელი, არათუ სასამართლო ნებართვა მიყურადების განხორციელებასთან დაკავშირებით. მომჩივნები ასევე აღნიშნავდნენ, რომ აუცილებელი იყო სელექტორებისა და საძიებო ტერმინების გამოყენებაზე დამოუკიდებელი ნებართვის არსებობა.

02 შიდა და გარე კომუნიკაციებს[3] შორის განსხვავება იყო არა მხოლოდ არასათანადოდ განსაზღვრული, არამედ ასევე უსარგებლოც, რადგან კომუნიკაციების უმრავლესობა შესაძლოა „გარე“ კატეგორიაში მოხვედრილიყო. მომჩივნების აზრით, შესაძლებელი იყო შიდა კომუნიკაციების უფრო მყარი დაცვის უზრუნველყოფა.

03 არსებობდა გარკვეული გარანტიები იმ პირების კომუნიკაციების შინაარსთან მიმართებით, ვინც ბრიტანეთში იმყოფებოდა, თუმცა ფაქტობრივად არავითარი გარანტია არ არსებობდა კომუნიკაციებთან დაკავშირებული მონაცემების დაცვის კუთხით.

[3] შიდა კომუნიკაცია გულისხმობს გაერთიანებულ სამეფოში მყოფ პირებს შორის კომუნიკაციას, ხოლო გარე კომუნიკაცია - გაერთიანებული სამეფოს გარეთ გადაცემულ ან მიღებულ კომუნიკაციას.

გაერთიანებულ სამეფოს შეეძლო, სრულად შეეფასა მასობრივი მიყურადების რეჟიმის შედეგად მოპოვებული კომუნიკაციებთან დაკავშირებული მონაცემები, ერთადერთ შეზღუდვას წარმოადგენდა მხოლოდ შენახვის მოცულობა და მაქსიმალური პერიოდი. ამ მონაცემების ძებნა ხორციელდებოდა მისი აუცილებლობისა და პროპორციულობის სახელმწიფო მდივნის მხრიდან დადასტურების გარეშე.

04 არსებული რეჟიმი არ აკონკრეტებდა იმ მიზანს, რისთვისაც მოპოვებული მასალა შესაძლოა შემოწმებულიყო.

05 კომუნიკაციების მიყურადების კომისარი ვერ ახორციელებდა მნიშვნელოვან და ეფექტიან ზედამხედველობას. საგამოძიებო ტრიბუნალის (IPT) ეფექტურობაც შეზღუდული იყო, რადგან ის ვერ უზრუნველყოფდა წინასწარი სასამართლო ნებართვის არარსებობით გამოწვეული ხარვეზის გამოსწორებას. გარდა ამისა, ადამიანებს უნდა ჰქონოდათ გარკვეული საფუძველი ვარაუდისთვის, რომ მათ მიმართ ფარული მეთვალყურეობა განხორციელდა, სანამ ტრიბუნალი მათ საჩივარს მიიღებდა.

მომჩივნები ასევე უთითებდნენ, რომ მასობრივი მიყურადების რეჟიმი არღვევდა მე-10 მუხლს - გამოხატვის თავისუფლებას, რადგან ფართომასშტაბიან მიყურადებას და მოცულობითი მონაცემთა ბაზების არსებობას მსუსხავი ეფექტი ჰქონდა ჟურნალისტების კომუნიკაციის თავისუფლებაზე. მედიის თავისუფლებაში ნებისმიერი ჩარევა, განსაკუთრებით წყაროს კონფიდენციალურობის ნაწილში, სათანადო პროცედურული გარანტიების არსებობას მოითხოვდა. კერძოდ, როდესაც გასატარებელ ზომას შედეგად, შესაძლოა, მოჰყოლოდა ჟურნალისტური წყაროს იდენტიფიცირება ან ჟურნალისტური მასალის გამჟღვანება, ნებართვა მოსამართლეს ან სხვა დამოუკიდებელ და მიუკერძოებელ ორგანოს უნდა გაეცა. ნებართვის გამცემ ორგანოს უნდა ჰქონოდა უფლებამოსილება, დაედგინა, ღონისძიება იყო თუ არა საჯარო ინტერესით გამართლებული და შეიძლებოდა თუ არა ნაკლებად ინვაზიური მეთოდის გამოყენება.

მომჩივნები ასევე აღნიშნავდნენ, რომ გაერთიანებული სამეფოს ხელისუფლების მიერ უცხოური დაზვერვის სამსახურიდან და საკომუნიკაციო მომსახურების მიმწოდებლებისგან მონაცემების მიღების რეჟიმი კონვენციის მე-8 მუხლს არღვევდა.

მთავრობის არგუმენტაცია

მთავრობის თანახმად, მიყურადების შედეგად მოპოვებულ ინფორმაციას გაერთიანებული სამეფოს ეროვნული უსაფრთხოების დასაცავად კრიტიკული მნიშვნელობა ჰქონდა. ეს რეჟიმი მათ შესაძლებლობას აძლევდა, გამოემჟღავნებინათ უცნობი საფრთხეები, ასევე მეთვალყურეობა განეხორციელებინათ ტერიტორიული იურისდიქციის მიღმა ცნობილ სამიზნეებზე.

ელექტრონული კომუნიკაციების გადაცემის მარშრუტის არაპროგნოზირებადი ხასიათის გათვალისწინებით, საზღვარგარეთ ცნობილი სამიზნეებიდან კომუნიკაციების თუნდაც მცირე ნაწილის მოსაპოვებლად, აუცილებელი იყო ყველა კომუნიკაციის მიყურადება, რომელიც გადაიცემოდა კომუნიკაციის კონკრეტული მატარებლებიდან.

მთავრობის თანახმად, მასობრივი მიყურადების რეჟიმი მხოლოდ იმ შემთხვევაში იქნებოდა მე-8 მუხლით გარანტირებულ უფლებაში მნიშვნელოვანი ჩარევა, თუკი კონკრეტული პირის კომუნიკაცია შესამოწმებლად შეირჩეოდა ან რეალურად შემოწმდებოდა ანალიტიკოსის მიერ. კომუნიკაციების დიდი ნაწილი ვერ შეირჩეოდა შესასწავლად და შესაბამისად, ჩამოწერას ექვემდებარებოდა.

გამოხატვის თავისუფლებასთან დაკავშირებით, მთავრობამ აღნიშნა, რომ სასამართლოს პრეცედენტული სამართალი სტრატეგიული მონიტორინგის განსახორციელებლად არ მოითხოვს წინასწარ სასამართლო (ან დამოუკიდებელ) ნებართვას მხოლოდ იმ მიზეზით, რომ შესაძლოა ეს პროცესი ჟურნალისტურ მასალასაც შეეხოს. სასამართლო მკვეთრად ასხვავებს ერთ მხრივ, კომუნიკაციების ან/და მასთან დაკავშირებული მონაცემების სტრატეგიულ მონიტორინგს, რაც შესაძლოა განზრახვის გარეშე ცალკეულ ჟურნალისტურ მასალასაც შეეხოს და მეორე მხრივ, მიზნობრივ ღონისძიებებს, რაც უშუალოდ ჟურნალისტურ მასალებს მიემართება. მთავრობის პოზიციით, მასობრივი მიყურადების რეჟიმის კონტექსტში წინასწარი სასამართლო ნებართვა აზრს მოკლებული იყო, რადგან მოსამართლეს აცნობებდნენ მხოლოდ იმ ფაქტს, რომ ორდერის აღსრულება შესაძლოა ცალკეულ კონფიდენციალურ ჟურნალისტურ მასალას შეხებოდა. მთავრობა ეთანხმებოდა პალატის დასკვნას იმის თაობაზე, რომ დამატებითი დაცვის მექანიზმი უზრუნველყოფილი უნდა ყოფილიყო იმ ეტაპზე, როდესაც კომუნიკაცია შესამოწმებლად შეირჩეოდა.

დაზვერვის მონაცემების მიმოცვლასთან დაკავშირებით, მთავრობამ აღნიშნა, რომ ამ რეჟიმს სათანადო საკანონმდებლო საფუძველი ჰქონდა და კანონი ხელმისაწვდომი იყო. კანონმდებლობა ნათლად აღწერდა იმ დანაშაულების ბუნებას, რასთან დაკავშირებითაც დაზვერვის მონაცემების მოპოვება ხორციელდებოდა; ამგვარი მონაცემების მიღების ხანგრძლივობის ლიმიტს; მოპოვებული მონაცემების შესწავლის, გამოყენებისა და შენახვის პროცესს; გარემოებებს, როდესაც მონაცემები უნდა წაიშალოს ან განადგურდეს.

რაც შეეხება საკომუნიკაციო მომსახურების მიმწოდებლებისგან კომუნიკაციების მონაცემების მიღებას, მთავრობას სადავოდ არ გაუხდია ევროპული სასამართლოს პალატის მიგნებები არსებული რეჟიმის კონვენციასთან შეუსაბამობის თაობაზე, შესაბამისად, მისი დასკვნების უარყოფის საფუძველი არ არსებობდა.

სასამართლოს შეფასება

ა. მასობრივი მიყუჩადების ხეჟიმი

სასამართლოში შესული საჩივარი შეეხებოდა დაზვერვის სამსახურების მიერ ტრანსსაზღვრო კომუნიკაციების მასობრივ მიყურადებას. სასამართლო მასობრივ მიყურადებას მიიჩნევს განგრძობად პროცესად, სადაც პირის უფლებაში ჩარევის ხარისხი ამ პროცესის მიმდინარეობასთან ერთად იზრდება. მისი ეტაპები შეიძლება შემდეგნაირად ჩამოყალიბდეს:

01 მიყურადება და კომუნიკაციისა და მასთან დაკავშირებული მონაცემების (ტრაფიკის მონაცემები) შენახვა - ამ ეტაპზე დაზვერვის სამსახურები ახორციელებენ ელექტრონული კომუნიკაციების მასობრივ მიყურადებას, რაც უკავშირდება ადამიანების ფართო ჯგუფს, მათ შორის იმ პირებსაც, რომლებიც დაზვერვის სამსახურებისთვის ინტერესს არ წარმოადგენენ. კომუნიკაციების გარკვეული ნაწილი, შესაძლოა, ამ ეტაპზე გაიფილტროს.

02 შენახული მონაცემების მიმართ სპეციალური სელექტორების გამოყენება - ეს ეტაპი გულისხმობს ძებნას, რაც უმეტესად ავტომატურად ხორციელდება, რომლის დროსაც გამოიყენება სხვადასხვა სახის სელექტორები, მათ შორის „ძლიერი სელექტორები“ (როგორიც არის ელექტრონული ფოსტა).

03 ანალიტიკოსების მიერ შერჩეული კომუნიკაციების/მასთან დაკავშირებული მონაცემების შესწავლა;

04 მონაცემების შემდგომი შენახვა და „საბოლოო პროდუქტის“ გამოყენება, მათ შორის, მესამე პირებისთვის გადაცემა - ამ ეტაპზე დაზვერვის სამსახურები უშუალოდ იყენებენ მოპოვებულ მასალას, კერძოდ, შეიძლება შეიქმნას დაზვერვის ანგარიში, მასალა გაეგზავნოს იმავე ქვეყნის სხვა დაზვერვის სამსახურებს ან უცხო ქვეყნის სამსახურებს.

სასამართლოს თანახმად, კონვენციის მე-8 მუხლი ყველა ზემოაღნიშნულ ეტაპზე ვრცელდება. პირის პირად ცხოვრებასთან დაკავშირებული მონაცემების მხოლოდ შენახვაც კი მე-8 მუხლის მიზნებისთვის, ჩარევას წარმოადგენს. როდესაც მონაცემების ავტომატურ დამუშავებას ეხება საქმე, დაცვის სათანადო გარანტიების არსებობა უფრო მეტ მნიშვნელობას იძენს. აღნიშნულს არ ცვლის ის ფაქტი, რომ შენახული მასალა კოდირებული ფორმით არსებობს, გასაგებია მხოლოდ კომპიუტერული ტექნოლოგიის გამოყენების შემთხვევაში და პირთა შეზღუდულ რაოდენობას შეუძლია მისი გაშიფვრა. საბოლოოდ, პროცესის დასასრულს, როდესაც კონკრეტულ პირთან დაკავშირებული ინფორმაციის ანალიზი ან კომუნიკაციის შინაარსის შესწავლა ხდება, სათანადო გარანტიების არსებობა ყველაზე მნიშვნელოვანია.

სასამართლომ აღნიშნა, რომ სახელმწიფოებს აქვთ ფართო დისკრეცია (მიხედულების ფარგლები) იმის გადასაწყვეტად, რა სახის მეთვალყურეობის სისტემა არის აუცილებელი მათი ეროვნული უსაფრთხოების დასაცავად. თანამედროვე საფრთხეებისა და განვითარებული ტექნოლოგიების გათვალისწინებით, სასამართლომ მასობრივი მიყურადების რეჟიმი ამგვარ მიხედულების ფარგლებს მიაკუთვნა და მიიჩნია, რომ ის თავისთავად არ არღვევდა კონვენციის მე-8 მუხლს.

სასამართლომ ყურადღება გაამახვილა ძველ საქმეებზე *(Weber and Saravia v. Germany; Liberty and Others v. the United Kingdom)* და ხაზი გაუსვა კანონმდებლობით გასათვალისწინებელ იმ 6 მინიმალურ გარანტიას, რაც საკუთარი პრაქტიკით იყო დადგენილი: იმ დანაშაულთა ბუნება, რასთან დაკავშირებითაც შეიძლება გაიცეს ფარული მიყურადების ბრძანება; პირთა იმ კატეგორიის განსაზღვრა, რომელთა სატელეფონო საუბრის მიყურადება შესაძლოა განხორციელდეს; სატელეფონო მიყურადების ხანგრძლივობის შეზღუდვა; მოპოვებული მონაცემების შესწავლის, გამოყენებისა და შენახვის პროცედურა; სხვა პირებისათვის მონაცემების გაზიარებასთან დაკავშირებული სიფრთხილის ზომები; გარემოებები, როდესაც ჩანაწერები შესაძლოა ან უნდა წაიშალოს/განადგურდეს.

სასამართლოს თანახმად, ძველ საქმეებში განხილული მეთვალყურეობის ფარგლები იყო ბევრად ვიწრო. მიუხედავად იმისა, რომ მოცემულ შემთხვევაში, მასობრივი მიყურადების რეჟიმი მსგავსია იმისა, რაც ზემოაღნიშნულ საქმეებში იყო განხილული, ძველი საქმეების განხილვიდან 10 წელზე მეტი გავიდა და ამ პერიოდში ტექნოლოგიურმა პროგრესმა მნიშვნელოვნად შეცვალა ადამიანების კომუნიკაციის გზები.

სასამართლომ აღნიშნა, რომ მოცემულ შემთხვევაში, მასობრივი მიყურადება მიემართება საერთაშორისო კომუნიკაციებს. მიუხედავად იმისა, რომ ქვეყნის შიგნით ადამიანების მეთვალყურეობა და მათი კომუნიკაციების შემოწმება გამორიცხული არ არის, მასობრივი მიყურადების გაცხადებული მიზანი ქვეყნის ტერიტორიული იურისდიქციის მიღმა მყოფი პირების კომუნიკაციების მონიტორინგია, რომლის განხორციელება მეთვალყურეობის სხვა ფორმებით შეუძლებელია.

გარდა ამისა, განსხვავებულია მასობრივი მიყურადების მიზანიც. სასამართლოს ადრინდელ გადაწყვეტილებებში, მიზნობრივი მეთვალყურეობა უმეტეს შემთხვევაში დანაშაულის გამოძიებას უკავშირდებოდა. მასობრივი მეთვალყურეობა შესაძლოა ემსახურებოდეს ცალკეული მძიმე დანაშაულების გამოძიებას, თუმცა ევროპის საბჭოს წევრ ქვეყნებში ის ძირითადად, უცხოური დაზვერვის მონაცემების შესაგროვებლად, კიბერშეტევების ადრეულ ეტაპზე გამოსავლენად და გამოსაძიებლად, ასევე კონტრდაზვერვისა და კონტრტერორისტული მიზნით გამოიყენება.

მიუხედავად იმისა, რომ კონვენციის მე-8 მუხლი ეროვნული უსაფრთხოებისა და სხვა სახელმწიფო ინტერესების დასაცავად არ კრძალავს მასობრივ მიყურადებას და ამ რეჟიმის შერჩევისას ქვეყნები დისკრეციით სარგებლობენ, ამგვარი სისტემის გამოყენებისას სახელმწიფოების მიხედულების ფარგლები ვიწროა და მნიშვნელოვანია სათანადო გარანტიების არსებობა. სასამართლოს თანახმად, თანამედროვე საკომუნიკაციო ტექნოლოგიების განვითარების გათვალისწინებით, აუცილებელია მიზნობრივი მეთვალყურეობის მიმართ არსებული ზოგადი მიდგომის ადაპტირება მასობრივი მიყურადების რეჟიმის კონკრეტული მახასიათებლების შესაბამისად.

სასამართლოს თანახმად, მიზნობრივ მიყურადებასთან დაკავშირებული ზემოაღნიშნული 6 მინიმალური გარანტიიდან პირველი ორი (იმ დანაშაულთა ბუნება, რასთან დაკავშირებითაც

შეიძლება მიყურადების ბრძანება გაიცეს; ირთა იმ კატეგორიის განსაზღვრა, რომელთა მიმართ შესაძლოა ეს ღონისძიება განხორციელდეს) მასობრივი მიყურადების რეჟიმს ნაკლებად მიემართება. აღნიშნულის მსგავსად, გამოძიების კონტექსტში სასამართლოს პრაქტიკით დამკვიდრებული „გონივრული ეჭვის“ მოთხოვნა ნაკლებად რელევანტურია მასობრივი მიყურადების რეჟიმისთვის, რადგან ამ უკანასკნელის მიზანი უფრო პრევენციულია და კონკრეტული დანაშაულის გამოძიებას არ უკავშირდება.

მიუხედავად ამისა, სასამართლო მიიჩნევს, რომ ადგილობრივი კანონმდებლობა უნდა ადგენდეს დეტალურ წესებს, როდის შეიძლება სახელმწიფო ორგანოებმა ამ ზომებს მიმართონ. კერძოდ, ეროვნულ დონეზე პროცესის ყველა ეტაპზე უნდა შეფასდეს მიღებული ზომების აუცილებლობა და პროპორციულობა; მასობრივი მიყურადება დამოუკიდებელი ორგანოს ნებართვას უნდა დაექვემდებაროს დასაწყისშივე, როდესაც ქმედების მიზნისა და ფარგლების განსზღვრა ხდება; ამგვარი ღონისძიებები უნდა დაექვემდებაროს ზედამხედველობასა და შემდგომ (ex post facto) დამოუკიდებელ შემოწმებას.

მასობრივი მიყურადების რეჟიმის კონვენციის სტანდარტებთან შესაბამისობის უზრუნველსაყოფად, სასამართლომ განსაზღვრა ადგილობრივი კანონმდებლობით გასათვალისწინებელი რამდენიმე მნიშვნელოვანი კრიტერიუმი:

01 მასობრივი მიყურადების განსახორციელებლად ნებართვის გაცემის საფუძვლები;

02 გარემოებები, როდესაც პირის კომუნიკაციის მიყურადება შეიძლება განხორციელდეს;

03 ნებართვის გაცემის პროცედურა;

04 მიყურადების მასალის შერჩევის, შემოწმებისა და გამოყენების პროცედურა;

05 მასალის მესამე პირებისათვის გადაცემის დროს მისაღები სიფრთხილის ზომები;

06 მიყურადების ხანგრძლივობისა და მასალის შენახვის ვადები; გარემოებები, როდესაც ეს მასალა უნდა წაიშალოს და განადგურდეს;

07 დამოუკიდებელი ორგანოს მხრიდან ზედამხედველობის პროცედურები და მეთოდები, ასევე ზემოაღნიშნულ გარანტიებთან შეუსაბამობის შემთხვევაში, რეაგირების უფლებამოსილება;

08 ამგვარი შესაბამისობის შემდგომი *(ex post facto)* დამოუკიდებელი შემოწმების პროცედურები და სათანადო ორგანოსთვის მინიჭებული რეაგირების უფლებამოსილება.

სასამართლომ დაადგინა, რომ მოცემულ შემთხვევაში, მასობრივ მიყურადებას ჰქონდა საკანონმდებლო საფუძველი, ასევე ემსახურებოდა შემდეგ ლეგიტიმურ მიზნებს: ეროვნული უსაფრთხოების დაცვა, უწესრიგობისა და დანაშაულის თავიდან აცილება და სხვათა უფლებებისა და თავისუფლების დაცვა. შესაბამისად, სასამართლოს უნდა შეეფასებინა, ეროვნული კანონმდებლობა იყო თუ არა ხელმისაწვდომი და შეიცავდა თუ არა სათანადო ეფექტურ გარანტიებს, რათა დაეკმაყოფილებინა „განჭვრეტადობისა“ და „დემოკრატიულ საზოგადოებაში აუცილებლობის“ მოთხოვნები.

სასამართლომ გაერთიანებული სამეფოს კანონმდებლობა „ხელმისაწვდომად“ მიიჩნია, ხოლო სათანადო ეფექტური გარანტიების დასადგენად ზემოაღნიშნული 8 კრიტერიუმით იხელმძღვანელა. სასამართლოს თანახმად, დიდი ბრიტანეთის მასობრივი მიყურადების რეჟიმი სამი არსებითი ხარვეზით ხასიათდებოდა: მასობრივი მიყურადების ორდერთან დაკავშირებით დამოუკიდებელი ორგანოს მხრიდან ნებართვა არ გაიცემოდა; ორდერის მისაღებ განაცხადში არ უთითებდნენ სელექტორების კატეგორიებს; ინდივიდთან დაკავშირებულ სელექტორთან მიმართებით არ იყო უზრუნველყოფილი წინასწარი შიდა ნებართვა. ეს ხარვეზები შეეხებოდა არა მხოლოდ კომუნიკაციის შინაარსის მიყურადებას, არამედ კომუნიკაციებთან დაკავშირებულ მონაცემებსაც. კომუნიკაციების მიყურადების კომისარი ახორციელებდა არსებული რეჟიმის დამოუკიდებელ და ეფექტურ ზედამხედველობას, ხოლო საგამოძიებო ტრიბუნალი უზრუნველყოფდა სამართლებრივი დაცვის საშუალებას მათთვის, ვისაც დაზვერვის სამსახურების მხრიდან მათი კომუნიკაციის მიყურადების ეჭვი ჰქონდა. მიუხედავად ამისა, სასამართლოს შეფასებით, ეს გარანტიები ზემოთ აღნიშნულ ხარვეზებს ვერ გადაწონიდა.

არსებული ნაკლოვანებები გულისხმობდა იმას, რომ მასობრივი მიყურადების რეჟიმის ფარგლებში, ადამიანების პირად ცხოვრებაში ჩარევა არ იყო „აუცილებელი დემოკრატიულ საზოგადოებაში.“ შესაბამისად, დაირღვა კონვენციის მე-8 მუხლი.

ბ. *დაზვერვის მონაცემების მიღება უცხო ქვეყნის მთავრობისგან ან/და დაზვერვის სამსახურებიდან*

სასამართლოს შეფასებით, კონვენციის არაწევრი სახელმწიფოდან დაზვერვის მონაცემების მოთხოვნასა და მიღებას ცხადი საკანონმდებლო საფუძველი ჰქონდა. ის ემსახურებოდა შემდეგ ლეგიტიმურ მიზნებს: ეროვნული უსაფრთხოების უზრუნველყოფას, უწესრიგობისა და დანაშაულის თავიდან აცილებასა და სხვათა უფლებებისა და თავისუფლების დაცვას. კანონმდებლობა მკაფიოდ არეგულირებდა, რა შემთხვევებში და რა პირობების არსებობისას შეეძლო ხელისუფლებას სხვა ქვეყნიდან მონაცემების მოთხოვნა. მასალის შენახვის, წვდომის, შემოწმებისა და გამოყენების, სხვა პირებისთვის გადაცემის, ასევე წაშლისა და განადგურების პროცედურები იყო საკმარისად ცხადი და უფლებამოსილების ბოროტად გამოყენებისგან დაცვის სათანადო გარანტიებს ქმნიდა.

სასამართლომ ასევე აღნიშნა, რომ კომუნიკაციების მიყურადების კომისარი ახორციელებდა ზედამხედველობას დაზვერვის მონაცემების მიმოცვლის რეჟიმზე. მას ატყობინებდნენ ყველა იმ მოთხოვნის შესახებ, რომელთანაც დაკავშირებითაც ორდერი არ არსებობდა. ის ასევე ზედამხედველობდა ორდერების გაცემას და დაზვერვის სამსახურების მიერ მასალების შენახვას. გარდა ამისა, საგამოძიებო ტრიბუნალი ახორციელებდა დაზვერვის მონაცემების მიმოცვლის რეჟიმზე შემდგომ *(ex post facto)* ზედამხედველობას. ნებისმიერ პირს შეეძლო კონკრეტული ან ზოგადი საჩივრით ამ ტრიბუნალისთვის მიმართვა.

შესაბამისად, სასამართლომ დაადგინა, რომ მასალების მოთხოვნისა და მიღების რეჟიმი კონვენციის მე-8 მუხლს შეესაბამებოდა.

გ. საკომუნიკაციო მომსახურების მიმწოდებლებისგან კომუნიკაციების მონაცემების მიღება

პალატის მიერ საქმის განხილვის ეტაპზე მთავრობამ აღნიშნა, რომ ისინი არსებული სამართლებრივი ჩარჩოს შეცვლის ეტაპზე იყვნენ. საკომუნიკაციო მომსახურების მიმწოდებლების მიერ მონაცემების შენახვის რეჟიმის მარეგულირებელი ახალი კანონმდებლობა ადგილობრივ დონეზე იყო გასაჩივრებული. ამ პროცესის მიმდინარეობისას მთავრობამ დაადასტურა, რომ შესაბამისი ნორმები ევროკავშირის სამართლის მოთხოვნებს არ შეესაბამებოდა. იგივე აღნიშნა ადგილობრივმა სასამართლომაც, რომელმაც მიუთითა, რომ შენახულ მონაცემებზე წვდომა არ იყო „მძიმე დანაშაულის“ აღკვეთის მიზნით შეზღუდული, ასევე არ ექვემდებარებოდა სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მხრიდან წინაწარ შემოწმებას. ევროპული სასამართლოს პალატამ გაითვალისწინა აღნიშნული მსჯელობა და მიუთითა, რომ ახალი, ასევე მისი წინამორბედი რეჟიმი ერთნაირი ხარვეზებით ხასიათდებოდა და ვერ ჩაითვლებოდა კანონის შესაბამისად. შედეგად, სასამართლოს პალატამ კონვენციის მე-8 მუხლის დარღვევა დაადგინა, რაც ასევე გაიზიარა დიდმა პალატამ.

დ. კონვენციის მე-10 მუხლი - გამოხატვის თავისუფლება

სასამართლომ კიდევ ერთხელ ხაზგასმით აღნიშნა, რომ ჟურნალისტური წყაროს დაცვა პრესის თავისუფლების უზრუნველყოფის ძირითადი წინაპირობაა. გაერთიანებული სამეფოს კანონმდებლობით, დაზვერვის სამსახურებს, შესაძლოა, კონფიდენციალურ ჟურნალისტურ მასალაზე წვდომა ჰქონოდათ მიზანმიმართულად, ჟურნალისტთან ან მედია საშუალებასთან დაკავშირებული სელექტორების ან საძიებო ტერმინების გამოყენებით, ან განზრახვის გარეშე, მასობრივი მიყურადების რეჟიმის ოპერირების უნებლიე შედეგის სახით.

სასამართლოს თანახმად, იმის მიუხედავად, დაზვერვის სამსახურის მიზანი არის თუ არა წყაროს იდენტიფიცირება, ჟურნალისტთან დაკავშირებული სელექტორების ან საძიებო ტერმინების გამოყენება, მაღალი ალბათობით, გამოიწვევს დიდი ოდენობით კონფიდენციალური ჟურნალისტური მასალის მოპოვებას, რაც ძირს უთხრის წყაროს დაცულობას. შესაბამისად, სასამართლომ მიიჩნია, რომ დაზვერვის სამსახურების მიერ ჟურნალისტთან დაკავშირებული ან იმგვარი სელექტორების ან საძიებო ტერმინების გამოყენებამდე, რაც მაღალი ალბათობით, კონფიდენციალური ჟურნალისტური მასალის შესამოწმებლად შერჩევას გამოიწვევდა, აუცილებელი იყო მოსამართლის ან სხვა დამოუკიდებელი და მიუკერძოებელი ორგანოს ნებართვა. მოსამართლეს ან შესაბამის ორგანოს უნდა დაედგინა, სელექტორების ან საძიებო ტერმინების გამოყენება გამართლებული იყო თუ არა აღმატებული საჯარო ინტერესით და არსებობდა თუ არა სხვა ნაკლებად ინვაზიური მეთოდის გამოყენების შესაძლებლობა.

გაერთიანებული სამეფოს კანონმდებლობა ზემოაღნიშნულ მოთხოვნებს არ ითვალისწინებდა. გარდა ამისა, სამართლებრივი ჩარჩო არ უზრუნველყოფდა იმას, რომ ის კომუნიკაცია, რომელიც სელექტორის ან საძიებო ტერმინის მეშვეობით შესამოწმებლად არ

შეირჩა და კონფიდენციალურ ჟურნალისტურ მასალას მოიცავდა, მხოლოდ მოსამართლის ან დამოუკიდებელი ორგანოს ნებართვის საფუძველზე შეენახათ და შეემოწმებინათ. ამ ნაკლოვანებების, ასევე მე-8 მუხლთან დაკავშირებით იდენტიფიცირებული ხარვეზების საფუძველზე, სასამართლომ დაადგინა, რომ მასობრივი მიყურადების რეჟიმი ასევე არღვევდა კონვენციის მე-10 მუხლს - გამოხატვის თავისუფლებას.

დაზვერვის მონაცემების მიმოცვლის რეჟიმთან დაკავშირებით სასამართლომ აღნიშნა, რომ ის მე-8 მუხლის ფარგლებში განხილულისგან განსხვავებულ პრობლემურ საკითხს არ წარმოშობდა, შესაბამისად, ამ ნაწილში მე-10 მუხლი არ დარღვეულა.

სასამართლომ მე-10 მუხლის დარღვევა დაადგინა საკომუნიკაციო მომსახურების მიმწოდებლების მიერ მონაცემების შენახვის რეჟიმთან დაკავშირებით იმ საფუძვლით, რომ ამ რეჟიმის ოპერირება კანონის შესაბამისად არ ხორციელდებოდა.

საქმის შედეგი

მასობრივი მიყურადებისა და საკომუნიკაციო მომსახურების მიმწოდებლებისგან მონაცემების მიღების რეჟიმთან დაკავშირებით, სასამართლომ ერთხმად დაადგინა კონვენციის მე-8 (პირადი და ოჯახური ცხოვრების დაცულობის უფლება) და მე-10 (გამოხატვის თავისუფლება) მუხლების დარღვევა. უცხოური დაზვერვის სამსახურებიდან დაზვერვის მონაცემების მიღებასთან დაკავშირებით, სასამართლომ 12 ხმით 5-ის წინააღმდეგ მე-8 და მე-10 მუხლების დარღვევა არ დაადგინა.

სასამართლომ მოპასუხე სახელმწიფოს ერთხმად დააკისრა პირველი მომჩივნისათვის 227,500 ევროს, მეორე მომჩივნისთვის 90,000 ევროს, ხოლო მესამე მომჩივნისთვის 36,000 ევროს გადახდა.

მოსამართლეების ლემენსის, ვეჰაბოვიჩისა და ბოშნიაკის გაერთიანებული ნაწილობრივ თანმხვედრი აზრი

მოსამართლეებმა ლემენსმა, ვეჰაბოვიჩმა და ბოშნიაკმა ნაწილობრივ თანმხვედრ აზრში აღნიშნეს, რომ ამ გადაწყვეტილებით, დიდმა პალატამ ხელიდან გაუშვა არაჩვეულებრივი შესაძლებლობა, რომ სრულად განემტკიცებინა პირადი ცხოვრებისა და კორესპონდენციის დაცულობის უფლება მასობრივი მიყურადების კონტექსტში. სამმა მოსამართლემ ყურადღება გაამახვილა იმ ფაქტზე, რომ მასობრივი მიყურადების პროგრამები პირადი ცხოვრების ხელშეუხებლობის გარდა, სხვა უფლებებსაც ზღუდავს, როგორიც არის სიტყვის თავისუფლება და გაერთიანების თავისუფლება. როდესაც ადამიანებმა იციან, რომ ხელისუფლება მათ მუდმივად უთვალთვალებს, ისინი მეტ სიფრთხილეს იჩენენ მოსაზრებების გამოხატვისას და

ამ უფლებებით სარგებლობისას. აქედან გამომდინარე, სასამართლოს უფრო მეტი წონა უნდა მიენიჭებინა ზოგადად პირადი ცხოვრებისთვის, კონკრეტულად კი კორესპონდენციის კონფიდენციალურობისთვის, როდესაც მოპასუხე სახელმწიფოს ლეგიტიმურ ინტერესებთან მის შეპირისპირებას ახორციელებდა. დიდ პალატას უნდა განესაზღვრა მკაფიო მინიმალური გარანტიები, რაც ადამიანებს თვითნებური და გადამეტებული ჩარევისგან დაიცავდა, ასევე უფრო მკაცრად უნდა შეეფასებინა მასობრივი მიყურადების სქემა.

მოსამართლეების უმრავლესობამ გადაწყვეტილებაში აღნიშნა, რომ მასობრივი მიყურადების სისტემის საწყის ეტაპზე, კომუნიკაციებისა და მასთან დაკავშირებული მონაცემების მიყურადება და თავდაპირველი შენახვა, რასაც კომუნიკაციების ნაწილის მყისიერი წაშლა მოყვებოდა, განსაკუთრებით მნიშვნელოვან ჩარევას არ წარმოადგენდა. სამი მოსამართლე ამ მიდგომას არ დაეთანხმა. მათი მოსაზრებით, ამ ეტაპზეც ჩარევა მნიშვნელოვანია იმიტომ, რომ ნებისმიერი პიროვნების ყველა კომუნიკაცია, რომელიც კონკრეტულ ელექტრონულ მატარებლებში გადაიცემა, ასევე მასთან დაკავშირებული მონაცემები თავს იყრის სახელმწიფო ორგანოების ხელში. მიუხედავად იმისა, რომ ამ ეტაპზე კომუნიკაციების შინაარსის ანალიზი არ ხდება და კონკრეტულ პირთან დაკავშირებით არავითარი ქმედება არ ხორციელდება, პირველი ეტაპი წარმოადგენს ნებისმიერი მომდევნო ეტაპის სავალდებულო წინაპირობას. ვითარებას ამძიმებს ისიც, რომ ხალხმა არ იცის ამგვარი ჩარევის შესახებ. როდესაც ადამიანებმა არ იციან მათი კომუნიკაციები როდის არის დაზვერვის სამსახურების სამიზნე, თუმცა აცნობიერებენ, რომ მაღალი ალბათობით მიყურადება ხორციელდება, მათ შესაძლოა მათი ქცევის ადაპტირება მოახდინონ, რაც მნიშვნელოვან შედეგებს იწვევს.

გადაწყვეტილების თანახმად, კომუნიკაციების ნაწილი მყისიერად იშლება, თუმცა სასამართლო არ ფლობს ინფორმაციას, ეს როგორ ხდება. სავარაუდოდ, ეს შემთხვევითი პრინციპით არ ხდება და დაზვერვის სამსახურები სასარგებლო და უსარგებლო მასალების განცალკევების მიზნით, გარკვეულ კრიტერიუმებს იყენებენ. ის ფაქტი, რომ ეს ბუნდოვნად ხორციელდება, გარკვეულ შეშფოთებას იწვევს. გამჭვირვალობის ამგვარი ნაკლებობა, სულ მცირე, განჭვრეტადობის მოთხოვნას ვერ აკმაყოფილებს, რაც კონვენციის მე-8 მუხლით გარანტირებულ უფლებაში ჩარევის კანონიერების ერთ-ერთი წინაპირობაა. სამწუხაროდ, მოსამართლეების უმრავლესობას ამ ნაკლოვანებაზე ყურადღება არ გაუმახვილებია, რაც თანმხვედრი აზრის ავტორებს გადაწყვეტილების მნიშვნელოვან ხარვეზად მიაჩნიათ.

დიდმა პალატამ განსაზღვრა 8 კრიტერიუმი, რასაც ადგილობრივი კანონმდებლობა უნდა აკმაყოფილებდეს, რათა კონვენციის მე-8 მუხლთან შესაბამისი იყოს. სამი მოსამართლე მიიჩნევს, რომ ეს კრიტერიუმები არგუმენტირებულია და ნამდვილად ემსახურება თვითნებობისა და უფლებამოსილების ბოროტად გამოყენების პრევენციას, თუმცა გარკვეული ხარვეზებითაც ხასიათდება:

ა. ისინი არ წარმოადგენს ცალკე მდგომ მინიმალურ სტანდარტებს, რომელიმე მათგანთან შეუსაბამობა შესაძლოა „გამოსწორდეს“ საერთო შეფასების პროცესში.

ბ. მოითხოვს ცალკეული გარანტიების ცხად განმარტებას ეროვნულ კანონმდებლობაში, მაგრამ თავად არ ადგენს მინიმალურ გარანტიებს.

გ. არ უზრუნველყოფს ინდივიდის არსებით დაცვას არაპროპორციული ჩარევისგან, კერძოდ, შეგროვებული მასალების მიმართ ძლიერი სელექტორების გამოყენების ეტაპზე, ასევე ამ კრიტერიუმებით გარანტირებული პროცედურული დაცვა საკმარისი არ არის.

გაერთიანებული სამეფოს კანონმდებლობით, მასობრივი მიყურადების ორდერი შესაძლოა გაიცეს, როდესაც ეს აუცილებელია: ა) ეროვნული უსაფრთხოების დასაცავად; ბ) მძიმე დანაშაულის თავიდან ასაცილებლად ან გამოსავლენად; გ) გაერთიანებული სამეფოს ეკონომიკური კეთილდღეობის უზრუნველსაყოფად, თუ ეს ინტერესები ეროვნული უსაფრთხოებისთვისაც არის რელევანტური.

სამმა მოსამართლემ ხაზი გაუსვა, რომ ეროვნული უსაფრთხოება და მასთან დაკავშირებული ინტერესები არსად არის განმარტებული. „ეროვნული უსაფრთხოების“ პრაქტიკაში აღქმის შესახებ კომუნიკაციების მიყურადების კომისრის განმარტება განჭვრეტადობის თვალსაზრისით არასაკმარისია. ცხადი განმარტების არარსებობის გათვალისწინებით, ადამიანებს არ შეუძლიათ, თუნდაც კვალიფიციური რჩევის საფუძველზე განსაზღვრონ, რა საფუძვლით შეუძლიათ დაზვერვის სამსახურებს მათი კომუნიკაციების მიყურადება და გაანალიზება.

მეორე მიზანი - სერიოზული დანაშაულის თავიდან აცილება და გამოვლენა - ზემოაღნიშნული ხარვეზებით არ ხასიათდება. მძიმე დანაშაულად ითვლება დანაშაული, რომელიც სასჯელის სახით ითვალისწინებს პატიმრობას 3 ან მეტი წლის ვადით ან ქმედება არის ძალადობრივი, უკავშირდება მნიშვნელოვანი ფინანსური სარგებლის მიღებას ან ჩადენილია ადამიანთა ჯგუფის მიერ საერთო მიზნის მისაღწევად. ამგვარი განმარტება ქმედებათა ფართო სპექტრს მოიცავს, რაც მის პროპორციულობასთან დაკავშირებით ეჭვებს აჩენს.

გარდა ამისა, დემოკრატიულ საზოგადოებაში დაზვერვის სამსახურებს არ უნდა ჰქონდეთ დანაშაულის აღკვეთის უფლებამოსილება, გარდა იმ შემთხვევისა, როდესაც დანაშაულებრივი საქმიანობა ეროვნულ უსაფრთხოებას უქმნის საფრთხეს. მთავრობის განმარტება იმის თაობაზე, რომ მასობრივი მიყურადების შედეგად მოპოვებული ინფორმაცია არ გამოიყენება სისხლისსამართლებრივი დევნისთვის, დამაჯერებელი არ იყო. მოპოვებული ინფორმაციის საფუძველზე, სამართალდამცავ ორგანოებს შეუძლიათ საგამოძიებო მოქმედებების განხორციელება ან პირების დაკავება, შესაბამისად, სისხლისსამართლებრივი დევნისთვის მტკიცებულებების მოპოვება. საბოლოოდ, სამი მოსამართლის შეფასებით, ადვილად შესაძლებელია, არცთუ შორეულ მომავალში დანაშაულის გამოძიებამ მიზნობრივი მეთვალყურეობიდან მასობრივი მიყურადებისკენ გადაინაცვლოს.

მოსამართლე პინტო დე ალბუქერქეს ნაწილობრივ თანმხვედრი და ნაწილობრივ განსხვავებული აზრი

მოსამართლე პინტო დე ალბუქერქე არ დაეთანხმა უმრავლესობის მოსაზრებას იმის თაობაზე, რომ დაზვერვის მონაცემების მიმოცვლის რეჟიმი მე-8 და მე-10 მუხლებს არ არღვევდა. გადაწყვეტილების მიხედვით, უცხოური დაზვერვის სამსახურებისთვის მასობრივი მიყურადების შედეგად მიღებული ინფორმაციის გადაცემა „დამოუკიდებელ კონტროლს“ უნდა დაექვემდებაროს, ხოლო უცხოური დაზვერვის სამსახურიდან მიღებული მასალები - არა. თუკი პირდაპირ მეთვალყურეობასთან დაკავშირებით გაერთიანებული სამეფოს მიერ უზრუნველყოფილი გარანტიები საკმარისი არ არის, ის არასაკმარისად უნდა ჩაითვალოს არაპირდაპირი მეთვალყურეობის შემთხვევაშიც, რაც გულისხმობს მესამე მხარის მიერ მოპოვებული დაზვერვის მასალების მიღებას, განსაკუთრებით მაშინ, როდესაც ეს მხარე არ არის კონვენციის მონაწილე.

როდესაც მაღალია რისკი იმისა, რომ მონაცემების შეგროვება და შენახვა კონვენციის მოთხოვნებს არ შეესაბამება და დამოუკიდებელი ზედამხედველობა ყველაზე მეტად საჭიროა, სასამართლომ უარი თქვა ამ გარანტიაზე ყოველგვარი დამაჯერებელი დასაბუთების გარეშე. კომუნიკაციების მიყურადების კომისრისა და საგამოძიებო ტრიბუნალის მხრიდან ზედამხედველობა არაეფექტურია მესამე მხარის მიერ მოპოვებული დაზვერვის მასალების მიმოცვლის კუთხით, რადგან ტრიბუნალი მხოლოდ საჩივრის არსებობის შემთხვევაში რეაგირებს, ხოლო კომისრის უფლებამოსილება მხოლოდ პრემიერ მინისტრისათვის ანგარიშის წარდგენით შემოიფარგლება, რათა მძიმე გადაცდომის შესახებ ინფორმაცია მიაწოდოს.

მოსამართლე ალბუქერქეს მაგალითად მოჰყავს იმგვარი შემთხვევა, როდესაც ლონდონში მცხოვრები პირი უგზავნის შეტყობინებას მეორეს, რომელიც ასევე ლონდონში იმყოფება და ეს კომუნიკაცია აშშ-ს სერვერის მეშვეობით გადაიცემა. სასამართლოს მსჯელობის თანახმად, გაერთიანებული სამეფოს მიერ ამ კომუნიკაციის მიყურადება დამოუკიდებელ ნებართვას საჭიროებს. თუმცა, როდესაც იმავე შეტყობინებას ეროვნული უსაფრთხოების სააგენტო აყურადებს და ასლს გაერთიანებულ სამეფოს უგზავნის, დამოუკიდებელ ნებართვასთან დაკავშირებული გარანტია არ მოქმედებს. მოსამართლის შეფასებით, სამართლებრივი დაცვის განსხვავებული რეჟიმი ერთი და იმავე მონაცემების მიმართ გაუმართლებელია და არ უნდა იყოს დამოკიდებული მხოლოდ იმ ფაქტზე, ვინ განახორციელა თავდაპირველი მიყურადება. შესაბამისად, გაერთიანებული სამეფოს კანონმდებლობა არ არის საკმარისი თვითნებობისა და უფლებამოსილების ბოროტად გამოყენების თავიდან ასაცილებლად.

ალბუქერქე ასევე არ დაეთანხმა უმრავლესობის დასაბუთებას მე-8 და მე-10 მუხლების დარღვევის ნაწილში. მოსამართლის თანახმად, არამიზანმიმართული, მასობრივი მიყურადება აკრძალულია 23 ევროპულ ქვეყანაში. ამასთან, PACE-მა და ევროპის საბჭოს ადამიანის უფლებების კომისარმა აჩვენეს, რომ კომუნიკაციების მასობრივი მეთვალყურეობა არაეფექტურია ტერორიზმის თავიდან ასაცილებლად, საფრთხეს უქმნის ადამიანის უფლებებს და წარმოადგენს რესურსების ფლანგვას.შესაბამისად, თუკი ევროპაში არსებობს კონსენსუსი მასობრივ მიყურადებასთან დაკავშირებით, ეს კონსენსუსი არის იმის თაობაზე, რომ ის უნდა

აიკრძალოს, რაზეც სასამართლოს ყურადღება არ გაუმახვილებია. ევროპის საბჭოს წევრი მხოლოდ 7 ქვეყანა იყენებს ამგვარ რეჟიმს, რაც ძირითადად ისეთი დანაშაულების თავიდან აცილებას, გამოვლენას და გამოძიებას ემსახურება, როგორიც არის ტერორიზმი, ჯაშუშობა, კიბერ შეტევები და სხვა „მძიმე დანაშაულები“.

ალბუქერქეს თანახმად, თუკი სახელმწიფოს დისკრეცია ფართოა, ყველაზე მკაცრი კონტროლიც კი არასაკმარისი გარანტიაა უფლებამოსილების ბოროტად გამოყენებისგან დასაცავად. სახელმწიფოს მიხედულების ფარგლები ერთნაირი უნდა იყოს ორივე შემთხვევაში: სისტემის შექმნისა და ფუნქციონერების ეტაპზე. მეთვალყურეობის ინვაზიური ბუნებიდან და ამ უფლებამოსილების ბოროტად გამოყენების მაღალი რისკის გათვალისწინებით, ეს ფარგლები ვიწრო უნდა იყოს.

ალბუქერქეს აზრით, არ არსებობს ბრიტანეთის ფარგლებს გარეთ მყოფი ადამიანების მიმართ განსხვავებული მოპყრობის ობიექტური გამართლება, გარდა იმ დაშვებისა, რომ საფრთხე უფრო ხშირად საზღვარგარეთიდან მომდინარეობს და კონკრეტული ქვეყნის მოქალაქეებთან შედარებით, უცხოელები ნაკლები ნდობით სარგებლობენ. ეს ასევე ვლინდება უცხოელების მიერ თავიანთი უფლების დაცვის ნაწილშიც. საგამოძიებო ტრიბუნალი საჩივრებს არ იღებს მომჩივნებისგან, რომლებიც გაერთიანებული სამეფოს ტერიტორიის მიღმა არიან. უცხოელებისადმი ამგვარი მიდგომა კონვენციის სულისკვეთებას ეწინააღმდეგება. კონვენციის ცენტრში არის ინდივიდი და არა ქვეყნის მოქალაქე, რაც გულისხმობს იმას, რომ კონვენციით გარანტირებულმა უფლებებმა ადამიანების დაცვა უნდა უზრუნველყოს იმის მიუხედავად, სახელმწიფო სად, ვის მიმართ და რა სახით მოქმედებს.

სისტემის რეგულირებასთან დაკავშირებულ ხარვეზს ასევე ამწვავებს კომუნიკაციების მიყურადების კომისრის სტატუსი, რომელიც დამოუკიდებელი ორგანო არ არის და ეფექტურ ზედამხედველობას ვერ ახორციელებს. კომისარს ნიშნავს პრემიერ-მინისტრი, ანგარიშვალდებულია მის წინაშე და დამოკიდებულია სახელმწიფო მდივნის მიერ განსაზღვრულ თანამშრომლებზე. გარდა ამისა, ეს იყო ნახევარ განაკვეთიანი სამუშაო და კომისარი პრემიერ-მინისტრს შესაძლოა ნებისმიერ დროს გაეთავისუფლებინა. ამგვარი სტატუსი შეუთავსებელია დამოუკიდებლობის იმ ხარისხთან, რაც აუცილებელია ეფექტური ზედამხედველობისთვის. უფრო კონკრეტულად, კომისარი არ არის ინსტიტუციურად, ფუნქციურად და ფინანსურად დამოუკიდებელი იმ ინსტიტუტებისგან, რომელსაც ზედამხედველობს.

იმ შემთხვევაშიც კი, თუ დავუშვებთ, რომ კომისარი დამოუკიდებელია, ის არ არის ეფექტური, რადგან მძიმე გადაცდომის შემთხვევაში, მას შეუძლია მხოლოდ ანგარიშის წარდგენა პრემიერ-მინისტრისათვის. მას არ შეუძლია საქმე ტრიბუნალს წარუდგინოს ან მსხვერპლს გადამეტებული მიყურადების შესახებ აცნობოს.

გარდა ამისა, მიყურადების პროცესის ბოლოს არ არსებობს შეტყობინების ვალდებულება. ამგვარი შეტყობინების არარსებობისას, სასამართლოსთვის მიმართვა უშედეგოა. საგამოძიებო ტრიბუნალი რეაგირებს მხოლოდ იმ პირების საჩივრებზე, ვინც მიიჩნევს, რომ მათ მიმართ ფარული მიყურადება განხორციელდა. შესაბამისად, ტრიბუნალი არის მხოლოდ თეორიული გარანტია იმ სუბიექტებისთვის, რომლებმაც არც იციან, რომ მათი მიყურადება

განხორციელდა. გარდა ამისა, საგამოძიებო ტრიბუნალის გადაწყვეტილებები გასაჩივრებას არ ექვემდებარება. სახელმწიფო მდივანი უფლებამოსილია, მიიღოს საგამოძიებო ტრიბუნალის პროცედურული წესები, რაც პრაქტიკულად გულისხმობს იმას, რომ ის ორგანო, რომლის ზედამხედველობაც ხორციელდება, განსაზღვრავს იმ წესებს, რაც საზედამხედველო ორგანოს საქმიანობას არეგულირებს.

გადაწყვეტილება მნიშვნელოვნად ცვლის ბალანსს პირადი ცხოვრების პატივისცემის უფლებასა და ეროვნული უსაფრთხოების ინტერესს შორის, რადგან ის უშვებს ელექტრონული კომუნიკაციების შინაარსისა და მასთან დაკავშირებული მონაცემების მასობრივ მიყურადებას, უფრო მეტიც, ინფორმაციის მიმოცვლას იმ ქვეყნებთან, რომლებიც არ უზრუნველყოფენ მონაცემების დაცვას იმავე სტანდარტით, როგორც ევროპის საბჭოს წევრი ქვეყნები. მოსამართლე ალბუქერქეს დასკვნით, ამ გადაწყვეტილებით სტრასბურგის სასამართლომ გზა გაუხსნა ელექტრონულ „დიდ ძმას“ ევროპაში.

მოსამართლეების ლემენსის, ვეჰაბოვიჩის, რანზონისა და ბოშნიაკის გაერთიანებული ნაწილობრივ განსხვავებული აზრი

მოსამართლეებმა ლემენსმა, ვეჰაბოვიჩმა, რანზონმა და ბოშნიაკმა არ გაიზიარეს უმრავლესობის მოსაზრება იმასთან დაკავშირებით, რომ დაზვერვის მონაცემების მიმოცვლის რეჟიმი კონვენციის მე-8 და მე-10 მუხლებს არ არღვევდა.

მიყურადების პროცესში უფლებამოსილების ბოროტად გამოყენების თავიდან ასაცილებლად, სასამართლომ სამი ძირითადი გარანტია განსაზღვრა: 1) აღმასრულებელი ხელისუფლებისგან დამოუკიდებელი ორგანოს მიერ მასობრივი მიყურადების ნებართვის გაცემა დასაწყისშივე; 2) წინასწარი შიდა ნებართვა იდენტიფიცირებად პირებთან დაკავშირებული ძლიერი სელექტორების გამოყენებისას; 3) დამოუკიდებელი ორგანოს მხრიდან ზედამხედველობა და ეფექტური შემდგომი *(ex post facto)* კონტროლი.

ოთხი მოსამართლის აზრით, მასობრივ მიყურადებასთან დაკავშირებული ზემოაღნიშნული გარანტიები უნდა გავრცელდეს იმ შემთხვევებზეც, როდესაც სახელმწიფო თავად არ ახორციელებს მიყურადებას, თუმცა უცხოურ დაზვერვის სამსახურებს სთხოვს მიყურადებას ან უკვე მოპოვებული მონაცემების გადაცემას. მიუხედავად იმისა, რომ მასალების მიღების შემდეგ, შემოწმებასთან, გამოყენებასთან, შენახვასთან, შემდგომ გადაცემასთან, წაშლასა და განადგურებასთან დაკავშირებული გარანტიები თანაბრად მოქმედებს, პირველ ეტაპზე დამოუკიდებელი ორგანოს მხრიდან ნებართვის გაცემის აუცილებლობა სრულიად გამქრალია მოსამართლეთა უმრავლესობის მიდგომაში. ოთხი მოსამართლის აზრით, ანალოგიური გარანტიები უნდა გავრცელდეს პირველივე ეტაპზეც - მონაცემების უცხო ქვეყნიდან მიღებისას.

მოსამართლეთა უმრავლესობა აპელირებდა იმაზე, რომ ინფორმაციის გადაცემის მოთხოვნა ეფუძნებოდა სახელმწიფო მდივნის მიერ გაცემულ ან დადასტურებულ ორდერს. ოთხი მოსამართლის აზრით, სახელმწიფო მდივანი არ არის „დამოუკიდებელი ორგანო“, შესაბამისად, ორდერს გასცემდა „დაინტერესებული მხარე“, რაც მათი შეხედულებით, ხელშემკვრელი მხარის მიერ საერთაშორისო ვალდებულების დარღვევა იყო.

BREYER V. GERMANY

30/01/2020

ფაქტობრივი გარემოებები

გერმანიის ორმა მოქალაქემ, პატრიკ და იონას ბრეიერებმა (შემდგომ „მომჩივნები“) ადამიანის უფლებათა ევროპულ სასამართლოს (შემდგომ „სასამართლო“) მიმართეს იმ საფუძვლით, რომ ტელეკომუნიკაციების კანონის დებულებები არღვევდა მათ პირადი და ოჯახური ცხოვრების პატივისცემის უფლებას, რომელიც ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის (შემდგომ „კონვენცია“) მე-8 მუხლით არის გათვალისწინებული.

2004 წლის ივნისში, გერმანიამ სატელეკომუნიკაციო მომსახურების მიმწოდებლებისათვის შემოიღო სამართლებრივი ვალდებულება, შეეგროვებინათ და შეენახათ თავიანთი მომხმარებლების პირადი მონაცემები, მათ შორის, იმ მომხმარებლების, რომელთა მონაცემები გადასახადის დარიცხვის ან სხვა სახელშეკრულებო მიზნებისთვის საჭირო არ იყო. ამ ცვლილების განხორციელებამდე, მიმწოდებლები უფლებამოსილი იყვნენ, შეეგროვებინათ და შეენახათ მხოლოდ ის მონაცემები, რაც აუცილებელი გახლდათ სახელშეკრულებო ურთიერთობისთვის. წინასწარი გადახდის სიმ-ბარათებთან დაკავშირებით კი ამგვარი მონაცემები საჭირო არ იყო.

ტელეკომუნიკაციების კანონის 111-ე მუხლი სიმ-ბარათის გააქტიურებამდე მოითხოვს მომხმარებლის ტელეფონის ნომრის, სახელის, მისამართის, დაბადების თარიღის, ხელშეკრულების მოქმედების ვადის და (ზოგიერთ შემთხვევაში) მოწყობილობის ნომრის დარეგისტრირებას. 112-ე და 113-ე მუხლების თანახმად, სატელეკომუნიკაციო მომსახურების მიმწოდებლებმა 111-ე მუხლის საფუძველზე შეგროვებული მონაცემები მომხმარებლის მონაცემთა ფაილებში უნდა შეინახონ და უზრუნველყონ ქსელების ფედერალური სააგენტოს მიერ ნებისმიერ დროს მონაცემების ავტომატიზებული მიღების შესაძლებლობა.

2005 წლის 13 ივლისს, მომჩივნებმა ტელეკომუნიკაციების კანონის ზემოაღნიშნული მუხლები საკონსტიტუციო სასამართლოში გაასაჩივრეს. გერმანიის ფედერალურმა საკონსტიტუციო სასამართლომ აღნიშნა, რომ გასაჩივრებული დებულებები ინფორმაციული თვითგამორკვევის უფლებაში ჩარევას წარმოადგენდა, რაც „პრინციპის დონეზე უზრუნველყოფს პიროვნების უფლებამოსილებას, თავად გადაწყვიტოს თავისი პერსონალური მონაცემების გამჟღავნებისა და გამოყენების საკითხი“. სასამართლომ მიიჩნია, რომ ქვემოთ მოცემული თითოეული საკითხი დამოუკიდებლად ხელყოფდა ინფორმაციული თვითგამორკვევის უფლებას: მონაცემთა შეგროვება და შენახვა, ცენტრალიზებულ ბაზაში მონაცემთა ხელმისაწვდომობის ვალდებულება, ქსელების ფედერალური სააგენტოს უფლებამოსილება, მოეპოვებინა და გადაეცა მონაცემები შესაბამისი უწყებისათვის და უფლებამოსილი უწყებების მიერ წინასწარი მოთხოვნის გაკეთების შესაძლებლობა.

111-ე მუხლთან დაკავშირებით სასამართლომ აღნიშნა, რომ მონაცემთა ბაზის შექმნა სისხლისსამართლებრივი დევნის განხორციელების ლეგიტიმურ მიზანს ემსახურებოდა და შედარებით შეზღუდული ხასიათის გამო გამართლებული იყო. შენახული მონაცემები ასრულებდა მხოლოდ სატელეკომუნიკაციო ნომრების რეესტრის ფუნქციას და ინდივიდების კონკრეტულ ქმედებებს არ ააშკარავებდა.

მსჯელობისას სასამართლომ განმარტა, რომ ტელეკომუნიკაციების კანონის 112-ე მუხლი აღებს მონაცემთა გადაცემის კარს, თუმცა ამით სპეციალიზებული ორგანოებისთვის არ იხსნება მონაცემთა შეგროვების კარი. მოქმედებს ე.წ. „ორმაგი კარის პრინციპი“. სასამართლომ მიუთითა, რომ 112-ე მუხლი ბევრად ამარტივებდა მონაცემების მოპოვებას და, შესაბამისად, ჩარევა უფრო მძიმე ხასიათის იყო. თუმცა, ფედერალური საკონსტიტუციო სასამართლო გადაწყვეტილებაში აღნიშნავს, რომ ინფორმაციის შინაარსი შეზღუდული რჩება და დამოკიდებულია შემდგომ გამოძიებაზე, რომლის კანონიერება უნდა შეფასდეს სხვადასხვა დებულებით. ამასთან, მონაცემთა გადაცემის მიზნები უკავშირდება უსაფრთხოების უზრუნველყოფას და შესაბამისი საგამოძიებო ღონისძიებები უნდა ჩატარდეს სწრაფად და დაზარალებულთა ცოდნის გარეშე, შესაბამისად, ჩარევა არის პროპორციული.

113-ე მუხლის შეფასების კონტექსტში, სასამართლომ განმარტა, რომ ეს დებულება ინდივიდუალურ საქმეში ყოველთვის იძლევა ინფორმაციის მიღების შესაძლებლობას, თუ ეს აუცილებელია ზემოაღნიშნული მოვალეობების შესასრულებლად.

მიუხედავად ამისა, სასამართლომ მიუთითა, რომ მონაცემების მოპოვებისთვის საჭირო იყო დამატებითი სამართლებრივი საფუძველი (დაცვის გარანტია) და მნიშვნელოვანი იყო უწყებების სამსახურებრივი მოვალეობების ეფექტურად შესრულება. სასამართლომ ასევე გაითვალისწინა ინფორმაციის შეზღუდული შინაარსი და დაადგინა, რომ სადავო ნორმები კონსტიტუციას არ ეწინააღმდეგებოდა.

მომჩივნების არგუმენტაცია

მომჩივნების პოზიციით, ტელეკომუნიკაციების კანონის 111-ე მუხლით მათ პირად ცხოვრებაში ჩარევა ხდებოდა, რამდენადაც ის მათ აიძულებდა გაემჟღავნებინათ თავიანთი პერსონალური მონაცემები, რაც შემდგომ ინახებოდა.

მათი მოსაზრებით, ამგვარი ჩარევა არ იყო პროპორციული და აუცილებელი დემოკრატიულ საზოგადოებაში. ეს ნორმა არ წარმოადგენდა შესაფერის ინსტრუმენტს, რადგან მარტივად იყო შესაძლებელი არასწორი სახელით, ასევე, მოპარული, მეორადი ან უცხო ქვეყნის სიმ-ბარათების გამოყენებით, იდენტიფიკაციის გვერდის ავლა. ჩარევა არ იყო აუცილებელი, რადგან საეჭვო მომხმარებლების იდენტიფიცირება სხვა საგამოძიებო ღონისძიებებით შეიძლებოდა. საბოლოოდ, ტელეკომუნიკაციების კანონის 111-ე მუხლის სადავო ცვლილებას დანაშაულის ოდენობის შემცირება არ გამოუწვევია.

მომჩივნების აზრით, ჩარევა მძიმე ხასიათის იყო, რამდენადაც ყველა იმ პირის პერსონალური მონაცემების წინასწარ მასობრივ შენახვას გულისხმობდა, ვინც ტელეკომუნიკაციებს იყენებდა. კანონის ეს ნორმა მონაცემთა შენახვისთვის არანაირ წინაპირობას არ ითვალისწინებდა და ზოგადად ყველა მობილური ტელეფონის მომხმარებელზე ვრცელდებოდა. იმ პირთა უმრავლესობა, ვისაც ეს ჩანაწერი შეეხებოდა, უდანაშაულო იყო და სახელმწიფო უსაფრთხოებისთვის საფრთხეს/რისკს არ წარმოადგენდა. უფრო მეტიც, ნორმა არ განასხვავებდა „ჩვეულებრივ" კომუნიკაციასა და კომუნიკაციას, რომელიც განსაკუთრებულად იყო დაცული კონვენციით, მაგალითად, ადვოკატისა და მისი კლიენტის ან ექიმისა და პაციენტის კომუნიკაციას. გარდა ამისა, მონაცემთა შენახვამ გაზარდა მონაცემთა გაჟონვისა და მათი ბოროტად გამოყენების, შესაბამისად, იდენტობის გაყალბების/მითვისების რისკი.

მთავრობის არგუმენტაცია

მთავრობამ დაადასტურა, რომ 111-ე მუხლი სერვისის მიმწოდებლებს ავალდებულებდა, შეენახათ მომხმარებლების პერსონალური მონაცემები, რაც მომჩივნების პირად ცხოვრებაში ჩარევას წარმოადგენდა. მთავრობის განმარტებით, ამ პროცესში არ მიმდინარეობდა ტრაფიკის მონაცემების შეგროვება, (რომელიც, თავის მხრივ, კომუნიკაციის პროცესში წარმოიქმნება) ინახებოდა მხოლოდ აბონენტების მონაცემები. ამასთან, მთავრობის მოსაზრებით, 111-ე მუხლი უნდა განიმარტოს ტელეკომუნიკაციების კანონის 112-ე და 113-ე მუხლებთან და იმ სხვა მზღუდავ დებულებებთან ურთიერთკავშირში, რომლებიც შენახულ მონაცემებზე წვდომას არეგულირებენ.

არგუმენტაციაში ნათქვამია, რომ ეს შეზღუდული ჩარევა საზოგადოებრივი უსაფრთხოების, დანაშაულის ან უწესრიგობის თავიდან აცილების და სხვების უფლებებისა და თავისუფლებების დაცვის ლეგიტიმურ მიზანს ემსახურებოდა და ამ მიზნის მიღწევის შესაფერისი ინსტრუმენტი იყო, რამდენადაც ის უსაფრთხოების ორგანოებს შესაძლებლობას აძლევდა, წინასწარ გადახდილი (pre-paid) სიმ-ბარათების მობილური ტელეფონის ნომრები კონკრეტულ პირებთან დაეკავშირებინათ.

მთავრობის შეხედულებით, ეს შესაძლებლობა ხელს უწყობდა კანონის ეფექტურად აღსრულებას და ემსახურებოდა საფრთხის თავიდან აცილებას. სადავო ნორმა ასევე შეესაბამებოდა სასამართლოს მიერ *S. and Marper v. the United Kingdom* საქმეზე პრაქტიკით დადგენილ მოთხოვნებს: მონაცემთა შენახვის ვადა მკაფიოდ იყო განსაზღვრული და არ აღემატებოდა მიზნის მისაღწევად აუცილებელ პერიოდს. გარდა ამისა, 112-ე და 113-ე მუხლები, ტელეკომუნიკაციების კანონის სპეციალურ დებულებებთან ერთად, ბოროტად გამოყენებისგან დაცვის ეფექტურ საშუალებებს წარმოადგენდა.

ისიც გასათვალისწინებელია, რომ სახელმწიფოებისთვის მინიჭებული მიხედულების ფარგლები იყო საკმაოდ ფართო არა მხოლოდ იმიტომ, რომ გერმანიის უწყებებს სათანადო ბალანსი უნდა დაეცვათ დაპირისპირებულ უფლებებსა და ინტერესებს შორის, არამედ იმიტომ, რომ ევროპულ სახელმწიფოთა შორის არ არსებობდა კონსენსუსი მობილური ტელეფონის წინასწარ გადახდილი სიმ-ბარათების შეძენისას მონაცემების შენახვის ვალდებულებასთან დაკავშირებით. დასკვნის სახით, მინიმალური ოდენობის მონაცემების შენახვა, რომელთა დაცვის სათანადო გარანტიები უზრუნველყოფილი იყო, წარმოადგენდა პროპორციულ საშუალებას საზოგადოების უსაფრთხოების დაცვისა და დანაშაულისა და უწესრიგობის პრევენციისთვის.

მესამე მხარეთა მოსაზრებები

ორგანიზაციებმა Privacy International-მა და ARTICLE 19-მა ხაზი გაუსვეს დემოკრატიულ საზოგადოებაში ანონიმურობისა და ანონიმური საუბრის, მოქალაქეთა პირადი ცხოვრების პატივისცემის უფლებისა და გამოხატვის თავისუფლების მნიშვნელობას. ეს ფუნდამენტური როლი სულ უფრო და უფრო აღიარებულია ეროვნული სასამართლოებისა და საერთაშორისო ორგანიზაციების მიერ, მაგალითად, როგორიც არის გაერთიანებული ერების ორგანიზაცია და ევროპის საბჭო. გარდა ამისა, თავად სასამართლომ დაადასტურა ანონიმურობის მნიშვნელობა გადაწყვეტილებაში *Delfi AS v. Estonia.* მათ აღნიშნეს, რომ ევროპული სასამართლოები სულ უფრო ხშირად აღიარებენ, რომ მაიდენტიფიცირებელი ინფორმაციისა და ტრაფიკის მონაცემების ბლანკეტურად და განურჩევლად შენახვა არის არაპროპორციული საშუალება მძიმე დანაშაულის წინააღმდეგ ბრძოლის მიზნებისთვის. აღნიშნულს ადასტურებს ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება საქმეზე *Digital Rights Ireland and Seitlinger and Others.*

სასამართლოს შეფასება

სასამართლომ აღნიშნა, რომ ეროვნული უსაფრთხოების ინტერესსა და პირადი ცხოვრების პატივისცემის უფლებას შორის ბალანსის დაცვისას სახელმწიფოები გარკვეული მიხედულების ფარგლებით სარგებლობენ და შეუძლიათ ლეგიტიმური მიზნის მისაღწევად სათანადო საშუალება აირჩიონ. თუმცა, ეს ფარგლები განსხვავებულია და რამდენიმე ფაქტორზეა დამოკიდებული, მაგალითად, კონვენციის შესაბამისი მუხლის ბუნებაზე, მის მნიშვნელობაზე,

ჩარევის ხასიათსა და მისაღწევ მიზანზე. მიხედულების ფარგლები ვიწროა მაშინ, როდესაც რისკის ქვეშ დგება ადამიანის ინტიმურ სფეროსთან დაკავშირებული ან სხვა არსებითი უფლებით ეფექტური სარგებლობა. იმ შემთხვევაში, როდესაც ევროპის საბჭოს წევრ ქვეყნებში არ არსებობს კონსენსუსი კონკრეტული ინტერესის შეფარდებით მნიშვნელობას ან მისი დაცვის საუკეთესო საშუალებასთან დაკავშირებით, მიხედულების ფარგლები უფრო ფართოა.

მხარეები სადავოდ არ ხდიან იმ გარემოებას, რომ ტელეკომუნიკაციების კანონის 111-ე მუხლის საფუძველზე, მომსახურების მიმწოდებლების მიერ მონაცემთა შენახვა მომჩივნების პირად ცხოვრებაში ჩარევას წარმოადგენს. სასამართლომ კიდევ ერთხელ განმარტა, რომ იმ მონაცემების უბრალო შენახვა, რომელიც ინდივიდის პირად ცხოვრებას ეხება, კონვენციის მე-8 მუხლით გათვალისწინებული ჩარევაა.

სასამართლოს განმარტებით, ადამიანის პირად ცხოვრებაში ჩარევა მე-8 მუხლის დარღვევად არ ჩაითვლება, თუ ის ხორციელდება კანონის შესაბამისად, ემსახურება ერთ ან მეტ ლეგიტიმურ მიზანს და აუცილებელია დემოკრატიულ საზოგადოებაში ამ მიზნის მისაღწევად.

სასამართლოს პრაქტიკის თანახმად, კანონთან შესაბამისობის კრიტერიუმი მხოლოდ საკანონმდებლო საფუძვლის არსებობას არ გულისხმობს. აუცილებელია, კანონი იყოს ხელმისაწვდომი და განჭვრეტადი. უნდა არსებობდეს მონაცემთა შენახვის, გამოყენების, მესამე პირთა მიერ წვდომის, მონაცემთა მთლიანობისა და კონფიდენციალურობის დაცვის მარეგულირებელი მკაფიო, გასაგები და დეტალური წესები/პროცედურები, რომელიც დაცვის მინიმალურ გარანტიებს აწესებს.

სასამართლოს შეფასებით, ტელეკომუნიკაციების კანონის 111-ე მუხლი იყო საკმარისად ცხადი და განჭვრეტადი, დადგენილი გახლდათ მონაცემთა შენახვის ხანგრძლივობაც. ამასთან, მონაცემთა შენახვის ტექნიკური მხარე შესაბამისი რეგულაციისა და ტექნიკური დირექტივის გამოქვეყნების შემდეგ, მკაფიოდ განსაზღვრული იყო.

რაც შეეხება დაცვის გარანტიებსა და მესამე პირთა მიერ მონაცემებზე წვდომას, სასამართლომ აღნიშნა, რომ 111-ე მუხლი უნდა განიმარტოს 112-ე და 113-ე მუხლებთან ურთიერთკავშირში, ფედერალური საკონსტიტუციო სასამართლოს მიერ ჩამოყალიბებული „ორმაგი კარის კონცეფციის“ შესაბამისად. სასამართლომ მიიჩნია, რომ განჭვრეტადობისა და საკმარისი დეტალურობის საკითხი დაკავშირებული იყო უფრო ფართო თემასთან - იყო თუ არა ჩარევა აუცილებელი და პროპორციული დემოკრატიულ საზოგადოებაში.

სასამართლო დაეთანხმა მთავრობის არგუმენტს, რომ ჩარევა ემსახურებოდა საზოგადოებრივი უსაფრთხოების დაცვის, უწესრიგობის ან დანაშაულის თავიდან აცილების და სხვათა უფლებებისა და თავისუფლებების დაცვის ლეგიტიმურ მიზანს. ეს მიზნები კიდევ უფრო გამოკვეთილია ტელეკომუნიკაციების კანონით, რომელიც აცხადებს, რომ ინფორმაციის გამოთხოვა დასაშვებია მაშინ, როდესაც ის აუცილებელია დამნაშავეთა სისხლის სამართლის პასუხისგებაში მისაცემად, საფრთხის თავიდან ასაცილებლად და სადაზვერვო ამოცანების შესასრულებლად.

ლეგიტიმური მიზნის მისაღწევად უფლებაში ჩარევა დემოკრატიულ საზოგადოებაში აუცილებლად ჩაითვლება, თუ ის პასუხობს მწვავე სოციალურ საჭიროებას და არის ამ მიზნის მიღწევის პროპორციული საშუალება. სასამართლოს თანახმად, დანაშაულთან, განსაკუთრებით ორგანიზებულ დანაშაულთან და ტერორიზმთან ბრძოლა, საზოგადოებრივი უსაფრთხოებისა და მოქალაქეთა დაცვა „მწვავე სოციალურ საჭიროებას“ წარმოადგენს.

სასამართლო ადასტურებს, რომ მობილური ტელეფონის აბონენტების წინასწარი რეგისტრაცია სამართალდამცავი ორგანოებისთვის გამოძიების პროცესს მნიშვნელოვნად ამარტივებს და აჩქარებს და, შესაბამისად, კანონის ეფექტურად აღსრულებისა და დანაშაულის პრევენციის საშუალებაა. სამართლებრივი ვალდებულებების გვერდის ავლის შესაძლებლობების არსებობა არ შეიძლება იყოს საფუძველი იმისა, რომ ეჭვქვეშ დადგეს სამართლებრივი ნორმის საერთო სარგებლიანობა და ეფექტურობა. სასამართლომ კიდევ ერთხელ განმარტა, რომ ეროვნული უსაფრთხოების კონტექსტში ლეგიტიმური მიზნის მისაღწევი საშუალების არჩევისას ხელისუფლება გარკვეული მიხედულების ფარგლებით სარგებლობს, რამდენადაც წევრ სახელმწიფოებს შორის არ არსებობს კონსენსუსი წინასწარ გადახდილი სიმ-ბარათების მომხმარებელთა მონაცემების შენახვასთან დაკავშირებით. მიხედულების ფარგლების გათვალისწინებით, სასამართლომ მიიჩნია, რომ კომუნიკაციის მახასიათებლებისა და სატელეკომუნიკაციო საშუალებების ცვლილებების ფონზე, 111-ე მუხლი შესაფერის რეაგირებას წარმოადგენს.

სასამართლო დაეთანხმა ფედერალური საკონსტიტუციო სასამართლოს მსჯელობას, რომ ინახებოდა ლიმიტირებული პერსონალური მონაცემები, რომელიც არ შეიცავდა უკიდურესად პირადი სახის მონაცემებს. ეს არ იძლეოდა პიროვნების პირადი პროფილების შექმნისა და ტელეფონების მომხმარებლების გადაადგილების მიკვლევის შესაძლებლობას. შესაბამისად, სასამართლომ დაასკვნა, რომ ჩარევა საკმაოდ შეზღუდული ხასიათის იყო.

რაც შეეხება დაცვის გარანტიებს, სასამართლომ მიუთითა, რომ მონაცემთა შენახვის ხანგრძლივობა შემოფარგლული იყო სააბონენტო ხელშეკრულების დასრულების კალენდარული წლის მომდევნო წლით, რაც არ იყო შეუსაბამო, რამდენადაც სისხლის სამართლის დანაშაულების გამოძიებას შეიძლება გარკვეული დრო დასჭირდეს და გაგრძელდეს სახელშეკრულებო ურთიერთობების დასრულების შემდეგ. უფრო მეტიც, ინახებოდა მხოლოდ ის საჭირო ინფორმაცია, რაც აუცილებელი იყო შესაბამისი აბონენტის იდენტიფიცირებისთვის.

სასამართლომ აღნიშნა, რომ მომავალში მონაცემებზე წვდომის და მათი გამოყენების სათანადო შეფასების გარეშე პროპორციულობის შესახებ ვერ იმსჯელებდა.

ცენტრალიზებული და ავტომატიზებული პროცედურა სამართალდამცავი ორგანოს წარმომადგენელებისთვის მონაცემებს ხელმისაწვდომს ხდის ნებისმიერ დროს, დაყოვნების გარეშე. 112-ე მუხლი სრულად ჩამოთვლის ინფორმაციის გამოთხოვაზე უფლებამოსილ პირებს, რაც მზღუდავ ფაქტორს წარმოადგენს. 112-ე მუხლისგან განსხვავებით, 113-ე ინფორმაციის გამოთხოვისათვის წერილობითი მოთხოვნის წარდგენას ითვალისწინებს. ამ ორ ნორმას შორის კიდევ ერთი განსხვავება ის გახლავთ, რომ 113-ე მუხლის მიხედვით, უფლებამოსილი

პირები განისაზღვრებიან მათ სამსახურებრივ მოვალეობებზე მითითებით და არა ჩამონათვალის გზით, რაც სასამართლოს შეხედულებით, ინტერპრეტაციის შესაძლებლობას ტოვებს. თუმცა, ნორმა საკმარისად ნათელია იმისათვის, რომ განისაზღვროს, თუ ვის აქვს ინფორმაციის გამოთხოვის უფლებამოსილება.

ორივე მუხლთან მიმართებით სასამართლომ აღნიშნა, რომ მონაცემები დაცულია მომავალში გადამეტებული ან არაკეთილსინდისიერი გამოყენებისაგან, რამდენადაც ინფორმაციის მომთხოვნ ორგანოს დამატებითი სამართლებრივი საფუძველი სჭირდება, რათა სასურველი ინფორმაცია მოიპოვოს.

ამ ელემენტების გათვალისწინებით, სასამართლო დაეთანხმა ფედერალური საკონსტიტუციო სასამართლოს დასკვნას, რომ ტელეკომუნიკაციების კანონის 113-ე მუხლით გათვალისწინებული ბარიერები კონსტიტუციური სამართლის თვალსაზრისით მისაღები იყო. ასევე, ინფორმაციის წერილობით მოთხოვნის ვალდებულება უფლებამოსილ პირს სავარაუდოდ უბიძგებდა, ინფორმაცია მხოლოდ მაშინ მიეღო, როცა ამის საჭიროება არსებობდა.

სასამართლომ მიიჩნია, რომ პროპორციულობის შეფასებისას ზედამხედველობისა და კონტროლის ხარისხის ანალიზი მნიშვნელოვანია, მაგრამ ასეთი შეზღუდული სახით მონაცემთა შენახვისა და შეგროვების დროს გადამწყვეტი ელემენტი არ არის. 113-ე მუხლის მეორე პარაგრაფის თანახმად, ინფორმაციის გამოთხოვის კანონიერება თავად მომთხოვნი პირის პასუხისმგებლობას წარმოადგენს. სატელეკომუნიკაციო მომსახურების მიმწოდებლების კომპეტენციაში არ შედის მოთხოვნის დასაშვებობის განხილვა, გარდა იმ შემთხვევისა, როცა ის წერილობით არის წარდგენილი და მოხმობილია სამართლებრივი საფუძველი. ამასთან, 112-ე მუხლის მიხედვით, ქსელების ფედერალურ სააგენტოს შეუძლია მონაცემთა გადაცემის დასაშვებობა შეამოწმოს, როცა ამის კონკრეტული მიზეზი არსებობს. ამასთან, პერსონალურ მონაცემთა დაცვის ზედამხედველობის მიზნით, მონაცემთა მოპოვების თითოეული შემთხვევა აღირიცხება. ამგვარ ზედამხედველობას დამოუკიდებელი ორგანო ახორციელებს.

სასამართლოს შეხედულებით, რამდენადაც აბონენტის შესახებ ლიმიტირებული რაოდენობის მონაცემების შეგროვებასა და შენახვასთან დაკავშირებით წევრ ქვეყნებს შორის კონსესუსი არ არსებობს, სახელმწიფოები უსაფრთხოების დაცვისა და დანაშაულთან ბრძოლის ლეგიტიმური მიზნის მისაღწევი საშუალებების შერჩევისას, გარკვეული მიხედულების ფარგლებით სარგებლობენ. სასამართლომ დაასკვნა, რომ მოცემულ საქმეში გერმანია ამ ფარგლებს არ გასცდენია და 111-ე მუხლის საფუძველზე მომჩივნების პერსონალური მონაცემების შენახვა იყო პროპორციული და აუცილებელი დემოკრატიულ საზოგადოებაში.

საქმის შედეგი

მოცემულ საქმეში, ადამიანის უფლებათა ევროპულმა სასამართლომ ექვსი ხმით ერთის წინააღმდეგ არ დაადგინა მომჩივნების მიმართ კონვენციის მე-8 მუხლის - პირადი და ოჯახური ცხოვრების პატივისცემის უფლების დარღვევა.

მოსამართლე რანზონის განსხვავებული აზრი

შესავალი

მოსამართლე რანზონი აღნიშნავს, რომ ის არ ეთანხმება უმრავლესობის მსჯელობას და მან მხარი დაუჭირა კონვენციის მე-8 მუხლის დარღვევას. რანზონის მითითებით, აქ მსჯელობის მთავარ საკითხს წარმოადგენს, თუ რა წინაპირობები აქვს მე-8 მუხლს ლიმიტირებული პერსონალური მონაცემების შენახვის მიმართულებით, რომელიც შეიძლება საკმაოდ დიდი რაოდენობით იყოს მოპოვებული არაერთი უწყების მიერ.

ჩარევის ხარისხი

განსხვავებულ მოსაზრებაში ნათქვამია, რომ უფლებაში ჩარევის ხარისხზე მსჯელობისას სასამართლოს მხედველობიდან გამორჩა რამდენიმე მნიშვნელოვანი ფაქტი. მართალია, ამ შემთხვევაში, განსაკუთრებული კატეგორიის პერსონალური მონაცემები არ ინახება, თუმცა არ უნდა დაგვავიწყდეს, რომ ეს ინფორმაცია იძლევა იმ პირების იდენტიფიკაციის საშუალებას, რომლებიც სატელეფონო ზარის ან შეტყობინების მეშვეობით ერთმანეთში სენსიტიურ ინფორმაციას ცვლიან და არსებობს ალბათობა იმისა, რომ მოხდება იდენტიფიცირებადი პირის სენსიტიურ ინფორმაციასთან დაკავშირება. სამწუხაროდ, უმრავლესობამ ეს ასპექტი არ გაითვალისწინა. ასევე, არ განიხილა ინფორმაციის შენახვის ყოვლისმომცველი ხასიათი, რამდენადაც ის ეხება ყველა მომხმარებელს, ვინც მობილური ტელეფონით სარგებლობს. გამომდინარე იქიდან, რომ სასამართლომ სათანადოდ არ იმსჯელა ჩარევის ხარისხზე და გვერდი აუარა რამდენიმე რელევანტური საკითხის შეფასებას, მან დაასკვნა, რომ ჩარევა შეზღუდული ხასიათის იყო.

პროპორციულობა

რანზონი არც პროპორციულობის შეფასების კუთხით დაეთანხმა უმრავლესობის მსჯელობას. აღსანიშნავია, რომ აქ მონაცემებზე წვდომა არ შემოიფარგლება სისხლის სამართლის მძიმე დანაშაულების გამოძიების მიზნით. წევრი სახელმწიფოების უმრავლესობა კი მას ითვალისწინებს მხოლოდ დანაშაულის გამოძიებისა და საზოგადოებრივი წესრიგის საფრთხეების პრევენციის მიზნებისათვის.

მოსამართლის თქმით, უმრავლესობასთან უთანხმოების მთავარი მიზეზი გახლდათ დაცვის გარანტიების შეფასება - იყო თუ არა გათვალისწინებული საკმარისი გარანტიები უფლება-მოსილების არაკეთილსინდისიერად და ბოროტად გამოყენების თავიდან ასაცილებლად. რანზონის მოსაზრებით, ეს დაცვა უნდა გასცდეს სამართლებრივ ნორმებს განსაკუთრებით მაშინ, როდესაც ეს წესები და უფლებამოსილებები ჩამოყალიბებულია ფართო შინაარსით და მონაცემთა მოპოვება ძალიან გამარტივებულია. მონაცემთა მიღების მარეგულირებელი ნორმები არის საკმაოდ ფართო და ზოგადი. მათ შეიძლება დააკმაყოფილონ „ორმაგი კარის პრინციპი“, თუმცა არ არსებობს შემდგომი მექანიზმი, რომელიც შეამოწმებს გასულ ინფორმაციას. კარი მარტივად შეიძლება გაიღოს ამ გასაღებით, მაგრამ მის მეორე მხარეს არავინ არის, რომ გადაამოწმოს, რა საგანი გაივლის კარს. ამასთან, უმრავლესობა მიუთითებდა მხოლოდ საჭირო ინფორმაციით შემოსაზღვრის გარანტიაზე, თუმცა „დაცვის ეს გარანტიაც“ დაკავშირებულია ზოგად დანაწესთან, რომ არასაჭირო ინფორმაცია უნდა წაიშალოს. სწორედ ამიტომ, მოსამართლე რანზონი ვერ ხედავს მონაცემთა არაკეთილ-სინდისიერად და ბოროტად გამოყენებისგან დაცვის რეალურ საშუალებებს.

საკონსტიტუციო სასამართლომ სწორად აღნიშნა, რომ რამდენადაც ინფორმაციის მომპოვებელ უწყებას არ აქვს ვალდებულება, მოთხოვნის წარდგენისას მიუთითოს მიზეზები/არგუმენტები, რთულად წარმოსადგენია ეს საკითხი მოგვიანებით წამოიჭრას. შესაბამისად, ქსელების ფედერალური სააგენტო ვერ იქნება უფლების დაცვის ეფექტური გარანტი.

ამასთან, მონაცემთა ავტომატური დამუშავებისას არ არსებობს მონაცემების მოპოვების თაობაზე აბონენტის ან სატელეკომუნიკაციო მომსახურების მიმწოდებლის შეტყობინების ვალდებულება, რაც მონაცემთა სუბიექტის მიერ დავის წარმოებას შეუძლებელს ხდის. 113-ე მუხლის მიხედვით, მონაცემთა მექანიკურად (ხელით) დამუშავებისას, სატელეკომუნიკაციო მომსახურების მიმწოდებელმა უნდა დაიცვას ინფორმაციის მოთხოვნის კონფიდენ-ციალურობა. შესაბამისად, უფლებაში ჩარევის მსხვერპლს არ აქვს ჩარევის შესახებ ინფორ-მაცია და ვერ მოითხოვს მის შემოწმებას. შედეგად, აბონენტების მცირე რაოდენობის მიმართ განხორციელებული საგამოძიებო ღონისძიება (შემთხვევების უმეტესობა ამ ეტაპამდე არ მიდის) შეიძლება გასაჩივრდეს, თუმცა ინფორმაციის მოპოვება და შენახვა - არა.

▲● დასკვნა

ზემოთ მოყვანილ მსჯელობაზე დაყრდნობით, მოსამართლე რანზონი ასკვნის, რომ დაცვის გარანტიები ვერ უზრუნველყოფდა დიდი რაოდენობის პერსონალური მონაცემების ბოროტად გამოყენების პრევენციას. უფლებაში ჩარევა არ იყო ლეგიტიმური მიზნის მიღწევის პროპორ-ციული საშუალება, ის არ პასუხობდა „მწვავე სოციალურ საჭიროებას“ და, შესაბამისად, არ იყო აუცილებელი დემოკრატიულ საზოგადოებაში.

CATT V. THE UNITED KINGDOM

24/01/2019

ფაქტობრივი გარემოებები

2015 წელს ბრიტანეთის მოქალაქემ - ჯონ ოლდროიდ ქეთმა (შემდგომ „მომჩივანი“) ადამიანის უფლებათა ევროპულ სასამართლოს (შემდგომ „სასამართლო“) მიმართა იმ საფუძვლით, რომ პოლიციის მიერ მისი პერსონალური მონაცემების სისტემატური დამუშავებით ირღვეოდა ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის (შემდგომ „კონვენცია“) მე-8 მუხლით გათვალისწინებული პირადი ცხოვრების პატივისცემის უფლება.

მომჩივანი დაიბადა 1925 წელს და მისი ცხოვრების განმავლობაში ბევრი სხვადასხვა დემონსტრაციის მშვიდობიანი მონაწილე და აქტივისტი იყო. 2005 წელს მან მონაწილეობის მიღება დაიწყო ჯგუფის - “Smash EDO“-ის მიერ ორგანიზებულ საპროტესტო აქციებში, რომელიც ამერიკული იარაღის კომპანიის, EDO MBM Technology Ltd, ბრაიტონში მდებარე ქარხნის წინააღმდეგ იყო მიმართული. პროტესტს თან ახლდა არეულობა, რის გამოც, ის მიმდინარეობდა დიდი რაოდენობით პოლიციელების მობილიზების ფონზე. მომჩივანი ორჯერ დააკავეს გზატკეცილის გადაკეტვისთვის, თუმცა ის არასდროს უცვნიათ დამნაშავედ.

2010 წელს აქტივისტმა პოლიციას მიმართა და 1998 წლის პერსონალურ მონაცემთა დაცვის აქტის საფუძველზე, გამოითხოვა მის შესახებ შენახული ნებისმიერი სახის ინფორმაცია. პოლიციამ გაამჟღავნა 2005 წლის მარტიდან 2009 წლის ოქტომბრის პერიოდში შეგროვებული 66 ჩანაწერი, რომელთა ძირითადი ნაწილი ეხებოდა Smash EDO-ს აქციებს, თუმცა ასევე აღმოჩნდა 13 სხვა დემონსტრაციასთან დაკავშირებული ინფორმაციაც. ჩანაწერები, მათ შორის, მოიცავდა პროფესიული კავშირის კონგრესის 2006 წლის ბრაიტონის კონფერენციაზე, ლეიბორისტული პარტიის კონფერენციის 2007 წლის დემონსტრაციასა და 2009 წელს ღაზას მხარდამჭერ შეხვედრაზე დასწრების შესახებ ინფორმაციას. მის შესახებ არსებული ინფორმაცია მოპოვებული იყო სხვა პირთა ჩანაწერებიდან, სადაც ის შემთხვევით იყო ნახსენები და ინახებოდა პოლიციის მონაცემთა ბაზაში სახელწოდებით „შიდა ექსტრემიზმი.“

ჩანაწერები ძირითადად შეიცავდა ღონისძიებაზე მისი დასწრების, სახელისა და გვარის, დაბადების თარიღის, მისამართისა და ზოგჯერ მისი გარეგნობის შესახებ ინფორმაციას. 2010 წლის აგვისტოში, მომჩივანმა „პოლიციის უფროს ოფიცერთა ასოციაციას“ ("ACPO") მის შესახებ მონაცემების წაშლა სთხოვა, მაგრამ ასოციაციამ უარი განაცხადა ამ მოთხოვნის შესრულებაზე.

მომჩივანმა სარჩელი შეიტანა სასამართლოში და მიუთითა, რომ არ არსებობდა მონაცემთა შენახვის „აუცილებლობა“ ევროპული კონვენციის მე-8 მუხლის მე-2 პუნქტის მიხედვით. 2012 წლის მაისში, სასამართლომ დაადგინა, რომ კონვენციის მე-8 მუხლი ამ საქმესთან არ იყო კავშირში და რომც ყოფილიყო, ეს ჩარევა გამართლებული იქნებოდა. სააპელაციო სასამართლომ მისი მონაცემების შენახვა არაპროპორციულად მიიჩნია, თუმცა, 2015 წლის

მარტში, უზენაესმა სასამართლომ 4 ხმით ერთის წინააღმდეგ დაადგინა, რომ მონაცემთა შენახვა იყო პროპორციული და კანონის შესაბამისი. კერძოდ, სასამართლომ აღნიშნა, რომ პირად ცხოვრებაში ჩარევა იყო მცირე მასშტაბის და მიღებული ინფორმაცია ისედაც საჯაროდ გავრცელებული გახლდათ. ამასთან, მონაცემები არ იყო ინტიმური ან/და მგრძნობიარე ხასიათის. სასამართლოს შეფასებით, ასევე არსებობდა შესაბამისი საპოლიციო მიზეზები, რის გამოც, ამგვარი მონაცემები უნდა შეგროვებულიყო და შენახულიყო, მიუხედავად იმისა, რომ ის ეხებოდა მომიტინგეებს, რომელთაც სისხლის სამართლის დანაშაული არ ჩაუდენიათ და არ არსებობდა მათ მიერ ძალადობის ჩადენის ალბათობაც. გარდა ამისა, არ არსებობდა მესამე პირებისათვის, მაგალითად, დამსაქმებლისათვის ამ ინფორმაციის მიწოდების ან მისი პოლიტიკური მიზნით გამოყენების პერსპექტივა, ამასთან, პერიოდულად განიხილებოდა მონაცემების შენახვის ან წაშლის საკითხი.

უნდა აღინიშნოს ისიც, რომ სასამართლოსთან კომუნიკაციის ფარგლებში, პოლიციამ დამატებით ოთხი ჩანაწერი გაამჟღავნა და აღმოჩნდა, რომ საქმის ეროვნულ დონეზე განხილვის ეტაპზე, პოლიციამ არ წარადგინა მასთან არსებული ყველა ჩანაწერი. ამასთან, სამართალდამცავმა ორგანომ ვერ წარმოადგინა ახსნა-განმარტება, თუ რატომ არ გასცა ეს ჩანაწერები თავდაპირველ ეტაპზე.

მომჩივნის არგუმენტაცია

მომჩივანი მიუთითებდა, რომ მისი მონაცემების სისტემატური შეგროვება და მონაცემთა ბაზაში შენახვა ექცეოდა მე-8 მუხლის სფეროში და წარმოადგენდა მის პირად ცხოვრებაში ჩარევას. იგი ამტკიცებდა, რომ ეს ჩარევა არ იყო გამართლებული, რადგან მონაცემთა ბაზა, რომელშიც ეს მონაცემები ინახებოდა, არ იყო დაცვის საკმარისი გარანტიებით უზრუნველყოფილი, შესაბამისად, კანონის მოთხოვნებს არ შეესაბამებოდა. კერძოდ, მონაცემთა ბაზა პოლიციას, შესაძლოა, თვითნებურად გამოეყენებინა. გარდა ამისა, ინფორმაცია ინახებოდა ზედმეტად ხანგრძლივი ვადით და ექვემდებარებოდა როგორც ავტომატიზებულ, ისე მექანიკურ (ხელით) დამუშავებას.

საჩივარში მომჩივანს არ მოუყვანია არგუმენტები მონაცემთა დაცვის კანონმდებლობაზე დაყრდნობით, მაგრამ აღნიშნა, რომ მონაცემთა შენახვა იყო გაუმართლებელი იმის გათვალისწინებით, რომ მონაცემები ინახებოდა კანონიერ პოლიტიკურ საპროტესტო აქციებში მის ჩართულობასთან დაკავშირებით და არასდროს ყოფილა სასარგებლო პოლიციის რომელიმე საქმიანობისთვის. მომჩივანი მიუთითებდა, რომ ამგვარი მონაცემების შენახვას, სავარაუდოდ, მსუსხავი ეფექტი ექნებოდა.

მომჩივანმა ყურადღება გაამახვილა იმ ფაქტზეც, რომ დარჩენილი 4 ჩანაწერი უზენაესი სასამართლოს გადაწყვეტილების გამოქვეყნების შემდეგ გამოჩნდა და სასამართლომ დავა არასრულ ფაქტობრივ გარემოებებზე დაყრდნობით გადაწყვიტა. მომჩივნის არგუმენტით,

მონაცემთა დაცვის არასათანადო გარანტიების არსებობაზე ისიც მეტყველებს, რომ მონაცემების არათანმიმდევრულ გამჟღავნებას აქვს ადგილი და საქმის განხილვის დროს უზენაესი სასამართლოსთვისაც კი ხელმიუწვდომელი იყო ჩანაწერების დიდი ნაწილი.

მომჩივნის მითითებით, არ არსებობდა კონტროლის ან მონაცემთა შენახვის/წაშლის საჭიროების გადახედვის რეალური სისტემა. მონაცემთა დაცვის აქტის მიხედვით, „სუბიექტის წვდომის მოთხოვნა" ("subject access request") მხოლოდ მაშინ იქნება ეფექტური, თუ პოლიცია მოთხოვნის შემთხვევაში, ყველა შესაბამის მონაცემს გასცემს. მომჩივანი ასევე ამტკიცებდა, რომ გადაწყვეტილების მიღებისას ადგილობრივი სასამართლოების მიხედულების ფარგლები შეზღუდულია იმის გათვალისწინებით, რომ ამ სასამართლოებს სრულ ინფორმაციაზე წვდომა არ ჰქონდათ.

მთავრობის არგუმენტაცია

მთავრობამ დაადასტურა, რომ მომჩივნის შესახებ ინფორმაციის შეგროვება და შენახვა წარმოადგენდა მის პირადი ცხოვრების უფლებაში ჩარევას, თუმცა უზენაესი სასამართლოს დასკვნებზე დაყრდნობით განაცხადა, რომ ჩარევა ძალზე შეზღუდული ხასიათის იყო. მთავრობის პოზიციით, ჩარევა ხდებოდა კანონის შესაბამისად, რაც ეფუძნებოდა მონაცემთა დაცვის 1998 წლის კანონს, ნორმატიულ კოდექსს და სახელმძღვანელო მითითებებს.

მომჩივნის ინფორმაციის შენახვის აუცილებლობასთან დაკავშირებით, მთავრობამ მიუთითა ეროვნულ დონეზე სააპელაციო და უზენაეს სასამართლოებში გამოთქმულ მოსაზრებებზე და განმარტა, რომ ეს საკითხი ექცეოდა ქვეყნის მიხედულების ფარგლებში.

უზენაესი სასამართლოს გადაწყვეტილების მიღების შემდეგ, დამატებით 4 ჩანაწერის გამჟღავნებასთან დაკავშირებით, მთავრობამ აღნიშნა, რომ ამ გარემოებას არანაირი გავლენა არ აქვს ეროვნულ დონეზე მიღებულ გადაწყვეტილებებზე. ამასთან, ადამიანის უფლებათა ევროპულ სასამართლოში საჩივრის წარდგენამდე, მომჩივანს უნდა ამოეწურა ეროვნულ დონეზე არსებული ყველა მექანიზმი, მაგალითად, მას უნდა მოეთხოვა საქმის სასამართლო წესით გადახედვა.

მესამე მხარეთა მოსაზრებები

ა. *თანასწორობისა და ადამიანის უფლებების კომისიის (EHRC) პოზიცია*

თანასწორობისა და ადამიანის უფლებების კომისიამ წარადგინა „შიდა ექსტრემიზმის" მონაცემთა ბაზასთან დაკავშირებული შენიშვნები, რომელშიც ის დახასიათებულია, როგორც კომპიუტერიზებული და ძიების ფუნქციის მქონე პოლიციის მონაცემთა ბაზა, რომელიც

კანონიერი საზოგადოებრივი საპროტესტო აქციებისა და მათი მონაწილეების შესახებ დიდი რაოდენობით ცნობებს ინახავს.

EHRC–ის თანახმად, მონაცემთა ბაზა არ არის შექმნილი რომელიმე კანონზე დაყრდნობით, არ გააჩნია სამართლებრივი საფუძველი და არც გამოქვეყნებული სამოქმედო გეგმები ან პოლიტიკის დოკუმენტები ეხება მის შექმნას, მიზნებს ან ფუნქციებს. კომისიის მოსაზრებით, ადამიანის უფლებათა ევროპული სასამართლოს და ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტულ სამართალზე დაყრდნობით, იმისათვის, რომ იურიდიული რეჟიმი იყოს „კანონის შესაბამისი", საჭიროა ის აკმაყოფილებდეს ძირითად მინიმალურ პრინციპებს. ამ შემთხვევაში, დასახელებული მიზნებისა და პოლიციის მონაცემთა ბაზის კონტექსტის გათვალისწინებით, ეს კრიტერიუმებია:

1) პოლიციის უფლებამოსილება უნდა იყოს გამოქვეყნებული და საჯაროდ ხელმისაწვდომი; 2) საჭიროა მკაფიო და საჯაროდ ხელმისაწვდომი გარანტიები, რომ თვითნებური, შეუფერებელი ან არასაჭირო მეთოდის გამოყენებით არ მოხდეს უფლებაში ჩარევა; 3) უნდა არსებობდეს ცხადი და ხელმისაწვდომი კრიტერიუმები, რომლებიც მონაცემთა სუბიექტებს მათი მონაცემების წაშლის შესაძლებლობას მისცემს, მათ შორის, დამოუკიდებელი განხილვის მეშვეობით; 4) ინფორმაცია იმ პირთა შესახებ, რომლებიც არ არიან დანაშაულებრივ საქმიანობაში ეჭვმიტანილი, უნდა წაიშალოს.

EHRC–მა დაასკვნა, რომ „შიდა ექსტრემიზმის" მონაცემთა ბაზასთან მიმართებით, მინიმალური დაცვის გარანტიები უზრუნველყოფილი არ არის. კომისიამ ასევე ხაზი გაუსვა კანონიერ პოლიტიკურ საპროტესტო აქციებზე მსუსხავი ეფექტის საშიშროებას, რადგან ექსტრემიზმის მონაცემთა ბაზა შეიცავს ინფორმაციას პოლიტიკური აქტივობების შესახებ.

ბ. *Privacy International-ის მოსაზრებები*

Privacy International არ დაეთანხმა უზენაესი სასამართლოს პოზიციას მომჩივნის პირად ცხოვრებაში ჩარევის უმნიშვნელო ხასიათის შესახებ და გააკრიტიკა საზოგადოებრივი თავშეყრის ადგილებზე განხორციელებული აქტივობების კონტექსტში მონაცემთა შეგროვების განხილვა.

სამოქალაქო სექტორის წარმომადგენელი ამტკიცებდა, რომ სწრაფი ტექნოლოგიური განვითარების პირობებში, ეს მიდგომა საჯარო სივრცეებში ხელმისაწვდომი დიდი რაოდენობის ინფორმაციის მონიტორინგის საშუალებას იძლევა. ასეთია მაგალითად, სოციალური მედიიდან, სახის ამომცნობი ტექნოლოგიებიდან, სამხრე კამერებიდან, სანომრე ნიშნის ავტომატური ამოცნობის ტექნოლოგიიდან და სხვა გზებით მიღებული ინფორმაცია. ორგანიზაცია აკრიტიკებდა ასეთი წყაროებიდან მიღებული მონაცემების შეგროვებისა და გამოყენების შესახებ საკანონდებლო რეგულირების არარსებობას.

Privacy International-ის შეფასებით, ასეთი მონაცემების შენახვა წარმოადგენს პირადი ცხოვრების უფლებისა და გამოხატვის თავისუფლების დარღვევას.

სასამართლოს შეფასება

სასამართლომ განმარტა, რომ პირის პერსონალური მონაცემების შეგროვება და შენახვა ევროპული კონვენციის მე-8 მუხლით გათვალისწინებულ უფლებაში ჩარევაა. შეფასების საგანს წარმოადგენს, თუ რამდენად აუცილებელი იყო ხსენებული ჩარევა დემოკრატიულ საზოგადოებაში დანაშაულის აღკვეთის ლეგიტიმური მიზნის მისაღწევად.

სასამართლოს პრაქტიკის თანახმად, ჩარევა აუცილებელია დემოკრატიულ საზოგადოებაში, როდესაც ის პასუხობს „მწვავე სოციალურ საჭიროებას", არის ლეგიტიმური მიზნის პროპორციული და მის გასამართლებლად ეროვნული ხელისუფლება წარმოადგენს საფუძვლიან და საკმარის დასაბუთებას.

„კანონის შესაბამისად" ჩარევა ნიშნავს არა მხოლოდ სათანადო საკანონდებლო საფუძვლის არსებობას, არამედ მის ხელმისაწვდომობას და განჭვრეტადობას. ეროვნული კანონმდებლობა უნდა ითვალისწინებდეს თვითნებობისგან დაცვის გარანტიებს, მკაფიოდ აყალიბებდეს კომპეტენტური ორგანოს უფლებამოსილების ფარგლებსა და მისი განხორციელების წესს.

სასამართლოს თანახმად, მოცემულ შემთხვევაში, მონაცემთა შეგროვება ხორციელდებოდა საერთო სამართლის (common law) ზოგადი საპოლიციო უფლებამოსილების ფარგლებში. თუმცა, გამოთქვა წუხილი იმის თაობაზე, რომ მონაცემთა ბაზის მიზნებისთვის მონაცემთა შეგროვებას არ ჰქონდა უფრო მკაფიო და გასაგები სამართლებრივი საფუძველი. „შიდა ექსტრემიზმს" სხვადასხვა უწყება სხვადასხვაგვარად განმარტავდა და სასამართლოსთვის გაუგებარი იყო, თუ რა კრიტერიუმზე დაყრდნობით აგროვებდა პოლიცია ცნობებს. „შიდა ექსტრემიზმის" მკაფიო განმარტების არარსებობამ სასამართლოს შეშფოთება გამოიწვია.

სასამართლომ დაასკვნა, რომ ინფორმაციის საჯაროდ ხელმისაწვდომობის გათვალისწინებით, მომჩივნისთვის მოსალოდნელი უნდა ყოფილიყო, რომ პოლიცია, დიდი ალბათობით, შეაგროვებდა მის შესახებ ცნობებს. ამასთან, სასამართლომ გაიზიარა მომჩივნის მოსაზრება, რომ ხელმისაწვდომი ინფორმაციით რთული იყო „შიდა ექსტრემიზმის" ბაზის ფორმირებისათვის საჭირო მონაცემთა შინაარსისა და შეგროვების ფარგლების განსაზღვრა.

სასამართლომ მსჯელობა განავითარა არა მონაცემთა მოპოვების, არამედ მათი შენახვის შეფასების კუთხით; მიუთითა, რომ მონაცემთა შეგროვებაზე გადაწყვეტილების მიღება ექცეოდა სახელმწიფოს მიხედულების ფარგლებში და აქცენტი გააკეთა მომჩივნის მონაცემების ფლობით განპირობებულ უფლებაში ჩარევაზე.

მოცემულ საქმეში პოლიციის მიერ მონაცემთა ბაზის შექმნის ლეგიტიმურ მიზანთან დაკავშირებით, დავა არ ყოფილა. სასამართლომაც მიიჩნია, რომ მომჩივნის მონაცემების დამუშავება შემდეგ ლეგიტიმურ მიზნებს ემსახურებოდა: დანაშაულისა და უწესრიგობის პრევენციას, ასევე სხვათა უფლებებისა და თავისუფლებების დაცვას.

უზენაესი სასამართლოს მსგავსად, ევროპულმა სასამართლომაც დაადგინა, რომ არსებობდა სათანადო საპოლიციო მიზეზები, რის გამოც ასეთ მონაცემებს აგროვებდნენ. უშუალოდ

მომჩივნის მონაცემთა შეგროვება გამართლებულად ჩაითვალა იმ გარემოებაზე დაყრდნობით, რომ Smash EDO-ს აქტივისტების ქმედებები, უმეტეს შემთხვევაში, იყო ძალადობრივი და პოტენციურად დანაშაულებრივი. მიუხედავად იმისა, რომ თავად მომჩივანი არასდროს ყოფილა ძალადობრივი ან არ გამოუმჟღავნებია მიდრეკილება ასეთი ქცევისკენ, მან თავი არაერთგზის საჯაროდ გააიგივა ამ ჯგუფთან. ამავე დროს, სასამართლომ აღნიშნა, რომ მონაცემთა შენახვის მაქსიმალური ვადა არ იყო განსაზღვრული და არ არსებობდა მათი შენახვის მწვავე საზოგადოებრივი საჭიროება.

გადაწყვეტილებაში ნათქვამია, რომ მომჩივანი ვინმესთვის არ წარმოადგენდა საფრთხეს, მათ შორის, მისი ასაკის გათვალისწინებით (ის საქმის განხილვის ეტაპისთვის 95 წლის იყო). სასამართლომ ხაზგასმით აღნიშნა, რომ შეგროვებული ჩანაწერები ასახავდა მომჩივნის პოლიტიკურ შეხედულებებს, ეს უკანასკნელი კი წარმოადგენს განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს და სარგებლობს დაცვის მაღალი სტანდარტით. სასამართლოს პოზიციით, მონაცემთა სენსიტიური ხასიათი გახლდათ საქმისთვის ცენტრალური მნიშვნელობის მქონე და ამ კონტექსტში უნდა განეხილა ხსენებული დავა ეროვნულ დონეზე არსებულ სასამართლოებს.

გადაწყვეტილების თანახმად, როცა სახელმწიფოსთვის მინიჭებული უფლებამოსილებები ბუნდოვანია, რაც ქმნის თვითნებობის რისკს, და როდესაც ტექნოლოგიები მუდმივად ვითარდება და იხვეწება, მნიშვნელოვანია, შემოწმდეს კონვენციის მე-8 მუხლის პრინციპებთან შესაბამისობა.

სასამართლომ მიუთითა, რომ განსხვავებით *M.M v. United Kingdom* საქმისაგან, მოცემულ შემთხვევაში, მონაცემების მესამე პირისთვის გადაცემა არ ხდებოდა და მომჩივანს ჰქონდა ჩანაწერების წაშლის მოთხოვნის უფლებამოსილება, თუმცა არ არსებობდა მონაცემთა დაცვის სათანადო პროცედურული გარანტიები. გარანტიების ნაკლებობა მოიცავდა მონაცემთა შენახვის ვადის არარსებობას. გაურკვეველი იყო, თუ რამდენ ხანს უნდა შენახულიყო მონაცემები, რაც აპლიკანტის შესახებ ცნობების განუსაზღვრელი ვადით შენახვის რისკს ქმნიდა. შეგროვებული მონაცემები ინახებოდა მინიმუმ 6 წლის განმავლობაში. ამ ვადის გასვლის შემდეგ, ხდებოდა შენახული მონაცემების გადახედვა და ფასდებოდა მათი შემდგომი შენახვის აუცილებლობა. მომჩივნის საქმეში არ იყო ნათელი, მსგავსი გადახედვა საერთოდ განხორციელდა თუ არა და განხორციელების შემთხვევაში, ჰქონდა თუ არა მას არსებითი მნიშვნელობა. მთავრობის არგუმენტზე, რომ მონაცემთა გადახედვა და წაშლა დიდ ძალისხმევას უკავშირდებოდა, სასამართლომ მიუთითა, რომ მართალია, მომჩივნის შემთხვევაში გადახედვა არ მომხდარა, მაგრამ ზოგადად, მონაცემთა გადახედვა და წაშლა რეალური შესაძლებლობა იყო.

გადაწყვეტილების თანახმად, საქმის გარემოებებმა აჩვენა ევროპის საბჭოს მინისტრთა კომიტეტის რეზოლუციასთან წინააღმდეგობა (კერძოდ, ევროპის საბჭოს მინისტრთა კომიტეტის რეზოლუცია (74)29 „საჯარო სექტორში მონაცემთა ელექტრონული ბანკის პირისპირ ფიზიკურ პირთა პირადი ცხოვრების დაცვის შესახებ“), რომლის მიხედვითაც, დადგენილი უნდა იყოს გარკვეული სახის ინფორმაციის ფლობის მაქსიმალური ვადები.

დაცვის გარანტიების ეფექტურობასთან მიმართებით, სასამართლომ შეშფოთება გამოხატა იმ გარემოებასთან დაკავშირებითაც, რომ პოლიცია რეალურად იმაზე მეტ ინფორმაციას ინახავდა, ვიდრე ეს გამოვლინდა ეროვნულ სასამართლოებში საქმის განხილვის დასრულებამდე. გადაწყვეტილების თანახმად, დამატებით 4 ჩანაწერის აღმოჩენამ უფრო მეტად გამოკვეთა არსებული დაცვის გარანტიების არაეფექტურობა და ის გარემოება, რომ შესაბამისი უწყებები მხედველობაში არ იღებდნენ შეგროვებული მონაცემების სენსიტიურ ბუნებას, რის საფუძველზეც, მათი დაცვის მაღალი ხარისხი უნდა ყოფილიყო უზრუნველყოფილი.

სასამართლომ დაადგინა, რომ მომჩივნის მონაცემების განუსაზღვრელი ვადით შენახვა ლეგიტიმური მიზნის მისაღწევად გამოყენებულ არაპროპორციულ ზომას წარმოადგენდა, რადგან საქმე ეხებოდა ისეთ პერსონალურ მონაცემებს, რაც დაკავშირებულია პოლიტიკურ მოსაზრებებთან და შესაბამისად, ექცეოდა უფრო ძლიერი დაცვის სფეროში.

საქმის შედეგი

სასამართლომ ერთხმად დაადგინა კონვენციის მე-8 მუხლის - პირადი და ოჯახური ცხოვრების პატივისცემის უფლების დარღვევა და გაერთიანებულ სამეფოს მომჩივნის სასარგებლოდ 27,000 ევროს გადახდა დააკისრა.

მოსამართლე კოსკელოს თანმხვედრი აზრი, რომელსაც მოსამართლე ფელიჩიც შეუერთდა

მოსამართლე კოსკელო თანმხვედრ მოსაზრებაში აღნიშნავს, რომ ის ეთანხმება საქმის საერთო შედეგს, კერძოდ იმას, რომ დაირღვა კონვენციის მე-8 მუხლის მე-2 პუნქტი და გადაწყვეტილებაში განვითარებულ მსჯელობასთან დაკავშირებით მნიშვნელოვანი შენიშვნა არ აქვს. თუმცა, ის ეჭვით უყურებს „კანონთან შესაბამისობის“ კრიტერიუმის დასაბუთებას. კოსკელოს აზრით, მართალია, ამ მიმართულებით შენიშვნები გამოითქვა, თუმცა „კანონთან შესაბამისობის“ კრიტერიუმის დაკმაყოფილების თაობაზე მკაფიო დასკვნა არ გაკეთებულა. ის მიიჩნევს, რომ სამწუხაროდ, სასამართლოს ეს დასაბუთება არ არის მტკიცე და არ შეესაბამება აქამდე ჩამოყალიბებულ პრეცედენტულ სამართალს. ჩარევის საფუძველი არა მარტო კანონით უნდა იყოს გათვალისწინებული, არამედ ის ასევე უნდა შეესაბამებოდეს კანონის უზენაესობის პრინციპს - კანონი უნდა იყოს ხელმისაწვდომი, გასაგებად ჩამოყალიბებული, განჭვრეტადი და ინდივიდს საკუთარი ქმედების დარეგულირების შესაძლებლობას აძლევდეს. იმისათვის, რომ ეროვნული კანონმდებლობა შეესაბამებოდეს ამ მოთხოვნებს, საჭიროა, ის ითვალისწინებდეს თვითნებობისგან დაცვის სათანადო გარანტიებს, მკაფიოდ მიუთითებდეს დისკრეციის ფარგლებზე და უფლებამოსილების განხორციელების წესზე. ამ მოთხოვნათა შესრულების სიზუსტის ხარისხი დამოკიდებულია თავად კანონის კონტექსტსა და შინაარსზე, მაგალითად იმ სფეროზე, რომლის დასარეგულირებლადაც ის შეიქმნა.

სასამართლო არსებითად მიიჩნევს, რომ მონაცემთა დაცვის სფეროში მოქმედი კანონმდებლობა უნდა ითვალისწინებდეს შესაბამისი ზომების გამოყენების მკაფიო, დეტალურ წესებს და პერსონალურ მონაცემთა დამუშავების თითოეულ ეტაპზე მათი ბოროტად გამოყენებისა და თვითნებობის რისკისგან დაცვის საკმარის გარანტიებს.

მოსამართლის შეხედულებით, მიუხედავად იმისა, რომ პერსონალური მონაცემების შეგროვება და შემდგომი დამუშავება სამართალდამცავი ორგანოების ფუნქციონირების შეუცვლელი ნაწილია, ამავდროულად არსებობს მნიშვნელოვანი თანმხლები რისკები, რომლებიც იმ ინდივიდთა უფლებებისა და თავისუფლებების განხორციელებას უქმნის საფრთხეს, რომელთა მონაცემებიც მუშავდება.

კოსკელოს მოსაზრებით, ამ საქმეში პრობლემურია უფრო კანონი, ვიდრე „აუცილებლობის“ საკითხი. საერთო სამართლის (Common law) მიხედვით, პოლიციას მონაცემთა შეგროვების უფლებამოსილება აქვს „საპოლიციო მიზნებისთვის“, არ არსებობს მონაცემთა დამუშავების გამოკვეთილი ნორმატიული საფუძველი, ხოლო არაკანონისმიერი საფუძველი ბუნდოვანია. მთავრობის არგუმენტი, რომ მონაცემთა შეგროვება ხორციელდება დანაშაულის სამომავლო რისკების აღსაკვეთად, ისევე ბუნდოვანი და გაურკვეველია, როგორც თავად „საპოლიციო მიზნებისა“ და „შიდა ექსტრემიზმის“ განმარტება. აღნიშნული კი ნიშნავს, რომ არ არსებობს ზომების მიღების მომწესრიგებელი მკაფიო რეგულირება. ამ კონტექსტში უნდა აღინიშნოს, რომ აუცილებელია არა მხოლოდ ზომების მარეგულირებელი მკაფიო, დეტალური წესები, არამედ აგრეთვე იმ გარანტიების აღიარება, რომლებიც უკავშირდება მონაცემთა გამოყენებას, შენახვის ხანგრძლივობას, მათზე წვდომას, აგრეთვე კონფიდენციალობასა და მათ განადგურებას.

მოსამართლე თანმხვედრ მოსაზრებაში აღნიშნავს, რომ მესამე პირებზე ინფორმაციის გაუცემლობას და მონაცემთა ფარული საგამოძიებო მოქმედებების გარეშე მოპოვებას, ამ საქმეში არსებითი მახასიათებელი არ შემოაქვს; არც ამ მონაცემების საჯარო თავშეყრის ადგილას მოპოვების ფაქტს აქვს გადამწყვეტი მნიშვნელობა. პერსონალური მონაცემების დაცვის საჭიროება ხშირად დამოკიდებულია ისეთ ელემენტებზე, როგორიც არის კონტექსტი, ასეთი მონაცემების კომბინაცია, გამოყენება და ხელმისაწვდომობა.

დასკვნის სახით, კოსკელო მიუთითებს, რომ მიღებული შედეგი განპირობებული იყო კანონმდებლობის ხარვეზებიდან გამომდინარე, რაც საკმარისი იყო მერვე მუხლის დარღვევის დასადგენად. პერსონალური მონაცემების დამუშავებით დაირღვა იმ პირის პირადი ცხოვრების პატივისცემის უფლება, რომელიც არასდროს ყოფილა გასამართლებული ან ეჭვმიტანილი რაიმე დანაშაულის ჩადენაში, არც მისი პირდაპირი მონაწილეობა დგინდებოდა Smash EDO-ს დანაშაულებრივ საქმიანობებში და აღიარებული იყო ისიც, რომ მომჩივნისგან არ მომდინარეობდა არანაირი საფრთხე.

LÓPEZ RIBALDA AND OTHERS V. SPAIN

17/10/2019

ფაქტობრივი გარემოებები

მოცემულ საქმეში მომჩივნები იყვნენ ესპანური სუპერმარკეტის ქსელის - M.-ის თანამშრომლები, რომელთა ინფორმირების გარეშე, დანაშაულის გამოვლენის მიზნით, მიმდინარეობდა იმ სამუშაო სივრცის ფარული ვიდეო კონტროლი, სადაც ისინი თავიანთ სამსახურებრივ მოვალეობებს ასრულებდნენ. მომჩივნებმა მიმართეს ადამიანის უფლებათა ევროპულ სასამართლოს (შემდგომ „სასამართლო“) და მიუთითეს, რომ ფარული ვიდეო მეთვალყურეობის შედეგად, დაირღვა მათი პირადი ცხოვრების პატივისცემის უფლება, რომელიც ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის (შემდგომ „კონვენცია“) მე-8 მუხლით არის გათვალისწინებული. მომჩივნები მიიჩნევდნენ, რომ ეროვნულმა სასამართლოებმა ვერ შეძლეს მათი პირადი ცხოვრების პატივისცემის უფლების ეფექტურად დაცვა.

2009 წელს, მომჩივნები სუპერმარკეტში დასაქმებული იყვნენ მოლარის/გაყიდვების ასისტენტის პოზიციებზე. მას შემდეგ, რაც გამოვლინდა შეუსაბამობა საწყობში არსებულ საქონლის მარაგსა და გაყიდვების ოდენობას შორის (ხუთი თვის განმავლობაში მიღებულმა ზარალმა დაახლოებით 80 000 ევროს მიაღწია), სუპერმარკეტის მენეჯერმა გადაწყვიტა, სამუშაო სივრცეში დაეყენებინა როგორც ხილული, ისე ფარული ვიდეოკამერები. თანამშრომლებს ეცნობათ მხოლოდ ხილული ვიდეოკამერების დამონტაჟების შესახებ, რომლებიც სუპერმარკეტის შესასვლელსა და გასასვლელს მეთვალყურეობდა. ფარული კამერებით კი მიმდინარეობდა სალარო აპარატების არეალის კონტროლი. კამერების ზუსტი რაოდენობა მხარეთა მიერ არ დაზუსტებულა, თუმცა გაირკვა, რომ მოწმდებოდა მინიმუმ ოთხი სალაროს დახლი.

ფარული კამერების საშუალებით, მომჩივნები, სხვა თანამშრომლებთან ერთად, ამხილეს საქონლის ქურდობაში. ქურდობის კადრები აჩვენეს ევროპის პროფესიული კავშირების კონფედერაციის (ETUC) წარმომადგენელს. მალევე თოთხმეტი თანამშრომელი - მომჩივნების ჩათვლით - სამსახურიდან გათავისუფლდა დისციპლინური გადაცდომის საფუძვლით, რადგან კადრებზე დაფიქსირდა, რომ ისინი მომხმარებლებსა და სხვა თანამშრომლებს ეხმარებოდნენ ქურდობაში, ასევე თავადაც იპარავდნენ საქონელს. ხუთი მომჩივნიდან სამმა ხელი მოაწერა მორიგების დოკუმენტს (acuerdo transaccional), რომლითაც ისინი აღიარებდნენ ქურდობაში მონაწილეობას და იღებდნენ ვალდებულებას, რომ არ გახდიდნენ სადაოდ მათი სამსახურიდან გათავისუფლების შესახებ გადაწყვეტილებას და არ აწარმოებდნენ შრომით დავას სასამართლოში. დამსაქმებელმა აიღო ვალდებულება, რომ მათ წინააღმდეგ არ წამოიწყებდა სისხლის სამართლის საქმის წარმოებას. ამ შეთანხმებას ხელს ასევე აწერდა კონფედერაციის წარმომადგენელი.

გათავისუფლების შემდეგ, ყველა მომჩივანმა მიმართა შრომის ტრიბუნალს და დაიწყო კომპანიის წინააღმდეგ დავა უსამართლო გათავისუფლებაზე მითითებით. ზოგადად,

ტრიბუნალი ეჭვქვეშ აყენებდა ფარული ჩანაწერების მტკიცებულებად დაშვებას და ამგვარი მასალის გამოყენებას პირადი ცხოვრების ხელშეუხებლობის დარღვევად მიიჩნევდა. თუმცა, ამ კონკრეტულ საქმეში, ტრიბუნალმა არ დაადგინა პირადი ცხოვრების პატივისცემის უფლების დარღვევა ორი მომჩივნის მიმართ, რომელთაც არ ჰქონდათ ხელი მოწერილი მორიგების დოკუმენტზე და დაასკვნა, რომ ჩანაწერები იყო დასაშვები მტკიცებულება, ხოლო მათი დაკავებული თანამდებობიდან გათავისუფლება - კანონიერი.

ამასთან, ტრიბუნალმა უარი თქვა დანარჩენი სამი მომჩივნის მოთხოვნის დაკმაყოფილებაზე და გაითვალისწინა დამსაქმებლის პრეტენზია, რომ მათი საჩივარი უსაფუძვლო იყო, რადგან მათ ხელი ჰქონდათ მოწერილი მორიგების შეთანხმებაზე, რომელიც გამორიცხავდა გათავისუფლების შესახებ გადაწყვეტილების გასაჩივრებას. მომჩივნების მტკიცებაზე, რომ მათ მორიგებაზე ხელი იძულებით მოაწერინეს, სისხლის სამართლის საქმის აღძვრაზე მითითებით, ტრიბუნალმა დასძინა, რომ დაშინებისა და ზეწოლის არსებობას გამორიცხავდა 2 მომჩივნის მიერ შეთანხმების გაფორმებაზე უარი და დაასკვნა, რომ მორიგების დოკუმენტი არ იყო შედგენილი არაკანონიერ საფუძველზე დაყრდნობით და ის წარმოადგენდა ორმხრივი დათმობის მეშვეობით დავის გადაწყვეტის საშუალებას.

კატალონიის უმაღლესმა სასამართლომ ძალაში დატოვა პირველი ინსტანციის გადაწყვეტილება და მიუთითა, რომ შრომის რეგულაციის 20(3) პარაგრაფი, პერსონალურ მონაცემთა დაცვის შესახებ საკანონდებლო აქტის 6(2) დებულების გათვალისწინებით, არ საჭიროებდა ვიდეო მეთვალყურების განხორციელებაზე დასაქმებულის წინასწარ თანხმობას, თუმცა ჩარევა უნდა შემოწმებულიყო საკონსტიტუციო სასამართლოს პროპორციულობის ტესტის შესაბამისად. სასამართლომ მიიჩნია, რომ სუპერმარკეტის მეთვალყურეობა აკმაყოფილებდა საჭირო კრიტერიუმებს, რადგან იგი გამართლებული იყო დანაშაულის ჩადენის ეჭვების გამო, შესაბამისი და აუცილებელი ზომა იყო მიზნის მისაღწევად, რადგან სხვა უფრო ნაკლებად მზღუდავი ფორმით შეუძლებელი იქნებოდა მიზნის მიღწევა და იყო პროპორციული, რამდენადაც ჩანაწერები შემოფარგლული იყო გარკვეული დროითა და სივრცით, რომელიც უკავშირდებოდა ეჭვების მართებულობის დადასტურებას. თანამშრომელთა წინასწარი ინფორმირების ხარვეზთან დაკავშირებით, სასამართლომ აღნიშნა, რომ იმ შემთხვევაში, თუ დასაქმებულებს ეცოდინებოდათ ფარული მეთვალყურეობის შესახებ, სავარაუდოდ, მიზნის მიღწევა ვერ მოხერხდებოდა.

სამ მომჩივანთან დაკავშირებით, უმაღლესმა სასამართლომ ძალაში დატოვა ტრიბუნალის გადაწყვეტილება და დასძინა, რომ მორიგების შეთანხმება იყო მოქმედი, ჰქონდა იურიდიული ძალა და არ გამოვლენილა რამე ხარვეზი, რომელიც საპირისპიროზე მიუთითებდა. სასამართლოს შეფასებით, შეთანხმებები გაფორმდა კონფედერაციის წარმომადგენლის თანდასწრებით და ტექსტის ფორმულირება ეჭვს არ ტოვებდა, რომ თანამშრომლებმა იცოდნენ საქმის გარემოებები და მათ სურვილი გამოთქვეს, შეეწყვიტათ შრომითი ხელშეკრულება.

▲● *მომჩივნების მიმართ გატარებული სისხლის სამართლის პროცედურები*

მას შემდეგ, რაც მომჩივნებმა ტრიბუნალს მიმართეს, დამსაქმებელმა კომპანიამ თოთხმეტივე თანამშრომლის მიმართ საჩივარი შეიტანა პოლიციაში, რის საფუძველზეც, მათ წინააღმდეგ სისხლის სამართლის საქმე აღიძრა. ჩატარებული გამოძიების თანახმად, თანამშრომლებს შორის შეთანხმებული კავშირი არ დადგინდა და იმის გათვალისწინებით, რომ თითოეულის მიერ მოპარული საქონელი 400 ევროს არ აღემატებოდა, მოსამართლემ გადაწყვიტა დანაშაული გადაეკვალიფიცირებინა, როგორც მცირე მნიშვნელობის დანაშაული (falta). 2011 წლის სექტემბერში, მოსამართლემ სისხლისსამართლებრივი დევნა შეწყვიტა იმ საფუძვლით, რომ ამ ტიპის დანაშაულებზე კანონმდებლობა პროცედურების განხორციელების შეზღუდულ პერიოდს ადგენდა.

▲● *ადამიანის უფლებათა ევროპული სასამართლოს პალატის გადაწყვეტილება*

2018 წლის 9 იანვრის გადაწყვეტილებაში სასამართლომ აღნიშნა, რომ მოცემულ საქმეზე კონვენციის მე-8 მუხლი ვრცელდებოდა და რადგან საქმე შეეხებოდა კერძო პირის მიერ ვიდეო მონიტორინგის განხორციელებას, სასამართლოს უნდა დაედგინა, სახელმწიფო ორგანოებმა შეასრულეს თუ არა პოზიტიური ვალდებულება, კერძოდ, დაიცვა თუ არა სახელმწიფომ ბალანსი მომჩივნების პირადი ცხოვრების პატივისცემის უფლებასა და კომპანიის ქონებრივ ინტერესებს შორის.

პალატის შეფასებით, მიუხედავად იმისა, რომ ვიდეო კონტროლი დაწესდა ქურდობის ლეგიტიმური ეჭვების გამო, იგი ფართო მასშტაბის გახლდათ - არ იყო დროში შეზღუდული, გავლენას ახდენდა ყველა თანამშრომელზე და მოიცავდა ყველა სამუშაო საათს. ასევე, დარღვეული იყო ეროვნული კანონმდებლობით გათვალისწინებული ვალდებულება წინასწარი ინფორმირების შესახებ. შესაბამისად, სასმართლომ კონვენციის მე-8 მუხლის დარღვევა დაადგინა.

მომჩივნების არგუმენტაცია

მომჩივნები ამტკიცებდნენ, რომ მათი გათავისუფლების შესახებ დამსაქმებლის გადაწყვეტილება ეფუძნებოდა სამუშაო ადგილზე არაკანონიერი ვიდეო-მეთვალყურეობის საშუალებით მიღებულ ჩანაწერებს, რის შედეგადაც მათი პირადი ცხოვრების პატივისცემის უფლება დაირღვა. ეროვნულმა სასამართლოებმა გათავისუფლების შესახებ გადაწყვეტილების ბათილად ცნობაზე უარის თქმით, ვერ შეასრულეს თავიანთი მოვალეობა, დაეცვათ ევროპული კონვენციის მე-8 მუხლით გათვალისწინებული უფლება. მომჩივნების პოზიციით, მართალია, დამსაქმებელს უფლება ჰქონდა, კამერა დაეყენებინა საკუთარი ქონების დასაცავად, თუმცა, დასაქმებულთა ინფორმირების გარეშე, რამდენიმე კვირის განმავლობაში მათი სრული სამუშაო დღის მონიტორინგი ეწინააღმდეგებოდა კონვენციის მე-8 მუხლით დადგენილ სტანდარტს, ასევე ესპანეთის ეროვნულ კანონმდებლობას. კამერების დაყენების შესახებ ინფორმირებითა და დასაქმებულთა პირადი ცხოვრების უფლების დაცვით, კომპანია შეძლებდა საკუთარი ქონების დაცვას.

მომჩივნები მიუთითებდნენ, რომ მათი შემთხვევა განსხვავდებოდა *Köpke v. Germany* საქმისაგან, რამდენადაც მოცემულ შემთხვევაში, დამსაქმებელმა დაარღვია კანონმდებლობით გათვალისწინებული ინფორმირების ვალდებულება, ვიდეო მონიტორინგი არ იყო დროში შეზღუდული და ხდებოდა არა მხოლოდ სავარაუდო დამნაშავეების კონტროლი, არამედ მთელი სუპერმარკეტის პერსონალის. ისინი მიიჩნევდნენ, რომ სასამართლოს უნდა ეხელმძღვანელა *Bărbulescu v. Romania* საქმეში მოცემული მიდგომის შესაბამისად და შეეფასებინა პროპორციულობის კრიტერიუმი. მათი მოსაზრებით, ნათელი იყო, რომ დამსაქმებლის მიერ მიღებული ზომა არ იყო პროპორციული, რამდენადაც ორივე მხარის ინტერესების დაცვა შეიძლებოდა კანონით გათვალისწინებული ინფორმირების ვალდებულების შესრულებით.

მთავრობის არგუმენტზე, რომ მათ ეროვნულ დონეზე არსებული უფლების დაცვის ყველა საშუალება არ გამოუყენებიათ და არ მიუმართავთ პერსონალურ მონაცემთა დაცვის სააგენტოსათვის, მომჩივნებმა აღნიშნეს, რომ დამსაქმებლისათვის ადმინისტრაციული პასუხისმგებლობის დაკისრებით, ისინი მაინც ვერ მიიღებდნენ უფლების დარღვევისთვის სათანადო კომპენსაციას. მათი მტკიცებით, მხოლოდ შრომითი დავების განმხილველი სასამართლოს იურისდიქციაში შედიოდა ამ საქმის განხილვა.

მთავრობის არგუმენტაცია

მთავრობის მოსაზრებით, იქიდან გამომდინარე, რომ თავად მომჩივნებიც მიუთითებდნენ კერძო პირის და არა სახელმწიფო ორგანოების მიერ პირადი ცხოვრების პატივისცემის უფლების დარღვევის შესახებ, დიდ პალატას უნდა ეხელმძღვანელა *Von Hannover (no. 2) v. Germany* საქმეში განვითარებული მიდგომით. კერძოდ, ევროპულ სასამართლოს უნდა ემსჯელა, შეაფასეს თუ არა ესპანეთის სასამართლოებმა მხარეთა დაპირისპირებული ინტერესები და დაადგინეს თუ არა მათ შორის სამართლიანი ბალანსი. მთავრობის შეხედულებით, ეროვნულმა სასამართლოებმა მხედველობაში მიიღეს მომჩივანთა პირადი ცხოვრების პატივისცემის უფლება და სწორად დაადგინეს უფლებათა შორის ბალანსი.

მთავრობის პოზიციით, მიუხედავად იმისა, რომ სასურველი იყო თანამშრომელთა ინფორმირება, უფლებაში ჩარევა მაინც პროპორციული და გამართლებული იყო. მომჩივნები მუშაობდნენ საზოგადოებისთვის ღია სივრცეში და ამ სივრცეში ქურდობის გამოვლენის მიზნით დაყენებული რამდენიმე კამერის შესახებ მათი ინფორმირების მიუხედავად, თანამშრომლებმა გაცნობიერებულად ჩაიდინეს დანაშაული. მთავრობის განმარტებით, ვიდეო მეთვალყურეობა გაგრძელდა მხოლოდ ათი დღის განმავლობაში და ის მიემართებოდა მხოლოდ იმ თანამშრომლებს, რომლებიც სალარო სივრცეებში მუშაობდნენ და პირდაპირი კონტაქტი ჰქონდათ მომხმარებლებთან. გარდა ამისა, ისინი, რომელთა მიმართაც არსებობდა ქურდობასთან დაკავშირებული ეჭვი, დაბარებულები იყვნენ ინდივიდუალურ ინტერ-

ვიუებზე. ამასთან, *Bărbulescu v. Romania* საქმისგან განსხვავებით, აქ საუბარია ისეთი სამუშაო სივრცის გაკონტროლებაზე, სადაც დასაქმებულებს პირდაპირი შეხება აქვთ საზოგადოებასთან, რის გამოც მათი პრივატულობის აღქმა შემცირებული უნდა იყოს, განსხვავებით ელ-ფოსტის და კონფიდენციალური პირადი კომუნიკაციის მიმოწერისა. მთავრობა ასევე მიუთითებდა იმ გარემოებაზე, რომ მომჩივნებს არ მიუმართავთ ესპანეთის პერსონალურ მონაცემთა დაცვის სააგენტოსთვის, რათა სააგენტოს შეეფასებინა ვიდეო მონიტორინგის კანონიერების საკითხი და მათ დავა წარმართეს მხოლოდ სამსახურიდან გათავისუფლების შესახებ გადაწყვეტილების გაუქმების ჭრილში. გარდა ამისა, პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის დარღვევა ავტომატურად არ ნიშნავს პირადი ცხოვრების პატივისცემის უფლების დარღვევას. მთავრობის მოსაზრებით, მომჩივნებს კომპენსაციის მიღებისა და მიყენებული ზიანის ანაზღაურების მიზნით უნდა ედავათ სამოქალაქო კუთხითაც.

მთავრობის წარმომადგენელი მიუთითებდა, რომ სახელმწიფომ კონვენციის მე-8 მუხლის მიზნებისთვის შეასრულა თავისი პოზიტიური ვალდებულება და მას არ უნდა დაეკისროს პასუხისმგებლობა კერძო პირის მიერ უფლების დარღვევის ან მომჩივანთა მიერ კომპეტენტური ორგანოსთვის არ მიმართვის გამო.

მესამე მხარის მოსაზრებები

ევროპის პროფესიული კავშირების კონფედერაციის მიერ წარდგენილი მოსაზრებების თანახმად, შესაძლებელია სახელმწიფომ სათანადოდ არ დაიცვა დასაქმებულთა პირადი ცხოვრების უფლება სამუშაო ადგილზე. ახალი ტექნოლოგიების განვითარებით წარმოქმნილი რისკების ფონზე, პირადი ცხოვრების უფლების პატივისცემის უზრუნველყოფა, განსაკუთრებით შრომით სამართლებრივ ურთიერთობებში, არის საერთაშორისო დონეზე ადამიანის უფლებების დაცვის ახალი ასპექტი. სწორედ ამიტომ განმტკიცდა საერთაშორისო, მათ შორის, ევროპის დონეზე არსებულ პერსონალურ მონაცემთა დაცვის კანონმდებლობაში მონაცემთა დამუშავების შესახებ სუბიექტის ინფორმირების ვალდებულება.

ევროპის პროფესიული კავშირების კონფედერაციის შეხედულებით, ევროკავშირისა და ევროპის საბჭოს წევრ ქვეყნებში, მათ შორის ესპანეთის კანონმდებლობაში მოცემული ინფორმირების ვალდებულება წარმოადგენს კონვენციის მე-8 მუხლიდან გამომდინარე პროცედურულ გარანტიას.

სასამართლოს შეფასება

სასამართლომ განმარტა, რომ კონვენციის მე-8 მუხლის არსი და მთავარი დანიშნულება არის ინდივიდის პირადი ცხოვრების თვითნებური ჩარევისაგან დაცვა. სახელმწიფოს ამ ვალდებულების შესასრულებლად და პირადი ცხოვრების ხელშეუხებლობის უფლების უზრუნველ-

საყოფად შეიძლება დასჭირდეს გარკვეული ზომების მიღება ინდივიდთა ურთიერთობების სფეროშიც კი. სასამართლომ აღნიშნა, რომ მოცემული საქმის გარემოებები უნდა შეფასდეს კონვენციის მე-8 მუხლით დადგენილი სახელმწიფოს პოზიტიური ვალდებულების ჭრილში. მოცემულ საქმეში, ვიდეო მონიტორინგს ახორციელებდა კერძო კომპანია, შესაბამისად, სასამართლოს პოზიციით, „სახელმწიფოს მხრიდან უფლებაში ჩარევად“ ეს ქმედება ვერ განიხილებოდა. მიუხედავად იმისა, რომ კონვენციით გათვალისწინებული სახელმწიფოს პოზიტიური და ნეგატიური ვალდებულებების ზუსტი განმარტება რთულია, მოქმედი პრინციპები მაინც ერთმანეთის მსგავსია. ორივე კონტექსტში გასათვალისწინებელია, დადგინდა თუ არა სამართლიანი ბალანსი კონკურენტულ კერძო და საჯარო ინტერესებს შორის.

სასამართლომ კიდევ ერთხელ გაიმეორა, რომ გარკვეულ შემთხვევებში, მე-8 მუხლით გათვალისწინებული სახელმწიფოს პოზიტიური ვალდებულების შესასრულებლად საჭიროა სათანადო საკანონმდებლო ჩარჩოს მიღება, რათა დაცული იყოს პირადი ცხოვრების ხელშეუხებლობის უფლება.

სასამართლოს შეხედულებით, კონვენციის მე-8 მუხლით, სახელმწიფოების მიხედულების ფარგლებში შედის იმის განსაზღვრა, სამუშაო ადგილის ვიდეო მონიტორინგის საკითხს მოაწესრიგებენ თუ არა სპეციფიკური კანონმდებლობით. თუმცა, განურჩევლად სახელმწიფოს არჩევანისა, ხელისუფლებამ უნდა უზრუნველყოს, რომ დამსაქმებლის მიერ განხორციელებული მონიტორინგის ზომები არის პროპორციული და თან ახლავს უფლების ბოროტად გამოყენებისგან დაცვის ადეკვატური და საკმარისი გარანტიები.

ევროპულმა სასამართლომ აღნიშნა, რომ მოცემული საქმე უნდა შეფასდეს *Bărbulescu v. Romania*-ს საქმეში დადგენილი პრინციპების შესაბამისად და ამ კრიტერიუმების განხილვა უნდა მოხდეს შრომითი ურთიერთობებისა და ახალი, უფლებაში ჩარევის სულ უფრო მზარდი რისკის მქონე, ტექნოლოგიების სპეციფიკის გათვალისწინებით.

გამოყენებული ღონისძიების პროპორციულობის დასადგენად, ეროვნულმა სასამართლოებმა მხედველობაში უნდა მიიღონ შემდეგი ფაქტორები:

I წინასწარ იყვნენ თუ არა გაფრთხილებული თანამშრომლები სამუშაო ადგილის ვიდეო მეთვალყურეობის შესახებ. თითოეული საქმის ფაქტობრივი გარემოებების გათვალისწინებით, ეს შეტყობინება უნდა იყოს გასაგები და მონიტორინგის დაწყებამდე გაკეთებული;

II კონტროლის მოცულობა და პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევის ხარისხი. ყურადღება უნდა გამახვილდეს მეთვალყურეობის დროსა და სივრცეზე, ასევე, თუ რამდენ პირს ჰქონდა წვდომა ვიდეო მონიტორინგის შედეგებზე;

III დაასაბუთა თუ არა დამსაქმებელმა კონტროლის საჭიროება ლეგიტიმური მიზნის არსებობით. რაც უფრო ინტენსიურია უფლებაში ჩარევა, მით უფრო დამაჯერებელი უნდა იყოს დამსაქმებლის არგუმენტაცია;

IV შესაძლებელი იყო თუ არა ნაკლებად მზღუდავი კონტროლის საშუალების გამოყენება და მიიღწეოდა თუ არა ლეგიტიმური მიზანი ამ ღონისძიებების გამოყენებით;

V მონიტორინგის შედეგები, კერძოდ, დამსაქმებელმა გამოიყენა თუ არა მოპოვებული კადრები დასახული მიზნის მისაღწევად;

VI უზრუნველყოფილია თუ არა თანამშრომელი შესაბამისი დაცვის გარანტიებით. ამგვარი გარანტიები შეიძლება იყოს მაგალითად, პერსონალისთვის ინფორმაციის მიწოდება მონიტორინგის დაწყების და მასშტაბის შესახებ, მიღებული ზომების თაობაზე დამოუკიდებელი ორგანოს ინფორმირება ან საჩივრის შეტანის შესაძლებლობა.

გადაწყვეტილებაში ნათქვამია, რომ ესპანეთის პერსონალურ მონაცემთა დაცვის აქტი ითვალისწინებდა დასაქმებულთა პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვის გარანტიებს და მათი დარღვევა შესაძლებელია გამხდარიყო ადმინისტრაციული ან სამოქალაქო პასუხისმგებლობის საფუძველი. ამასთან, დასაქმების შესახებ რეგულაციები დამსაქმებელს ავალდებულებდა, რომ გამოყენებული მონიტორინგის ღონისძიება თანხვედრაში ყოფილიყო დასაქმებულთა ღირსებასთან. უფრო მეტიც, ესპანეთში მოქმედი საპროცესო კანონმდებლობა კრძალავდა ადამიანის ძირითადი უფლებების დარღვევით მოპოვებული მტკიცებულების გამოყენებას. ამ ვითარებაში, სასამართლომ აღნიშნა, რომ მოქმედი კანონმდებლობა სადავო საკითხს არ წარმოადგენდა. შესაბამისად, ის შეაფასებდა ეროვნული სასამართლოების მიერ საქმის განხილვის ხასიათს, ასევე, ეროვნულ დონეზე არსებული დაცვის სხვა გარანტიები უზრუნველყოფდნენ თუ არა მომჩივნების უფლების სათანადო დაცვას.

სასამართლომ აღნიშნა, რომ ესპანეთის საკონსტიტუციო სასამართლოს პრაქტიკის შესაბამისად, დამსაქმებელმა ვიდეო კამერები დააყენა ქურდობის გამოვლენის ლეგიტიმური მიზნის მისაღწევად, რამდენადაც კომპანია თვეების განმავლობაში განიცდიდა საქონლის დაკარგვით გამოწვეულ ფინანსურ ზარალს.

დიდმა პალატამ გაითვალისწინა ეროვნული სასამართლოების დასაბუთება მონიტორინგის მოცულობასთან დაკავშირებით, რომელიც მიუთითებდა კონტროლის დროითა და სივრცით შეზღუდვაზე - მეთვალყურეობა მხოლოდ იმ პერიოდით გაგრძელდა, რაც საჭირო იყო დარღვევის გამოსავლენად და კამერები მიმართული იყო სალარო აპარატებისაკენ, სადაც დიდი ალბათობით უნდა მომხდარიყო ქურდობის ფაქტი. სასამართლომ ასევე ხაზი გაუსვა სამუშაო ადგილის სპეციფიკას და დასძინა, რომ დასაქმებულები საქმიანობას ახორციელებდნენ საზოგადოებისთვის ღია სივრცეში, სადაც პრივატულობის ნაკლები მოლოდინი არსებობს, განსხვავებით ისეთი ადგილებისაგან, როგორიც არის მაგალითად, სველი წერტილები, გასახდელი ოთახები, დახურული სამუშაო ოფისები და სხვა. ამასთან, ირკვეოდა, რომ მოპოვებული ვიდეო კადრები, სანამ ამის შესახებ დასაქმებულებს შეატყობინებდნენ, ნახა მხოლოდ სუპერმარკეტის მენეჯერმა და ევროპის პროფესიული კავშირების კონფედერაციის წარმომადგენელმა. ამ ფაქტორებზე დაყრდნობით, სასამართლომ მიიჩნია, რომ მომჩივანთა უფლებაში ჩარევა სიმძიმის მაღალ ხარისხს ვერ აღწევდა. სასამართლომ ყურადღება გაამახვილა მონიტორინგის შედეგებზეც, რადგან სწორედ მასზე დაყრდნობით გაათავისუფლეს თანამშრომლები სამსახურიდან.

სასამართლოს შეფასებით, კომპანია ვერ მიაღწევდა მიზანს სხვა ნაკლებად მზღუდავი ღონისძიების გამოყენებით, ხოლო თანამშრომელთა წინასწარ ინფორმირება სავარაუდოდ ხელს შეუშლიდა ქურდობის ფაქტის გამოვლენას. გადაწყვეტილებაში ასევე აღნიშნულია, რომ თანამშრომლებს ინფორმაცია მიეწოდათ ხილულად დაყენებული კამერების შესახებ, სუპერმარკეტში კი ასევე განთავსებული იყო ვიდეო კონტროლის განხორციელების შესახებ ნიშანი, რომელიც მონიტორინგის შესახებ კონკრეტულ ინფორმაციას არ შეიცავდა. მონიტორინგის და მისი მასშტაბის შესახებ პირის ინფორმირება მხოლოდ ერთ-ერთი კრიტერიუმია განსახილველი ღონისძიების პროპორციულობის შესაფასებლად. თუმცა, ამგვარი ინფორმირების არარსებობის დროს, სხვა კრიტერიუმებიდან გამომდინარე დაცვის ღონისძიებები განსაკუთრებულად მნიშვნელოვანი იქნება.

სასამართლომ აღნიშნა, რომ ეროვნულმა სასამართლოებმა სწორად დაიცვეს ბალანსი პირადი ცხოვრების პატივისცემის უფლებასა და დამსაქმებლის ინტერესებს შორის, სახელმწიფოს მიხედულების ფარგლებს გაცდენის გარეშე. სასამართლოს მოსაზრებით, მხოლოდ მნიშვნელოვანი საჯარო ან კერძო ინტერესის არსებობით შეიძლება გამართლდეს კანონმდებლობით განმტკიცებული წინასწარი ინფორმირების ვალდებულების არ შესრულება. მოცემულ შემთხვევაში, საქმე ეხებოდა თვეების განმავლობაში განგრძობად დანაშაულს, რამაც სოლიდური ზიანი წარმოშვა, ასევე, არა ერთის, არამედ რამდენიმე დასაქმებულის შეთანხმებულ ქმედებას, რომელიც ზოგადად თანამშრომლების მიმართ უნდობლობას იწვევდა. დიდმა პალატამ დაასკვნა, რომ მომჩივნების პირად ცხოვრებაში ჩარევა „მძიმე დანაშაულის გონივრული ეჭვის გამო“ იყო პროპორციული და გამართლებული. შესაბამისად, არ დაადგინა კონვენციის მე-8 მუხლით გათვალისწინებული უფლების დარღვევა.

სასამართლომ ასევე გაიზიარა მთავრობის არგუმენტაცია იმის თაობაზე, რომ მომჩივნებს შეეძლოთ, კომპანიისთვის ადმინისტრაციული პასუხისმგებლობის დაკისრების მიზნით დამოუკიდებელი სააგენტოსათვის მიემართათ, ასევე, საერთო სასამართლოების მეშვეობით მოეთხოვათ კომპენსაცია პერსონალურ მონაცემთა დაცვის აქტით გათვალისწინებული მათი უფლებების დარღვევისათვის, თუმცა მათ ამ საშუალებებით არ ისარგებლეს.

საქმის შედეგი

ადამიანის უფლებათა ევროპული სასამართლოს დიდმა პალატამ 14 ხმით 3-ის წინააღმდეგ დაასკვნა, რომ მომჩივნების პირადი ცხოვრების პატივისცემის უფლება არ დარღვეულა. სასამართლომ ერთხმად გადაწყვიტა, რომ ვიდეო მონიტორინგის შედეგად მოპოვებული კადრების მტკიცებულებად გამოყენებით, ევროპული კონვენციის მე-6 მუხლი არ დარღვეულა. დიდმა პალატამ ასევე ერთხმად დაადგინა, რომ საქმის სამართლიანი განხილვის უფლება არ დარღვეულა მესამე, მეოთხე და მეხუთე მომჩივნის მიერ ხელმოწერილი მორიგების შეთანხმების აღიარებით.

მოსამართლეების დე გაეტანოს, იუდკივსკასა და გროზევის გაერთიანებული განსხვავებული აზრი

განსხვავებული აზრის ავტორი მოსამართლეები მიუთითებენ, რომ ისინი არ იზიარებენ დიდი პალატის გადაწყვეტილებას და მიიჩნევენ, რომ ეროვნულმა სასამართლოებმა ვერ დაადგინეს სამართლიანი ბალანსი დაპირისპირებულ ინტერესებს შორის. მათი შეხედულებით, ეს საქმე არის ნათელი მაგალითი იმისა, თუ როგორ იზრდება ტექნოლოგიების გავლენა ჩვენს პირად ცხოვრებაზე და სასამართლომ არა მხოლოდ უნდა აღიაროს ეს გარემოება, არამედ უნდა განავითაროს ადეკვატური დაცვის გარანტიები, რათა დაცული იყოს ინდივიდების მე-8 მუხლით გათვალისწინებული უფლება.

გადაწყვეტილებაზე დართული მოსაზრების თანხმად, ბოლო წლების განმავლობაში არსებითად შეიცვალა და განვითარდა ვიდეო მეთვალყურეობის ტექნოლოგიები, რაც პოტენციურად ზრდის პირადი ცხოვრების პატივისცემის უფლების დარღვევის რისკებს. სწორედ ამიტომ, ეროვნულ დონეზე არსებული ელექტრონული მეთვალყურეობის მარეგულირებელი საკანონმდებლო ჩარჩო უნდა იყოს მკაფიო და განჭვრეტადი. აღნიშნული განსაკუთრებით დიდ მნიშვნელობას იძენს წინამდებარე საქმეში, როცა დამსაქმებელი ახორციელებს ფარულ ვიდეო კონტროლს სამუშაო ადგილზე. მოსამართლეები ფიქრობენ, რომ რიგ შემთხვევაში, ეროვნული სასამართლოებისათვის კონფლიქტის გადაწყვეტისათვის თავისუფალი მოქმედების შესაძლებლობის მიცემა დასაშვებია, თუმცა არა მაშინ, როცა საქმე ელექტრონულ მეთვალყურეობას ეხება. ამრიგად, მოსამართლეები ამ სპეციფიკურ საქმეზე შეუთანხმებლობის მიზეზად დიდი პალატის მიერ ეროვნულ დონეზე სასამართლოების რეაგირების მოწონებას ასახელებენ.

განსხვავებული მოსაზრების თანახმად, კანონმდებლობა ერთადერთ დაცვის გარანტიას - წინასწარი ინფორმირების ვალდებულებას ითვალისწინებდა ყოველგვარი გამონაკლისის გარეშე, რასაც გადამწვეტი მნიშვნელობა ჰქონდა მოცემული საქმისათვის. ეს საკანონმდებლო ჩანაწერი განსაკუთრებით მნიშვნელოვანია შრომით ურთიერთობებში, როდესაც დამსაქმებელი დასაქმებულთან შედარებით ბევრად მეტი ძალაუფლებით სარგებლობს. ვიდეო მეთვალყურეობის შესახებ ინფორმირება არსებითია იმისათვის, რომ პირს ჰქონდეს შესაძლებლობა, მოითხოვოს პერსონალურ მონაცემებზე წვდომა, მათი შესწორება ან წაშლა. მოსამართლეთა შეხედულებით, ეროვნულ დონეზე უფლებათა შორის სამართლიანი ბალანსის ვერ დადგენაზე ყველაზე კარგად მიუთითებს სახელმწიფო დონეზე არსებული კანონმდებლობის ანალიზი. უმრავლესობა შეთანხმდა, რომ ესპანეთის კანონმდებლობა მოითხოვდა ამ კატეგორიის პერსონალურ მონაცემთა დამუშავებამდე მონაცემთა სუბიექტის წინასწარ ინფორმირებას, რაც ცალსახად შეიძლება ითქვას, რომ ამ შემთხვევაში არ შესრულებულა. ჩარევის პროპორციულობის შეფასებისას, ტრიბუნალს არც უმსჯელია წინასწარი ინფორმირების ვალდებულების დარღვევაზე, ეროვნულმა სასამართლოებმა არ მიიღეს მხედველობაში საქმის ინდივიდუალური მახასიათებლები და არ შევიდნენ მის დეტალურ განხილვაში. ამასთან, სასამართლოებმა დაასკვნეს, რომ ფარული ვიდეო კონტროლი იყო აუცილებელი ღონისძიება, რომელიც ლეგიტიმური მიზნის მიღწევის შესაძლებლობას იძლეოდა, თუმცა არ იმსჯელეს ნაკლებად მზღუდავი საშუალებების გამოყენების შესახებ.

განსხვავებული მოსაზრების ავტორ მოსამართლეთა პოზიციით, გამომდინარე იქედან, რომ საქმე ეხებოდა სისხლის სამართლის კანონმდებლობით დასჯად ქმედებას, დამსაქმებელს პირველ რიგში, უნდა მიემართა პოლიციისათვის და საკუთარი ინიციატივით არ უნდა მიეღო მსგავსი ზომები. დანაშაულის გამოვლენის საჭიროება არ ამართლებს კერძო გამოძიების ჩატარებას, მით უფრო, თუ ეს ფარული მეთვალყურეობის ფორმით ხდება და წარმოადგენს სხვის პირად ცხოვრებაში უხეშ ჩარევას. ამ მიდგომის გაუკიცხაობით, სტრასბურგის სასამართლო ახალისებს კერძო პირებს, საკუთარ თავზე აიღონ სამართლებრივი ღონისძიებების განხორციელება, მაშინ როდესაც სწორედ ამგვარ სიტუაციებში არის საჭირო კომპეტენტური ორგანოს მოქმედება.

„მძიმე დანაშაულის გონივრული ეჭვის“ საფუძველზე უფლებაში ამგვარი ჩარევის დიდი პალატის მიერ გამართლება მოსამართლეებმა გააკრიტიკეს და მიუთითეს, რომ მკაფიო კრიტერიუმის არარსებობის გამო, შესაძლებელია მსგავსი მიდგომა ბევრ შემთხვევაში გაუმართლებლად იყოს გამოყენებული. „მნიშვნელოვანი ეჭვი“ ელექტრონული მეთვალყურების შემთხვევაში ვერ იქნება საკმარისი დაცვის გარანტია.

მონაცემთა სუბიექტს უნდა ჰქონოდა მისი გამოსახულების დამუშავებისა და გამოყენების შესახებ წინასწარი ინფორმაცია, თუმცა, სამწუხაროდ, თანამშრომლების ინფორმირება ვიდეო მონიტორინგის დაწყებამდე არ მომხდარა.

კიდევ ერთი საკითხი, რაც კრიტიკის საგანი გახდა, იყო უმრავლესობის მსჯელობა ვიდეო მონიტორინგის შედეგებზე, რომლის მიხედვითაც, მოპოვებული პერონალური მონაცემები მხოლოდ ლეგიტიმური მიზნის მისაღწევად გამოიყენეს. სამი მოსამართლის შეხედულებით, თანამედროვე ტექნოლოგიების ფართო შესაძლებლობების გათვალისწინებით, პერსონალურ მონაცემთა შეგროვებისა და გამოყენების შედეგები სასამართლოს სათანადოდ არ შეუფასებია.

განსხვავებული აზრის მიხედვით, ესპანეთის ეროვნულმა სასამართლოებმა და ადამიანის უფლებათა ევროპულმა სასამართლომ ვერ დაადგინეს სამართლიანი ბალანსი უფლებებს შორის და ამ მიდგომით წაახალისეს სამუშაო ადგილზე ფარული ვიდეო მეთვალყურეობის შეუზღუდავი გამოყენება.

SZABÓ AND VISSY V. HUNGARY

12/01/2016

ფაქტობრივი გარემოებები

2014 წელს უნგრეთის მოქალაქეებმა - მათე საბომ და ბეატრიქს ვისიმ (შემდგომ - „მომჩივნებმა“) ადამიანის უფლებათა ევროპულ სასამართლოს (შემდგომ „სასამართლო“) მიმართეს იმ საფუძვლით, რომ მათ მიმართ შესაძლოა განხორციელებულიყო გაუმართლებელი და არაპროპორციული ფარული მეთვალყურეობის ღონისძიებები, სასამართლო კონტროლის გარეშე.

უნგრეთის კანონმდებლობით ფარული მეთვალყურეობის ნებართვის გაცემის პროცედურა დამოკიდებული იყო იმაზე, ღონისძიება მიემართებოდა კანონით გათვალისწინებული კონკრეტული დანაშაულის გამოძიებას თუ ეროვნული უსაფრთხოების უზრუნველსაყოფად მონაცემების შეგროვებას. პირველ შემთხვევაში, კანონი ითვალისწინებდა სასამართლოს წინასწარ ნებართვას, ხოლო მეორე შემთხვევაში თანხმობას იუსტიციის მინისტრი გასცემდა. გამოძიების მიზნით ფარული მეთვალყურეობის განხორციელება დამოკიდებული იყო ცალკეული მძიმე დანაშაულების შესახებ ეჭვის არსებობაზე, ხოლო ეროვნული უსაფრთხოების უზრუნველყოფის მიზნით ამ ღონისძიებების გამოყენებას კანონმდებლობა კონკრეტული გარემოებების არსებობას არ უკავშირებდა.

კანონი ადგენდა ეროვნული უსაფრთხოების მიზნით მეთვალყურეობის ვადას - 90 დღეს, ასევე ითვალისწინებდა ამ ვადის დამატებით 90 დღით გაგრძელებას მინისტრის მიერ. თუმცა, ვადის გაგრძელების შესახებ გადაწყვეტილების მიღებისას იუსტიციის მინისტრი არ იყო ინფორმირებული მიმდინარე მეთვალყურეობის შედეგების შესახებ. გარდა ამისა, მეთვალყურეობის ღონისძიების დასრულების შემდეგ კანონმდებლობა არ ითვალისწინებდა არარელევანტური ინფორმაციის განადგურების ვალდებულებას.

2012 წელს მომჩივნებმა საკონსტიტუციო სარჩელით მიმართეს ადგილობრივ სასამართლოს, რადგან მიიჩნევდნენ, რომ ამგვარი რეგულირება კონსტიტუციით გარანტირებულ პირადი ცხოვრების ხელშეუხებლობის უფლებას არღვევდა. საკონსტიტუციო სასამართლომ არ გაიზიარა მათი არგუმენტების უმრავლესობა და მოსარჩელეებს მხოლოდ იმ ნაწილში დაეთანხმა, რომ მინისტრის გადაწყვეტილება დასაბუთებული უნდა ყოფილიყო. სასამართლომ აღნიშნა, რომ ეროვნულ უსაფრთხოებასთან დაკავშირებული ამოცანების ფარგლები იყო უფრო ფართო და ამ მიზნით გარკვეული მოვლენების შეფასება შესაძლოა არც ყოფილიყო დაკავშირებული კონკრეტულ დანაშაულთან. გარდა ამისა, საკონსტიტუციო სასამართლომ ყურადღება გაამახვილა პარლამენტის ეროვნული უსაფრთხოების კომიტეტისა (რომელსაც შეეძლო მინისტრის დაბარება ანგარიშის მოსასმენად) და ომბუდსმენის მიერ განხორციელებულ გარე კონტროლზე და მიიჩნია, რომ ამგვარი რეგულირება საკმარისად უზრუნველყოფდა პირადი ცხოვრების ხელშეუხებლობის დაცვას. სასამართლომ ასევე აღნიშნა, რომ ეროვნული უსაფრთხოების აქტი შეიცავდა არასაჭირო მონაცემების წაშლის შესახებ ზოგად დებულებებს.

მომჩივნები მიიჩნევდნენ, რომ დაირღვა ადამიანის უფლებათა ევროპული კონვენციით (შემდგომ - „კონვენცია“) გარანტირებული მე-8 (პირადი და ოჯახური ცხოვრების დაცულობის უფლება), მე-6 (საქმის სამართლიანი განხილვის უფლება) და მე-13 (სამართლებრივი დაცვის ქმედითი საშუალების უფლება) მუხლები.

მომჩივნების არგუმენტაცია

მომჩივნები აღნიშნავდნენ, რომ ფარული მეთვალყურეობის ღონისძიებების გამოყენების წინაპირობები და დაზვერვის მონაცემების შეგროვების მეთოდები კანონით მკაფიოდ არ იყო განსაზღვრული და სასამართლო კონტროლის არარსებობის გათვალისწინებით, ამას შესაძლოა გადაწყვეტილებების თვითნებურად მიღება გამოეწვია.

მომჩივნებმა ყურადღება გაამახვილეს უსაფრთხოების სამსახურების დემოკრატიული ზედამხედველობის შესახებ ვენეციის კომისიის ანგარიშზე (CDL-AD(2007)016) და აღნიშნეს, რომ ამ დოკუმენტის გათვალისწინებით, არ შეიძლებოდა იმის მტკიცება, რომ ეროვნული უსაფრთხოების უზრუნველსაყოფად ფარული მეთვალყურეობის განხორციელებისას სასამართლო კონტროლი ნაკლებად შესაფერისი კონტროლის მექანიზმია. აღნიშნული ანგარიშის რეალური დასკვნა იყო ის, რომ უსაფრთხოების სამსახურების კონტროლის მხოლოდ კომპლექსურ მოწყობას შეუძლია ინდივიდების სათანადოდ დაცვა. ვენეციის კომისიის ანგარიშის თანახმად, „სასამართლო კონტროლის ეფექტურობის უზრუნველსაყოფად მოსამართლეები უნდა იყვნენ დამოუკიდებელი და გააჩნდეთ სპეციალური ცოდნა.“

მომჩივნებმა ასევე აღნიშნეს, რომ მონაცემთა დაცვის ომბუდსმენი და ეროვნული უსაფრთხოების საპარლამენტო კომიტეტი ვერ ჩაანაცვლებდა სასამართლო კონტროლს, რადგან ისინი წარმოადგენდა ზედამხედველობის მექანიზმებს, რაც გავლენას ვერ ახდენდა კონკრეტულ შემთხვევებზე. ამ ორი ორგანოსადმი მიმართვის საფუძველზე, მომჩივნებმა გამოარკვიეს, რომ არცერთ მათგანს არ ქონია შეხება მოქალაქეთა მეთვალყურეობის შემთხვევებთან. შესაბამისად, კონტროლის ეს პოტენციური მექანიზმები ეფექტური არ იყო.

მთავრობის არგუმენტაცია

სასამართლოს ნებართვის აუცილებლობასთან დაკავშირებით მთავრობამ მიუთითა უსაფრთხოების სამსახურების დემოკრატიული ზედამხედველობის შესახებ ვენეციის კომისიის ანგარიშზე. ამ ანგარიშის ცალკეულ მოსაზრებებზე დაყრდნობით, მოპასუხემ აღნიშნა, რომ ადგილობრივ სასამართლოებს არ შეუძლიათ ეროვნული უსაფრთხოების უზრუნველსაყოფად ინფორმაციის ფარულად შეგროვების აუცილებლობის განსაზღვრა მონაცემთა ბუნების, რისკის შეფასების სუბიექტურობის, ეროვნული უსაფრთხოების ცნების პოლიტიკური ხასიათისა და მთავრობისთვის მინიჭებული ფართო მიხედულების გათვალისწინებით.

მთავრობის თანახმად, მოსამართლე აფასებს შეთავაზებული ღონისძიების შესაბამისობას პოზიტიური სამართლიდან გამომდინარე ნორმებთან. უსაფრთხოების უზრუნველსაყოფად ფარული მეთვალყურეობის განხორციელებაზე ნებართვის გაცემასთან დაკავშირებით არ არსებობს და ვერც იარსებებს ზუსტი კრიტერიუმების დამდგენი კანონმდებლობა, რაზეც სასამართლო გადაწყვეტილებას დააფუძნებს. ეს განპირობებულია იმით, რომ გადაწყვეტილება, რომლის მიმღებს აქვს პოლიტიკური პასუხისმგებლობა, მიღებულ უნდა იქნას ქვეყნის უსაფრთხოების ინტერესების შეფასების საფუძველზე, ასევე ქვეყნის შიგნით და გარეთ არსებული პოლიტიკური ასპექტების მხედველობაში მიღებით. შესაბამისად, ამგვარი გადაწყვეტილებების მისაღებად იუსტიციის მინისტრი - პოლიტიკური პასუხისმგებლობის მქონე პირი - არის უფრო მეტად კვალიფიციური, ვიდრე მოსამართლეები.

მთავრობამ ასევე აღნიშნა, რომ იუსტიციის მინისტრის მიერ თანხმობის გაცემას ყოველთვის აკონტროლებდა ეროვნული უსაფრთხოების საპარლამენტო კომიტეტი და მონაცემთა დაცვის ომბუდსმენი. გარდა ამისა, არ არსებობდა არავითარი ნიშნები იმისა, რომ ნებართვის გაცემის მექანიზმი იყო ფორმალური ან თვითნებური.

მესამე მხარეთა მოსაზრებები

სასამართლოს გადაწყვეტილებაში ასახულია მესამე მხარეების - დემოკრატიისა და ტექნოლოგიის ცენტრისა (CDT) და Privacy International-ის მოსაზრებები.

ა. *დემოკრატიისა და ტექნოლოგიის ცენტრის (CDT) მოსაზრებები*

დემოკრატიისა და ტექნოლოგიის ცენტრმა ყურადღება გაამახვილა თანამედროვე მეთვალყურეობის სისტემების განვითარებულ შესაძლებლობებზე, ასევე მოპოვებული მონაცემებით ინდივიდის საქმიანობისა და ურთიერთობების შესახებ დეტალური პროფილის შექმნის საშუალებაზე. მასობრივი მეთვალყურეობისა და მოპოვებული მონაცემების რთული ანალიზის გარდა, სახელმწიფოებს ასევე შეუძლიათ კონკრეტული პირების მიმართ მიზნობრივი მეთვალყურეობა განახორციელონ, მათ შორის მოწყობილობებში დისტანციურად საზიანო პროგრამული უზრუნველყოფის ინსტალირების გზით, რაც შესაბამის სამსახურებს შესაძლებლობას აძლევს ფარულად ჩაწერონ ხმა, ფოტოები და ვიდეოები.

დემოკრატიისა და ტექნოლოგიის ცენტრის თანახმად, კონვენციის მე-8 მუხლი ეროვნული უსაფრთხოების უზრუნველსაყოფად განხორციელებულ ფარულ მეთვალყურეობაზე სასამართლო ზედამხედველობას მოითხოვს. ცენტრი ასევე აღნიშნავდა, რომ ფარული მეთვალყურეობის ყველა მსხვერპლისთვის უზრუნველყოფილი უნდა იყოს ეფექტური სამართლებრივი დაცვის საშუალება.

ბ. *Privacy International-ის მოსაზრებები*

Privacy International-მა მიმოიხილა როგორც ადამიანის უფლებათა ევროპული სასამართლოს, ისე ევროპის, კანადისა და ამერიკის შეერთებული შტატების ეროვნული

სასამართლოების პრაქტიკა, რაც ხაზს უსვამს მეთვალყურეობის ღონისძიებებზე სასამართლო კონტროლის ან სასამართლო ნებართვის აუცილებლობას. გარდა ამისა, ორგანიზაციამ მიმოიხილა ადამიანის უფლებათა საერთაშორისო სტანდარტები, რომლებიც ადასტურებს სასამართლო კონტროლისა და ეფექტური სამართლებრივი დაცვის საშუალების საჭიროებას.

სასამართლოს შეფასება

უნგრეთის ეროვნული უსაფრთხოების აქტით გათვალისწინებული ზომები, კერძოდ მეთვალყურეობა საცხოვრებელ სახლზე, საფოსტო გზავნილებისა და ამანათების შემოწმება, ელექტრონული კომუნიკაციებისა და კომპიუტერული მონაცემების გადაცემის მონიტორინგი და ამ მეთოდებით მოპოვებული მონაცემების ჩანაწერის გაკეთება შესაძლებელია განხილულ იქნას კონვენციის მე-8 მუხლით გათვალისწინებული „პირადი ცხოვრების“, „საცხოვრისისა“ და „მიმოწერის“ ცნების ფარგლებში, რასაც მხარეები სადავოდ არ ხდიან.

კონვენციის მე-8 მუხლის მე-2 პუნქტის თანახმად, პირადი ცხოვრების ხელშეუხებლობის უფლების განხორციელებაში ჩარევა შესაძლოა გამართლებული იყოს მხოლოდ მაშინ, თუ ის ხორციელდება კანონის შესაბამისად, ემსახურება ერთ ან მეტ ლეგიტიმურ მიზანს და აუცილებელია დემოკრატიულ საზოგადოებაში ამ მიზნის მისაღწევად.

მოცემულ შემთხვევაში, ჩარევის მიზანია ეროვნული უსაფრთხოების უზრუნველყოფა ან/და უწესრიგობისა და დანაშაულის თავიდან აცილება, რასაც მხარეები სადავოდ არ ხდიან. მეორე მხრივ, უნდა დადგინდეს ამ მიზნის მისაღწევად კანონმდებლობით გათვალისწინებული საშუალებები არის თუ არა აუცილებელი დემოკრატიულ საზოგადოებაში.

ევროპულმა სასამართლომ თავის პრაქტიკაში ფარულ მეთვალყურეობასთან დაკავშირებით კანონით გასათვალისწინებელი შემდეგი მინიმალური გარანტიები განსაზღვრა, რაც უფლებამოსილების ბოროტად გამოყენების თავიდან აცილებას ემსახურება: იმ დანაშაულთა ბუნება, რასთან დაკავშირებითაც შეიძლება გაიცეს ფარული მიყურადების ბრძანება; პირთა იმ კატეგორიის განსაზღვრა, რომელთა სატელეფონო საუბრის მიყურადება შესაძლოა განხორციელდეს; სატელეფონო მიყურადების ხანგრძლივობის შეზღუდვა; მოპოვებული მონაცემების შესწავლის, გამოყენებისა და შენახვის პროცედურა; სხვა პირებისათვის მონაცემების გაზიარებასთან დაკავშირებული სიფრთხილის ზომები; გარემოებები, როდესაც ჩანაწერები შესაძლოა ან უნდა წაიშალოს/განადგურდეს.

ეროვნული უსაფრთხოების ლეგიტიმური მიზნის მისაღწევი მეთოდების შერჩევისას სახელმწიფოები გარკვეული მიხედულების ფარგლებით სარგებლობენ. თუმცა, არსებობს რისკი ეროვნული უსაფრთხოების უზრუნველსაყოფად შექმნილმა ფარული მეთვალყურეობის სისტემამ, დემოკრატიის დაცვის სახელით, პირიქით საფრთხე შეუქმნას დემოკრატიას. აქედან გამომდინარე, სასამართლომ უნდა დაადგინოს, არსებობს თუ არა სათანადო ეფექტური გარანტიები უფლებამოსილების ბოროტად გამოყენების თავიდან ასაცილებლად.

ევროპულმა სასამართლომ შეაფასა უნგრეთის კანონმდებლობა და ფარული მეთვალყურეობის სისტემაში გათვალისწინებული გარანტიები და არა მომჩივნებთან დაკავშირებით მიღებული კონკრეტული ზომების პროპორციულობა.

ტერმინი „კანონის შესაბამისად“ მოითხოვს, რომ ღონისძიებას ჰქონდეს საკანონმდებლო საფუძველი. ის ასევე მოიაზრებს კანონის ხარისხს და მოითხოვს, რომ დაცული უნდა იყოს კანონის უზენაესობის პრინციპი და კანონი ხელმისაწვდომი იყოს კონკრეტული პირებისთვის, რომელთაც შეუძლიათ წინასწარ განსაზღვროს მისი შედეგები. მოცემულ საქმეში ჩარევას ჰქონდა საკანონმდებლო საფუძველი და კანონის ხელმისაწვდომობა ეჭვქვეშ არ დამდგარა. თუმცა, მომჩივნები აღნიშნავდნენ, რომ კანონი არ იყო საკმარისად დეტალური და ზუსტი, შესაბამისად, ვერ აკმაყოფილებდა განჭვრეტადობის მოთხოვნას, რადგან უფლებამოსილების ბოროტად გამოყენებისა და თვითნებობის თავიდან ასაცილებლად საკმარის გარანტიებს ვერ უზრუნველყოფდა.

სასამართლოს თანახმად, აღმასრულებელი ხელისუფლებისთვის მინიჭებული უფლებამოსილების ფარულად განხორციელებისას თვითნებობის რისკები აშკარაა. ეროვნული კანონმდებლობა უნდა იყოს საკმარისად ცხადი იმისთვის, რომ მოქალაქეებმა იცოდნენ, რა შემთხვევაში და რა პირობებით შეიძლება საჯარო დაწესებულებამ ამგვარი ღონისძიებები გამოიყენოს.

მოცემულ საქმეში, ფარული მეთვალყურეობა ორ სიტუაციაში ხორციელდება: უნგრეთში ტერორისტული აქტების თავიდან ასაცილებლად, გამოსავლენად და აღსაკვეთად, ასევე საზღვარგარეთ მყოფი უნგრეთის მოქალაქეების გადარჩენის მიზნით დაზვერვის მონაცემების შესაგროვებლად.

სასამართლომ აღნიშნა, რომ სადავო ნორმის საფუძველზე ფაქტობრივად ნებისმიერი ადამიანი შეიძლება ფარულ მეთვალყურეობას დაექვემდებაროს. კანონმდებლობა არ უთითებს ადამიანების კატეგორიას, რომელთა მიმართ შესაძლოა მოსმენა განხორციელდეს. სასამართლოს შეფასებით, არსებული ჩანაწერი მეტისმეტად ფართოა, რადგან კანონი არ მოითხოვს, რომ ნაჩვენები უნდა იყოს რეალური ან სავარაუდო კავშირი შესაბამის ადამიანებსა და ტერორისტული საფრთხის თავიდან აცილებას შორის. შესაბამისად, ნებართვის გამცემი ვერ გააანალიზებს მიზნის მისაღწევად გამოყენებული საშუალებები არის თუ არა მკაცრად აუცილებელი.

სასამართლოს თანახმად, ტერორიზმის თანამედროვე ფორმების გათვალისწინებით, ბუნებრივია, რომ სახელმწიფოები ამგვარი აქტების თავიდან ასაცილებლად მოწინავე ტექნოლოგიებს იყენებენ, მათ შორის იმ კომუნიკაციების მასობრივ მონიტორინგს, რაც შესაძლოა მოახლოებული ინციდენტების შესახებ ინფორმაციას შეიცავდეს. მონიტორინგის პროცესში გამოყენებულმა ტექნიკამ იმდენად თვალსაჩინო პროგრესი განიცადა და იმ დონის სირთულეს მიაღწია, რომ რიგითი მოქალაქისთვის ამგვარი სისტემა შესაძლოა რთულად აღსაქმელი იყოს, მითუმეტეს, რომ მონაცემთა ავტომატური და სისტემური დამუშავება ტექნიკურად შესაძლებელი და ფართოდ გავრცელებულია. სასამართლომ უნდა შეაფასოს, მეთვალყურეობის მეთოდების ამგვარ განვითარებას თან ახლავს თუ არა სამართლებრივი გარანტიების განვითარებაც, რაც აუცილებელია კონვენციით გარანტირებული უფლებების დასაცავად.

მოცემულ შემთხვევაში, სასამართლო ვერ დარწმუნდა, რომ ეროვნულ უსაფრთხოებასთან დაკავშირებული ფუნქციების განხორციელების პროცესში კანონმდებლობა მისაღწევი მიზნისა და გამოყენებული საშუალებების სათანადო ანალიზის შესაძლებლობას იძლევა. ჩანაწერი იმის თაობაზე, რომ შესაბამისმა ორგანოებმა უნდა დაასაბუთონ ფარული მეთვალყურეობის ჩატარების მოთხოვნა, ვერ აკმაყოფილებს მკაცრი აუცილებლობის შეფასების მოთხოვნას. კანონმდებლობა არ ითვალისწინებს დამხმარე მასალების ან საკმარისი ფაქტობრივი საფუძვლების წარმოდგენის ვალდებულებას, რაც სამიზნე პირის მიმართ ინდივიდუალური ეჭვის არსებობის საფუძველზე, შეთავაზებული ღონისძიების აუცილებლობის შეფასებას უზრუნველყოფს. მხოლოდ ამგვარი ინფორმაციის წარმოდგენა მისცემს ნებართვის გამცემს სათანადო პროპორციულობის ტესტის გამოყენების შესაძლებლობას.

უნგრეთის ეროვნული უსაფრთხოების აქტი ითვალისწინებს პერიოდს, რომლის გასვლის შემდეგ ფარული მეთვალყურეობის ნებართვა ძალას კარგავს (მაქსიმუმ 90 დღე), ასევე უთითებს პირობებს, რომლის არსებობისას შესაძლებელია ნებართვის განახლება. შესაბამისი სამსახურის დასაბუთებული წინადადების საფუძველზე, მინისტრი გადაწყვეტილებას იღებს ვადის გაგრძელების თაობაზე. სასამართლომ აღნიშნა, რომ კანონში ბუნდოვანია, მეთვალყურეობის ნებართვის ამგვარი განახლება დასაშვებია ერთჯერადად თუ რამდენჯერმე, რაც უფლებამოსილების ბოროტად გამოყენების რისკის კიდევ ერთი ელემენტია.

ევროპულმა სასამართლომ ხაზი გაუსვა ფარული მიყურადების განსახორციელებლად წინასწარი სასამართლო ნებართვის მნიშვნელობას სამართალდამცავი ორგანოების დისკრეციის შესაზღუდად. მოცემულ შემთხვევაში, როგორც ნებართვის გაცემის, ასევე ფარული მეთვალყურეობის ღონისძიების ჩატარების ეტაპზე მთავარი პრობლემური საკითხი სასამართლო კონტროლის არარსებობაა. ევროპული სასამართლოს თანახმად, იუსტიციის მინისტრის ზედამხედველობა, რაც აშკარად პოლიტიკური ხასიათისაა, ვერ უზრუნველყოფს მკაცრი აუცილებლობის სათანადო შეფასებას. ნებართვის გაცემისა და ზედამხედველობის პოლიტიკური ხასიათი უფლებამოსილების ბოროტად გამოყენების რისკს აძლიერებს.

ფარული მეთვალყურეობის ღონისძიებების როგორც ზოგადი, ისე ინდივიდუალური შემთხვევების გარე კონტროლი (უმჯობესია სასამართლო კონტროლი) განსაკუთრებულ მნიშვნელობას იძენს, რადგან განამტკიცებს მოქალაქეების ნდობას, რომ კანონის უზენაესობის გარანტიები დაცულია და უფლების დაცვის მექანიზმები უზრუნველყოფილია.

ევროპულმა სასამართლომ ყურადღება გაამახვილა აღმასრულებელი ხელისუფლების მიერ საპარლამენტო კომიტეტისათვის ანგარიშის წარდგენაზე, რაც დაკავშირებულია ზოგად ვითარებასთან და არა ინდივიდუალურ შემთხვევებთან. სასამართლომ ასევე აღნიშნა, რომ უნგრეთის კანონმდებლობაში არ არის ჩანაწერი, რაც სამართლებრივი დაცვის საშუალებას უზრუნველყოფს იმ პირებისთვის, რომელთა მიმართ ფარული მეთვალყურეობა განხორციელდა, თუმცა ამის შესახებ ინფორმირებული არ არიან. მინისტრი ვალდებულია შესაბამის კომიტეტს წელიწადში არანაკლებ ორჯერ ეროვნული უსაფრთხოების სამსახურების ფუნქციონირებაზე ზოგადი ანგარიში წარუდგინოს. თუმცა, ეს ანგარიში არ არის საზოგადოებისთვის ხელმისაწვდომი, რაც საზოგადოებრივი კონტროლის სათანადო გარანტიებს ვერ უზრუნველყოფს. უნგრეთის კანონმდებლობით კომიტეტი უფლებამოსილია საკუთარი ინიცი-

ატივით მინისტრისა და შესაბამისი სამსახურების ხელმძღვანელებისგან ინფორმაცია მოითხოვოს. თუმცა, ამგვარი ზედამხედველობა ვერ უზრუნველყოფს ფარული მეთვალყურეობის შედეგად ინდივიდუალური დარღვევის შემთხვევაში უფლების დაცვის გარანტიებს, ასევე შესაბამისი ორგანოების ყოველდღიური საქმიანობის ეფექტურ კონტროლს, განსაკუთრებით იმის გათვალისწინებით, რომ კომიტეტს არ აქვს სათანადო დოკუმენტებზე დეტალური წვდომა. შესაბამისად, ამგვარი ზედამხედველობის ფარგლები შეზღუდულია.

გარდა ამისა, არაეფექტურია ეროვნული უსაფრთხოების აქტით გათვალისწინებული გასაჩივრების პროცედურაც, რადგან იმ პირებმა, ვის მიმართაც ფარული მეთვალყურეობა განხორციელდა, არც იციან მათ მიმართ გამოყენებული ღონისძიების შესახებ.

ევროპულმა სასამართლომ აღნიშნა, რომ განხორციელებული ფარული მეთვალყურეობის შესახებ შემდგომი შეტყობინება მჭიდრო კავშირშია უფლების სამართლებრივი დაცვის საშუალებებთან, შესაბამისად, უფლებამოსილების ბოროტად გამოყენების თავიდან აცილების გარანტიების არსებობასთან. თუკი იმ მიზანს, რისთვისაც მეთვალყურეობა განხორციელდა, საფრთხე აღარ ექმნება, შესაბამის პირებს უნდა ეცნობოთ მათ მიმართ გატარებული ღონისძიებების შესახებ. უნგრეთის კანონმდებლობა არ ითვალისწინებს ამგვარი შეტყობინების არავითარ სახეს, რაც უფლების დაცვის საშუალების არარსებობასთან ერთად ცხადყოფს, რომ კანონმდებლობა ამ კუთხით სათანადო გარანტიებს ვერ უზრუნველყოფს.

საბოლოო ჯამში, სასამართლომ დაადგინა, რომ უნგრეთის კანონმდებლობით ფარული მეთვალყურეობის ღონისძიებები შესაძლოა ნებისმიერ პირს შეეხოს, ხორციელდება აღმასრულებელი ხელისუფლების მიერ და მკაცრი აუცილებლობის შეფასების გარეშე, ახალი ტექნოლოგიები სახელმწიფოს შესაძლებლობას აძლევს მასობრივად შეაგროვოს მონაცემები და არ არსებობს სამართლებრივი დაცვის ეფექტური საშუალება, რომ არაფერი ვთქვათ სასამართლოს მეშვეობით უფლების დაცვის შესაძლებლობაზე. შესაბამისად, ევროპულმა სასამართლომ დაადგინა, რომ დაირღვა კონვენციის მე-8 მუხლი.

საქმის შედეგი

ადამიანის უფლებათა ევროპულმა სასამართლომ ერთხმად დაადგინა კონვენციის მე-8 მუხლის - პირადი და ოჯახური ცხოვრების დაცულობის უფლების დარღვევა. სასამართლომ აღნიშნა, რომ არ დარღვეულა მე-13 მუხლი (სამართლებრივი დაცვის ქმედითი საშუალების უფლება) მე-8 მუხლთან ერთობლიობაში, ასევე მე-8 მუხლთან დაკავშირებით მიღებული გადაწყვეტილების გათვალისწინებით, საჭიროდ არ მიიჩნია კონვენციის მე-6 მუხლის (საქმის სამართლიანი განხილვის უფლება) საფუძველზე განაცხადის განხილვა.

სასამართლომ ჩათვალა, რომ უფლების დარღვევის დადგენა წარმოადგენდა მოთხოვნის საკმარის და სამართლიან დაკმაყოფილებას და მომჩივნებისთვის ზიანის ანაზღაურება საჭიროდ არ მიიჩნია.

მოსამართლე პინტო დე ალბუქერქეს თანმხვედრი აზრი

სასამართლოს გადაწყვეტილებას ერთვის მოსამართლე პინტო დე ალბუქერქეს თანმხვედრი აზრი, რომლის თანახმად, მოცემულ შემთხვევაში, პალატამ არ იხელმძღვანელა მასობრივ მეთვალყურეობასთან დაკავშირებული ევროპული სტანდარტით, რაც დიდმა პალატამ დაადგინა საქმეში *ჰომან ზახახოვი ჰუსეთის წინააღმდეგ.*

მოსამართლის თანახმად, უნგრეთის ეროვნული უსაფრთხოების აქტი არ მოითხოვს, რომ იმ პირებთან დაკავშირებით, ვის მიმართაც მონიტორინგი ხორციელდება, უნდა არსებობდეს „გონივრული ეჭვის“ სტანდარტი. არსებული ჩანაწერი მინისტრს შეუზღუდავ დისკრეციას ანიჭებს და „სტრატეგიული, ფართომასშტაბიანი მიყურადების“ შესაძლებლობას ქმნის. პინტო და ალბუქერქე აღნიშნავს, რომ პალატამ გადაწყვეტილების დასაბუთებაში უფრო დაბალი სტანდარტი - „ინდივიდუალური ეჭვი“ აირჩია, რაც მნიშვნელოვნად ამცირებს დაცვის იმ ხარისხს, რაც *ჰომან ზახახოვის* საქმეში, ხოლო მანამდე საქმეში *იოხდაჩი და სხვები მოლდოვის წინააღმდეგ დადგინდა.*

ევროპული სასამართლოს პალატისა და საკონსტიტუციო სასამართლოს გადაწყვეტილების დასაბუთება ეფუძნება იმ დაშვებას, რომ ეროვნული უსაფრთხოების დაცვა არ შემოიფარგლება წარსული, მიმდინარე ან სამომავლო დანაშაულის გამოძიებით და შესაბამისად, „გონივრული ეჭვის“ კრიტერიუმზე უარი უნდა ითქვას. მოცემულ შემთხვევაში, ევროპულმა სასამართლომ დიდი პალატის „ინდივიდუალური ეჭვის“ კრიტერიუმი არ გაიზიარა იმ მიზეზით, რომ ტერორიზმთან ბრძოლა მოითხოვს დიდი ოდენობით ინფორმაციას შეგროვებასა და მასობრივი მონაცემების დამუშავებას პოტენციურად თითოეული ადამიანის შესახებ, რომელიც შესაძლოა დაკავშირებული იყოს საეჭვო სუბიექტებთან ან დაგეგმილი ტერორისტული შეტევების ობიექტებთან. მოსამართლე პინტო დე ალბუქერქემ მოცემულ შემთხვევაში ამგვარი დაშვება არასწორად მიიჩნია.

პალატის გადაწყვეტილებაში საუბარია „მკაცრი აუცილებლობის“ ტესტზე, რაც ორ მიზანს უკავშირდება: დემოკრატიული ინსტიტუტების დაცვასა და ინდივიდუალურ ოპერაციაში მნიშვნელოვანი დაზვერვის მონაცემების მოპოვებას. ალბუქერქეს აზრით, სამართლებრივი ტესტის ამგვარი ფორმულირება რამდენიმე პრობლემას წარმოშობს. პირველ რიგში, *ჰომან ზახახოვის* საქმესთან შედარებით, ის უფრო მკაცრ კრიტერიუმს ადგენს. მეორე მხრივ, ის არ შეესაბამება ეჭვის იმ ხარისხს, რაც მოცემულ გადაწყვეტილებაშია მითითებული. ლოგიკურად არათანმიმდევრულია, რომ პალატის გადაწყვეტილება ერთი მხრივ „მკაცრი აუცილებლობის“ ტესტს ითვალისწინებს, ხოლო მეორე მხრივ, ინდივიდუალური ეჭვის დაბალ სტანდარტს ადგენს. გარდა ამისა, პალატა არ განმარტავს, რას მოიცავს „მკაცრი აუცილებლობის“ ტესტი და მას მხოლოდ მისაღწევ მიზნებს უკავშირებს. აუცილებლობის ტესტი მოითხოვს, რომ მეთვალყურეობის ღონისძიება უნდა განხორციელდეს მხოლოდ მაშინ, როდესაც ფაქტების დადგენა სხვა ნაკლებად ინვაზიური მეთოდებით წარუმატებელი აღმოჩნდა ან გამონაკლის შემთხვევებში მიიჩნევა, რომ ნაკლებად ინვაზიური მეთოდები წარუმატებელი იქნება. მოსამართლის თანახმად, პალატის გადაწყვეტილებაში ეს მოთხოვნა ნახსენები არ არის.

მოსამართლე პინტო დე ალბუქერქეს შეფასებით, სასამართლო ნებართვასა და ზედამხედველობას აკნინებს პალატის მიერ განსაზღვრული კრიტერიუმი, რადგან ნებისმიერი სახის ეჭვი საკმარისი იქნება მოქალაქეებზე მასობრივი მეთვალყურეობის განსახორციელებლად და არსებობს რისკი, მოსამართლე იქცეს მთავრობის მხრიდან ადამიანების კონტროლის სტრატეგიაზე შტამპის დამსმელად. „ინდივიდუალური ეჭვი“ უთანაბრდება ზოგადი ეჭვის არსებობას და იქმნება შთაბეჭდილება, რომ ევროპული სასამართლოს პალატა ეთანხმება ეროვნული უსაფრთხოების უზრუნველსაყოფად ფართომასშტაბიანი, „სტრატეგიული მეთვალყურეობის“ განხორციელებას.

ევროკავშირის მართლმსაჯულების სასამართლოს მიერ მიღებული გადაწყვეტილებები

DIGITAL RIGHTS IRELAND LTD V MINISTER FOR COMMUNICATIONS, MARINE AND NATURAL RESOURCES AND OTHERS AND KÄRNTNER LANDESREGIERUNG AND OTHERS

08/04/2014

ევროკავშირის მართლმსაჯულების სასამართლოს წინასწარი გადაწყვეტილება 2006/24/EC დირექტივისა და 2002/58/EC დირექტივის შესწორების ვალიდურობის საკითხის შესწავლას შეეხება. ეს დირექტივა ითვალისწინებდა კერძო პროვაიდერების ვალდებულებას, სამართალდამცავი მიზნებისთვის შეენახათ ელექტრონული კომუნიკაციების მეტამონაცემები მნიშვნელოვანი პერიოდის განმავლობაში.

სამართლებრივი საფუძვლები

95/46/EC დირექტივა

95/46/EC დირექტივის 1(1) მუხლის თანახმად, დირექტივის მიზანი არის ფიზიკური პირების ძირითადი უფლებებისა და თავისუფლებების დაცვა, განსაკუთრებით კი მათი პირადი ცხოვრების პატივისცემის უფლებისა, რომელიც პერსონალური მონაცემების დამუშავებასთან არის დაკავშირებული.

95/46/EC დირექტივა, მუხლი 17(1)

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ დამმუშავებლის მიერ სათანადო ტექნიკური და ორგანიზაციული ზომების დანერგვა, რათა პერსონალური მონაცემები დაცული იყოს შემთხვევითი ან უკანონო განადგურებისაგან ან დაკარგვისაგან, ცვლილებისგან, უნებართვო გამჟღავნებისგან ან წვდომისგან, განსაკუთრებით მაშინ, როდესაც დამუშავება გულისხმობს მონაცემთა გადაცემას ქსელის მეშვეობით, და დამუშავების ყველა სხვა უკანონო ფორმისაგან.

ტექნიკის დონისა და მათი განხორციელების ღირებულების გათვალისწინებით, ასეთი ზომები უნდა უზრუნველყოფდეს უსაფრთხოების დონეს, რომელიც შეესაბამება დამუშავების და დაცული მონაცემების ხასიათიდან გამომდინარე რისკებს.

2002/58/ დირექტივა

დირექტივის მიზანია წევრ ქვეყნებს შორის კანონმდებლობის ჰარმონიზაცია, რათა უზრუნველყოფილი იყოს ძირითადი უფლებებისა და თავისუფლებების თანაბარი დაცვა, კერძოდ, პირადი ცხოვრებისა და კონფიდენციალურობის უფლების, რომელიც ელექტრონული კომუნიკაციების სექტორში პერსონალური მონაცემების დამუშავებას უკავშირდება, და ევროკავშირის ფარგლებში ასეთი მონაცემებისა და ელექტრონული საკომუნიკაციო აღჭურვილობისა და სერვისების თავისუფლად გადაადგილების უზრუნველყოფა. 1(2) მუხლის თანახმად, ამ დირექტივის დებულებები აკონკრეტებს და ავსებს 95/46 დირექტივას ამ უკანასკნელის 1(1) მუხლში აღნიშნული მიზნებისთვის.

▶● *2002/58 დირექტივის მე-4 მუხლი*

საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების მომსახურების მიმწოდებლებმა (პროვაიდერებმა) უნდა მიიღონ სათანადო ტექნიკური და ორგანიზაციული ზომები თავისი მომსახურების უსაფრთხოების დასაცავად, საჭიროების შემთხვევაში, ქსელის უსაფრთხოებასთან დაკავშირებული ეს ზომები უნდა გატარდეს საჯარო კომუნიკაციების ქსელების პროვაიდერთან ერთობლივად. ტექნიკის დონისა და მათი დანერგვის ღირებულების გათვალისწინებით, ეს ზომები უნდა უზრუნველყოფდეს უსაფრთხოების იმ ხარისხს, რომელიც არსებულ რისკებს შეესაბამება.

▶● *2002/58 დირექტივის მე-5 მუხლის პირველი და მესამე პუნქტები*

ეროვნული კანონმდებლობის მეშვეობით, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ კომუნიკაციების და მასთან დაკავშირებული ტრაფიკის მონაცემების კონფიდენციალურობის დაცვა, საჯარო კომუნიკაციების ქსელისა და საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების სერვისების საშუალებით. კერძოდ, მომხმარებლების გარდა ყველა სხვა პირს მათ უნდა აუკრძალონ კომუნიკაციებისა და მასთან დაკავშირებული ტრაფიკის მონაცემების მოსმენა, ჩაწერა, შენახვა ან მიყურადება ან სხვა სახის თვალთვალი შესაბამისი მომხმარებლების თანხმობის გარეშე, გარდა იმ შემთხვევისა, როდესაც 15(1) მუხლის შესაბამისად, მას/მათ კანონი ანიჭებს ამის გაკეთების უფლებამოსილებას. ეს პუნქტი არ კრძალავს იმგვარ ტექნიკურ შენახვას, რომელიც აუცილებელია კომუნიკაციის გადასაცემად, კონფიდენციალურობის პრინციპის შელახვის გარეშე.

▶● *2002/58 დირექტივის 6 (1) მუხლი*

საჯარო კომუნიკაციების ქსელის ან საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის მიერ აბონენტებისა და მომხმარებლების შესახებ არსებული ტრაფიკის მონაცემები უნდა წაიშალოს ან ანონიმური გახდეს იმ დროიდან, როცა ის საჭირო აღარ არის კომუნიკაციის გადაცემის მიზნებისთვის.

▶● *2002/58 დირექტივის 15 (1) მუხლი*

წევრმა ქვეყნებმა შეიძლება მიიღონ საკანონმდებლო ზომები, რომლებიც ზღუდავს დირექტივის მე-5 და მე-6 მუხლებით, მე-8 მუხლის 1-ლი, მე-2, მე-3 და მე-4 პუნქტებითა და მე-9 მუხლით დადგენილი უფლებებისა და ვალდებულებების ფარგლებს, როცა ამგვარი შეზღუდვა არის აუცილებელი, სათანადო და პროპორციული საშუალება დემოკრატიულ საზოგადოებაში ეროვნული უსაფრთხოების, თავდაცვის, საზოგადოებრივი უსაფრთხოების, ელექტრონულ საკომუნიკაციო სისტემაზე არაავტორიზებული წვდომის ან დანაშაულის პრევენციის, გამოძიების, გამოვლენისა და სისხლის სამართლებრივი დევნის განხორციელების მიზნით, როგორც ეს მითითებულია 95/46 დირექტივის მე-13 მუხლის 1-ელ პუნქტში. ამ მიზნით, წევრ სახელმწიფოებს შეუძლიათ მიიღონ საკანონმდებლო ზომები, რომლებიც უზრუნველყოფს

მონაცემთა შეზღუდული პერიოდით შენახვას ამ პუნქტით განსაზღვრული მიზნების მისაღწევად. ამ პუნქტში მითითებული ყველა ზომა უნდა შეესაბამებოდეს ევროკავშირის კანონმდებლობის ძირითად პრინციპებს, მათ შორის, ევროკავშირის შესახებ ხელშეკრულების მე-6 მუხლის 1-ელ და მე-2 პუნქტებს.

● 2006/24 დირექტივა

2002/58/EC დირექტივის 15(1) მუხლი ადგენს პირობებს, რომლითაც წევრ სახელმწიფოებს შეუძლიათ, შეზღუდონ ამ დირექტივის მე-5, მე-6 და მე-9 მუხლები, ასევე, მე-8 მუხლის 1-4 პუნქტებით გათვალისწინებული უფლებებისა და მოვალეობების ფარგლები. ნებისმიერი ასეთი შეზღუდვა უნდა იყოს აუცილებელი, შესაბამისი და პროპორციული დემოკრატიულ საზოგადოებაში კონკრეტული საზოგადოებრივი წესრიგის მიზნებისთვის, როგორიცაა ეროვნული უსაფრთხოება (სახელმწიფო უსაფრთხოება), თავდაცვა, საზოგადოებრივი უსაფრთხოება ან სისხლის სამართლის დანაშაულების ან ელექტრონული კომუნიკაციების სისტემების უნებართვო გამოყენების პრევენცია, გამოვლენა, გამოძიება და სისხლის-სამართლებრივი დევნის განხორციელება.

2006/24 დირექტივის პრეამბულის მე-5 პუნქტის პირველი წინადადების თანახმად, „რამდენიმე წევრმა სახელმწიფომ მიიღო კანონმდებლობა, რომელიც სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენისა და დევნის მიზნებისთვის სერვისის პროვაიდერების მიერ მონაცემთა შენახვას ითვალისწინებს.“

►● *2006/24 დირექტივის პრეამბულის მე-16 პუნქტი*

სერვისის პროვაიდერების ვალდებულება მონაცემთა ხარისხის უზრუნველყოფის ზომების თაობაზე, რომელიც 95/46/EC დირექტივიდან მომდინარეობს, ასევე, მათი ვალდებულება მონაცემთა დამუშავების კონფიდენციალობისა და უსაფრთხოების ზომების შესახებ, რომელიც ხსენებული დირექტივის მე-16 და მე-17 მუხლებიდან წარმოიშობა, სრულად ვრცელდება იმ მონაცემებზე, რომელიც წინამდებარე დირექტივის შესაბამისად ინახება.

►● *2006/24 დირექტივის მე-4 მუხლი, მონაცემებზე ხელმისაწვდომობა*

წევრმა სახელმწიფოებმა უნდა მიიღონ ზომები, რათა უზრუნველყონ, რომ ამ დირექტივის შესაბამისად დაცული მონაცემები მიეწოდება მხოლოდ უფლებამოსილ სახელმწიფო ორგანოებს კონკრეტულ შემთხვევებში და ეროვნული კანონმდებლობის შესაბამისად. აუცილებლობისა და პროპორციულობის მოთხოვნების შესაბამისად, მონაცემებზე წვდომის მოსაპოვებლად გასავლელი პროცედურები და შესასრულებელი პირობები თითოეულმა წევრმა სახელმწიფომ უნდა მოაწესრიგოს ეროვნული კანონმდებლობით, რომელიც შეესაბამება ევროპის კავშირის ან საერთაშორისო საჯარო სამართლის რელევანტური კანონმდებლობის დებულებებს, განსაკუთრებით, ადამიანის უფლებათა ევროპული სასამართლოს მიერ გაკეთებულ განმარტებებს.

▶● *2006/24 დირექტივის მე-6 მუხლი, შენახვის ხანგრძლივობა*

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ მე-5 მუხლში ჩამოთვლილი მონაცემთა კატეგორიების შენახვა კომუნიკაციის განხორციელების თარიღიდან არანაკლებ 6 თვისა და არაუმეტეს 2 წლის განმავლობაში.

▶● *2006/24 დირექტივის მე-8 მუხლი, მონაცემთა შენახვის პირობები*

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ მე-5 მუხლში ჩამოთვლილი მონაცემების ამ დირექტივის შესაბამისად იმგვარი შენახვა, რომ შენახული მონაცემები და მასთან დაკავშირებული ნებისმიერი სხვა საჭირო ინფორმაცია მოთხოვნის საფუძველზე უფლებამოსილ ორგანოებს ზედმეტი შეფერხების გარეშე გადაეცეს.

▶● *2006/24 დირექტივის მე-9 მუხლი, ზედამხედველი ორგანო*

01 თითოეულმა წევრმა სახელმწიფომ უნდა განსაზღვროს ერთი ან მეტი საჯარო ორგანო, რომელიც მისი ტერიტორიის ფარგლებში პასუხისმგებელი იქნება მე-7 მუხლის შესაბამისად, შენახული მონაცემების უსაფრთხოებასთან დაკავშირებით წევრი სახელმწიფოების მიერ მიღებული რეგულაციების მონიტორინგზე. ეს ორგანოები შეიძლება იყოს იგივე ორგანოები, რომლებიც მითითებულია 95/46/EC დირექტივის 28-ე მუხლში.

02 პირველ პუნქტში მითითებული ორგანოები სრულად დამოუკიდებლად უნდა მოქმედებდნენ ამავე პუნქტში მითითებული მონიტორინგის განხორციელებისას.

▶● *2006/24 დირექტივის მე-11 მუხლი, 2002/58/EC დირექტივის ცვლილება*

1-ლი პუნქტი არ ვრცელდება იმ მონაცემებზე, რომლის შენახვაც სპეციალურად არის მოთხოვნილი [დირექტივის 2006/24/EC მიერ] იმ მიზნებისათვის, რომლებიც მითითებულია ამ დირექტივის 1(1) მუხლში.

▶● *2006/24 დირექტივის მე-13 მუხლი, დაცვის საშუალებები, პასუხისმგებლობა და ჯარიმა*

01 თითოეული წევრი სახელმწიფო იღებს აუცილებელ ღონისძიებებს იმისათვის, რომ 95/46/EC დირექტივის III თავის იმპლემენტაციის ზომები ითვალისწინებდეს სასამართლო დაცვის საშუალებებს, პასუხისმგებლობასა და სანქციებს ამ დირექტივის საფუძველზე მონაცემთა დამუშავებასთან დაკავშირებით.

02 თითოეულმა წევრმა სახელმწიფომ უნდა მიიღოს საჭირო ზომები იმის უზრუნველსაყოფად, რომ დირექტივის შესაბამისად შენახულ მონაცემებზე განზრახ განხორციელებული ნებისმიერი წვდომა ან გადაცემა, რომელიც ამ დირექტივის მიხედვით

მიღებული ეროვნული კანონმდებლობით არ არის დაშვებული, იქნება დასჯადი, მათ შორის ეფექტური, პროპორციული და გადამარწმუნებელი ადმინისტრაციული ან სისხლის სამართლის სახდელით/სასჯელით.

ფაქტობრივი გარემოებები

▶● *საქმე C-293/12*

2006 წლის 11 აგვისტოს, სამოქალაქო ორგანიზაციამ „Digital Rights Ireland" (ის აცხადებდა, რომ ფლობდა და იყენებდა მობილურ ტელეფონს) მიმართა უმაღლეს სასამართლოს, ეჭვქვეშ დააყენა ეროვნული საკანონმდებლო და ადმინისტრაციული ღონისძიებების კანონიერება და მოითხოვა 2006/24 დირექტივისა და სისხლის სამართლის აქტის მე-7 ნაწილის (ტერორისტული დანაშაულები) გაუქმება, რომლის მიხედვითაც სატელეფონო კომუნიკაციის მომსახურების პროვაიდერებს (მიმწოდებლებს) ჰქონდათ ტრაფიკისა და ადგილმდებარეობის მონაცემების გარკვეული დროით შენახვის ვალდებულება დანაშაულის აღკვეთის, გამოვლენის, გამოძიებისა და სისხლისსამართლებრივი დევნის განხორციელების, ასევე სახელმწიფო უსაფრთხოების უზრუნველყოფის მიზნებისთვის.

უმაღლესმა სასამართლომ მიიჩნია, რომ მას არ შეეძლო ეროვნულ კანონმდებლობასთან დაკავშირებით წამოჭრილ კითხვებზე პასუხის გაცემა მანამ, სანამ 2006/24 დირექტივის ვალიდურობა არ იქნებოდა გამოკვლეული. სასამართლომ შეაჩერა საქმის განხილვა და წინასწარი გადაწყვეტილების მისაღებად, ევროპის მართლმსაჯულების სასამართლოს მიმართა შემდეგი კითხვებით:

01 2006/24 დირექტივის მე-3, მე-4 ... და მე-6 მუხლების მოთხოვნებიდან გამომდინარე, მოსარჩელის უფლებების შეზღუდვა, რომელიც მის მიერ მობილური ტელეფონის გამოყენებას უკავშირდება, არის თუ არა შეუსაბამო ევროკავშირის შესახებ ხელშეკრულებასთან (კერძოდ, 5(4) მუხლთან) როგორც არაპროპორციული, არასაჭირო და შეუსაბამო ლეგიტიმური მიზნების მისაღწევად:

ა. მძიმე დანაშაულის გამოძიების, გამოვლენისა და სისხლისსამართლებრივი დევნის განსახორციელებლად გარკვეული მონაცემების ხელმისაწვდომობის უზრუნველსაყოფად?

ან/და

ბ. ევროკავშირის შიდა ბაზრის გამართული ფუნქციონირების უზრუნველსაყოფად?

02 კერძოდ,

I არის თუ არა 2006/24 დირექტივა შესაბამისობაში ევროკავშირის ფუნქციონირების შესახებ ხელშეკრულების 21-ე მუხლით გათვალისწინებულ მოქალაქეების უფლებასთან, თავისუფლად გადაადგილდნენ და იცხოვრონ წევრი სახელმწიფოების ტერიტორიაზე?

II არის თუ არა 2006/24 დირექტივა შესაბამისობაში პირადი ცხოვრების პატივისცემის უფლებასთან, რომელიც ევროპის კავშირის ძირითადი უფლებების შესახებ ქარტიის (შემდგომში „ქარტია“) მე-7 მუხლითა და ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის (შემდგომში „ევროპული კონვენცია“) მე-8 მუხლით არის გათვალისწინებული?

III არის თუ არა 2006/24 დირექტივა შესაბამისობაში ქარტიის მე-8 მუხლით გათვალისწინებულ პერსონალურ მონაცემთა დაცვის უფლებასთან?

IV არის თუ არა 2006/24 დირექტივა შესაბამისობაში ქარტიის მე-11 და ევროპული კონვენციის მე-10 მუხლებით გათვალისწინებულ გამოხატვის თავისუფლებასთან?

V არის თუ არა 2006/24 დირექტივა შესაბამისობაში ქარტიის 41-ე მუხლით გათვალისწინებულ უფლებასთან კარგი მმართველობის შესახებ?

03 რა მოცულობით მოითხოვს ხელშეკრულებები - კონკრეტულად ევროკავშირის შესახებ ხელშეკრულების 4(3) მუხლით გათვალისწინებული ლოიალური თანამშრომლობის პრინციპი - სასამართლოს მხრიდან 2006/24 დირექტივის იმპლემენტაციისთვის ეროვნულ დონეზე მიღებული ზომების ქარტიის მე-7 და ევროპული კონვენციის მე-8 მუხლებთან შესაბამისობის გამოკვლევასა და შეფასებას?

▶ ● *საქმე C–594/12*

ავსტრიის საკონსტიტუციო სასამართლოს (Verfassungsgerichtshof) მიერ წინასწარი გადაწყვეტილების გამოტანის მიზნით, ევროკავშირის მართლმსაჯულების სასამართლოსადმი მიმართვას წინ უძღვოდა საკონსტიტუციო სასამართლოს წარმოებაში არსებული სარჩელები, რომელთა მოთხოვნაც ტელეკომუნიკაციების შესახებ კანონის 102(ა) პარაგრაფის გაუქმება იყო, იმ საფუძველზე მითითებით, რომ ის არღვევდა ინდივიდების ძირითად უფლებას, დაეცვათ თავიანთი მონაცემები.

უფრო ზუსტად, საკონსტიტუციო სასამართლოს აინტერესებს, შეესაბამება თუ არა 2006/24 დირექტივა ქარტიას, რამდენადაც ის იძლევა განუსაზღვრელ პირებთან დაკავშირებით მრავალი სახის მონაცემების შენახვის შესაძლებლობას დიდი ხნის განმავლობაში. საკონსტიტუციო სასამართლოს პოზიციით, არსებობს დიდი რისკი იმისა, რომ ამ პირთა

მონაცემებს ბევრი განსხვავებული მიზნით გაეცნობიან ხელისუფლების შესაბამისი წარმომადგენლები, იმის გათვალისწინებითაც, რომ ადამიანთა დაუდგენელ რაოდენობას აქვს წვდომა მონაცემებზე მინიმუმ ექვსი თვის განმავლობაში. ამასთან, არსებობს ეჭვები, დირექტივა მიაღწევს თუ არა დასახულ მიზანს და ჩარევა არის თუ არა პროპორციული.

საკონსტიტუციო სასამართლომ გადაწყვიტა, შეეჩერებინა სამართალწარმოება და მართლმსაჯულების სასამართლოს წარუდგინა შემდეგი კითხვები:

01 ევროკავშირის ინსტიტუციების აქტების ვალიდურობის შესახებ:

2006/24დირექტივის მე-3 და მე-9 მუხლები შესაბამისობაშია თუ არა ქარტიის მე-7, მე-8 და მე-11 მუხლებთან?

02 ხელშეკრულებების ინტერპრეტაციასთან დაკავშირებით:

ა. ჩარევის დასაშვებობის შეფასებისას, 95/46 დირექტივა და 45/2001 რეგულაცია უნდა გაითვალისწინოს თუ არა სასამართლომ, როგორც ქარტიის 8(2) და 52(1) მუხლების პირობების თანაბარი მნიშვნელობის მქონე?

ბ. რა ურთიერთკავშირია ქარტიის 52-ე მუხლის მე-3 პუნქტის ბოლო წინადადებაში მითითებულ „კავშირის სამართალსა“ და დირექტივებს შორის მონაცემთა დაცვის კანონმდებლობის სივრცეში?

გ. იმის გათვალისწინებით, რომ დირექტივა 95/26 და რეგულაცია No 45/2001 შეიცავს პირობებსა და შეზღუდვებს ქარტიის შესაბამისად მონაცემთა დაცვის ძირითადი უფლების უზრუნველსაყოფად, მეორეული კანონმდებლობიდან გამოწვეული ცვლილებები უნდა იქნას თუ არა მხედველობაში მიღებული ქარტიის მე-8 მუხლის ინტერპრეტაციის მიზნებისთვის?

დ. ქარტიის 52(4) მუხლის გათვალისწინებით, ქარტიის 53-ე მუხლით დადგენილი დაცვის მაღალი ხარისხის შენარჩუნების პრინციპიდან გამომდინარეობს თუ არა, რომ დასაშვები შეზღუდვების ფარგლები უფრო ვიწროდ უნდა იყოს განსაზღვრული მეორეული კანონმდებლობით?

ე. შესაძლებელია თუ არა ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტული სამართლის გამოყენება ქარტიის მე-8 მუხლის ინტერპრეტაციისას?

საქმეები C-293/12 და C-594/12 ზეპირი წარმოებისა და გადაწყვეტილების მიზნებისათვის, სასამართლომ ერთად განიხილა.

სასამართლოს შეფასება

C-293/12 საქმის მეორე შეკითხვის „ბ“ და „დ“ პუნქტები და C-594/12 საქმის პირველი შეკითხვა

C-293/12 საქმის მეორე შეკითხვის „ბ“ და „დ“ პუნქტები და C-594/12 საქმის პირველი შეკითხვა ეხება 2006/24 დირექტივის ვალიდურობის შემოწმებას ქარტიის მე-7, მე-8 და მე-11 მუხლების შუქზე.

ქარტიის მე-7, მე-8 და მე-11 მუხლების მიმართება 2006/24 დირექტივის ვალიდურობასთან დაკავშირებით

როგორც პირველი მუხლიდან და პრეამბულიდან ჩანს, 2006/24 დირექტივის მთავარი მიზანი არის წევრ ქვეყნებს შორის მოახდინოს იმ დებულებების ჰარმონიზება, რომლებიც საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების სერვისებისა ან საჯარო კომუნიკაციების ქსელების პროვაიდერების მიერ გენერირებული ან დამუშავებული მონაცემების შენახვას ეხება მძიმე დანაშაულის აღკვეთის, გამოძიების, გამოვლენისა და სისხლისსამართლებრივი დევნის განსახორციელებლად, ქარტიის მე-7 და მე-8 მუხლებით გათვალისწინებული უფლებების შესაბამისად.

საჭიროების არსებობისას, 2006/24 დირექტივის მე-5 მუხლში ჩამოთვლილ ინფორმაციაზე ხელისუფლების უფლებამოსილი პირების ხელმისაწვდომობა კითხვებს წარმოშობს ქარტიის მე-7, მე-8 და მე-11 მუხლებთან დაკავშირებით.

2006/24 დირექტივის მე-3 და მე-5 მუხლების მიხედვით, პროვაიდერებმა უნდა შეინახონ მონაცემები, რომლებიც აუცილებელია კომუნიკაციის წყაროსა და დანიშნულების დასადგენად, კომუნიკაციის დროის, ხანგრძლივობის და ტიპის იდენტიფიცირებისათვის, მომხმარებლების კომუნიკაციის მოწყობილობის (აპარატურის) დადგენა, სატელეფონო (მობილური) კომუნიკაციის მოწყობილობის ადგილმდებარეობის იდენტიფიცირება, ასევე, აბონენტის ან რეგისტრირებული მომხმარებლის ვინაობა და მისამართი, ტელეფონის ნომერი, რომლიდანაც ზარი განხორციელდა, ისევე როგორც ნომერი, რომელსაც დაურეკეს, ხოლო ინტერნეტ სერვისებისთვის - IP მისამართი. ეს მონაცემები შესაძლებელს ხდის, დადგინდეს თუ ვისთან და რა საშუალებით ჰქონდა კომუნიკაცია აბონენტს ან რეგისტრირებულ მომხმარებელს, ასევე იძლევა კომუნიკაციის დროისა და ადგილის, ისევე როგორც კომუნიკაციის სიხშირის გაგების შესაძლებლობას.

მთლიანობაში, ამ მონაცემების მეშვეობით, იმ ინდივიდების ცხოვრებასთან დაკავშირებით, რომელთა მონაცემებიც ინახება, შეიძლება ძალიან ზუსტი დასკვნების გამოტანა, მაგალითად, მათი ყოველდღიური ჩვევების, დროებითი ან მუდმივი საცხოვრებელი ადგილის, საქმიანობის, სოციალური ურთიერთობებისა და გარემოს შესახებ.

მართალია, 2006/24 დირექტივა არ იძლევა კომუნიკაციის შინაარსის შენახვის შესაძლებლობას, თუმცა წარმოუდგენელი არ უნდა იყოს, რომ ჩამოთვლილი მონაცემების შენახვამ შეიძლება გავლენა იქონიოს აბონენტების ან რეგისტრირებული მომხმარებლების მიერ კომუნიკაციის საშუალებების გამოყენებაზე და ამის შედეგად, ქარტიის მე-11 მუხლით გარანტირებულ გამოხატვის თავისუფლებაზე.

ხსენებულ მონაცემებზე ხელისუფლების უფლებამოსილი წარმომადგენლების შესაძლო წვდომის მიზნით ამ მონაცემთა შენახვა გავლენას ახდენს ინდივიდთა პირად ცხოვრებაზე და, შესაბამისად, ხვდება ქარტიის მე-7 და მე-8 მუხლებით დაცულ სფეროში. რაც გულისხმობს იმას, რომ ის უნდა აკმაყოფილებდეს ამ მუხლებით დადგენილ მონაცემთა დაცვის მოთხოვნებს.

სასამართლო მიუთითებს, რომ ხსენებულ შეკითხვებზე პასუხის გასაცემად 2006/24 დირექტივის ვალიდურობა ქარტიის მე-7 და მე-8 მუხლებთან მიმართებით უნდა შემოწმდეს.

2006/24 დირექტივა გადახვევას აკეთებს 95/46 და 2002/58 დირექტივების მონაცემთა დაცვის სისტემიდან, რომელიც ელექტრონული კომუნიკაციების სექტორში მონაცემთა დამუშავებას უკავშირდება და უზრუნველყოფს როგორც კომუნიკაციის, ისევე ტრაფიკის მონაცემების კონფიდენციალობას, ამასთან, აწესებს მონაცემების წაშლისა და ანონიმიზაციის ვალდებულებას, როცა მათი კომუნიკაციის გადაცემის მიზნით შენახვა საჭირო აღარ არის, გარდა იმ შემთხვევისა, როდესაც ისინი აუცილებელია გადასახადის დარიცხვის მიზნებისთვის და მხოლოდ იმ ვადით, რა ხანგრძლივობითაც ეს საჭიროება დგას.

▶● *ჩახევა*

პირად ცხოვრებაში ჩარევის დასადგენად არ აქვს მნიშვნელობა პირადი ცხოვრების შესახებ ინფორმაცია არის თუ არა სენსიტიური ხასიათის ან შეექმნათ თუ არა დაინტერესებულ პირებს რაიმე სახის დისკომფორტი. იმ მონაცემების შენახვა, რომლებიც ეხება პირის პირად ცხოვრებას და მის კომუნიკაციებს, მაგალითად, 2006/24 დირექტივის მე-5 მუხლში მითითებული მონაცემებისა, თავისთავად წარმოადგენს ქარტიის მე-7 მუხლით გარანტირებულ უფლებებში ჩარევას. მეტიც, ხელისუფლების წარმომადგენელი უფლებამოსილი პირების წვდომა ამ ინფორმაციაზე წარმოადგენს დამატებით ჩარევას. შესაბამისად, 2006/24 დირექტივის მე-4 და მე-8 მუხლები, რომლებიც ადგენს უფლებამოსილი ორგანოების მიერ მონაცემებზე წვდომასთან დაკავშირებულ წესებს, წარმოადგენს ქარტიის მე-7 და მე-8 მუხლებით გათვალისწინებულ უფლებებში ჩარევას.

სასამართლომ მიუთითა გენერალური ადვოკატის მიერ წარდგენილ მოსაზრებაზე და აღნიშნა, რომ საქმე ეხება ფართო დიაპაზონის მქონე, განსაკუთრებით მძიმე ჩარევას. ამასთან, ის ფაქტი, რომ მონაცემები ინახება და შემდგომში გამოიყენება აბონენტის ან რეგისტრირებული მომხმარებლის ინფორმირების გარეშე, დაინტერესებული პირების გონებაში, სავარაუდოდ, წარმოშობს განცდას, რომ მათი პირადი ცხოვრება მუდმივი მეთვალყურეობის საგანია.

▶● *ჩახევის გამახთღება*

ქარტიის 52-ე მუხლის 1-ლი პუნქტი ადგენს, რომ ქარტიით გარანტირებული უფლებებისა და თავისუფლებების განხორციელების ნებისმიერი შეზღუდვა გათვალისწინებული უნდა იყოს კანონით, პატივს უნდა სცემდეს უფლების არსს და პროპორციულობის პრინციპის

შესაბამისად, შეზღუდვა შეიძლება მხოლოდ იმ შემთხვევაში, თუ ეს აუცილებელია და ნამდვილად აკმაყოფილებს კავშირის მიერ აღიარებულ საჯარო ინტერესების მიზნებს ან აუცილებელია სხვათა უფლებებისა და თავისუფლებების დასაცავად.

მიუხედავად იმისა, რომ ჩარევა არის განსაკუთრებით მძიმე ხასიათის, ის არ არის იმგვარი, რომ დამაზიანებელ გავლენას ახდენდეს ამ უფლებების არსზე იმის გათვალისწინებით, რომ 2006/24 დირექტივის 1-ლი მუხლის მე-2 პუნქტიდან გამომდინარე, დირექტივა არ იძლევა ელექტრონული კომუნიკაციების შინაარსის გაგების შესაძლებლობას. ამასთან, 2006/24 დირექტივის თანახმად, 95/46 და 2002/58 დირექტივების შესაბამისად მიღებული დებულებების დარღვევის გარეშე, პროვაიდერებმა უნდა დაიცვან მონაცემთა დაცვის გარკვეული პრინციპები და მონაცემთა უსაფრთხოება. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ შესაბამისი ტექნიკური და ორგანიზაციული ზომების მიღება შემთხვევით ან უკანონოდ მონაცემთა განადგურების, დაკარგვის ან შეცვლის წინააღმდეგ.

რაც შეეხება საკითხს, ჩარევა შეესაბამება თუ არა საჯარო ინტერესებიდან გამომდინარე მიზანს, ყურადღება უნდა გამახვილდეს თავად დირექტივის ამოცანაზე, რომელიც მძიმე დანაშაულის წინააღმდეგ ბრძოლაში წვლილის შეტანა, მაშასადამე, საზოგადოების უსაფრთხოების უზრუნველყოფაა.

სასამართლოს პრაქტიკიდან ირკვევა, რომ საერთაშორისო ტერორიზმთან ბრძოლა, საერთაშორისო მშვიდობისა და უსაფრთხოების შენარჩუნება წარმოადგენს საერთო ინტერესის ობიექტს. იგივე შეიძლება ითქვას საზოგადოების უსაფრთხოების მიზნით მძიმე დანაშაულთან ბრძოლის შესახებ.

ელექტრონული კომუნიკაციების გამოყენებასთან დაკავშირებული მონაცემები განსაკუთრებით მნიშვნელოვანია და, შესაბამისად, ღირებული ინსტრუმენტია სამართალდარღვევების თავიდან არიდებისა და დანაშაულთან ბრძოლის მიზნებისთვის, განსაკუთრებით ორგანიზებულ დანაშაულთან გამკლავების თვალსაზრისით.

ამრიგად, უნდა ითქვას, რომ მონაცემთა შენახვა ხელისუფლების უფლებამოსილი პირების დაშვების მიზნით, ნამდვილად აკმაყოფილებს საჯარო ინტერესის მიზანს.

ასეთ გარემოებებში, აუცილებელია, დადგინდეს არსებული ჩარევის პროპორციულობა.

სასამართლოს მიერ დადგენილი პრაქტიკის თანახმად, პროპორციულობის პრინციპი მოითხოვს რომ ევროკავშირის ინსტიტუტების აქტები შესაბამისობაში იყოს კანონმდებლობით გათვალისწინებულ ლეგიტიმურ მიზნებთან და არ აღემატებოდეს იმ საზღვრებს, რაც არის შესაბამისი და აუცილებელი ამ მიზნების მისაღწევად.

როცა სახეზეა ძირითად უფლებაში ჩარევა, ევროკავშირის საკანონმდებლო ორგანოს დისკრეცია შეიძლება შეიზღუდოს, ეს დამოკიდებულია მთელ რიგ ფაქტორებზე, კერძოდ, ქარტიით გარანტირებული უფლების ბუნებაზე, ჩარევის ხასიათზე, სიმძიმესა და მიზანზე.

წინამდებარე საქმეში, იმ მნიშვნელოვანი როლის გათვალისწინებით, რომელსაც პერსონალური მონაცემების დაცვა პირადი ცხოვრების პატივისცემის ძირითადი უფლების შუქზე თამაშობს, ასევე, 2006/24 დირექტივის უფლებაში ჩარევის მასშტაბისა და სიმძიმის მხედველობაში მიღებით, ევროკავშირის საკანონმდებლო ორგანოს დისკრეციის ფარგლები შემცირებულია, რის შედეგადაც, ამ დისკრეციის შემოწმება მკაცრი უნდა იყოს.

ელექტრონული კომუნიკაციის საშუალებების მზარდი მნიშვნელობის გათვალისწინებით, დირექტივით გათვალისწინებული მონაცემების შენახვა დანაშაულის გამოძიებისთვის ღირებული ინსტრუმენტია. შესაბამისად, ასეთი მონაცემების შენახვა შეიძლება 2006/24 დირექტივით დასახული მიზნის მიღწევის შესაფერის საშუალებად ჩაითვალოს.

ის გარემოება, რომ არსებობს ელექტრონული კომუნიკაციის საშუალებები, რომლებიც 2006/24 დირექტივის მოქმედების ფარგლებში არ ექცევა ან რომლებიც იძლევა ანონიმური კომუნიკაციის განხორციელების შესაძლებლობას არ ნიშნავს იმას, რომ მონაცემთა შენახვა მიზნის მიღწევის შეუსაბამო საშუალებაა.

2006/24 დირექტივით გათვალისწინებული მონაცემების შენახვის აუცილებლობასთან დაკავშირებით, უნდა აღინიშნოს, რომ დანაშაულის წინააღმდეგ ბრძოლას, კერძოდ, ორგანიზებული დანაშაულისა და ტერორიზმის წინააღმდეგ ბრძოლას საზოგადოების უსაფრთხოების უზრუნველყოფისათვის უდიდესი მნიშვნელობა აქვს და მისი ეფექტურობა შეიძლება დიდწილად იყოს დამოკიდებული თანამედროვე საგამოძიებო მეთოდებზე. თუმცა საჯარო ინტერესიდან მომდინარე ასეთი მიზანი, რაც არ უნდა ფუნდამენტური იყოს ის, დანაშაულთან ბრძოლის მიზნით, თავისთავად არ ამართლებს შენახვის ისეთ ზომას, როგორიც 2006/24 დირექტივით არის დადგენილი.

სასამართლოს პრაქტიკის თანახმად, პერსონალურ მონაცემთა დაცვის უფლებიდან გადახვევის ან მისი შეზღუდვის გამოყენება, ნებისმიერ შემთხვევაში, მხოლოდ მკაცრი აუცილებლობის არსებობისას შეიძლება.

ამასთან დაკავშირებით, უნდა აღინიშნოს, რომ პერსონალური მონაცემების დაცვის ვალდებულება, რომელიც ქარტიის 8(1) მუხლიდან ცალსახად გამომდინარეობს, განსაკუთრებით მნიშნელოვანია ქარტიის მე-7 მუხლით გარანტირებული პირადი ცხოვრების პატივისცემის უფლებისთვის.

შესაბამისად, ევროკავშირის სადავო კანონმდებლობა უნდა განსაზღვრავდეს მკაფიო და ზუსტ წესებს, რომლებიც ღონისძიების გამოყენების ფარგლებს არეგულირებს და აწესებს დაცვის მინიმალურ გარანტიებს, რათა პირებს, რომელთა მონაცემებიც ინახება, ჰქონდეთ საკმარისი გარანტიები მათი პერსონალური მონაცემების ბოროტად გამოყენების რისკის და მონაცემებზე უკანონო წვდომისა და გამოყენებისგან ეფექტურად დასაცავად.

ასეთი გარანტიების საჭიროება მით უფრო დიდია, როცა პერსონალური მონაცემები ექვემდებარება ავტომატურ დამუშავებას (როგორც ეს 2006/24 დირექტივით არის გათვალისწინებული) და იმ შემთხვევაში, როდესაც არსებობს მათზე უკანონო წვდომის მნიშვნელოვანი რისკი.

რაც შეეხება საკითხს, შემოიფარგლება თუ არა 2006/24 დირექტივით გამოწვეული ჩარევა მკაცრი აუცილებლობით, უნდა აღინიშნოს, რომ დირექტივა მოითხოვს ტრაფიკის ყველა მონაცემის შენახვას, რომელიც შეეხება ფიქსირებულ ტელეფონს, მობილურ ტელეფონს, ინტერნეტზე წვდომას, ელ. ფოსტასა და ინტერნეტ ტელეფონს. შესაბამისად, ის ვრცელდება ელექტრონული კომუნიკაციის ყველა საშუალებაზე, რომლის გამოყენებაც და მნიშვნელობაც იზრდება ხალხის ყოველდღიურ ცხოვრებაში. გარდა ამისა, დირექტივა ფარავს ყველა აბონენტსა და რეგისტრირებულ მომხმარებელს. ამიტომ ეს იწვევს ჩარევას პრაქტიკულად მთელი ევროპის მოსახლეობის ძირითად უფლებებში.

ამასთან დაკავშირებით, პირველ რიგში, უნდა აღინიშნოს, რომ 2006/24 დირექტივა, მძიმე დანაშაულთან ბრძოლის მიზნის ფონზე, განზოგადებულად ფარავს ყველა პირს და ელექტრონული კომუნიკაციის საშუალებას, ისევე როგორც ტრაფიკის მონაცემს ყოველგვარი დიფერენციაციის, შეზღუდვის ან გამონაკლისის გარეშე.

დირექტივა ვრცელდება ყველა იმ ადამიანზე, რომელიც იყენებს ელექტრონული კომუნიკაციების სერვისებს. ის ეხება იმ პირებსაც, ვისთან მიმართებითაც არ არსებობს მტკიცებულება, რომელიც მიუთითებს იმაზე, რომ მათ ქცევას შეიძლება ჰქონდეს, თუნდაც არაპირდაპირი ან დისტანციური კავშირი მძიმე დანაშაულთან. გარდა ამისა, დირექტივა არ ითვალისწინებს რაიმე გამონაკლისს, რის გამოც იგი ვრცელდება იმ პირებზეც, რომელთა კომუნიკაციები ეროვნული კანონმდებლობის მიხედვით, პროფესიულ საიდუმლოებას წარმოადგენს.

მძიმე დანაშაულთან ბრძოლაში წვლილის შეტანის მცდელობის ფონზე, 2006/24 დირექტივა არ მოითხოვს რაიმე კავშირის არსებობას შესანახ მონაცემებსა და საზოგადოების უსაფრთხოებასთან დაკავშირებულ საშიშროებას შორის, ამასთან, შენახვა არ შემოიფარგლება კონკრეტული დროის მონაკვეთით ან/და კონკრეტული გეოგრაფიული ზონით ან/და კონკრეტული პირთა წრით, რომელიც შესაძლოა, ამა თუ იმ ფორმით, ჩართული იყოს მძიმე დანაშაულში ან რომელთა მონაცემების შენახვამ შეიძლება ხელი შეუწყოს მძიმე დანაშაულის აღკვეთას, გამოვლენასა და სისხლისსამართლებრივი დევნის განხორციელებას.

მეორე რიგში, ზოგადი ჩარჩოების არქონასთან ერთად, 2006/24 დირექტივა ვერ ადგენს რაიმე ობიექტურ კრიტერიუმს, რომლითაც განისაზღვრება უფლებამოსილი სახელმწიფო ორგანოების მონაცემებზე წვდომისა და დანაშაულის პრევენციის, გამოვლენისა და სისხლისსამართლებრივი დევნის განხორციელების მიზნით მათი შემდგომი გამოყენების ფარგლები. ქმედების სიმძიმიდან გამომდინარე, დანაშაულთან ბრძოლის მიზანი შეიძლება იმდენად მნიშვნელოვანი იყოს, რომ ჩარევის მოცულობისა და სიმძიმის გათვალისწინებით, ქარტიის მე-7 და მე-8 მუხლებით გარანტირებულ ძირითად უფლებაში ჩარევა გამართლებული იყოს. თუმცა, ამის საწინააღმდეგოდ, დირექტივის 1(1) მუხლი უბრალოდ ზოგადად ეხება წევრი სახელმწიფოების მიერ ეროვნული კანონმდებლობით განსაზღვრულ მძიმე დანაშაულს.

გარდა ამისა, დირექტივა არ შეიცავს არსებით და პროცედურულ პირობებს უფლებამოსილი სახელმწიფო ორგანოების მხრიდან მონაცემებზე წვდომის და მათი შემდგომი გამოყენების შესახებ. დირექტივის მე-4 მუხლი ცალსახად არ მიუთითებს, რომ მონაცემებზე წვდომა და

მათი გამოყენება მკაცრად უნდა იყოს შეზღუდული ზუსტად განსაზღვრული მძიმე დანაშაულების აღკვეთის, გამოვლენის ან სისხლისსამართლებრივი დევნის განხორციელების მიზნით. ის უბრალოდ ითვალისწინებს, რომ თითოეულმა წევრმა სახელმწიფომ უნდა განსაზღვროს პროცედურები და პირობები, რომელთა დაცვაც საჭიროა მონაცემებზე წვდომის მისაღებად, აუცილებლობისა და პროპორციულობის მოთხოვნების შესაბამისად.

უფრო ზუსტად, დირექტივა არ აწესებს რაიმე ობიექტურ კრიტერიუმს, რომლის მიხედვითაც შენახულ ინფორმაციაზე წვდომისა და გამოყენების უფლებამოსილების მქონე პირების რაოდენობა მკაცრი აუცილებლობით იქნება შემოსაზღვრული. უპირველეს ყოვლისა, უნდა ითქვას, რომ ინფორმაციაზე წვდომის მოპოვება არ არის დამოკიდებული სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს გადაწყვეტილებაზე, რომელიც მიმართულია ხელმისაწვდომობის მკაცრი აუცილებლობით შეზღუდვისკენ და ეფუძნება მძიმე დანაშაულთან ბრძოლის ლეგიტიმურ მიზანს. ის არც წევრი სახელმწიფოებისთვის აწესებს კონკრეტულ ვალდებულებას, დანერგონ მსგავსი ჩარჩოები.

მესამე რიგში, მონაცემთა შენახვის პერიოდთან დაკავშირებით, 2006/24 დირექტივის მე-6 მუხლი მოითხოვს, რომ მონაცემები ინახებოდეს მინიმუმ ექვსი თვის განმავლობაში, მე-5 მუხლში ჩამოთვლილი ინფორმაციის კატეგორიებს შორის ყოველგვარი დიფერენციაციის გარეშე, რომელიც მიზნის მიღწევის თვალსაზრისით, მათი შესაძლო სარგებლიანობის შეფასებას დაეფუძნება.

ამას გარდა, დირექტივით დადგენილია მინიმუმ 6 და მაქსიმუმ 24 თვიანი შენახვის პერიოდი, თუმცა არ არის ნათქვამი, რომ შენახვის ვადის განსაზღვრა უნდა ეფუძნებოდეს ობიექტურ კრიტერიუმებს, რათა უზრუნველყოფილი იყოს მკაცრი აუცილებლობით მისი შეზღუდვა.

ზემოაღნიშნულიდან გამომდინარეობს, რომ დირექტივა 2006/24 არ ადგენს ქარტიის მე-7 და მე-8 მუხლებით გათვალისწინებულ ძირითად უფლებებში ჩარევის ფარგლების მარეგულირებელ მკაფიო და ზუსტ წესებს. აქედან გამომდინარე, სასამართლომ დაადგინა, რომ დირექტივა ითვალისწინებს ძირითად უფლებებში ფართო დიაპაზონის მქონე, განსაკუთრებით მძიმე ჩარევას, ამ ჩარევის მკაცრი აუცილებლობით შემოსაზღვრის გარეშე.

უფრო მეტიც, დირექტივა ვერ უზრუნველყოფს პროვაიდერების მიერ შენახულ მონაცემთა ბოროტი გამოყენებისა და უკანონო წვდომისაგან სათანადო დაცვას. პირველ რიგში, დირექტივის მე-7 მუხლი 2006/24 არ ადგენს წესებს, რომლებიც სპეციფიკური და ადაპტირებულია (1) მონაცემთა დიდ რაოდენობაზე, რომელთა შენახვასაც დირექტივა მოითხოვს, (2) ამ მონაცემების სენსიტიურ ხასიათზე, (3) მონაცემებზე კანონსაწინააღმდეგო წვდომის რისკებზე. წევრი სახელმწიფოებისთვის ასეთი წესების დაწესების კონკრეტული ვალდებულება ასევე არ არის დადგენილი.

ამას გარდა, 2006/24 დირექტივის მე-7, 2002/58 დირექტივის 4(1) და 95/46 დირექტივის 17(1) მუხლების ერთობლიობით, არ არის გათვალისწინებული პროვაიდერებისთვის ტექნიკური და ორგანიზაციული ზომებით მონაცემთა უსაფრთხოების განსაკუთრებით მაღალი ხარისხის დაცვის ვალდებულება, მეტიც, დირექტივა ამ პროვაიდერებს საშუალებას აძლევს,

უსაფრთხოების დონის განსაზღვრის პროცესში გაითვალისწინონ ეკონომიკური გარემოებები, რაც უკავშირდება უსაფრთხოების ზომების გატარების ხარჯებს. ამასთან, დირექტივა ვერ უზრუნველყოფს მონაცემთა შეუქცევად განადგურებას მონაცემთა შენახვის პერიოდის ამოწურვის შემდეგ.

დამატებით უნდა აღინიშნოს, რომ დირექტივა არ მოითხოვს მონაცემთა ევროკავშირის ფარგლებში შენახვას, შედეგად, ქარტიის 8(3) მუხლით გათვალისწინებული დამოუკიდებელი უწყების კონტროლი მონაცემთა უსაფრთხოების მოთხოვნათა დაცვაზე სრულად უზრუნველყოფილი არ არის. ევროკავშირის კანონმდებლობის საფუძველზე განხორციელებული ასეთი კონტროლი არის არსებითი კომპონენტი მონაცემთა დამუშავებისას ინდივიდთა უფლებების დაცვისთვის.

ყველა ზემოაღნიშნული მოსაზრების გათვალისწინებით, უნდა ითქვას, რომ 2006/24 დირექტივის მიღებით, ევროკავშირის საკანონმდებლო ორგანომ გადააჭარბა პროპორციულობის პრინციპით დაწესებულ საზღვრებს ქარტიის მე-7, მე-8 და 52(1) მუხლების შუქზე.

ამ პირობებში, აღარ არის საჭირო 2006/24 დირექტივის ვალიდურობის შესწავლა ქარტიის მე-11 მუხლთან მიმართებით.

შესაბამისად, პასუხი C-293/12 საქმის მეორე კითხვის „ბ“ და „დ“ პუნქტებზე, ასევე C-594/12 საქმის პირველ შეკითხვაზე არის ის, რომ დირექტივა 2006/24 არის ძალადაკარგული.

წინა აბზაცში ხსენებულიდან გამომდინარეობს, რომ პასუხის გაცემა საჭირო არ არის C-293/12 საქმის პირველ, მეორე კითხვის „ა“ და „ე“ პუნქტებსა და მესამე კითხვებზე, ასევე, C-594/12 საქმის მეორე კითხვაზე.

დიდი პალატის გადაწყვეტილება

ევროპარლამენტის 2006/24 დირექტივა საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების სერვისებისა ან საჯარო კომუნიკაციების ქსელების უზრუნველყოფასთან დაკავშირებით გენერირებული ან დამუშავებული მონაცემების შენახვის შესახებ, ასევე, 2002/58EC შესწორების შემტანი დირექტივა ძალადაკარგულია.

LA QUADRATURE DU NET AND OTHERS V. PREMIER MINISTRE AND OTHERS

06/10/2020

ევროპის კავშირის მართლმსაჯულების სასამართლოს წინასწარი გადაწყვეტილების მისაღებად წარდგენილი მიმართთვა ევროკავშირის ძირითადი უფლებების ქარტიის (შემდგომ „ქარტია“) მე-4, მე-5, მე-6, მე-7, მე-8 და მე-11 მუხლების შუქზე, 2002/58/EC დირექტივის მე-15(1) მუხლის განმარტებას შეეხება. ეს დირექტივა ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებასა და პირადი ცხოვრების ხელშეუხებლობის დაცვას უკავშირდება. მიმართთვა ასევე შეეხება 2000/31/EC დირექტივის მე-12-15 მუხლების განმარტებას, რომელიც ინფორმაციული საზოგადოების სერვისების[4] კონკრეტულ სამართლებრივ ასპექტებს, კერძოდ კი, ევროკავშირის შიდა ბაზარზე ელექტრონულ ვაჭრობას არეგულირებს.

უფრო კონკრეტულად, საქმე C 511/18 საფრანგეთში სადაზვერვო საქმიანობასა და მეთოდებთან დაკავშირებით 2015-2016 წლებში მიღებული რამდენიმე ბრძანების კანონიერების საკითხებს უკავშირდება. საქმე C 512/18 კი საფრანგეთის საფოსტო და ელექტრონული კომუნიკაციების კოდექსის მმე-10-13 მუხლების, ასევე მონაცემთა შენახვისა და კომუნიკაციის თაობაზე 2011 წლის 25 თებერვლის N2011-219 ბრძანების კანონიერების საკითხს შეეხება.

რაც შეეხება საქმეს C 512/18, ის ბელგიის ელექტრონული ტელეკომუნიკაციების სექტორში მონაცემთა შენახვისა და შეგროვების შესახებ 2016 წლის 29 მაისის კანონის კანონიერების საკითხს მიემართება.

წინამდებარე გადაწყვეტილებით, სასამართლო ელექტრონულ საკომუნიკაციო სექტორში ტრაფიკისა და ადგილმდებარეობის მონაცემებზე მეთვალყურეობის წესებს განსაზღვრავს. მიუხედავად იმისა, რომ მანამდე ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტური და განურჩეველი შენახვა დაუშვებლად გამოცხადდა, სასამართლომ ამ გადაწყვეტილებით რამდენიმე მნიშვნელოვანი გამონაკლისი დააწესა.

4 ავტორის შენიშვნა: ინფორმაციული საზოგადოების სერვისებს წარმოადგენს ანაზღაურების სანაცვლოდ, დისტანციურად, მონაცემთა შენახვისა და დამუშავების (მათ შორის, ციფრული კომპრესირების) ელექტრონული მოწყობილობის საშუალებებით და სერვისის მიმღების დამოუკიდებელი მოთხოვნის საფუძველზე გაწეული ნებისმიერი მომსახურება (მაგალითად, ონლაინ საქონლის ან მომსახურების ყიდვა-გაყიდვა).

ფაქტობრივი გარემოებები

• საქმე C 511/18

2015 წლის 30 ნოემბერსა და 2016 წლის 16 მარტს საფრანგეთის სხვადასხვა არაკომერციულმა/სამოქალაქო ორგანიზაციებმა საფრანგეთის სახელმწიფო საბჭოს განაცხადით მიმართეს. მათ მოითხოვეს N2015-1185, N2015-1211, N2015-1639 და N2016-76 ბრძანებების გაუქმება იმ საფუძვლით, რომ ქარტიის მე-7, მე-8 და 47-ე მუხლების გათვალისწინებით, ისინი საფრანგეთის კონსტიტუციას, ადამიანის უფლებათა და ძირითად თავისუფლებათა შესახებ ევროპულ კონვენციას, ასევე, 2000/31 და 2002/58 დირექტივებს არღვევდა.

2000/31 დირექტივის სავარაუდო დარღვევასთან დაკავშირებულ საჩივრებზე, ეროვნულმა სასამართლომ განაცხადა, რომ საფრანგეთის შიდა უსაფრთხოების კოდექსის 851-3 L. მუხლით გათვალისწინებული პუნქტებით, ელექტრონული კომუნიკაციების ოპერატორები და ტექნიკური მომსახურების მიმწოდებლები ვალდებულნი არიან, საკუთარ ქსელებში დანერგონ მონაცემთა ავტომატური დამუშავების პრაქტიკა, რომელიც, ავტორიზაციაში მითითებული პარამეტრების ფარგლებში, გამიზნული იქნება იმ კავშირების გამოსავლენად, რომლებიც შესაძლოა ტერორისტულ საფრთხეს წარმოადგენდეს. ამ მეთოდის მიზანია, შეზღუდული დროით, ოპერატორებისა და მომსახურების მიმწოდებლების მიერ დამუშავებული კავშირის ყველა მონაცემიდან იმგვარი მონაცემების შეგროვების გაიოლება, რომელიც შესაძლოა ამ ტიპის მძიმე დანაშაულს უკავშირდებოდეს. ეროვნული სასამართლოს მოსაზრებით, ეს პუნქტები სისტემატური მეთვალყურეობის ზოგად ვალდებულებებს არ შეიცავს და ამდენად, 2000/31 დირექტივის მე-15 მუხლს არ არღვევს.

ადგილობრივი სასამართლოს მოსაზრებით, ეროვნული დებულებები, რომლებიც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს ვალდებულებებს უდგენს, როგორიც არის მომხმარებელთა და აბონენტთა ტრაფიკისა და ადგილმდებარეობის მონაცემების განურჩეველი და ბლანკეტური შენახვა, 2002/58 დირექტივის 15(1) მუხლში გაცხადებული მიზნებისთვის, რომელიც ეროვნული უსაფრთხოების, თავდაცვისა და საზოგადოებრივი უსაფრთხოების დაცვას მოიცავს, ექცევა ამ დირექტივის ფარგლებში, ვინაიდან ეს წესები არეგულირებს ამ მიმწოდებელთა საქმიანობას. ასევე, დირექტივა ვრცელდება იმ დებულებებზე, რომლებიც ეროვნული ხელისუფლების ორგანოების მიერ ამ მონაცემებზე წვდომასა და მათ გამოყენებას შეეხება.

ამავდროულად, სასამართლო მიიჩნევდა, რომ შიდა უსაფრთხოების კოდექსის L. 851-1 მუხლით გათვალისწინებული მონაცემების შენახვის ვალდებულება და L. 851-1, L. 851-2 და L. 851-4 მუხლებით გათვალისწინებული ადმინისტრაციული ორგანოების მიერ ამ მონაცემებზე, მათ შორის, რეალურ დროში, წვდომის შესახებ ნორმები, 2002/58 დირექტივის ფარგლებში ექცევა. იგივე შეიძლება ითქვას კოდექსის L. 851-3 მუხლზეც. მიუხედავად იმისა, რომ ეს მუხლები ოპერატორებს ბლანკეტურად მიწოდებას არ ავალდებულებს, ისინი მოითხოვს, რომ შესაძლო ტერორისტული საფრთხის წყაროების გამოსავლენად, მათ ქსელებში ავტომატური დამუშავება დანერგონ.

მეორე მხრივ, სასამართლოს მოსაზრებით, 2002/58 დირექტივის ფარგლებში არ ექცევა შიდა უსაფრთხოების კოდექსის ის მუხლები, რომლებიც სახელმწიფოს მიერ დაზვერვის მიზნით ინფორმაციის შეგროვების მეთოდებს შეეხება, ვინაიდან ისინი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის საქმიანობას არ არეგულირებს და მათ კონკრეტულ ვალდებულებებს არ აკისრებს.

ამდენად, 2002/58 დირექტივის გათვალისწინებით, N2015-1185, N2015-1211, N2015-1639 და N2016-67ბრძანებების (მიღებულ იქნა შიდა უსაფრთხოების კოდექსის 851-1 - L. 851-4 მუხლების განხორციელების მიზნით) კანონიერების შესახებ დავის გადასაწყვეტად, ევროკავშირის კანონმდებლობის განმარტების თაობაზე სამი კითხვა წარმოიშვება.

2002/58 დირექტივის მე-15(1) მუხლთან მიმართებით, ქარტიის მე-6 მუხლით გარანტირებული უსაფრთხოების უფლების შუქზე, ასევე, ეროვნული უსაფრთხოების ინტერესებიდან გამომდინარე, რაც ევროკავშირის შესახებ ხელშეკრულების მე-4 მუხლის შესაბამისად მხოლოდ წევრი ქვეყნების მიხედულების სფეროს წარმოადგენს, სასამართლოს აინტერესებს, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისთვის L. 851-1 და R. 851-5 მუხლების საფუძველზე დაკისრებული ბლანკეტური და განურჩეველი შენახვის ვალდებულება, თუ შეიძლება შეფასდეს უფლებაში მართლზომიერ ჩარევად, იმ გარანტიებისა და კონტროლის გათვალისწინებით, რომლებსაც ადმინისტრაციული ორგანოების მიერ კავშირის მონაცემებზე წვდომა და მათი გამოყენება ექვემდებარება?

ეროვნული სასამართლო აცხადებდა, რომ ტერორიზმის პრევენციის მიზნით ინფორმაციისა და დოკუმენტაციების შეგროვება, რეალურ დროში, იმ პირებთან მიმართებით ხორციელდება, რომლებზეც მანამდე არსებობდა ეჭვი, რომ ისინი შესაძლო ტერორიზმისგან მომდინარე საფრთხეების წყაროს წარმოადგენენ. იგივე შეიძლება ითქვას იმავე კოდექსის L. 851-4 მუხლზე, რომელიც ოპერატორების მიერ მხოლოდ ტერმინალური მოწყობილობის ადგილმდებარეობასთან დაკავშირებული ტექნიკური მონაცემების რეალურ დროში გადაცემის უფლებას ითვალისწინებს. ამავდროულად, ფოსტისა და ელექტრონული კომუნიკაციებისა და ციფრული ეკონომიკის ნდობის შესახებ კანონების საფუძველზე, ეს მეთოდები ადმინისტრაციული ორგანოების შენახულ მონაცემებზე რეალურ დროში წვდომას სხვადასხვა მიზნითა და საშუალებით უშვებს. თუმცა, გადასახადის დარიცხვისა და მომსახურების მიწოდებისთვის აუცილებელი მონაცემების გარდა, სხვა დამატებითი მონაცემების შენახვა მიმწოდებლებს არ ევალებათ. ეროვნული სასამართლოს მოსაზრებით, არც შიდა უსაფრთხოების კოდექსის L. 851-3 მუხლის დებულებები იწვევს ბლანკეტურ და განურჩეველ შენახვას (ეს მუხლი, კავშირების ანალიზის მიზნით, მომსახურების მიმწოდებელს მათ ქსელებზე ავტომატური დამუშავების სისტემის დანერგვას ავალდებულებს).

ეროვნული სასამართლო მიიჩნევს, რომ მონაცემთა ბლანკეტური, განურჩეველი შენახვა და კავშირის მონაცემებზე რეალურ დროში წვდომა განსაკუთრებულ პრაქტიკულ მნიშვნელობას ატარებს სერიოზულ და მუდმივ საფრთხეებთან, განსაკუთრებით კი ტერორიზმის საფრთხესთან ბრძოლის კუთხით. მონაცემების განურჩეველი შენახვა დაზვერვის სამსახურს უფლებამოსილებას აძლევს, კომუნიკაციის მონაცემებზე წვდომა ჰქონდეს მანამ, სანამ

გაჩნდება ეჭვები, რომ პირი საშიშროებას წარმოადგენს საზოგადოებრივი უსაფრთხოების, თავდაცვის თუ სახელმწიფო უსაფრთხოებისთვის. დამატებით, კავშირის მონაცემებზე რეალურ დროში წვდომა იმ ინდივიდების ქმედებებზე დაკვირვების შესაძლებლობას იძლევა, რომლებმაც საზოგადოებრივ წესრიგს შეიძლება მყისიერი საფრთხე შეუქმნან.

ეროვნულ სასამართლოს ასევე აინტერესებდა, არის თუ არა კავშირის მონაცემების შეგროვების პროცედურების კანონიერების წინაპირობა ის, რომ მონაცემთა სუბიექტების ინფორმირება ხდება მაშინ, როდესაც მათი ინფორმირება კომპეტენტური ორგანოების მიერ ჩატარებულ გამოძიებას საფრთხეს აღარ შეუქმნის.

ეროვნული სასამართლო აცხადებდა, რომ საფრანგეთის კანონმდებლობით, ნებისმიერ პირს, რომელსაც სურს შეამოწმოს, განხორციელდა თუ არა მის მიმართ უკანონო სადაზვერვო ღონისძიებები, შეუძლია მიმართოს სახელმწიფო საბჭოს სპეციალურ ჯგუფს, რომელიც ადგენს, გატარდა თუ არა მომჩივნის მიმართ სადაზვერვო ღონისძიება საფრანგეთის შიდა უსაფრთხოების კოდექსის შესაბამისად. სასამართლო მიუთითებდა, რომ კანონმდებლობით სპეციალისტთა ჯგუფი უფლებამოსილია, მოიკვლიოს და გამოიძიოს განცხადებაში დასმული საკითხები, განაცხადოს გამოვლენილი უკანონო ქმედებების შესახებ და უკანონობის გამოსასწორებლად ხელისუფლებას სათანადო ზომების გატარება დაავალოს. ამავდროულად, სადაზვერვო ღონისძიებათა ზედამხედველი კომისია აკონტროლებს ინფორმაციის მოპოვების მეთოდების შიდა უსაფრთხოების კოდექსთან შესაბამისობას. ამგვარი დაცვის გარანტიების საფუძველზე, სასამართლო მიიჩნევდა, რომ იმ პირთა შეტყობინების საკანონმდებლო ვალდებულების არარსებობა, რომელთა მიმართაც სამეთვალყურეო ზომები განხორციელდა, არ წარმოადგენდა პირადი ცხოვრების დაცვის უფლებაში გადამეტებულ ჩარევას.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, საფრანგეთის სახელმწიფო საბჭომ შეაჩერა სამართალწარმოება და ევროკავშირის მართლმსაჯულების სასამართლოს წინასწარი გადაწყვეტილების მისაღებად, შემდეგი კითხვებით მიმართა:

01 **დირექტივის მე-15 მუხლის პირველი პუნქტის საფუძველზე, ეროვნული უსაფრთხოების, კერძოდ კი, ტერორიზმის სერიოზული და მუდმივი საფრთხეების ფონზე, მიმწოდებლებისთვის დაწესებული ბლანკეტური და განურჩეველი შენახვის ვალდებულება, ქარტიის მე-6 მუხლით გარანტირებული უსაფრთხოების უფლების გათვალისწინებით, ასევე, ეროვნული უსაფრთხოების ინტერესების შუქზე, რაც ევროკავშირის შესახებ ხელშეკრულების მე-4 მუხლის შესაბამისად მხოლოდ წევრი ქვეყნების პასუხისმგებლობას განეკუთვნება, უნდა ჩაითვალოს თუ არა მართლზომიერ ჩარევად?**

02 **ქარტიის გათვალისწინებით, 2002/58 დირექტივა უნდა განიმარტოს თუ არა იმგვარად, რომ ის დასაშვებად მიიჩნევს საკანონმდებლო ზომებს, როგორიც არის კონკრეტული პირების შესახებ რეალურ დროში ტრაფიკისა და ადგილმდებარეობის მონაცემთა შეგროვება, რომლებიც, მართალია, გავლენას ახდენს ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელთა ვალდებულებებსა და უფლებებზე, თუმცა, მათგან მონაცემების შენახვისთვის კონკრეტული ვალდებულებების შესრულებას არ მოითხოვს?**

03 **ქარტიის გათვალისწინებით, 2002/58 დირექტივა უნდა განიმარტოს თუ არა იმგვარად, რომ კომუნიკაციის მონაცემების შეგროვების პროცედურების კანონიერად მიჩნევის წინაპირობას მონაცემთა სუბიექტების შეტყობინება წარმოადგენს მაშინ, როცა პირის ინფორმირება გამოძიებას საფრთხეს აღარ უქმნის? თუ შესაძლებელია, რომ კომუნიკაციის მონაცემების შეგროვების პროცედურები კანონიერად ჩაითვალოს, როცა ეროვნული კანონმდებლობა სხვა პროცედურულ გარანტიებს ითვალისწინებს და ეს გარანტიები პირს სამართლებრივი დაცვის ქმედითი საშუალებით უზრუნველყოფს?**

● საქმე C 512/18

2015 წლის 1 სექტემბერს, ორგანიზაციებმა საფრანგეთის სახელმწიფო საბჭოს მიმართეს მათ განცხადებაზე პრემიერ-მინისტრის უარის გაუქმების მოთხოვნით. ისინი ამ განცხადებით, ფოსტისა და ელექტრონული კომუნიკაციების კოდექსის R. 10-13 მუხლებისა და N2011-219 ბრძანების გაუქმებას მოითხოვდნენ იმ საფუძვლით, რომ ისინი, ქარტიის მე-7, მე-8 და მე-11 მუხლების გათვალისწინებით, 2002/58 დირექტივის მე-15(1) მუხლს არღვევდა.

საფრანგეთის ფოსტისა და ელექტრონული კომუნიკაციების კოდექსის R. 10-13 მუხლებთან დაკავშირებით, რომლებიც კომუნიკაციების მონაცემების ბლანკეტურ და განურჩეველ შენახვას ითვალისწინებს, ეროვნული სასამართლო აღნიშნავდა, რომ კანონმდებლობით ამგვარი შენახვა სასამართლო ხელისუფლებას უფლებამოსილებას ანიჭებს, ჰქონდეს წვდომა პირთა კომუნიკაციებთან დაკავშირებულ მონაცემებზე მანამ, სანამ ეს პირები დანაშაულის ჩადენაში ეჭვმიტანილებად გამოცხადდებიან, რის გამოც ამ მონაცემთა შენახვას დანაშაულის გამოძიების, გამოვლენისა და სისხლის სამართლებრივი დევნის დაწყებისთვის უპრეცედენტოდ დიდი მნიშვნელობა აქვს.

რაც შეეხება N2011-219 ბრძანებას, სასამართლო მიიჩნევდა, რომ ბრძანებით გათვალისწინებულ მე-6 (II) მუხლზე დირექტივა 2002/58 არ უნდა გავრცელებულიყო, რადგან ეს დირექტივა ევროპის კავშირის საჯარო საკომუნიკაციო ქსელებში არსებულ საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიწოდებასთან დაკავშირებულ წესებს განსაზღვრავს. ბრძანების ზემოხსენებული მუხლი კი იმ მონაცემების შენახვის ვალდებულებას წარმოშობს, რომლებიც კონტენტის შექმნას უკავშირდება. სასამართლოს მოსაზრებით, ეს მუხლი მხოლოდ 2000/31 დირექტივის ფარგლებში ექცეოდა, რომლის მე-15 მუხლის პირველი და მე-2 პუნქტები თავისთავად არ კრძალავს იმ მონაცემთა შეგროვებას, რომელიც კონტენტის შენახვას უკავშირდება, საიდანაც გადახვევა მხოლოდ გამონაკლის შემთხვევებში იქნებოდა შესაძლებელი.

სახელმწიფო საბჭომ შეაჩერა საქმისწარმოება და ევროკავშირის მართლმსაჯულების სასამართლოს წინასწარი გადაწყვეტილების მისაღებად შემდეგი კითხვებით მიმართა:

01 **2002/58 დირექტივის მე-15(1) მუხლის საფუძველზე მიმწოდებლისთვის დაკისრებული ბლანკეტური და განურჩეველი შენახვის ვალდებულება არის თუ არა გამართლებული ქარტიის მე-6 მუხლით გარანტირებული უსაფრთხოების უფლებითა და ეროვნული უსაფრთხოების მოთხოვნებით, რაც მხოლოდ წევრი სახელმწიფოების პასუხისმგებლობას განეკუთვნება, იმ გარანტიებისა და კონტროლის მექანიზმების გათვალისწინებით, რასაც კავშირის მონაცემების შეგროვება და გამოყენება ექვემდებარება?**

02 **2000/31 დირექტივის მუხლები, ქარტიის მე-6, მე-7, მე-8, მე-11 და 52(1)-ე მუხლების გათვალისწინებით, ანიჭებს თუ არა სახელმწიფოს იმგვარი ეროვნული კანონმდებლობის მიღების უფლებამოსილებას, რომელიც ონლაინ საჯარო საკომუნიკაციო მომსახურებაზე წვდომის შეთავაზების განმახორციელებელ პირებს, ასევე იმ ფიზიკურ და იურიდიულ პირებს, რომლებიც უფასოდ და ონლაინ საჯარო საკომუნიკაციო მომსახურების მეშვეობით, საზოგადოებისათვის მომსახურების მიწოდების მიზნით მომსახურებათა მიმღებების მიერ მათთვის გადაცემულ ნებისმიერი სახის სიგნალებს, ნაწერებს, სურათებს, ხმებს ან ტექსტურ შეტყობინებებს აგროვებენ, აკისრებს იმ მონაცემების შენახვის ვალდებულებას, რომელიც ამ მომსახურების კონტენტის ან კონტენტის ზოგიერთი ნაწილის შექმნაში მონაწილე პირის ამოცნობის საშუალებას იძლევა, რათა სასამართლო ხელისუფლებას, სამოქალაქო და სისხლის სამართლის პასუხისმგებლობის დამდგენ ნორმებთან შესაბამისობის უზრუნველყოფის მიზნით, საჭიროების შემთხვევაში, ჰქონდეს ამ მონაცემების შესახებ ინფორმაციის მოთხოვნის შესაძლებლობა?**

● საქმე C 520/18

2017 წელს რამდენიმე ორგანიზაციამ 2016 წლის 29 მაისის კანონის გაუქმების მოთხოვნით ბელგიის საკონსტიტუციო სასამართლოს მიმართა. მათ მიაჩნდათ, რომ ეს კანონი ეწინააღმდეგებოდა ბელგიის კონსტიტუციის მე-10 და მე-11 მუხლებს, ადამიანის უფლებათა ევროპული კონვენციის მე-5, მე-6-11, მე-14, მე-15, მე-17 და მე-18 მუხლებს, ქარტიის მე-7, მე-8, მე-11 და 47-ე და 52(1) მუხლებს, სამოქალაქო და პოლიტიკური უფლებების შესახებ პაქტის მე-17 მუხლს, სამართლებრივი განჭვრეტადობის, პროპორციულობის, ინფორმაციული თვითგამორკვევის ზოგად პრინციპებს და ევროკავშირის შესახებ ხელშეკრულების მე-5 მუხლის მე-4 პუნქტს.

მომჩივანთა მოსაზრებით, კანონი სცილდებოდა მკაცრი აუცილებლობის ფარგლებს და არ ითვალისწინებდა დაცვის სათანადო გარანტიებს. მომჩივნები ასევე თვლიდნენ, რომ კანონის ნორმები არ შეესაბამებოდა 2014 წლის 8 აპრილის *(Digital Rights Ireland)* და 2016 წლის 21 დეკემბრის *(Tele2 Sverige)* გადაწყვეტილებებით მონაცემთა შენახვასა და წვდომასთან დაკავშირებით დადგენილ სტანდარტებს. მომჩივანთა მტკიცებით, კანონი ქმნიდა ინდივიდუალური პროფილების შექმნის რისკებს, რომლებიც შეიძლება კომპეტენტურ ორგანოებს ბოროტად გამოყენებინათ, შენახული მონაცემების დაცვისა და უსაფრთხოების სათანადო გარანტიებს კი არ უზრუნველყოფდა. ამასთან, კანონი ვრცელდებოდა იმ პირებზეც, რომელთაც პროფესიული საიდუმლოებისა და კონფიდენციალურობის დაცვას კანონი აკისრებდა.

ბელგიის საკონსტიტუციო სასამართლომ განაცხადა, რომ მონაცემები, რომლებიც სატელეფონო მომსახურების მიმწოდებლებისა და საჯარო ელექტრონული საკომუნიკაციო ქსელის ოპერატორებმა, დაინტერესებული პირების ან მისაღწევი მიზნის განურჩევლად, 2016 წლის 29 მაისის კანონის საფუძველზე უნდა შეინახონ, 2006 წლის 15 მარტის 2006/24/EC დირექტივაში ჩამოთვლილი მონაცემების იდენტურია. კანონით მისაღწევი მიზანი შეიძლება მრავალგვარი იყოს. ის არ შემოიფარგლება მხოლოდ ტერორიზმისა და ბავშვთა პორნოგრაფიასთან ბრძოლის მიზნებით და შესაძლებლობას იძლევა, შენახული მონაცემები დანაშაულის გამოძიებისას სხვადასხვა ვითარებაში იქნას გამოყენებული. ამავდროულად, ადგილობრივი სასამართლოს განმარტებით, ეროვნულმა საკანონმდებლო ორგანომ შეუძლებლად მიიჩნია მონაცემების მიზნობრივი და შერჩევითი შენახვის ვალდებულების დადგენა და ბლანკეტური და განურჩეველი შენახვა არჩია, თუმცა უსაფრთხოების მკაცრი გარანტიებით, რათა პირადი ცხოვრების დაცვის უფლებაში ჩარევა მინიმუმამდე დაეყვანა.

საკონსტიტუციო სასამართლოს განცხადებით, 2016 წლის 29 მაისის კანონის ამოცანაა იმ საქმეების ეფექტიანი გამოძიება და შესაბამისი სასჯელის განსაზღვრა, რომელიც არასრულწლოვანთა მიმართ სექსუალურ ძალადობას შეეხება, რათა გამოვლინდეს დამნაშავე იმ შემთხვევაშიც, როცა ელექტრონული საკომუნიკაციო სისტემები გამოიყენება.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, ბელგიის საკონსტიტუციო სასამართლომ შეაჩერა სამართალწარმოება და ევროპული კავშირის მართლმსაჯულების სასამართლოს წინასწარი გადაწყვეტილების მისაღებად, შემდეგი კითხვებით მიმართა:

01 **2002/58 დირექტივის მე-15(1) მუხლი, ქარტიის მე-6 მუხლით გარანტირებული უსაფრთხოების უფლებისა და ქარტიის მე-7, მე-8 და 52(1)-ე მუხლებით გარანტირებული პერსონალური მონაცემების დაცვის უფლების გათვალისწინებით, გამორიცხავს თუ არა ეროვნულ კანონმდებლობას, რომელიც ელექტრონული საკომუნიკაციო მომსახურებების მიმწოდებლებისა და ოპერატორებისთვის აწესებს ზოგად ვალდებულებას, შეინახონ მომსახურების მიწოდების მიზნით შეგროვებული ან დამუშავებული ტრაფიკისა და ადგილმდებარეობის მონაცემები; ეროვნულ კანონმდებლობას, რომლის მიზნები არის არა მხოლოდ მძიმე დანაშაულის გამოძიება, გამოვლენა და სისხლისსამართლებრივი დევნა, არამედ ასევე ეროვნული უსაფრთხოების, ტერიტორიისა და საზოგადოებრივი უსაფრთხოების დაცვა, ელექტრონული საკომუნიკაციო სისტემების არაკანონიერი გამოყენების პრევენცია, 2016/679 რეგულაციის 23(1) მუხლით გათვალისწინებული სხვა მიზნების მიღწევა, და რომელიც მონაცემთა შენახვისა და მათზე წვდომის დამატებით, კონკრეტულ გარანტიებს ექვემდებარება?**

02 **2002/58 დირექტივის მე-15(1) მუხლი, ქარტიის მე-4, მე-7, მე-8, მე-11 და 52(1)-ე მუხლების გათვალისწინებით, გამორიცხავს თუ არა ეროვნულ კანონმდებლობას, რომელიც ელექტრონული საკომუნიკაციო მომსახურებების მიმწოდებლებსა და ოპერატორებს აკისრებს ზოგად ვალდებულებას, შეინახონ ამ მომსახურებების მიწოდების მიზნით შეგროვებული ან დამუშავებული ტრაფიკისა და ადგილმდებარეობის მონაცემები, როცა ამ კანონმდებლობის მიზანია ქარტიის მე-4 და მე-7 მუხლებით დაკისრებული**

პოზიტიური ვალდებულებების შესრულება, რაც გამოიხატება არასრულწლოვანთა მიმართ სექსუალური ძალადობის საქმეების ეფექტიანი გამოძიებისა და ეფექტიანი სანქცირების საკანონმდებლო ჩარჩოს შექმნაში და დამნაშავის იდენტიფიკაციის ეფექტიან საშუალებას წარმოადგენს, მაშინაც კი, როდესაც ელექტრონული საკომუნიკაციო სისტემები გამოიყენება?

03 **იმ შემთხვევაშიც, თუ ბელგიის საკონსტიტუციო სასამართლომ წინა შეკითხვების პასუხების საფუძველზე, უნდა მიიჩნიოს, რომ სადავო კანონი ერთ ან მეტ ვალდებულებას ეწინააღმდეგება, შეიძლება თუ არა კანონის მოქმედების ძალის დროებით შენარჩუნება, რათა სამართლებრივი განუსაზღვრელობა თავიდან იქნას აცილებული და მანამდე შეგროვებული და შენახული მონაცემები კანონის მიზნების მისაღწევად იქნას გამოყენებული?**

სასამართლოს შეფასება

სასამართლოს მსჯელობა C 511/18 და C 512/18 საქმეების პირველ შეკითხვებზე და C 520/18 საქმის პირველ და მეორე შეკითხვებზე

სასამართლომ განმარტა, რომ ეროვნულ სასამართლოებს ამ შეკითხვებით სურთ გამოარკვიონ, 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტი გამორიცხავს თუ არა ეროვნული კანონმდებლობით, ამავე პუნქტით განსაზღვრული ერთ-ერთი რომელიმე მიზნის მისაღწევად, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისთვის ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვის ვალდებულების დაკისრებას.

როგორც სასამართლომ აღნიშნა, შესაფასებელი კანონმდებლობა ვრცელდება ყველა ელექტრონულ საკომუნიკაციო სისტემასა და ამ სისტემის ყველა მომხმარებელზე, გამონაკლისის გარეშე. ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებმა უნდა შეინახონ მონაცემები, რომლებიც საჭიროა კომუნიკაციის წყაროსა და დანიშნულების ადგილის დასადგენად, კომუნიკაციის ტიპის, ხანგრძლივობის, დროისა და თარიღის გამოსარკვევად, გამოყენებული კომუნიკაციის მოწყობილობის გამოსავლენად, საბოლოო მოწყობილობისა და კომუნიკაციების ადგილმდებარეობის განსასაზღვრად; მონაცემები, რომლებიც მოიცავს მომხმარებლის მისამართსა და სახელს, ზარის მიმღებისა და გამშვების ტელეფონის ნომრებს, ინტერნეტ მომსახურების შემთხვევაში კი IP მისამართს. აღნიშნული მონაცემები არ მოიცავს კომუნიკაციის შინაარს. ამდენად, ეს მონაცემები, რომლებიც ერთი წლის მანძილზე უნდა იქნას შენახული, იძლევა იმ პირის ამოცნობის შესაძლებლობას, ვისაც მომხმარებელი ელექტრონული საკომუნიკაციო სისტემის მეშვეობით დაეკონტაქტა, ასევე, გამოყენებული საშუალების, კომუნიკაციისა და ინტერნეტ კავშირის თარიღის, დროისა და ხანგრძლივობისა და იმ ადგილების გამოვლენის საშუალებას, სადაც ეს კომუნიკაციები და კავშირები დამყარდა, საბოლოო მოწყობილობის ადგილმდებარეობის განსაზღვრის

შესაძლებლობას იმ შემთხვევაშიც, თუ კომუნიკაციის გადაცემა არ მომხდარა. ამ მონაცემების ანალიზის შედეგად, შესაძლებელი ხდება გარკვეული პერიოდის მანძილზე მომხმარებლის კონკრეტულ პირებთან კომუნიკაციის სიხშირის განსაზღვრაც. C 511/18 და C 512/18 საქმეებზე, ვინაიდან კანონმდებლობა ასევე ფარავს ქსელების მეშვეობით ელექტრონული კომუნიკაციების გადაცემასთან დაკავშირებულ მონაცემებს, ის ონლაინ ნანახი ინფორმაციის ტიპის განსაზღვრის შესაძლებლობას ქმნის.

რაც შეეხება მისაღწევ მიზნებს, C 511/18 და C 512/18 საქმეებზე სადავოდ გამხდარი კანონმდებლობა ასახელებს დანაშაულის გამოძიებას, გამოვლენასა და სისხლისსამართლებრივი დევნის დაწყებას; ეროვნული დამოუკიდებლობისა და ტერიტორიული მთლიანობის დაცვასა და თავდაცვას, საგარეო პოლიტიკის ძირითადი ინტერესების განხორციელებას, ნაკისრი ევროპული და საერთაშორისო ვალდებულებების შესრულებას; საფრანგეთის ძირითადი ეკონომიკური, ინდუსტრიული და სამეცნიერო ინტერესების გატარებას; ტერორიზმის, სახელმწიფოს რესპუბლიკურ ინსტიტუტებზე თავდასხმის, არსებული კანონისა და წესრიგის ძირგამომთხრელი კოლექტიური ძალადობის პრევენციას.C 520/18 საქმეზე სადავოდ გამხდარი კანონმდებლობის მიზანს კი, მათ შორის, დანაშაულის გამოძიების, გამოვლენისა და სისხლისსამართლებრივი დევნის დაწყება; ეროვნული, ტერიტორიული და საზოგადოებრივი უსაფრთხოების დაცვა წარმოადგენს.

ეროვნულ სასამართლოებს აინტერესებთ, ქარტიის მე-6 მუხლში გარანტირებული უსაფრთხოების უფლების შესაძლო ზეგავლენა 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტის განმარტებაზე. ასევე, მართლზომიერია თუ არა ეროვნული კანონმდებლობით დადგენილი მონაცემთა შენახვის ვალდებულება, რომელიც შედეგად, ქარტიის მე-7 და მე-8 მუხლებით განსაზღვრულ ძირითად უფლებებში ჩარევას იწვევს, თუმცა ეროვნულ ხელისუფლებას შენახულ მონაცემებზე წვდომის შემზღუდველ წესებს უდგენს. ამავდროულად, საფრანგეთის სახელმწიფო საბჭომ განაცხადა, რომ ქვეყნის უსაფრთხოების წინაშე არსებული სერიოზული და მუდმივი საფრთხეების გამო, კანონმდებლობა უნდა შეფასდეს ევროკავშირის შესახებ ხელშეკრულების მე-4 მუხლის მე-2 პუნქტის გათვალისწინებით. ბელგიის საკონსტიტუციო სასამართლო კი უთითებდა, რომ ეროვნული კანონმდებლობით სახელმწიფო ასრულებს ქარტიის მე-4 და მე-7 მუხლებით გათვალისწინებულ პოზიტიურ ვალდებულებებს, კერძოდ, ის ქმნის სამართლებრივ ჩარჩოს, რომელიც არასრულწლოვანთა მიმართ სექსუალური ძალადობის შემთხვევების ეფექტიან პრევენციასა და სასჯელის დაწესებას უზრუნველყოფს.

მიუხედავად იმისა, რომ საფრანგეთის სახელმწიფო საბჭო და ბელგიის საკონსტიტუციო სასამართლო მიიჩნევდნენ, რომ არსებული კანონმდებლობა 2002/58 დირექტივის ფარგლებში ექცევა, ზოგიერთი მხარე და წევრი ქვეყანა, რომლებმაც წერილობითი მოსაზრებები წარუდგინეს სასამართლოს, არ დაეთანხმნენ ამ მოსაზრებას. შესაბამისად, სასამართლომ აუცილებლად მიიჩნია გამოეკვლია, სადავო კანონმდებლობა ექცევა თუ არა დირექტივის ფარგლებში.

დირექტივის ფარგლები

სასამართლომ, პირველ რიგში, ყურადღება გაამახვილა 2002/58 დირექტივის პირველი მუხლის პირველი პუნქტით გათვალისწინებულ დირექტივის მიზანზე - შიდა სახელმწიფოებრივი ნორმების ჰარმონიზაციის, ძირითადი უფლებებისა და თავისუფლებების, განსაკუთრებით კი, ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით, პირადი ცხოვრების ხელშეუხებლობისა და კონფიდენციალურობის უფლების დაცულობის თანაბარი დონის უზრუნველყოფაზე. ამავდროულად აღნიშნა, რომ იმავე მუხლის მე-3 პუნქტი გამორიცხავს დირექტივის გავრცელებას იმ საქმიანობებზე, რომლებიც უკავშირდება საზოგადოებრივ უსაფრთხოებას, თავდაცვას და სახელმწიფო უსაფრთხოებას (მათ შორის, სახელმწიფოს ეკონომიკურ უსაფრთხოებას, როცა ის სახელმწიფო უსაფრთხოების საკითხებს უკავშირდება) და სახელმწიფოს საქმიანობას სისხლის სამართლის სფეროში. ამდენად, ეს პუნქტი მიემართება იმ საქმიანობებს, რომლებიც დამახასიათებელია სახელმწიფოსა და მისი ორგანოებისთვის, ხოლო უცხო იმ სფეროებისთვის, სადაც ინდივიდები საქმიანობენ.

დირექტივის მე-3 მუხლის მიხედვით, ის ვრცელდება პერსონალური მონაცემების დამუშავებაზე, რომელიც უკავშირდება ევროკავშირში, საჯარო საკომუნიკაციო ქსელებში საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას, იმ საჯარო საკომუნიკაციო ქსელების ჩათვლით, რომლებიც მონაცემთა შეგროვებასა და მოწყობილობათა იდენტიფიცირებას უზრუნველყოფენ. ამდენად, დირექტივა ამ მომსახურებათა მიმწოდებლის საქმიანობებს არეგულირებს.

სასამართლომ მიიჩნია, რომ ვინაიდან დირექტივის მე-15 მუხლის 1-ლი პუნქტი სახელმწიფოს უფლებამოსილებას ანიჭებს, მიიღოს საკანონმდებლო ზომები, რომლებიც, დადგენილი დათქმების შესაბამისად, დირექტივის ცალკეული მუხლებით უზრუნველყოფილ უფლებებსა და ვალდებულებებს ზღუდავს, ის უშვებს, რომ ამ ეროვნულ საკანონმდებლო ზომებზე დირექტივის ფარგლები ვრცელდება. ამასთან, წევრ ქვეყნებს საკანონმდებლო ზომების მიღების უფლება მხოლოდ იმ შემთხვევაში აქვთ, თუ დირექტივის სხვა მოთხოვნები შესრულდება. ეს საკანონმდებლო ზომები კი, თავის მხრივ, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების საქმიანობას არეგულირებს, რაშიც მოიაზრება არა მხოლოდ ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისათვის ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვის მავალდებულებელი საკანონმდებლო ზომები, არამედ ისინიც, რომლებიც მიმწოდებლებისგან ამ მონაცემებზე ეროვნული ხელისუფლების შესაბამისი ორგანოების წვდომის დაშვებას მოითხოვს. შედეგად, საკანონმდებლო ზომები მიმწოდებლებს ამ მონაცემთა დამუშავებას ავალდებულებს, რაც არ შეიძლება სახელმწიფოს საქმიანობად შეფასდეს.

ამავდროულად, დირექტივის 1-ლი მუხლის მე-3 პუნქტით განსაზღვრული მიზნები და მე-15 მუხლის 1-ლი პუნქტით განსაზღვრული საკანონმდებლო ზომების მიზნები მნიშვნელოვანწილად გადაფარავს ერთმანეთს. ამ საფუძვლით დირექტივის მე-15(1) მუხლში გათვალისწინებული საკანონმდებლო ზომების დირექტივის ფარგლებს გარეთ დატოვება კი ამ მუხლს

პრაქტიკაში განუხორციელებელს გახდიდა. ამდენად, დირექტივის მე-15 მუხლის პირველ პუნქტში მითითებული საკანონმდებლო ზომები არ წარმოადგენს პირველი მუხლის მე-3 პუნქტით გათვალისწინებულ სახელმწიფო საქმიანობებს, რომლებზეც დირექტივა არ ვრცელდება.

სასამართლოს განმარტებით, მიუხედავად იმისა, რომ გარე და შიდა უსაფრთხოების უზრუნველმყოფი ზომების მიღება მხოლოდ წევრი ქვეყნების მიხედულების არეალში ექცევა, ეროვნული უსაფრთხოების დაცვის მიზნით გატარებული ნებისმიერი ზომა წევრ ქვეყნებს ავტომატურად ევროკავშირის კანონმდებლობის მიღმა არ ტოვებს და არ ათავისუფლებს ამ კანონმდებლობის დაცვის ვალდებულებისგან.

დიხექტივის ფარგლებში ექცევა ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ პერსონალური მონაცემების ნებისმიერი ტიპის დამუშავება, მათ შორის, საჯარო ხელისუფლების ორგანოების მიერ მათთვის დაკისრებული ვალდებულების შესრულების მიზნით დამუშავება. როცა წევრი ქვეყნები ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისთვის ვალდებულების დაკისრების გარეშე გაატარებენ ელექტრონული კომუნიკაციების კონფიდენციალურობის პრინციპიდან გადამხვევ საკანონმდებლო ზომებს, მაშინ დაინტერესებული პირების მონაცემთა დაცულობა აღარ მოექცევა 2002/58 დირექტივის ფარგლებში. ამდენად, ეს უკანასკნელი ვრცელდება იმ ეროვნულ კანონმდებლობაზე, რომელიც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს, ეროვნული უსაფრთხოებისა და დანაშაულთან ბრძოლის მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვას ავალდებულებს.

● 2002/58 დირექტივის მე-15 მუხლის 1-ლი პუნქტის განმარტება

სასამართლომ დირექტივის მე-15 მუხლის პირველი პუნქტის განმარტებისას, პირველ რიგში, დირექტივის მიზანზე გაამახვილა ყურადღება. დირექტივის მიზანს კი წარმოადგენს ახალი ტექნოლოგიებისა და მონაცემთა ავტომატური დამუშავებისა და შენახვის მზარდი შესაძლებლობებიდან მომდინარე საფრთხეებისგან ელექტრონული საკომუნიკაციო მომსახურების მომხმარებელთა პერსონალური მონაცემებისა და პირადი ცხოვრების ხელშეუხებლობის დაცვა. პერსონალურ მონაცემთა დაცვის მაღალი დონის უზრუნველსაყოფად, დირექტივის მე-5 მუხლის პირველ პუნქტში განმტკიცებულია კონფიდენციალურობის პრინციპი, რომლითაც პირებს, მომხმარებელთა თანხმობის გარეშე, ელექტრონული კომუნიკაციისა და მასთან დაკავშირებული ტრაფიკის მონაცემების შენახვა ეკრძალებათ.

დირექტივით, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს ტრაფიკის მონაცემების დამუშავება და შენახვა მხოლოდ იმ მოცულობითა და ხანგრძლივობით შეუძლიათ, რაც აუცილებელია მარკეტინგისა და მომსახურების ანგარიშსწორებისთვის, ასევე, დამატებითი ღირებულების მომსახურების მისაწოდებლად. ამ პერიოდის გასვლის შემდეგ კი დამუშავებული და შენახული მონაცემები უნდა წაიშალოს ან ანონიმური გახდეს (დირექტივის მე-6 მუხლი). რაც შეეხება ადგილმდებარეობის მონაცემებს, ისინი შეიძლება დამუშავდეს მხოლოდ კონკრეტული პირობების დადგომისას და მხოლოდ მათი ანონიმიზაციის ან მომხმარებელთა და აბონენტთა თანხმობის მიღების შემდეგ (დირექტივის მე-9 მუხლის 1-ლი პუნქტი).

მიუხედავად ამისა, დირექტივის მე-15 მუხლის 1-ლი პუნქტი წევრ ქვეყნებს უფლებამოსილებას ანიჭებს, შემოიღონ საკანონმდებლო ზომები, რომლებიც პროპორციულობის პრინციპის დაცვით და ამავე მუხლით დადგენილი მიზნების მისაღწევად, შეზღუდული დროით კონფიდენციალურობის პრინციპიდან და, ამდენად, დირექტივის მე-6 და მე-9 მუხლებიდან გადაუხვევენ. თუმცა, სასამართლოს განმარტებით, დირექტივის შესაბამისი უფლებებიდან და ვალდებულებებიდან გადახვევის შესაძლებლობა წესიდან გამონაკლისს უნდა წარმოადგენდეს. ამავდროულად, **ამ უფლებებიდან და ვალდებულებებიდან გადახვევა უნდა განხორციელდეს ევროკავშირის კანონმდებლობისა და ქარტიით განმტკიცებული უფლებების შესაბამისად. როგორც სასამართლომ წინა გადაწყვეტილებებში მიუთითა, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისთვის ტრაფიკის მონაცემების შენახვის ვალდებულების დაკისრება იმისათვის, რომ საჭიროების შემთხვევაში, შესაბამის ორგანოებს მათზე წვდომა ჰქონდეთ, გავლენას ახდენს არა მხოლოდ ქარტიის მე-7 და მე-8 მუხლებით დაცულ პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის უფლებებზე, არამედ მე-11 მუხლით დაცულ გამოხატვის თავისუფლებაზეც.**

ამავდროულად, ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვით, პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვის უფლებაში ჩარევა ხდება იმის მიუხედავად, წარმოადგენს თუ არა ეს მონაცემები განსაკუთრებული კატეგორიის მონაცემებს ან მოხდა თუ არა მათი შემდგომი გამოყენება. ეს უკანასკნელი ძირითად უფლებებში ცალკე ჩარევად ფასდება.

ტრაფიკისა და ადგილმდებარეობის მონაცემები პირის პირადი ცხოვრების შესახებ დიდი რაოდენობის ინფორმაციას შეიძლება ამჟღავნებდეს, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს - სექსუალური ორიენტაციის, პოლიტიკური მოსაზრებების, რელიგიური, ფილოსოფიური, საზოგადოებრივი თუ სხვა სახის მრწამსისა და ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციას. ეს მონაცემები ადამიანების ცხოვრების შესახებ ზუსტი დასკვნების გამოტანისა და პირთა პროფილების შექმნის შესაძლებლობას იძლევა. აქედან გამომდინარე, ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვა თავისთავად იწვევს ქარტიით გათვალისწინებული კომუნიკაციის ხელშეუხებლობის უფლების დარღვევას და შესაძლოა, ელექტრონული საკომუნიკაციო სისტემების მომხმარებლებს საკუთარი გამოხატვის თავისუფლების შეზღუდვისაკენ უბიძგოს. ბლანკეტური და განურჩეველი შენახვის შედეგად არსებული ტრაფიკისა და ადგილმდებარეობის მონაცემების აურაცხელი რაოდენობიდან გამომდინარე, ასევე, ამ ინფორმაციის სენსიტიურობიდან გამომდინარე, მიმწოდებლების მიერ ამ მონაცემების შენახვას თავისთავად თან სდევს მისი ბოროტად გამოყენებისა და მათზე არაკანონიერი წვდომის რისკები. მართალია, დირექტივის მე-15 მუხლის პირველი პუნქტი იძლევა გადახვევის შესაძლებლობას, ის მხოლოდ იმ ფაქტს ასახავს, რომ ქარტიის მე-7, მე-8 და მე-11 უფლებები აბსოლუტურ უფლებებს არ წარმოადგენს. სასამართლოს განმარტებით, უნდა შეფასდეს, ერთი მხრივ, ქარტიით გარანტირებული უფლებებისა და მეორე მხრივ, ეროვნული უსაფრთხოებისა და მძიმე დანაშაულთან ბრძოლის მნიშვნელობა სხვათა უფლებებისა და თავისუფლებების დაცვის უზრუნველსაყოფად.

სასამართლომ ხაზი გაუსვა ქარტიის მე-6 მუხლითა და ადამიანის უფლებათა ევროპული კონვენციის მე-5 მუხლით გარანტირებული უფლებების თანაბარ მნიშვნელობას - ორივე მათგანი პირთათვის თავისუფლებისა და უსაფრთხოების უფლებას უზრუნველყოფს. ქარტიის 52-ე მუხლის მე-3 პუნქტი კი მიზნად ისახავს ამ ორი მნიშვნელოვანი დოკუმენტით გარანტირებულ უფლებებს შორის მინიმალური თანმიმდევრულობის განმტკიცებას. აქედან გამომდინარე, ქარტიის განმარტების მიზნით, სასამართლომ ადამიანის უფლებათა კონვენციის მე-5 მუხლზეც იმსჯელა. სასამართლომ აღნიშნა, რომ კონვენციის მე-5 მუხლი ინდივიდებს თავისუფლების თვითნებური და გაუმართლებელი აღკვეთისგან იცავს, თუმცა, ვინაიდან ეს ნორმა მხოლოდ საჯარო ხელისუფლების თვითნებური ქმედებისგან დაცვას მოიაზრებს, ქარტიის მე-6 მუხლიც არ უნდა განიმარტოს ისე, თითქოს საჯარო ხელისუფლებას გარკვეული დანაშაულების გამოძიების მიზნით კონკრეტული ზომების მიღებას ავალდებულებს.

რაც შეეხება ბელგიის საკონსტიტუციო სასამართლოს მიერ აღნიშნულ არასრულწლოვანთა და სხვა მოწყვლადი პირების მიმართ ჩადენილი დანაშაულების წინააღმდეგ ეფექტიანი ბრძოლის მიზანს, სასამართლომ განმარტა, რომ პოზიტიური ვალდებულებები მომდინარეობს ქარტიის მე-7 მუხლიდან, რომელიც ადამიანის პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და კომუნიკაციის ხელშეუხებლობის დასაცავად საკანონმდებლო ზომების გატარებას მოითხოვს, ასევე ქარტიის მე-3 და მე-4 მუხლებიდან, რომლებიც პირთა ფიზიკური და ფსიქიკური ხელშეუხებლობის დაცვასა და წამების, არაადამიანური და დამამცირებელი მოპყრობის აკრძალვას შეეხება. სასამართლომ განმარტა, რომ განსხვავებული პოზიტიური ვალდებულებების გათვალისწინებით, მნიშვნელოვანია სხვადასხვა ინტერესსა და უფლებას შორის ბალანსის განსაზღვრა.

სასამართლომ მოიხმო ადამიანის უფლებათა ევროპული სასამართლოს განმარტებები კონვენციის მე-3 და მე-8 მუხლებთან მიმართებით, რომლებიც ქარტიის მე-4 და მე-7 მუხლებით დაცულ უფლებებს ესატყვისება. ეს მუხლები იმგვარი მატერიალური და საპროცესო კანონმდებლობისა და პრაქტიკული ზომების მიღებას მოითხოვს, რომლებიც ეფექტიანი გამოძიებისა და სისხლისსამართლებრივი დევნის წარმოებით, დანაშაულთან ბრძოლის მიზნით ქმედითი ზომების გატარებას უზრუნველყოფს. ეს ვალდებულებები მით უფრო მნიშვნელოვანია, როცა ბავშვის ფიზიკურ და მორალურ კეთილდღეობას ემუქრება საფრთხე. თუმცა, მიღებული ზომები არ უნდა გასცდეს იმ ფარგლებს, რასაც ჯეროვანი სამართლებრივი პროცედურის პრინციპი და სხვათა უფლებებისა და თავისუფლებების დაცვა მოითხოვს. სამართლებრივი ჩარჩო სხვადასხვა უფლებასა და ინტერესს შორის ბალანსს უნდა უზრუნველყოფდეს.

სასამართლოს თანახმად, წევრი სახელმწიფოებისთვის მე-15 მუხლის 1-ლი პუნქტით მინიჭებული კონფიდენციალურობის პრინციპიდან გადახვევის უფლება უნდა განხორციელდეს მხოლოდ იმ შემთხვევაში, თუ მიღებული ზომა წარმოადგენს აუცილებელ, სათანადო და პროპორციულ საშუალებას დემოკრატიულ საზოგადოებაში, რომელიც მხოლოდ ამ მუხლით განსაზღვრული მიზნების მიღწევას მოემსახურება. ამასთან, პერსონალური მონაცემების დაცვის უფლების შეზღუდვა ან მისგან გადახვევა აბსოლუტურ აუცილებლობას უნდა წარმოადგენდეს.

სასამართლოს განმარტებით, პროპორციულობის პრინციპი მოითხოვს, რომ კანონმდებლობამ გაითვალისწინოს მკაფიო და ზუსტი ნორმები, რომლებიც მიღებული ზომის ფარგლებსა და მის პრაქტიკულ გამოყენებას განსაზღვრავენ, ასევე, უზრუნველყოფენ მინიმალურ გარანტიებს, რათა პირებს პერსონალური მონაცემების არაკანონიერი გამოყენების რისკების თავიდან არიდების საკმარისი გარანტიები ჰქონდეთ. კანონმდებლობას უნდა ჰქონდეს შესასრულებლად სავალდებულო ძალა და მიუთითებდეს იმ პირობებსა და ვითარებას, რომელთა არსებობისას ამგვარ მონაცემთა დამუშავება შესაძლებელია. ამ გარანტიების არსებობა მით უფრო აუცილებელია ავტომატური დამუშავებისას, განსაკუთრებით იმ შემთხვევებში, როცა არსებობს ამ მონაცემებზე არაკანონიერი წვდომის რისკი, ასევე როდესაც საქმე ეხება განსაკუთრებული კატეგორიის მონაცემებს. ამავდროულად, პერსონალური მონაცემების შენახვის მავალდებულებელი კანონმდებლობა ყოველთვის უნდა განსაზღვრავდეს ობიექტურ კრიტერიუმებს, რომლებიც შესანახ მონაცემებსა და მისაღწევ მიზანს შორის კავშირს დაადგენს.

– ეროვნული უსაფრთხოების დაცვის მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების პრევენციული შენახვის უზრუნველმყოფი საკანონმდებლო ზომები

სასამართლოს თანახმად, წევრი ქვეყნების უსაფრთხოების, სახელმწიფოს ფუნქციონირებისა და საზოგადოების ფუნდამენტური ინტერესების დაცვა, რაც ევროკავშირის შესახებ ხელშეკრულების მე-4 მუხლიდან გამომდინარე მხოლოდ წევრი ქვეყნების მიხედულების სფეროს წარმოადგენს, მოიცავს იმგვარი ქმედებების პრევენციასა და დასჯას, რომლებმაც შესაძლოა ქვეყნის ძირითადი კონსტიტუციური, პოლიტიკური, ეკონომიკური ან სოციალური სტრუქტურების რღვევა გამოიწვიოს, მათ შორის, პირდაპირი საფრთხე შეუქმნას საზოგადოებას, მოსახლეობას ან თავად სახელმწიფოს. სასამართლოს განმარტებით, ამგვარი საქმიანობები, თავიანთი არსისა და სერიოზული ბუნების გათვალისწინებით, უნდა განსხვავდებოდეს ქვეყანაში სერიოზული არეულობის გამომწვევი ქმედებებისგან. სასამართლომ აღნიშნა, რომ სხვა მიზნებისგან განსხვავებით, ეროვნული უსაფრთხოების დაცვის მიზანმა შეიძლება გაამართლოს უფლებაში ინტენსიური ხასიათის ჩარევა.

ეროვნული უსაფრთხოების კონტექსტში, დირექტივის მე-15 მუხლის პირველი პუნქტი თავისთავად არ გამორიცხავს შესაბამისი ორგანოების მიერ ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისთვის ტრაფიკისა და ადგილმდებარეობის შესახებ მონაცემების შეზღუდული დროით შენახვის მავალდებულებელი საკანონმდებლო ზომის გატარებას, თუკი არსებობს საკმარისი საფუძველი ვარაუდისთვის, რომ შესაბამისი წევრი ქვეყნის ეროვნული უსაფრთხოება რეალური და მიმდინარე ან განჭვრეტადი სერიოზული საფრთხის წინაშეა. იმ შემთხვევაშიც, თუ ეს ზომა ელექტრონული საკომუნიკაციო მომსახურების ყველა მომხმარებელს განურჩევლად შეეხება და, ერთი შეხედვით, არ არსებობს მათი კავშირი ეროვნული უსაფრთხოების წინაშე არსებულ საფრთხესთან, უნდა ჩაითვალოს, რომ ამგვარი საფრთხის არსებობას შეუძლია ეს კავშირი თავისთავად წარმოშვას.

ელექტრონული საკომუნიკაციო სისტემების ყველა მომხმარებლის მონაცემების პრევენციული შენახვა დროში შეზღუდული უნდა იყოს იმით, რაც მკაცრად აუცილებელია.

საფრთხის მიმდინარე ხასიათის გათვალისწინებით, მითითება ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ მონაცემების შენახვის შესახებ შეიძლება განახლდეს. თუმცა, მან განსაზღვრულ ხანგრძლივობას არ უნდა გადააჭარბოს და დაცვის მყარ გარანტიებს უნდა დაექვემდებაროს, რათა პირთა პერსონალური მონაცემების თვითნებურად გამოყენების რისკები თავიდან იქნას აცილებული. ამდენად, სასამართლოს განმარტებით, მონაცემთა შენახვას არ უნდა ჰქონდეს სისტემატური ხასიათი.

ქარტის მე-7 და მე-8 მუხლით გათვალისწინებულ ძირითად უფლებებში ჩარევის სიმძიმის გათვალისწინებით, მონაცემთა ბლანკეტური და განურჩეველი შენახვის ზომა გამოყენებულ უნდა იქნას მხოლოდ მაშინ, როდესაც ეროვნულ უსაფრთხოებას სერიოზული საფრთხე ექმნება. ამასთან, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისადმი გაცემული მითითება მონაცემების შენახვის შესახებ სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ განხილვას უნდა დაექვემდებაროს, რომელთა გადაწყვეტილებებსაც სავალდებულო ძალა ექნება. ამგვარი განხილვა აუცილებელია, რათა დადასტურდეს, რომ სერიოზული საფრთხე ნამდვილად არსებობს და ამ ზომის გამოყენების წინაპირობები და დაცვის გარანტიები დაცულია.

– საზოგადოებრივი უსაფრთხოების დაცვისა და დანაშაულთან ბრძოლის მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების პრევენციული შენახვის უზრუნველმყოფი საკანონმდებლო ზომები

სასამართლოს განმარტებით, დანაშაულის პრევენციის, გამოძიების, გამოვლენისა და სისხლისსამართლებრივი დევნის დაწყების მიზნით ქარტიის მე-7 და მე-8 მუხლებით გათვალისწინებულ უფლებებში სერიოზული ჩარევა შეიძლება გამართლებულ იქნეს მხოლოდ **მძიმე** დანაშაულთან ბრძოლით ან იმ შემთხვევაში, როცა საზოგადოებრივი უსაფრთხოება **სერიოზული საშიშროების** წინაშეა. შესაბამისად, ამ უფლებებში მხოლოდ მსუბუქი ხასიათის ჩარევა შეიძლება გამართლდეს ზოგადად დანაშაულის პრევენციის, გამოძიების, გამოვლენისა და სისხლის სამართლებრივი დევნის დაწყების მიზნით.

ეროვნული კანონმდებლობა, რომელიც მძიმე დანაშაულთან ბრძოლის ან საზოგადოებრივი უსაფრთხოების დაცვის მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტურ და განურჩეველი ხასიათის შენახვას უშვებს, აჭარბებს აბსოლუტური აუცილებლობის ფარგლებს და ვერ ჩაითვლება დასაშვებად დემოკრატიულ საზოგადოებაში. მათი სენსიტიური ბუნებიდან გამომდინარე, მნიშვნელოვანია, რომ ეს მონაცემები შენახულ იქნას საგამონაკლისო წესით.

ტრაფიკისა და ადგილმდებარეობის მონაცემების განურჩეველი და ბლანკეტური შენახვის წესი პრაქტიკულად მთელ საზოგადოებას ეხება, გამოანკლისის გარეშე. ამგვარი კანონმდებლობა ყოვლისმომცველია და იმ პირებზეც ვრცელდება, რომელთაც არაპირდაპირი შემხებლობაც კი არ აქვთ შესაძლო სისხლის სამართლის საქმესთან. კანონმდებლობით მონაცემთა შენახვა შეზღუდული არ არის დროით, გეოგრაფიული სივრცით, დანაშაულთან შესაძლო შემხებლობის მქონე პირთა ჯგუფით, ასევე პირთა წრით, რომლებმაც, სხვა მიზეზების გამო, შეიძლება გარკვეული წვლილი შეიტანონ მძიმე დანაშაულთან ბრძოლაში.

სასამართლოს განმარტებით, ამის საპირისპიროდ, მძიმე დანაშაულთან ბრძოლისა და საზოგადოებრივ უსაფრთხოებაზე სერიოზული თავდასხმების პრევენციის და მითუმეტეს, ეროვნული უსაფრთხოების დაცვის მიზანი ამართლებს ტრაფიკისა და ადგილმდებარეობის მონაცემების **მიზნობრივი** შენახვით უფლებაში სერიოზულ ჩარევას.

2002/58 დირექტივის მე-15(1) მუხლი, ქარტიის მე-7, მე-8, მე-11 და 52(1) მუხლების შუქზე, არ უკრძალავს წევრ სახელმწიფოს იმგვარი კანონმდებლობის მიღებას, რომელიც მძიმე დანაშაულთან ბრძოლის, საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული საფრთხეების თავიდან აცილებისა და ეროვნული უსაფრთხოების უზრუნველყოფის მიზნით, პრევენციული ზომის სახით, ტრაფიკისა და ადგილმდებარეობის მონაცემების მიზნობრივ შენახვას ითვალისწინებს, თუკი მონაცემების კატეგორიების, კომუნიკაციის საშუალებების, შესაბამისი პირების იდენტიფიცირებისა და შენახვის პერიოდის თვალსაზრისით, ამგვარი შენახვა მკაცრი აუცილებლობით არის შეზღუდული.

2002/58 დირექტივის მე-15(1) მუხლი, ქარტიის მე-7, მე-8, მე-11 და 52(1) მუხლების შუქზე, არ უკრძალავს წევრ სახელმწიფოს იმგვარი კანონმდებლობის მიღებას, რომელიც მძიმე დანაშაულთან ბრძოლის, საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული საფრთხეების თავიდან აცილებისა და ეროვნული უსაფრთხოების უზრუნველყოფის მიზნით, პრევენციული ზომის სახით, ტრაფიკისა და ადგილმდებარეობის მონაცემების **მიზნობრივ** შენახვას ითვალისწინებს, თუკი მონაცემების კატეგორიების, კომუნიკაციის საშუალებების, შესაბამისი პირების იდენტიფიცირებისა და შენახვის პერიოდის თვალსაზრისით, ამგვარი შენახვა მკაცრი აუცილებლობით არის შეზღუდული.

რაც შეეხება მონაცემთა შენახვასთან დაკავშირებულ შეზღუდვებს, ის შეიძლება შემოისაზღვროს პირთა კატეგორიების მიხედვით, თუ არსებობს ობიექტური მტკიცებულება, რომ ცალკეულ პირთა ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვით, შეიძლება გამომჟღავნდეს მძიმე დანაშაულთან მათი სულ მცირე არაპირდაპირი კავშირი ან თუ ამ მონაცემების შენახვა ამა თუ იმ ფორმით ხელს შეუწყობს მძიმე დანაშაულთან ბრძოლას ან საზოგადოებრივ ან ეროვნულ უსაფრთხოებასთან დაკავშირებული სერიოზული რისკების თავიდან აცილებას. ამ თვალსაზრისით, მნიშვნელოვანია, რომ შესაბამისი ეროვნული პროცედურებითა და ობიექტური მტკიცებულების საფუძველზე, წინასწარ მოხდეს იმ პირთა იდენტიფიცირება, რომლებიც წევრი სახელმწიფოს საზოგადოებრივ ან ეროვნულ უსაფრთხოებას საფრთხეს უქმნიან.

ასევე, შენახვა შეიძლება შემოსაზღვრული იყოს გეოგრაფიული არეალით, თუ ობიექტური და არადისკრიმინაციული გარემოებების საფუძველზე შესაბამისი ორგანოები მიიჩნევენ, რომ ამ ადგილებში მძიმე დანაშაულის ჩადენის მაღალი რისკი არსებობს. ამასთან, შენახვის ხანგრძლივობის განსაზღვრისას მხედველობაში უნდა იქნას მიღებული მისაღწევი მიზანი და იმ გარემოებათა არსებობა, რომლებიც უფლებაში ჩარევას ამართლებენ.

– საზოგადოებრივი უსაფრთხოების დაცვისა და დანაშაულთან ბრძოლის მიზნით, პირის ვინაობასთან დაკავშირებული მონაცემებისა და IP მისამართების პრევენციული შენახვის უზრუნველმყოფი საკანონმდებლო ზომები

სასამართლომ განმარტა, რომ IP მისამართები ტრაფიკის მონაცემებს წარმოადგენს, თუმცა, ისინი სხვა ნებისმიერი კომუნიკაციის მონაცემებისგან დამოუკიდებლად, ცალკე გროვდება და ძირითადად, იმ საბოლოო მოწყობილობის მესაკუთრის იდენტიფიცირების მიზანს ემსახურება, საიდანაც ინტერნეტ კავშირი დამყარდა. ელექტრონული ფოსტისა და ინტერნეტ-სატელეფონო საუბრებისგან განსხვავებით, ეს მონაცემი მხოლოდ იმ პირის შესახებ მონაცემებს ამჟღავნებს, რომელმაც კომუნიკაცია განახორციელა, ხოლო მესამე პირების შესახებ ინფორმაციას არ შეიცავს. შესაბამისად, ამ მხრივ, ის ნაკლებად სენსიტიური ხასიათისაა. თუმცა, სასამართლოს განმარტებით, რადგან IP მისამართები ინტერნეტ-მომხმარებლის სრული ონლაინ აქტივობების აღსარიცხად გამოიყენება, ის პირთა დეტალური პროფილის შექმნის შესაძლებლობას იძლევა. შესაბამისად, მათი შენახვა და შემდგომი ანალიზი ქარტიის მე-7 და მე-8 მუხლებით გარანტირებულ ძირითად უფლებებში სერიოზულ ჩარევას იწვევს.

მეორე მხრივ, სასამართლომ ხაზი გაუსვა, რომ დანაშაულის ონლაინ ჩადენის შემთხვევაში, IP მისამართი შეიძლება ერთადერთი საშუალება იყოს, რომელიც გამოძიებას შესაძლო დამნაშავის იდენტიფიცირების საშუალებას მისცემს. თუმცა, რადგანაც მომსახურების მიმწოდებლებს ანგარიშსწორებისთვის IP მისამართების შენახვა მხოლოდ ამ მონაცემთა განსაზღვრისთვის საჭირო ხანგრძლივობით სჭირდებათ, ონლაინ ჩადენილი დანაშაულის გამოვლენა შეუძლებელი ხდება დირექტივის მე-15 მუხლის პირველი პუნქტით გათვალისწინებული საკანონმდებლო ზომის მიღების გარეშე. ეს მონაცემები განსაკუთრებით მნიშვნელოვანია, როცა საქმე ბავშვთა პორნოგრაფიას, მის მოპოვებას, გავრცელებას, გადაცემას ან ონლაინ ხელმისაწვდომობას ეხება.

● პირთა ვინაობასთან დაკავშირებული მონაცემები

სასამართლომ განმარტა, რომ ელექტრონული საკომუნიკაციო სისტემების მომხმარებელთა ვინაობის შესახებ მონაცემი თავისთავად არ ქმნის კომუნიკაციების თარიღის, დროის, ხანგრძლივობისა და მიმღების ან კომუნიკაციის ადგილმდებარეობის გამჟღავნების შესაძლებლობას და ამ მომხმარებელთა საკონტაქტო დეტალების გარდა (როგორიც არის მათი მისამართები), მათი პირადი ცხოვრების შესახებ არანაირ ინფორმაციას არ ამჟღავნებს. შესაბამისად, ამ მონაცემების შენახვით უფლებაში ჩარევა სერიოზულად ვერ შეფასდება. აქედან გამომდინარე, სასამართლომ დასაშვებად მიიჩნია საკანონმდებლო ზომები, რომლებიც ამ მონაცემთა დამუშავებას, მათ შორის, მხოლოდ და მხოლოდ ამ მომხმარებელთა ვინაობის დადგენის მიზნით მონაცემთა შენახვასა და მათზე წვდომას შეეხება. სასამართლომ განმარტა, რომ დანაშაულის პრევენციის, გამოძიების, გამოვლენისა და სისხლისსამართლებრივი დევნის დაწყების მიზნებით და იმ შემთხვევაშიც კი, თუ არ არსებობს მისაღწევ მიზანსა და ელექტრონული საკომუნიკაციო სისტემების მომხმარებელთა მონაცემებს შორის კავშირი, დირექტივის მე-15 მუხლის 1-ლი პუნქტი არ გამორიცხავს იმგვარი საკანონმდებლო ზომების მიღებას, რომლებიც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს შეუზღუდავი დროით ამ მონაცემების შენახვას დაავალდებულებს.

- მძიმე დანაშაულთან ბრძოლის მიზნით ტრაფიკისა და ადგილმდებარეობის მონაცემების გადაუდებელი წესით შენახვის უზრუნველმყოფი საკანონმდებლო ზომები

2002/58 დირექტივის შესაბამისად, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის მიერ დამუშავებული და შენახული ტრაფიკისა და ადგილმდებარეობის მონაცემები კანონით დადგენილი ვადის გასვლის შემდგომ უნდა წაიშალოს ან ანონიმური გახდეს. თუმცა, მონაცემთა შენახვისა და დამუშავებისას შეიძლება წარმოიშვას ვითარება, როცა აუცილებელი ხდება, მიმწოდებელმა გააგრძელოს ამ მონაცემთა შენახვა მძიმე დანაშაულის ან ეროვნული უსაფრთხოებისათვის საშიშროების შემქმნელი საქმიანობების გამოვლენის მიზნით, როცა დანაშაული ან საქმიანობა, რომელიც ეროვნული უსაფრთხოებისთვის საფრთხის შემცველია, უკვე მოხდა ან შესაბამისი გარემოებების ობიექტური გამოკვლევით ამგვარი ქმედებების ჩადენის გონივრული ეჭვი ჩნდება. ამ შემთხვევებში, შესაბამისი ორგანოს გადაწყვეტილებით, რომელიც სასამართლო განხილვას ექვემდებარება, შესაძლებელია ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებმა გააგრძელონ მათთან არსებული ტრაფიკისა და ადგილმდებარეობის მონაცემების გადაუდებელი წესით შენახვა.

ამავდროულად, წევრი ქვეყნები ვალდებულნი არიან ჩამოაყალიბონ კონკრეტული მიზნები, რომელთა მისაღწევად აუცილებელია მონაცემთა გადაუდებელი წესით შენახვა. სასამართლოს განმარტებით, უფლებაში ასეთი სერიოზული ჩარევა შეიძლება მხოლოდ მძიმე დანაშაულთან ბრძოლისა და ეროვნული უსაფრთხოების დაცვის მიზნებით გამართლდეს. ამას გარდა, იმისათვის, რომ ჩარევა არ გასცდეს აბსოლუტური აუცილებლობის ფარგლებს, ტრაფიკისა და ადგილმდებარეობის მხოლოდ ის მონაცემები უნდა იქნას შენახული, რომელსაც შეუძლია მძიმე დანაშაული ან ეროვნული უსაფრთხოებისათვის საფრთხის შემცველი საქმიანობები გამოამჟღავნოს. ასევე, შენახვის ვადა უნდა შეიზღუდოს აბსოლუტურ მინიმუმამდე, თუმცა სათანადო გარემოებების არსებობისას, დასაშვებია ამ ვადის გახანგრძლივება.

ტრაფიკისა და ადგილმდებარეობის მონაცემების გადაუდებელი წესით შენახვა შეიძლება გავრცელდეს იმ პირებზეც, რომლებიც არ არიან ეჭვმიტანილი მძიმე დანაშაულის ან ეროვნული უსაფრთხოებისთვის საფრთხის შემცველი საქმიანობის ჩადენასა თუ მათ დაგეგმვაში, თუ მონაცემებმა, ობიექტური და არადისკრიმინაციული ფაქტორების გათვალისწინებით, შეიძლება ნათელი მოჰფინოს მძიმე დანაშაულს ან ეროვნული უსაფრთხოებისთვის საშიშროების შემქმნელ საქმიანობას. ეს მონაცემები შეიძლება შეეხებოდეს მსხვერპლს, მის სოციალურ ან პროფესიულ წრეს, კონკრეტულ გეოგრაფიულ სივრცეს, სადაც მსგავსი დანაშაულებრივი ქმედებები დაიგეგმა ან მოხდა. შენახულ ტრაფიკისა და ადგილმდებარეობის მონაცემებზე წვდომა დასაშვებია მხოლოდ იმ მიზნების მისაღწევად, რომელთა მიღწევისთვისაც მიმწოდებლებს მონაცემების შენახვა დაევალათ. თუმცა, ეს წესი არ ეხება ეროვნული უსაფრთხოების დაცვის მიზნით მონაცემებზე წვდომის მოთხოვნას.

C 511/18 და C 512/18 საქმეთა პირველ შეკითხვასა და C 520/18 საქმის პირველ და მეორე შეკითხვაზე სასამართლოს პასუხი არის ის, რომ 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტი, ქარტიის მე-7, მე-8, მე-11 მუხლებისა და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, კრძალავს მე-15 მუხლის პირველი პუნქტით გათვალისწინებული მიზნების მისაღწევად იმგვარი საკანონმდებლო ზომების მიღებას, რომლებიც პრევენციული მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტურ და განურჩეველ შენახვას

ითვალისწინებს. ამის საპირისპიროდ, დირექტივის მე-15 მუხლის 1-ლი პუნქტი, ქარტიის მე-7, მე-8, მე-11 მუხლებისა და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, არ გამორიცხავს საკანონმდებლო ზომის გატარებას, რომელიც:

- ეროვნული უსაფრთხოების დაცვის მიზნით, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისათვის ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტური და განურჩეველი წესით შენახვის თაობაზე მითითების გაცემას ითვალისწინებს, როცა წევრი ქვეყნების ეროვნული უსაფრთხოება მნიშვნელოვანი საფრთხის წინაშეა, რაც არის ნამდვილი და მიმდინარე ან განჭვრეტადი ხასიათის. ამგვარი მითითების გაცემის შესახებ გადაწყვეტილება სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ ეფექტურ განხილვას უნდა დაექვემდებაროს, რომლის გადაწყვეტილება შესასრულებლად სავალდებულოა. განხილვის მიზანი უნდა იყოს იმის დადასტურება, რომ ასეთი ვითარება არსებობს და შესაბამისი პირობები და გარანტიები დაცულია. ამგვარი მითითება შეიძლება გაიცეს მკაცრად აუცილებელი შეზღუდული ვადით, რაც შეიძლება გახანგრძლივდეს, როდესაც საფრთხე განაგრძობს არსებობას.

- ეროვნული უსაფრთხოების დაცვის, მძიმე დანაშაულთან ბრძოლისა და საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული საშიშროების პრევენციის მიზნით, ითვალისწინებს ტრაფიკისა და ადგილმდებარეობის მონაცემების მიზნობრივ შენახვას, რომელიც ობიექტური და არადისკრიმინაციული გარემოებების საფუძველზე, შეზღუდულია შესაბამის პირთა კატეგორიებით ან გეოგრაფიული არეალით და ხორციელდება მკაცრად აუცილებელი ვადით, რომელიც შეიძლება გახანგრძლივდეს;

- ეროვნული უსაფრთხოების დაცვის, მძიმე დანაშაულთან ბრძოლისა და საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული საფრთხეების პრევენციის მიზნით, ითვალისწინებს ინტერნეტ კავშირის წყაროსთვის მინიჭებული IP მისამართების ბლანკეტურ და განურჩეველ შენახვას მკაცრად აუცილებელი განსაზღვრული ვადით;

- ეროვნული და საზოგადოებრივი უსაფრთხოების დაცვის, ასევე დანაშაულთან ბრძოლის მიზნით, ითვალისწინებს ელექტრონული საკომუნიკაციო სისტემების მომხმარებლების ვინაობის შესახებ ინფორმაციის ბლანკეტურ და განურჩეველ შენახვას;

- მძიმე დანაშაულთან ბრძოლისა და ეროვნული უსაფრთხოების დაცვის მიზნით, დასაშვებად მიიჩნევს ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისათვის მითითების მიცემას, უფლებამოსილი ორგანოს გადაწყვეტილების საფუძველზე (რომელიც ეფექტურ სასამართლო კონტროლს ექვემდებარება), შეზღუდული ვადით, გადაუდებელი წესით გააგრძელონ ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვა.

● სასამართლოს მსჯელობა C 511/18 საქმის მე-2 და მე-3 შეკითხვებზე

C 511/18 საქმეზე დასმული მე-2 და მე-3 კითხვებით, ეროვნულ სასამართლოს აინტერესებს, 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტი გამორიცხავს თუ არა ეროვნული კანონმდებლობის მიღებას, რომელიც ელექტრონული საკომუნიკაციო მომსახურების მიმწო-

დებლებს საკუთარ ქსელებში იმგვარი ზომის დანერგვას ავალდებულებს, რომელიც ტრაფიკისა და ადგილმდებარეობის მონაცემების ავტომატური ანალიზისა და რეალურ დროში შეგროვების, ასევე, დაინტერესებულ პირთათვის მათი მონაცემების დამუშავების შესახებ ინფორმაციის მიწოდების გარეშე, გამოყენებული საბოლოო მოწყობილობის ადგილმდებარეობის შესახებ ტექნიკური მონაცემების რეალურ დროში შეგროვების შესაძლებლობას იძლევა.

სასამართლომ თავდაპირველად მიმოიხილა ზემოაღნიშნული საკითხების მარეგულირებელი ნორმები და მიუთითა, რომ სადაზვერვო მეთოდები, რომლებსაც საფრანგეთის შიდა უსაფრთხოების კოდექსის L. 851-2 - L. 851-4 მუხლები ითვალისწინებს, მიმწოდებლებს ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვის სპეციალურ ვალდებულებას არ აკისრებს. რაც შეეხება შიდა უსაფრთხოების კოდექსის L. 851-3 მუხლით გათვალისწინებულ ავტომატურ ანალიზს, ეროვნული სასამართლოს განცხადებით, დამუშავების მიზანი შესაძლო ტერორისტული საფრთხის წყაროს გამოვლენაა. შიდა უსაფრთხოების კოდექსის L. 851-2 მუხლით გათვალისწინებული რეალურ დროში შეგროვება შეეხება მხოლოდ ერთ ან მეტ პირს, რომლებზეც მანამდე არსებობდა ეჭვი, რომ მათ შესაძლოა ტერორიზმის საფრთხესთან ჰქონდეთ კავშირი.

ამავდროულად, იმავე კოდექსის L. 851-3 მუხლის თანახმად, ამ მუხლით გათვალისწინებული ავტომატური ანალიზით შესაძლებელი არ არის მომხმარებელთა ვინაობის გამჟღავნება, თუმცა, ეს ხელს არ უშლის მის პერსონალურ მონაცემებად კლასიფიცირებას. სასამართლოს განმარტებით, იმავე მუხლის მე-4 პუნქტით გათვალისწინებული ღონისძიების შედეგად, შესაძლებელია, ამ პირთა ვინაობის მოგვიანებით გამორკვევა. ყველა პირი, რომელთა მონაცემებიც ავტომატურ ანალიზს დაექვემდებარა, იდენტიფიცირებადია. შესაბამისად, ეს მონაცემები პერსონალურ მონაცემებად უნდა ჩაითვალოს.

ტრაფიკისა და ადგილმდებარეობის მონაცემების ავტომატური ანალიზი

ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ შენახული ტრაფიკისა და ადგილმდებარეობის მონაცემების ავტომატურ ანალიზს, უფლებამოსილი ორგანოების მიერ განსაზღვრული პარამეტრების გამოყენებით და მათი მოთხოვნის საფუძველზე, თავად ეს მიმწოდებლები ახორციელებენ. შესაბამისად, მოწმდება ამ პარამეტრების შესაბამისი მომხმარებლის ყველა მონაცემი. ამდენად, უნდა მივიჩნიოთ, რომ ასეთი ავტომატური ანალიზი მიმწოდებლებს ელექტრონული საკომუნიკაციო სისტემის ყველა მომხმარებლის ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტურად და განურჩევლად დამუშავებას ავალდებულებს. სასამართლომ ეს წესი ქარტიის მე-7, მე-8 და მე-11 მუხლებში მნიშვნელოვან ჩარევად და დირექტივის მე-15 მუხლიდან გადახვევად შეაფასა. სასამართლოს განმარტებით, ჩარევის სერიოზულობას ადასტურებს ის ფაქტიც, რომ მონაცემთა ავტომატური ანალიზით შეიძლება ონლაინ ნანახი ინფორმაციის ტიპის განსაზღვრა და ის ეხება აბსოლუტურად ყველა პირს, ვინც ელექტრონული კომუნიკაციების სისტემას იყენებს.

ამ შემთხვევაში, უფლებაში ჩარევა პროპორციულად შეიძლება ჩაითვალოს მხოლოდ მაშინ, თუ კანონმდებლობა, რომელიც ამ მონაცემებზე უფლებამოსილი ორგანოების წვდომას

უშვებს, არა მხოლოდ მისაღწევი მიზნის შესაბამისია, არამედ მონაცემთა გამოყენების მატერიალურ და საპროცესო პირობებსაც განსაზღვრავს.

ასევე, ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტური და განურჩეველი შენახვით, განსაკუთრებით კი ამ მონაცემთა ავტომატური ანალიზის შედეგად, უფლებაში ჩარევა პროპორციულობის პრინციპს მხოლოდ იმ შემთხვევაში შეესაბამება, როცა წევრი სახელმწიფოების ეროვნულ უსაფრთხოებას მნიშვნელოვანი საფრთხე ემუქრება და ეს საფრთხე ნამდვილი და მიმდინარე ან განჭვრეტადია. ამავდროულად, მონაცემების შენახვის ხანგრძლივობა მკაცრი აუცილებლობის ფარგლებს არ უნდა გასცდეს, ხოლო ავტომატურ ანალიზზე ნებართვის გაცემა სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ განხილვას უნდა დაექვემდებაროს, რომლის მიერ მიღებულ გადაწყვეტილებას სავალდებულო ძალა აქვს.

წინასწარ შედგენილი მოდელები და ჩამოყალიბებული კრიტერიუმები, რომლის საფუძველზეც მონაცემები მუშავდება, უნდა იყოს კონკრეტული, უტყუარი, არადისკრიმინაციული და უნდა შეეძლოს იმგვარი შედეგების მოტანა, რომელიც პირთა ვინაობის განსაზღვრის შესაძლებლობას იძლევა.

ამავდროულად, მოდელები და კრიტერიუმები, რომელთა მიხედვითაც ავტომატურად ანალიზდება მონაცემები, არ უნდა ეფუძნებოდეს წანამძღვრებს, რომ რასობრივი ან ეთნიკური წარმომავლობა, პოლიტიკური შეხედულებები, რელიგიური ან ფილოსოფიური მრწამსი, პროფკავშირის წევრობა, ან ინფორმაცია პირის ჯანმრთელობისა და სქესობრივი ცხოვრების შესახებ, თავისთავად და პირის ქმედებისგან დამოუკიდებლად, უშუალოდ დაკავშირებულია ტერორიზმის პრევენციის მიზანთან. ამდენად, ტერორიზმის პრევენციის მიზნით ავტომატური ანალიზისათვის წინასწარ განსაზღვრული მოდელები და კრიტერიუმები არ შეიძლება იზოლირებულად განსაკუთრებული კატეგორიის მონაცემებს ეფუძნებოდეს.

ამასთან, ავტომატური ანალიზისას, არსებობს შეცდომის დაშვების რისკი. შესაბამისად, ამგვარი დამუშავების ნებისმიერი დადებითი შედეგი უნდა შემოწმდეს ინდივიდუალურად, არაავტომატური საშუალებებით, დაინტერესებული პირების უფლებებზე ზეგავლენის მქონე ინდივიდუალური ღონისძიების განხორციელებამდე (მაგალითად, როგორიც არის ტრაფიკისა და ადგილმდებარეობის მონაცემების რეალურ დროში შემდგომი შეგროვება). მხოლოდ ავტომატური დამუშავება არ შეიძლება იყოს ამგვარი ღონისძიების გატარების საფუძველი. სისტემატურად უნდა შემოწმდეს, არის თუ არა წინასწარ განსაზღვრული მოდელები და კრიტერიუმები სანდო და განახლებული, რათა ისინი, მათი გამოყენება და გამოყენებული მონაცემთა ბაზები დისკრიმინაციულ ხასიათს არ ატარებდეს, შემოფარგლული იყოს მკაცრი აუცილებლობით და ემსახურებოდეს ტერორისტული საქმიანობის პრევენციის მიზანს.

ტრაფიკისა და ადგილმდებარეობის მონაცემების ხელით ძიებაში შეგროვება

საფრანგეთის შიდა უსაფრთხოების კოდექსის L. 851 2 მუხლის თანახმად, ტრაფიკისა და ადგილმდებარეობის მონაცემები რეალურ დროში შეიძლება შეგროვდეს ტერორიზმის საფრთხეებთან შესაძლო კავშირის მქონე პირებისა და მათთან დაკავშირებული პირის ან პირთა მიმართ (ინდივიდუალურად), როცა არსებობს მყარი საფუძვლები, რომ ეს პირი ან

ან პირები ნებართვის მიზანთან შემხებლობის მქონე ინფორმაციას ფლობენ. ამ მონაცემებით, უფლებამოსილ ორგანოებს შეუძლიათ ავტორიზაციის განმავლობაში, რეალურ დროში, თვალი ადევნონ, თუ ვისთან აქვთ კომუნიკაცია ამ პირებს, მათი კომუნიკაციის ხანგრძლივობას, საცხოვრებელ ადგილს და მოძრაობის არეალს. ამით შეიძლება ასევე, გამჟღავნდეს ონლაინ ნანახი ინფორმაციის სახე. ეს მონაცემები პირადი ცხოვრების შესახებ ზუსტი დასკვნების გაკეთებისა და პირთა პროფილების შექნის შესაძლებლობას იძლევა, რაც კომუნიკაციების შინაარსზე არანაკლებ სენსიტიური ინფორმაციაა.

საფრანგეთის შიდა უსაფრთხოების კოდექსის L. 851-4 მუხლი მიუთითებს, რომ მონაცემების რეალურ დროში შეგროვება შესაძლებელია ასევე, განხორციელდეს საბოლოო მოწყობილობის ადგილმდებარეობის განმსაზღვრელი ტექნიკური მონაცემების მიმართ. ეს მონაცემები შესაბამის დეპარტამენტს რეალურ დროში მიეწოდება, რომელიც პრემიერ-მინისტრს ცნობებს წარუდგენს. შესაბამისად, დეპარტამენტს რეალურ დროში ხელი მიუწვდება საბოლოო მოწყობილობათა (მაგალითად, მობილური ტელეფონების) ადგილმდებარეობის შესახებ. ყოველივე ეს 2002/58 დირექტივით გათვალისწინებული მონაცემების კონფიდენციალურობის პრინციპიდან გადახვევას და ქარტიის მე-7, მე-8 და მე-11 მუხლებში ჩარევას წარმოადგენს. ეს ჩარევა განსაკუთრებით სერიოზული ხასიათის არის, ვინაიდან უფლებამოსილ ორგანოებს მობილური ტელეფონების მომხმარებლების მოძრაობის ტრაექტორიის შესახებ ზუსტ ინფორმაციას აწვდის. ის ასევე, ითვალისწინებს დაინტერესებული პირების ტრაფიკის მონაცემების რეალურ დროში შეგროვებას.

სასამართლომ განმარტა, რომ ტერორიზმის პრევენციის მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების შეგროვება დასაშვებია, თუმცა მხოლოდ იმ პირთა შესახებ, რომელთა მიმართ ტერორისტულ საქმიანობაში ჩართულობის საფუძვლიანი ეჭვი არსებობს. ამ შემთხვევაში, მონაცემების რეალურ დროში შეგროვების შესახებ გადაწყვეტილება ეროვნული კანონმდებლობით გათვალისწინებულ ობიექტურ და არადისკრიმინაციულ კრიტერიუმებს უნდა დაეფუძნოს. გარდა ამისა, გადაწყვეტილება უნდა ექვემდებარებოდეს სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ წინასწარ განხილვას, ხოლო გადაუდებელი აუცილებლობისას, მისი კანონიერება უნდა შემოწმდეს მოკლე ვადაში.

● იმ პირთა შეტყობინება, რომელთა მონაცემები შეგროვდა და გაანალიზდა

უფლებამოსილი ორგანოები ვალდებული არიან დაინტერესებულ პირებს აცნობონ ტრაფიკისა და ადგილმდებარეობის მონაცემების რეალურ დროში შეგროვების შესახებ მას შემდეგ, რაც ამგვარი შეტყობინება დასახული ამოცანების შესრულებას ხელს ვეღარ შეუშლის. ინფორმირება მნიშვნელოვანია, რამდენადაც პირებს ეძლევათ ქარტიის მე-7 და მე-8 მუხლებით გათვალისწინებული უფლებების რეალიზების შესაძლებლობა, შეუძლიათ მოითხოვონ შეგროვებულ მონაცემებზე წვდომა, მათი შეცვლა, წაშლა. შეტყობინებით მათთვის შესაძლებელი ხდება სასამართლოს წინაშე სამართლებრივი დაცვის ეფექტიანი საშუალების გამოყენება.

რაც შეეხება ტრაფიკისა და ადგილმდებარეობის მონაცემების ავტომატური ანალიზის კონტექსტში შეტყობინებას, უფლებამოსილი ორგანო ვალდებულია ამგვარი ანალიზის

შესახებ ზოგადი ხასიათის ინფორმაცია გამოაქვეყნოს, კონკრეტული პირების შეტყობინების გარეშე. თუმცა, თუ მონაცემები ნებართვის გადაწყვეტილებაში მითითებულ პარამეტრებს ემთხვევა, რის შედეგადაც ხელისუფლება განსაზღვრავს დაინტერესებულ პირს, რომლის მონაცემების უფრო სიღრმისეული ანალიზია საჭირო, ამ შემთხვევაში, ამ პირის ინდივიდუალური ინფორმირება აუცილებელია.

C 511/18 საქმის მეორე და მესამე შეკითხვებზე სასამართლოს პასუხი არის ის, რომ 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტი, ქარტიის მე-7, მე-8, მე-11 და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, არ გამორიცხავს ეროვნულ კანონმდებლობას, რომელიც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს ტრაფიკისა და ადგილმდებარეობის მონაცემების ავტომატურ ანალიზსა და რეალურ დროში შეგროვებას, ასევე გამოყენებული საბოლოო მოწყობილობის ადგილმდებარეობის შესახებ ტექნიკური მონაცემების რეალურ დროში შეგროვებას ავალდებულებს, თუკი:

- ავტომატური ანალიზი დაიშვება მხოლოდ იმ ვითარებაში, როცა წევრი ქვეყნების ეროვნული უსაფრთხოება, ნამდვილი და მიმდინარე ან განჭვრეტადი, მნიშვნელოვანი საშიშროების წინაშეა და ამგვარი ანალიზი სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ ეფექტურ განხილვას ექვემდებარება, რომლის გადაწყვეტილება შესასრულებლად სავალდებულოა. განხილვის მიზანია დადასტურდეს, რომ არსებობს ვითარება, რომელიც ამ ზომის გამოყენების აუცილებელი წინაპირობაა და შესაბამისი პირობები და გარანტიები დაცულია;
- ტრაფიკისა და ადგილმდებარეობის მონაცემების რეალურ დროში შეგროვება შემოიფარგლება იმ პირთა წრით, რომელთა მიმართ ტერორისტულ საქმიანობაში ამა თუ იმ ფორმით ჩართულობის შესახებ საფუძვლიანი ეჭვი არსებობს, შეგროვება კი ექვემდებარება სასამართლოს ან დამოუკიდებელი ადამინისტრაციული ორგანოს მიერ წინასწარ განხილვას, რომლის მიერ მიღებული გადაწყვეტილება შესასრულებლად სავალდებულოა. ეს ემსახურება მონაცემების რეალურ დროში შეგროვების მკაცრი აუცილებლობის ფარგლებში განხორციელებას. გადაუდებელი აუცილებლობისას, ამგვარი განხილვა უნდა შედგეს უმოკლეს ვადაში.

C 512/18 საქმეზე მეორე შეკითხვა

ეროვნულ სასამართლოს ამ შეკითხვით სურდა გამოერკვია, 2000/31 დირექტივის დებულებები, ქარტიის მე-6, მე-7, მე-8, მე-11 მუხლებისა და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, გამორიცხავს თუ არა ეროვნულ კანონმდებლობას, რომელიც საჯარო კომუნიკაციების მომსახურებაზე ონლაინ წვდომის მიმწოდებელსა და ჰოსტინგის მომსახურების მიმწოდებელს ამ მომსახურებასთან დაკავშირებული პერსონალურ მონაცემების ბლანკეტურად და განურჩეველი წესით შენახვას ავალდებულებს.

ეროვნული სასამართლო მიიჩნევდა, რომ ამ მომსახურებაზე 2000/31 დირექტივა ვრცელდება, თუმცა, სასამართლომ განმარტა, რომ პერსონალური მონაცემების და კომუნიკაციების კონფიდენციალურობის დაცვის საკითხები 2002/58 დირექტივის ან 2016/679 რეგულაციის (მონაცემთა დაცვის ზოგადი რეგულაცია) საფუძველზე უნდა განიმარტოს.

სასამართლომ მიუთითა, რომ რეგულაციის 23-ე მუხლის პირველი პუნქტი, მსგავსად 2002/58 დირექტივის მე-15 მუხლის 1 პუნქტისა, წევრ სახელმწიფოებს უფლებამოსილებას ანიჭებს, კანონით დადგენილი მიზნის მისაღწევად შემოღებული საკანონმდებლო ზომების გამოყენებით, შეზღუდონ ამ მუხლში მითითებული ვალდებულებების და უფლებების ფარგლები, თუ ეს შეზღუდვა ძირითადი უფლებებისა და თავისუფლებების არსს არ აზიანებს და დემოკრატიულ საზოგადოებაში სათანადო და პროპორციულ ზომას წარმოადგენს.

სასამართლომ მიუთითა, რომ რეგულაციის 23-ე მუხლის პირველი პუნქტი, მსგავსად 2002/58 დირექტივის მე-15 მუხლის 1 პუნქტისა, წევრ სახელმწიფოებს უფლებამოსილებას ანიჭებს, კანონით დადგენილი მიზნის მისაღწევად შემოღებული საკანონმდებლო ზომების გამოყენებით, შეზღუდონ ამ მუხლში მითითებული ვალდებულებების და უფლებების ფარგლები, თუ ეს შეზღუდვა ძირითადი უფლებებისა და თავისუფლებების არსს არ აზიანებს და დემოკრატიულ საზოგადოებაში სათანადო და პროპორციულ ზომას წარმოადგენს.

სასამართლოს განმარტებით, C 511/18 და C 512/18 საქმეების პირველ შეკითხვასა და C 520/18 საქმის პირველ და მეორე შეკითხვებზე სასამართლოს მიერ გაკეთებული შეფასებები და განმარტებები ასევე ესადაგება 2016/679 რეგულაციის 23-ე მუხლს.

C 512/18 საქმის მე-2 შეკითხვაზე სასამართლოს პასუხი არის ის, რომ 2000/31 დირექტივა უნდა განიმარტოს იმგვარად, რომ ის არ ვრცელდება კომუნიკაციების კონფიდენციალურობის დაცვასა და ინფორმაციული საზოგადოების სერვისების კონტექსტში ფიზიკური პირების პერსონალური მონაცემების დამუშავებაზე. ამგვარ დაცვას არეგულირებს, შესაბამისად, 2002/58 დირექტივა ან 2016/679 რეგულაცია. 2016/679 რეგულაციის 23-ე მუხლის პირველი პუნქტი, ქარტიის მე-7, მე-8 და მე-11 მუხლებისა და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, გამორიცხავს ეროვნულ კანონმდებლობას, რომელიც საჯარო კომუნიკაციების მომსახურებაზე ონლაინ წვდომის მიმწოდებელსა და ჰოსტინგის მომსახურების მიმწოდებელს ამ მომსახურებასთან დაკავშირებული პერსონალური მონაცემების ბლანკეტურად და განურჩეველი წესით შენახვას ავალდებულებს.

● C 520/18 საქმეზე მესამე შეკითხვა

სასამართლოს ამ შეკითხვით აინტერესებს, შეუძლია თუ არა ეროვნულ სასამართლოს ადგილობრივი კანონის გამოყენება, რომელიც მას უფლებამოსილებას ანიჭებს, ეროვნული უსაფრთხოების დაცვისა და დანაშაულთან ბრძოლის მიზნის მისაღწევად, გადაავადოს, ეროვნული კანონმდებლობით ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისთვის დაწესებული ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტური და განურჩეველი შენახვის უკანონოდ ცნობა (რისი ვალდებულებაც მას ამ კანონმდებლობით ეკისრება) იმ შემთხვევაში, თუ ის არ შეესაბამება 2002/58 დირექტივის მე-15 მუხლის 1-ლ პუნქტს, ქარტიის მე-7, მე-8, მე-11 მუხლებისა და 52 მუხლის 1-ლი პუნქტების გათვალისწინებით.

სასამართლომ აღნიშნა, რომ ევროკავშირის კანონმდებლობა წევრი ქვეყნების კანონმდებლობის მიმართ უპირატესი ძალის მქონეა. თუ ევროკავშირის კანონმდებლობის

მოთხოვნათა შესაბამისად ეროვნული სამართლებრივი ნორმების განმარტება შეუძლებელია, ადგილობრივი სასამართლო ვალდებულია, უპირატესობა ევროკავშირის ნორმებს მიანიჭოს და არ გამოიყენოს ეროვნული კანონმდებლობის დებულებები, რომლებიც მას ეწინააღმდეგება.

სასამართლოს განმარტებით, ეროვნული კანონმდებლობის მიმართ ევროკავშირის კანონმდებლობის პრიმატს და მისი ერთგვაროვანი გამოყენების წესს საფუძველი გამოეცლება, თუ ადგილობრივ სასამართლოებს მიეცემათ უფლებამოსილება, თუნდაც დროებით, უპირატესობა იმ ეროვნულ ნორმებს მიანიჭონ, რომლებიც ევროკავშირის დებულებებს ეწინააღმდეგება.

სასამართლომ მიუთითა, რომ განსახილველი ეროვნული კანონმდებლობის მოქმედების ძალის შენარჩუნებით, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს ადგილობრივი სამართლებრივი ნორმები ევროკავშირის კანონმდებლობის საწინააღმდეგო ვალდებულებებს დააკისრებს, რაც იმ პირთა ძირითად უფლებაში მნიშვნელოვან ჩარევას წარმოადგენს, რომელთა მონაცემებიც იქნა შენახული. შესაბამისად, ეროვნულ სასამართლოს არ შეუძლია გამოიყენოს საკანონმდებლო ნორმა, რომელიც უფლებამოსილებას ანიჭებს, განსახილველი ეროვნული კანონმდებლობის უკანონოდ ცნობა გადაავადოს.

სასამართლოს განმარტებით, ეროვნული კანონმდებლობის საფუძველზე უნდა გადაწყდეს, დაიშვება თუ არა ევროკავშირის კანონმდებლობის დარღვევის შედეგად შენახული ტრაფიკისა და ადგილმდებარეობის მონაცემებიდან მიღებული ინფორმაციისა და მტკიცებულებების გამოყენება იმ პირთა მიმართ აღძრულ სისხლის სამართლის საქმეებში, რომლებიც მძიმე დანაშაულის ჩადენაში არიან ეჭვმიტანილნი. ამასთან, 2002/58 დირექტივის მოთხოვნათა დარღვევით მოპოვებული ინფორმაციისა და მტკიცებულებათა დასაშვებობისა და გამოყენების მარეგულირებელი წესები არ უნდა იყოს შიდა კანონმდებლობის დარღვევით მოპოვებული ინფორმაციისა და მტკიცებულებათა დასაშვებობისა და გამოყენების შესახებ ნორმებზე ნაკლებად ხელსაყრელი.

ევროკავშირის კანონმდებლობის მოთხოვნების დარღვევით მოპოვებული მტკიცებულებების საქმიდან გამორიცხვაზე მსჯელობისას, მხედველობაშია მისაღები, ხომ არ არის შეჯიბრებითობის პრინციპისა და, შესაბამისად, ამ მტკიცებულებებითა და ინფორმაციის დაშვების შედეგად, სამართლიანი სასამართლოს უფლების დარღვევის რისკი. თუ სასამართლო მიიჩნევს, რომ მხარეს არ აქვს მოსაზრებების სათანადოდ გამოთქმის შესაძლებლობა იმ სფეროსთან დაკავშირებულ მტკიცებულებასთან მიმართებით, რომელზეც მოსამართლეებს არ გააჩნიათ სათანადო ცოდნა და თუ ამ მტკიცებულებას შეიძლება გადამწყვეტი მნიშვნელობა ჰქონდეს ფაქტების შეფასებისთვის, სასამართლომ ის უნდა გამორიცხოს საქმიდან.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, სასამართლომ დაადგინა, რომ დირექტივის მე-15 მუხლის პირველი პუნქტი სისხლის სამართლის საქმის განმხილველ ეროვნულ სასამართლოებს ავალდებულებს, არ დაურთონ საქმეს მტკიცებულება ან ინფორმაცია,რომელიც მოპოვებულ იქნა ევროკავშირის კანონმდებლობის დარღვევით, მონაცემთა ბლანკეტური და

სასამართლოს გადაწყვეტილება

01 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტი, ქარტიის მე-7, მე-8, მე-11 მუხლებისა და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, კრძალავს მე-15 მუხლის პირველი პუნქტით გათვალისწინებული მიზნების მისაღწევად იმგვარი საკანონმდებლო ზომების მიღებას, რომლებიც პრევენციული მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტურ და განურჩეველ შენახვას ითვალისწინებს. ამის საპირისპიროდ, დირექტივის მე-15 მუხლის 1-ლი პუნქტი, ქარტიის მე-7, მე-8, მე-11 მუხლებისა და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, არ გამორიცხავს საკანონმდებლო ზომის გატარებას, რომელიც:

ეროვნული უსაფრთხოების დაცვის მიზნით, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისათვის ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტური და განურჩეველი წესით შენახვის თაობაზე მითითების გაცემას ითვალისწინებს, როცა წევრი ქვეყნების ეროვნული უსაფრთხოება მნიშვნელოვანი საფრთხის წინაშეა, რაც არის ნამდვილი და მიმდინარე ან განჭვრეტადი ხასიათის. ამგვარი მითითების გაცემის შესახებ გადაწყვეტილება სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ ეფექტურ განხილვას უნდა დაექვემდებაროს, რომლის გადაწყვეტილება შესასრულებლად სავალდებულოა. განხილვის მიზანი უნდა იყოს იმის დადასტურება, რომ ასეთი ვითარება არსებობს და შესაბამისი პირობები და გარანტიები დაცულია. ამგვარი მითითება შეიძლება გაიცეს მკაცრად აუცილებელი შეზღუდული ვადით, რაც შეიძლება გახანგრძლივდეს, როდესაც საფრთხე განაგრძობს არსებობას.

ეროვნული უსაფრთხოების დაცვის, მძიმე დანაშაულთან ბრძოლისა და საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული საშიშროების პრევენციის მიზნით, ითვალისწინებს ტრაფიკისა და ადგილმდებარეობის მონაცემების მიზნობრივ შენახვას, რომელიც ობიექტური და არადისკრიმინაციული გარემოებების საფუძველზე, შეზღუდულია შესაბამის პირთა კატეგორიებით ან გეოგრაფიული არეალით და ხორციელდება მკაცრად აუცილებელი ვადით, რომელიც შეიძლება გახანგრძლივდეს;

ეროვნული უსაფრთხოების დაცვის, მძიმე დანაშაულთან ბრძოლისა და საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული საფრთხეების პრევენციის მიზნით, ითვალისწინებს ინტერნეტ კავშირის წყაროსთვის მინიჭებული IP მისამართების ბლანკეტურ და განურჩეველ შენახვას მკაცრად აუცილებელი განსაზღვრული ვადით;

ეროვნული და საზოგადოებრივი უსაფრთხოების დაცვის, ასევე დანაშაულთან ბრძოლის მიზნით, ითვალისწინებს ელექტრონული საკომუნიკაციო სისტემების მომხმარებლების ვინაობის შესახებ ინფორმაციის ბლანკეტურ და განურჩეველ შენახვას;

მძიმე დანაშაულთან ბრძოლისა და ეროვნული უსაფრთხოების დაცვის მიზნით, დასაშვებად მიიჩნევს ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისათვის მითითების მიცემას, უფლებამოსილი ორგანოს გადაწყვეტილების საფუძ-

ველზე (რომელიც ეფექტურ სასამართლო კონტროლს ექვემდებარება), შეზღუდული ვადით, გადაუდებელი წესით გააგრძელონ ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვა,

იმ პირობით, თუ ცხადი და ზუსტი ნორმების საფუძველზე, ეს ზომები უზრუნველყოფენ მონაცემების შენახვის სათანადო მატერიალურ და პროცედურულ პირობებთან შესაბამისობას და შესაბამისი პირებისათვის უფლებამოსილების ბოროტად გამოყენების რისკისგან დაცვის ეფექტური გარანტიების არსებობას.

02 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტი, ქარტიის მე-7, მე-8, მე-11 და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, არ გამორიცხავს ეროვნულ კანონმდებლობას, რომელიც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს ტრაფიკისა და ადგილმდებარეობის მონაცემების ავტომატურ ანალიზსა და რეალურ დროში შეგროვებას, ასევე გამოყენებული საბოლოო მოწყობილობის ადგილმდებარეობის შესახებ ტექნიკური მონაცემების რეალურ დროში შეგროვებას ავალდებულებს, თუკი:

ავტომატური ანალიზი დაიშვება მხოლოდ იმ ვითარებაში, როცა წევრი ქვეყნების ეროვნული უსაფრთხოება, ნამდვილი და მიმდინარე ან განჭვრეტადი, მნიშვნელოვანი საშიშროების წინაშეა და ამგვარი ანალიზი სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ ეფექტურ განხილვას ექვემდებარება, რომლის გადაწყვეტილება შესასრულებლად სავალდებულოა. განხილვის მიზანია დადასტურდეს, რომ არსებობს ვითარება, რომელიც ამ ზომის გამოყენების აუცილებელი წინაპირობაა და შესაბამისი პირობები და გარანტიები დაცულია;

ტრაფიკისა და ადგილმდებარეობის მონაცემების რეალურ დროში შეგროვება შემოიფარგლება იმ პირთა წრით, რომელთა მიმართ ტერორისტულ საქმიანობაში ამა თუ იმ ფორმით ჩართულობის შესახებ საფუძვლიანი ეჭვი არსებობს, შეგროვება კი ექვემდებარება სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ წინასწარ განხილვას, რომლის მიერ მიღებული გადაწყვეტილება შესასრულებლად სავალდებულოა. ეს ემსახურება მონაცემების რეალურ დროში შეგროვების მკაცრი აუცილებლობის ფარგლებში განხორციელებას. გადაუდებელი აუცილებლობისას, ამგვარი განხილვა უნდა შედგეს უმოკლეს ვადაში.

03 2000/31 დირექტივა („დირექტივა ელექტრონული კომერციის შესახებ“) უნდა განიმარტოს იმგვარად, რომ ის არ ვრცელდება კომუნიკაციების კონფიდენციალურობის დაცვასა და ინფორმაციული საზოგადოების სერვისების კონტექსტში ფიზიკური პირების პერსონალური მონაცემების დამუშავებაზე. ამგვარ დაცვას არეგულირებს, შესაბამისად, 2002/58 დირექტივა ან 2016/679 რეგულაცია. 2016/679 რეგულაციის 23-ე მუხლის პირველი პუნქტი, ქარტიის მე-7, მე-8 და მე-11 მუხლებისა და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, გამორიცხავს ეროვნულ კანონმდებლობას, რომელიც საჯარო კომუნიკაციების მომსახურებაზე ონლაინ წვდომის მიმწოდებელსა და ჰოსტინგის მომსახურების მიმწოდებელს ამ მომსახურებასთან დაკავშირებული პერსონალური მონაცემების ბლანკეტურად და განურჩეველი წესით შენახვას ავალდებულებს.

04 ეროვნულ სასამართლოს არ შეუძლია გამოიყენოს ადგილობრივი საკანონმდებლო ნორმა, რომელიც უფლებამოსილებას ანიჭებს, იმ ეროვნული კანონმდებლობის უკანონოდ ცნობა გადაავადოს, რომელიც ეროვნული უსაფრთხოების დაცვისა და დანაშაულთან ბრძოლის მიზნით, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს ტრაფიკისა და ადგილმდებარეობის მონაცემების ბლანკეტურ და განურჩეველ შენახვას ავალდებულებს, რაც არ შეესაბამება 2002/58 დირექტივის მე-15 მუხლის პირველ პუნქტს, ძირითად უფლებათა ქარტიის მე-7, მე-8 და მე-11 მუხლებისა და 52-ე მუხლის პირველი პუნქტის გათვალისწინებით. მე-15 მუხლის პირველი პუნქტი, ეფექტურობის პრინციპის გათვალისწინებით, ეროვნულ სასამართლოებს ავალდებულებს, არ დაურთონ საქმეს მტკიცებულება ან ინფორმაცია, რომელიც მოპოვებულ იქნა ევროკავშირის კანონმდებლობის დარღვევით, მონაცემთა ბლანკეტური და განურჩეველი შენახვის გზით იმ პირთა მიმართ სისხლის სამართლის საქმისწარმოების კონტექსტში, რომლებიც ეჭვმიტანილნი არიან დანაშაულის ჩადენაში, თუ მათ არ შეუძლიათ სათანადოდ გამოთქვან მოსაზრებები იმ სფეროსთან დაკავშირებულ ინფორმაციასა და მტკიცებულებებთან მიმართებით, რომელზეც მოსამართლეებს არ გააჩნიათ სათანადო ცოდნა და თუ მათ შეიძლება გადამწყვეტი მნიშვნელობა ჰქონდეს ფაქტების შეფასებისთვის.

TELE2 SVERIGE AB V POST- OCH TELESTYRELSEN AND SECRETARY OF STATE FOR THE HOME DEPARTMENT V TOM WATSON AND OTHERS

21/12/2016

ევროკავშირის მართლმსაჯულების სასამართლოს წინასწარი გადაწყვეტილება 2002/58/EC დირექტივის მე-15(1) მუხლის განმარტებას შეეხება. ეს დირექტივა ელექტრონული კომუნიკაციების სექტორში პერსონალური მონაცემების დამუშავებასა და პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვას უკავშირდება.

სასამართლოს შეკითხვით ორი დავის ფარგლებში მიმართეს: 1. ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელ Tele2 Sverige-სა და შვედეთის საფოსტო და სატელეკომუნიკაციო უწყებას (შემდგომ - PTS) შორის დავა, სადაც ამ უკანასკნელმა Tele2 Sverige-ს აბონენტთა და რეგისტრირებულ მომხმარებელთა შესახებ ტრაფიკისა და ადგილმდებარეობის მონაცემთა შენახვა მოსთხოვა (საქმე C-203-15). 2. ბატონ უოთსონს, ბრაისს, ლუისსა და შინაგან საქმეთა დეპარტამენტის სახელმწიფო მდივანს შორის დავა (გაერთიანებული სამეფო). ამ შემთხვევაში, დავა მონაცემთა შენახვისა და საგამოძიებო უფლებამოსილებების შესახებ აქტის (DRIPA) პირველი მუხლის ევროკავშირის კანონმდებლობასთან შესაბამისობას (საქმე C-698/15) შეეხებოდა.

სამართლებრივი საფუძვლები

- **ევროკავშირის კანონმდებლობა**
- **2002/58 დირექტივა**
- **2002/58 დირექტივის პრეამბულაში აღნიშნულია:**

02 ეს დირექტივა მიზნად ისახავს ევროპის კავშირის ძირითად უფლებათა ქარტიაში განმტკიცებული ძირითადი უფლებებისა და პრინციპების დაცვას, კერძოდ, ამ დირექტივის მიზანია ქარტიის მე-7 და მე-8 მუხლებით განმტკიცებულ უფლებათა სრულყოფილად დაცვის უზრუნველყოფა.

06 ინტერნეტი საერთო, გლობალური ინფრასტრუქტურის შექმნით, ელექტრონული კომუნიკაციების მომსახურების ფართო სპექტრის მიწოდებას უზრუნველყოფს და ამით ის ტრადიციული ბაზრის სტრუქტურას თავდაყირა აყენებს. ინტერნეტის მეშვეობით, საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების სერვისები მომხმარებლებს ახალ შესაძლებლობებს სთავაზობს, თუმცა, პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობისთვის ახალ რისკებსაც წარმოქმნის.

07 საჯარო კომუნიკაციების ქსელებთან მიმართებით, კონკრეტული სამართლებრივი, მაკონტროლებელი და დარგობრივი მუხლების მიღება აუცილებელია ფიზიკური პირების ძირითადი უფლებებისა და თავისუფლებების, ასევე იურიდიული პირების ლეგიტიმური ინტერესების დასაცავად, განსაკუთრებით, თუ გავითვალისწინებთ, რომ აბონენტებისა და მომხმარებლების მონაცემთა ავტომატური დამუშავებისა და შენახვის შესაძლებლობები უფრო და უფრო იზრდება.

11 95/46/EC დირექტივის (პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა) მსგავსად, ეს დირექტივა არ ეხება ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვის იმ საკითხებს, რომლებიც არ რეგულირდება ევროკავშირის სამართლით. ამდენად, ის არ ცვლის არსებულ ბალანსს ინდივიდის პირადი ცხოვრების ხელშეუხებლობის უფლებასა და წევრი ქვეყნების შესაძლებლობას შორის, მიიღონ დირექტივის მე-15 მუხლის 1-ელ პუნქტში აღნიშნული ზომები, რომლებიც აუცილებელია საზოგადოებრივი უსაფრთხოების, თავდაცვის, სახელმწიფო უსაფრთხოების (მათ შორის, სახელმწიფოს ეკონომიკური კეთილდღეობის, როცა ეს სახელმწიფო უსაფრთხოების საკითხებს უკავშირდება) დასაცავად და სისხლის სამართლის კანონმდებლობის აღსასრულებლად. შედეგად, დირექტივა ზეგავლენას არ ახდენს წევრი ქვეყნების შესაძლებლობაზე, განახორციელონ ელექტრონული კომუნიკაციების კანონიერი გადაჯერა ან მიიღონ სხვა ზომები, თუ ეს აუცილებელია ზემოხსენებული რომელიმე მიზნის მისაღწევად და შეესაბამება ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპულ კონვენციას (შემდგომ - „ევროპული კონვენცია“), როგორც ეს განმარტებულია ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებებით. ეს ზომები უნდა იყოს შესაბამისი, განსაზღვრული მიზნის მისაღწევად მკაცრად პროპორციული და აუცილებელი დემოკრატიულ საზოგადოებაში, ასევე უზრუნველყოფილი უნდა იყოს ევროპული კონვენციის შესაბამისი სათანადო დაცვის გარანტიები.

21 საჯარო კომუნიკაციების ქსელებისა და საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების მომსახურების საშუალებით, კომუნიკაციებზე არაავტორიზებული წვდომის პრევენციის მიზნით, მიღებულ უნდა იქნას ზომები, რათა დაცული იყოს კომუნიკაციების როგორც შინაარსის, ისე ამგვარ კომუნიკაციებთან დაკავშირებული ნებისმიერი მონაცემის კონფიდენციალურობა. ზოგიერთ წევრ ქვეყანაში, ეროვნული კანონმდებლობა კომუნიკაციებზე მხოლოდ განზრახ არაავტორიზებულ წვდომას კრძალავს.

22 კომუნიკაციებისა და მასთან დაკავშირებული ტრაფიკის მონაცემების შენახვის აკრძალვა იმ პირებისთვის, რომლებიც არ წარმოადგენენ მომხმარებლებს ან მათი თანხმობის არარსებობის შემთხვევაში, არ გულისხმობს, რომ აკრძალულია ინფორმაციის ნებისმიერი ავტომატური, დროებითი და ხანმოკლე შენახვა, თუ მისი ერთა-

დერთი მიზანია ელექტრონული კომუნიკაციების ქსელში გადაცემის განხორციელება და ინფორმაცია არ ინახება იმაზე მეტი ვადით, ვიდრე ეს გადაცემისა და ტრაფიკის ადმინისტრირებისთვის არის საჭირო, ასევე თუ შენახვის პერიოდის განმავლობაში კონფიდენციალურობა გარანტირებულია.

26 ელექტრონული კომუნიკაციების ქსელში აბონენტებთან დაკავშირებული მონაცემები, რომლებიც კავშირის დამყარებისა და ინფორმაციის გადაცემის მიზნით მუშავდება, შეიცავს ინფორმაციას ფიზიკური პირების პირად ცხოვრებაზე და უკავშირდება კორესპონდენციის ხელშეუხებლობის უფლების დაცვას ან იურიდიული პირების ლეგიტიმურ ინტერესებს. ასეთი მონაცემები შეიძლება შეინახოს მხოლოდ იმ მოცულობით, რაც საჭიროა მომსახურების მისაწოდებლად, გადასახადის დარიცხვისა და მასთან დაკავშირებული გადახდების მიზნით, მხოლოდ შეზღუდული დროით. ამ მონაცემთა შემდგომ დამატებით სხვა მიზნებით დამუშავება შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ აბონენტი თანხმობას განაცხადებს და მას საფუძვლად უდევს საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის მიერ მიწოდებული ზუსტი და სრულყოფილი ინფორმაცია მონაცემთა შემდგომი დამუშავების სახეების, ასევე მომხმარებლის უფლების შესახებ, არ გასცეს ან გამოითხოვოს თანხმობა ამგვარ დამუშავებაზე.

30 ელექტრონული კომუნიკაციების ქსელებისა და მომსახურების მიწოდების სისტემები იმგვარად უნდა იქნას შემუშავებული, რომ პერსონალურ მონაცემთა აუცილებელი რაოდენობა მკაცრ მინიმუმამდე იყოს დაყვანილი.

● დირექტივა 2002/58, მუხლი 1, „ფარგლები და მიზანი:“

01 ამ დირექტივის მიზანია შიდა სახელმწიფოებრივი ნორმების ჰარმონიზაცია, რათა უზრუნველყოფილ იქნას ძირითადი უფლებებისა და თავისუფლებების, განსაკუთრებით კი პირადი ცხოვრების ხელშეუხებლობისა და კონფიდენციალურობის უფლების დაცულობის თანაბარი დონე ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებასთან მიმართებით, ასევე უზრუნველყოფილ იქნას ამ მონაცემებისა და ელექტრონული კომუნიკაციების აღჭურვილობისა და სერვისების თავისუფალი მიმოცვლა გაერთიანებაში.

02 ამ დირექტივის მუხლები აკონკრეტებს და ავსებს 95/46 დირექტივას ამ მუხლის პირველ პუნქტში აღნიშნული მიზნების შესაბამისად. დამატებით, ისინი უზრუნველყოფენ იმ აბონენტთა ლეგიტიმური ინტერესების დაცვას, რომლებიც იურიდიულ პირებს წარმოადგენენ.

03 ეს დირექტივა არ ვრცელდება იმ საქმიანობებზე, რომლებიც ევროგაერთიანების დამფუძნებელი ხელშეკრულების ფარგლებში არ ექცევა, როგორიც არის ევროკავშირის შესახებ ხელშეკრულების V და VI თავით გათვალისწინებული, ასევე ის საქმიანობები, რომლებიც უკავშირდება საზოგადოებრივ უსაფრთხოებას, თავდაცვას

და სახელმწიფო უსაფრთხოებას (მათ შორის, სახელმწიფოს ეკონომიკურ კეთილდღეობას, როცა ის სახელმწიფო უსაფრთხოებას უკავშირდება) და სახელმწიფოს საქმიანობას სისხლის სამართლის სფეროში.

● დირექტივა 2002/58, მუხლი 2, „განმარტებები:"

თუ სხვაგვარად არ არის დადგენილი, გამოყენებულ უნდა იქნას 95/46 დირექტივასა და ელექტრონული საკომუნიკაციო ქსელებისა და მომსახურების საერთო მარეგულირებელი ჩარჩოს შესახებ ევროპული პარლამენტისა და საბჭოს 2002 წლის 7 მარტის 2002/21/EC დირექტივაში მოცემული განმარტებანი.

ასევე გამოიყენება შემდეგი განმარტებები:

...

(ბ) „ტრაფიკის მონაცემები" გულისხმობს ნებისმიერ მონაცემს, რომელიც მუშავდება ელექტრონული კომუნიკაციების ქსელით კომუნიკაციის გადაცემის ან გადასახადის დარიცხვის მიზნით;

(გ) „ადგილმდებარეობის მონაცემები" ნიშნავს ნებისმიერ მონაცემს, რომელიც მუშავდება ელექტრონული კომუნიკაციების ქსელში ან ელექტრონული საკომუნიკაციო მომსახურების მიერ და მიუთითებს საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მომხმარებლის საბოლოო მოწყობილობის გეოგრაფიულ ადგილმდებარეობას;

(გ) „კომუნიკაცია" ნიშნავს შეზღუდული რაოდენობის მხარეებს შორის ნებისმიერი ინფორმაციის გაცვლას ან გადაცემას საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მეშვეობით. ეს არ მოიცავს ინფორმაციას, რომელიც საზოგადოებას მიეწოდება სამაუწყებლო მომსახურებით ელექტრონული საკომუნიკაციო ქსელების მეშვეობით იმდენად, რამდენადაც ეს ინფორმაცია არ უკავშირდება ინფორმაციის მიმღებ იდენტიფიცირებად აბონენტს ან მომხმარებელს.

● 2002/58 დირექტივა, მე-3 მუხლი, „მომსახურება:"

ეს დირექტივა ვრცელდება პერსონალური მონაცემების დამუშავებაზე, რომელიც უკავშირდება ევროკავშირში, საჯარო საკომუნიკაციო ქსელებში საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას, იმ საჯარო საკომუნიკაციო ქსელების ჩათვლით, რომლებიც მონაცემთა შეგროვებასა და მოწყობილობათა იდენტიფიცირებას უზრუნველყოფენ.

● დირექტივის მე-4 მუხლი, „დამუშავების უსაფრთხოება:"

01 საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელმა უნდა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები, რათა

დაცული იყოს მომსახურებათა უსაფრთხოება. რაც შეეხება ქსელის უსაფრთხოებას, აუცილებლობის შემთხვევაში, ეს უნდა განხორციელდეს საჯარო საკომუნიკაციო ქსელების მიმწოდებელთან ერთად. ტექნიკური მდგომარეობისა და შესრულების ხარჯების გათვალისწინებით, ამ ზომებმა უნდა უზრუნველყოს არსებული რისკის საპირწონე უსაფრთხოების დონე.

1ა. პირველ პუნქტში მითითებულმა ზომებმა სულ მცირე:

უნდა უზრუნველყოს, რომ პერსონალურ მონაცემებზე წვდომა ექნება უფლებამოსილ პერსონალს, რომელთაც ეს უფლება კანონით დადგენილი მიზნებისთვის მიენიჭათ;

უნდა დაიცვას პერსონალური მონაცემები, რომლებიც ინახება ან რომელთა გადაცემაც ხდება, შემთხვევითი ან უკანონო განადგურების, შემთხვევითი დაკარგვის ან შეცვლის, არაავტორიზებული ან უკანონო შენახვის, დამუშავების, წვდომის ან გამჟღავნების რისკისგან, და

უნდა უზრუნველყოს უსაფრთხოების პოლიტიკის განხორციელება პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით.

● დირექტივის მე-5 მუხლი, „კომუნიკაციების კონფიდენციალურობა:“

01 წევრმა სახელმწიფოებმა ეროვნული კანონმდებლობით უნდა უზრუნველყონ საჯარო საკომუნიკაციო ქსელისა და საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების საშუალებით კომუნიკაციებისა და მასთან დაკავშირებული ტრაფიკის მონაცემების კონფიდენციალურობა. კერძოდ, უნდა აიკრძალოს კომუნიკაციათა (მასთან დაკავშირებული ტრაფიკის მონაცემების ჩათვლით) მოსმენა, მიყურადება, შენახვა ან სხვა სახის გადაჯერა ან კონტროლი იმ პირების მიერ, რომლებიც არ არიან მომხმარებლები ან მათი თანხმობის გარეშე, გარდა იმ შემთხვევისა, როცა მათ დირექტივის მე-15 მუხლის პირველი პუნქტის შესაბამისი კანონიერი უფლებამოსილება გააჩნიათ. ეს პუნქტი ხელს არ უშლის კომუნიკაციის გადასაცემად მონაცემთა ტექნიკურ შენახვას, თუ ეს უკანასკნელი არ არღვევს კონფიდენციალურობის პრინციპს.

03 წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მომხმარებლის ან აბონენტის საბოლოო მოწყობილობაში არსებული ინფორმაციის შენახვა ან უკვე შენახულ ინფორმაციაზე წვდომა დაიშვება მხოლოდ იმ შემთხვევაში, თუ მომხმარებელი ან აბონენტი თანხმობას განაცხადებს. ამასთან, თანხმობის გაცემამდე მათ უნდა მიეწოდოთ მკაფიო და სრულყოფილი ინფორმაცია 95/46 დირექტივის შესაბამისად, მათ შორის, დამუშავების მიზნებთან დაკავშირებით. აღნიშნული არ ვრცელდება ტექნიკურ შენახვაზე ან წვდომაზე, თუ მისი ერთადერთი მიზანია კომუნიკაციის ელექტრონულ საკომუნიკაციო ქსელში გადაცემა ან თუ ეს წარმოადგენს აბსოლუტურ აუცილებლობას, რომ საინფორმაციო საზოგადოების მომსახურების მიმწოდებელმა, აბონენტის ან მომხმარებლის მოთხოვნით, გაწიოს ეს მომსახურება.

● დირექტივის მე-6 მუხლი, „ტრაფიკის მონაცემები:“

თუ სხვაგვარად არ არის დადგენილი, გამოყენებულ უნდა იქნას 95/46 დირექტივასა და ელექტრონული საკომუნიკაციო ქსელებისა და მომსახურების საერთო მარეგულირებელი ჩარჩოს შესახებ ევროპული პარლამენტისა და საბჭოს 2002 წლის 7 მარტის 2002/21/EC დირექტივაში მოცემული განმარტებანი.

01 საჯარო კომუნიკაციების ქსელის ან საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის მიერ გამომწერთა და მომხმარებელთა შესახებ არსებული ტრაფიკის მონაცემები უნდა წაიშალოს ან ანონიმური გახდეს იმ დროიდან, როცა ის საჭირო აღარ არის კომუნიკაციის გადაცემის მიზნებისთვის.

02 ტრაფიკის მონაცემები შეიძლება დამუშავდეს გადასახადის დარიცხვის და მასთან დაკავშირებული გადახდების მიზნით. გადასახადის დარიცხვის მიზნით, მონაცემები შესაძლებელია დამუშავდეს მხოლოდ იმ პერიოდით, რაც საჭიროა მისი კანონის შესაბამისად გასაჩივრების ან გადასახადის მიღებისთვის.

03 ელექტრონული საკომუნიკაციო მომსახურების მარკეტინგის მიზნით ან დამატებითი ღირებულების მომსახურების მიწოდებისთვის, საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელმა შესაძლებელია დაამუშავოს ამ მუხლის პირველ პუნქტში მითითებული მონაცემები იმ ფარგლებში და იმ ხანგრძლივობით, რაც აუცილებელია ამგვარი მომსახურებისთვის ან მარკეტინგისთვის, თუ მომხმარებელი ან აბონენტი, რომლის მონაცემიც მუშავდება, წინასწარ განაცხადებს თანხმობას. მომხმარებელს ან აბონენტს უნდა მიეცეს შესაძლებლობა, ნებისმიერ დროს გამოითხოვოს ტრაფიკის მონაცემების დამუშავებაზე საკუთარი თანხმობა.

...

05 ამ მუხლის 1-ლი, მე-2, მე-3 და მე-4 პუნქტების შესაბამისად, ტრაფიკის მონაცემების დამუშავება შეუძლიათ მხოლოდ იმ პირებს, ვისაც ეს უფლებამოსილება გადაეცათ საჯარო კომუნიკაციების ქსელისა და საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისგან, რომლებიც ახორციელებენ გადასახადის დარიცხვისა და ტრაფიკის სისტემის მართვას, მომხმარებელთა შემოწმებას, თაღლითობის გამოვლენას, ახორციელებენ ელექტრონული საკომუნიკაციო მომსახურების მარკეტინგს ან უზრუნველყოფენ დამატებითი ღირებულების მომსახურებას.

● დირექტივის მე-9 მუხლი, „ადგილმდებარეობის მონაცემები, გარდა ტრაფიკის მონაცემებისა:“

საკომუნიკაციო ქსელის ან საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მომხმარებლებთან ან აბონენტებთან დაკავშირებული ადგილმდებარეობის მონაცემების (ტრაფიკის მონაცემების გარდა) დამუშავება შესაძლებელია მხოლოდ მათი

ანონიმიზაციის შემდეგ ან იმ შემთხვევაში, თუ არსებობს მომხმარებელთა ან აბონენტთა თანხმობა. დამუშავება შესაძლებელია იმ ფარგლებში და იმ ხანგრძლივობით, რაც აუცილებელია დამატებითი ღირებულების მომსახურების მიწოდებისთვის. მომსახურების მიმწოდებელმა მომხმარებელსა და აბონენტებს თანხმობის მიღებამდე უნდა აცნობოს, რა სახის ადგილმდებარეობის მონაცემი (ტრაფიკის მონაცემის გარდა) დამუშავდება, დამუშავების ხანგრძლივობა და მიზნები, ასევე, გადაეცემა თუ არა ეს მონაცემები მესამე პირებს დამატებითი ღირებულების მომსახურებით უზრუნველყოფის მიზნით.

● დირექტივის მე-15 მუხლი, „95/46 დირექტივის ზოგიერთი დებულების გამოყენების წესი:“

01 წევრმა ქვეყნებმა შეიძლება მიიღონ საკანონმდებლო ზომები, რომლებიც ზღუდავს დირექტივის მე-5 და მე-6 მუხლებით, მე-8 მუხლის 1-ლი, მე-2, მე-3 და მე-4 პუნქტებითა და მე-9 მუხლით დადგენილი უფლებებისა და ვალდებულებების ფარგლებს, როცა ამგვარი შეზღუდვა არის აუცილებელი, სათანადო და პროპორციული საშუალება დემოკრატიულ საზოგადოებაში ეროვნული უსაფრთხოების, თავდაცვის, საზოგადოებრივი უსაფრთხოების, დანაშაულის ან ელექტრონულ საკომუნიკაციო სისტემაზე არაავტორიზებული წვდომის პრევენციის, გამოძიების, გამოვლენისა და სისხლის სამართლებრივი დევნის დაწყების მიზნით, როგორც ეს მითითებულია 95/46 დირექტივის მე-13 მუხლის 1-ელ პუნქტში. ამ მიზნით, წევრ სახელმწიფოებს შეუძლიათ მიიღონ საკანონმდებლო ზომები, რომლებიც უზრუნველყოფს მონაცემთა შეზღუდული პერიოდით შენახვას ამ პუნქტით განსაზღვრული მიზნების მისაღწევად. ამ პუნქტში მითითებული ყველა ზომა უნდა შეესაბამებოდეს ევროკავშირის კანონმდებლობის ძირითად პრინციპებს, მათ შორის, ევროკავშირის შესახებ ხელშეკრულების მე-6 მუხლის 1-ელ და მე-2 პუნქტებს.

...

1ბ. მომხმარებელთა პერსონალურ მონაცემებზე წვდომის მოთხოვნებთან დაკავშირებით, მიმწოდებლებმა უნდა ჩამოაყალიბონ შიდა პროცედურები, რომელებიც დაეფუძნება ამ მუხლის პირველი პუნქტის შესაბამისად მიღებულ ეროვნულ ნორმებს. მოთხოვნის შემთხვევაში, მათ შესაბამის ეროვნულ უწყებას უნდა მიაწოდონ ინფორმაცია ამ პროცედურების, მიღებული მოთხოვნების რაოდენობის, სამართლებრივი საფუძვლებისა და მათი პასუხის შესახებ.

02 95/46 დირექტივის მე-3 თავის მუხლები, რომლებიც სასამართლო წესით უფლების დაცვას, პასუხისმგებლობის განსაზღვრასა და სახდელებს შეეხება, ვრცელდება ამ დირექტივის შესაბამისად მიღებულ ეროვნულ ნორმებზე და ამ დირექტივიდან გამომდინარე ინდივიდუალურ უფლებებზე.

ფაქტობრივი გარემოებები

• საქმე C-203/15

2014 წლის 9 აპრილს, შვედეთში დაფუძნებულმა ელექტრონული კომუნიკაციების მომსახურების მიმწოდებელმა Tele2 Sverige-მ შვედეთის საფოსტო და სატელეკომუნიკაციო უწყებას (შემდგომ -PTS) შეატყობინა, რომ ევროკავშირის მართლმსაჯულების სასამართლოს 2014 წლის 8 აპრილის გადაწყვეტილების *(Digital Rights Ireland and others)* საფუძველზე, 2006/24 დირექტივამ ძალა დაკარგა და ის (მიმწოდებელი) 2014 წლის 14 აპრილიდან ვალდებული იყო, შეეწყვიტა კანონმდებლობით გათვალისწინებული ელექტრონული კომუნიკაციების მონაცემთა შენახვა;[5] ასევე, მას უნდა წაეშალა ამ თარიღამდე მოპოვებული მონაცემებიც.

2014 წლის 15 აპრილს, შვედეთის ეროვნულმა საპოლიციო უწყებამ PTS-ს საჩივარი გაუგზავნა იმასთან დაკავშირებით, რომ Tele2 Sverige-მ მათთვის ამ მონაცემთა მიწოდება შეწყვიტა.

2014 წლის 29 აპრილს, *Digital Rights Ireland* გადაწყვეტილების შუქზე შვედეთის კანონმდებლობის შესაფასებლად, შვედეთის იუსტიციის მინისტრმა სპეციალური მომხსენებელი დანიშნა. მან თავის 2014 წლის ანგარიშში დაასკვნა, რომ მონაცემთა შენახვის მარეგულირებელი ეროვნული სამართლებრივი ნორმები ევროკავშირის კანონმდებლობასა და ევროპულ კონვენციასთან შეუსაბამო არ იყო. სპეციალურმა მომხსენებელმა განმარტა, რომ გადაწყვეტილება საქმეზე *Digital Rights Ireland and others* არ უნდა განიმარტოს ისე, თითქოს მონაცემების ბლანკეტური და განურჩეველი შეგროვება პრინციპულად არასწორია. ეს გადაწყვეტილება არც ისე უნდა იქნას გაგებული, რომ სასამართლომ ჩამოაყალიბა კრიტერიუმები, რომლებიც სრულად უნდა იყოს დაცული იმისთვის, რომ კანონმდებლობა პროპორციულად ჩაითვალოს. მომხსენებელმა მიიჩნია, რომ შვედეთის კანონმდებლობის ევროკავშირის კანონმდებლობასთან შესაბამისობის შესაფასებლად საჭირო იყო ყველა გარემოების, მათ შორის, მონაცემთა შენახვის ფარგლების, მონაცემთა ხელმისაწვდომობის, შენახვის ხანგრძლივობის, მონაცემთა დაცვისა და უსაფრთხოების შესახებ წესების მხედველობაში მიღება.

შედეგად, 2014 წლის 19 ივნისს PTS-მა ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელს - Tele2 Sverige-ს აცნობა, რომ მან დაარღვია კანონის მოთხოვნები, როცა დანაშაულის წინააღმდეგ ბრძოლის მიზნით, მონაცემთა შენახვაზე უარი განაცხადა და 2014 წლის 27 ივნისის ბრძანებით, იმავე წლის 25 ივლისამდე ამ მონაცემთა შენახვის დაწყება მოსთხოვა.

Tele2 Sverige-მ მიიჩნია, რომ 2014 წლის ანგარიში სასამართლო გადაწყვეტილების არასწორ განმარტებას ეფუძნებოდა და მონაცემთა შენახვა ქარტიით გარანტირებულ ადამიანის ძირითად უფლებებს არღვევდა. მან 2014 წლის 27 ივნისის ბრძანება სტოკჰოლმის ადმინისტრაციულ სასამართლოში გაასაჩივრა. სასამართლომ, 2014 წლის 13 ოქტომბრის გადაწყვეტილებით, სარჩელი არ დააკმაყოფილა, რაც Tele2 Sverige-მ სააპელაციო წესით გაასაჩივრა.

[5] ავტორის შენიშვნა: ტელეკომუნიკაციების სფეროში მონაცემთა შენახვა მიემართება სატელეფონო ზარების, ინტერნეტ ტრაფიკისა და ტრანზაქციების შესახებ სხვადასხვა ტიპის მონაცემებს, მათ შორის, ადგილმდებარეობის შესახებ მონაცემებსაც.

სააპელაციო სასამართლოს მოსაზრებით, შვედეთის კანონმდებლობის ევროკავშირის კანონმდებლობასთან შესაბამისობის საკითხი უნდა შეფასებულიყო 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტის საფუძველზე. დირექტივის ზოგადი წესის მიხედვით, ტრაფიკისა და ადგილმდებარეობის მონაცემები ანონიმური უნდა გახდეს ან უნდა წაიშალოს, როდესაც ისინი კომუნიკაციის გადასაცემად საჭირო აღარ არის. დირექტივის მე-15(1) მუხლი აწესებს გამონაკლისს და წევრ სახელმწიფოებს ნებას რთავს, კონკრეტული საფუძვლის არსებობისას, წაშლისა და ანონიმიზაციის მოთხოვნა შეზღუდოს და მეტიც, ელექტრონული კომუნიკაციების მონაცემთა შენახვის წესები დაადგინოს. შესაბამისად, სააპელაციო სასამართლო მიიჩნევდა, რომ ევროკავშირის კანონმდებლობით, კონკრეტული გარემოებების არსებობისას, დასაშვები იყო ელექტრონული კომუნიკაციების მონაცემთა შენახვა.

სააპელაციო სასამართლოს აინტერესებდა, *Digital Rights Ireland* გადაწყვეტილების, 2002/58 დირექტივის მე-15 მუხლის პირველი პუნქტისა და ევროპის კავშირის ძირითად უფლებათა ქარტიის მე-7, მე-8 და 52(1) მუხლების გათვალისწინებით, ელექტრონული კომუნიკაციების მონაცემთა ბლანკეტური და განურჩეველი შენახვის ვალდებულება შეესაბამებოდა თუ არა ევროკავშირის კანონმდებლობას.

სტოკჰოლმის სააპელაციო სასამართლომ შეაჩერა სამართალწარმოება და წინასწარი გადაწყვეტილების მისაღებად, ევროკავშირის მართლმსაჯულების სასამართლოს შემდეგი კითხვებით მიმართა:

01 დანაშაულთან ბრძოლის მიზნით, ყველა პირის შესახებ, ელექტრონული კომუნიკაციების ნებისმიერი საშუალებიდან, ტრაფიკის ყველა მონაცემის განურჩევლად, გამონაკლისებისა და შეზღუდვების გარეშე შენახვის ზოგადი ვალდებულება არის თუ არა თავსებადი ევროკავშირის 2002/58 დირექტივის მე-15(1) მუხლთან, ქარტიის მე-7, მე-8 და 52(1)-ე მუხლების გათვალისწინებით?

02 თუ პირველი კითხვის პასუხი უარყოფითია, ნებადართულია თუ არა შენახვა მაშინ, როცა:

ა. შენახულ მონაცემებზე ეროვნული ხელისუფლების ორგანოების წვდომას კანონი განსაზღვრავს ისე (როგორც ეს აღწერილია მიმართვის ბრძანების 19-36 პუნქტებში[6]) და

[6] საქმის განხილვის პერიოდში მოქმედი შვედეთის კანონმდებლობის თანახმად, დაზვერვის მიზნით მონაცემთა შეგროვებისათვის უფლებამოსილ ორგანოებს შეეძლოთ, ელექტრონული საკომუნიკაციო ქსელის ან მომსახურების მიმწოდებლების შეტყობინების გარეშე, საკომუნიკაციო ქსელში ან ელექტრონული საკომუნიკაციო მოწყობილობების მეშვეობით გადაცემულ შეტყობინებებთან დაკავშირებული მონაცემების შეგროვება. ამ ზომების გამოყენების შესახებ გადაწყვეტილება სასამართლოს ან სხვა დამოუკიდებელი ორგანოს მიერ წინასწარ განხილვას არ ექვემდებარებოდა. ამავდროულად, ელექტრონული კომუნიკაციის მიმწოდებლებს ხელმისაწვდომი უნდა გაეხადათ მომხმარებელთან დაკავშირებული მონაცემები შესაბამისი უწყებების მოთხოვნის შემთხვევაში, თუ ისინი სავარაუდო დანაშაულებრივ ქმედებას (ნაკლებად მძიმე დანაშაულის შემთხვევაშიც) უკავშირდებოდა. დამატებით, შვედეთის კანონმდებლობა წინასწარი გამოძიების ფარგლებშიც აძლევდა ეროვნული ხელისუფლების ორგანოებს შენახულ მონაცემებზე წვდომის უფლებას, მათ შორის, იმ შემთხვევაშიც, როცა გამოძიება შეეხებოდა იმგვარ დანაშაულებს, რომლებიც 6 თვემდე პატიმრობას ითვალისწინებდა. უფრო დაწვრილებით, იხ. ევროკავშირის მართლმსაჯულების სასამართლოს ამ გადაწყვეტილების 21-26 პუნქტები.

ბ. მონაცემთა დაცვისა და უსაფრთხოების მოთხოვნები მოწესრიგებულია ისე (როგორც ეს აღწერილია მიმართვის ბრძანების 28-43 პუნქტებში[7]) და

გ. ყველა შესაბამისი მონაცემის შენახვა ნებადართულია 6 თვით, რომელიც აითვლება კომუნიკაციის დასრულების დღიდან, ხოლო შემდგომ ის იშლება (როგორც ეს აღწერილია მიმართვის ბრძანების 37-ე პუნქტში[8])?

საქმე C-698/15

მისტერ უოთსონმა, ბრაისმა და ლუისმა ინგლისისა და უელსის მართლმსაჯულების უმაღლეს სასამართლოში საჩივარი შეიტანეს მონაცემთა შენახვისა და საგამოძიებო უფლებამოსილებების შესახებ აქტის (DRIPA) პირველი მუხლის კანონიერების შესამოწმებლად, ვინაიდან მიიჩნევდნენ, რომ ეს მუხლი ქარტიის მე-7 და მე-8 მუხლებთან და ევროპული კონვენციის მე-8 მუხლთან თავსებადი არ იყო.

სასამართლოს 2015 წლის 17 ივლისის გადაწყვეტილების თანახმად, Digital Rights Ireland გადაწყვეტილებაში ჩამოყალიბდა ევროკავშირის კანონმდებლობის სავალდებულო მოთხოვნები, რომლებიც კომუნიკაციების შესახებ მონაცემთა შენახვასა და მათზე წვდომას შეეხება. სასამართლომ აღნიშნა, რომ ვინაიდან ზემოაღნიშნული გადაწყვეტილებით ევროკავშირის N2006/24 დირექტივა პროპორციულობის პრინციპთან შეუსაბამოდ გამოცხადდა, ეროვნული კანონმდებლობაც, რომელიც იმავე მუხლებს შეიცავს, რასაც ხსენებული დირექტივა შეიცავდა, ასევე შეუსაბამოდ უნდა გამოცხადდეს. ამდენად, სასამართლომ მიიჩნია, რომ DRIPA-ს პირველი მუხლი არ შეესაბამებოდა ქარტიის მე-7 და მე-8 მუხლებს, ვინაიდან ის არ აყალიბებდა მკაფიო და კონკრეტულ წესებს შენახული მონაცემების გამოყენებასა და მასზე წვდომასთან დაკავშირებით. ამავდროულად, ამ მონაცემებზე წვდომა შესაძლებელი იყო სასამართლოს ან სხვა დამოუკიდებელი ადმინისტრაციული ორგანოს წინასწარი განხილვის გარეშე.

შინაგან საქმეთა დეპარტამენტის სახელმწიფო მდივანმა ეს გადაწყვეტილება სააპელაციო სასამართლოში გაასაჩივრა. სააპელაციო სასამართლოს განმარტებით, DRIPA-ს პირველი მუხლი შინაგან საქმეთა დეპარტამენტის სახელმწიფო მდივანს უფლებამოსილებას ანიჭებს, სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს ნებართვის გარეშე მიიღოს

[7] ევროკავშირის მართლმსაჯულების სასამართლოს ამ გადაწყვეტილების 28-ე პარაგრაფი შვედეთის კანონმდებლობით მოწესრიგებულ მონაცემთა დაცვისა და უსაფრთხოების მოთხოვნებთან მიმართებით მიუთითებს, რომ ელექტრონული კომუნიკაციების მომსახურების მიმწოდებლები ვალდებულნი არიან მონაცემთა შენახვისთვის სათანადო ტექნიკური და ორგანიზაციული ზომები მიიღონ, რათა დამუშავების პროცესში მონაცემთა დაცულობა გარანტირებული იყოს, თუმცა კანონმდებლობა არ ითვალისწინებს კონკრეტულად სად უნდა ინახებოდეს ეს მონაცემები.

[8] ევროკავშირის მართლმსაჯულების სასამართლოს ამ გადაწყვეტილების მე-19 პარაგრაფის თანახმად, შვედეთის კანონმდებლობა ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს ავალდებულებს, რომ ელექტრონული კომუნიკაციების შესახებ კანონით განსაზღვრული მონაცემები შეინახონ კომუნიკაციის დასრულებიდან 6 თვის განმავლობაში. ამ დროის გასვლის შემდგომ მონაცემები უნდა წაიშალოს, თუ არ არსებობს იმავე კანონით დადგენილი რომელიმე გამონაკლისი.

ზოგადი წესები, რომლებიც საჯარო ტელეკომუნიკაციების ოპერატორებს უწესებს მოთხოვნას, შეინახონ საფოსტო ან სხვა სატელეკომუნიკაციო მომსახურებასთან დაკავშირებული ყველა მონაცემი არაუმეტეს 12 თვისა, როცა ეს აუცილებელია და მიზნის მიღწევის თანაზომიერი საშუალებაა. სასამართლოს პოზიციით, მიუხედავად იმისა, რომ ეს მონაცემები არ შეიცავს კომუნიკაციის შინაარსს, ამგვარი წესი შესაძლოა საკომუნიკაციო მომსახურების მომხმარებელთა პირადი ცხოვრების უფლებაში მძიმე ჩარევად შეფასდეს. ამავდროულად, სასამართლო მიუთითებს 2002/58 დირექტივის 1-ლი მუხლის მე-3 პუნქტზე, რომლის მიხედვითაც, ევროკავშირის კანონმდებლობა შენახულ მონაცემთა წვდომასთან დაკავშირებული წესების უნიფიცირებას არ ახდენს.

სააპელაციო სასამართლოს თანახმად, *Digital Rights Ireland* გადაწყვეტილებაში ევროკავშირის მართლმსაჯულების სასამართლო მხოლოდ 2006/24 დირექტივის კანონიერებაზე მსჯელობდა და მას არ შეუფასებია რომელიმე სახელმწიფოს ეროვნული კანონმდებლობა. ამავდროულად, სააპელაციო სასამართლო მიუთითებდა, რომ მართლმსაჯულების ევროპული სასამართლოს მიზანი არ ყოფილა წევრი სახელმწიფოებისთვის სავალდებულო მოთხოვნების განსაზღვრა, რომლებიც შენახულ მონაცემთა წვდომის მარეგულირებელ ეროვნულ კანონმდებლობაში უნდა ასახულიყო.

ყოველივე ზემოაღნიშნულის საფუძველზე, სააპელაციო სასამართლომ შეაჩერა სამართალწარმოება და წინასწარი გადაწყვეტილების მისაღებად ევროკავშირის მართლმსაჯულების სასამართლოს შემდეგი კითხვებით მიმართა:

01 ევროპის კავშირის ძირითად უფლებათა ქარტიის მე-7 და მე-8 მუხლებთან კანონმდებლობის შესაბამისობის მიზნით, *Digital Rights Ireland* გადაწყვეტილება აყალიბებს თუ არა ევროკავშირის კანონმდებლობის სავალდებულო მოთხოვნებს წევრი სახელმწიფოების იმ შიდა კანონმდებლობისთვის, რომელიც შენახულ მონაცემებზე წვდომას არეგულირებს?

02 სცილდება თუ არა ქარტიის მე-7 და მე-8 მუხლის *Digital Rights Ireland* გადაწყვეტილებით ჩამოყალიბებული ფარგლები ევროპული კონვენციის მე-8 მუხლის ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკით ჩამოყალიბებულ ფარგლებს?

სასამართლოს შეფასება

▸ პირველი შეკითხვა საქმეზე C-203/15

▸ 2002/58/EC დირექტივის ფარგლები

დანაშაულთან ბრძოლის მიზნით, ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვასა და წვდომასთან დაკავშირებულ ეროვნულ კანონმდებლობაზე დირექტივის გავრცელებასთან

დაკავშირებით, წევრი სახელმწიფოების წერილობითი მოსაზრებები ერთმანეთისგან განსხვავდებოდა. ბელგიის, დანიის, გერმანიის, ესტონეთის, ირლანდიისა და ნიდერლანდების მთავრობები მიუთითებდნენ, რომ დირექტივა ვრცელდებოდა როგორც მონაცემთა შენახვაზე, ისე წვდომაზე. ჩეხეთის აზრით, დირექტივის მოქმედების ფარგლებში არცერთი მათგანი არ ექცეოდა, ხოლო გაერთიანებული სამეფო მიუთითებდა, რომ ის მხოლოდ მონაცემთა შენახვის მარეგულირებელ კანონმდებლობაზე ვრცელდებოდა.

სასამართლოს განმარტებით, დირექტივის 1-ლი მუხლის 1-ლი პუნქტი მიუთითებს, რომ დირექტივის მიზანია შიდასახელმწიფოებრივი ნორმების ჰარმონიზაცია, რათა უზრუნველყოფილ იქნას ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებასთან მიმართებით, ძირითადი უფლებებისა და თავისუფლებების, განსაკუთრებით კი პირადი ცხოვრების ხელშეუხებლობისა და კონფიდენციალურობის დაცულობის თანაბარი დონე. ამავდროულად, დირექტივის 1-ლი მუხლის მე-3 პუნქტი გამორიცხავს ცალკეულ საკითხებზე, მათ შორის, სისხლის სამართლის, საზოგადოებრივი უსაფრთხოების, თავდაცვისა და სახელმწიფო უსაფრთხოების სფეროში სახელმწიფოთა საქმიანობებზე დირექტივის გავრცელებას.

დირექტივის მე-15 მუხლის 1-ლი პუნქტის თანახმად, სახელმწიფოებმა შესაძლებელია მიიღონ საკანონმდებლო ზომები, რომლებიც, დადგენილი პირობების გათვალისწინებით, დირექტივის მე-5, მე-6, მე-9 მუხლებისა და მე-8 მუხლის პირველ, მე-2, მე-3 და მე-4 პუნქტებით უზრუნველყოფილი უფლებებისა და ვალდებულებების ფარგლებს ზღუდავენ. მე-15 მუხლის 1-ლი პუნქტის მეორე წინადადებაში კი ამის მაგალითად მოყვანილია მონაცემთა შენახვის უზრუნველმყოფი ზომები.

სასამართლოს განმარტებით, დირექტივის მე-15 მუხლის პირველ პუნქტში მითითებული საკანონმდებლო ზომები მიემართება იმ საქმიანობებს, რომლებიც დამახასიათებელია სახელმწიფოსა და მისი ორგანოებისთვის, ხოლო უცხო იმ სფეროებისთვის, სადაც ინდივიდები საქმიანობენ. ამასთან, პირველი მუხლის მე-3 პუნქტით გათვალისწინებული საქმიანობები[9] ძირითადად იმავე მიზნებს ემსახურება, რასაც მე-15 მუხლის პირველი პუნქტით განსაზღვრული საკანონმდებლო ზომები. ეს მიზნებია თავდაცვა, სახელმწიფო უსაფრთხოების, საზოგადოებრივი უსაფრთხოების დაცვა და დანაშაულის ჩადენის ან ელექტრონული კომუნიკაციების სისტემის არაავტორიზებული გამოყენების შემთხვევათა პრევენცია, გამოძიება და სისხლისსამართლებრივი დევნის დაწყება.

მიუხედავად ამისა, დირექტივის ზოგადი სტრუქტურის გათვალისწინებით, სასამართლომ დაასკვნა, რომ დირექტივის მე-15 მუხლის პირველ პუნქტში მოცემული საკანონმდებლო ზომები დირექტივის ფარგლებს არ სცილდება, ვინაიდან, წინააღმდეგ შემთხვევაში, ამ მუხლს საფუძველი გამოეცლებოდა. მე-15 მუხლის 1-ლი პუნქტი უშვებს, რომ სახელმწიფოს მიერ გატარებული ზომები, როგორიც არის დანაშაულთან ბრძოლის მიზნით მონაცემთა შენახვა, დირექტივის ფარგლებში ექცევა, ვინაიდან ის აშკარად ანიჭებს სახელმწიფოებს ამგვარი ზომების მიღებას უფლებას, თუ ეს დირექტივით დადგენილი წესების შესაბამისად მოხდება.

[9] ავტორის შენიშვნა: საქმიანობები, რომლებიც გამორიცხულია დირექტივის მოქმედების ფარგლებიდან.

სასამართლომ მიუთითა, რომ დირექტივის მე-15 მუხლის 1-ელ პუნქტში მითითებული საკანონმდებლო ზომები არეგულირებს ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების საქმიანობას და ამდენად, მასზე დირექტივა უნდა გავრცელდეს.

სასამართლომ აღნიშნა, რომ დირექტივის ფარგლები იმ საკანონმდებლო ზომებზე ვრცელდება, რომლებიც მიმწოდებლებს ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვას ავალდებულებს, ვინაიდან ამ პროცესში მიმწოდებლები პერსონალურ მონაცემებს ამუშავებენ. დირექტივა ვრცელდება იმ საკანონმდებლო ზომებზეც, რომლებიც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ შენახულ მონაცემებზე ეროვნული ხელისუფლების შესაბამისი ორგანოების წვდომას არეგულირებს.

ელექტრონული კომუნიკაციებისა და მასთან დაკავშირებული ტრაფიკის მონაცემების კონფიდენციალურობის დაცვა უზრუნველყოფილია დირექტივის მე-5(1) მუხლით, რომელიც ვრცელდება თავად მომხმარებელთა გარდა ნებისმიერი პირის, მათ შორის კერძო თუ სახელმწიფო ორგანოს მიერ გატარებულ ზომებზე. დირექტივის პრეამბულის 21-ე პუნქტი ადასტურებს, რომ მისი ერთ-ერთი მიზანი კომუნიკაციებზე, მათ შორის, ამ კომუნიკაციებთან დაკავშირებულ ნებისმიერ მონაცემზე არაავტორიზებული წვდომის პრევენციაა.

ამდენად, როცა სახელმწიფო მოითხოვს ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებთან შენახულ მონაცემებზე წვდომას, ეს მოიცავს ამ მიმწოდებელთა მიერ პერსონალური მონაცემების დამუშავებას და სწორედ ეს დამუშავება ექცევა დირექტივის ფარგლებში.

სასამართლოს განმარტებით, ვინაიდან მონაცემები მხოლოდ იმ მიზნით ინახება, რომ აუცილებლობის შემთხვევაში, ის ხელმისაწვდომი გახდეს შესაბამისი ეროვნული ხელისუფლების ორგანოსთვის, ეროვნული კანონმდებლობით ამ მონაცემთა შენახვის ვალდებულების დაწესება თავისთავად გამოიწვევს იმ ნორმათა არსებობასაც, რომლებიც შესაბამისი ორგანოების მიერ ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების მიერ შენახულ მონაცემებზე წვდომას არეგულირებს. ნორმის ასეთ განმარტებას ადასტურებს დირექტივის მე-15 მუხლის 1ბ პუნქტიც, რომლითაც მიმწოდებლებს მომხმარებელთა პერსონალურ მონაცემების წვდომის მოთხოვნებზე შიდა პროცედურების შემოღების ვალდებულება ეკისრებათ.

ამდენად, სასამართლომ დაადგინა, რომ ორივე საქმეში ეროვნული კანონმდებლობა დირექტივის ფარგლებში ხვდება.

- **2002/58/EC დირექტივის მე-15 მუხლის პირველი პუნქტის განმარტება ევროპის კავშირის ძირითადხ უფლებათა ქარტიის მე-7, მე-8, მე-11 და 52(1)-ე მუხლების შუქზე.**

სასამართლოს თანახმად, გასათვალისწინებელია, რომ დირექტივის 1-ლი მუხლის მე-2 პუნქტის თანახმად, მოცემული დირექტივის მუხლები აკონკრეტებს და ავსებს 95/46 დირექტივას. 2002/58 დირექტივის პრეამბულის მე-2 პუნქტი კი მიზნად ისახავს ქარტიის მე-7 და მე-8

მუხლით გათვალისწინებული უფლებების სრულად დაცვის უზრუნველყოფას. ამავდროულად, ევროკავშირის კანონმდებლობის მიზანია, ყველა ელექტრონული საკომუნიკაციო მომსახურებისთვის უზრუნველყოფილ იყოს პერსონალური მონაცემებისა და პირადი ცხოვრების უფლებების განსაკუთრებული დაცვა, გამოყენებული ტექნოლოგიის ტიპის მიუხედავად.

2002/58 დირექტივის პრეამბულის მე-6 და მე-7 პუნქტები დირექტივის ერთ-ერთ ამოცანად ახალი ტექნოლოგიების, მონაცემთა ავტომატური შენახვისა და დამუშავების მზარდი შესაძლებლობებიდან მომდინარე რისკებისგან ელექტრონული საკომუნიკაციო მომსახურების მომხმარებელთა დაცვას სახავენ. დირექტივის მე-5 მუხლის პირველი პუნქტის თანახმად, წევრმა სახელმწიფოებმა ეროვნული კანონმდებლობით უნდა უზრუნველყონ იმ კომუნიკაციების კონფიდენციალურობა, რომელიც იქმნება საერთო სარგებლობის საკომუნიკაციო ქსელისა და საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მეშვეობით, ასევე დაცული უნდა იყოს ამ კომუნიკაციებთან დაკავშირებული ტრაფიკის მონაცემების კონფიდენციალურობა.

სასამართლოს განმარტებით, დირექტივაში ასახული კომუნიკაციების კონფიდენციალურობის პრინციპი გულისხმობს იმას, რომ ზოგადი წესით, მომხმარებლის გარდა და მისი თანხმობის გარეშე, ნებისმიერ პირს ეკრძალება ელექტრონულ კომუნიკაციებთან დაკავშირებული ტრაფიკის მონაცემების შენახვა. გამონაკლისი დაიშვება მხოლოდ მონაცემთა ტექნიკურ შენახვაზე, რაც აუცილებელია კომუნიკაციის გადაცემისათვის. გამონაკლისი ასევე შეეხება იმ პირებს, რომლებსაც კანონის შესაბამისად მონაცემთა შენახვის უფლებამოსილება აქვთ მინიჭებული, რაც ასევე უნდა განხორციელდეს დირექტივის მე-15(1) მუხლის მოთხოვნების დაცვით.

აქედან გამომდინარე, 2002/58 დირექტივის პრეამბულის 22-ე და 26-ე პუნქტებისა და მე-6 მუხლის შესაბამისად, ტრაფიკის მონაცემების დამუშავება და შენახვა დაიშვება მხოლოდ იმ ფარგლებში და იმ ხანგრძლივობით, რაც აუცილებელია მომსახურების გაყიდვისა და გადასახადის დარიცხვის მიზნით, ასევე, დამატებითი ღირებულების სერვისებისთვის. მომსახურებაზე გადასახადის დარიცხვის მიზნით მონაცემები შესაძლებელია დამუშავდეს მხოლოდ იმ პერიოდით, რაც საჭიროა გასაჩივრებისთვის ან გადასახადის ამოღების მიზნით სასამართლოში საქმისწარმოების დასაწყებად. ამ პერიოდის გასვლისთანავე, დამუშავებული და შენახული მონაცემები უნდა წაიშალოს ან ანონიმური გახდეს. რაც შეეხება ადგილმდებარეობის მონაცემებს, დირექტივის მე-9 მუხლის პირველი პუნქტის თანახმად, მონაცემები შესაძლოა დამუშავდეს მხოლოდ კონკრეტული პირობების არსებობისას და მას შემდეგ, რაც ის ანონიმური გახდება ან იმ შემთხვევაში, როცა დამუშავებაზე არსებობს მომხმარებელთა ან აბონენტთა თანხმობა.

სასამართლომ მიუთითა, რომ დირექტივის მე-5, მე-6 და მე-9 მუხლები უნდა განიმარტოს დირექტივის პრეამბულის 30-ე პუნქტის შუქზე, რომლის თანახმად, ელექტრონული საკომუნიკაციო ქსელებისა და მომსახურების მიწოდების სისტემები ისე უნდა იქნას მოწყობილი, რომ პერსონალურ მონაცემთა აუცილებელი რაოდენობა მკაცრ მინიმუმამდე იყოს დაყვანილი.

თუმცა, დირექტივის მე-15(1) მუხლი წევრ სახელმწიფოებს ნებას რთავს, გამონაკლისები დააწესოს დირექტივის მე-5(1) მუხლით დადგენილ პერსონალური მონაცემების კონფიდენციალურობის პრინციპზე და მე-6 და მე-9 მუხლებით გათვალისწინებულ ვალდებულებებზე. მიუხედავად იმისა, რომ 2002/58 დირექტივის მე-15(1) მუხლი წევრ სახელმწიფოებს აძლევს შესაძლებლობას ამ პრინციპის ფარგლები შეზღუდოს, სასამართლო პრაქტიკით დადგენილია, რომ ეს ნორმა უნდა განიმარტოს ვიწროდ. ეს მუხლი თავად პრინციპის სავალდებულოობაზე, კერძოდ, მონაცემთა შენახვის აკრძალვაზე, როგორც შესასრულებლად სავალდებულო ნორმაზე, გამონაკლისს ვერ დააწესებს, ვინაიდან წინააღმდეგ შემთხვევაში, დირექტივის მე-5 მუხლით გარანტირებული კონფიდენციალურობის პრინციპი მნიშვნელობას დაკარგავდა.

უნდა აღინიშნოს ისიც, რომ დირექტივის მე-15(1) მუხლის პირველი ნაწილით, საკანონმდებლო ზომები, რომლებიც კონფიდენციალურობის პრინციპიდან უხვევენ, შეიძლება შემოღებულ იქნას კონკრეტული მიზნით, კერძოდ, ეროვნული უსაფრთხოების, თავდაცვის, საზოგადოებრივი უსაფრთხოების, დანაშაულთა ან ელექტრონულ კომუნიკაციებზე არაავტორიზებული წვდომის პრევენციის, გამოძიების, სისხლისსამართლებრივი დევნის დაწყების ან 95/46 დირექტივის მე-13 მუხლის პირველ პუნქტში გათვალისწინებული მიზნებით. ამდენად, ამ მიზნების ჩამონათვალი ამომწურავია და მიღებული საკანონმდებლო ზომები მხოლოდ ამ მიზნებს უნდა დაეფუძნოს.

დამატებით, დირექტივის მე-15(1) მუხლის მესამე წინადადება მიუთითებს, რომ ყველა ზომა ევროკავშირის კანონმდებლობის ზოგად პრინციპებს უნდა შეესაბამებოდეს, რაც ასევე მოიცავს იმ ძირითად უფლებებს, რომლებსაც ქარტია ითვალისწინებს და დირექტივის მე-15(1) მუხლიც სწორედ ამ ძირითადი უფლებების შუქზე უნდა განიმარტოს.

სასამართლომ ხაზგასმით აღნიშნა, რომ ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებისთვის დაწესებული ვალდებულებები, რომლებიც მათ მიერ ტრაფიკის მონაცემების შენახვას მოითხოვს იმ მიზნით, რომ აუცილებლობისას ხელისუფლების შესაბამის ორგანოს ჰქონდეს მათზე წვდომა, ქარტიის არა მხოლოდ მე-7 და მე-8 მუხლებთან დაკავშირებით, არამედ მე-11 მუხლით განმტკიცებულ გამოხატვის თავისუფლებასთან მიმართებითაც აჩენს კითხვებს. სასამართლომ აღნიშნა, რომ მე-15 მუხლის 1-ლი ნაწილის განმარტებისას პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის უფლების მნიშვნელობა მხედველობაში უნდა იქნას მიღებული. იმავეს თქმა შეიძლება გამოხატვის თავისუფლებაზეც იმ განსაკუთრებული მნიშვნელობიდან გამომდინარე, რაც მას დემოკრატიულ საზოგადოებაში ენიჭება. ეს ძირითადი უფლება დემოკრატიული, პლურალისტული საზოგადოების არსებობის აუცილებელ ფუნდამენტს და იმ ღირებულებას წარმოადგენს, რომელზეც ევროკავშირი დაეფუძნა. სასამართლომ ასევე მოიხმო ქარტიის 52-ე მუხლის პირველი პუნქტი, რომლის თანახმად, ქარტიით გათვალისწინებული უფლებებისა და თავისუფლებებით სარგებლობაზე შეზღუდვები უნდა ეფუძნებოდეს კანონს, ხოლო დაწესებულმა შეზღუდვებმა უფლებათა და თავისუფლებათა ძირითადი არსი არ უნდა შელახონ. პროპორციულობის პრინციპის გათვალისწინებით, შეზღუდვები შესაძლებელია დაწესდეს, თუ ეს აუცილებელია და შეესაბამება ევროკავშირის მიერ აღიარებული საჯარო ინტერესებიდან მომდინარე მიზნებს ან საჭიროა სხვათა უფლებებისა და თავისუფლებების დასაცავად.

დირექტივის მე-15 მუხლის 1-ლი პუნქტის თანახმად, ამ მუხლით განსაზღვრული ამოცანების გათვალისწინებით, წევრმა სახელმწიფოებმა შესაძლებელია კომუნიკაციების და მასთან დაკავშირებული ტრაფიკის მონაცემების კონფიდენციალურობის პრინციპიდან გადაუხვიონ იმ შემთხვევაში, როცა ეს აუცილებელ, სათანადო და პროპორციულ ზომას წარმოადგენს დემოკრატიულ საზოგადოებაში. რაც შეეხება დირექტივის პრეამბულის მე-11 პუნქტს, ის აცხადებს, რომ მიღებული ზომა მისაღწევი მიზნის მკაცრად პროპორციული საშუალება უნდა იყოს. ამავდროულად, მონაცემთა შენახვა დაიშვება მხოლოდ კონკრეტული ვადით და მას საფუძვლად უნდა ედოს დირექტივის მე-15(1) მუხლით გათვალისწინებული რომელიმე მიზანი.

მოცემულ საქმეში (C-203/15), ეროვნული კანონმდებლობით მონაცემები ინახება ბლანკეტურად და განურჩევლად და ის მიემართება ყველა ელექტრონული კომუნიკაციის საშუალებიდან, *თითოეული* აბონენტისა და რეგისტრირებული მომხმარებლის შესახებ ტრაფიკისა და ადგილმდებარეობის ყველა მონაცემს. ამავდროულად, კანონმდებლობა ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს აკისრებს ვალდებულებას, მონაცემები გამონაკლისების გარეშე, სისტემატურად და უწყვეტად შეინახონ. კანონმდებლობით განსაზღვრული ეს მონაცემთა კატეგორიები კი იგივეა, რასაც გაუქმებული დირექტივა 2006/24 ითვალისწინებდა.

მაშასადამე, მონაცემები, რომლებიც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებმა უნდა შეინახონ, შესაძლებელს ხდის კომუნიკაციის წყაროს და მისი დანიშნულების ადგილის განსაზღვრას, ასევე თარიღის, დროის, ხანგრძლივობის, კომუნიკაციის ტიპის, მომხმარებელთა მიერ გამოყენებული საკომუნიკაციო აღჭურვილობის განსაზღვრას და მობილური საკომუნიკაციო აღჭურვილობის ადგილმდებარეობის დადგენას. ეს მონაცემები, აგრეთვე, შეიცავს აბონენტის ან რეგისტრირებული მომხმარებლის სახელსა და მისამართს, ზარის განმახორციელებელი პირის ტელეფონის ნომერს, ზარის მიმღების ნომერს და ინტერნეტით მომსახურების შემთხვევაში - IP მისამართს. ეს მონაცემები შესაძლებელს ხდის თითოეული პირის იდენტიფიცირებას, ვისთანაც აბონენტმა ან რეგისტრირებულმა მომხმარებელმა კომუნიკაცია დაამყარა, ასევე, განსაზღვრავს კომუნიკაციის დასამყარებლად გამოყენებულ საშუალებას, ადგენს კომუნიკაციის დროსა და ადგილს. მონაცემებით, ასევე, ცნობილი ხდება, აბონენტი ან რეგისტრირებული მომხმარებელი დროის განსაზღვრულ პერიოდში კონკრეტულ პირებთან რა სიხშირით ამყარებდა კომუნიკაციას.

სასამართლომ ხაზგასმით აღნიშნა, რომ ეს მონაცემები, საერთო ჯამში, პირთა პირად ცხოვრებასთან, მათ ყოველდღიურ ჩვევებთან, მუდმივ ან დროებით საცხოვრებელ ადგილებთან, პირთა ყოველდღიურ გადაადგილებასთან, მათ საქმიანობებთან, სოციალურ ურთიერთობებთან და სოციალურ გარემოსთან დაკავშირებით საკმაოდ ზუსტი დასკვნების გამოტანის შესაძლებლობას იძლევა. ეს მონაცემები პირთა შესახებ საკმაოდ დეტალურ, ინდივიდუალურ აღწერილობებს შეიცავს, რაც პირადი ცხოვრების ხელშეუხებლობის თვალსაზრისით, კომუნიკაციების შინაარსზე ნაკლებ სენსიტიურ ინფორმაციას არ წარმოადგენს.

სასამართლომ მიუთითა, რომ ქარტიის მე-7 და მე-8 მუხლებით გარანტირებულ უფლებაში ამგვარი ჩარევა სიმწვავის მნიშვნელოვან ხარისხს აღწევს და ის განსაკუთრებულად მძიმე ჩარევად უნდა შეფასდეს. აბონენტთა ან რეგისტრირებულ მომხმარებელთა შეტყობინების

გარეშე ამ მონაცემთა შენახვამ შესაძლებელია მათ აფიქრებინოს, რომ მათ პირად ცხოვრებაზე გამუდმებული მეთვალყურეობა მიმდინარეობს. მიუხედავად იმისა, რომ ამ მონაცემებით საუბრის შინაარსი არ დგინდება, ტრაფიკის და ადგილმდებარეობის მონაცემების შენახვამ შესაძლებელია უარყოფითი ზეგავლენა მოახდინოს მომხმარებელთა მიერ ელექტრონული საკომუნიკაციო საშუალებების გამოყენებაზე და შედეგად, მათ გამოხატვის თავისუფლებაზე. ჩარევის სიმძიმიდან გამომდინარე, ამგვარი ზომის გამოყენება მხოლოდ მძიმე დანაშაულებთან ბრძოლის მიზნით შეიძლება გამართლდეს. მართალია, მძიმე დანაშაულის, განსაკუთრებით კი ორგანიზებული დანაშაულისა და ტერორიზმის წინააღმდეგ ბრძოლის ეფექტიანობა დიდწილად თანამედროვე საგამოძიებო მეთოდებს უკავშირდება, ეს მიზანი არ შეიძლება იყოს ზოგადი. დანაშაულთან ბრძოლის ზოგადი მიზნებით, ტრაფიკისა და ადგილმდებარეობის ნებისმიერი მონაცემის შენახვის ბლანკეტური და განურჩეველი წესი ვერ ჩაითვლება მიზნის მიღწევის აბსოლუტურად აუცილებელ საშუალებად. ამგვარი კანონმდებლობა წესიდან გამონაკლისს კი არ განსაზღვრავს, არამედ ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვას ხდის ზოგადი წესად, მაშინ როდესაც დირექტივა ადგენს, რომ მონაცემთა შენახვა მხოლოდ გამონაკლის შემთხვევებში შეიძლება განხორციელდეს.

ამავდროულად, სასამართლოს განმარტებით, კანონმდებლობა მისაღწევი მიზნის შესაბამისად არ ადგენს განსხვავებულ წესებს, არ აწესებს შეზღუდვებს ან გამონაკლისებს. ის ყოვლისმომცველია, ვინაიდან შეეხება ყველა პირს, ვინც ელექტრონული საკომუნიკაციო მომსახურებით სარგებლობს, იმ პირებსაც კი, რომლებიც არაპირდაპირაც კი არ შეიძლება აღმოჩნდნენ იმგვარ ვითარებაში, რომელიც საფუძვლად დაედება სისხლის სამართლის საქმის წარმოების დაწყებას. ამდენად, კანონმდებლობა მიემართება იმ ადამიანებსაც, რომელთაც მძიმე დანაშაულთან შემხებლობა საერთოდ არ აქვთ. მეტიც, მოცემული რეგულირება იმ პირებსაც შეეხება, ვისაც ეროვნული კანონმდებლობით პროფესიული საიდუმლოების შენახვის ვალდებულება აკისრიათ.

ამგვარი კანონმდებლობა აგრეთვე არ აწესებს არავითარ შეზღუდვას მონაცემთა შენახვისთვის:

01 გარკვეულ პერიოდთან დაკავშირებული მონაცემების ან/და გეოგრაფიული არეალის ან/და მძიმე დანაშაულთან სავარაუდო შემხებლობაში მყოფ პირთა ჯგუფების მიხედვით;

02 იმ პირთა მიხედვით, რომელთა შესახებ მონაცემების შენახვამ სხვადასხვა მიზეზით შესაძლოა დანაშაულთან ბრძოლას გარკვეული დახმარება გაუწიოს.

ამდენად, სასამართლომ ჩათვალა, რომ ეროვნული კანონმდებლობა არ წარმოადგენდა დემოკრატიულ საზოგადოებაში მიზნის მიღწევის მკაცრად აუცილებელ საშუალებას.

სასამართლომ ასევე მიუთითა, რომ წევრმა ქვეყნებმა პრევენციული მიზნებით შესაძლოა მიიღონ კანონმდებლობა, რომელიც მძიმე დანაშაულთან საბრძოლველად ტრაფიკისა და ადგილმდებარეობის მონაცემების შენახვის კონკრეტულ პირებზე მიმართულ წესს დაადგენს,

თუ მონაცემთა შენახვა შეზღუდულია შენახული მონაცემების კატეგორიების, საკომუნიკაციო საშუალებების, ჩართული პირების და შენახვის ხანგრძლივობის მიხედვით. მნიშვნელოვანია, რომ ეროვნულმა კანონმდებლობამ ჩამოაყალიბოს ზუსტი და მკაფიო წესები, რომელიც მონაცემთა შენახვის ფარგლებსა და მათ გამოყენებას შეეხება. ასევე, შემოღებულ უნდა იქნას მინიმალური გარანტიები, რათა იმ პირებს, რომელთა მონაცემებიც ინახება, ჰქონდეთ მათი პერსონალური მონაცემების ბოროტად გამოყენების რისკისგან თავის დაცვის საკმარისი გარანტიები. კანონმდებლობა უნდა უთითებდეს იმ პირობებსა და გარემოებებს, რომელთა დადგომის შემთხვევაშიც შეიძლება მონაცემთა შენახვის, როგორც პრევენციული მექანიზმის, გამოყენება, რაც უზრუნველყოფს მხოლოდ მკაცრი აუცილებლობის შემთხვევაში მათ შენახვას. სასამართლოს თანახმად, წესები შესაძლოა განსხვავდებოდეს ქვეყნების მიხედვით, თუმცა მონაცემთა შენახვა ყოველთვის ობიექტური კრიტერიუმების საფუძველზე უნდა განხორციელდეს. ეს ობიექტური კრიტერიუმები ცხადად უნდა მიუთითებდეს, რომ მისაღწევ მიზანსა და მონაცემთა შენახვას შორის მჭიდრო კავშირია. ამავდროულად, ეროვნული კანონმდებლობა უნდა ემყარებოდეს ობიექტურ მოცემულობას, რომელიც შესაძლებელს ხდის საზოგადოების იმ ნაწილის განსაზღვრას, რომელთა მონაცემების შენახვამ შეიძლება გამოამჟღავნოს მძიმე დანაშაულებთან მათი არაპირდაპირი კავშირი მაინც. მაგალითად, ეს ფარგლები შეიძლება ემყარებოდეს გეოგრაფიულ კრიტერიუმებს, როცა ხელისუფლების შესაბამისი ორგანოები მიიჩნევენ, რომ ობიექტური მტკიცებულების საფუძველზე, ამა თუ იმ ტერიტორიაზე მძიმე დანაშაულის მომზადების ან ჩადენის მნიშვნელოვანი საფრთხე არსებობს.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, სასამართლომ დაასკვნა, რომ საქმეში C-203-15, ქარტიის მე-7, მე-8, მე-11 და 52(1)-ე მუხლების გათვალისწინებით, ეროვნული კანონმდებლობა დირექტივის მე-15(1) მუხლს არ შეესაბამება, ვინაიდან კანონმდებლობით მონაცემები ინახება ბლანკეტურად და განურჩევლად და ის მიემართება ყველა ელექტრონული კომუნიკაციის საშუალებიდან, *თითოეული* აბონენტისა და რეგისტრირებული მომხმარებლის შესახებ ტრაფიკისა და ადგილმდებარეობის ყველა მონაცემს.

● მეორე შეკითხვა საქმეზე C203-15 და პირველი შეკითხვა საქმეზე C-698/15

სასამართლოს თანახმად, შინაარსობრივად ორივე შეკითხვა ეძებს პასუხს კითხვაზე, უნდა განიმარტოს თუ არა 2002/58 დირექტივის მე-15 მუხლი იმგვარად, რომ ის ეროვნული კანონმდებლობით ადგილმდებარეობისა და ტრაფიკის მონაცემების დაცვისა და უსაფრთხოების წესების, განსაკუთრებით კი ამ მონაცემებზე ხელისუფლების შესაბამისი ორგანოების წვდომის წესების იმგვარ რეგულირებას კრძალავს, რომელიც არ შემოფარგლავს მონაცემებთან წვდომას მხოლოდ მძიმე დანაშაულთან ბრძოლის მიზნით, რომელიც არ მოითხოვს, წვდომა განხორციელდეს სასამართლოს ან სხვა დამოუკიდებელი ორგანოს მიერ წინასწარი განხილვის საფუძველზე, და რომელიც არ აწესებს მონაცემების მხოლოდ ევროკავშირის ფარგლებში შენახვის ვალდებულებას.

სასამართლომ აღნიშნა, რომ კონფიდენციალურობის პრინციპიდან გადახვევა დირექტივის მე-15(1) მუხლში ამომწურავად ჩამოთვლილი მიზნებიდან ერთ-ერთს უნდა ემსახურებოდეს. ვინაიდან შენახულ მონაცემებზე წვდომისას ძირითად უფლებაში ჩარევა საკმაოდ მძიმე ხასიათის არის, ხოლო საკანონმდებლო ზომა მისაღწევი მიზნის პროპორციული უნდა იყოს. დანაშაულის პრევენციის, გამოვლენის, გამოძიების, სისხლისსამართლებრივი დევნის დაწყების სფეროში ამ ტიპის მონაცემებზე წვდომა მხოლოდ მძიმე დანაშაულთან ბრძოლის მიზანმა შეიძლება გაამართლოს.

რაც შეეხება პროპორციულობის პრინციპს, სასამართლომ განმარტა, რომ ეროვნული კანონმდებლობით დადგენილი წესები, რომლითაც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლები ვალდებულნი არიან ამ მონაცემებზე ხელისუფლების შესაბამისი ორგანოების წვდომა დაუშვან, არ უნდა სცდებოდეს აბსოლუტური აუცილებლობის ფარგლებს. დამატებით, საკანონმდებლო ზომები, რომლებზეც დირექტივის მე-15(1) მუხლი მიუთითებს, უნდა ექვემდებარებოდეს სათანადო გარანტიებს, უნდა არსებობდეს მონაცემთა შენახვასთან დაკავშირებით მკაფიო და ზუსტი ნორმები, რომლებიც იმ გარემოებებსა და პირობებზე მიუთითებს, რომელთა დადგომის შემთხვევაშიც, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლები ვალდებულნი იქნებიან, შენახულ მონაცემებზე ხელისუფლების შესაბამისი ორგანოების წვდომა დაუშვან. კანონმდებლობა ასევე უნდა მოიცავდეს მატერიალურ და პროცედურულ ნორმებს, რომლებიც ამ მონაცემებზე ხელისუფლების შესაბამისი ორგანოების წვდომას არეგულირებს.

შესაბამისად, სასამართლოს განმარტებით, ყველა მონაცემზე წვდომის ზოგადი წესი, როცა ეს ზომა პირდაპირ ან არაპირდაპირ არ უკავშირდება მისაღწევ მიზანს, ვერ შეფასდება აბსოლუტურად აუცილებელ საშუალებად. მნიშვნელოვანია, რომ ეროვნული კანონმდებლობა ობიექტურ კრიტერიუმებს ეფუძნებოდეს, განსაზღვრავდეს იმ გარემოებებსა და პირობებს, რომელთა არსებობის შემთხვევაშიც ეროვნული ხელისუფლების შესაბამის ორგანოებს აბონენტთა და რეგისტრირებულ მომხმარებელთა მონაცემებზე წვდომის უფლება მიენიჭებათ. ზოგადი წესით იმის განსაზღვრა, რომ ხელისუფლების შესაბამის ორგანოებს დანაშაულთან ბრძოლის მიზნით უფლება აქვთ შენახულ მონაცემებზე წვდომა ჰქონდეთ, შეიძლება მხოლოდ იმ პირების მონაცემებთან დაკავშირებით, რომლებიც ეჭვმიტანილნი არიან მძიმე დანაშაულის დაგეგმვაში, აპირებენ დანაშაულის ჩადენას ან უკვე ჩაიდინეს დანაშაული, ასევე იმ შემთხვევაში, როცა ამა თუ იმ სახით მათი დანაშაულთან შემხებლობა დგინდება. მიუხედავად ამისა, განსაზღვრულ შემთხვევებში, როცა ტერორისტული საქმიანობის შედეგად, ეროვნულ უსაფრთხოებას, თავდაცვას ან საზოგადოებრივ უსაფრთხოებას საფრთხე ემუქრება, სხვა პირთა მონაცემებზე წვდომაც შეიძლება დაიშვას, როცა ობიექტური მტკიცებულებებით დგინდება, რომ ეს მონაცემები, ამ კონკრეტულ შემთხვევაში, ამგვარ ქმედებებთან ბრძოლას მნიშვნელოვნად შეუწყობს ხელს.

სასამართლომ ასევე ხაზი გაუსვა, ზოგადი წესით, გადაუდებელი აუცილებლობის შემთხვევების გარდა, შენახულ მონაცემებთან ეროვნული ხელისუფლების შესაბამისი ორგანოების წვდომაზე სასამართლოს ან დამოუკიდებელი ადმინისტრაციული მექანიზმის მიერ წინასწარ განხილვის მნიშვნელობას და აღნიშნა, რომ გადაწყვეტილება მიღებულ უნდა იქნას დასაბუთებული შუამდგომლობის საფუძველზე დანაშაულის პრევენციის, გამოვლენის ან სისხლისსამართლებრივი დევნის დაწყების პროცედურული ჩარჩოს ფარგლებში.

სასამართლომ ასევე მიუთითა ეროვნული ხელისუფლების შესაბამისი ორგანოების ვალდებულებაზე, შეატყობინონ იმ პირებს, რომელთა მონაცემებზეც მათ წვდომა ჰქონდათ, მას შემდეგ, რაც ამგვარი შეტყობინება გამოძიების ინტერესებს საფრთხეს აღარ უქმნის. სასამართლოს განმარტებით, შეტყობინების წესი ამ პირებისთვის დირექტივის მე-15 მუხლის მე-2 ნაწილით გათვალისწინებული სამართლებრივი დაცვის გარანტიების არსებობას უზრუნველყოფს.

გარდა ამისა, დირექტივა ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს შესაბამისი ტექნიკური და ორგანიზაციული ზომების მიღებას ავალდებულებს, რათა მონაცემები მათი ბოროტად გამოყენების ან/და მათზე არაკანონიერად წვდომის რისკებისგან დაცული იყოს. სასამართლოს განმარტებით, ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლები ვალდებულნი არიან სათანადო ტექნიკური და ორგანიზაციული ზომებით უზრუნველყონ ამ მონაცემთა კონფიდენციალურობა და მათი მაღალ დონეზე დაცვა. კერძოდ, მათ უნდა შემოიღონ დებულება, რომელიც აწესებს, რომ მონაცემები შეინახება ევროკავშირის ფარგლებში და განადგურდება შენახვის ვადის დასრულებისთანავე.

ნებისმიერ შემთხვევაში, წევრმა ქვეყნებმა უნდა უზრუნველყონ პერსონალური მონაცემების დამუშავების ევროკავშირის კანონმდებლობით გარანტირებულ დაცვის ხარისხთან შესაბამისობის დამოუკიდებელი ორგანოს მიერ განხილვა, წინააღმდეგ შემთხვევაში, პირებს, რომელთა მონაცემებიც შენახულ იქნა, არ მიეცემათ პერსონალური მონაცემების დაცვის მიზნით ეროვნულ საზედამხედველო ორგანოში საჩივრის შეტანის შესაძლებლობა.

სასამართლომ დაადგინა, რომ დირექტივის მე-15 მუხლის ზემოაღნიშნული განმარტება კრძალავს ეროვნული კანონმდებლობით ადგილმდებარეობისა და ტრაფიკის მონაცემების დაცვისა და უსაფრთხოების წესების, განსაკუთრებით კი ამ მონაცემებზე ხელისუფლების შესაბამისი ორგანოების წვდომის წესების იმგვარ რეგულირებას, რომელიც მონაცემებთან წვდომას მხოლოდ მძიმე დანაშაულთან ბრძოლის მიზნით არ შემოფარგლავს, რომელიც არ მოითხოვს წვდომა განხორციელდეს სასამართლოს ან სხვა დამოუკიდებელი ორგანოს მიერ წინასწარი განხილვის საფუძველზე, და რომელიც არ აწესებს მონაცემების მხოლოდ ევროკავშირის ფარგლებში შენახვის ვალდებულებას.

● საქმეზე C-698/15 სასამართლოსთვის დასმული მე-2 შეკითხვა

მეორე შეკითხვა გულისხმობს იმის დადგენას, სცილდება თუ არა *Digital Rights Ireland* გადაწყვეტილებაში სასამართლოს მიერ ქარტიის მე-7 და მე-8 მუხლების განმარტება ევროპული კონვენციის მე-8 მუხლის ფარგლებს.

სასამართლომ მიუთითა, რომ ევროპული კონვენციით აღიარებული უფლებები ევროკავშირის კანონმდებლობის ძირითად პრინციპებს წარმოადგენს, თუმცა ის ოფიციალურად ევროკავშირის კანონმდებლობის ნაწილი არ არის. შესაბამისად, 2002/58 დირექტივა შესაძლებელია განიმარტოს მხოლოდ ქარტიით გარანტირებული ძირითადი უფლებების

შუქზე. ამავდროულად, ქარტიის 52-ე მუხლის მე-3 პუნქტი მიზნად ისახავს ევროპულ კონვენციასა და ევროპის კავშირის ძირითად უფლებათა ქარტიას შორის თანმიმდევრულობის უზრუნველყოფას, თუმცა არ გამორიცხავს, ევროკავშირის კანონმდებლობამ შემოიღოს დაცვის უფრო მაღალი გარანტიები, ვიდრე ამას ევროპული კონვენცია ითვალისწინებს.

სასამართლომ აღნიშნა, რომ განსახილველი დავის ფარგლებში, მისი შეფასების საგანს წარმოადგენს 2002/58 დირექტივა, დასმულ კითხვაზე პასუხს კი დირექტივის განმარტებაზე ზეგავლენა ვერ ექნება. აღნიშნულ კითხვაზე პასუხი ვერც ევროკავშირის კანონმდებლობის იმგვარი ინტერპრეტაციის შესაძლებლობას იძლევა, რომელიც დავის გადასაწყვეტად აუცილებელი იქნება. ამ მსჯელობის საფუძველზე, სასამართლომ ეს კითხვა დაუშვებლად ცნო.

სასამართლოს გადაწყვეტილება

01 **ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ ევროპარლამენტის და საბჭოს 2002 წლის 12 ივლისის 2002/58/EC დირექტივის (პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ დირექტივა) მე-15(1) მუხლი ევროკავშირის ძირითად უფლებათა ქარტიის მე-7, მე-8, მე-11 და 51(1)-ე მუხლების შუქზე განიმარტება იმგვარად, რომ კრძალავს ეროვნული კანონმდებლობით, დანაშაულთან ბრძოლის მიზნით, ყველა აბონენტისა და რეგისტრირებული მომხმარებლის შესახებ ელექტრონული კომუნიკაციების ნებისმიერი საშუალებიდან ტრაფიკისა და ადგილმდებარეობის ყველა მონაცემის ბლანკეტურ და განურჩეველ შენახვას.**

02 **2002/58 დირექტივის მე-15(1) მუხლი ძირითად უფლებათა ქარტიის მე-7, მე-8, მე-11 და 51(1)-ე მუხლების შუქზე განიმარტება იმგვარად, რომ კრძალავს ეროვნული კანონმდებლობით ადგილმდებარეობისა და ტრაფიკის მონაცემების დაცვისა და უსაფრთხოების, განსაკუთრებით კი ამ მონაცემებზე ხელისუფლების შესაბამისი ორგანოების წვდომის იმგვარ რეგულირებას, რომელიც მონაცემებზე წვდომას მძიმე დანაშაულთან ბრძოლის მიზნით არ შემოფარგლავს, რომელიც არ მოითხოვს წვდომის საკითხის სასამართლოს ან სხვა დამოუკიდებელი ორგანოს მიერ წინასწარ განხილვას, და რომელიც არ აწესებს მონაცემების მხოლოდ ევროკავშირის ფარგლებში შენახვის ვალდებულებას.**

03 **ინგლისისა და უელსის სააპელაციო სასამართლოს მიერ დასმული მე-3 შეკითხვა დაუშვებლად იქნას ცნობილი.**

ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI)

ტ. შევჩენკოს ქ. 20 +995 32 2 921514 INFO@IDFI.GE WWW.IDFI.GE