საერთაშორისო გამჭვირვალობა საქართველო

DCAF a centre for security, development and the rule of law

ადამიანის უფლებების სწავლებისა და მონიტორინგის ცენტრი EMC Human Rights Education and Monitoring Center

ღია საზოგადოების ფონდი

უსაფრთხოების სამსახურის მართვისა და ზედამხედველობის საერთაშორისო სტანდარტები და საუკეთესო პრაქტიკები

თბილისი 2018

ნაზლი ილდირიმ შირკოლკ/Nazli Yildirim Schierkolk

კვლევა და ანგარიშზე მუშაობა ფინანსურად მხარდაჭერილი იყო შეიარაღებული ძალების დემოკრატიული კონტროლის ჟენევის ცენტრის მიერ (DCAF). დოკუმენტში წარმოდგენილი ანალიზი და შეფასებები შესაძლოა ცენტრის შეხედულებებს არ ემთხვეოდეს.

სარჩევი

შესავალი

პროექტის მიზნები

საქართველოს შინაგან საქმეთა სამინისტროს რეფორმის ფარგლებში, სახელმწიფო უსაფრთხოების სამსახური გამოეყო სამინისტროს და ცალკე ინსტიტუტად ჩამოყალიბდა. სახელმწიფო უსაფრთხოების სამსახურის შესახებ[1] ახალი კანონი არეგულირებს მის მანდატს, უფლებამოსილებებს და ფუნქციებს. კანონი სამსახურს არსებითად ფართო მანდატს ანიჭებს, რომელიც მათ შორის მოიცავს, ტრანსნაციონალური ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლას და კორუფციის პრევენციას, იდენტიფიცირებასა და აღმოფხვრას. ამის გარდა, სახელმწიფო უსაფრთხოების სამსახურს ენიჭება სამართალდამცავი ორგანოების უფლებამოსილებებიც, როგორებიცაა გამოძიება, ჩხრეკა, ბრალდებულის და დამნაშავის დაკავება და დაპატიმრება. ასეთი ფართო მანდატი და საპოლიციო უფლებამოსილებები უსაფრთხოების სამსახურის ზედამხედველობის მყარი გარანტიების გარეშე, საერთაშორისო და ადგილობრივი აქტორების შეშფოთებას იწვევს, რომლებიც სახელმწიფო უსაფრთხოების სამსახურის დემოკრატიული მართვის და ზედამხედველობის გაძლიერების საჭიროებაზე უთითებენ.

ამ საკითხებზე საჯარო დებატების ხელშეწყობის მიზნით, საერთაშორისო გამჭვირვალობა საქართველომ (TI Georgia) და ადამიანის უფლებების სწავლებისა და მონიტორინგის ცენტრმა (EMC) ფონდი ღია საზოგადოების ფინანსური მხარდაჭერით პროექტის „უსაფრთხოების სექტორის თანამედროვე სისტემის შექმნის ადვოკატირება“ განხორციელება დაიწყეს. პროექტი მიზნად ისახავს ანგარიშვალდებული, ადამიანის უფლებების დაცვაზე ორიენტირებული, თანამედროვე უსაფრთხოების სამსახურის ადვოკატირებას, რომელიც საკუთარ საქმიანობას საერთაშორისო სტანდარტებთან შესაბამისობაში წარმართავს.

მეთოდოლოგია და ანგარიშის სტრუქტურა

პროექტის ადვოკატირების კომპონენტის ნაწილია ანგარიშის გამოქვეყნება, რომელიც მიმოიხილავს საერთაშორისო სტანდარტებს და საუკეთესო პრაქტიკებს უსაფრთხოების სამსახურის მართვისა და ზედამხედველობის კუთხით. ამ მიმართულებით, TI საქართველომ და EMC-იმ ერთობლივად ანგარიშში განსახილველი ოთხი მთავარი საკითხის იდენტიფიცირება მოახდინეს: (i) უსაფრთხოების სამსახურის მანდატი და ფუნქციები; (ii) აღმასრულებელი კონტროლი უსაფრთხოების სამსახურზე (iii) უსაფრთხოების სამსახურის ზედამხედველობა და ანგარიშვალდებულება; (iv) უსაფრთხოების სამსახურების გამჭვირვალობა.

ანგარიში შედგება ოთხი ნაწილისგან, რომელიც შესაბამისად დასახელებულ ოთხ საკითხს ეხება. თითოეული თავი იწყება ისეთი ავტორიტეტული საერთაშორისო და ევროპული ორგანოების და აქტორების მიერ განსაზღვრული საერთაშორისო სტანდარტების მიმოხილვით, როგორებიცაა გაეროს სპეციალური მომხსენებელი ტერორიზმთან ბრძოლის დროს ადამიანის უფლებებისა და თავისუფლებების მხარდაჭერის და დაცვის საკითხებში; ევროპული კომისია სამართლის მეშვეობით დემოკრატიის დასაცავად (ვენეციის კომისია), ევროპის საბჭოს ადამიანის უფლებათა კომისარი და ევროკავშირის ადამიანის ძირითადი უფლებების სააგენტო (EU FRA).

1 ხელმისაწვდომია: https://matsne.gov.ge/ru/document/download/2905260/1/en/pdf

თითოეულ თავში საერთაშორისო სტანდარტებს მოსდევს შერჩეული ოთხი ქვეყნის რელევანტური პრაქტიკების მოკლე მიმოხილვაც. ამ ანგარიშის მიზნებისთვის, საქართველოს ზოგადი ევრო-ატლანტიკური პერსპექტივის გათვალისწინებით, შემდეგი ოთხი ქვეყანა იქნა შერჩეული:

- გერმანია და ბელგია - ორი ევროპული ქვეყანა კარგად განვითარებული ზედამხედველობის და ანგარიშვალდებულების სისტემით, რომლებსაც ხშირად საუკეთესო პრაქტიკების მაგალითებად მოიხსენიებენ;
- ხორვატია - ევროპული ქვეყანა დემოკრატიზაციის ახლო წარსულით, რომელმაც ევროკავშირთან ინტეგრაციის პროცესში უსაფრთხოების სამსახურების მნიშვნელოვანი რეფორმა გაატარა;
- კანადა - არაევროპული ქვეყანა, ამ დროისთვის ნატოს და ეუთოს წევრი, რომელსაც საუკეთესო პრაქტიკის მაგალითად ხშირად მოიხსენიებენ.

უნდა აღინიშნოს, რომ უსაფრთხოების სამსახურის და სახელმწიფო დაზვერვის ერთიანი მართვისა და ზედამხედველობის სისტემა არც ერთ ქვეყანაში არ გვხვდება. თითოეული ქვეყანა განსხვავებულ გარემოებებსა და მუდმივად ცვალებად გლობალურ უსაფრთხოების გარემოში ცდილობს არაერთ ტრანსნაციონალურ საფრთხესთან დაპირისპირებას. ამ ოთხი ქვეყნის პრაქტიკების აღწერა მიზნად არ ისახავს საქართველოში არსებული გამოწვევების გადაწყვეტის ერთი გზის დასახვას. ისინი იმ განსხვავებულ მიდგომებს ხდიან თვალსაჩინოს, რომელთა საშუალებით ამ ქვეყნებში საერთაშორისო სტანდარტების იმპლემენტაცია ხდება და დაინტერესებული პირებისთვის საქართველოში წარმოადგენენ პლატფორმას, ქართული კონტექსტისთვის ყველაზე ეფექტიან მექანიზმებზე დისკუსიისა და რეფლექსიისთვის.

შენიშვნა ტერმინოლოგიაზე

ევროკავშირის ადამიანის ძირითადი უფლებების სააგენტო ფუნდამენტურ განსხვავებას უსვამს ხაზს დაზვერვის და უსაფრთხოების სამსახურებს შორის: დაზვერვის სამსახური არის უწყება, რომელიც სარგებლობს საგარეო მანდატით და მუშაობს საგარეო საფრთხეების წინააღმდეგ, სახელმწიფო უსაფრთხოების სამსახური კი ადგილობრივ საფრთხეებს ებრძვის.[2] საერთაშორისო სტანდარტები და პრაქტიკა ამ ანგარიშში ძირითადად უსაფრთხოების სამსახურს ეხება, თუმცა საჭიროების შემთხვევაში მითითებას აკეთებს დაზვერვის სამსახურზეც.

უსაფრთხოების სამსახური

მოცემულ ანგარიშში „უსაფრთხოების სამსახური“ აღნიშნავს „სახელმწიფო უწყებებს, მათ შორის ავტონომიურ უწყებებს და მთავრობის ქვეშ არსებულ დეპარტამენტებს/სამმართველოებს, რომელთაც აქვთ მანდატი შეაგროვონ, გაანალიზონ და გაავრცელონ ინფორმაცია ქვეყნის მასშტაბით, რათა პოლიტიკის განმსაზღვრელმა პირებმა, გამომძიებლებმა და სასაზღვრო/საბაჟო სააგენტოებმა ინფორმირებული გადაწყვეტილება მიიღონ ეროვნული უსაფრთხოების და სხვა მნიშვნელოვანი ეროვნული ინტერესების საკითხებზე.[3]

ზედამხედველობა

2 European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks, (hereinafter EU FRA, Surveillance by Intelligence Services)* (Luxembourg, 2015), p. 13, available from: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

3 Council of Europe (2015) Democratic and Effective Oversight of Security Services, p.18, available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

ანგარიშში ტერმინი ზედამხედველობა ხშირად არის ნახსენები, ამიტომ დასაწყისშივე მნიშვნელოვანია მისი ზუსტი განმარტება. ზედამხედველობა კომპლექსური ტერმინია და რამდენიმე პროცესს ახასიათებს, მათ შორისაა: წინასწარი კონტროლი, მიმდინარე მონიტორინგი, შემდგომი გადასინჯვა, ასევე შეფასება და გამოძიება. უსაფრთხოების სამსახურის ზედამხედველობა ხორციელდება რამდენიმე გარე აქტორის მიერ, მათ შორის სასამართლო ხელისუფლების, პარლამენტის, ადამიანის უფლებების ეროვნული ინსტიტუტების (NHRI), ომბუდსმენის ტიპის ინსტიტუტების, პრევენციის ეროვნული მექანიზმის (NPM), აუდიტორული უწყებების, სპეციალიზებული ზედამხედველობის ორგანოების, მედიისა და არასამთავრობო ორგანიზაციების მიერ. ზედამხედველობა უნდა განვასხვავოთ კონტროლისგან, რადგან ეს უკანასკნელი გულისხმობს ორგანიზაციის პოლიტიკის და საქმიანობის მართვის უფლებამოსილებას. ასეთი კონტროლი კი, როგორც წესი, ასოცირდება აღმასრულებელი ხელისუფლების შტოსთან.[4]

4 Born and Geisler Mesevage, 'Introducing Intelligence Oversight' in Born and Wills (ed.) 'Overseeing Intelligence Services: A Toolkit' (DCAF, 2012) p.6.

თავი 1: უსაფრთხოების სამსახურის მანდატი და ფუნქციები

უსაფრთხოების სამსახურის სტრუქტურის, მანდატის და ფუნქციების განსაზღვრა მნიშვნელოვან გავლენას ახდენს სამსახურის ფუნქციონირებასა და დემოკრატიულ საზოგადოებაში ფუნდამენტური უფლებების და თავისუფლებების დაცვაზე. ნაშრომის პირველი თავი მიმოიხილავს ძირითად საერთაშორისო სტანდარტებს ზემოთხსენებულ საკითხებზე, განსაკუთრებული ფოკუსით უსაფრთხოების სამსახურის სტრუქტურაზე, მანდატზე და ეროვნული უსაფრთხოების რისკების განმარტებაზე; უსაფრთხოების სამსახურისთვის სამართალდამცავი უფლებამოსილებების მინიჭების და ფარული მეთვალყურეობის განხორციელების სადავო საკითხებზე.

1.1 უსაფრთხოების/დაზვერვის სამსახურების სტრუქტურა

უსაფრთხოებისა და დაზვერვის სამსახურების ინსტიტუციური წყობა ზოგადად განეკუთვნება სახელმწიფოების შიდა კომპეტენციის სფეროს, რომელიც განისაზღვრება კონკრეტული სახელმწიფოსთვის დამახასიათებელი საფრთხეებისა და საჭიროებების საფუძველზე. თუმცა, მკაფიო ტენდენცია იკვეთება სამოქალაქო და სამხედრო სამსახურების განსხვავების კუთხით. 2017 წლის მდგომარეობით, მალტას და ლუქსემბურგის გარდა, ევროკავშირის ყველა ქვეყანაში, სამოქალაქო და სამხედრო საკითხებზე პასუხისმგებელი როგორც მინიმუმ ორი სხვადასხვა სამსახური ფუნქციონირებს.[5] ეს ანგარიში ყურადღებას ამახვილებს უსაფრთხოების სამსახურის სამოქალაქო ნაწილზე (შემდგომში სამოქალაქო უსაფრთხოების სამსახური).

მნიშვნელოვანი განსხვავებები არსებობს სამოქალაქო უსაფრთხოების სამსახურების სტრუქტურის კუთხით. ზოგიერთ ევროპულ ქვეყანაში ერთი სამოქალაქო უწყება ფუნქციონირებს, რომელიც სარგებლობს როგორც შიდა ეროვნული უსაფრთხოების, ისე საგარეო დაზვერვის მანდატით. დანიის, ჰოლანდიის, სლოვენიის და პორტუგალიის უსაფრთხოების/დაზვერვის სამსახურები ამ მიდგომის მაგალითებს წარმოადგენენ. სხვა ევროპულ ქვეყნებში ჩამოყალიბებულია ორი სხვადასხვა უწყება განსხვავებული - ეროვნული უსაფრთხოების და საგარეო დაზვერვის მანდატებით. ასეთი ქვეყნებია ჩეხეთი, საფრანგეთი, იტალია, ინგლისი და გარკვეულწილად გერმანია.[6] ამის გარდა, მაგალითად ავსტრიასა და ფინეთში არსებობს ერთი სამოქალაქო უსაფრთხოების სამსახური მხოლოდ შიდა ეროვნული უსაფრთხოების მანდატით.[7]

არ არსებობს ერთი ფართოდ აღიარებული საერთაშორისო სტანდარტი სამოქალაქო უსაფრთხოების და დაზვერვის სამსახურების სტრუქტურასთან დაკავშირებით. ერთიანი სამოქალაქო უსაფრთხოების სამსახური შიდა უსაფრთხოების და საგარეო დაზვერვის მანდატით გარდაუვლად იწვევს ერთ ინსტიტუციაში ძალაუფლების გადაჭარბებულ კონცენტრაციას. მკაფიო საკანონმდებლო ბაზისა და ზედამხედველობის ძლიერი მექანიზმების გარეშე, არსებობს რისკი, რომ საგარეო დაზვერვის ღონისძიებები (რომელიც, როგორც წესი, ნაკლებად მკაცრად არის რეგულირებული) გამოყენებულ იქნეს ეროვნული უსაფრთხოების მანდატის კონტექსტშიც (რომელიც როგორც წესი უფრო მკაცრ

5 EU FRA, Surveillance by Intelligence Services, (2015), p.13, also see the table in Annex of the same publication on p.94.

6 At the federal level, Germany has a distinct domestic security service (BfV). The federal intelligence service (BND), although most of its focus is on foreign intelligence, is categorized by the EU FRA as an agency with both an internal and external mandate. See EU FRA, Surveillance by Intelligence Services, (2015),, p.94

7 Ibid. In these countries, foreign intelligence is carried out by the military intelligence service.

კონტროლს ექვემდებარება). მეორე მხრივ, რადგან შიდა და გარე საფრთხეებს შორის ზღვარი უფრო და უფრო ბუნდოვანი ხდება, შიდა და გარე მანდატით ორი სხვადასხვა უწყების ფუნქციონირება შესაძლოა ძალაუფლებისთვის ბრძოლაში, სააგენტოებს შორის კოორდინაციის/თანამშრომლობის პრობლემებში და ზედამხედველობის ფრაგმენტაციაში გადაიზარდოს.[8]

აქედან გამომდინარე, ინსტიტუციური წყობის მიღმა, განმსაზღვრელი მნიშვნელობისაა საერთაშორისო სამართალთან და სტანდარტებთან შესაბამისი, ყოვლისმომცველი სამართლებრივი საფუძვლის არსებობა, რომელიც დაარეგულირებს უსაფრთხოების და სპეციალური სამსახურების საქმიანობის ყველა ასპექტს; ასევე ანგარიშვალდებულების ძლიერი სისტემა, როდესაც აღმასრულებელი, საკანონმდებლო, სასამართლო ხელისუფლება და დამოუკიდებელი უწყებები შესაბამის საზედამხედველო როლს და ვალდებულებებს ეფექტიანად შეასრულებენ.

საკითხები, რომლებიც უსაფრთხოების სამსახურების იერარქიულ მოწყობას და სუბორდინაციას ეხება განხილული იქნება მეორე თავში, რომელიც სახელმწიფო სამსახურების აღმასრულებელ კონტროლს შეეხება.

1.2. უსაფრთხოების სამსახურის მანდატი

„ტერორიზმის წინააღმდეგ მიმართული სპეციალური სამსახურების საქმიანობის დროს ადამიანის უფლებების დაცვის უზრუნველყოფისთვის სამართლებრივი და ინსტიტუციური ჩარჩოს და ღონისძიებების შესახებ გაეროს საუკეთესო პრაქტიკების მიმოხილვის“ (შემდგომში გაეროს საუკეთესო პრაქტიკების მიმოხილვა) თანახმად, უსაფრთხოების სამსახურის მთავარი მიზანია *‘შეაგროვოს, გაანალიზოს და გაავრცელოს* ინფორმაცია, რომელიც პოლიტიკის განმსაზღვრელ პირებს და სხვა საჯარო უწყებებს სახელმწიფო უსაფრთხოების დაცვის ღონისძიებების განხორციელებაში შეუწყობს ხელს,[9] მანდატი მკაცრად შემოიფარგლება საჯაროდ ხელმისაწვდომ კანონმდებლობასა და სახელმწიფო უსაფრთხოების პოლიტიკის დოკუმენტებში განსაზღვრული ლეგიტიმური ეროვნული უსაფრთხოების ინტერესების დაცვით და მიმართულია იმ ეროვნული უსაფრთხოების რისკების იდენტიფიცირებაზე, რომელზე მუშაობაც სპეციალური სამსახურების კომპეტენციაში შედის.[10]

ამ კუთხით, ეროვნული უსაფრთხოების რისკების განმარტებას მნიშვნელოვანი გავლენა აქვს უსაფრთხოების სამსახურის მანდატის ფარგლებზე. ეროვნული უსაფრთხოების განმარტება და შესაბამისი რისკების იდენტიფიცირება უდავოდ შიდა პროცესია, რა დროსაც ქვეყნის უნიკალური გეოპოლიტიკური და უსაფრთხოების გარემოებები მხედველობაში უნდა იყოს მიღებული. აქედან გამომდინარე, საერთაშორისო დონეზე შეუძლებელია ეროვნული უსაფრთხოების რისკების მკაცრად განსაზღვრული ერთიანი სიის შემუშავება. თუმცა, ევროპული სასამართლოს იურისპრუდენცია, ისევე როგორც ევროპის საბჭოს საპარლამენტო ასამბლეის (PACE) რეკომენდაციები მინიშნებებს იძლევიან, თუ რა შეიძლება და რა არ შეიძლება ჩაითვალოს ეროვნული უსაფრთხოების რისკად.

ბორნი და ლეი (Born and Leigh) ჩამოთვლიან საქმიანობებს, რომლებიც ევროპული სასამართლოს პრაქტიკის შესაბსამისად, ეროვნული უსაფრთხოების რისკებად არის აღიარებული:

- ჯაშუშობა (საქმეზე კლასი და სხვები გერმანიის ფედერალური რესპუბლიკის წინააღმდეგ)[11]

---

8 Venice Commission, *Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session* (2007), (hereinafter Venice Commission, *Democratic Oversight of the Security Services* (2007)) paras 94-97 available from: http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx

9 UN Compilation of Good Practices, Practice 1

10 იქვე, Practice 2

11 http://hudoc.echr.coe.int/eng?i=001-57510 para 48

- ტერორიზმი
- ტერორიზმისკენ მოწოდება/მისი მხარდაჭერა (საქმეზე ზანა თურქეთის წინააღმდეგ) [12]
- საპარლამენტო დემოკრატიის დამხობა (ლეანდერი შვედეთის წინააღმდეგ)[13]
- სეპარატისტული ექსტრემისტული ორგანიზაციები საქმიანობა, რომელიც ქვეყნის მთლიანობასა და უსაფრთხოებას უქმნიან საფრთხეს (თურქეთის გაერთიანებული კომუნისტური პარტია და სხვები თურქეთის წინააღმდეგ)[14]

უნდა აღინიშნოს, რომ ეს სია ამომწურავი არ არის, და სხვა საქმიანობაც, როგორიცაა თავდაცვასთან, საგარეო საქმეებთან და სახელმწიფოს სხვა უმნიშვნელოვანეს ინტერესებთან დაკავშირებულ ელექტრონულ მონაცემებში შეღწევა, ასევე შეიძლება ეროვნული უსაფრთხოების რისკად განიხილებოდეს.[15]

ევროპის საბჭოს საპარლამენტო ასამბლეა, მის პრეცედენტულ რეკომენდაციაში 1402 (1999) „ევროპის საბჭოს წევრი ქვეყნების შიდა სახელმწიფო უსაფრთხოების სამსახურების კონტროლის შესახებ“ აცხადებს: „ეკონომიკური, ან როგორც ასეთი ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის მიზნებზე, არ უნდა გავრცელდეს ეროვნული უსაფრთხოების სამსახურის საქმიანობა. მათ ეკონომიკურ მიზნებსა და ორგანიზებულ დანაშაულზე მხოლოდ იმ შემთხვევაში უნდა იმუშაონ, თუ ისინი რეალურ და იმწუთიერ საფრთხეს უქმნიან ეროვნული უსაფრთხოების ინტერესებს“.[16]

ეს განსაზღვრება ღიაა ინტერპრეტაციისთვის, რადგან არ არსებობს ობიექტური საზომი, რა სახის ეკონომიკური/ორგანიზებული დანაშაული წარმოადგენს რეალურ საფრთხეს ეროვნული უსაფრთხოებისთვის. მაგალითად, ცოტა ხნის წინ მიღებულ გადაწყვეტილებაში (*C.G and others v. Bulgaria*), ევროპულმა სასამართლომ განმარტა, რომ „ნარკოტიკების ტრეფიკინგი“ კონკრეტული საქმის კონტექსტში, ეროვნული უსაფრთხოების რისკად ვერ განიხილებოდა.[17]

აღნიშნულ ნორმატიულ სტანდარტებსა და სასამართლო პრაქტიკასთან შესაბამისობაში, არაერთი სახელმწიფო უსაფრთხოების სამსახურს არ ანიჭებს ორგანიზებული და მაგალითად კორუფციის მსგავსად ეკონომიკურ სარგებელთან დაკავშირებული სხვა დანაშაულის წინააღმდეგ ბრძოლის მანდატს. ევროპის ისეთ განვითარებულ დემოკრატიულ სახელმწიფოებში, როგორიცაა გერმანია და დიდი ბრიტანეთი, ორგანიზებულ დანაშაულთან და კორუფციასთან ბრძოლა პოლიციის ან სპეციალური სამართალდამცავი ორგანოების/დანაყოფების, და არა უსაფრთხოების სამსახურების კომპეტენციაში შედის.

თუმცა, ზოგიერთი ქვეყანა ეროვნული უსაფრთხოების ინტერესში მოიაზრებს „უმნიშვნელოვანესი ეკონომიკური ინტერესების დაცვას“. იმ შემთხვევაში, თუ „უმნიშვნელოვანესი ეკონომიკური ინტერესი“ კანონში სათანადოდ არ არის განსაზღვრული, შეიძლება გაჩნდეს უსაფრთხოების სამსახურის მანდატის ბოროტად გამოყენების რისკი. ამ კუთხით, ვენეციის კომისია განმარტავს, რომ მასობრივი განადგურების იარაღის გავრცელება, გაეროს/ევროკავშირის სანქციების გვერდის ავლა და დიდი ოდენობით ფულის გათეთრება - ის სამი სფეროა, რომელიც აღნიშნული მანდატის ქვეშ შეიძლება

12 http://hudoc.echr.coe.int/eng?i=001-58115, para 49-50
13 http://hudoc.echr.coe.int/eng?i=001-57519 para 59
14 http://hudoc.echr.coe.int/eng?i=001-58128 para 39-41
15 Council of Europe, Experts Report: European Committee on Crime Problems (CDPC), Group of Specialists on Internal Security Services (PC-S-SEC), Addendum IV, Final Activity Report, 40703, para. 3.2.
16 PACE Recommendation 1402, Guidelines A2, available from: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en
17 http://hudoc.echr.coe.int/eng?i=001-86093, paras 40-43

ლეგიტიმურად მოექცეს.[18]

მოცემულ ქვეთავში ყურადღება იყო გამახვილებული უსაფრთხოების სამსახურის მანდატზე ეროვნული უსაფრთხოების რისკებთან მიმართებით. როგორც წესი, სამსახურს ასევე აქვს მინიჭებული უფლებამოსილება განახორციელოს ისეთი საქმიანობა, როგორიცაა სპეციალური შემოწმება, ასევე განსაზღვრული პირების (მაღალი თანამდებობის პირები) და კრიტიკული ინფრასტრუქტურის დაცვა.

1.3. სამართალდამცავი უფლებამოსილებები

ზემოთხსენებული გაეროს სახელმძღვანელო დოკუმენტის თანახმად, უსაფრთხოების სამსახურის მთავარი ფუნქცია უნდა იყოს ეროვნული უსაფრთხოების დაცვის მიზნით ინფორმაციის შეგროვება, ანალიზი და გავრცელება. შესაბამისად, როდესაც უსაფრთხოების სამსახური გამოავლენს ეროვნული უსაფრთხოების რისკს, ისინი შეგროვებულ ინფორმაციას უზიარებენ იმ სახელმწიფო ორგანოებს, რომლებსაც აქვთ მიღებულ ინფორმაციაზე **ზომების მიღების** და **კანონის აღსრულების** უფლებამოსილება, როგორიცაა პოლიცია და სხვა სამართალდამცავი ორგანოები. ამდენად, სახელმწიფო უსაფრთხოების და სამართალდამცავი ორგანოების ინსტიტუციური გაყოფა განიხილება მნიშვნელოვან გარანტიად ერთ ორგანოში ძალაუფლების კონცენტრაციის და ფარული ღონისძიებების შედეგად მოპოვებული ინფორმაციის თვითნებური გამოყენების წინააღმდეგ.[19]

ამ კუთხით, ევროპის საბჭოს საპარლამენტო ასამბლეის რეკომენდაცია 1402 მკაფიოდ განმარტავს, რომ „შიდა უსაფრთხოების სამსახურები არ უნდა იყვნენ უფლებამოსილი განახორციელონ სამართალდამცავი ორგანოების ისეთი ფუნქციები, როგორებიცაა სისხლის სამართლის საქმის გამოძიება, დაკავება ან დაპატიმრება. უფლებამოსილებების ბოროტად გამოყენების მაღალი რისკის და ტრადიციული საპოლიციო საქმიანობის დუბლირების თავიდან ასაცილებლად, ასეთი უფლებამოსილებები ექსკლუზიურად უნდა განეკუთვნებოდეს სხვა სამართალდამცავ ორგანოებს“. [20] ანალოგიურად, სადაზვერვო და სამართალდამცავი უფლებამოსილებების ერთ ორგანოში გაერთიანების წინააღმდეგ ამ მნიშვნელოვან არგუმენტებს, მათ შორის პარალელური სამართალდამცავი სისტემის გაჩენის რისკების გათვალისწინებით, გაეროს საუკეთესო პრაქტიკების მიმოხილვაც აღიარებს.[21]

ამ საერთაშორისო სტანდარტებთან შესაბამისობაში, დემოკრატიული სახელმწიფოების უმრავლესობაში უსაფრთხოების სამსახურების მანდატი შეზღუდულია ინფორმაციის შეგროვებით, გადამუშავებითა გავრცელებით, და მათ სამართალდამცავი უფლებამოსილებები არ აქვთ მინიჭებული.[22] გამონაკლისი შემთხვევებისთვის, როდესაც უსაფრთხოების სამსახურებს აქვთ დაკავების და დაპატიმრების უფლებამოსილება, გაეროს საუკეთესო პრაქტიკების მიმოხილვის სახელმძღვანელო პრაქტიკები 28-30 რამდენიმე მნიშვნელოვან სტანდარტს ადგენს:

► **პრაქტიკა 28**: დაკავების და დაპატიმრების უფლებამოსილება ვრცელდება მხოლოდ იმ

---

18 Venice Commission , *Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session,* CDL-AD (2015) 011, p.20 available from: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e,

19 European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU*- - Volume II: field perspectives and legal update (Luxembourg, 2017) (hereinafter EU FRA, Surveillance by Security Services, (2017) ,p.28 available from http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and/publications,

20 PACE Recommendation 1402, Guidelines B3

21 UN Compilation of Good Practices, Para 41

22 Except, for instance, in cases of close protection and safeguarding critical infrastructure, see Belgium case below.

შემთხვევებზე, როდესაც არსებობს გონივრული ვარაუდი, რომ პირმა ჩაიდინა ან აპირებს ჩაიდინოს კონკრეტული სისხლის სამართლის დანაშაული. ამის გარდა, საუკეთესო პრაქტიკაა ამ ფუნქციის გავრცელება არა სრული მანდატის ფარგლებში, არამედ კონკრეტულ ეროვნული უსაფრთხოების რისკებზე, როგორიცაა ტერორიზმი[23].

- **პრაქტიკა 28:** სპეციალურ სამსახურებს არ აქვთ პირის თავისუფლების აღკვეთის უფლებამოსილება მხოლოდ ინფორმაციის შეგროვების მიზნით.

- **პრაქტიკა 28:** ნებისმიერი უფლებამოსილების, ასევე დაკავებისა და დაპატიმრების გამოყენება სპეციალური სამსახურების მიერ ექვემდებარება იმავე ხარისხის ზედამხედველობას, რომელიც სამართალდამცავი ორგანოების მიერ მათ გამოყენებაზე ვრცელდება, მათ შორის დაკავების კანონიერების სასამართლოს მიერ შემოწმებას.

- **პრაქტიკა 29**: ამ უფლებამოსილებების გამოყენებისას, სპეციალური სამსახურები მოქმედებენ, იმ საერთაშორისო სტანდარტებთან შესაბამისობაში, რომლებიც განსაზღვრულია, მათ შორის ნებისმიერი ფორმის თავისუფლებააღკვეთილი ან დაპატიმრებული პირის დაცვისთვის მოქმედი პრინციპებით, სამართალდამცავი ორგანოების ქცევის კოდექსითა და სამართალდამცავების მიერ ძალის და ცეცხლსასროლი იარაღის გამოყენების ძირითადი წესებით.

- **პრაქტიკა 30**: დაუშვებელია სპეციალურ სამსახურებს მათი თავისუფლების აღკვეთის დაწესებულება ჰქონდეთ ან მესამე პირების მიერ ადმინისტრირებული ისეთი თავისუფლების აღკვეთის დაწესებულება გამოიყენონ, რომელიც ოფიციალურ დაკავების დაწესებულებად არ არის აღიარებული. ეს მნიშვნელოვანი გარანტიაა „ინკომუნიკადო“ პატიმრობის, წამების და არასათანადო მოპყრობის სხვა ფორმების წინააღმდეგ.

1.4 უსაფრთხოების სამსახურის ფარული მეთვალყურეობის ფუნქცია

როგორც წინა ქვეთავში იქნა განხილული, უსაფრთხოების სამსახურებს მათი მანდატის ფარგლებში აქვთ რამდენიმე ფუნქცია მათ შორის ინფორმაციის შეგროვება, ანალიზი, გავრცელება, სპეციალური შემოწმება, კონტრდაზვერვა და კრიტიკული ინფრასტრუქტურის დაცვა. უსაფრთხოების სამსახურის ფუნქციებს შორის, ინფორმაციის შეგროვების ფუნქცია, სავარაუდოდ ყველაზე სადავოა, რადგან შესაძლოა მან მნიშვნელოვანი გავლენა მოახდინოს ძირითადი უფლებების დაცვაზე, განსაკუთრებით პირადი ცხოვრების უფლებაზე. აქედან გამომდინარე, ამ ქვეთავში ყურადღება იქნება გამახვილებული ინფორმაციის შეგროვებაზე და მიმოიხილავს ინფორმაციის შეგროვების სახეებსა და ძირითად შესაბამის საერთაშორისო სტანდარტებს.

ინფორმაციის შეგროვების სახეები

ფარული და ღია მეთოდებით ინფორმაციის მოპოვება: მეთოდებთან მიმართებით, უსაფრთხოების სამსახურის მიერ ინფორმაციის შეგროვება ზოგადად შეიძლება დაიყოს ორ კატეგორიად - ფარული და ღია მეთოდებით ინფორმაციის მოპოვება. ღია მეთოდები მოიცავს ინფორმაციის შეგროვებას საჯაროდ ხელმისაწვდომი წყაროებიდან, მედია საშუალებებიდან, ვებსაიტებიდან, ბლოგებიდან და ა.შ. ამ წყაროებს ასევე უწოდებენ OSINT (ინფორმაცია ღია წყაროდან). ფარული მეთოდები მიმართულია ინფორმაციის მოპოვებაზე პირისგან, რომელმაც არ იცის და არც თანხმობა აქვს გაცემული აღნიშნულზე. ეს მეთოდი მოიცავს მეთოდებს HUMINT (ინფორმაცია პირისგან) როგორიცაა კონფიდენტების გამოყენება ან ღონისძიებები ფარული აგენტების მონაწილეობით; SIGINT

23 UN Compilation of Good Practices, Para 41

(ინფორმაცია სიგნალით), რომელიც გულისხმობს ინფორმაციის შეგროვებას ელექტრონული ან/და ტელეკომუნიკაციის საშუალებებით გადაცემული ინფორმაციის ჩაწერა/მიყურადებით და IMINT (ინფორმაცია გამოსახულებით), რომელიც აგროვებს ინფორმაციას სატელიტის და საჰაერო ფოტოგრაფიის საშუალებით.[24] ამ კატეგორიზაციის მიღმა, სახელმწიფო სამსახურები იყენებენ შედარებით ტრადიციულ მეთოდებსაც, როგორიცაა საფოსტო გზავნილის კონტროლი, ასევე უფრო თანამედროვე მეთოდებს, მათ შორის კომპიუტერული ქსელის ექსპლუატაციას (ჰაკერობა). ამ კონტექსტში, სამიზნის ცოდნის გარეშე განხროციელებული ინფორმაციის შეგროვების ფარული, ინტენსიური ჩარევის ღონისძიებები ზოგადად მოიხსენიება როგორც ფარული მეთვალყურეობა/მიყურადება.[25] ეს ანგარიში ძირითად აქცენტს გააკეთებს ელექტრონული და საკომუნიკაციო საშუალებების ფარულ მიყურადებაზე.

მიზანმიმართული და მასობრივი ფარული მეთვალყურეობა: მასშტაბის მიხედვით, უსაფრთხოების სამსახური ახორციელებს ორი სახის ფარულ მეთვალყურეობას. მიზანმიმართული მიყურადება მიზნად ისახავს იდენტიფიცირებული პირების ან პირთა ჯგუფის მონიტორინგს, რომელთა მიმართ არსებობს ეჭვი სამსახურის მანდატში შემავალი დანაშაულის ჩადენის შესახებ.[26] მეორე მხრივ, როგორც ამას ვენეციის კომისიაც განმარტავს, მასობრივი ფარული მეთვალყურეობა „აუცილებელი არ არის ემყარებოდეს კონკრეტული პირის ან პირების მიმართ ეჭვს; უფრო მეტიც, ის პროაქტიულია და მიზნად ისახავს პოტენციური საფრთხეების იდენტიფიცირებას“.[27] არ არსებობს ერთიანი მიდგომა „მასობრივი მეთვალყურეობის“ ტერმინთან მიმართებით: გაერო, ევროკავშირი, და ევროსაბჭოს ორგანოები სხვადასხვა ტერმინებს იყენებენ, მათ შორის „ფართო მეთვალყურეობა“, „სტრატეგიული მეთვალყურეობა“, „მოცულობითი წვდომა კომუნიკაციებზე“, თითოეული ოდნავ განსხვავებული განმარტებითა და აქცენტებით.[28] თუმცა, ამ ანგარიშში გამოყენებული იქნება მასობრივი მეთვალყურეობა, გარდა იმ შემთხვევისა, როდესაც ეროვნული კანონმდებლობა კონკრეტულად უთითებს სხვა ტერმინზე.

საუკეთესო პრაქტიკაა ამ ორი ტიპის ფარული მეთვალყურეობის კანონით დარეგულირება. ევროკავშირის ადამიანის ძირითადი უფლებების სააგენტოს (EU FRA) მიმოხილვამ გამოავლინა, რომ ევროკავშირის ყველა წევრ სახელმწიფოში, გარდა კვიპროსისა, უსაფრთხოების და დაზვერვის სამსახურების მიერ მიზანმიმართული ფარული მეთვალყურეობის ღონისძიებები კოდიფიცირებულია. წევრი სახელმწიფოების უმრავლესობის სამართლებრივი ჩარჩო, როგორც ასეთი, მასობრივი მეთვალყურეობის მკაფიო რეგულირებას არ ახდენს. თუმცა, ახალ ტენდენციას წარმოადგენს უსაფრთხოების/დაზვერვის სამსახურების მიერ მასობრივი ფარული მეთვალყურეობის განხორციელების კანონმდებლობით დარეგულირების საუკეთესო პრაქტიკა.[29] გერმანია, საფრანგეთი, დიდი ბრიტანეთი, შვედეთი მათი ახლად მიღებული კანონმდებლობით, რომელიც მასობრივ ფარულ მეთვალყურეობას ეხება, ამ სფეროში პირველები არიან.

ქვეყნის ფარგლებში და ფარგლებს გარეთ ფარული მეთვალყურეობა: უსაფრთხოების სამსახურის მიერ ფარული მეთვალყურეობა შეიძლება განსხვავდებოდეს გეოგრაფიული არეალით, რომელსაც ის ფარავს. საუკეთესო პრაქტიკაა, როგორც ქვეყნის ფარგლებში ისე მის გარეთ განხორციელებული

---

24 Lauren Hutton, ‘Tool 5: Overseeing Information Collection’ p.90 in Born and Wills, *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012).

25 UNODC, ‘Current practices in electronic surveillance in the investigation of serious and organized crime’ (New York, 2009) available from: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf;

26 EU FRA, Surveillance by Intelligence Services, (2015), p.20

27 Venice Commission, Report on the Democratic Oversight of Signals Intelligence Agencies (2015), paras 38-46.

28 For a detailed overview of which term is used by which institution, see EU FRA, Surveillance by Intelligence Services, (2015), p.16

29 Ibid, p.17

მეთვალყურეობის კანონით რეგულირება ადამიანის უფლებების დარღვევის თავიდან ასაცილებლად საჭირო დაცვის მექანიზმებით; თუმცა, პრაქტიკაში სახელმწიფოები უფრო მკაცრ რეგულირებას და მაღალ სტანდარტს აწესებენ ქვეყნის შიგნით ფარული მეთვალყურეობის ღონისძიებებზე. ეს იმიტომ, რომ აღმასრულებელი ხელისუფლების მიერ დემოკრატიული წყობის საზიანოდ ქვეყნის შიგნით ფარული მეთვალყურეობის პოლიტიკური მიზნებისთვის გამოყენების უფრო დიდი რისკი არსებობს.[30] თუმცა, ეს მიდგომა გაკრიტიკებულია ექსპერტთა წრეებში გერმანიაში, იმ არგუმენტზე დაყრდნობით, რომ პირადი ცხოვრების უფლება, როგორც ის გერმანიის ძირითად კანონში არის აღიარებული (Grundgesetz) უნივერსალურია, და აქედან გამომდინარე, მოქალაქეობა ან წარმოშობის ქვეყანა არ უნდა იყოს გადამწყვეტი უცხოელი ინფორმაციის წყაროს მიმართ უფლებების იმაზე მეტად შესაზღუდად, ვიდრე ეს გერმანიის მოქალაქეებისა და გერმანიაში კანონიერი რეზიდენტების შემთხვევაში ხდება.[31]

შინაარსობრივი ინფორმაცია და მეტადატა: ბოლოს, ფარული მეთვალყურეობა შეიძლება ორ კატეგორიად გაიყოს, იმის მიხედვით, კომუნიკაციიდან რა სახის ინფორმაციის მოპოვება ხდება. უსაფრთხოების სამსახურს წვდომა აქვს ან უშუალოდ კომუნიკაციის შინაარსზე ან მეტადატაზე - ინფორმაციაზე კომუნიკაციის შესახებ, რომელიც მათ შორის მოიცავს ადგილმდებარეობას, საიდანაც კომუნიკაცია ხორციელდება; მოწყობილობას, რომელიც გზავნის ან ახორციელებს კომუნიკაციას; კომუნიკაციის დროს; კომუნიკაციის მიმღებ პირს, მის ადგილმდებარეობას და გამოყენებულ მოწყობილობას, გზავნილის/კომუნიკაციის მიღების დროს; გამგზავნთან და მიმღებთან დაკავშირებულ ინფორმაციას, მაგალითად ელექტრონული ფოსტას, ინფორმაციას სამისამართო/სატელეფონო ცნობარიდან, ელექტრონული ფოსტის მომწოდებელს, ინტერნეტ მომსახურების მომწოდებელს (ISPs) და IP მისამართს.[32] ტრადიციულად, ზედამხედველობა შედარებით სუსტი მექანიზმებით ხორციელდებოდა მეტადატას შეგროვებასა და გამოყენებაზე, იმ საფუძვლით, რომ ის არ შეიცავს შინაარსობრივ ინფორმაციას კომუნიკაციის შესახებ და მისი შეგროვება ხდება ავტომატური, კომპიუტერული სისტემების საშუალებით, რომელიც მიყურადებისგან განსხვავებით ადამიანის პირადი ცხოვრების უფლებაში ნაკლები ინტენსივობის ჩარევას წარმოადგენს. თუმცა, არსებული ტექნოლოგიით მეტადატას კომბინირებით და გაანალიზებით შესაძლებელია პირის კომპლექსური პროფილის შექმნა, მათ შორის სად იმყოფება სხვადასხვა დროს, ვისთან საუბრობს, რამდენი ხნით, ქცევის მახასიათებლები, შეხედულებები, კომუნიკაციები და საზოგადოებრივი ასოციაციები.[33]

ბოლო პერიოდში იკვეთება სტანდარტი უსაფრთხოების სამსახურის მიერ მეტადატის შეგროვების უფრო მკაცრად რეგულირების შესახებ. ამასთან კავშირში, ევროკავშირის მართლმსაჯულების სასამართლომ გააუქმა ევროკავშირის მონაცემების შენახვის შესახებ დირექტივა (EU Data Retention Directive) იმ საფუძვლით, რომ ის განსაკუთრებით ინტენსიურად ერევა ძირითად უფლებებში პირადი ცხოვრების უფლების და პერსონალური მონაცემების დაცვის კუთხით.“[34] ცოტა ხნის წინ გერმანიის სასამართლომაც მიიღო გადაწყვეტილება, რომლის თანახმად გერმანიის საგარეო დაზვერვის სააგენტომ (BND) სპეციალური სამსახურების მიერ დასამუშავებლად არ უნდა შეინახოს საერთაშორისო ზარების ისეთი მეტადატა, როგორიცაა ტელეფონის ნომრები.[35]

---

30 EU FRA, Surveillance by Intelligence Services Vol.2, (2017), p.91

31 See the discusssion in Thorsten Wetzling, ‘Germany’s Intelligence Reform: More surveillance, modest restraints and inefficient controls’ SNV Policy Brief (2017), p.6 available from: https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency/publikationen,

32 Privacy International, *Explainers : What is Metadata*, available from: https://www.privacyinternational.org/node/53

33 იქვე

34 იხ.: Court of Justice of the European Union, *The Court of Justice declares the Data Retention Directive to be invalid*, Judgment in Joined Cases C-293/12 and C-594/12, Press Release No 54/14, (Luxembourg, 8 April 2014), available from: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

35 https://www.reuters.com/article/us-germany-surveillance/german-court-rules-against-foreign-intelligence-mass-communication-surveillance-idUSKBN1E82RS?feedType=RSS&feedName=technologyNews

მნიშვნელოვანი საერთაშორისო სტანდარტები ფარული მეთვალყურეობის რეგულირების შესახებ

წინა ქვეთავი მიმოიხილავდა უსაფრთხოების სამსახურების მიერ განხორციელებული ფარული მეთვალყურეობის მეთოდებს, სახეებს და ფარგლებს, რამდენიმე ბოლო პერიოდის ტენდენციებთან ერთად. თუ არ მოხდება ფარული მეთვალყურეობის ეფექტიანი რეგულირება, კონტროლი და ზედამხედველობა, იარსებებს ფარული მეთვალყურეობის უფლებამოსილებების და შეგროვებული ინფორმაციის ბოროტად გამოყენების მაღალი რისკი. ამ კუთხით, კონვენციის მე-8 მუხლთან (პირადი ცხოვრების უფლება) დაკავშირებით ევროპული სასამართლოს პრაქტიკისა და გაეროს საუკეთესო პრაქტიკების მიმოხილვის თანახმად, ფარული მეთვალყურეობის შესახებ საკანონმდებლო რეგულირებებთან მიმართებით ჩამოყალიბებულია შემდეგი სტანდარტები:

- **კანონიერება:** ყველაზე ფუნდამენტური სტანდარტია ნებისმიერი ფორმით ფარული მეთვალყურეობის უფლებამოსილების საჯაროდ ხელმისაწვდომ კანონმდებლობაში განსაზღვრა. ეროვნული კანონმდებლობა ფარულ მეთვალყურეობაზე არ შეიძლება ეწინააღმდეგებოდეს საერთაშორისო სამართლსა და ადამიანის უფლებების სტანდარტებს.

- **აუცილებლობა და თანაზომიერება:** უსაფრთხოების სამსახურების ფარული მეთვალყურეობის უფლებამოსილების კანონმდებლობით განსაზღვრა თავისთავად არ გულისხმობს მისი გამოყენების მიზანშეწონილობას ნებისმიერ შემთხვევაში. საკანონმდებლო ნორმები უნდა შეესაბამებოდეს აუცილებლობისა და პროპორციულობის პრინციპებს, და აქედან გამომდინარე, ფარული მეთვალყურეობის ღონისძიების გამოყენება დაშვებული უნდა იყოს მხოლოდ ისეთი შემთხვევებისთვის, როდესაც ეს აბსოლუტურად აუცილებელია რისკების აღმოსაფხვრელად, ასევე თავად ჩარევის ინტენსივობა უნდა იყოს სავარაუდო საფრთხის პროპორციული.[36]

- **სპეციფიკური საკანონმდებლო დაცვის მექანიზმები:** გაეროს საუკეთესო პრაქტიკების მიმოხილვა ჩამოთვლის კონკრეტულ დაცვის მექანიზმებს ფარული მეთვალყურეობის კანონმდებლობისთვის, რომ ის შეესაბამებოდეს აუცილებლობის და პროპორციულობის პრინციპებს. პრაქტიკა 21-ს თანახმად, ეროვნული კანონმდებლობის საუკეთესო მაგალითები განსაზღვრავენ:

  - ინფორმაციის შეგროვების ღონისძიებების სახეებს, რომელთა განხორციელების უფლებამოსილებაც აქვთ სპეციალურ სამსახურებს;

  - ინფორმაციის შეგროვების დასაშვებ მიზნებს *(ევროპული სასამართლოს მიერ განხილული ერთ-ერთი უმნიშვნელოვანესი კრიტერიუმია. სასამართლო აფასებს, ფარული მეთვალყურეობის ღონისძიება ემსახურება ლეგიტიმური მიზნის მიღწევას, და არის თუ არა ის აუცილებელი დემოკრატიულ სახელმწიფოში ამ მიზნის მისაღწევად)*[37]*;*

  - პირთა და საქმიანობის კატეგორიებიც, რომლებიც შესაძლოა დაექვემდებარონ ოპერატიულ ღონისძიებებს;

  - ინფორმაციის შეგროვების ღონისძიებების გამოყენებისთვის აუცილებელი ვარაუდის სტანდარტი;

  - შეზღუდული ვადები ასეთი ღონისძიებების გამოყენებისთვის.

- **დაცული პროფესიები:** გაეროს სახელმძღვანელო დოკუმენტის თანახმად, საუკეთესო პრაქტიკაა

---

36 Lauren Hutton, 'Overseeing Information Collection', Tool 5, p. 100, in Born and Wills, *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012)., Also see UN Compilation of Good Practices, paras 27-30

37 See EU fra, *Surveillance by Intelligence Services Vol 2.*2017, p.37

გარკვეული პროფესიის წარმომადგენლების, განსაკუთრებით იურისტებისა და ჟურნალისტების მიმართ ფარული მეთვალყურეობის ღონისძიების გამოყენებაზე შეზღუდვების დაწესება. დამცველისა და კლიენტის კომუნიკაციის კონფიდენციალურობის, ისევე როგორც ჟურნალისტების მეირ წყაროს დაცვის ინტერესები უმნიშვნელოვანესია ძირითადი უფლებების განხორციელებისთვის (უფლება სამართლიან სასამართლოზე), ისევე როგორც თავისუფალი საზოგადოებისთვის.[38]

- **კონტროლი, ნებართვის გაცემა და ზედამხედველობა:** სამართლებრივი დაცვის მექანიზმები თავისთავად არ არის საკმარისი ფარული მეთვალყურეობის უფლებამოსილების სათანადო განხორციელების უზრუნველსაყოფად. გაეროს საუკეთესო პრაქტიკების მიმოხილვის პრაქტიკა 22 განმარტავს:
  - „ინფორმაციის შეგროვების ღონისძიებები, რომლებიც მნიშვნელოვან შეზღუდვებს აწესებენ ადამიანის უფლებებზე ნებადართულია და ზედამხედველობას ექვემდებარება როგორც მინიმუმ ერთი გარე, სპეციალური სამსახურებისგან დამოუკიდებელი ინსტიტუციის მიერ. ამ ინსტიტუციას შეუძლია ღონისძიების გადახედვაზე, შეჩერებასა და შეწყვეტაზე მითითების მიცემა. ინფორმაციის შეგროვების ღონისძიებები, რომლებიც მნიშვნელოვან შეზღუდვებს აწესებენ ადამიანის უფლებებზე, ექვემდებარებიან რამდენიმე საფეხურიან ნებართვის გაცემის პროცედურებს, რომელიც მოიცავს სპეციალური სამსახურების შიგნით, აღმასრულებელი ხელისუფლებისგან და ორივე მათგანისგან დამოუკიდებელი ორგანოს თანხმობის მიღებას.“

გაეროს ამ სტანდარტთან შესაბამისობაში, ფარული მეთვალყურეობის ღონისძიებები უმრავლესობა დემოკრატიულ სახელმწიფოებში ექვემდებარება კონტროლის, ნებართვის გაცემის და ზედამხედველობის პროცედურებს რამდენიმე აქტორის ჩართულობით. რელევანტური საერთაშორისო სტანდარტები და ქვეყნების საუკეთესო პრაქტიკები მიმოხილული იქნება ამ ანგარიშის შემდეგ თავებში:

- ფარული მეთვალყურეობის აღმასრულებელი კონტროლი მე-2 თავში;
- მეთვალყურეობის ღონისძიებების სასამართლო და კვაზი-სასამართლო წინასწარი კონტროლი 3.3 თავში;
- საპარლამენტო კომიტეტების და სპეციალიზებული ზედამხედველობის ორგანოების მიერ ღონისძიების განხორციელებაზე განგრძობადი და შემდგომი ზედამხედველობა შესაბამისად თავებში 3.1 და 3.2;
- სამოქალაქო საზოგადოების როლი ფარულ მეთვალყურეობასთან დაკავშირებული პოლიტიკის მონიტორინგში, ასევე მეთვალყურეობის მარეგულირებელ კანონმდებლობასთან კავშირში სტრატეგიული საქმეების წარმოება 3.4 თავში;
- ინდივიდუალური პირების წვდომა უსაფრთხოების სამსახურში მათ შესახებ არსებულ პირად ინფორმაციაზე განხილულია მე-4 თავში, აქედან გამომდინარე ეს საკითხები ამ ქვეთავში აღარ იქნება განმეორებული.

ფარული ღონისძიებების შესახებ საერთაშორისო სტანდარტები ცხადია არ შემოიფარგლება ამ ქვეთავში მიმოხილული სტანდარტებით. თუმცა, უფრო დეტალური სამართლებრივი მიმოხილვა გასცდებოდა ამ ანგარიშის მიზნებს. სახელმწიფოები აწყდებიან წინააღმდეგობებს ფარულ მეთვალყურეობაზე რეგულირებების მიღებისას, რადგან რთულია მონაცემების შეგროვების კუთხით ტექნოლოგიურ პროგრესსა და შესაძლებლობებს დაეწიო. ქვემოთ წარმოდგენილი მიმოხილვა ქვეყნების მიხედვით მიზნად არ ისახავს სრულყოფილ სამართლებრივ ანალიზს, ის მხოლოდ მოკლედ მიმოიხილავს ძირითად დაცვის გარანტიებს.

38 UN Compilation of Good Practices, Para 20 and 34

შერჩეული ქვეყნების საუკეთესო პრაქტიკები:

ხორვატია

სტრუქტურა: ხორვატიაში ფუნქციონირებს ორი უსაფრთხოების/დაზვერვის სამსახური, ერთი სამხედრო (სამხედრო უსაფრთხოების სპეციალური სამსახური/Vojna sigurnosno- obavještajna agencija -VSOA) და ერთი სამოქალაქო (სახელმწიფო უსაფრთხოების სამსახური Sigurnosno-obavještajna agencija -SOA). ეს ქვეთავი შეეხება ამ უკანასკნელს. SOA სარგებლობს შიდა და საგარეო მანდატით. იერარქიული წყობის და ქვემდებარეობის შესახებ იხილეთ მე-2 თავი უსაფრთხოების სამსახურების აღმასრულებელი კონტროლის შესახებ.

მანდატი: სახელმწიფო უსაფრთხოების სამსახურების სადაზვერვო საქმიანობის შესახებ კანონის 23-ე მუხლი[39] (შემდგომში კანონი), განსაზღვრავს სამსახურის (SOA) მანდატს შემდეგნაირად: SOA აგროვებს, აანალიზებს, ამუშავებს და აფასებს პოლიტიკურ, ეკონომიკურ, მეცნიერულ/ტექნოლოგიურ და უსაფრთხოებასთან დაკავშირებულ ინფორმაციას, რომელიც ეხება სხვა სახელმწიფოებს, უცხოურ ორგანიზაციებს, პოლიტიკურ და ეკონომიკურ ალიანსებს, ჯგუფებს და პირებს, განსაკუთრებით მათ, ვინც ავლენენ განზრახვას, პოტენციას, შეიმჩნევიან დაფარულ გეგმებსა და საიდუმლო საქმიანობაში ეროვნული უსაფრთხოების ინტერესების წინააღმდეგ, ან სხვა ინფორმაციას, რომელიც დაკავშირებულია ხორვატიის რესპუბლიკის ეროვნულ უსაფრთხოებასთან.

საუკეთესო პრაქტიკის მაგალითად, კანონი პირდაპირ ჩამოთვლის ეროვნული უსაფრთხოების შემდეგ რისკებს:

- ტერორისტული აქტები და ძალადობის სხვა ფორმები;
- სხვა ქვეყნების სპეციალური სამსახურების, უცხოური ორგანიზაციების და პირების სადაზვერვო საქმიანობა;
- ჯგუფების და პირების ექსტრემისტული საქმიანობა;
- მაღალი თანამდებობის პირებისთვის, დაცული დაწესებულებებისა და ლოკაციებისთვის საფთხის შექმნა;
- ორგანიზებული და ეკონომიკური დანაშაული;
- სპეციალურ სამსახურებში დაცულ ინფორმაციაზე და საკომუნიკაციო სისტემებზე უნებართვო წვდომა;
- თანამდებობის პირების, საჯარო მოხელეების, სამეცნიერო დაწესებულებების და საჯაროსამართლებრივი უფლებამოსილების განმახორციელებელი იურიდიული პირების მიერ საიდუმლო ინფორმაციის გასაჯაროება, და სხვა საქმიანობა ეროვნული უსაფრთხოების წინააღმდეგ;

ევროპის საბჭოს საპარლამენტო ასამბლეის (PACE) რეკომენდაცია 1402 თანახმად, ორგანიზებული დანაშაული შედის ეროვნული უსაფრთხოების რისკებში და შესაბამისად, ხორვატიის სახელმწიფო უსაფრთხოების სამსახურის (SOA) მანდატში. თუმცა, უნდა აღინიშნოს, რომ საერთაშორისო სტანდარტის

39 See https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

შესაბამისად, სამსახურის მანდატი შეზღუდულია მონაცემების შეგროვებით, ანალიზით და დამუშავებით, შესაბამისად მას არ აქვს საგამოძიებო ფუნქციები. ხორვატიის სახელმწიფო უსაფრთხოების სამსახური ვალდებულია ორგანიზებულ დანაშაულთან დაკავშირებული ინფორმაცია გაუზიაროს პოლიციის და პროკურატურის ორგანოებს, რომელთაც ამ დანაშაულის გამოძიება ევალებათ.

სამართალდამცავი ფუნქციები: რადგან ხორვატიის უსაფრთხოების სამსახურს არ აქვს სამართალდამცავი ფუნქციები, მას არ აქვს მინიჭებული გამოძიების, დაკავების და დაპატიმრების უფლებამოსილებები. კანონის 27-ე მუხლი ადგენს, რომ სამსახურის თანამშრომლებს შეუძლიათ პირების გამოკითხვა, პირის წინასწარ გამოხატული თანხმობით, მხოლოდ სამსახურის ოფიციალურ ადმინისტრაციულ შენობაში, რაზეც უნდა შედგეს გამოკითხვის ოქმი, რომელიც სასამართლოს და ზედამხედველობის ორგანოს გადაეცემა. იმ შემთხვევაში, თუ პირი არ იძლევა თანხმობას ასეთ გასაუბრებაზე, ხორვატიის უსაფრთხოების სამსახური ვალდებულია პოლიციას დაავალოს მისი გამოკითხვა, თუ არსებობს ვარაუდი, რომ პირი ფლობს ინფორმაციას ეროვნული უსაფრთხოების რისკების შესახებ. ხორვატიის კანონმდებლობა, რომელიც მკაფიო წესებს ადგენს უსაფრთხოების სამსახურისა და სამართალდამცავი ორგანოების თანამშრომლობისთვის, ნამდვილად არის საუკეთესო პრაქტიკის მაგალითი.

კანონი არ ეხება ძალის გამოყენებას უსაფრთხოების სამსახურის მიერ. თუმცა, საჯაროდ ხელმისაწვდომი ბრძანება[40] განმარტავს, რომ უსაფრთხოების სამსახურის იმ თანამშრომლებს, რომლებსაც აქვთ ცეცხლსასროლი იარაღის ტარების ნებართვა, აქვთ მათი გამოყენების უფლებამოსილება მხოლოდ გამონაკლის შემთხვევებში, მათი ან სხვა პირის სიცოცხლის დასაცავად, ასევე კონტრდაზვერვითი მანდატის ფარგლებში სახელმწიფო ორგანოების (მათ შორის სახელმწიფო უსაფრთხოების სამსახური), დაცული პირების ან კრიტიკული ინფრასტრუქტურის დასაცავად.

ფარული მეთვალყურეობის ღონისძიებები და ძირითადი დაცვის გარანტიები: ხორვატიის კანონმდებლობა მხოლოდ მიზანმიმართულ ფარულ მეთვალყურეობას ცნობს. კანონის მუხლები 33-37 ეხება მიზანმიმართული ფარული მეთვალყურეობის რეგულირებას, და პირდაპირ ჩამოთვლის ინფორმაციის მოპოვების ფარულ ღონისძიებებს, კანონიერების პრინციპთან შესაბამისობაში. ღონისძიებები მოიცავს ტელეკომუნიკაციის ფარულ მეთვალყურეობას, საფოსტო გზავნილი კონტროლს, ფიზიკურ მეთვალყურეობას (ფარული მეთვალყურეობისთვის მოწყობილობის დაყენება), საჯარო სივრცეში აუდიო/ვიდეო საშუალებებით გამოსახულების და კომუნიკაციის შინაარსის მეთვალყურეობას (მუხლი 33). კანონი უშვებს, როგორც შინაარსობრივი ინფორმაციის, ისე მეტადატის მოპოვებას, მაგრამ მათ განსხვავებული წინასწარი კონტროლის მექანიზმებს უსადაგებს, ასევე აკონკრეტებს ღონისძიების ხანგრძლივობის ვადას (მეტი დეტალისთვის, იხილეთ თავი 3.3. სასამართლო ზედამხედველობის შესახებ). საუკეთესო პრაქტიკის მაგალითია, კანონის მიერ აუცილებლობის და პროპორციულობის პრინციპების მკაფიო რეგლამენტირება, შემდეგი განმარტებით, რომ ფარული მეთვალყურეობის ღონისძიებები „შეიძლება გამოყენებული იყოს იმ შემთხვევაში თუ ინფორმაცია ვერ იქნება მოპოვებული სხვა ფორმით ან მისი სხვა სახით მოპოვება არაპროპორციულ სიძნელეებთან არის დაკავშირებული. იმ შემთხვევებში, როდესაც ინფორმაციის მოპოვების სხვადასხვა ღონისძიებას შორის არჩევანის შესაძლებლობა არსებობს, გამოყენებული უნდა იყოს კონსტიტუციით აღიარებულ უფლებებში და თავისუფლებებში ჩარევის შედარებით ნაკლებად ინტენსიური საშუალება (მუხლი 33). კანონი არ ითვალისწინებს ჟურნალისტების და ადვოკატების დაცვისთვის განსაკუთრებულ რეჟიმს

40 https://www.soa.hr/UserFiles/File/Decree_bear_and_use_firearms.pdf

სტრუქტურა: კანადას აქვს ერთი სამოქალაქო უსაფრთხოების/დაზვერვის სამსახური (კანადის უსაფრთხოების სადაზვერვო სამსახური CSIS) და ერთი სამხედრო სადაზვერვო სამსახური (კანადის შეირაღებული ძალების სადაზვერვო დანაყოფი). დამატებით, თავდაცვითი კომპეტენციით, კანადაში ჩამოყალიბებულია კომუნიკაციების უსაფრთხოების დაწესებულება, რომლის მანდატში შედის საგარეო სადაზვერვო საქმიანობის განხორციელება. ეს ქვეთავი ყურადღებას გაამახვილებს სამოქალაქო უსაფრთხოების სამსახურზე CSIS-ზე. CSIS სარგებლობს როგორც შიდა ისე საგარეო მანდატით. შესაბამისად, მას აქვს ინფორმაციის ქვეყნის ფარგლებს გარეთ მოპოვების შესაძლებლობა. კანადის უსაფრთხოების სადაზვერვო საქმიანობის შესახებ კანონის (შემდგომში კანონი) 12 (2) მუხლი[41], როგორც საუკეთესო პრაქტიკის მაგალითი, პირდაპირ უთითებს, რომ სამსახურს შეუძლია მისი ფუნქციების განხორციელება როგორც ქვეყნის ფარგლებში ისე მის გარეთ.

CSIS - ის იერარქიული წყობის და ქვემდებარეობის შესახებ იხილეთ მე-2 თავი უსაფრთხოების სამსახურების აღმასრულებელი კონტროლის შესახებ.

მანდატი: როგორც კანონით არის განსაზღვრული CSIS - ს აქვს მანდატი

შეაგროვოს, მოკვლევით ან სხვა ფორმით, მკაცრი აუცილებლობის პირობებში, და გაანალიზოს, შეინახოს ეს ინფორმაცია იმ საქმიანობასთან მიმართებით, რომელიც გონივრული ვარაუდის სტანდარტით შეიძლება კანადის უსაფრთხოებისთვის რისკს წარმოადგენდეს. ამასთან კავშირში, სამსახურმა უნდა მიაწოდოს ინფორმაცია და წარუდგინოს რეკომენდაციები კანადის მთავრობას (მუხლი 12(1)). საერთაშორისო სტანდარტებთან შესაბამისობაში, კანონის მეორე თავი დეტალურად ჩამოთვლის რა იგულისხმება კანადის უსაფრთხოების რისკების ქვეშ:

(ა) ჯაშუშობა ან საბოტაჟი კანადის წინააღმდეგ ან კანადის სახელმწიფო ინტერესების საზიანოდ ან საქმიანობა მიმართული ასეთი ჯაშუშობის ან საბოტაჟის მხარდასაჭერად;

(ბ) საქმიანობა უცხოური ზეგავლენით კანადაში ან კანადასთან კავშირში, რომლებიც საზიანოა კანადის სახელმწიფო ინტერესებისთვის და ფარულია, შეცდომაში შეყვანას ემსახურება ან შეიცავს საფრთხეს ნებისმიერი პირისთვის;

(c) ადამიანის ან ქონების წინააღმდეგ საფრთხის ან სერიოზული ძალადობის აქტების მხარდამჭერი საქმიანობა კანადაში ან კანადასთან კავშირში პოლიტიკური, რელიგიური ან იდეოლოგიური მიზნების მისაღწევად კანადაში ან სხვა სახელმწიფოში;

d) ფარული უკანონო მოქმედებით, კანადის კონსტიტუციური წყობის დასუსტებისკენ, ან ძალადობრივი საშუალებებით მისი დამხობისკენ ან გადატრიალებისკენ მიმართული ან ამ განზრახვით განხორციელებული საქმიანობა;

მნიშვნელოვანია აღინიშნოს, რომ არც ორგანიზებული/ეკონომიკური დანაშაული, არც კორუფცია არ გვხვდება ეროვნული უსაფრთხოების რისკების ჩამონათვალში და შესაბამისად გამორიცხულია CSIS - ის მანდატიდან.

სამართალდამცავი უფლებამოსილებები: კანონი წარმოადგენს საუკეთესო პრაქტიკის მაგალითს, სამსახურის მანდატიდან სამართალდამცავი უფლებამოსილებების მკაფიო ამორიცხვის

41 Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23) available from: http://laws-lois.justice.gc.ca/eng/acts/c-23/index.html

თვალსაზრისით. კანონის მუხლი 12.1(1) განსაზღვრავს სამსახურის ფუნქციებს შემდეგნაირად: „თუ არსებობს გონივრული ეჭვი იმის შესახებ, რომ რომელიმე საქმიანობა კანადის უსაფრთხოებისთვის რისკს წარმოადგენს, სამსახურმა შესაძლოა მიიღოს ზომები, კანადის ფარგლებში ან მის გარეთ, საფრთხის შესამცირებლად.“ აქვე დაკონკრეტებულია: „მეტი სიცხადისთვის, ქვეპარაგრაფი 1-ის არცერთი დანაწესი არ ანიჭებს სამსახურს სამართალდამცავ კომპეტენციებს“. საპოლიციო უფლებამოსილებების მკაფიო აკრძალვის გარდა, მუხლი 12.2(1) დამატებით დაუშვებლად მიიჩნევს შემდეგ საქმიანობას:

სამსახურმა არ შეიძლება:

(a) განზრახ ან გაუფრთხილებლობით გამოიწვიოს პირის სიცოცხლის მოსპობა ან ფიზიკური დაზიანება;

(b) განზრახი მცდელობით დააბრკოლოს, ხელი შეუშალოს სამართლის აღსრულებას;

(c) დაარღვიოს პირის სექსუალური ხელშეუხებლობა.

კანონის ასეთი მკაფიო დებულებები წარმოადგენს მნიშვნელოვან დაცვის მექანიზმს წამების, არასათანადო მოპყრობის და ინკომუნიკადო პატიმრობის წინააღმდეგ.

ფარული მეთვალყურეობის ღონისძიებები და დაცვის გარანტიები: კანონიერების პრინციპთან შესაბამისობაში, კანონის მუხლები 21-28, არეგულირებს CSIS - ის მიერ განხორციელებულ მიზანმიმართულ ფარულ მეთვალყურეობას. კანონი ჩამოთვლის ღონისძიებებს, რომელთა განხორციელების უფლებამოსილებაც გააჩნიათ CSIS - ის მოხელეებს, კერძოდ „ნებისმიერი კომუნიკაციის მიყურადება ან ნებისმიერი ინფორმაციის, ჩანაწერის, დოკუმენტის ან საგნის მოპოვება, და ამ მიზნით (ა) ნებისმიერ ადგილას შესვლა ან ნებისმიერი საგნის გახსნა ან მასზე წვდომის მოპოვება; (ბ) ინფორმაციის, ჩანაწერის, დოკუმენტის ან საგნის მოძებნა, ამოღება ან დაბრუნება, ან შემოწმება, ნიმუშის აღება ან ასლის გაკეთება, ან ნებისმიერი სხვა ფორმით ჩაწერა; ან (გ) ნებისმიერი საგნის დამონტაჟება, შენარჩუნება, ან ამოღება (მუხლი. 21(3)). საერთაშორისო სტანდარტებთან შესაბამისობაში, კანონი ავალდებულებს, რომ CSIS - მ ნებართვის მისაღებად წარდგენილ შუამდგომლობაში ნებისმიერი ღონისძიების აუცილებლობა (21(2)ბ), და მიზანშეწონილობა & თანაზომიერება (21.1(2)c) ამტკიცოს. მნიშვნელოვანია აღინიშნოს, რომ კანონი ადგენს განსხვავებულ კრიტერიუმებს ფარული მეთვალყურეობის ღონისძიების საშუალებით „საფრთხის გამოსაკვლევად“ და „კანადისთვის შექმნილი საფრთხის შესამცირებლად“. (ფარული მეთვალყურეობის ღონისძიებაზე ნებართვის გაცემაზე უფრო დეტალური ინფორმაციისთვის იხილეთ თავი 3.3. სასამართლო ზედამხედველობაზე). კანონში არ არის გათვალისწინებული სპეციალური დაცვის გარანტიები ჟურნალისტებისა და იურისტებისთვის.

სტრუქტურა: ბელგიაში ფუნქციონირებს ორი უსაფრთხოების/დაზვერვის სამსახური: შეირაღებული ძალების ზოგადი დაზვერვის და უსაფრთხოების სამსახური (GISS), რომელიც წარმოადგენს სამხედრო სადაზვერვო სააგენტოს; და სახელმწიფო უსაფრთხოების სამსახური (Sûreté de l'État), რომელიც წარმოადგენს სამოქალაქო უსაფრთხოების/სადაზვერვო სამსახურს (შემდგომში სამსახური) როგორც შიდა ისე საგარეო მანდატით. ეს თავი ყურადღებას გაამახვილებს ამ უკანასკნელ სამსახურზე. სამსახურის იერარქიული წყობის და ქვემდებარეობის შესახებ იხილეთ მე-2 თავი უსაფრთხოების სამსახურების აღმასრულებელი კონტროლის შესახებ.

მანდატი: დაზვერვის და უსაფრთხოების სამსახურის შესახებ ორგანული კანონი[42] (შემდგომში კანონი), არეგულირებს სამსახურის მანდატს, უფლებამოსილებებს, და ფუნქციებს. კანონის მე-7 მუხლი განსაზღვრავს სამსახურის მანდატს შემდეგნაირად:

- ინფორმაციის მოკვლევა, ანალიზი და დამუშავება ყველა იმ საქმიანობის შესახებ, რომელიც ემუქრება სახელმწიფოს შიდა უსაფრთხოებას ან შეიძლება დაემუქროს მას, ასევე დემოკრატიული და კონსტიტუციური წყობის შენარჩუნებას, სახელმწიფოს საგარეო უსაფრთხოებას და საერთაშორისო ურთიერთობებს, მეცნიერულ ან ეკონომიკურ პოტენციალს როგორც ეს განსაზღვრულია ეროვნული უსაფრთხოების საბჭოს მიერ, ან მეფის მიერ განსაზღვრულ ყველა სხვა ფუნდამენტურ ინტერესს, ეროვნული უსაფრთხოების საბჭოს წარდგინების შესაბამისად;
- სპეციალური შემოწმების ჩატარება ეროვნული უსაფრთხოების საბჭოს დირექტივების შესაბამისად;
- ინფორმაციის კვლევა, ანალიზი და დამუშავება ბელგიის ტერიტორიაზე განხორციელებული უცხოური სადაზვერვო საქმიანობის შესახებ;
- კანონით გათვალისწინებული ყველა სხვა ფუნქციის განხორციელება.

საუკეთესო პრაქტიკებთან შესაბამისობაში, კანონის მე-8 მუხლი ჩამოთვლის ეროვნული უსაფრთხოების რისკებს. ისინი მოიცავს ნებისმიერ ინდივიდუალურ ან კოლექტიურ საქმიანობას ქვეყნის შიგნით და მის გარეთ, რომელიც შეიძლება უკავშირდებოდეს ჯაშუშობას, ტერორიზმს, ექსტრემიზმს, იარაღის გავრცელებას, საზიანო სექტანტურ ორგანიზაციებს. მართალია, ერთი შეხედვით ეს კატეგორიები ფართო ჩანს, თუმცა კანონი მათ დეტალურ განმარტებას ახდენს. ამის გარდა, სამსახურს ამ საფრთხეების შესახებ ინფორმაციის შეგროვება შეუძლიათ იმდენად, რამდენადაც ისინი შეეხება ქვეყნის შიდა უსაფრთხოებას და დემოკრატიული, კონსტიტუციური წყობის შენარჩუნებას, საგარეო უსაფრთხოებას და საერთაშორისო ურთიერთობებს, მეცნიერულ და ეკონომიკურ პოტენციალს.

ამდენად, უნდა აღინიშნოს, რომ ბელგიური მოდელი შეესაბამება საერთაშორისო სტანდარტებს, რადგან ის სამსახურის მანდატს შემოფარგლავს ინფორმაციის შეგროვებით, ანალიზით და დამუშავებით. სამსახურს არ გააჩნია მისი მანდატის ფარგლებში გათვალისწინებული დანაშაულების უშუალოდ გამოძიების უფლებამოსილება. თუმცა, მოთხოვნის შემთხვევაში, სამსახურს შეუძლია სასამართლო გამოძიების ფარგლებში ტექნიკური მხარდაჭერა გაუწიოს სისხლის მართლმსაჯულების ორგანოებს (მაგალითად ტერორიზმის საქმეებზე), იმ დაშვებით რომ ასეთი მხარდაჭერა შესაბამისი მინისტრების მიერ მიღებული პროტოკოლის დაცვით მოხდება.[43]

---

42 Loi Organique des Services de Renseignement et de Securite (18 decembre 1988), available from: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032

43 Article 20 of the Law, also see http://www.comiteri.be/index.php/en/39-pages-gb/305-what-do-intelligence-and-security-services-stand-for

სამართალდამცავი ფუნქციები: როგორც წესი, სამსახურს არ აქვს სამართალდამცავი ფუნქციები, როგორიცაა შეჩერების და ჩხრეკის უფლებამოსილება, დაკავება და დაპატიმრება, რაც საერთაშორისო სტანდარტებთან შესაბამისობაშია. თუმცა, სამსახურს ჰყავს იუსტიციის სამინისტროს მიერ გამოყოფილი „ჩარევის ჯგუფი“, იმ ერთადერთი მიზნისთვის, რომ მათ დაიცვან სამსახურის კონკრეტული თანამშრომლები და მისი ინფრასტრუქტურა. ამ ჯგუფის წევრებს მინიჭებული აქვთ გარკვეული საპოლიციო უფლებამოსილებები, თუმცა კანონი დეტალურად განსაზღვრავს შემთხვევებს, როდესაც მათ ამ უფლებამოსილებების გამოყენება შეუძლიათ.

მაგალითად, კანონი აკონკრეტებს, რომ ჩარევის ჯგუფის წევრებმა, შეიძლება, თუ ეს აბსოლუტურად აუცილებელი იქნება, დააკავონ პირი, თუ ამ პირის მიმართ არსებობს გონივრული ეჭვი, დანაშაულის ჩადენის ან მისი მომზადების შესახებ, თუ ეს დანაშაული სერიოზულ საფრთხეს უქმნის დაცული მოხელის სიცოცხლეს ან ფიზიკურ ხელშეუხებლობას ან საფრთხის შემცველია დაცული ინფრასტრუქტურისთვის. ამ შემთხვევაში, პირის დაკავება დაშვებულია მხოლოდ მანამ, სანამ პოლიცია გამოცხადდება ადგილზე, მაგრამ ნებისმიერ შემთხვევაში ასეთ დროს დაკავება არ შეიძლება გაგრძელდეს ერთ საათზე მეტ ხანს (კანონის 27-ე მუხლი).

ფარული მეთვალყურეობის ღონისძიებები და დაცვის განარტიები: კანონის თანახმად, სამსახურს მხოლოდ მიზანმიმართული მეთვალყურეობის განხორციელების უფლებამოსილება გააჩნია. კანონიერების პრინციპთან შესაბამისობაში, კანონის მუხლები 14-18 დეტალურად არეგულირებს მეთვალყურეობის ღონისძიებების გამოყენებას. კანონი ფარულ მეთვალყურეობას რამდენიმე კატეგორიად ყოფს, „ორდინალურ“, „სპეციალურ“ და „საგამონაკლისო“ ღონისძიებებად ჩარევის ინტენსივობიდან გამომდინარე, რაც საუკეთესო პრაქტიკის მაგალითია. ორდინალური ღონისძიებები მოიცავს, მათ შორის ინფორმაციის გამოთხოვას სისხლის მართლმსაჯულების ორგანოებიდან (ესეც კი გარკვეულ შეზღუდვებს ექვემდებარება), ასევე საჯარო სექტორის მონაცემთა ბაზებზე წვდომის მოპოვებას (მუხლი 14). კონკრეტული ღონისძიებები მოიცავს:

- ტექნიკური მოწყობილობების გამოყენებით საჯარო ადგილებში შესვლას, ჩხრეკას და მეთვალყურეობას;
- საფოსტო გზავნილის საიდენტიფიკაციო მონაცემების შემოწმებას;
- კომუნიკაციების საიდენტიფიკაციო, ზარზე და ადგილმდებარეობაზე ინფორმაციის (მეტადატა) შემოწმებას;

გამონაკლისი ღონისძიებები მოიცავს (კანონის მუხლები 16-18)

- კერძო საკუთრებაში შესვლა, მისი ჩხრეკა, მეთვალყურეობა;
- შენიღბული იდენტობის შექმნა და ფარული აგენტების გამოყენება;
- პერსონალური საფოსტო გზავნილის კონტროლი;
- საბანკო ანგარიშებზე და ტრანზაქციებზე ინფორმაციის შეგროვება;
- ინფორმაციული ტექნოლოგიის (IT) სისტემაში შეღწევა (კომპიუტერული ქსელის ექსპლუატაცია/ ჰაკერობა);
- კომუნიკაციის შინაარსის მონიტორინგი, მიყურადება, ჩაწერა;[44]

44 Also see http://www.comiteri.be/images/pdf/Jaarverslagen/Activity_Report_2014_15.pdf p.148-149

ჩარევის ინტენსივობის განსხვავების და ღონისძიებების განხორციელებისთვის საჭირო გარემოებების დეტალურად განსაზღვრით, ბელგიის კანონი აუცილებლობის და პროპორციულობის პრინციპების რეალიზების საუკეთესო პრაქტიკას წარმოადგენს. ბელგიის კანონი ძალიან პროგრესულ მაგალითად განიხილება, რადგან ის ჰაკერობასა და ფარული აგენტის ჩანერგვის ღონისძიებას მხოლოდ გამონაკლის ფარული მეთვალყურეობის ღონისძიებად მიიჩნევს, და შესაბამისად ყველაზე მკაცრი კონტროლის მექანიზმს ითვალისწინებს მათზე.

<u>დაცული პროფესიები:</u> საერთაშორისო სტანდარტებთან შესაბამისობაში, კანონი ადგენს კონკრეტულ შეზღუდვებს მეთვალყურეობის მეთოდების გამოყენებაზე, ადვოკატის და ექიმის პროფესიულად კონფიდენციალურ ინფორმაციასთან, ასევე ჟურნალისტის საიდუმლო წყაროსთან მიმართებით (მუხლი 2).

სტრუქტურა: გერმანიაში უსაფრთხოების სამსახურებს საკმაოდ განსხვავებული სტრუქტურა აქვს. თითოეულს ქვეყნის 16 შტატიდან (მიწა) ჰყავს მისი ადგილობრივი უსაფრთხოების სამსახური. ფედერალურ დონეზე არსებობს სამი სამსახური: სამხედრო კონტრდაზვერვის სამსახური (MAD), კონსტიტუციის დაცვის ფედერალური ოფისი (Bundesamt für Verfassungschutz - BfV), რომელიც წარმოადგენს სამოქალაქო უსაფრთოხების სამსახურს და ფედერალური დაზვერვის სამსახური (Bundesnachrichtendienst -BND), რომელიც წარმოადგენს სამოქალაქო საგარეო დაზვერვის სამსახურს.[45] ეს ქვეთავი და ანგარიში ყურადღებას გაამახვილებს კონსტიტუციის დაცვის ფედერალურ ოფისზე BfV-ზე, თუმცა, როდესაც რელევანტური იქნება, მითითება გაკეთდება ფედერალური დაზვერვის სამსახურზე BND-ზეც. სამსახურის იერარქიული წყობის და ქვემდებარეობის შესახებ იხილეთ მე-2 თავი უსაფრთხოების სამსახურების აღმასრულებელი კონტროლის შესახებ.

მანდატი: კონსტიტუციის დაცვის საკითხებზე და კონსტიტუციის დაცვის ფედერალურ ოფისთან მიმართებით ფედერაციასა და შტატებს შორის თანამშრომლობის მარეგულირებელი აქტის (შემდგომში BfV კანონი) თანახმად,[46] კონსტიტუციის დაცვის ფედერალური ოფისის (BfV) მანდატი მდგომარეობს ინფორმაციის შეგროვებასა და ანალიზში ისეთ საქმიანობებთან დაკავშირებით, რომელიც:

- მიმართულია თავისუფალი დემოკრატიული წყობის წინააღმდეგ;
- ფედერაციის ან მისი რომელიმე შტატის და მისი უსაფრთხოების წინააღმდეგ;
- მიზნად ისახავს ფედერაციის ან რომელიმე მისი შტატის კონსტიტუციური ორგანოების ან მათი წევრების საქმიანობის უკანონო ხელშეშლას;
- ძალადობრივად ხელყოფს გერმანიის ფედერაციული რესპუბლიკის საგარეო ინტერესებს ან აღნიშნულისთვის მზადებას წარმოადგენს;
- მიმართულია საერთაშორისო შეთანხმების იდეის წინააღმდეგ (ძირითადი კანონის მე-9 მუხლის მე-2 პარაგრაფის შესაბამისად, განსაკუთრებით ადამიანთა მშვიდობიანი თანაცხოვრების წინააღმდეგ)

ამ ძირითადი მანდატის მიღმა, კონსტიტუციის დაცვის ფედერალური ოფისი აგროვებს ინფორმაციას უცხოური ძალების მიერ განხორციელებული სადაზვერვო საქმიანობის შესახებ (კონტრდაზვერვა) და ასრულებს საბოტაჟისგან დაცვის საქმიანობას და ხელს უწყობს პერსონალის/ფიზიკურ უსაფრთხოებას.[47]

უნდა აღინიშნოს, რომ კონსტიტუციის დაცვის ფედერალური ოფისის შეზღუდული მანდატი საერთაშორისო სტანდარტებთან შესაბამისობაშია: BfV - ის მანდატი არ ვრცელდება კორუფციასა და ორგანიზებულ დანაშაულზე. თუმცა, გერმანიაში, გარკვეულ უსაფრთხოების რისკზე სპეციალიზებულ ორგანოს, როგორიცაა ფედერალური კრიმინალური პოლიცია, კონტრტერორისტული საქმიანობის ნაწილში მინიჭებული აქვს სპეციალური სამსახურებისთვის დამახასიათებელი უფლებამოსილებები; ანალოგიურად, ასეთი უფლებამოსილებებით სარგებლობს საბაჟო დანაშაულებზე გამოძიების დანაყოფი იარაღის გავრცელების, კონტრაბანდის, ფულის გათეთრების და სხვა საერთაშორისო ორგანიზებული დანაშაულის საქმეებზე.[48]

---

45 As stated earlier, although the BND has a predominantly foreign focus, it is also mandated to carry out domestic-foreign surveillance, and therefore can be categorized as having both an internal and external mandate.

46 https://www.gesetze-im-internet.de/bverfschg/

47 BfV Law, article 3 see https://www.verfassungsschutz.de/en/about-the-bfv/tasks/what-exactly-are-the-tasks-of-the-domestic-intelligence-services

48 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and

ფედერალური დაზვერვის სამსახურს აქვს მანდატი შეაგროვოს და გაანალიზოს ინფორმაცია, რომელიც ეხება ქვეყნის გარეთ მიმდინარე მნიშვნელოვან პოლიტიკურ, ეკონომიკურ და ტექნიკურ მოვლენებს, ისევე როგორც ფედერალური რესპუბლიკის და მისი მოქალაქეების აბსტრაქტულ ან კონკრეტულ უსაფრთხოებას. უფრო კონკრეტულად, დაზვერვის სამსახურს აქვს მანდატი განახორციელოს სტრატეგიული ფარული ღონისძიებები შეიარაღებულ თავდასხმასთან, საერთაშორისო ტერორიზმთან, იარაღის გავრცელებასთან, დიდი ოდენობით ნარკოტიკის ევროკავშირში კონტრაბანდასთან, ფულის გაყალბებასთან, რომელიც ევროს სტაბილურობას უქმნის საფრთხეს, ფულის გათეთრებასთან და არსებითი მნიშვნელობის ადამიანით ვაჭრობასთან კავშირში.[49]

ამის გარდა, სამსახურის მოვალეობებში შედის[50]:

- ფედერალური მთავრობის მხარდაჭერა უსაფრთხოებასა და საგარეო პოლიტიკასთან დაკავშირებულ საკითხებზე გადაწყვეტილებების მიღებისას, სხვა სახელმწიფოების შესახებ ინფორმაციის მიწოდებით.
- სამხედროებისთვის ინფორმაციის მიწოდება საგარეო მისიებთან დაკავშირებით.
- მსოფლიოს მასშტაბით ჰუმანიტარულ მოლაპარაკებებში მედიაცია,
- სამინისტროების და საჯარო უწყებების ინფორმირება კონკრეტულ საკითხებზე.

სამართალდამცავი ფუნქცია: კონსტიტუციის დაცვის ფედერალურ ოფისს არ აქვს სისხლის სამართლის საქმეზე გამოძიების და სამართალდამცავი ფუნქციის განხორციელების უფლებამოსილება. საუკეთესო პრაქტიკას წარმოადგენს ასევე რეგულირება, რომლის თანახმად ოფისს, მათ შორის არ შეუძლია პოლიციას დაავალოს მის ნაცვლად განახორციელოს პირის დაკავება. თუმცა, BfV კანონი დეტალურად მიმოიხილავს იმ კონკრეტულ გარემოებებს, როდესაც BfV - ის მიერ სამართალდამცავი ორგანოებისთვის ინფორმაციის გაზიარება დაშვებულია (კანონის მუხლები 20-23).

საუკეთესო პრაქტიკის მაგალითს წარმოადგენს BND კანონის რეგულირება, რომლის თანახმად ფედერალური დაზვერვის სამსახურს პირდაპირ ეკრძალება საპოლიციო უფლებამოსილებების განხორციელება. მუხლი 2(3) ადგენს: „BND არ აქვს რომელიმე სამართალდამცავი უფლებამოსილების/ ფუნქციის განხორციელების უფლებამოსიელბა. ასევე, მას არ შეუძლია მიმართოს პოლიციას ორმხრივი თანამშრომლობის შესახებ იმ ღონისძიებებთან დაკავშირებით, რომელთა განხორციელების უფლებამოსილება თავად არ გააჩნია“[51].

სამართალდამცავი ფუნქციის უპირობო აკრძალვა უსაფრთხოების/დაზვერვის სამსახურებისთვის გერმანიაში საუკეთესო პრაქტიკას წარმოადგენს.

დაცვის გარანტიები ფარულ ღონისძიებებთან მიმართებით

კანონიერება: ფარული მეთვალყურეობა გერმანიაში რეგულირებულია კანონით ფოსტის და ტელეკომუნიკაციების საიდუმლოების შესახებ (მოხსენიებული როგორც G-10 კანონი გერმანიის ძირითადი კანონის (GrundGesetz) მე-10 მუხლის - პირად ცხოვრებაზე უფლების და BND კანონის შესაბამისად). BfV ახორციელებს ფარულ ღონისძიებებს ქვეყნის შიგნით, როდესაც BND ძირითადად კონცენტრირებულია საგარეო დაზვერვაზე (თუმცა მას შეუძლია მოუსმინოს გერმანიიდან გასულ/

surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.16 available from: http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

49 Germany, Act on the Federal Intelligence Service, Sections 1 (1) and 2(1); Germany, G 10 Act, Section 5 (1).

50 http://www.bnd.bund.de/DE/Auftrag/Aufgaben/aufgaben_node.html

51 https://www.gesetze-im-internet.de/bndg/

გერმანიაში შემოსულ საერთაშორისო ზარებს, G10 კანონის რეგულირების ფარგლებში). როდესაც ორივე მათგანს შეუძლია მიზანმიმართული ფარული მეთვალყურეობის განხორციელება, BND-ს ასევე აქვს მასობრივი მეთვალყურეობის განხორციელების უფლებამოსილება (გერმანულ კანონმდებლობაში 'სტრატეგიული მეთვალყურეობა').

აუცილებლობა და თანაზომიერება: თანაზომიერების პრინციპთან შესაბამისობაში, G10 კანონი ჩამოთვლის იმ კატეგორიის პირებს, რომლებიც შესაძლოა დაექვემდებარონ ინტენსიურ მეთვალყურეობის ღონისძიებებს ეჭვის კონკრეტულ გარემოებებზე დაყრდნობით. მათ შორის არიან პირები, რომელთა მიმართ არსებობს ეჭვი სახელმწიფო ღალატის, კანონის უზენაესობისთვის საფრთხის შექმნის, ეროვნული თავდაცვის და შეირაღებული ძალების უსაფრთხოების წინააღმდეგ დანაშაულის, გერმანიის შიდა და გარე უსაფრთხოების წინააღმდეგ მიმართული კიბერდანაშაულის ჩადენის შესახებ (მუხლი 3(1)). ამის გარდა, კანონი შესაბამისობაშია აუცილებლობის პრინციპთან, რადგან ის ამ ღონისძიებების გამოყენებას დასაშვებად მიიჩნევს, თუ ამ საფრთხეების გამოძიება სხვა შემთხვევაში შეუძლებელია ან არსებითად გართულებული იქნებოდა (მუხლი 3(2)).

საერთაშორისო სტანდარტებთან შესაბამისობაში, კანონის მუხლები 9-13 მოიცავს დეტალურ დებულებებს, როგორ უნდა მოხდეს ფარული ღონისძიებების შესახებ შუამდგომლობის დაყენება, ნებართვის გაცემა, განხორციელება, და შეწყვეტა. ფარულ ღონისძიებებზე ნებართვის გაცემის შესახებ უფრო დეტალური ინფორმაციისთვის იხილეთ თავი 3.2 სასამართლო ზედამხედველობაზე).

დაცული პროფესიები: გერმანიის სისხლის სამართლის საპროცესო კოდექსი ჩამოთვლის რამდენიმე პროფესიას, რომელთა წარმომადგენლებს აქვთ უფლება უარი თქვან ჩვენების მიცემაზე მათ პროფესიულ საქმიანობაზე დაყრდნობით, მათ შორის, რელიგიურ პირებს, იურისტებს, ექიმებს, პარლამენტის წევრებს და ჟურნალისტებს (მუხლი 53)[52]. საუკეთესო პრაქტიკას წარმოადგენს G-10 კანონით კოდექსში ჩამოთვლილ ამ პროფესიებზე მითითება და მათი წარმომადგენლების მიმართ ფარული ღონისძიებების გამოყენების დროს გარკვეული შეზღუდვების დაწესება (G-10 კანონის მუხლი 3ბ).

52 14 Code of Criminal Procedure in the version published on 7 April 1987 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, 1319), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410) https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

თავი 2: უსაფრთხოების სამსახურების აღმასრულებელი კონტროლი

2.1. აღმასრულებელი ხელისუფლების როლი და მისი კონტროლის ფარგლები

გაეროს საუკეთესო პრაქტიკების მიმოხილვის თანახმად, სახელმწიფოები საერთაშორისო დონეზე არიან პასუხისმგებელი მათი სპეციალური სამსახურების, [53] აგენტების, და ნებისმიერი მათ მიერ დაქირავებული კერძო პირის საქმიანობაზე, იმის მიუხედავად, სად ხორციელდება ეს საქმიანობა და საერთაშორისოდ აღიარებული უკანონო ქმედების მსხვერპლი ვინ არის. აქედან გამომდინარე, აღმასრულებელი ხელისუფლება უზრუნველყოფს და ახორციელებს ზოგად კონტროლს და პასუხისმგებელია სპეციალური სამსახურების საქმიანობაზე.[54] შესაბამისი სამთავრობო სტრუქტურული დანაყოფების ზუსტი როლი და მათ მიერ განხორციელებული კონტროლის ფარგლები განსხვავდება ქვეყნების მიხედვით. როგორც წესი, აღმასრულებელი ხელისუფლების როლი და პასუხისმგებლობა შემდეგია:[55]

- ***სამსახურის ხელმძღვანელის დანიშვნა:*** გარე ზედამხედველობის აქტორებთან კონსულტაციის სხვადასხვა პრაქტიკები არსებობს (იხილეთ შემდეგი ქვეთავი), თუმცა ზოგადად მიღებულია, რომ აღმასრულებელი ხელისუფლება, როგორც სამსახურის საქმიანობაზე პოლიტიკური პასუხისმგებლობის ორგანო, წამყვან როლს ასრულებს ხელმძღვანელის კანდიდატის წარდგენასა და დანიშვნაში.

- ***პოლიტიკის განსაზღვრა და უსაფრთხოების სამსახურებისთვის დირექტივების შემუშავება:*** როგორც ეს მთავრობის კონტროლის ქვეშ არსებული სხვა სააგენტოების შემთხვევაში ხდება, უსაფრთხოების და დაზვერვის სფეროში მთავრობა არის პოლიტიკის შემუშავებაზე პასუხისმგებელი. დამატებით, მთავრობა გამოსცემს დირექტივებს უსაფრთხოების სამსახურების საქმიანობის შესახებ, მათ შორის სახელმძღვანელო პრინციპებს სამსახურების მიერ ადამიანის უფლებების დაცვის კუთხით.[56]

- ***უცხოურ უსაფრთხოების სამსახურებთან თანამშრომლობაზე წინასწარი თანხმობის გაცემა:*** ფართოდ გავრცელებული პრაქტიკაა უსაფრთხოების სამსახურების მიერ სხვა უცხოელ კოლეგებთან თანამშრომლობისთვის აღმასრულებელი ხელისუფლების წინასწარი თანხმობის აუცილებლობის განსაზღვრა. თითქმის ყველა ევროკავშირის ქვეყანაში, უსაფრთხოების სამსახურებმა უნდა მიიღონ აღმასრულებელი ხელისუფლების თანხმობა საერთაშორისო შეთანხმების გაფორმებამდე. [57]

- ***ინტენსიურ ოპერაციებსა და ფარულ ღონისძიებებზე ნებართვის გაცემა:*** საერთაშორისო პრაქტიკის შესაბამისად, აღმასრულებელი ხელისუფლების კიდევ ერთი მნიშვნელოვანი ფუნქციაა თანხმობის და ნებართვის გაცემა უსაფრთხოების სამსახურების ისეთ საქმიანობასა და მეთოდებზე,

---

53 UN Compilation of Good Practices' reference to intelligence services, cover both intelligence and security services as used in this report. See p.4

54 UN Compilation of Good Practices, Practice 14

55 The list is adapted from Born and Mesevage, Introducing Intelligence Oversight, in Born and Wills (ed) 'Overseeing Intelligence Services : A Toolkit' ,(2012), p.8

56 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p. 57 available from:https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

57 EU FRA *Surveillance by Intelligence Services Vol 2.* 2017, p.101

რომლებსაც ადამიანის უფლებების ხელყოფის ყველაზე მაღალ რისკებს შეიცავენ. რამდენიმე ევროსაბჭოს და ევროკავშირის ქვეყანაში, აღმასრულებელი ხელისუფლებაც მონაწილეობს ნებართვის გაცემის პროცესში.[58] თუმცა, მნიშვნელოვანია აღინიშნოს, რომ არ შეიძლება აღმასრულებელი ხელისუფლება იყოს ერთადერთი ორგანო, რომელიც ნებართვის გაცემაზეა პასუხისმგებელი; სასამართლო ან კვაზი სასამართლო ორგანოს ფუნქცია უნდა იყოს ასეთი ღონისძიებების კანონიერების, თანაზომიერების და აუცილებლობის გადახედვა.

- ***პარლამენტთან ანგარიშის წარდგენა:*** ზემოაღნიშნული კრიტიკული როლისა და ფუნქციის გათვალისწინებით, აღმასრულებელი ხელისუფლება სახელმწიფო უსაფრთხოების სამსახურების საქმიანობაზე პოლიტიკურ პასუხისმგებლობას ატარებს. [59] ამ პასუხისმგებლობის ერთ-ერთი ძირითადი შედეგია, უსაფრთხოების სამსახურების საქმიანობაზე აღმასრულებელი ხელისუფლების ანგარიშვალდებულება პარლამენტის წინაშე. აქედან გამომდინარე, მინისტრებს აქვთ ვალდებულება პარლამენტს წარუდგინონ ანგარიში სახელმწიფო უსაფრთხოების სამსახურების ზოგადი ფუნქციონირების შესახებ.

2.2. აღმასრულებელი ხელისუფლების მიერ უფლებამოსილებების ბოროტად გამოყენებისგან დაცვის მექანიზმები

აღმასრულებელი კონტროლი უსაფრთხოების სამსახურების საქმიანობაზე მნიშვნელოვანია მისი სწორად და ეფექტიანად წარმართვისთვის, თავისთავად ეს კონტროლიც შეიცავს აღმასრულებელი ხელისუფლების მხრიდან უფლებამოსილებების ბოროტად გამოყენების რისკებს, როგორიცაა პერსონალური ან პირადი პოლიტიკური მიზნებისთვის სამსახურის საქმიანობის გამოყენება, ან უსაფრთხოების სამსახურებზე პოლიტიკური გავლენების და ზეწოლის განხორციელება. ნაწილი საერთაშორისო სტანდარტების სწორედ აღმასრულებელი ხელისუფლების მხრიდან უფლებამოსილებების ბოროტად გამოყენების თავიდან აცილებას მიემართება.

დაქვემდებარება/ ღია კარის პოლიტიკა: უსაფრთხოების სამსახურები, როგორც წესი, ექვემდებარებიან აღმასრულებელ ხელისუფლებაში შემავალ რომელიმე სამინისტროს, როგორიცაა მაგალითად შინაგან საქმეთა ან იუსტიციის სამინისტრო. თუმცა, არის უშუალოდ პრემიერ-მინისტრისთვის, პრეზიდენტისთვის ან ორივე მათგანისთვის (როგორც ეს ხორვატიაშია) დაქვემდებარების მაგალითები.[60] გარკვეულწილად, ერთ პირზე ან სამინისტროზე უშუალო დაქვემდებარება ატარებს უსაფრთხოების სამსახურის პერსონალური/პოლიტიკური მიზნებისთვის გამოყენების რისკებს. ერთი შესაძლო დაცვის მექანიზმი ასეთი რისკების წინააღმდეგ შესაძლოა იყოს „ღია კარის პოლიტიკა“, მაგალითად სამსახურის ხელმძღვანელისთვის პირდაპირი კავშირი სხვა სამინისტროსთან, რომელსაც თავად არ ექვემდებარება. მაგალითად, დიდ ბრიტანეთში, უსაფრთხოების სამსახურის, საიდუმლო დაზვერვის სამსახურის, მთავრობის კომუნიკაციების მთავარი სამმართველოს ხელმძღვანელები მართალია ექვემდებარებიან შესაბამისად შინაგან საქმეთა მინისტრსა (Home Secretary) და საგარეო საქმეთა მინისტრს (Foreign Secretary), მაგრამ პირდაპირი კავშირი აქვთ ასევე პრემიერ მინისტრთან.[61]

- ***კონტროლისა და მართვის გამიჯვნა:*** მაშინ როდესაც აღმასრულებელი ხელისუფლება ზოგად

58 EU FRA , *Surveillance by Intelligence Services* 2015, p.34, also see CoE, 2015, p.57-58

59 Born and Mesevage, Introducing Intelligence Oversight, in Born and Wills (ed) 'Overseeing Intelligence Services : A Toolkit' ,(2012), p.10

60 For further discussion and examples, see Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015),p.57

61 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005), p.70

კონტროლს ახორციელებს უსაფრთხოების სამსახურებზე, მან ამ ფუნქციაში არ უნდა იგულისხმოს პირდაპირი მართვის პასუხისმგებლობა სპეციალურ და სადაზვერვო ოპერაციებზე. ვენეციის კომისიის თანახმად: „პოლიტიკური ლიდერებისთვის შეუძლებელი იქნება გარე კონტროლის როლის შენარჩუნება თუ ისინი ზედმეტად მჭიდროდ იქნებიან ჩართული სამსახურების საქმიანობის ყოველდღიურ საკითხებში, ასე ზედამხედველობის მექანიზმი სრულად დასუსტდება. ასევე არსებობს საფრთხე ინფორმაციის დამუშავების პროცესის პოლიტიზირების, იმ შედეგით, რომ ანალიზის ეტაპი და საბოლოო პროდუქტი ნაკლებად გამოსადეგი აღმოჩნდება.'[62] ამდენად, იმისთვის, რომ უფლებამოსილების ბოროტად გამოყენების და გაუმართლებელი ჩარევის პრევენცია მოხდეს, ეროვნულმა კანონმდებლობამ შესაბამისი სამინისტროს (ან პასუხისმგებელი საჯარო უწყების) და სამსახურის ხელმძღვანელის ფუნქციების მკაფიო რეგლამენტირება უნდა მოახდინოს.

- ***სამთავრობო მითითებების გამჭვირვალობა:*** კიდევ ერთი დაცვის მექანიზმი, აღმასრულებელი ხელისუფლების მხრიდან მითითებების პოლიტიკური მიზნებისთვის გამოყენების თავიდან ასაცილებლად, არის სამთავრობო მითითებების გარე კონტროლზე დაქვემდებარება. მართალია სრულიად გასაგებია, რომ კონფიდენციალური ინფორმაციის დაცვის მიზნით, აუცილებელი შეიძლება იყოს ასეთი მითითებების საზოგადოებისგან დაფარვა, ექსპერტების საზედამხედველო ჯგუფი ასეთ მითითებებზე წვდომისთვის შესაბამისი მექანიზმი იქნება. [63]

- ***პოლიტიკური მიზნებისთვის და პოლიტიკური ოპონენტების წინააღმდეგ უსაფრთხოების სამსახურების გამოყენების აკრძალვა:*** გაეროს სახელმძღვანელო დოკუმენტის თანახმად, საუკეთესო პრაქტიკას წარმოადგენს სპეციალური სამსახურების პოლიტიკურ საქმიანობაში ჩართვის, ან რომელიმე პოლიტიკური, რელიგიური, ეთნიკური, სოციალური ან ეკონომიკური ჯგუფის ინტერესების მხარდაჭერის ან დაცვის კანონმდებლობით აკრძალვა'[64]. მაგალითად, დიდი ბრიტანეთის უსაფრთხოების სამსახურის შესახებ კანონი შეიცავს პირდაპირ მითითებას იმის შესახებ, რომ სამსახური ვერ მიიღებს ზომებს რომელიმე პოლიტიკური პარტიის მიზნების მხარდასაჭერად.[65] გაეროს მიერ მხარდაჭერილი საუკეთესო პრაქტიკის თანახმად, სპეციალურ სამსახურებს ეკრძალებათ მათი უფლებამოსილებების გამოყენება კანონიერი პოლიტიკური საქმიანობის ან გაერთიანების, შეკრების და გამოხატვის თავისუფლების სხვა კანონიერი ფორმების წინააღმდეგ.[66] ასეთი ნორმა კანონში პოლიტიკური ნეიტრალიტეტის მყარ საფუძველს წარმოადგენს.

- ***დანიშვნის პროცედურები:*** როგორც უკვე აღინიშნა, გავრცელებული პრაქტიკაა აღმასრულებელი ხელისუფლების მიერ წამყვანი როლის შესრულება უსაფრთხოების სამსახურის ხელმძღვანელის კანდიდატურის წარდგენასა და მის დანიშვნაში. თუმცა, მნიშვნელოვანი სტანდარტია, კანდიდატურის წარდგენის პროცესში დემოკრატიული და ინკლუზიური საკონსულტაციო მექანიზმის ფუნქციონირება. ამ კუთხით განსხვავდება სახელმწიფოების პრაქტიკა. ავსტრალიაში, პრემიერ-მინისტრმა ხელმძღვანელის დანიშვნამდე კონსულტაცია უნდა გაიაროს ოპოზიციური პოლიტიკური პარტიის ლიდერებთან.[67] რამდენიმე ევროპულ ქვეყანაში, მათ შორის ესტონეთში, პორტუგალიაში, უნგრეთში და ხორვატიაში, კომპეტენტური საპარლამენტო კომიტეტები ატარებენ მოსმენას კანდიდატის მონაწილეობით და შემოთავაზებულ კანდიდატურაზე შეუძლიათ შესასრულებლად არასავალდებულო მოსაზრების ან რეკომენდაციის გამოცემა. შესაბამისი საპარლამენტო კომიტეტების ასეთი ჩართულობა (ძირითადად კომიტეტი, რომელიც უსაფრთხოების სამსახურებს

62 Venice Commission, *Democratic Oversight of the Security Services* (2007), para 143

63 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005), p.69, available from: http://www.dcaf.ch/making-intelligence-accountable

64 UN Compilation of Good Practices, Practice 11

65 UK , Security Service act, 1989, Section 2 (2)b, https://www.legislation.gov.uk/ukpga/1989/5/section/2

66 UN Compilation of good practices, Practice 12

67 Australia, Security Intelligence Organisation Act, section 17(3),

ზედამხედველობს) უზრუნველყოფს კანდიდატის ფართო პოლიტიკურ მხარდაჭერას. ბოლოს, ზოგიერთ ქვეყანაში, მაგალითად ამერიკის შეერთებულ შტატებსა და რუმინეთში, საპარლამენტო კომიტეტის მოსმენის შემდეგ კანდიდატისთვის მხარდაჭერის გამოსაცხადებლად მას პლენარულ სხდომაზე უყრიან კენჭს. უნდა აღინიშნოს, რომ მართალია პარლამენტში ხმის მიცემა კანდიდატურის დაყენების ძირითად დემოკრატიულ ფორმას წარმოადგენს, ის მაინც მოიცავს დამახასიათებელ პროცესის პოლიტიზირების რისკებს, პარტიულ საკითხად გადაქცევის პოტენციალს.[68] ამის გარდა, საპარლამენტო მოდელებში, სადაც მმართველი კოალიცია არაპროპორციულად ფლობს საპარლამენტო მანდატებს (მინიმალური საარჩევნო ზღვრის გამო), ხმის მიცემამ შესაძლოა ის შედეგი არ მოიტანოს, რისთვისაც გამიზნული იყო ის. ასეთ შემთხვევებში, ოპოზიციის ლიდერებთან სავალდებულო კონსულტაცია და მოსმენები საპარლამენტო კომიტეტებში შესაძლოა უფრო ეფექტიანი აღმოჩნდეს.

- ***წინასწარ განსაზღვრული თანამდებობის დაკავების ვადა და გათავისუფლების პროცედურები:*** კიდევ ერთ სტანდარტს წარმოადგენს სამსახურის ხელმძღვანელისთვის თანამდებობის დაკავების მინიმალური ვადის კანონით განსაზღვრა, რაც ხელმძღვანელს აძლევს საშუალებას გათავისუფლების მოლოდინის გარეშე განახორციელოს მისი საქმიანობა, ეს კი უზრუნველყოფს უსაფრთხოების სამსახურების დაცვას აღმასრულებელი ხელისუფლების მიერ ძალაუფლების ბოროტად გამოყენებისგან. გათავისუფლების პროცედურები მკაფიოდ უნდა იყოს განსაზღვრული კანონით, ის ფართო ინტერპრეტაციების შესაძლებლობასა და დისკრეციას არ უნდა ანიჭებდეს აღმასრულებელს.

- ***ინფორმაციის გასაჯაროება და ინფორმატორობა (whistleblowing):*** ბოლოს, უსაფრთხოების სამსახურების წარმომადგენლებს და თანამშრომლებს უნდა ჰქონდეთ კანონით განსაზღვრული შესაძლებლობა და მექანიზმი, სამსახურის გარეთ სხვა ორგანოებისთვის ხელმისაწვდომი გახადონ ინფორმაცია, როდესაც მათ გააჩნიათ წუხილი სამსახურის მართლსაწინააღმდეგო საქმიანობასთან დაკავშირებით (მაგალითად უკანონო მითითებები აღმასრულებელი ხელისუფლებისგან, გაუმართლებელი პოლიტიკური ზეწოლა და სხვა). გაეროს სტანდარტების შესაბამისად, საუკეთესო პრაქტიკას წარმოადგენს, უკანონო ადმინისტრაციულ პრაქტიკაზე სპეციალური სამსახურების თანამშრომლების პრეტენზიების გასაჯაროების კონკრეტული პროცედურების ეროვნული კანონმდებლობით რეგლამენტირება. შესაბამისად, სპეციალური სამსახურების წარმომადგენლები უნდა იყვნენ დაცული სამართლებრივი პასუხისმგებლობის დაკისრებისგან.[69] ასეთი სამართლებრივი დაცვის მექანიზმების პირობებში, როდესაც აღმასრულებელი ხელისუფლების წარმომადგენლებმა იციან მათი ქმედებების განსაჯაროების შესაძლებლობის შესახებ, უფლებამოსილებების ბოროტად გამოყენების და პოლიტიკური ზეწოლის განხორციელების ნაკლები რისკები იარსებებს.

68 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.107, 108

69 UN Compilation of Good Practices, Practice 18

კანადა

კანადის უსაფრთხოების სადაზვერვო საქმიანობის შესახებ კანონის[70] (შემდგომში კანონი) არის ყველაზე კარგი მაგალითი სამართლებრივი საფუძვლის, რომელიც მოიცავს უმეტესობა საერთაშორისო სტანდარტებს და დაცვის გარანტიებს ამ ქვეთავში განხილული ძალაუფლების ბოროტად გამოყენების რისკების წინააღმდეგ. კანადაში, აღმასრულებელი ხელისუფლებას განსაკუთრებით კი მინისტრს აქვს არსებითი კონტროლი კანადის უსაფრთხოების სადაზვერვო სამსახურზე (CSIS). ამ ქვეთავში მოხსენებული ძირითადი ფუნქციების შესაბამისად, ზედამხედველ სამინისტროს პასუხიმგებლობებში შედის, მათ შორის:

- სამსახურისთვის დირექტივების შემუშავება
- CSIS - ის მიერ უცხოელ კოლეგებთან გაფორმებულ შეთანხმებაზე თანხმობის გაცემა (კანონის მუხლი 13(3))
- CSIS - ის კანადაში სხვა ადგილობრივ უსაფრთხოების სამსახურებთან თანამშრომლობაზე წინასწარი ნებართვის გაცემა (მუხლი 17)
- სამსახურის საქმიანობის შესახებ პერიოდული ანგარიშების გადახედვა (მუხლი 4)
- შესაბამის მოსამართლესთან წარდგენამდე შუამდგომლობის (სპეციალური ღონისძიებების გამოყენების შესახებ) გადახედვა (მუხლი 6(2)).

***ქვემდებარეობა**:* კანადის უსაფრთხოების სადაზვერვო სამსახური (CSIS) ანგარიშს წარადგენს საჯარო უსაფრთხოებისა და გადაუდებელი ღონისძიებების სამინისტროს წინაშე.

კონტროლისა და მართვის გამიჯვნა: საერთაშორისო სტანდარტებთან შესაბამისობაში, კანონი აკონკრეტებს, რომ „ხელმძღვანელი, <u>მინისტრის მითითების საფუძველზე, ახორციელებს სამსახურის და მასთან დაკავშირებული საქმეების კონტროლსა და მართვას</u> (მუხლი 6(1)). კანონის შემდეგი ქვეთავები ასევე მკაფიოდ ჩამოთვლის სამსახურის დირექტორის მოვალეობებსა და პასუხისმგებლობებს, იმასთან დაკავშირებითაც, თუ მან როდის უნდა წარადგინოს მინისტრის წინაშე ანგარიში, რა გარემოებებში და რა საკითხებზე უნდა მოხდეს მასთან კონსულტაცია (მუხლი 6(4)).

სამთავრობო დირექტივების გამჭვირვალობა: კანონის თანახმად, მინისტრის მიერ CSIS-ისთვის გაცემული თითოეული წერილობითი მითითების ასლი უნდა წარედგინოს უსაფრთხოების დაზვერვის საზედამხედველო კომიტეტს (SIRC) (მუხლი 6(2)). პროაქტიულად უსაფრთხოების სამსახურის დავალდებულებით ექსპერტთა საზედამხედველო ჯგუფს გაუზიაროს მინისტრის მითითებები, კანადის მოდელმა შეიმუშავა მნიშვნელოვანი დაცვის გარანტია სამინისტროს მიერ ძალაუფლების ბოროტად გამოყენების წინააღმდეგ და შესაბამისად, საერთაშორისო დონეზე საუკეთესო პრაქტიკის მაგალითია.

პოლიტიკური ინტერესებისთვის და პოლიტიკური ოპონენტების წინააღმდეგ უსაფრთხოების

70 Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23) available from: http://laws-lois.justice.gc.ca/eng/acts/c-23/index.html

სამსახურების გამოყენების აკრძალვა: საუკეთესო პრაქტიკის კიდევ ერთი მაგალითია კანონის მე-2 მუხლი, რომელიც პირდაპირ უკრძალავს CSIS-ს „კანონიერი ადვოკატირების, პროტესტის და განსხვავებული აზრის“ გარშემო გამოძიების წარმოებას, თუ ეს არ ხდება კანონით გათვალისწინებულ რომელიმე საფრთხესთან დაკავშირებული საქმიანობის შესწავლის ფარგლებში.

დანიშვნა და თანამდებობის დაკავების ვადა: სამსახურის ხელმძღვანელს ნიშნავს მთავრობა (პროცედურის გავლით, რომელსაც კანადაში ეძახიან დანიშვნას საბჭოს მმართველის მიერ (Governon in Council - GIC)), ხუთი წლის ვადით, მაქსიმუმ მეორე ვადით არჩევის შესაძლებლობით (მუხლი 4). ზედამხედველი სამინისტრო პასუხისმგებელია კანდიდატურის წარდგენაზე, თუმცა GIC დანიშვნის პროცესი არის ღია კანადის ყველა მოქალაქისთვის, გამჭვირვალე და შერჩევის ეტაპზე მიღებულ შეფასებაზე დამოკიდებული (merit-based).[71]

ინფორმაციის გასაჯაროება და ინფორმატორობა: ინფორმაციული უსაფრთხოების შესახებ კანადის კანონის ერთ-ერთი ქვეთავი უშუალოდ ეხება პირებს, რომლებსაც აქვთ საიდუმლოების შენახვის მუდმივი ვალდებულება. კანონი განსაზღვრავს საჯარო ინტერესის შემთხვევაში CSIS- ის მოხელეებისთვის ინფორმაციის გასაჯაროების სპეციალურ პროცედურებს. თუმცა, ინფორმაციის გასაჯაროებამდე, მოხელემ საკითხი უნდა წარადგინოს მთავარი პროკურორის მოადგილესთან, მისგან პასუხის მიუღებლობის შემთხვევაში კი, უსაფრთხოების დაზვერვის საზედამხედველო კომიტეტთან (მუხლი 15(5)).[72]

71 This is a quite a unique approach and do not have much equivalence in Europe. For more information, see https://www.appointments-nominations.gc.ca/prsnt.asp?menu=3&page=FAQ&lang=eng

72 Canada, Security of Information Act (R.S.C., 1985, c. O-5), available from http://laws-lois.justice.gc.ca/eng/acts/O-5/

ქვემდებარეობა: ხორვატიის სახელმწიფო უსაფრთხოების სამსახური (SOA) ექვემდებარება, როგორც პრეზიდენტს, ისე პრემიერ მინისტრს ეროვნული უსაფრთხოების საბჭოს (NSC) საშუალებით. სახელმწიფო უსაფრთხოების სამსახურების სადაზვერვო საქმიანობის შესახებ კანონის[73] (შემდგომში კანონი) თანახმად, ეროვნული უსაფრთხოების საბჭოს დანიშნულებაა რესპუბლიკის პრეზიდენტსა და მთავრობას შორის თანამშრომლობის უზრუნველყოფა უსაფრთხოების სამსახურის საქმიანობისთვის მიმართულების მიცემის მიზნით (მუხლი 3(1)). საბჭოს ხელმძღვანელობს პრეზიდენტი, ყველა გადაწყვეტილება საჭიროებს მის და პრემიერ მინისტრის კონტრასიგნაციას. კანადის მოდელისგან განსხვავებით, SOA ექვემდებარება არა ერთ კონკრეტულ სამინისტროს, არამედ ეროვნული უსაფრთხოების საბჭოს. საბჭო ახორციელებს აღმასრულებელი კონტროლის თითქმის ყველა ფუნქციას, მათ შორის:

- განსაზღვრავს სამსახურის საქმიანობის ყოველწლიურ გაიდლაინებს
- წარადგენს ბიუჯეტს
- საერთაშორისო თანამშრომლობის შეთანხმებებს ამტკიცებს
- SOA - ის ანგარიშებს გადახედავს, და აფასებს პრეზიდენტის და პრემიერ-მინისტრის მეირ გამოცემული გადაწყვეტილებების/დირექტივების შესრულებას

ეროვნული უსაფრთხოების საბჭოში ფუნქციონირებს აღმასრულებელი კონტროლის ფუნქციის უზრუნველყოფისთვის განსაზღვრული სამმართველო. ხორვატიის მოდელი მნიშვნელოვან დაცვის გარანტიას ითვალისწინებს უფლებამოსილებების ბოროტად გამოყენების რისკის აღმოსაფხვრელად, რადგან სამსახურის კონტროლის უფლებამოსილება არ არის კონცენტრირებული ერთ სამინისტროში და ყველა გადაწყვეტილება პრეზიდენტისა და პრემიერ-მინისტრის კონტრასიგნაციას მოითხოვს.

ხელმძღვანელის დანიშვნა: ქვემდებარეობის სტრუქტურის პირობებში, უსაფრთხოების სამსახურის ხელმძღვანელი, 4 წლის ვადით და მეორე ვადით არჩევის შესაძლებლობით, ინიშნება გადაწყვეტილებით, რომელიც პრეზიდენტის და პრემიერ მინისტრის კონტრასიგნაციას მოითხოვს. თუმცა, საერთაშორისო სტანდარტებთან შესაბამისობაში, კანონი ითვალისწინებს შიდა პოლიტიკისა და ეროვნული უსაფრთხოების საპარლამენტო კომიტეტის დასკვნის მიღებას (მუხლი 66(1)). მართალია, საპარლამენტო კომიტეტს ვეტოს უფლებამოსილება არ გააჩნია, თუმცა მკაფიოდ ფორმულირებული ნეგატიური დასკვნა კანდიდატის შესახებ კითხვის ნიშნის ქვეშ დააყენებს პრეზიდენტის და პრემიერ-მინისტრის კანდიდატურის ლეგიტიმურობას.

ხელმძღვანელის გათავისუფლება: კანონი გათავისუფლების პროცედურას დეტალურად განსაზღვრავს, გათავისუფლების საფუძვლების გრძელი ჩამონათვალით. ხელმძღვანელების გათავისუფლების საფუძველი მათ შორის შეიძლება გახდეს: "ვალდებულებების შესრულების განგრძობადი შეუძლებლობა; რესპუბლიკის პრეზიდენტის და მთავრობის გადაწყვეტილებების აღუსრულებლობა, რომლებიც უსაფრთხოების და დაზვერვის სამსახურების საქმიანობის მიმართულებებს განსაზღვრავენ, ასევე ზედამხედველობის ღონისძიებების აღუსრულებლობა; კონსტიტუციის, კანონის, სხვა წესების და რეგულაციების დარღვევა, უფლებამოსილებების ბოროტად გამოიყენება ან უფლებამოსილების გადამეტება; ინფორმაციის საიდუმლოების დარღვევა; მათ წინააღმდეგ კანონიერ ძალაში შესული გადაწყვეტილება, რაც მათ თანამდებობისთვის შეუსაბამოს

73 https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

ხდის.”(კანონის მუხლი 66(4)). მართალია გათავისუფლების საფუძვლების დეტალური ჩამოთვლა საუკეთესო პრაქტიკას წარმოადგენს, თუმცა ისეთი ფართო ფორმულირება, როგორიცაა ‘წესების და რეგულაციების დარღვევა’ აღმასრულებელ ხელისუფლებას ფართო დისკრეციას ანიჭებს, იმის გათვალისწინებით, რომ ასეთი წესები და რეგულაციები კანონით არის გასაიდუმლოებული. კანონის შესაბამისად, გათავისუფლების საბოლოო გადაწყვეტილების მიღებამდე, შესაძლებელია ხორვატიის პარლამენტის მოსაზრების მოსმენა (მუხლი 66(5)). იქიდან გამომდინარე, რომ ეს უკანასკნელი სავალდებულო არ არის, ის თვითნებური გათავისუფლების წინააღმდეგ ძლიერ გარანტიად ვერ ჩაითვლება.

პოლიტიკური ინტერესებისთვის უსაფრთხოების სამსახურების საქმიანობის გამოყენების აკრძალვა: კანონის 77-ე მუხლი პირდაპირ უკრძალავს უსაფრთხოების სამსახურების თანამშრომლებს ‘იყვნენ პოლიტიკური პარტიების წევრები, მონაწილეობა მიიღონ მათ საქმიანობაში, წარმოადგინონ რომელიმე პოლიტიკური პარტია უსაფრთხოების და დაზვერვის სამსახურში,’ რაც საუკეთესო პრაქტიკის მაგალითია.

მითითებების გამჭვირვალობა: უსაფრთხოების სამსახურებთან მიმართებით მთავრობის მიერ მიღებული რეგულაციები (პრეზიდენტის თანხმობით) გასაიდუმლოებულია (მუხლი 62) და ზედამხედველობის ორგანოებთან მათი პროაქტიულად გაზიარების ვალდებულება კანადისგან განსხვავებით არ არსებობს.

სახელმწიფო უსაფრთხოების სამსახურის თანამშრომლების მიერ ინფორმაციის გასაჯაროება: ინფორმაციის განსაჯაროების წინააღმდეგ მკაცრი რეგულაციები მოქმედებს და კანადის სისტემისგან განსხვავებით, არ არსებობს საზოგადოებრივი ინტერესების დაცვისთვის მართლსაწინააღმდეგო საქმიანობის შესახებ ინფორმაციის განსაჯაროების მექანიზმი. მხოლოდ იმ შემთხვევაში, თუ საჯარო მოხელე ხელმძღვანელისგან უკანონო დავალებას მიიღებს, რაც სისხლის სამართლის დანაშაულს წარმოადგენს, პირს ექნება საპარლამენტო კომიტეტის თავჯდომარის და ეროვნული უსაფრთხოების საბჭოს ხელმძღვანელის ინფორმირების ვალდებულება (მუხლი 67(2)).

გარე კონტროლის ფარგლები უსაფრთხოების ბელგიურ სისტემაში კანადურ და ხორვატიულ მოდელთან შედარებით შეზღუდულია. სამართლის ექსპერტების მოსაზრებით, რეალური აღმასრულებელი კონტროლი სამოქალაქო დაზვერვის სამსახურზე არ არსებობს, რადგან ის საერთოდ არ მოითხოვს მთავრობის თანხმობას რომელიმე მისიის განხორციელებისას.[74] აქედან გამომდინარე, სამართლებრივი ჩარჩო ნაკლებად აკეთებს აქცენტს აღმასრულებელი ხელისუფლების მხრიდან ძალაუფლების ბოროტად გამოყენების წინააღდეგ დაცვის მექანიზმებზე.

ქვემდებარეობა: დაზვერვის და უსაფრთხოების სამსახურების შესახებ ორგანული კანონის თანახმად. „სახელმწიფო უსაფრთხოება“- ბელგიის სამოქალაქო დაზვერვის სამსახური, ძირითადად იუსტიციის სამინისტროს ექვემდებარება, თუმცა შინაგან საქმეთა სამინისტროს მანდატი ასევე ვრცელდება სამსახურზე, რამდენადაც ის ეხება საჯარო წესრიგის და ადამიანების დაცვას.[75] ასეთი ნაწილობრივი ზედამხედველობა გამოიხატება მაგალითად იმაში, რომ გარკვეულ სიტუაციებში იუსტიციის მინისტრი შინაგან საქმეთა მინისტრის ხელმოწერას საჭიროებს ან მისი მოსაზრების მოსმენას ავალდებულებს იუსტიციის მინისტრს.[76] იუსტიციის მინისტრის როლი მდგომარეობს ხარჯვაზე, ადამიანური რესურსების მართვასა და თანამშრომლების მომზადებაზე, შიდა წესებსა და დისციპლინაზე, თანამდებობრივ სარგოებზე, ტექნიკურ აღჭურვილობაზე ზედამხედველობაში (კანონის მუხლი 5(3)).

უსაფრთხოების სისტემის ბოლოდროინდელი რეფორმის ფარგლებში, ბელგიამ დააფუძნა ეროვნული უსაფრთხოების საბჭო, რომელსაც პასუხისმგებლობა დაეკისრა, მათ შორის უსაფრთხოების სამსახურის პოლიტიკის და პრიორიტეტების განსაზღვრაზე. დამატებით, საბჭოს კომპეტენციაში შედის სამსახურის უცხოელ კოლეგებთან თანამშრომლობის პირობების დადგენა. სამართლებრივი რეგულირების გარდა, რომლის თანახმად უსაფრთხოების სამსახურმა მისი საქმიანობა საბჭოს მიერ დადგენილ დირექტივებთან შესაბამისობაში უნდა განახორციელოს, სხვა მხრივ სამსახური საბჭოს კონტროლს არ ექვემდებარება.[77] შედარებისთვის, ხორვატიის ეროვნული უსაფრთხოების საბჭოს უსაფრთხოების სამსახურზე უფრო ფართო ზედამხედველობის მანდატი გააჩნია.

დანიშვნა: სამსახურის დირექტორს ნიშნავს მეფე, კანონის თანახმად იუსტიციის სამინისტროს, ხოლო პრაქტიკაში ერთიანად მთავრობის წარდგინების საფუძველზე. თანამდებობის დაკავების ვადა ხუთ წელს შეადგენს, მეორე ვადით დანიშვნის შესაძლებლობით.[78] მართალია, დანიშვნაში ფორმალურ დონეზე პარლამენტის მონაწილეობა გათვალისწინებული არ არის, თუმცა თანამდებობის დაკავებამდე ხელმძღვანელი ფიცს უსაფრთხოების და დაზვერვის სამსახურების მონიტორინგის კომიტეტის თავჯდომარის წინაშე დებს.[79]

ინფორმაციის გასაჯაროება: კანადის მოდელის მსგავსად, სამართლებრივი ჩარჩო ბელგიაში

74 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.19 available from: http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

75 Loi Organique des Services de Renseignement et de Securite (18 decembre 1988), Article 6, available from : http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032

76 Wauter Van Laetham, The Belgian Civil Intelligence Service: Roles, Powers, Organisation and Supervision , EJIS, Volume 2, (2008), p.21 available from : http://www.comiteri.be/index.php/en/publications/specialized-literature

77 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.23

78 Wauter Van Laetham, The Belgian Civil Intelligence Service: Roles, Powers, Organisation and Supervision , EJIS, Volume 2, (2008), p.22

79 Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, (DCAF: 2005),p.34

ითვალისწინებს მნიშვნელოვან დაცვის მექანიზმს აღმასრულებელი ხელისუფლების მხრიდან ძალაუფლების ბოროტად გამოყენების წინააღმდეგ, კერძოდ უსაფრთხოების სამსახურის წარმომადგენლებს ექსპერტთა საზედამხედველო ჯგუფთან ინფორმაციის გაზიარების შესაძლებლობას ანიჭებს. კომიტეტი I უფლებამოსილია: განიხილოს იმ პირთა საჩივრები და შეტყობინებები დანაშაულის შესახებ, რომელთაც სადაზვერვო სამსახურის საქმიანობა პირადად შეეხო. ასევე ხელმძღვანელებისგან წინასწარი თანხმობის გარეშე საჩივრის წარდგენა შეუძლია ნებისმიერ საჯარო მოხელეს, პირს, რომელიც საჯარო უფლებამოსილებას ასრულებს და შეირაღებული ძალების წარმომადგენელს, რომელთაც სამსახურის დირექტივები, გადაწყვეტილებები და მათთან დაკავშირებული რეგულაციები, ასევე მეთოდები ან ქმედებები პირადად შეეხო.[80]

80 Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment, Articles 40, available from: http://www.ennir.be/sites/default/files/pictures/pdf_11.pdf

დაქვემდებარება: როგორც უკვე აღინიშნა, გერმანიაში ფუნქციონირებს ორი სამოქალაქო უსაფთხოების სამსახური: BfV (კონსტიტუციის დაცვის ფედერალური ოფისი), და BND (ფედერალური დაზვერვის სამსახური). BfV ექვემდებარება შინაგან საქმეთა სამინისტროს, BND კი ანგარიშვალდებულია ფედერალური კანცლერის წინაშე.

ბელგიური მოდელისგან განსხვავებით, აღმასრულებელი ხელისუფლება უფრო მნიშვნელოვან როლს ასრულებს გერმანიაში, განსაკუთრებით ეს ეხება ფარული ღონისძიებების კონტროლს. სადაზვერვო სამსახურის ხელმძღვანელის მოთხოვნის საფუძველზე, ფედერალური მთავრობის შინაგან საქმეთა სამინისტრო არსებითად განიხილავს ფარული მეთვალყურეობის შესახებ ბრძანებას, დადებითი დასკვნის შემთხვევაში წერილობით გამოსცემს გადაწყვეტილებას და მას G10 კომისიას უგზავნის, რომელიც ნებართვის გაცემაზე პასუხისმგებელ ექსპერტთა საზედამხედველო ჯგუფს წარმოადგენს. გადაუდებელი აუცილებლობის შემთხვევაში ნებართვა შესაძლებელია შინაგან საქმეთა სამინისტრომაც გასცეს, თუმცა ის საბოლოოდ G 10 კომისიის შემდგომ (ex-post) გადასინჯვას დაექვემდებარება.[81]

ხელმძღვანელების დანიშვნა და გათავისუფლება: BfV და BND-ის ხელმძღვანელებს აღმასრულებელი ხელისუფლება ნიშნავს.[82]

სამთავრობო დირექტივების გამჭვირვალობა: უსაფრთხოების/დაზვერვის სისტემის უკანასკნელი რეფორმის ფარგლებში, გერმანიამ ცვლილებები შეიტანა კანონში, რომლითაც „სამსახურების მანდატის განხორციელებისთვის არსებითი გავლენის მქონე ადმინისტრაციული დირექტივების/მიმდინარე პროცესების შესახებ“ საპარლამენტო საზედამხედველო კომიტეტის პროაქტიულად ინფორმირების შესახებ BfV-ს და BND-ს დავალდებულება მოხდა.[83] ეს ადმინისტრაციული პრაქტიკა ჰგავს კანადის მოდელს, რაც შეიძლება აღმასრულებლის მიერ უსაფრთხოების სამსახურისთვის საკუთარი პოლიტიკური მიზნებისთვის თვითნებური მითითებების მიცემის წინაღმდეგ გათვალისწინებულ გარანტიად განვიხილოთ.

სამსახურის მოხელეების მიერ ინფორმაციის გასაჯაროება: გერმანიის საკანონმდებლო ჩარჩო უსაფრთხოების/დაზვერვის სამსახურების თანამშრომლებს მართლსაწინააღმდეგო საქმიანობის შესახებ ინფორმაციის საპარლამენტო საზედამხედველო კომიტეტთან გაზიარების უფლებამოსილებას ანიჭებს. თუმცა, კომიტეტისთვის ინფორმაციის მიწოდებამდე, მოხელეებმა საკითხი ჯერ სამსახურის შიგნით უნდა დასვან.[84] ეს პირობა შეიძლება მაგალითად ბელგიის მოდელთან შედარებით ნაკლებად ოპტიმალურ პრაქტიკად განვიხილოთ, სადაც მოხელეს შეუძლია მართლსაწინააღმდეგო საქმიანობის შესახებ ინფორმაცია პირდაპირ საზედამხედველო კომიტეტს გაუზიაროს, პირველ რიგში სამსახურის შიგნით ასეთი ინფორმაციის გაჟღერების გარეშე.

---

81 EU FRA, Surveillance by Intelligence Services (2015), p.33

82 In the framework of the research for this report, no information was found concerning the involvement of the Parliament in the appointment /dismissal processes of service directors.

83 The Law on the Parliamentary Control of Federal Intelligence Services Art.4.1, available from : http://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html

84 Ibid, Article 8(1)

თავი 3: უსაფრთხოების სამსახურების ზედამხედველობა და ანგარიშვალდებულება

არ არსებობს ერთი იდეალური მოდელი უსაფრთხოების სამსახურების ზედამხედველობისთვის. თუმცა საერთაშორისო სტანდარტების თანახმად, ზედამხედველობა უნდა იყოს კომპლექსური და მასში უნდა იყოს ჩართული რამდენიმე აქტორი, მათ შორის პარლამენტი, სპეციალიზებული ორგანოები, აღმასრულებელი ხელისუფლება, სასამართლო, ასევე სამოქალაქო საზოგადოების წარმომადგენელი ორგანიზაციები.[85] ზედამხედველობის ასეთი ორგანოების მანდატი და უფლებამოსილებები უნდა იყოს დეტალურად განსაზღვრული, რათა თავიდან იქნეს აცილებული მათ შორის დამთხვევა და დუბლირება, ასევე უსაფრთხოების სამსახურების საქმიანობის არც ერთი ასპექტი არ უნდა დარჩეს ზედამხედველობის სისტემის მიღმა. ეს ქვეთავი მიმოიხილავს საერთაშორისო სტანდარტებსა და საუკეთესო პრაქტიკებს, რომლებიც შეეხება ზემოთ მითითებული ორგანოების მიერ განხორციელებულ ზედამხედველობას.

3.1. უსაფრთხოების სამსახურებზე საპარლამენტო კონტროლი

პარლამენტი ზედამხედველობის სისტემის მნიშვნელოვან კომპონენტს წარმოადგენს, რადგან ის არის „დემოკრატიული ლეგიტიმურობის“ საფუძველი და ამ შემთხვევაში არჩეული პარლმანტარები ზედამხედველობენ უსაფრთხოების სამსახურებს.[86] მართალია საპარლამენტო ზედამხედველობის მანდატი და ფარგლები სხვადასხვა ქვეყანაში განსხვავდება, თუმცა ძირითადად პარლამენტი სამ ძირითად ფუნქციას ასრულებს უსაფრთხოების სამსახურებთან მიმართებით: (i) უსაფრთხოების სამსახურების მარეგულირებელი კანონმდებლობის შემუშავება და მიღება, (ii) უსაფრთხოების სამსახურების ბიუჯეტის გადახედვა და დამტკიცება, (iii) უსაფრთხოების სამსახურების პოლიტიკის და საქმიანობის ზედამხედველობა.[87] ეს ქვეთავი ყურადღებას გაამახვილებს მესამე ფუნქციაზე და მიმოიხილავს ეფექტიანი ზედამხედველობის რამდენიმე მნიშვნელოვან მახასიათებელს.

საპარლამენტო კომიტეტები: მართალია საპარლამენტო ზედამხედველობის რამდენიმე მექანიზმი არსებობს (პლენარული დებატების, მინისტრის გამოკითხვის, სპეციალური მოკვლევის და სხვა ფორმატები), ფართოდ გავრცელებული საერთაშორისო სტანდარტია, განგრძობადი და სრულყოფილი ზედამხედველობის განხორციელებისთვის უსაფრთხოების სამსახურის ზედამხედველობის მანდატის როგორც მინიმუმ ერთი მუდმივმოქმედი კომიტეტისთვის მინიჭება.[88] ევროკავშირის 28 ქვეყნიდან 26-ში, როგორც მინიმუმ ერთი საპარლამენტო კომიტეტი არის პასუხისმგებელი უსაფრთხოების სამსახურების ზედამხედველობაზე. ზოგიერთ ქვეყანაში ფუნქციონირებს სპეციალიზებული კომიტეტი ექსკლუზიური მანდატით უსაფრთხოების სამსახურებზე, სხვა ქვეყნებში ზედამხედველობის ფუნქციას ასრულებს უფრო ფართო მანდატის მქონე ერთი კომიტეტი, რომელიც თავდაცვის და სამართალდამცავ უწყებებსაც ეხება.[89] თუმცა, ევროსაბჭოს ქვეყნებში, უსაფრთხოების სამსახურებზე ექსკლუზიური

85 UN Compilation of Good Practices, para 13.

86 Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2010), p. 42, available from: http://www.dcaf.ch/guidebook-understanding-intelligence-oversight

87 Ibid. p.34

88 See Venice Commission, *Democratic Oversight of the Security Services* (2007) p.33 ; Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p.87

89 EU FRA, *Surveillance by Intelligence Services Vol 2* (2017), p.66

მანდატის მქონე ერთი სპეციალიზებული საპარლამენტო კომიტეტების მანდატის გავრცელების მზარდი ტენდენცია შეინიშნება. [90]

მანდატი: საპარლამენტო ზედამხედველობის მანდატი შესაძლოა თითოეულ ქვეყანაში განსხვავებული იყოს. თუმცა, ევროკავშირის მასშტაბით ჩატარებული გამოკითხვების და შედარებითი კვლევების შედეგები, ადასტურებენ, რომ უმრავლესობა საპარლამენტო კომიტეტები ზედამხედველობას ახორციელებენ უსაფრთხოების სამსახურების პოლიტიკაზე, ადმინისტრაციასა და ფინანსებზე. ამ საერთო მანდატთან ერთად, ზოგიერთ კომიტეტს დამატებით აქვს დასრულებული სპეციალური ოპერაციების, რამდენიმე მათგანს, კი მიმდინარე სპეციალური ოპერაციების ზედამხედველობის უფლებამოსილება. თუმცა, უნდა აღინიშნოს, რომ საპარლამენტო კომიტეტები ძირითადად ასრულებენ შემდგომ (ex-post facto) ზედამხედველობას, გარდა თანხების გამოყოფისა და ხელმძღვანელების დანიშვის პროცესში ჩართულობის ფუნქციებისა.[91] ვენეციის კომისიის თანახმად, შემდგომი ზედამხედველობის ეს პრაქტიკა შეესაბამება საერთაშორისო სტანდარტებს, რადგან საზედამხედველო ორგანოებს, არ უნდა ჰქონდეთ წინასწარი ინფორმაციის მიღების და გარკვეულ სპეციალურ ოპერაციებზე ნებართვის გაცემის უფლებამოსილება, რაც მათ იმ სისტემის ნაწილს გახდიდა, რომლის ზედამხედველობის ფუნქციაც ექნებოდა.[92]

აღნიშნულის გარდა, ზოგიერთი საპარლამენტო კომიტეტი ევროპაში ასევე სარგებლობს მანდატით განახორციელოს ზედამხედველობა უსაფრთხოების სამსახურების საქმიანობის სპეციფიკურ ასპექტებზე, როგორებიცაა ზედამხედველობა ინფორმაციის მოპოვების ღონისძიებებზე, პერსონალური ინფორმაციის გამოყენებაზე, ასევე სამსახურის წინააღმდეგ წარდგენილი ინდივიდუალური საჩივრების განხილვაზე. თუმცა, ამ ფუნქციების კომპლექსურობის, ასევე მისთვის საჭირო დროის, სპეციალური ცოდნის და რესურსების გათვალისწინებით, ევროპის ქვეყნების უმრავლესობა არჩევანს აკეთებს ექსპერტებისგან შემდგარი რამდენიმე სხვადასხვა საზედამხედველო ორგანოს შექმნაზე (ამ დრომდე 16 ევროკავშირის ქვეყანაში)[93]უსაფრთხოების სამსახურების ზედამხედველობაზე ექსკლუზიური და ფართო უფლებამოსილებებით. შემდეგ ქვეთავში უფრო დეტალურად იქნება განხილული ასეთ ექსპერტთა საზედამხედველო ორგანოების მანდატი და უფლებამოსილებები.

ზედამხედველობის მეთოდები და უფლებამოსილებები: საპარლამენტო კომიტეტებს აქვთ ზედამხედველობის განხორციელების სხვადასხვა საშუალებები. მათ შორის ყველაზე გავრცელებულია უსაფრთხოების სამსახურების წლიური ანგარიშების გადახედვა, საკომიტეტო მოსმენების ჩატარება და ახსნა-განმარტებისთვის სამსახურების მაღალი თანამდებობის პირების, ასევე თემატურად გარე ექსპერტების მოწვევა, სამსახურების წარმომადგენლებთან რეგულარული შეხვედრების გამართვა და უსაფრთხოების სამსახურების ადმინისტრაციული შენობების დათვალიერება.[94] ზედამხედველობის ასეთი ფუნქციების ეფექტიანად განხორციელებისთვის, საპარლამენტო კომიტეტებს მინიჭებული უნდა ჰქონდეთ საკმარისი უფლებამოსილებები, განსაკუთრებით კი უნდა ჰქონდეთ ინფორმაციაზე წვდომა. საერთაშორისო აქტორები, მათ შორის ვენეციის კომისია, გაერო[95] და ევროპის საბჭოს ადამიანის უფლებების კომისარი ყურადღებას ამახვილებენ ინფორმაციაზე წვდომის კრიტიკულ მნიშვნელობაზე. ეს უკანასკნელი განმარტავს:

---

90 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.42

91 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p.102, EU FRA, *Surveillance by Intelligence Services* (2015) p.34

92 Venice Commission, *Democratic Oversight of the Security Services* (2007) para 74

93 EU FRA, *Surveillance by Intelligence Services Vol 2* (2017)p.68, See Table 2 for the countries which have established.

94 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.135

95 UN Compilation of Good Practices (2011), Practice 7

"უსაფრთხოების სამსახურებზე ზედამხედველობის ფუნქციის მქონე ნებისმიერ ორგანოს უნდა ჰქონდეს წვდომა ყველა იმ ინფორმაციაზე, მისი გასაიდუმლოების ხარისხის მიუხედავად, რომელთაც ისინი მათი მანდატის შესრულებისთვის რელევანტურად მიიჩნევენ. ასეთ წვდომაზე შესაძლებლობა ზედამხედველობის ორგანოებისთვის კანონის დონეზე უნდა იყოს გაწერილი, ასევე ისეთი საგამოძიებო უფლებამოსილებებით და საშუალებებით უნდა იყოს გამყარებული, რომლებიც ინფორმაციაზე მათ წვდომას უზრუნველყოფენ. საიდუმლო ინფორმაციაზე წვდომის შეზღუდვის ნებისმიერი მცდელობა დაუშვებელია და საჭიროების შემთხვევაში, პასუხისმგებლობას უნდა იწვევდეს."[96]

ამ სტანდარტთან შესაბამისობაში, ევროპული პარლამენტების უმრავლესობაში, პარლამენტარებს, განსაკუთრებით კი საზედამხედველო კომიტეტების წევრებს აქვთ წვდომა საიდუმლო ინფორმაციაზე. თუმცა, უმრავლესობა ამ ქვეყნებში მოქმედებს გარკვეული შეზღუდვებიც, როგორებიცაა „გაცნობის საჭიროების" პრინციპი[97], გაუთქმელობის შესახებ შეთანხმებები, ან საპარლამენტო კომიტეტში დანიშვნამდე პარლამენტარების მიერ სპეციალური შემოწმების გავლის პროცედურა. [98] უნდა აღინიშნოს, რომ პარლამენტარების სპეციალური შემოწმება რეკომენდირებულ პრაქტიკას არ წარმოადგენს, რადგან უმეტეს შემთხვევებში პარლამენტარების სპეციალურ შემოწმებას უსაფრთხოების სამსახურები ახორციელებენ, რომელთა ზედამხედველობის ფუნქციას თავად ეს პარლამენტარები ასრულებენ. იმ შემთხვევებში, როდესაც სპეციალური შემოწმება კანონით არის განსაზღვრული, სასურველია უსაფრთხოების სამსახურის დასკვნა სარეკომენდაციო ხასიათის ოყოს, და დანიშვნის შესახებ საბოლოო გადაწყვეტილებაზე უფლებამოსილება პარლამენტს ჰქონდეს .[99]

კომიტეტის შემადგენლობა: საერთაშორისო სტანდარტებთან შესაბამისობაში, უსაფრთხოების სამსახურების ყოფილი თანამშრომლები ასეთი საპარლამენტო კომიტეტებისთვის შესაბამისი კანდიდატები არ არიან, განსაკუთრებით რეპრესიული უსაფრთხოების სამსახურების ისტორიის მქონე ქვეყნებში.[100] საპარლამენტო კომიტეტებში, პოლიტიკური წარმომადგენლობის კუთხით, ევროპული პარლამენტების უმრავლესობა მისდევს პროპორციული წარმომადგენლობის მიდგომას, ზოგიერთი კი ასეთ საზედამხედველო საპარლამენტო კომიტეტებში ჩართულობის კუთხით, დამატებით გარანტიებს ითვალისწინებს ოპოზიციისა და პოლიტიკური უმცირესობებისთვის. [101] ზოგადად, საუკეთესო პრაქტიკად განიხილება კომიტეტის თავჯდომარის თანამდებობის ოპოზიციისთვის განსაზღვრა.[102] ამის გარდა, ამ კომიტეტის წევრების არჩევა პლენარულ სხდომაზე კენჭისყრით, პოლიტიკური პარტიის ლიდერის ან საპარლამენტო სპიკერის მიერ დანიშვნის ნაცვლად, კომიტეტის ლეგიტიმურობას ზრდის.

რესურსები: უსაფრთხოების სამსახურების ზედამხედველობა კომპლექსური და რთული გამოწვევაა, რაც სპეციალურ ცოდნას მოითხოვს. პარლამენტარების განსხვავებული პრიორიტეტებისა და უსაფრთხოების სამსახურების საქმიანობის კუთხით ცოდნის ნაკლებობის გათვალისწინებით, ეფექტიანი ზედამხედველობის განხორციელებისთვის მნიშვნელოვანია საპარლამენტო კომიტეტების საჭირო ფინანსური, ტექნოლოგიური და ადამიანური რესურსით უზრუნველყოფა.[103] ეს მოიცავს რესურსებს კომიტეტის მუდმივი თანამშრომლებისთვის, განსაკუთრებული შემთხვევების დროს თემატურად გარე ექსპერტების მოწვევისთვის, ასევე ფიზიკურ ღონისძიებებს და მოწყობილობებს კონფიდენციალური ინფორმაციის გადახედვისა და დამუშავებისთვის.

---

96 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.13

97 According to this principle, persons can only access information if their official functions necessitate access to particular information, which applies in most parliaments.

98 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.117

99 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015) p.44

100 Venice Commission, *Democratic Oversight of the Security Services,* (2007), para 173

101 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), pp92-95

102 იქვე, para 176

103 The Tshwhane Principles, Principle 33

გერმანია

გერმანიაში ფუნქციონირებს საპარლამენტო ზედამხედველობის ერთ-ერთი ყველაზე განვითარებული ფორმა. საერთაშორისო სტანდარტებთან შესაბამისობაში, აქ სპეციალიზებულ საპარლამენტო კომიტეტს „საპარლამენტო კონტროლის ჯგუფს“ (შემდგომში „ჯგუფი“), აქვს სამივე ფედერალურ უსაფრთხოების/დაზვერვის სამსახურზე ზედამხედველობის მანდატი. ჯგუფის შექმნაზე ჩანაწერი არსებობს გერმანიის ძირითად კანონში, რაც საპარლამენტო ზედამხედველობის მნიშვნელობაზე მიანიშნებს. კანონი ფედერალური სპეციალური სამსახურების საპარლამენტო კონტროლის შესახებ [104] (შემდგომში კანონი), უფრო დეტალურად არეგულირებს ჯგუფის მიერ ზედამხედველობას.

მანდატი: ჯგუფს გააჩნია ყველა ფედერალური უსაფრთხოების სამსახურის საქმიანობაზე ზედამხედველობის მანდატი (მუხლი 1). თუმცა, ეს მანდატი ფართოდ განიმარტება და მოიცავს უსაფრთხოების სამსახურების პოლიტიკის და ფინანსური რესურსების კონტროლსაც. ჯგუფი სამსახურების მიერ ხარჯვის შემოწმებას მეორე სპეციალიზებულ საპარლამენტო კომიტეტთან ერთად ახორციელებს (ნდობის კომიტეტი). ჯგუფი რეგულარულად სწავლობს სამსახურების შიდა პოლიტიკას და მუშაობს ფარული ღონისძიებების შესახებ კანონმდებლობის აღსრულების საკითხებზე.[105] ჯგუფს ასევე აქვს მანდატი მიიღოს და დაამუშაოს ინდივიდუალური საჩივრები უსაფრთხოების სამსახურების წინააღმდეგ. ორწლიანი საანგარიშო პერიოდის განმავლობაში, ჯგუფმა მიიღო 65 პეტიცია, რომელთაგან 40 ეხებოდა ფარულ ღონისძიებებს.[106]

ზედამხედველობის მეთოდები და უფლებამოსილებები: ჯგუფს გააჩნია ფართო ზედამხედველობის საშუალებები და უფლებამოსილებები. ის იყენებს ყველა სტანდარტულ ზედამხედველობის საშუალებას (ანგარიშების გადახედვა, საკომიტეტო მოსმენების ჩატარება, დათვალიერება). ამ ფუნქციების განხორციელებისას, მას აქვს ფედერალური მთავრობისგან, ასევე უსაფრთხოების სამსახურებიდან დოკუმენტების და ელექტრონული მასალის მოწოდების მოთხოვნის შესაძლებლობა. უსაფრთხოების სამსახურების ყველა დეპარტამენტზე წვდომის პირობებში, ჯგუფის წარმომადგენლებს შეუძლიათ სპეციალური სამსახურების თანამშრომლებთან, სამთავრობო უწყებების წარმომადგენლებთან გასაუბრება ან მათგან წერილობით ინფორმაციის გამოთხოვა. მოთხოვნის შეუსრულებლობის შემთხვევაში, სასამართლო და სხვა საჯარო უწყებები ვალდებული არიან ოფიციალური დახმარება გაუწიონ ჯგუფს.[107] ამის გარდა, კანონი ავალდებულებს ფედერალურ მთავრობას პროაქტიულად მოახდინოს ჯგუფის ინფორმირება შემდეგ საკითხებზე (ა) გერმანიის საგარეო და შიდა უსაფრთხოების მდგომარეობის მნიშვნელოვან ცვლილებებზე; (ბ) სამსახურების მანდატის განხორციელებისთვის არსებითი გავლენის მქონე შიდა ადმინისტრაციულ ცვლილებებზე (გ) ინდივიდუალურ მოვლენებზე, რომლებიც პოლიტიკური დისკუსიების საგანი ან საჯაროდ ანგარიშის წარდგენის საფუძველია (კანონის მუხლი 4.1). ინფორმაციაზე წვდომის ფართო უფლებამოსილებებთან ერთად, მთავრობის დავალდებულება პროაქტიულად მოახდინოს ინფორმაციის საპარლამენტო ზედამხედველობის ორგანოსთვის გაზიარება საუკეთესო პრაქტიკის მაგალითია.

---

104 http://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html
105 EU FRA, Surveillance by Intelligence Services (2015), p.37
106 EU FRA, Surveillance by Intelligence Services Vol 2. (2017), p.117
107 Hans de With and Erhard Kathmann, ‘Annex A- Country Case Studies - Germany’, p.220, in Aidan Wills and Mathias Vermeulen, Parliamentary Oversight of Security and Intelligence Agencies in the European Union (2011)

***შემადგენლობა**:* ჯგუფი შედგება 9 წევრისგან, რომლებიც ყველა საპარლამენტო ჯგუფს წარმოადგენენ. ის, რომ ჯგუფის წევრები პარლამენტში ხმების უმრავლესობით აირჩევიან საუკეთესო პრაქტიკას წარმოადგენს,[108] რომელიც ფართო პოლიტიკურ მხარდაჭერას უზრუნველყოფს და ჯგუფის ლეგიტიმურობის ხარისხს ზრდის. წევრები სპეციალურ შემოწმებას არ გადიან, ისინი დებენ საიდუმლოების დაცვის შესახებ ფიცს. მათი ხმების უმრავლესობით არჩევის წესი სპეციალური შემოწმების სათანადო ალტერნატივად განიხილება, რადგან ეს წევრების პროფესიონალიზმის, კომპეტენციის და კეთილსინდისიერების მიმართ საკანონმდებლო ორგანოს ნდობის დადასტურებას წარმოადგენს.[109] ჯგუფის თავჯდომარის პოზიციას ყოველწლიურად მონაცვლეობით იკავებენ შესაბამისად მმართველი და ოპოზიციური პარტიების წარმომადგენლები.

რესურსები: ჯგუფის მხარდაჭერა ხდება მნიშვნელოვანი ადამიანური რესურსით. საქმიანობაში მხარდასაჭერად თანამშრომლების გარდა, ჯგუფის წევრებს აქვთ დამატებით მათი საპარლამენტო ჯგუფის თანამშრომლების ჩართვის შესაძლებლობა (ფედერალურ მთავრობასთან კონსულტაციისა და ჯგუფის თანხმობის მოპოვების შემდეგ). ჯგუფის წევრებისგან განსხვავებით, მისი თანამშრომლები სპეციალურ შემოწმებას გადიან.[110] განსაკუთრებულ შემთხვევებში ჯგუფს აქვს ასევე გარე ექსპერტებთან ხელშეკრულების გაფორმების საშუალებაც.

საპარლამენტო ზედამხედველობის კიდევ უფრო გაძლიერების მიზნით, გერმანიამ ცოტა ხნის წინ შეიტანა ცვლილებები კანონში და შექმნა საპარლამენტო წარმომადგენლის პოზიცია, რომელსაც ექნება ჯგუფის სახელით მოკვლევისა და ბიუჯეტის ხარჯვის შემოწმების უფლებამოსილება. წარმომადგენელს შეუძლია ნდობის ჯგუფის (უსაფრთხოების სამსახურების საბიუჯეტო ზედამხედველობის სპეციალიზებული საპარლამენტო კომიტეტი) და G10 კომისიის (ექსპერტთა ზედამხედველობის ორგანო), ყველა შეხვედრაზე დასწრება, რაც სხვადასხვა ზედამხედველობის მექანიზმებს შორის კოორდინაციის გაძლიერებასაც ხდის შესაძლებელს (კანონის მუხლი 5ა)

108 See https://www.bundestag.de/ausschuesse/ausschuesse18/gremien18/pkgr/einfuehrung/248044
109 Council of Europe, Democratic and Effective Oversight of National Security Services, (2015), p.66
110 Hans de With and Erhard Kathmann, 'Annex A- Country Case Studies - Germany', p.220, in Aidan Wills and Mathias Vermeulen, Parliamentary Oversight of Security and Intelligence Agencies in the European Union (2011)

უსაფრთხოების სამსახურებზე საპარლამენტო ზედამხედველობა კანადაში საუკეთესო პრაქტიკის მაგალითად არ განიხილება, რადგან აქ უსაფრთხოების სამსახურების საზედამხედველო ფუნქციის მქონე საპარლამენტო კომიტეტი არ ფუნქციონირებს. თუმცა, 2017 წლის ოქტომბერში, კანადამ კანონით განსაზღვრა და ჩამოაყალიბა „სახელმწიფო უსაფრთხოების და დაზვერვის პარლამენტის წევრების კომიტეტი“ (შემდგომში კომიტეტი).[111] მართალია, კანადაში საპარლამენტო ზედამხედველობა შესაძლოა სრულად არ შეესაბამებოდეს საერთაშორისო სტანდარტებს, თუმცა ის მაინც არის მისი გაუმჯობესების მაგალითი, და შემდეგ ქვეთავში განხილვას იმსახურებს.

***კომიტეტის სტრუქტურა**:* იმის მიუხედავად, რომ კომიტეტი შედგება პარლამენტის წევრებისაგან (სენატორებისა და არჩეული პარლამენტის წევრებისგან), ის არ წარმოადგენს პარლამენტის კომიტეტს მისი კლასიკური გაგებით, რადგან ის პარლამენტის ინსტიტუციური სტრუქტურის ნაწილი არაა (კანონის მუხლი 4). კომიტეტის წევრებს ნიშნავს საბჭოს მმართველი (აღმასრულებელი), პრემიერ-მინისტრის წარდგინების საფუძველზე (მუხლი 5 (1)). კომიტეტი პირველ რიგში ანგარიშს წარადგენს პრემიერ მინისტრის წინაშე, რომელიც მას გადახედავს და პარლამენტს წარუდგენს. პრემიერ მინისტრს ანგარიშის პარლამენტში წარდგენამდე შეუძლია კომიტეტს სთხოვოს ანგარიშის გადახედვა და მასში ცვლილებების შეტანა. კომიტეტის არაპირდაპირი ანგარიშვალდებულება პარლამენტის წინაშე საუკეთესო პრაქტიკის მაგალითად ვერ განიხილება.

***შემადგენლობა**:* კომიტეტი შედგება 11 წევრისგან (3 სენატორი და 8 არჩეული პარლამენტარი). კომიტეტში პარტიები პროპორციულად არ არის წარმოდგენილი, მაგრამ კანონი 8-დან 3 ადგილს ითვალისწინებს ოპოზიციური პარტიის წარმომადგენლებისთვის. თავჯდომარეს ნიშნავს საბჭოს მმართველი (აღმასრულებელი) პრემიერ-მინისტრის წარდგინების საფუძველზე (art 5(1)), ამდენად, ოპოზიციისთვის არ არსებობს გარანტირებულად ან მონაცვლეობით თავჯდომარის პოზიციის დაკავების მექანიზმი. საერთაშორისო საუკეთესო პრაქტიკის საპირისპირო და გერმანიის მოდელისგან განსხვავებით, წევრებმა უნდა გაიარონ მთავრობის სპეციალური შემოწმება (მუხლი10). კომიტეტი იკრიბება არა რეგულარულად, არამედ თავჯდომარის ინიციატივით (მუხლი 17), რომელიც ასევე არ წარმოადგენს ყველაზე ოპტიმალურ პრაქტიკას. შეიძლება ითქვას, რომ კომიტეტის შემადგენლობა და პროცედურები ოპოზიციას ზედამხედველობის პრიორიტეტების ეფექტიანად განსაზღვრის კუთხით შეზღუდულ შესაძლებლობებს უტოვებს.

მანდატი: კომიტეტს ფართო მანდატი გააჩნია, და მის ფარგლებში შედის სახელმწიფო უსაფრთხოების საკანონმდებლო, რეგულირების, პოლიტიკის, ადმინისტრაციული და ფინანსური ჩარჩოს, ასევე ნებისმიერი სახელმწიფო უსაფრთხოებასთან და დაზვერვასთან დაკავშირებული სხვა დეპარატმენტის საქმიანობის (თუ ის მიმდინარე ღონისძიებას არ წარმოადგენს) ზედამხედველობა. თუმცა, ასეთი კომპლექსური ზედამხედველობის მანდატი შეიძლება შეიზღუდოს თუ ‘შესაბამისი მინისტრი გადაწყვეტს, რომ საქმიანობის შემოწმება დააზიანებს სახელმწიფო უსაფრთხოებას“ (მუხლი 8). ასეთი შეზღუდვისთვის, მინისტრმა შესაბამისი დასაბუთება უნდა წარმოადგინოს (მუხლი 8(2)).

***ზედამხედველობის მეთოდები და უფლებამოსილებები**:* კანონი კომიტეტს მისი მანდატის განხორციელებისას ზედამხედველობის ღონისძიებების თავად განსაზღვრის თავისუფლებას ანიჭებს (მუხლი 20). კომიტეტს აქვს ‘წვდომა სამთავრობო უწყების კონტროლის ქვეშ არსებულ ნებისმიერ ინფორმაციაზე, რომელიც დაკავშირებულია კომიტეტის მანდატის განხორციელებასთან.’

111 National Security and Intelligence Committee of Parliamentarians Act (S.C. 2017, c. 15), available from: http://laws.justice.gc.ca/eng/AnnualStatutes/2017_15/page-1.html

(მუხლი13(1)). თუმცა, ეს უფლებამოსილება შეიძლება რამდენიმე შეზღუდვას დაექვემდებაროს, მათ შორის, იმ ინფორმაციასთან მიმართებით, რომელიც პირდაპირ უკავშირდება სამართალდამცავი ორგანოს მიერ წარმოებულ მიმდინარე გამოძიებას, რომელიც შესაძლოა შემდგომში სისხლის სამართლებრივი დევნის დაწყების საფუძველი გახდეს (მუხლი 14(1)).

რესურსები: საერთაშორისო სტანდარტებთან შესაბამისობაში, კომიტეტს დახმარებას უწევს სამდივნო და სრულ განაკვეთზე მყოფი თანამშრომლები.

ხორვატიაში, შიდა პოლიტიკის და სახელმწიფო უსაფრთხოების საპარლამენტო კომიტეტი, არის უსაფრთხოების სამსახურებზე საპარლამენტო ზედამხედველობის განმახორციელებელი ორგანო. თუმცა, გერმანული და კანადური მოდელებისგან განსხვავებით, ეს კომიტეტი უფრო ფართო მანდატით სარგებლობს, რომელიც ვრცელდება არა მარტო უსაფრთხოების სამსახურებზე, არამედ სამართალდამცავ უწყებებზეც. საერთაშორისო სტანდარტებთან შესაბამისობაში, კომიტეტის სამსახურს არეგულირებს კანონი (ხორვატიის რესპუბლიკის უსაფრთხოების და დაზვერვის სისტემის შესახებ კანონი).[112]

მანდატი: კომიტეტის მანდატი მოიცავს სამსახურების საქმიანობის (მათ შორის ფარული ღონისძიებებით ინფორმაციის მოპოვების სპეციალური ღონისძიებების) კანონიერების შემოწმებას, ფინანსურ მართვაზე ზედამხედველობას და ომბუდსმენის ანგარიშის გადახედვას უსაფრთხოების სამსახურის (SOA) საქმიანობის ნაწილში ადამიანის უფლებების დაცვის მდგომარეობის კუთხით (კანონის მუხლი 105/1). ამასთან, კომიტეტს აქვს SOA-ს წინააღმდეგ ინდივიდუალური საჩივრების მიღების და განხილვის უფლებამოსილებაც.[113]

ზედამხედველობის მეთოდები: საერთაშორისო სტანდარტებთან შესაბამისობაში, კომიტეტს სხვადასხვა ზედამხედველობის ღონისძიებების გამოყენების შესაძლებლობა აქვს, კერძოდ SOA -სგან სპეციალური ანგარიშების მოთხოვნა (როგორიცაა ანგარიშები ფარული ღონისძიებების გამოყენების შესახებ), მოსმენების ჩატარება და სამსახურის ხელმძღვანელების და მოხელეების გამოძახება და სამსახურის ადმინისტრაციული შენობების დათვალიერება. ამის გარდა, კომიტეტს ასევე შეუძლია ეროვნული უსაფრთხოების საბჭოს დაავალოს ასეთი ადგილის დათვალიერების განხორციელება (მუხლები 104 -105). კომიტეტის წევრებს აქვთ საიდუმლო ინფორმაციაზე წვდომა, თუმცა მათ უნდა მოიპოვონ სპეციალური შემოწმების წარმატებით გავლის დამადასტურებელი საბუთი.[114] ერთადერთი გამონაკლისი ინფორმაციაზე წვდომის კუთხით, ეხება ინფორმაციას იმ პირების შესახებ, რომელთანაც SOA მისი ფუნქციების განხორციელებისას თანამშრომლობს, ასევე ინფორმაცია, რომელიც უცხოური დაზვერვის სამსახურებისგან არის მიღებული.

შემადგენლობა: კომიტეტი შედგება 13 წევრისგან, რომლებიც აირჩევიან სახელმწიფო უსაფრთხოების საკითხებში დაინტერესებული პარლამენტის წევრებისგან საპარლამენტო კომიტეტების წევრების არჩევის ზოგადი წესების შესაბამისად.[115] კანონის თანახმად, კომიტეტს ყოველთვის ყველაზე დიდი ოპოზიციური პარტიის წარმომადგენელი თავმჯდომარეობს, (მუხლი 104/4), რაც საუკეთესო პრაქტიკის მაგალითია.

112 https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf
113 EU FRA, Surveillance by Intelligence Services (2015), p.70
114 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.9 available from: http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu
115 EU FRA, Surveillance by Intelligence Services (2015),p.39

საპარლამენტო ზედამხედველობა უსაფრთხოების სამსახურზე ბელგიაში საკმაოდ უნიკალურია, იმ გაგებით, რომ მართალია აქ არსებობს სპეციალური საპარლამენტო კომიტეტი[116] წარმომადგენლების პალატაში (ბელგიის პარლამენტის ქვედა პალატა), ის უსაფრთხოების სამსახურს უშუალოდ არ ზედამხედველობს, ნაცვლად ამისა, ის ახორციელებს ზედამხედველობის დამოუკიდებელ ექსპერტთა ჯგუფის 'მუდმივმოქმედი კომიტეტი I' მონიტორინგს, რომელსაც თავის მხრივ გააჩნია უსაფრთხოების სამსახურზე ზედამხედვლობის ექსკლუზიური მანდატი (იხილეთ შემდეგი ქვეთავი).

მანდატი: უნიკალური სტრუქტურიდან გამომდინარე, ბელგიის საპარლამენტო კომიტეტის მანდატი განსხვავდება მისი ანალოგებისგან განხილულ 3 ქვეყანაში. საპარლამენტო კომიტეტი შეიმუშავებს და გადახედავს კანონმდებლობას, ყოველწლიური საქმიანობის შესახებ მუდმივმოქმედი კომიტეტის ანგარიშს, ბიუჯეტის პროექტს და მუდმივმოქმედი კომიტეტის კვლევით ანგარიშს, რომელიც წელიწადში ორჯერ მზადდება და უსაფრთხოების სამსახურების მიერ გამოყენებულ ფარულ ღონისძიებებზე ამახვილებს ყურადღებას.[117]

ზედამხედველობის მეთოდები და უფლებამოსილებები: არაპირდაპირი ზედამხედველობის მანდატიდან გამომდინარე, საპარლამენტო კომიტეტს შეზღუდული უფლებამოსილებები აქვს. მას შეუძლია მუდმივმოქმედი კომიტეტისთვის მიმართვა იმ კანონპროექტების შესახებ სამართლებრივი დასკვნის თხოვნით, რომლებსაც საპარლამენტო კომიტეტი ამზადებს ან განიხილავს.[118]

შემადგენლობა: კომიტეტი შედგება წამომადგენლების პალატის 14 წევრისგან, რომლებიც ინიშნებიან პარლამენტის მიერ. საერთაშორისო საუკეთესო პრაქტიკასთან შესაბამისობაში, კომიტეტი დგება პროპორციული წარმომადგენლობის პრინციპით. წარმომადგენლების პალატის სპიკერი ხელმძღვანელობს კომიტეტს, რომელიც ამჟამად მმართველი პარტიის წარმომადგენელია.[119]

ამ ქვეთავში წარმოდგენილი იყო უსაფრთხოების სამსახურების საპარლამენტო ზედამხედველობაზე საერთაშორისო სტანდარტების და შერჩეული ქვეყნების საუკეთესო პრაქტიკების მოკლე მიმოხილვა. უსაფრთხოების სამსახურების საქმიანობის მზარდი მოცულობის და კომპლექსურობის გათვალისწინებით, ეჭვს არ იწვევს, რომ საპარლამენტო კომიტეტებს, მხარდაჭერის გარეშე, არ შეუძლიათ ეფექტიანი ზედამხედველობის განხორციელება. უფრო მეტიც, საპარლამენტო ზედამხედველობას რამდენიმე სუსტი მხარეც აქვს. პირველ რიგში, საპარლამენტო კომიტეტების ზედამხედველობა ატარებს უსაფრთხოების სამსახურების პოლიტიზირების რისკებს – მაგალითად პარლამენტის წევრები მმართველი პარტიიდან შესაძლოა სამსახურების დაცვით იყვნენ დაინტერესებული, ამ დროს კი ოპოზიციის წარმომადგენელმა პარლამენტის წევრებმა შესაძლოა, არა ზედამხედველობის, არამედ მთავრობაზე დარტყმის მიზნით, მოითხოვონ სამსახურების საქმიანობის შესახებ გამოძიება ან ამავე მიზნით ისარგებლონ ინფორმაციაზე წვდომით. ამის გარდა, როგორც წესი, პარლამენტის წევრებს არ აქვთ საკმარისი, დრო, რესურსი და ცოდნა უსაფრთხოების სამსახურების ეფექტიანი ზედამხედველობისთვის, განსაკუთრებით მათ ოპერაციულ ღონისძიებებთან დაკავშირებით, როგორიცაა ფარული ღონისძიებების გამოყენება.[120] მართალია შეუძლებელია საპარლამენტო

116 The full title of the parliamentary committee is 'Monitoring Committee responsible for monitoring the Standing Committee P and the Standing Committee I'

117 See http://www.comiteri.be/index.php/en/39-pages-gb/307-what-is-the-difference-between-the-standing-committee-i-and-the-monitoring-committee-of-the-chamber-of-representatives-responsible-for-monitoring-the-standing-committee-p-and-the-standing-committee-i

118 Ibid.

119 Ibid.

120 Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2010), pp.42-43

კომიტეტების მნიშვნელოვანი საქმიანობის, განსაკუთრებით მათი დემოკრატიული ლეგიტიმურობის უგულებელყოფა ან ჩანაცვლება, უსაფრთხოების სამსახურებზე ზედამხედველობის გასაძლიერებლად უმეტესობა ქვეყნები ექსპერტთა ზედამხედველობის ორგანოებს ანიჭებენ უპირატესობას (რომლებიც ხშირად ანგარიშვალდებული პარლამენტის წინაშე არიან).

3.2. უსაფრთხოების სამსახურების დამოუკიდებელი ზედამხედველობა - ექსპერტთა საზედამხედველო ორგანოების და ომბუდსმენის ინსტიტუტების როლი

ძლიერი ზედამხედველობის სისტემებში, უსაფრთხოების სამსახურების საქმიანობის სხვადასხვა ასპექტზე ზედამხედველობას ახორციელებენ დამოუკიდებელი ინსტიტუციები, როგორიცაა, ექსპერტებისგან შემდგარი ორგანოები, ომბუდსმენის ინსტიტუციები, მონაცემების დაცვის უწყებები/ ინფორმაციის კომისრები, და სახელმწიფო აუდიტის სერვისები. ეს ქვეთავი ყურადღებას გაამახვილებს მხოლოდ პირველ ორზე, ექსპერტთა საზედამხედველო ორგანოების და ომბუდსმენის ინსტიტუტების როლზე.

3.2.1 ექსპერტთა საზედამხედველო ორგანოები

ბოლო ათწლეულის განმავლობაში, დემოკრატიულ სახელმწიფოებში უსაფრთხოების სისტემის ანგარიშვალდებულების გაზრდის მიზნით შეინიშნება ექსპერტთა საზედამხედველო ორგანოების ჩამოყალიბების ტენდენცია. ექსპერტთა საზედამხედველო ორგანოები დამოუკიდებელი ინსტიტუტებია, რომლებიც ექსკლუზიურად უსაფრთხოების სამსახურების ზედამხედველობის მიზნით იქმნება, რომელთაც ჰყავთ სრულ განაკვეთზე დასაქმებული თანამშრომლები საჭირო უფლებამოსილებებითა და რესურსებით. ევროპის საბჭოს ადამიანის უფლებების კომისარი განმარტავს, რომ ექსპერტთა საზედამხედველო ორგანოები ხშირად ყველაზე კარგ პოზიციაში არიან დეტალური, უსაფრთხოების სამსახურების საქმიანობის კანონიერების ყოველდღიური ზედამხედველობის განსახორციელებლად'.[121] 2017 წლის დეკემბრის მდგომარეობით, ევროკავშირის 28 ქვეყნიდან 16-ში ზედამხედველობის სწორედ ასეთი ორგანოები ფუნქციონირებენ. [122] ქვემოთ მოკლედ იქნება მიმოხილული ექსპერტთა საზედამხედველო ორგანოების მთავარი მახასიათებლების შესახებ საერთაშორისო სტანდარტები.

ინსტიტუციური წყობა: მართალია სხვადასხვა ქვეყანაში განსხვავდება ექსპერტთა საზედამხედველო ორგანოების სტრუქტურა, თუმცა უმეტეს შემთხვევაში ასეთ ორგანოებს ქმნის პარლამენტი, და ისინი ანგარიშვალდებული არიან შესაბამისი საპარლამენტო საზედამხედველო კომიტეტის წინაშე. ასე ხდება უმრავლესობა ევროპულ ქვეყნებში, მათ შორის ბელგიაში და ხორვატიაში.[123] საერთაშორისო სტანდარტები უთითებენ, რომ პარლამენტის მიერ შექმნა და მის წინაშე ანგარიშვალდებულება ექსპერტთა საზედამხედველო ორგანოების ლეგიტიმურობას ზრდის.[124] თუმცა, არსებობს განსხვავებული მოდელები, მაგალითად კანადაში, სადაც ექსპერტთა საზედამხედველო ორგანოს ქმნის მოქმედი მთავრობა.

შემადგენლობა: როგორც დასახელებაც მიანიშნებს, ექსპერტთა საზედამხედველო ორგანოები შედგებიან სპეციალისტებისგან, ხშირად აპოლიტიკური და მაღალი რეპუტაციის მქონე, შესაბამისი მუშაობის გამოცდილების მქონე პირებისგან, რომლებიც მათი სპეციალური ცოდნისა და კვალიფიკაციის

121 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.8
122 *EU FRA, Surveillance by Intelligence Services Vol 2, (2017)* p.68
123 See the Country practices section below for details.
124 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.48 ; EU FRA, Surveillance by Intelligence Services (2015) p.43

საფუძველზე შეირჩევიან. როგორც წესი, მათ აქვთ თანამდებობის დაკავების წინასწარ განსაზღვრული ვადა, რომელიც მათი დამოუკიდებლობის მნიშვნელოვანი გარანტიაა. იქიდან გამომდინარე, რომ ხშირად ასეთ ორგანოებს სამსახურების საქმიანობის კანონიერების ზედამხედველობის მანდატი გააჩნიათ, გავრცელებული საერთაშორისო სტანდარტია, რომ ჯგუფის როგორც მინიმუმ ერთ წევრს ჰქონდეს იურიდიული განათლება (შესაბამისი გამოცდილების მქონე იურისტი ან ყოფილი მოსამართლე/პროკურორი).[125] თუმცა, ამის გარდა, ასევერეკომენდებულია, რომ ექსპერტთან საზედამხედველო ორგანოებში შესაძლებლობის ფარგლებში წარმოდგენილი იყოს განსხვავებული პროფესიული განათლების და გამოცდილების მქონე პირები, რათა უსაფრთხოების სამსახურების სულ უფრო და უფრო ტექნიკური და კომპლექსური სამუშაოს ეფექტიანი ზედამხედველობა იქნეს უზრუნველყოფილი.[126]

რესურსები: თითქმის ყველა ექსპერტთა საზედამხედველო ორგანოს ჰყავს სამდივნო და სრულ განაკვეთზე დასაქმებული თანამშრომლები. მუდმივი თანამშრომლების გარდა, საუკეთესო პრაქტიკაა, საჭიროების შემთხვევაში სპეციფიკურ ტექნიკურ საკითხებზე და მოკვლევისთვის გარე ექსპერტების განსაზღვრული პერიოდით დაქირავების შესაძლებლობის უზრუნველყოფა.[127]

მანდატი: ექსპერტთან საზედამხედველო ორგანოების მანდატი გარკვეულწილად განსხვავდება სპეციალური სამსახურების მანდატის, უფლებამოსილებების და სხვა საზედამხედველო ორგანოების ფუნქციის მიხედვით თითოეულ ქვეყანაში. თუმცა, საერთო სტანდარტია, ასეთი ორგანოების ზედამხედველობის მანდატში უსაფრთხოების სამსახურების საქმიანობის და პოლიტიკის კანონიერების, მათ შორის მათი ადამიანის უფლებებთან შესაბამისობის მოქცევა.[128] ამ კონტექსტში, მათ გააჩნიათ მანდატი განახორციელონ სპეციფიური ფუნქციები როგორიცაა ფარული ღონისძიებების ზედამხედველობა, რაც შეიძლება გამოიხატოს შემდეგში:

- წინასწარი ნებართვის/თანხმობის გაცემა: წინასწარი კონტროლი შეიძლება გამოიხატოს ექსპერტთა ჯგუფის მიერ უშუალოდ ღონისძიების მოთხოვნაზე ნებართვის გაცემაში ან ხელმოწერილ ორდერზე მისი ძალაში შესვლამდე თანხმობის გაცემაში[129], ამ კუთხით სასამართლო კონტროლის ჩამნაცვლებელი ან შემავსებელი ფუნქციით

- მიმდინარე კონტროლი: ინფორმაციის შეგროვების პროცესის მონიტორინგი და ორდერთან შესაბამისობის შემოწმება,

- შემდგომი (Ex-post) კონტროლი: უსაფრთხოების სამსახურების მიერ პერსონალური ინფორმაციის შენახვის, გამოყენების და გაზიარების გადასინჯვა[130]

უნდა აღინიშნოს, რომ ექსპერტთა საზედამხედველო ორგანოების მიერ წინასწარი ნებართვის/ თანხმობის გაცემა ფარული ღონისძიებების განხორციელებაზე ჯერ კიდევ არ წარმოადგენს ფართოდ გავრცელებულ პრაქტიკას ევროკავშირის წევრ ქვეყნებში. ამ მიდგომას ამ დრომდე მხოლოდ გერმანია, ბელგია და ავსტრია მისდევს, მაშინ როდესაც სხვა ქვეყნებში, მიზანმიმართულ ფარულ ღონისძიებებზე წინასწარ კონტროლს სასამართლო ხელისუფლება ახორციელებს.[131] უმეტესობა

125 Venice Commission, *Democratic Oversight of the Security Services,* (2007), para 228, Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p.97

126 EU FRA, Surveillance by Intelligence Services (2015)p.44

127 Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015), p.50, Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p. 101

128 Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015) p.47

129 *EU FRA, Surveillance by Intelligence Services Vol 2. (2017)* p.94

130 Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015)p. 49,

131 *EU FRA, Surveillance by Intelligence Services (2015),*p.52

ექსპერტთა ორგანოები ევროპაში კონცენტრირდება ფარული ღონისძიებების მიმდინარე და შემდგომ ზედამხედველობაზე.

ამის გარდა, გაეროს სახელმძღვანელო დოკუმენტის შესაბამისად, საუკეთესო პრაქტიკის თანახმად, 'ნებისმიერ პირს თუ ის თვლის, რომ მისი უფლებები დაირღვა სპეციალური სამსახურების მიერ, შეუძლია საჩივრით მიმართოს სასამართლოს ან ზედამხედველობის ორგანოს, როგორიცაა ომბუდსმენი, ადამიანის უფლებების კომისარი, ან ეროვნული ადამიანის უფლებების ინსტიტუცია'.[132] ამ კონტექსტში, უმრავლესობა ექსპერტთა საზედამხედველო ორგანოს მანდატი გულისხმობს უსაფრთხოების სამსახურების წინააღმდეგ წარდგენილი საჩივრების განხილვას.

ზედამხედველობის ფუნქცია: გაეროს საუკეთესო პრაქტიკების მიმოხილვა მკაფიო სტანდარტებს ადგენს საზედამხედველო ინსტიტუციების ფუნქციებისა და ზედამხედველობის მეთოდების კუთხით:

> *„ზედამხედველობის ინსტიტუტებს აქვთ უფლებამოსილებები, რესურსები და ცოდნა <u>მათი ინიციატივით მოკვლევის დაწყებისა და წარმოებისთვის,</u> ასევე მათი მანდატის განხორციელებისთვის საჭირო <u>სრული და დაუბრკოლებელი წვდომა ინფორმაციაზე, მოხელეებსა და მოწყობილობებზე</u>. ზედამხედველობის ინსტიტუტები დაუბრკოლებლად სარგებლობენ სპეციალური სამსახურების და სამართალდამცავი ორგანოების თანამშრომლობით მოწმეთა გამოკითხვის, დოკუმენტების და სხვა მტკიცებულებების მოპოვების ნაწილში."*[133]

ეს მნიშვნელოვანი გაეროს სტანდარტი შეიცავს კრიტიკულად მნიშვნელოვან ასპექტებს, რომლებიც უფრო ვრცელ ანალიზს საჭიროებს:

<u>*საკუთარი ინიციატივით მოკვლევის დაწყება:*</u> ამ ფუნქციის მნიშვნელობას აღიარებს ვენეციის კომისია, რომლის რეკომენდაციის თანახმად, ექსპერტთან საზედამხედველო ორგანოებს უნდა ჰქონდეთ მათი დღის წესრიგის, ზედამხედველობის პრიორიტეტების განსაზღვრის, საკუთარი ინიციატივით მოკვლევის დაწყების უფლებამოსილება.[134] ასე ეს ორგანოები არ იქნებიან შებოჭილი მხოლოდ იმ სფეროებზე ზედამხედველობით, რომლებზეც მათ მთავრობა ან პარლამენტი მიუთითებს. ამ სტანდარტთან შესაბამისობაში, უმრავლესობა ექსპერტთა ორგანოებს აქვთ მათი ინიციატივით მოკვლევის დაწყების უფლებამოსილება.

<u>*ინფორმაციაზე წვდომა*</u>: მათი მანდატის ეფექტიანად განხორციელებისთვის, ექსპერტთა ზედამხედველობის ორგანოებს უნდა ჰქონდეთ ფართო წვდომა ინფორმაციაზე. მართალია, მიღებულია ასეთ წვდომაზე კანონით გარკვეული შეზღუდვების დაწესება (მაგალითად ზედამხედველობის განმახორციელებელ ორგანოებს შესაძლოა არ ჰქონდეთ წვდომა წყაროს ან მიმდინარე მოკვლევის შესახებ ინფორმაციაზე), თუმცა ასეთი შეზღუდვები რაც შეიძლება ვიწროდ უნდა გაიწეროს კანონში, სხვა შემთხვევაში ეს შეიძლება გადაიზარდოს აღმასრულებელი ხელისუფლების მხრიდან ინფორმაციაზე წვდომის კუთხით თვითნებური შეზღუდვების დაწესებაში, რაც სერიოზულ დაბრკოლებებს შეუქმნის ექსპერტთა საზედამხედველო ორგანოების საქმიანობას. [135] მნიშვნელოვანი სტანდარტი, რომელიც საზედამხედველო ორგანოების ინფორმაციაზე წვდომის ხარისხს ზრდის, არის უსაფრთხოების სამსახურების და აღმასრულებელი ხელისუფლების კანონით დავალდებულება, ზედამხედველობის ორგანოებისთვის ინფორმაციის პროაქტიულად გაზიარების შესახებ[136], განსაკუთრებით ფარულ

---

132 UN Compilation of Good Practices, Practice 9
133 Ibid, Practice 7
134 Venice Commission, *Democratic Oversight of the Security Services* (2007), para 229
135 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p 123-124
136 Ibid, p.127

ღონისძიებებთან მიმართებით. თუმცა, აღნიშვნის ღირსია ისიც, რომ ინფორმაციაზე წვდომა არ არსებობს გარკვეული პასუხისმგებლობის გარეშე. როგორც ამაზე გაეროს საუკეთესო პრაქტიკების მიმოხილვა უთითებს, „ზედამხედველობის ინსტიტუციებმა უნდა მიიღონ ყველა საჭირო ზომა საიდუმლო და პერსონალური ინფორმაციის დაცვის კუთხით, რომელზე წვდომაც მათ სამსახურებრივი ფუნქციის განხორციელებისას აქვთ. კანონი ითვალისწინებს სანქციის დაკისრებას საზედამხედველო ინსტიტუტების წარმომადგენლების მიერ ამ მოთხოვნების დარღვევის შემთხვევაში'.[137] გავრცელებული პრაქტიკაა, ექსპერტთა საზედამხედველო ორგანოების წევრებისა და თანამშრომლებისთვის სპეციალური შემოწმების პროცედურის გათვალისწინება.

დაუბრკოლებელი თანამშრომლობა უსაფრთხოების და სამართალდამცავ ორგანოებთან:
უმეტესობა ექსპერტთა ზედამხედველობის ორგანოების მანდატი ვრცელდება უსაფრთხოების სამსახურების ადმინისტრაციული შენობების დათვალიერებაზე, საჩივრების გამოკვლევასა და ფარული ღონისძიებების აღსრულების მონიტორინგზე. აქედან გამომდინარე, ასეთ ექსპერტთა ორგანოებს მოკვლევის განხორციელებისას ან უნდა ჰქონდეთ უსაფრთხოების და სამართალდამცავ ორგანოებისგან თანამშრომლობის მოთხოვნის უფლებამოსილება ან მათ თავად უნდა ჰქონდეთ მინიჭებული გარკვეული საგამოძიებო უფლებამოსილებები. ასეთი უფლებამოსილებების გარეშე ექსპერტთა საზედამხედველო ჯგუფი მოკლებული იქნებოდა რეალურ ბერკეტებს და სპეციალური სამსახურების მხოლოდ კეთილი ნების იმედზე დარჩებოდა.

როგორც უკვე აღინიშნა, საზედამხედველო სისტემის შერჩევისას იკვეთება ექსპერტთა ორგანოებისთვის უპირატესობის მინიჭების ტენდენცია. ამ ორგანოების აქვთ შესაბამისი ექსპერტული ცოდნა და საკმარისი დრო უსაფრთხოების და დაზვერვის სამსახურების ზედამხედველობის განსახორციელებლად.[138] წინასწარ განსაზღვრული თანამდებობის დაკავების ვადის ფარგლებში, საპარლამენტო ზედამხედველობის ორგანოებისგან განსხვავებით, რომლებიც ძირითად შემთხვევაში არასასესიო ან არჩევნების პერიოდებში საქმიანობას აჩერებენ, განგრძობადი ზედამხედველობის განხორციელების შესაძლებლობა აქვთ.[139] თუმცა, ექსპერტთა საზედამხედველო ორგანოების დაფუძნება ვრცელი მანდატით და უფლებამოსილებებით მნიშვნელოვან ადამიანურ და ფინანსურ რესურსებს მოითხოვს. მათი მანდატი, უფლებამოსილებები და კომპეტენციები სწორად უნდა განისაზღვროს დუბლირების და რესურსების არაეფექტიანი გამოყენების თავიდან ასაცილებლად.

3.2.2. ომბუდსმენის ინსტიტუტები

ომბუდსმენის ინსტიტუტები იქმნება კონსტიტუციის ან კანონის შესაბამისად, და მათ ხელმძღვანელობენ დამოუკიდებელი მაღალი რანგის თანამდებობის პირები, რომლებიც ან სახელმწიფო უწყებების, თანამდებობის პირების, მოხელეების წინააღმდეგ ადამიანის უფლებების დარღვევების და ადმინისტრაციული გადაცდომის ფაქტების შესახებ იღებენ საჩივრებს ან საკუთარი ინიციატივით სხვადასხვა წყაროდან მიღებული ინფორმაციის საფუძველზე იღებენ ზომებს.[140] ომბუდსმენის ინსტიტუტს აქვს უფლებამოსილება, მათ შორის, გამოიკვლიოს, გააკრიტიკოს შესაბამისი უწყებები ან რეკომენდაციით მიმართოს მათ, ასევე წარადგინოს ახალი კანონის ან კანონში ცვლილებების კანონპროექტები. ეროვნული ინსტიტუტების სტატუსის შესახებ პრინციპები **(პარიზის პრინციპები)** ითვლება ეროვნული ადამიანის უფლებების ინსტიტუტების მანდატის, უფლებამოსილებების, შემადგენლობის და საქმიანობის ფარგლების ძირითად ნორმატიულ ჩარჩოდ, რომლებიც ძირითადად

137 UN Compilation of Good Practices, Practice 8
138 Venice Commission, *Democratic Oversight of the Security Services* (2007), para 219
139 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011)), p.90
140 The Parliamentary Ombudsman of Malta, Frequently Asked Questions, available from: http://www.ombudsman.org.mt/how-can-one-define-the-ombudsman-institution/

ომბუდსმენის ინსტიტუტებს ეხება. **პარიზის პრინციპების** თანახმად, ასეთ ინსტიტუტებს:

- უნდა ჰქონდეთ ფართო მანდატი;
- უნდა დაეკისროთ პასუხისმგებლობა, მოთხოვნის შემთხვევაში ან საკუთარი ინიციატივით წარადგინონ მოსაზრებები, რეკომენდაციები, ინიციატივები და ანგარიშები ნებისმიერი საკითხის გარშემო, რომელიც ადამიანის უფლებების დაცვას და მხარდაჭერას ეხება საკანონმდებლო, ადმინისტრაციულ, სასამართლო აქტებთან ან სხვა სიტუაციასთან მიმართებით, რომელთა გამო შესაძლოა ადამიანის უფლებები დაირღვეს;
- უნდა ჰქონდეთ მანდატი მთავრობის ყურადღება გაამახვილონ ისეთ სიტუაციებზე, ქვეყნის ნებისმიერ ნაწილში არსებულ სიტუაციაზე, სადაც ადამიანის უფლებები ირღვევა, მთავრობას ასეთი სიტუაციების აღმოსაფხვრელად რეკომენდაციებით მიმართონ და, საჭიროების შემთხვევაში, გამოხატონ მოსაზრება მთავრობის პოზიციასა და მის მიერ მიღებულ ზომებზე;
- თავისუფლად განიხილონ ნებისმიერი საკითხი, რომელიც მათი კომპეტენციის ფარგლებში ექცევა, მოუსმინონ ნებისმიერ პირს და მოიპოვონ ნებისმიერი ინფორმაცია სიტუაციის შესაფასებლად, რომელიც მათი კომპეტენციის ფარგლებში ექცევა, ასევე საჯარო გახადონ მათი მოსაზრებები და რეკომენდაციები.[141]

როგორც წესი ომბუდსმენის ინსტიტუტების მანდატი ვრცელდება ყველა სამთავრობო უწყებაზე, მათ შორის უსაფრთხოების სამსახურებზე. ქვეყნებში, სადაც უსაფრთხოების სამსახურებზე ექსპერტთა საზედამხედველო ორგანოები არ არსებობს, ომბუდსმენის ინსტიტუტებს შეუძლიათ მსგავსი, როგორიცაა საჩივრების განხილვის და დაწესებულების დათვალიერების ფუნქციები შეასრულონ. თუმცა, პრაქტიკაში ევროპაში ომბუდსმენის ინსტიტუტები წამყვან როლს არ თამაშობენ უსაფრთხოების სამსახურების (მათ შორის დამოუკიდებელი ინსტიტუციების) ზედამხედველობაში, გარდა რამდენიმე მაგალითისა როგორიცაა სერბიის ომბუდსმენი ან ფინეთის საპარლამენტო ომბუდსმენი, ეს უკანასკნელი კონკრეტულად ინფორმაციის მოპოვების ფარულ ღონისძიებებს და ფარული აგენტის ჩანერგვის ოპერაციებს ზედამხედველობს.[142] ამისთვის სამი ძირითადი მიზეზი არსებობს. პირველ რიგში, როგორც უკვე აღინიშნა, უფრო და უფრო მეტ ევროპულ ქვეყანაში ფუნქციონირებს ექსპერტთა საზედამხედველო ჯგუფი ფართო მანდატით და უფლებამოსილებებით სამსახურებზე ზედამხედველობისთვის. ამ ქვეყნებში, ომბუდსმენის ინსტიტუციები თამაშობენ მეორეხარისხოვან, ექსპერტთა საზედამხედველო ჯგუფის საქმიანობის შემავსებელ როლს. ამის გარდა, თითქმის ყველა ევროპულ ქვეყანაში ფუნქციონირებს პერსონალური ინფორმაციის დაცვის სააგენტოები (DPA), რომლებიც, გარკვეულ შემთხვევებში, უსაფრთხოების სამსახურების ადმინისტრაციული შენობების და მათი დოკუმენტების დათვალიერების ფუნქციებს კისრულობენ.[143] ასევე, ომბუდსმენის ინსტიტუტებს შესაძლოა არ ჰქონდეთ საკმარისი ცოდნა და რესურსი უსაფრთხოების სამსახურების მეტად კომპლექსურ და ტექნიკურ საქმიანობაზე ზედამხედველობისთვის.

ამის მიუხედავად, ეს არ ნიშნავს იმას, რომ ომბუდსმენის ინსტიტუციებს არ შეუძლიათ ან არ უნდა მიიღონ მონაწილეობა უსაფრთხოების სამსახურების ზედამხედველობაში. ქვემოთ წარმოდგენილია მაგალითები, როგორ შეიძლება მონაწილეობდნენ ომბუდსმენის ინსტიტუტები უსაფრთხოების სამსახურების ანგარიშვალდებულების უზრუნველყოფაში:

---

141 *The Paris Principles*, Principles 1-3, available from: http://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx

142 https://www.oikeusasiamies.fi/en_GB/web/guest/the-tasks-of-the-ombudsman

143 Mandate and powers of DPAs in the EU vary. Some countries entrust DPAs with powers to oversee security services, others exclude security services from the mandate of DPAs. See *EU FRA, Surveillance by Intelligence Services (2015), p.50*

- უსაფრთხოების სამსახურების საქმიანობის მარეგულირებელი კანონების და პოლიტიკის დოკუმენტების გადასინჯვა მათი საერთაშორისო ადამიანის უფლებების სტანდარტებთან შესაბამისობის შეფასების კუთხით. მთავრობის და პარლამენტის მისამართით ცვლილებებთან დაკავშირებით რეკომენდაციების გაცემა.

- უსაფრთხოების სამსახურების საქმიანობის სამართლებრივ საფუძვლებზე (მაგალითად ფარული ღონისძიებების შესახებ კანონმდებლობაზე) სასამართლოში დავების წარმოება,

- გამოძიების წარმოება (ინდივიდუალური საჩივრების ან უსაფრთხოების სამსახურების საქმიანობის თემატური მოკვლევის საფუძველზე); საჭიროების შემთხვევაში სხვა ზედამხედველობის აქტორებთნ თანამშრომლობა (ექსპერტთა ორგანოები, პერსონალური ინფორმაციის დაცვის სააგენტოები, სასამართლო ხელისუფლება);

- ცნობიერების ამაღლების ღონისძიებები/ადვოკატირება, რომელიც მიზნად ისახავს საზოგადოების ინფორმირებას, უსაფრთხოების სამსახურების საქმიანობის ფარგლებზე და ადამიანის უფლებებთან დაკავშირებულ პოტენციურ რისკებზე.[144]

144 For more information on ombuds institutions in overseeing security services, see Nazli Yildirim Schierkolk, Monitoring Security Services: A Guide for Ombuds Institutions (DCAF, forthcoming 2018).

შერჩეული ქვეყნების საუკეთესო პრაქტიკები:

ხორვატია

2006 წლიდან ხორვატიაში ფუნქციონირებს ერთი ექსპერტთა საზედამხედველო ორგანო დასახელებით „უსაფრთხოების და დაზვერვის სამსახურების სამოქალაქო ზედამხედველობის საბჭო“ (შემდგომში საბჭო). ხორვატიის რესპუბლიკის უსაფრთხოების და დაზვერვის სისტემის შესახებ კანონი[145] (შემდგომში კანონი) არეგულირებს მის მანდატს და უფლებამოსილებებს.

ინსტიტუციური წყობა: საბჭოს წევრებს ნიშნავს პარლამენტი და ის ანგარიშვალდებულია პარლამენტის წინაშე. შიდა პოლიტიკისა და ეროვნული უსაფრთხოების საპარლამენტო კომიტეტი ზედამხედველობს საბჭოს საქმიანობას (კანონის მუხლი 110). საბჭო პარლამენტის წინაშე ანგარიშს წარადგენს სპიკერის მოთხოვნის შემთხვევაში, ასევე რეგულარულად წელიწადში ორჯერ. მართალია ეს ინსტიტუციური წყობა საერთაშორისო სტანდარტებს შეესაბამება, თუმცა საუკეთესო პრაქტიკის მაგალითს არ წარმოადგენს, მაგალითად საბჭოს წევრებისთვის საპარლამენტო კომიტეტის წინასწარი თანხმობის გარეშე საჯარო განცხადებების აკრძალვა.[146] ასეთი წესი ქმნის საბჭოს პოლიტიკურ ორგანოზე არასასურველი დამოკიდებულების რისკებს, რომელიც მის დამოუკიდებლობას აზიანებს.

შემადგენლობა: საბჭოს შემადგენლობაში შედის თავჯდომარე და 6 წევრი, რომელთაც ხორვატიის პარლამენტი ნიშნავს, საჯარო კონკურსის შედეგად და კვალიფიკაციის საფუძველზე. საუკეთესო პრაქტიკის მაგალითია კანონის რეგულირება, რომლის თანახმად როგორც მინიმუმ საბჭოს ერთ წევრს უნდა ჰქონდეს იურიდიული განათლება, ასევე ერთს უნდა ჰქონდეს განათლება პოლიტიკურ, კიდევ ერთს კი ელექტრო/ტექნიკურ მეცნიერებებში (მუხლი 100). საბჭოს ვერც თავჯდომარე, ვერც წევრი ვერ იქნება პოლიტიკური პარტიის ლიდერი.[147] წევრებს კანონით ევალებათ დაიცვან ინფორმაციის კონფიდენციალობა, რომლებიც მათთვის საქმიანობის განხორციელების დროს გახდა ცნობილი (მუხლი 114).

მადნატი: საერთაშორისო სტანდარტებთან შესაბამისობაში, საბჭოს გააჩნია უსაფთხოების სამსახურების საქმიანობის კანონიერების შემოწმების, ასევე ფარული ღონისძიებების გამოყენების მონიტორინგის და ზედამხედველობის, ასევე უსაფრთხოების და სადაზვერვო სამსახურების უკანონო პროცედურებისა და მათი უკანონო საქმიანობის შესახებ საჩივრების მიღების და განხილვის მანდატი, განსაკუთრებით თუ აღნიშნული ადამიანის უფლებების და თავისუფლებების დარღვევაში გამოიხატება (მუხლი 112).

საბჭოს მანდატთან დაკავშირებულ პრობლემურ საკითხს წარმოადგენს შემდეგი: როდესაც ის ახორციელებს ხორვატიის უსაფრთხოების სამსახურის (SOA) მიერ ფარულ ღონისძიებებთან დაკავშირებული საქმიანობის მონიტორინგს, მას შეზღუდული მანდატი აქვს ტელეკომუნიკაციების მეთვალყურეობის ოპერატიული ტექნოლოგიის ცენტრზე (OTC), რომელიც რეალურად წარმოადგენს ფარული მიყურადების განმახორციელებელ ორგანოს. ეს იმის შედეგია, რომ OTC უსაფრთხოების სამსახურის ნაწილი არ არის, ის ცალკე ინსტიტუციაა, რომელსაც ეროვნული უსაფრთხოების საბჭო

145 https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

146 Gordan Bosanac, ‘Legal Update Report: Croatia’ National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.12

147 See Council for Civilian Oversight of Security and Intelligence Agencies, Fact Sheet, available from http://www.sabor.hr/0060

ზედამხედველობს, (მუხლი 8).

უფლებამოსილებები: საბჭო მისი მანდატის განხორციელებისას სარგებლობს უფლებამოსილებით დაიწყოს მოკვლევა საჩივრების და სხვა სახელმწიფო ორგანოს მოთხოვნის საფუძველზე. ამ პროცესში, საბჭომ შესაძლოა გადახედოს უსაფრთხოების სამსახურების ანგარიშებს და სხვა დოკუმენტებს და გაესაუბროს უსაფრთხოებისა და დაზვერვის სამსახურის ხელმძღვანელებს და სხვა მოხელეებს.[148] თუმცა, საბჭოს არ აქვს საკუთარი ინიციატივით მოკვლევის დაწყების უფლებამოსილება, რაც გულისხმობს არსებით ხარვეზს საერთაშორისო სტანდარტების თვალსაზრისით. მოკვლევის საფუძველზე, იმ შემთხვევაში თუ საბჭო დაადგენს უსაფრთხოების სამსახურის სამართლებრივ უსწორობას ან უკანონო საქმიანობას, ის ამის შესახებ აცნობებს პრეზიდენტს, პრემიერ მინისტრს, პარლამენტის სპიკერს და მთავარ პროკურორს (მუხლი 113).

ხორვატიის ომბუდსმენს უსაფრთხოების სამსახურების მიერ ადამიანის უფლებების შესაძლო დარღვევის ფაქტებზე ასევე აქვს მოკვლევის დაწყების უფლებამოსილება. მნიშვნელოვანია აღინიშნოს, რომ ომბუდსმენს (მათ შორის მის მოადგილეებს) საიდუმლო ინფორმაციაზე წვდომის მოსაპოვებლად სპეციალური შემოწმების გავლა არ ევალებათ.[149]

148 See Council for Civilian Oversight of Security and Intelligence Agencies, Fact Sheet

149 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.12

ბელგიის მაგალითი ექსპერტთა ზედამხედველობის ყველაზე განვითარებულ მოდელს წარმოადგენს, რომელსაც ორი სხვდასხვა ორგანო წარმოადგენს (ადმინისტრაციული კომისია და სპეციალური სამსახურების ზედამხედველობის მუდმივმოქმედი კომიტეტი - შემდგომში კომიტეტი I), რომელთაც უსაფრთოხების სამსახურების ზედამხედველობის ფართო მანდატი და უფლებამოსილებები გააჩნიათ.

ადმინისტრაციული კომისია: ორგანო, რომელიც შედგება სახელმწიფო პროკურორისა და ორი მოსამართლისგან, აღჭურვილია მანდატით შეამოწმოს უსაფრთხოების სამსახურების მიერ ინფორმაციის მოპოვების სპეციფიკური და საგამონაკლისო წესების გამოყენების კანონიერება და თანაზომიერება.[150] უსაფრთხოების სამსახურმა კომისიას უნდა მიაწოდოს სათანადოდ მოტივირებული, წერილობითი მოთხოვნა საგამონაკლისო ფარული ღონისძიებების გამოყენებამდე. ეს ღონისძიებები შესაძლოა განხორციელდეს მხოლოდ კომისიის მიერ თანხმობის გაცემის შემდეგ.[151] აქედან გამომდინარე, ბელგიური მოდელის ფარგლებში, ექსპერტთა საზედამხედველო ორგანო კვაზი სასამართლო ფუნქციით, პასუხისმგებელია ფარულ ღონისძიებებთან დაკავშირებით წინასწარი ნებართვის გაცემაზე.

მოქმედი სპეციალური სამსახურების ზედამხედველობის კომიტეტი: კომიტეტი I ერთ-ერთი პირველი იყო ექსპერტთა საზედამხედველო ორგანოებში, და ის არაერთხელ იქნა მოხსენიებული როგორც საუკეთესო პრაქტიკის მაგალითი.[152]

ინსტიტუციური წყობა: როგორც წინა ქვეთავში აღინიშნა, კომიტეტ I-ს ნიშნავს პარლამენტი, და ის ანგარიშს წარადგენს წარმომადგენლების პალატის შესაბამისი საპარლამენტო კომიტეტის წინაშე. საპარლამენტო კომიტეტი ზედამხედველობს კომიტეტის საქმიანობას ყოველწლიური ანგარიშების, ასევე გამოძიებების შესახებ სპეციალური ანგარიშების გადახედვის და ბიუჯეტის ხარჯვის მონიტორინგის გზით. თუმცა, ხორვატიის მოდელისგან განსხვავებით, კომიტეტ I-ს აქვს გამოძიების შესახებ ანგარიშების ნაწილობრივ ან სრულად გასაიდუმლოების თავისუფლება.[153] ეს საუკეთესო პრაქტიკას წარმოადგენს: მაშინ როდესაც ექსპერტთა ზედამხედველობის ორგანოს ზედამხედველობს საპარლამენტო კომიტეტი, ამ უკანასკნელს მასზე კონტროლის ბერკეტები მაინც არ აქვს. კომიტეტი I ავტონომიურია და თავად წყვეტს ინფორმაციის განსაჯაროების საკითხებს.

შემადგენლობა: კომიტეტი I შედგება ორი წევრისა და თავჯდომარისგან, მათ ნიშნავს პარლამენტი. საერთაშორისო სტანდარტთან შესაბამისობაში, ისინი შესაძლოა მეორე ვადითაც იქნენ არჩეული. თავჯდომარის პოზიციას იკავებს მოსამართლე. კომიტეტის ყველა თანამშრომელი გადის მაღალი დონის სპეციალურ შემოწმებას.

რესურსები: კომიტეტ I -ს საქმიანობაში ეხმარება 15 თანამშრომელი და მდივანი, რომლებიც პასუხისმგებელი არიან კომიტეტის ადმინისტრაციულ საქმიანობაზე, დოკუმენტების საიდუმლოების დაცვაზე და მათ დაარქივებაზე ისევე როგორც ადამიანური რესურსების საკითხებზე. საუკეთესო პრაქტიკას წარმოადგენს ის, რომ კომიტეტს გამოძიების 5-კაციანი საკუთარი ჯგუფი ჰყავს, რომელთაც

150 EU FRA Surveillance by Intelligence Services (2015), p.43
151 EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.94
152 Except otherwise indicated, all information in this section is retrieved from the official website of the Committee: http://www.comiteri.be/index.php/en/standing-committee-i/competences
153 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.20

აქვთ საპოლიციო უფლებამოსილებები უსაფრთხოების სამსახურებთან დაკავშირებული საქმეების მოკვლევისას. ამის გარდა, კომიტეტი I სარგებლობს შესაძლებლობით კონკრეტული საგამოძიებო ღონისძიებების ან დავალებების შესასრულებლად განსაზღვრული დროით დაიქირავოს ექსპერტები. მაგალითად, სნოუდენის მიერ ინფორმაციის გამჟღავნების შემდეგ, კომიტეტმა გარე ექსპერტი მოიწვია მოკვლევის ჩასატარებლად.[154]

მანდატი*:* კომიტეტი I პასუხისმგებელია როგორც „სახელმწიფო უსაფრთხოების სამსახურის“ (სამოქალაქო უსაფრთხოების სამსახური) ისე ზოგადი დაზვერვის და უსაფრთხოების სამსახურის (სამხედრო სადაზვერვო სამსახური) საქმიანობის ზედამხედველობაზე. მთლიანობაში, ის ფართო მანდატით სარგებლობს, რომელიც უკავშირდება კანონიერებაზე (რელევანტურ კანონმდებლობასთან და რეგულაციებთან შესაბამისობა), ეფექტიანობაზე (სპეციალური სამსახურების საქმიანობის ეფექტიანობა) და კოორდინირებაზე (უსაფრთხოების სამსახურების საქმიანობის ორმხრივი ჰარმონიზაცია) ზედამხედველობას. მისი ფართო მანდატის ფარგლებში, ის ასრულებს შემდეგ სპეციფიკურ ფუნქციებს:

- მოთხოვნის საფუძველზე, ის გადახედავს და სამართლებრივ დასკვნას გამოსცემს უსაფრთხოების სამსახურების საქმიანობის მარეგულირებელ კანონებთან და პოლიტიკის დოკუმენტებთან დაკავშირებით. ამის გარდა, ის ასევე სპეციალური სამსახურების მიერ სისხლის სამართლის საქმეზე გამოყენებული ინფორმაციის მოპოვების კანონიერების შესახებ სასამართლოში წარადგენს წერილობით მოსაზრებებს

- მიზანმიმართულ ფარულ ღონისძიებებზე შემდგომ კონტროლს ახორციელებს, როდესაც ადმინისტრაციული კომისია პასუხისმგებელია წინასწარი ნებართვის გაცემაზე.

- ზედამხედველობს სტრატეგიულ ფარულ მეთვალყურეობას, რომელსაც სამხედრო დაზვერვის სამსახური საზღვარგარეთ ატარებს. უნდა აღინიშნოს, რომ მხოლოდ რამდენიმე ზედამხედველობის ორგანოს აქვს მკაფიო მანდატი ქვეყნის ფარგლებს გარეთ განხორციელებული სტრატეგიული მეთვალყურეობის ზედამხედველობის ნაწილში. ამის გარდა, კომიტეტი ასევე ზედამხედველობს სპეციალური სამსახურების თანამშრომლობას უცხოელ კოლეგებთან, რაც ინოვაციურ მიდგომას წარმოადგენს ექსპერტთა ზედამხედველობის ორგანოებისთვის.

- საჩივრების, პარლამენტის ან სასამართლო ხელისუფლების მოთხოვნის საფუძველზე, აწარმოებს მოკვლევას, მათ შორის სამსახურების წარმომადგენლების წინააღმდეგ, რომელთაც ადმინისტრაციული სამართალდარღვევის (misdemeanor) ან სისხლის სამართლის დანაშაულის (felony) ჩადენაში ედებათ ბრალი.

- ასრულებს საჩივრის განმხილველი ორგანოს ფუნქციას სპეციალური შემოწმების საქმეებზე.

უფლებამოსილებები: ზემოაღწერილი ფართო მანდატის განხორციელებისთვის, კომიტეტს აქვს შემდეგი ექსკლუზიური უფლებამოსილებები.

- კომიტეტი სარგებლობს <u>თითქმის შეუზღუდავი წვდომით ინფორმაციაზე,</u> მათ შორის ინფორმაციაზე, რომელიც ეხება მიმდინარე სპეციალურ ოპერაციებს (რაც როგორც წესი გამონაკლისს წარმოადგენს საზედამხედველო ორგანოების უფლებამოსილებების კონტექსტში). კომიტეტის დაუბრკოლებელი წვდომა ინფორმაციაზე კიდევ ერთი უფრო მყარია აღმასრულებელი ხელისუფლების კანონით დავალდებულებით შიდა წესების და დირექტივების შესახებ ინფორმაცია, ასევე სამსახურების

154 Ibid. p.11

წარმომადგენლების ქცევის მარეგულირებელი ყველა დოკუმენტები პროაქტიულად გაუზიაროს მას. რაც კიდევ უფრო მეტ ყურადღებას იმსახურებს, კომიტეტს აქვს საკუთარი მოწყობილობები სპეციალური სამსახურების ადმინისტრაციულ შენობებში, რაც მას უსაფრთხოების სამსახურების ბაზებზე პირდაპირი წვდომის შესაძლებლობას აძლევს.[155] ბელგია ერთ-ერთია იმ ორი ევროპული ქვეყნიდან, რომლებმაც ექსპერტთა საზედამხედველო ორგანოს ეს განსაკუთრებული უფლებამოსილება მიანიჭა.

- საუკეთესო პრაქტიკის მაგალითია ის, რომ კომიტეტს აქვს საკუთარი ინიციატივით მოკვლევის დაწყების უფლებამოსილება. ამ უფლებამოსილების განხორციელებისას, კომიტეტი სარგებლობს სასამართლო ხელისუფლების უფლებამოსილებებით, მათ შორის ნებისმიერი პირის, განსაკუთრებით კი სპეციალური სამსახურების თანამშრომლების დაბარების, ნებისმიერ ადგილზე საგნის ან დოკუმენტის ამოღების, პოლიციელების და ექსპერტების დახმარების მოთხოვნის უფლებამოსილებებით.

- ფარულ ღონისძიებებზე ზედამხედველობის განხორციელებისას, კომიტეტს შეუძლია:

  - შეცვალოს ადმინისტრაციული კომისიის დადებითი გადაწყვეტილება ფარული ღონისძიების მოთხოვნის შესახებ[156] ან

  - თუ კომიტეტი დაადგენს, რომ უსაფრთხოების სამსახურებმა დაარღვიეს კანონი, პირის მიმართ ფარული მეთვალყურეობის ღონისძიების გამოყენებისას, მას აქვს ფარული ღონისძიების შეწყვეტის მოთხოვნის უფლებამოსილება.[157]

ომბუდსმენის ინსტიტუციები: იქიდან გამომდინარე, რომ ბელგიაში ფუნქციონირებს ორი ძლიერი ექსპერტთა ზედამხედველობის ორგანო, ბელგიის ომბუდსმენი მეორეხარისხოვან როლს ასრულებს ზედამხედველობის სისტემაში. მას აქვს მანდატი მიიღოს და განიხილოს საჩივრები. ომბუდსმენის კიდევ ერთი მნიშვნელოვანი ფუნქციაა საჩივრების შეფასება, და არარელევანტური, მცირე მნიშვნელობის და უსაფუძვლო საჩივრების გაცხრილვა. ომბუდსმენი მხოლოდ დასაბუთებულ საჩივრებს უგზავნის კომიტეტ I-ს, რომელიც მათ განხილვაზეა პასუხისმგებელი. ზედამხედველობის ორგანოებს შორის ასეთი თანამშრომლობა მიზნად ისახავს ანგარიშვალდებულების სისტემის ეფექტიანობის გაზრდას. [158]

155 Aidan Wills and Mathias Vermeulen, Parliamentary Oversight of Security and Intelligence Agencies in the European Union (2011), p.134

156 EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.94

157 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.17

158 EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.132

1984 წლიდან კანადაში ფუნქციონირებს უსაფრთხოების დაზვერვის საზედამხედველო კომიტეტი[6159](შემდგომში SIRC) კანადის უსაფრთხოების სადაზვერვო საქმიანობის შესახებ კანონის საფუძველზე (შემდგომში კანონი). The SIRC-ს ხშირად განიხილავენ სხვადასხვა ევროპული ქვეყნებისთვის ექსპერტთა საზედამხედველო ორგანოების შექმნის მოტივაციად.[160]

ინსტიტუციური წყობა: SIRC არის დამოუკიდებელი ზედამხედველობის ორგანო, რომელსაც ნიშნავს აღმასრულებელი ხელისუფლება. ის ყოველწლიურად ანგარიშს პარლამენტს წარუდგენს. ანგარიშები შეიცავენ SIRC -ის მიგნებების და რეკომენდაციების მიმოხილვას, ასევე კანადის უსაფრთხოების დაზვერვის სამსახურის პასუხებს ამ რეკომენდაციებზე, ისეთი სახით, რომ ისინი არ შეიცავენ გასაიდუმლოებულ ინფორმაციას.

შემადგენლობა: SIRC შედგება ხუთი წევრისგან, რომელთაც ხელმღვანელობს აღმასრულებელი დირექტორი. ევროპული მოდელისგან განსხვავებით, ყველა წევრს ნიშნავს საბჭოში მმართველი (GIC - პოზიცია აღმასრულებელი ხელისუფლების ფარგლებში), პრემიერ მინისტრთან და ოპოზიციური პარტიების ლიდერებთან კონსულტაციის შემდგომ. კანონის თანახმად, SIRC - ის წევრები არ შეიძლება იყვნენ მოქმედი სენატორები ან პარლამენტის წევრები. საერთაშორისო სტანდარტებთან შესაბამისობაში, წევრებს აქვთ წინასწარ განსაზღვრული თანამდებობის დაკავების ხუთწლიანი ვადა, მეორე ვადით არჩევის შესაძლებლობით (კანონის მუხლი 34). კომიტეტის ყველა წევრი და თანამშრომელი შებოჭილი არიან მუდმივი საიდუმლო ინფორმაციის გაუთქმელობის ვალდებულებით.

რესურსები: კომიტეტის საქმიანობას სრულ განაკვეთზე დასაქმებული მკვლევარების და იურისტების ჯგუფი უწევს მხარდაჭერას. თუმცა, კანონი არ განსაზღვრავს გარე ექსპერტების დაქირავების შესაძლებლობას კომპლექსური, ტექნიკური მოკვლევისთვის. იქიდან გამომდინარე, რომ კომიტეტი მუდმივად მზარდ უსაფრთხოების სამსახურებთან შედარებით პატარა უწყებაა, SIRC ატარებს რისკების შეფასების ღონისძიებებს ზედამხედველობის პრიორიტეტების დადგენისათვის.

მანდატი: ბელგიური მოდელისგან განსხვავებით, SIRC-ისმანდატი ვრცელდება მხოლოდ ერთ სააგენტოზე, სამოქალაქო უსაფრთხოების სამსახურზე. მას ფართო მანდატი გააჩნია, ის მათ შორის ზედამხედველობს სამსახურის საქმიანობის შესაბამისობას კანონთან, პოლიტიკის დოკუმენტებთან და შიდა რეგულაციებთან, მისი საქმიანობის შესწავლისა და საჩივრების გამოძიების საშუალებით. ამის გარდა, კანონი SIRC-ს ანიჭებს მკაფიო მანდატს გადახედოს ინფორმაციის გაცვლის საერთაშორისო ხელშეკრულებებს, რაც საუკეთესო პრაქტიკის მაგალითს წარმოადგენს.

უფლებამოსილებები: საერთაშორისო სტანდარტებთან შესაბამისობაში, SIRC აქვს თითქმის სრული წვდომა ინფორმაციაზე. ამასთან მიმართებით, კანონი იყენებს შემდეგ ფორმულირებას 'ნებისმიერი ინფორმაცია, რომელსაც SIRC მისი ფუნქციებისა და მოვალეობების შესრულებისთვის საჭიროდ მიიჩნევს' (მუხლი 39(2)) მიუხედავად იმისა, რამდენად სენსიტიური ან გასაიდუმლოებული შეიძლება იყოს ეს ინფორმაცია'. ამ კუთხით, ერთადერთ გამონაკლისს წარმოადგენს მინისტრებს შორის არსებული კომუნიკაცია. SIRC - ის წვდომა ინფორმაციაზე კიდევ ერთი უფრო მყარია უსაფრთხოების სამსახურის და სამინისტროს კანონით დავალდებულებით პროაქტიულად გაუზიაროს მას დოკუმენტები, მათ შორის, შიდა ოპერაციულ გაიდლაინებში, პოლიტიკის დოკუმენტებში შეტანილი ცვლილებები, და

159 Unless otherwise indicated, the information in this section is retrieved from: http://www.sirc-csars.gc.ca/abtprp/index-eng.html

160 Venice Commission, Democratic Oversight of the Security Services, (2007), para 220

ნებისმიერი დოკუმენტი, რომელიც გაეგზავნა მთავარ პროკურატურას სამსახურის მოხელის უკანონო ქმედების შესახებ.

საერთაშორისო სტანდარტებთან შესაბამისობაში, SIRC - ის აქვს უფლებამოსილება საკუთარი ინიციატივით ან საჩივრებზე დაყრდნობით დაიწყოს საქმის შესწავლა და მოკვლევა. გამოძიების წარმოებისას, SIRC-ს აქვს სასამართლოსთვის დამახასიათებელი უფლებამოსილებები, როგორიცაა პირთა დაბარება და მათი გამოცხადების უზრუნველყოფა, წერილობითი დოკუმენტების და მტკიცებულებების გამოთხოვა, ფიცის დადების და სხვა პროცედურების ადმინისტრირება (მუხლი 50). SIRC -ის კიდევ ერთი მნიშვნელოვანი უფლებამოსილებაა, უსაფრთხოების სამსახურისთვის 'მითითება' სამსახურის საქმიანობას გადახედოს და შესწავლის შედეგები წარუდგინოს კომიტეტს.

ომბუდსმენის ინსტიტუციები: კანადის ადამიანის უფლებების კომისიის მანდატი ფედერალურ დონეზე მოიცავს ყველა ფედერალური უწყების, მათ შორის უსაფრთხოების სამსახურების წინააღმდეგ, საჩივრების განხილვის უფლებამოსილებას. კანონი მოკვლევის განხორციელებისას SIRC - ის ანიჭებს ადამიანის უფლებების კომისიასთან თანამშრომლობის შესაძლებლობას, რაც ასევე საუკეთესო პრაქტიკის მაგალითია. რეგიონულ დონეზე მომუშავე ომბუდსმენის ინსტიტუციები ასევე აქტიურები არიან პირადი ცხოვრების უფლების, პერსონალური მონაცემების დაცვის და სამთავრობო ორგანოების გამჭვირვალობის საკითხებზე ცნობიერების ამაღლების კუთხით.[161]

161 See for instance the Manitoba Ombudsman http://www.theioi.org/ioi-news/current-news/ombudsman-celebrates-right-to-know-week

2016 წლის ბოლო პერიოდში, გერმანიამ უსაფრთხოების სამსახურების ზედამხედველობის სისტემის გასაძლიერებლად სამართლებრივი ჩარჩოს რეფორმა განახორციელა. დამატებით, საერთაშორისო დონეზე აღიარებული ექსპერტთა საზედამხედველო ჯგუფთან **G-10 კომისიასთან** ერთად, ახალმა კანონმა ჩამოაყალიბა მეორე ექსპერტთა საზედამხედველო ჯგუფი **დამოუკიდებელი კომიტეტი** (Unabhängiges Gremium), რომელსაც კონკრეტულად ქვეყნებს შორის კომუნიკაციის ფარულ მეთვალყურეობაზე ზედამხედველობა დაევალა. ეს ქვეთავი ძირითადად ყურადღებას გაამახვილებს G-10 კომისიაზე, და საჭიროების შემთხვევაში, შეეხება დამოუკიდებელ კომიტეტსაც.

ინსტიტუციური წყობა: G-10 კომისია წარმოადგენს ექსპერტთა საზედამხედველო ჯგუფს, რომელსაც ნიშნავს გერმანიის საპარლამენტო ზედამხედველობის კომიტეტი, საპარლმენტო კონტროლის ჯგუფი (G-10 კანონი[162], მუხლი 15/ 1). მართალია, კანონი განსაზღვრავს, რომ G-10 კომისია და საპარლამენტო კონტროლის ჯგუფი რეგულარულად ცვლის ინფორმაციას, არ არსებობს G-10 კომისიის სამართლებრივი ვალდებულება ანგარიში წარუდგინოს საპარლამენტო კონტროლის ჯგუფს. დამოუკიდებელ კომიტეტს ნიშნავს ფედერალური მთავრობა და ის მდებარეობს ფედერალურ მართლმსაჯულების სასამართლოში, თუმცა ის ასევე წელიწადში ორჯერ საპარლამენტო კონტროლის ჯგუფს წარუდგენს ანგარიშს (BND კანონის[163] მუხლი 16(6)).

შემადგენლობა: G-10 კომისია შედგება ოთხი წევრისგან, მათ ნიშნავს საპარლამენტო კონტროლის ჯგუფი ფედერალურ მთავრობასთან კონსულტაციის შედეგად (G-10 კანონის მუხლი 15/ 1). საერთაშორისო სტანდარტებთან შესაბამისობაში, თავჯდომარეს უნდა ჰქონდეს მოსამართლის პოზიციისთვის განსაზღვრული კვალიფიკაცია. კანადის მოდელისგან განსხვავებით, აქ არ არსებობს შეზღუდვა მოქმედ პარლამენტის წევრებთან მიმართებით; ისინი შესაძლოა დაინიშნონ G10 კომისიის წევრებად. დამოუკიდებელი კომიტეტი შედგება სამი წევრისგან, ორი ფედერალური მოსამართლისგან და ერთი პროკურორისგან, რომელთაც ფედერალური მთავრობა ნიშნავს, მართლმსაჯულების ფედერალური სასამართლოს და მთავარი პროკურორის რეკომენდაციის საფუძველზე.[164]

რესურსები: G-10 კომისიას მხარდაჭერას უწევს სამდივნო სრულ განაკვეთზე დასაქმებული თანამშრომლებით, რომელთა რიცხვი უკანასკნელი რეფორმის ფარგლებში 6-დან 13-მდე გაიზარდა.[165] როგორც კომისიის წევრებს, ისე თანამშრომლებს აქვთ კონფიდენციალობის დაცვის ვალდებულება, მათი თანამდებობის დაკავების ვადის გასვლის/სამსახურის დატოვების შემდგომაც, რაც გავრცელებულ პრაქტიკას წარმოადგენს;

მანდატი: როგორც G-10 კომისიის ასევე დამოუკიდებელი კომიტეტის მანდატი ვრცელდება ფარული ღონისძიებების ზედამხედველობაზე. G-10 კომისიის მანდატი ვრცელდება როგორც ყველა შიდა კომუნიკაციის მიყურადებაზე, ასევე ყველა სხვა კომუნიკაციაზე, რომელიც იწყება ან სრულდება გერმანიაში. ამ კონტექსტში, G-10 კანონის შესაბამისად, G-10 კომისია ასრულებს 3 ძირითად ფუნქციას:

- ფარულ ღონისძიებებზე წინასწარი თანხმობის გაცემა: უსაფრთხოების სამსახურები ფარული ღონისძიებების შესახებ მოთხოვნას წარუდგენენ შინაგან საქმეთა სამინისტროს.

162 https://www.gesetze-im-internet.de/g10_2001/index.html
163 https://www.gesetze-im-internet.de/bndg/
164 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.7
165 Ibid., p.18

თუ სამინისტრო თანხმობას გასცემს აღნიშნულ მოთხოვნაზე, ის გამოსცემს ორდერს და მას თანხმობის მისაღებად G-10 კომისიას წარუდგენს. სტრატეგიული (მასობრივი) ფარული ღონისძიებებისთვის, G-10 კომისია გადახედავს საძიებო სიტყვას (სელექტორი), ინფორმაციის მოპოვების გეოგრაფიულ არეალს, საკომუნიკაციო არხებს და კომუნიკაციების მაქსიმალურ მასშტაბს, რომლის მიყურადებაც იგეგმება. მხოლოდ G-10 კომისიის თანხმობის შემდეგ, იქნება ფარული მეთვალყურეობის ღონისძიების განხორციელება დაშვებული (გარდა გადაუდებელი გარემოებებისა რომელიც G-10 კანონით განისაზღვრება).[166] ეს ფუნქცია G-10 კომისიას კვაზი-სასამართლო ორგანო აქცევს.

- უსაფრთხოების სამსახურების მიერ პერსონალური ინფორმაციის შეგროვების, დამუშავების და გამოყენების სრული პროცესის ზედამხედველობა; და
- სამსახურების წინააღმდეგ საჩივრების მიღება და განხილვა ფარულ ღონისძიებებთან და პერსონალური ინფორმაციის დაცვასთან მიმართებით;

მეორე მხრივ, დამოუკიდებელ კომიტეტს აქვს BND-ის მიერ სრულად ქვეყნის გარეთ განხორციელებული კომუნიკაციის მიყურადების კანონიერებისა და საჭიროების ზედამხედველობის ფუნქცია.[167] ამ კონტექსტში, კომიტეტს აქვს წინასწარი კონტროლის ფუნქცია, რადგან ის თანხმობას გასცემს სრულად ქვეყნის გარეთ განხორციელებული კომუნიკაციის მიყურადებისას გამოყენებულ 'სელექტორებზე'.[168] გერმანია ერთ-ერთი პირველი ქვეყანაა, რომელმაც კომპლექსური სამართლებრივი ჩარჩო შექმნა უცხოეთში განხორციელებულ ფარულ მიყურადებასთან მიმართებით და ცალკე ექსპერტთა ჯგუფი დააფუძნა ექსკლუზიურად ასეთ ღონისძიებებზე ზედამხედველობისთვის.

უფლებამოსილებები: მისი მანდატის ეფექტურად განხორციელებისთვის, G-10 კომისიას მინიჭებული აქვს ფართო უფლებამოსილებები ყველა დოკუმენტზე, ინფორმაციაზე წვდომის სახით (მათ შორის ინფორმაციის ბაზებსა და ფარული ღონისძიებებისთვის გამოსაყენებლ კომპიუტერულ პროგრამებზე), რასაც კომისია მის მიერ ჩატარებული მოკვლევისთვის რელევანტურად მიიჩნევს; ამის გარდა კომისიას აქვს შესაძლებლობა ნებისმიერ დროს შევიდეს უსაფრთხოების სამსახურების ადმინისტრაციულ შენობებში. (G10 კანონის მუხლი 15/5). მისი სასამართლო ფუნქციების ფარგლებში, G-10 კომისიას აქვს შესასრულებლად სავალდებულო გადაწყვეტილებების მიღების უფლებამოსილება. მაგალითად, ბელგიის მუდმივმოქმედი კომიტეტი I-ის მსგავსად, თუ G-10 კომისია დაადგენს, რომ ფარული ღონისძიებების განსახორციელებლად სამართლებრივი წინაპირობები არ შესრულებულა, მას შეუძლია ღონისძიება უკანონოდ გამოაცხადოს, და მისი დაუყოვნებლივი შეწყვეტა მოითხოვოს.[169]

ომბუდსმენის ინსტიტუციები: გერმანიაში ფედერალურ დონეზე არ ფუნქციონირებს ომბუდსმენის ტიპის ინსტიტუტი. თუმცა, პარლამენტის საჩივრების კომიტეტი ომბუდსმენის მსგავს ფუნქციას ასრულებს და ყველა ფედერალური უწყების საქმიანობასთან დაკავშირებით იღებს საჩივრებს. ბელგიის ომბუდსმენის მსგავსად, საჩივრების კომიტეტი ასრულებს ფილტრის ფუნქციასაც, და დასაბუთებული საფუძვლებით წარდგენილ საჩივრებს მოკვლევისთვის უგზავნის საპარლამენტო კონტროლის ჯგუფს. ჯგუფს აქვს უფლებამოსილება თავად გამოიძიოს საჩივრები ან ისინი G-10 კომისიას გაუგზავნის,

166 Thorsten Wetzling, SNV Policy Brief: 'The Key to Intelligence Reform in Germany- Strengthening the G-10 Commission's role to authorize strategic surveillance' 2016, p.9 available from: : https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency/publikationen

167 EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.67

168 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.7

169 Aidan Wills and Mathias Vermeulen, Parliamentary Oversight of Security and Intelligence Agencies in the European Union (2011), p.223

განსაკუთრებით თუ ის ტექნიკურ ცოდნას მოითხოვს.[170]

3.3 უსაფრთხოების სამსახურების სასამართლო ზედამხედველობა

სასამართლო ზედამხედველობა არის ანგარიშვალდებულების სისტემის განუყოფელი ნაწილი. საერთაშორისო აქტორები, მათ შორის გაეროს სპეციალური მომხსენებლები, ევროპის საბჭოს ვენეციის კომისია და ადამიანის უფლებების კომისარი, ისევე როგორცევროკავშირი ადასტურებენ უსაფრთხოების სამსახურების სასამართლო ზედამხედველობის მნიშვნელობასა და აუცილებლობას. მის პრეცედენტულ გადაწყვეტილებაში, ადამიანის უფლებათა ევროპული სასამართლო აღნიშნავს:

> "კანონის უზენაესობა გულისხმობს, მათ შორის, ადამიანის უფლებებში აღმასრულებელი ხელისუფლების მხრიდან ჩარევის შემთხვევაში, ეფექტური კონტროლის აუცილებლობას, რაც როგორც წესი უნდა განხორციელდეს სასმართლოს მეშვეობით, როგორც მინიმუმ უფლების დაცვის საბოლოო მექანიზმის სახით, რადგან სასამართლო კონტროლი დამოუკიდებლობის, მიუკერძოებლობისა და სათანადო პროცედურების კუთხით, საუკეთესო გარანტიებს შეიცავს."[171]

მსგავსად, ევროსაბჭოს ვენეციის კომისია განმარტავს:

> "სასამართლო წინასწარი კონტროლის გარანტიები უსაფრთხოების საკითხებს კანონს უქვემდებარებს, და შესაბამისად კანონის დაცვის ინსტიტუციონალიზებას ახდენს."[172]

მართალია, სხვადასხვა ქვეყნებში სასამართლო ხელისუფლების ჩართულობის ფარგლები განსხვავებულია, თუმცა ძირითად შემთხვევაში მისი ფუნქცია მდგომარეობს უსაფრთხოების სექტორის ადამიანის უფლებების შემზღუდველი საქმიანობის წინასწარ კონტროლში (ნებართვის გაცემა), ასევე სამსახურების წინააღმდეგ წარდგენილი საჩივრების განხილვასა და უფლების აღმდეგნი საშუალების მინიჭებაში. ამ ძირითადი ფუნქციების გარდა, ზოგიერთ ქვეყანაში სასამართლო ხელისუფლება ასევე ჩართულია მიმდინარე ფარული ღონისძიებების ზედამხედველობაში. თუმცა, ევროკავშირის ადამიანის ძირითადი უფლებების სააგენტოს მიერ ჩატარებული შედარებითი კვლევის თანახმად, მიმდინარე ფარულ ღონისძიებებზე სასამართლო ხელისუფლების მზედამხედველობა გავრცელებული პრაქტიკა არ არის, უმეტესობა წევრი ქვეყნები ცალკე დამოუკიდებელ ზედამხედველობის ორგანოს ანიჭებენ ამ ფუნქციას. [173]

ინფორმაციის შეგროვების მეთოდებზე წინასწარი ნებართვის გაცემა:

უსაფრთხოების სამსახურები ინფორმაციის შეგროვებისთვის რამდენიმე მეთოდს იყენებენ, მათ შორის ფარული აგენტების ჩანერგვის ღონისძიებებს, კომუნიკაციების ფარულ მეთვალყურეობას (საფოსტო, სატელეფონო და ელექტრონული კომუნიკაციები), ჰაკერობისა და უკვე არსებულ მონაცემთა ბანკებში ძებნის შედეგად პირდაპირ წვდომას მონაცემებზე. უმეტესობა ევროსაბჭოს წევრ ქვეყანაში, სასამართლო ხელისუფლება *ყველა* ამ ღონისძიებაზე წინასწარ ნებართვას არ გასცემს, ამის ნაცვლად კომუნიკაციების ფარულ მეთვალყურეობაზე კონცენტრირდება. [174]

- *<u>მიზანმიმართულ ფარულ მიყურადებაზე წინასწარი ნებართვის გაცემა:</u>* კომუნიკაციების მიზანმიმართული ფარული მიყურადება უკიდურეს ზომას წარმოადგენს, რომელიც მნიშვნელოვან

170 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.21

171 Klass v. FRG http://hudoc.echr.coe.int/eng?i=001-57510 para 55

172 Venice Cmmission, *Democratic Oversight of the Security Services* (2007) para 204

173 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.97*

174 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.54

გავლენას ახდენს პირადი ცხოვრების უფლებაზე. აქედან გამომდინარე, უმრავლესობა ევროკავშირის და ევროპის საბჭოს ქვეყნებში, სასამართლო ხელისუფლება პასუხისმგებელია მიზანმიმართულ ფარულ ღონისძიებებთან დაკავშირებით ნებართვის გაცემაზე.[175]დანარჩენი სახელმწიფოები აღნიშნულ უფლებამოსილებას ან კვაზი სასამართლო ექსპერტთა ორგანოს (მაგალითად გერმანია, ბელგია, იხილეთ ქვემოთ) ან აღმასრულებელ ხელისუფლებას ანიჭებენ. სასამართლოს მიერ ნებართვის გაცემის მექანიზმის მთავარი არსი მდგომარეობს იმაში, რომ ასეთი ღონისძიებების კანონიერების, აუცილებლობის და პროპორციულობის შესაფასებლად მოსამართლეები ყველაზე შესაბამის პოზიციაში არიან. თუმცა, საერთაშორისო სტანდატები სასამართლო წინასწარი კონტროლის ეფექტიანობის უზრუნველყოფასაც მიემართებიან:

- <u>ღონისძიებებზე ნებართვის მოთხოვნის შესახებ შუამდგომლობები:</u> როგორც წესი, უსაფრთხოების სამსახურები ადგენენ შუამდგომლობას ფარულ ღონისძიებებზე ნებართვის მოთხოვნის შესახებ, რომელიც შემდგომში ეგზავნება სასამართლოებს. იმის უზრუნველსაყოფად, რომ მოსამართლეებმა შეძლონ ეფექტიანი ზედამხედველობის განხორციელება, შუამდგომლობები უნდა შეიცავდეს, როგორც მინიმუმ:
  - ინფორმაციას ფარული ღონისძიების სუბიექტის/სამიზნის, მეთვალყურეობის მოწყობილობის და ადგილმდებარეობის შესახებ;
  - მეთვალყურეობის აუცილებელ ხანგრძლივობას (საუკეთესო პრაქტიკის მაგალითია კანონმდებლობით შეზღუდვების პირდაპირ განსაზღვრა. ხანგრძლივობა განსხვავდება ქვეყნებში, სადაც ის რეგულირდება და მერყეობს 10 დღიდან 3 თვემდე)
  - ფარული ღონისძიებების გამოყენების დასაბუთებას (მითითებები იმასთან დაკავშირებით, თუ ნაკლებად მზღუდავი საშუალებები რატომ ვერ იქნება გამოყენებული)[176]
- <u>მოსამართლეების ცოდნა/კვალიფიკაცია:</u> სასამართლო ზედამხედველობის ეფექტიანობა დიდ წილად დამოკიდებულია მოსამართლეების სპეციალურ ცოდნაზე სახელმწიფო უსაფრთხოების რისკების შეფასების, ასევე ადამიანის უფლებებში ჩარევასთან მიმართებით ამ რისკების დაბალანსების კუთხით.[177] როდესაც საერთო სასამართლოებს აქვთ წინასწარი ნებართვის გაცემის უფლებამოსილება, მოსამართლეებმა, რომლებიც არ არიან გამოცდილი ასეთ საკითხებში, შესაძლოა ვერ შეძლონ სამსახურების მიერ წარდგენილი შუამდგომლობების კრიტიკულად შეფასება.[178] აქედან გამომდინარე, საერთაშორისო საუკეთესო პრაქტიკები რეკომენდაციას იძლევიან, რომ მაღალი რანგის მოსამართლემ ან მოსამართლეთა ჯგუფმა განიხილონ ნებართვის მოთხოვნის შესახებ შუამდგომლობები. მაგალითისთვის, პორტუგალიაში, ნებართვას გასცემს მოსამართლეთა ჯგუფი, რომელიც უზენაესი სასამართლოს სისხლის სამართლის ყველა პალატის პრეზიდენტებისგან და მაგისტრატების უმაღლესი საბჭოს მიერ დანიშნული მოსამართლისგან შედგება.[179] კიდევ ერთი საუკეთესო სტანდარტია, მოსამართლეების გადამზადება ნებართვის გაცემის პროცედურებსა და ფარულ ღონისძიებებზე.[180]
- <u>დასაბუთებული გადაწყვეტილებები:</u> როდესაც მოსამართლეები საკმარის ცოდნას და

175 In 19 out of 28 EU member states, the judiciary is in charge. See *EU FRA Surveillance by Intelligence Services Vol 2.*, p.95. For CoE countries, see Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015),, p.53

176 UNODC, 'Current practices in electronic surveillance in the investigation of serious and organized crime' (New York, 2009, p.17

177 Venice Commission, *Democratic Oversight of the Security Services,* (2007), para 15 ;

178 Council of Europe, *Democratic and Effective Oversight of National Security Services,* (2015), p.55

179 *EU FRA, Surveillance by Intelligence Services Vol 2. (2017)*, p. 96

180 Venice Commission, *Democratic Oversight of the Security Services,* 2007, para 211

გამოცდილებას არ ფლობენ სახელმწიფო უსაფრთხოების და ადამიანის უფლებების საკითხებზე, მათ შესაძლოა ავტომატურად დააკანონონ უსაფრთხოების სამსახურების შუამდგომლობები. იგივე ტენდენცია იკვეთება აღმასრულებლისგან სასამართლოს დამოუკიდებლობის პრობლემების შემთხვევაში. მნიშვნელოვანი გარანტია ასეთი ავტომატური ფორმალური კონტროლის წინააღმდეგ არის თითოეულ მოთხოვნაზე დასაბუთებული გადაწყვეტილების გამოცემის დავალდებულება, რაც საქმის გადაწყვეტისთვის მოსამართლეების მხრიდან ნებართვის გაცემამდე შუამდგომლობის გულმოდგინედ შესწავლასა და შეფასებას უზრუნველყოფს.[181]

- <u>ადვოკატების სპეციალური შემოწმება:</u> ნებართვის გაცემის პროცედურა თავისი არსით წარმოადგენს სასამართლოს ერთი მხარის მონაწილეობით, კერძოდ ამ დროს ის მეორე მხარის (ღონისძიების სამიზნე) მონაწილეობის გარეშე, ერთი მხარის (უსაფრთხოების სამსახური) მიერ წარდგენილი შუამდგომლობის საფუძველზე ტარდება. აქედან გამომდინარე, მოსამართლისთვის გამოწვევას წარმოადგენს მიუკერძოებელი გადაწყვეტილების მიღებაც. ადამიანის უფლებების დაცვის კუთხით ახალ იმედისმომცემ საერთაშორისო პრაქტიკას წარმოადგენს ნებართვის გაცემის პროცედურებში იმ ადვოკატის ჩართვა, რომელსაც სპეციალური შემოწმება აქვს გავლილი და წარმოადგენს ფარული ღონისძიებების მომავალი სამიზნის ინტერესებს. ადვოკატს შეუძლია კითხვის ქვეშ დააყენოს მტკიცებულებები და უფლებაში ჩარევის აუცილებლობის დასაბუთება, თუმცა ცხადია, მას დამატებითი ინფორმაციის მოპოვების მიზნით მომავალ სამიზნესთან დაკონტაქტების და მისი ინფორმირების შესაძლებლობა არ აქვს.[182] ნორვეგიამ უკვე დანერგა ეს ინოვაციური მიდგომა ფარულ ღონისძიებებზე ნებართვის გაცემის პროცედურის ფარგლებში.[183]

- <u>*გადაუდებელი სიტუაციები:*</u> მიზანმიმართულ ფარულ ღონისძიებებზე ნებართვის გაცემის პროცედურების გაწერის გარდა, საუკეთესო პრაქტიკის მაგალითია ასევე გადაუდებელ გარემოებებში მოქმედი წესების ეროვნული კანონმდებლობით მკაფიო განსაზღვრა, როდესაც სასამართლოს ნებართვისთვის გაცემის ხანგრძლივობამ შესაძლოა მნიშვნელოვანი რისკები შექმნას სახელმწიფო უსაფრთხოების კუთხით. ევროპული სასამართლოს პრაქტიკის თანახმად, ასეთ გარემოებებში უსაფრთხოების სამსახურებმა შესაძლოა ფარული ღონისძიებები განახორციელონ მხოლოდ 72 საათის განმავლობაში. თუმცა, ასეთი ღონისძიებები უნდა დაექვემდებაროს შემდგომ სასამართლო კონტროლს. [184]

- <u>*მასობრივი მეთვალყურეობის ღონისძიებებზე წინასწარი თანხმობის გაცემა:*</u> როგორც უკვე აღინიშნა, მასობრივი მეთვალყურეობა არ ეფუძნება ეჭვს კონკრეტულ პირთან მიმართებით. აქედან გამომდინარე, სასამართლოსთვის მეტ სირთულეს წარმოადგენს მასობრივი მეთვალყურეობის ღონისძიებებზე ზედამხედველობა. ამ კუთხით, გაეროს მომხსენებელმა განმარტა:

  - ‘მიზანმიმართულ ფარულ ღონისძიებებთან მიმართებით, შესაძლებელია მათი აუცილებლობისა და თანაზომიერების შესახებ ობიექტური შეფასების გაკეთება, მოცემული ჩარევის ინტენსივობის კონკრეტული გამოძიებისთვის მის ღირებულებასთან შეპირისპირების საშუალებით. თუმცა, მასობრივი წვდომა ციფრულ კომუნიკაციაზე არ იძლევა ინდივიდუალური თანაზომიერების ტესტით ხელმძღვანელობის შესაძლებლობას და, წინასწარი კონტროლის განხორციელება შესაძლებელი ხდება მხოლოდ მაღალი განზოგადების ხარისხში.”[185]

ამის მიუხედავად, საერთაშორისო სტანდარტის შესაბამისად, მასობრივ მეთვალყურეობაზე

181 *EU FRA Surveillance by Intelligence Services (2015)*, p.54
182 Ibid para 214
183 Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015),p.55
184 ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 81
185 UN, Human Rights Council, Emmerson, B. (2014), para. 7

წინასწარი ნებართვის გაცემა უნდა დაეფუძნოს ღონისძიების სიმძიმის და აუცილებლობის კუთხით მისი სერიოზულობის, თანაზომიერების ხარისხის (შესაძლებლობის ფარგლებში), და გამოყენებული სელექტორების (საძიებო სიტყვების) და სხვა ფილტრის ალგორითმების შემოწმებას, იმის უზრუნველსაყოფად, რომ მათ დისკრიმინაციული ხასიათი არ შეიძინონ.[186]

<u>ინფორმაციის შეგროვების ღონისძიებების მიმდინარე ზედამხედველობა:</u>

როგორც უკვე აღინიშნა, სასამართლო ხელისუფლების ჩართულობა (ზედამხედველი ორგანოს როლში) ფარული ღონისძიებების განხორციელების პროცესში, ევროპაში გავრცელებულ პრაქტიკას არ წარმოადგენს. ამის ნაცვლად, დამოუკიდებელ ზედამხედველობის ორგანოებს (ზოგიერთ ქვეყანაში ორგანოებს კვაზი სასამართლო ფუნქციით) აქვთ ფარული ღონისძიებების მიმდინარე ზედამხედველობის, მოკვლევის, დათვალიერების, პერსონალური მონაცემების დამუშავების, შენახვის და განადგურების პროცესების მონიტორინგის უფლებამოსილება.

ამის მიუხედავად, კიდევ ორი ძირითადი უფლებამოსილება უნდა მიენიჭოს ფარული მეთვალყურეობის ღონისძიებებზე ზედამხედველობის განმახორციელებელ ორგანოს:

- *<u>ღონისძიების შეწყვეტაზე მითითება:</u>* თუ ფარულ ღონისძიებებზე ზედამხედველობის ფუნქციის მქონე ორგანო აღმოაჩენს კანონის დარღვევას, მას უნდა ჰქონდეს ღონისძიების დაუყოვნებელ შეწყვეტაზე მითითების გაცემის უფლებამოსილება. ევროპული სასამართლოს პრაქტიკის თანახმად, ეს უფლებამოსილება არსებითია ეფექტიანი ზედამხედველობის სისტემისთვის.[187]
- *<u>მოპოვებული პერსონალური ინფორმაციის განადგურებაზე მითითება:</u>* იმ შემთხვევებში, როდესაც ზედამხედველობის ორგანო დაადგენს ფარული მეთვალყურეობის უკანონობას და მის შეწყვეტაზე გასცემს მითითებას, მას ასევე უნდა ჰქონდეს უკანონოდ მოპოვებული პერსონალური ინფორმაციის განადგურებაზე მითითების გაცემის უფლებამოსილება.

ერთი მნიშვნელოვანი დათქმა არსებობს პერსონალური ინფორმაციის განადგურებასთან დაკავშირებით. ინფორმაციის უკანონო მოპოვების შემთხვევების გარდა, სპეციალურ სამსახურებს ევალებათ მათ მიერ შენახული პერსონალური ინფორმაციის რეგულარულად გადახედვა და ნებისმიერი ინფორმაციის წაშლა, რომელიც მათი მანდატის შესასრულებლად აღარ არის მნიშვნელოვანი. თუმცა, პერსონალური ინფორმაციის წაშლა შესაძლოა ასევე საზიანო იყოს ზედამხედველობის ორგანოების საქმიანობისა და სასამართლო წარმოებისთვის. აქედან გამომდინარე, გაეროს სახელმძღვანელო დოკუმენტის თანახმად, საუკეთესო პრაქტიკას წარმოადგენს ნებისმიერი ასეთი ინფორმაციის წაშლაზე გარე ინსტიტუციის მიერ ზედამხედველობის განხორციელება.[188]

<u>სასამართლოს მიერ საქმის გადაწყვეტა</u>

წინასწარი კონტროლის გარდა, სასამართლო ხელისუფლებას აქვს უსაფრთხოების სამსახურების საქმიანობის ან ასეთის სამართლებრივი საფუძვლების შესახებ საქმეების გადაწყვეტის უფლებამოსილება. ეს საქმეები სასამართლოს წინაშე შესაძლოა წარდგენილი იყო ფარული მეთვალყურეობის სამიზნის (პირებს შეუძლიათ შეიტყონ მათ მიმართ განხორციელებული ფარული ღონისძიებების შესახებ შემდგომი შეტყობინების მექანიზმის, ინფორმატორების და მედიით გავრცელებული ინფორმაციის საშუალებით, ასევე შესაძლებელია მათ უბრალოდ ამის შესახებ გაუჩნდეთ ეჭვი) მიერ. სასამართლო პირებს აძლევს მათ პირად ცხოვრებაში ჩარევის გასაჩივრების და უფლების აღმდგენი საშუალებით უზრუნველყოფის შესაძლებლობას. ამ კონტექსტში, მოსამართლეები

186 *EU FRA, Surveillance by Intelligence Services Vol 2, (2017)*, p.96
187 *ECtHR*, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015,* para. 28
188 UN Compilation of Good Practices, Practices 24-25

ადგენენ, თუ რამდენად ხორციელდებოდა მოსარჩელის კომუნიკაციის მონიტორინგი, და ასეთი მონიტორინგის შემთხვევაში, იყო თუ არა ეს ღონისძიებები კანონიერი, აუცილებელი და არსებული ეჭვის/საფრთხის თანაზომიერი. ნებართვის გაცემის პროცედურის მსგავსი გამოწვევები აქაც სახეზეა: მოსამართლეებს უნდა ჰქონდეთ საჭირო გამოცდილება, ცოდნა და წვდომა საიდუმლო ინფორმაციაზე საქმეზე გადაწყვეტილების მისაღებად. უსაფრთხოების სამსახურებმა შესაძლოა ქვედა ინსტანციის საერთო სასამართლოებს კონფიდენციალურ ინფორმაციაზე შეზღუდული წვდომით 'არც უარყოფის და არც დადასტურების' პასუხები გასცეს. ამ კონტექსტში, საუკეთესო სტანდარტია სპეციალიზებული ტრიბუნალების დაფუძნება, სადაც მოსამართლეებს ექნებათ საკმარისი ცოდნა ტექნიკური საკითხების გადასაწყვეტად, ასევე ექნებათ წვდომა საიდუმლო ინფორმაციაზე.[189] ამ სტანდარტის კარგ მაგალითს წარმოადგენს დიდი ბრიტანეთის საგამოძიებო უფლებამოსილებების ტრიბუნალი (IPT), სპეციალური სასამართლო ორგანო ფარული ღონისძიებების და ადამიანის უფლებების საკითხებზე სამსახურების წინააღდეგ საჩივრების განხილვის ექსკლუზიური უფლებამოსილებით, რომელსაც შეუძლია მიმდინარე ფარული ღონისძიებების შესახებ გამოძიების წარმოება.[190]

სასამართლოები ასევე მსჯელობენ საქმეებზე, რომლებსაც არასამთავრობო ორგანიზაციები ან სხვა რელევანტური დაინტერესებული მხარეები წარადგენენ, რომლებიც არ არის აუცილებელი ემყარებოდეს საჩივარს, და შესაძლოა ზოგადად სამსახურების საქმიანობის ან მისი სამართლებრივი საფუძვლის კითხვის ნიშნის ქვეშ დაყენებას ემსახურებოდეს. ასეთ საქმეებზე გადაწყვეტილების მიღებით, სასამართლო ხელისუფლება ადგენს მნიშვნელოვან სტანდარტებს უსაფრთხოების სამსახურების საქმიანობისთვის, რასაც მათ შორის შეუძლია კანონმდებლობის ან სამთავრობო პოლიტიკის ცვლილების მოტანა.

ეს ქვეთავი მოკლედ მიმოიხილავდა სასამართლო ხელისუფლების როლს უსაფრთხოების სამსახურების ზედამხედველობის პროცესში, ასევე სასამართლო წინასწარი კონტროლის და სასამართლოში საქმის წარმოების გამოწვევებს. ამ გამოწვევების გათვალისწინებით, საერთაშორისო აქტორები, უფრო და უფრო ხშირად საუბრობენ ფარულ ღონისძიებებზე ნებართვის გაცემის მრავალშრიანი მიდგომის აუცილებლობაზე, მათ შორის აღმასრულებელი, სასამართლო ხელისუფლების და ექსპერტთა ზედამხედველობის ორგანოების ჩართულობით ფარული ღონისძიებების სხვადასხვა სახეობისა და ეტაპისთვის. შემდეგ ქვეთავში განხილული იქნება სხვადასხვა ქვეყნების მოდელები.

189 *EU FRA Surveillance by Intelligence Services (2015)*, p.66
190 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015, p.53

შერჩეული ქვეყნების საუკეთესო პრაქტიკები:

ხორვატია

მიზანმიმართულ ფარულ ღონისძიებებზე წინასწარი ნებართვის გაცემა:

ხორვატიის რესპუბლიკის უსაფრთხოების და დაზვერვის სისტემის შესახებ კანონის (შემდგომში კანონი) შესაბამისად, უსაფრთხოების სამსახურის (SOA) ხელმძღვანელი და სასამართლო მიზანმიმართულ მეთვალყურეობაზე ნებართვის გაცემის კომპეტენციებს ინაწილებენ. ხელმძღვანელის მიერ ნებართვის გაცემა ხორციელდება შემდეგ ღონისძიებებზე: ა) ტელეკომუნიკაციების გრაფიკის აღრიცხვა b) მომხმარებლის ადგილმდებარეობის იდენტიფიცირება *(ა და ბ უთითებენ მეტადატაზე)* გ) საერთაშორისო კომუნიკაციის მიყურადება დ) დოკუმენტების და საგნების საიდუმლო შესყიდვა (მუხლი 33 (3)). როდესაც დირექტორი გასცემს თანხმობას ასეთ ღონისძიებებზე, ის ასევე ვალდებულია ამის შესახებ ყოველთვიურად აცნობოს ეროვნული უსაფრთხოების საბჭოს. დოკუმენტების და საგნების საიდუმლო შესყიდვის ნაწილში, სამსახურის ხელმძღვანელმა ასევე ყოველთვიურად ანგარიში უნდა წარუდგინოს მთავარ პროკურორს (მუხლი 38(2)).

ქვემოთ ჩამოთვლილი ფარული ღონისძიებები, რომლებიც ზემოაღწერილზე უფრო ინტენსიურია, საჭიროებს წინასწარ სასამართლო ნებართვას: ა) კომუნიკაციის (შინაარსის) მიყურადება ბ) საფოსტო გზავნილის კონტროლი c) დაწესებულებებსა და დახურულ ადგილებში მოსასმენი მოწყობილობის დამონტაჟება (bugging), და d) ღია და საჯარო სივრცეებში ადამიანებს შორის კომუნიკაციის აუდიო ჩაწერა.

საერთაშორისო სტანდარტებთან შესაბამისობაში, კანონი დეტალურად განსაზღვრავს ღონისძიებებზე ნებართვის მოთხოვნის შუამდგომლობებისთვის აუცილებელ ინფორმაციას, ასევე ფარული ღონისძიებების გამოყენების მაქსიმალურ ხანგრძლიობას (თუმცა ასევე უნდა აღინიშნოს რომ მაქსიმალური ხანგრძლივობა (4 თვე) საშუალოზე მეტია) (კანონის მუხლები 36 -37). ფარულ ღონისძიებებზე ნებართვას გასცემს უზენაესი სასამართლოს მოსამართლე. როდესაც საქმე ეხება ფარული ღონისძიებების გაგრძელებას, ხორვატია წარმოადგენს საუკეთესო პრაქტიკის მაგალითს, სადაც ვადის გაგრძელების შესახებ ნებართვას გასცემს უზენაესი სასამართლოს სამი უფლებამოსილი მოსამართლისგან შემდგარი ჯგუფი. რეკომენდირებულია უფრო მკაცრი სტანდარტის და უფრო მაღალი დონის კონტროლის გამოყენება ფარული ღონისძიებების გახანგრძლივების შესახებ მოთხოვნების განხილვისას, სამსახურების მხრიდან ასეთი ინტენსიური ღონისძიებების აუცილებლობის გარეშე გახანგრძლივების თავიდან ასაცილებლად.

ასევე საერთაშორისო სტანდარტებთან შესაბამისობაში, განსაკუთრებულ შემთხვევებში სასამართლო ნებართვის გარეშე ფარული ღონისძიებების განხორციელების დრო შეზღუდულია 24 საათამდე (კანონის მუხლი 36(2)).

ფარული ღონისძიებების მიმდინარე ზედამხედველობა: კანონი სასამართლო ხელისუფლებას არ ანიჭებს ფარული ღონისძიების მიმდინარეობაზე ზედამხედველობის ფუნქციას. ამის ნაცვლად, უსაფრთხოებისა და დაზვერვის სამსახურებზე სამოქალაქო ზედამხედველობის საბჭოს და ხორვატიის პერსონალური ინფორმაციის დაცვის სააგენტოს ფარული ღონისძიებების განხორციელებაზე ზედამხედველობის ფუნქცია აქვთ საჩივრების გამოძიების, თემატური მოკვლევის დაწყების ან

ადგილზე დათვალიერების საშუალებით. საუკეთესო პრაქტიკას წარმოადგენს ის ფაქტი, რომ ხორვატიის პერსონალური ინფორმაციის დაცვის სააგენტოს გადაწყვეტილებები შესასრულებლად სავალდებულოა.[191]

191 See EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.115

წინასწარი ნებართვის გაცემა მიზანმიმართულ ფარულ ღონისძიებებზე

კანადამ დანერგა ორსაფეხურიანი ნებართვის გაცემის სისტემა, სადაც უსაფრთხოების სამსახურის (CSIS) ღონისძიებების მოთხოვნის შუამდგომლობებზე პირველ რიგში თანხმობა უნდა გასცეს მინისტრმა, და შემდგომში წარედგინოს სასამართლოს. კანადის სპეციალური სამსახურების კანონი შეიცავს ყოვლისმომცველ ქვეთავს დასახელებით 'სასამართლო კონტროლი', რომელშიც ნებართვის გაცემის პროცედურები დეტალურად არის გაწერილი. უნდა აღინიშნოს, რომ კანონი შესაძლებლობას აძლევს CSIS ფარული ღონისძიებები განახორციელოს როგორც ქვეყნის შიგნით, ისე მის ფარგლებს გარეთ. ნებისმიერ შემთხვევაში, სასამართლო ნებართვა აუცილებელია. CSIS კანონი[192] საუკეთესო პრაქტიკის მაგალითია, რადგან ის ამომწურავად ჩამოთვლის, ღონისძიების მოთხოვნის შუამდგომლობაში აუცილებლად მისათითებელ ინფორმაციას (კანონის მუხლი 21(2)), კერძოდ:

- ფაქტები, რომელიც ადასტურებს რწმენას იმის შესახებ, რომ შუამდგომლობის დაკმაყოფილება აუცილებელია CSIS - ის მიერ მისი ფუნქციების შესასრულებლად;
- რატომ ვერ იქნება სხვა ნაკლებად ინტენსიური საშუალებები წარმატებული
- კომუნიკაციის სახე, რომლის მიყურადებაც იგეგმება, ინფორმაცია, ჩანაწერი, დოკუმენტი, რომელიც უნდა იქნეს მოპოვებული და შესაბამისი უფლებამოსილებები
- ფარული ღონისძიებების სამიზნის მაიდენტიფიცირებელი ინფორმაცია და შემოთავაზებული პერიოდი
- იმ ადგილის ზოგადი დახასიათება, სადაც ფარული ღონისძიებების განხორციელება იგეგმება
- ინფორმაცია ფარული ღონისძიებების სამიზნესთან დაკავშირებულ ადრინდელ მიმართვებთან დაკავშირებით

ფარული ღონისძიებები, რომლებიც სასამართლო წინასწარ ნებართვას საჭიროებენ, შემდეგია: ნებისმიერი კომუნიკაციის მიყურადება ან ნებისმიერი ინფორმაციის, ჩანაწერის, დოკუმენტის, ან საგნის მოპოვება და, ამ მიზნით (i) ნებისმიერ ადგილზე შესვლა ან ნებისმიერ საგანზე წვდომის მოპოვება, (II) ინფორმაციის, ჩანაწერის, დოკუმენტის ან საგნის ძებნა, ამოღება ან დაბრუნება, ან შემოწმება, ამონარიდების ამოღება, ან ასლის, ჩანაწერის გაკეთება ნებისმიერი სხვა ფორმით (III) ნებისმიერი საგნის დამონტაჟება, შენარჩუნება ან ამოღება (მუხლი 21(3)).

საერთაშორისო სტანდარტებთან შესაბამისობაში, ღონისძიებების შესახებ მოთხოვნის შუამდგომლობები განიხილება მაღალი რანგის ფედერალური მოსამართლის მიერ. ორდერის მოქმედების ვადის გაგრძელებაზე ნებართვის გაცემის პროცედურაც ორსაფეხურიანია და საჭიროებს CSIS-ზე პასუხისმგებელი მინისტრის და ფედერალური მოსამართლის თანხმობას. კანადის უსაფრთხოების რისკების შემცირებაზე მიმართული ღონისძიებების განხორციელების ვადის გაგრძელება შეზღუდულია; ესეთი ღონისძიებები შეიძლება გაგრძელდეს მხოლოდ ორჯერ (მუხლი 22). ნაკლებად კონკრეტულ საფრთხეებთან მიმართებით ღონისძიებების გაგრძელების შესაძლებლობების შეზღუდვა შეგვიძლია საუკეთესო პრაქტიკის მაგალითად განვიხილოთ.

192 Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23) available from: http://laws-lois.justice.gc.ca/eng/acts/c-23/index.html

ფარული ღონისძიებების სამიზნის უფლებების დაცვის კონტექსტში, კანონი არ შეიცავს დებულებებს ადვოკატთან დაკავშირებით, რომელსაც სპეციალური სამსახურების შემოწმება აქვთ გავლილი და სასამართლო განხილვის ფარგლებში ღონისძიებების სუბიექტს დაიცავენ, ასევე კითხვის ნიშნის ქვეშ დააყენებენ ღონისძიებების მოთხოვნაზე წარდგენილი შუამდგომლობის სამართლებრივ საფუძვლებს. თუმცა, სამოქალაქო საზოგადოების წარმომადგენლები სწორედ ამ მოდელის დანერგვას ითხოვდნენ.[193]

სასამართლოს მიერ საქმის გადაწყვეტა

იმის მიუხედავად, რომ კანადის კანონმდებლობა ადგენს ნებართვის გაცემის ორსაფეხუროვან პროცედურას და სავალდებულოს ხდის დეტალური შეუამდგომლობის წარდგენას, ყოველთვის არსებობს რისკი, რომ უსაფრთხოების სამსახური ბოროტად გამოიყენებს სასამართლო ნებართვის შედეგად მოპოვებულ ფარული მეთვალყურეობის უფლებამოსილებებს. სასამართლო განხილვა უზრუნველყოფს სამართლებრივ დაცვას და ასევე მომავლისთვის სტანდარტებს ადგენს. ინდივიდუალური საჩივრის საფუძველზე, ფედერალურმა სასამართლომ შეამოწმა CSIS - ის მიერ ფარული ღონისძიებების გამოყენების პრაქტიკები და დაადგინა, რომ CSIS - მ სასამართლოს სათანადო ინფორმირება არ მოახდინა მნიშვნელოვან ინფორმაციის შეგროვების პროგრამაზე, რომელმაც შეინახა მეტადატა და საფრთხისთვის არარელევანტური პერსონალური ინფორმაცია 10 წლის განმავლობაში. შესაბამისად სასამართლომ განმარტა, რომ ასეთი ინფორმაციის შენახვა უკანონო იყო. CSIS - ის ხელმძღვანელმა და საზოგადოებრივი წესრიგის დაცვის მინისტრმა აღიარა შეცდომა და პირობა დადო, რომ მიიღებდნენ ყველა საჭირო ზომას, მათ შორის ასეთ ინფორმაციაზე წვდომის დაუყოვნებელი დახურვის ღონისძიებას გამოიყენებდნენ[194]

193 https://ablawg.ca/wp-content/uploads/2016/12/Blog_CSIS_Warrants.pdf

194 See http://www.cbc.ca/news/politics/csis-metadata-ruling-1.3835472 https://www.documentcloud.org/documents/3213882-DES-Warrant-Nov-3-2016-Media-Summary-FINAL.html

გერმანია იმ რამდენიმე ქვეყანას შორისაა ევროპაში, სადაც სასამართლო ხელისუფლება როლს არ თამაშობს ფარულ ღონისძიებებზე ნებართვის გაცემის პროცესში. ამის ნაცვლად, გერმანიაში ფუნქციონირებს ორი კვაზი სასამართლო ორგანო, რომელიც მათ შორის სხვადასხვა სახის ფარულ ღონისძიებებზე გასცემს ნებართვას. როგორც BfV (შიდა სახელმწიფო უსაფრთხოების სამსახური), ისე BND (საგარეო დაზვერვის სამსახური) იყენებენ სხვადასხვა ინტენსივობის ფარულ ღონისძიებებს. კომპლექსური, თუმცა ფრაგმენტული სისტემა ქვემოთ მოკლედ იქნება მიმოხილული:

მიზანმიმართულ ფარულ ღონისძიებებზე წინასაწარი ნებართვის გაცემა

პირველ რიგში, როგორც კარგი პრაქტიკის მაგალითი, გერმანული G-10 კანონი პირდაპირ ჩამოთვლის იმ პირთა კატეგორიას, რომლებიც შესაძლოა დაექვემდებარონ მიზანმიმართულ ფარულ ღონისძიებებს (G-10 კანონის მუხლი 1.3.11). სამსახურები (BfV და BND) ადგენენ შუამდგომლობას და მას ფედერალურ შინაგან საქმეთა სამინისტროში წარადგენენ. თუ სამინისტრო დაადგენს, რომ არსებობს გონივრული ეჭვის საფუძველი ფარულ ღონისძიებებზე შუამდგომლობის წარსადგენად, მაშინ ის მოთხოვნას წარადგენს G-10 კომისიაში. G-10 კომისია, პარლამენტის კვაზისასამართლო ორგანო (მეტი ინფორმაციისთვის იხილეთ თავები 3.1. და 3.2.) თვეში ერთხელ განიხილავს წარდგენილი მოთხოვნების კანონიერებისა და აუცილებლობის საკითხს. ფარული მიყურადების ღონისძიების გამოყენება დაშვებულია მხოლოდ G-10 კომისიის თანხმობის შემდეგ. თუმცა, გადაუდებელ გარემოებებში, ფარული ღონისძიებების განხორციელება შესაძლებელია G-10 კომისიის ნებართვის გარეშეც, თუ შემდგომ მისი დაკანონება დროულად მოხდება. მიზანმიმართული ფარული ღონისძიებები გრძელდება მაქსიმუმ 3 თვე, და ვადის გაგრძელება იმავე პროცედურით ხდება.[195]

სტრატეგიულ (მასობრივ) ფარულ ღონისძიებებზე წინასაწარი ნებართვის გაცემა

საუკეთესო პრაქტიკის მაგალითია გერმანიის დეტალური კანონმდებლობა BND-ს სტრატეგიული ფარული ღონისძიებების შესახებ. როგორც პირველი ამ სფეროში, გერმანიის კანონმდებლობა არეგულირებს არა მარტო ქვეყანასთან შემხებლობაში მყოფ კომუნიკაციას (ისეთი კომუნიკაციების მიყურადება, რომელიც იწყება ან სრულდება გერმანიაში) ასევე სრულად ქვეყნის ფარგლებს გარეთ განხორციელებულ კომუნიკაციას (BND-ს მიერ ქვეყნის ფარგლებს გარეთ განხორციელებული კომუნიკაციის მიყურადება).

- *ისეთი სტრატეგიულ ფარულ ღონისძიებებზე წინასაწარი ნებართვის გაცემა, რომელიც იწყება ან სრულდება გერმანიაში*

ამ შემთხვევაში BND ადგენს ღონისძიებების მოთხოვნის შესახებ შუამდგომლობას, რომელიც მოიცავს სელექტორებს (საძიებო სიტყვები მოპოვებული მასობრივი ინფორმაციის გასაფილტრად) და მას ფედერალურ შინაგან საქმეთა სამინისტროს წარუდგენს. სამინისტრო, საპარლამენტო კონტროლის ჯგუფის თანხმობის მოპოვების შემდგომ, მოთხოვნას წარადგენს G-10 კომისიაში. მხოლოდ კომისიის მიერ შემოწმების და პოზიტიური გადაწყვეტილების გამოცემის შემდგომ, შეიძლება სტრატეგიული ფარული ღონისძიების გამოყენება. გადაუდებელი აუცილებლობის შემთხვევებში, ფარული ღონისძიებების განხორციელება შესაძლოა დაიწყოს, მანამ სანამ G 10 კომისია ნებართვას გასცემს,

195 Hans de With and Erhard Kathmann, 'Annex A- Country Case Studies - Germany', p.223, in Aidan Wills and Mathias Vermeulen, Parliamentary Oversight of Security and Intelligence Agencies in the European Union (2011), Also see G-10 Law, article 10

თუმცა ამ პერიოდში მოპოვებული ინფორმაციის გამოყენება დაუშვებელია[196], რაც საუკეთესო პრაქტიკის მაგალითია. მასობრივ ფარულ ღონისძიებებთან მიმართებით, G10 კომისია ასევე ზედამხედველობს ფარული ღონისძიებების შედეგად ინფორმაციის მოპოვებისას პერსონალური მონაცემების მაქსიმალურ დაცვას.[197] როგორც იკვეთება, გერმანული მოდელი მასობრივი მეთვალყურეობისთვის იყენებს მრავალსაფეხურიან ნებართვის გაცემის პროცედურებს აღმასრულებელი და საკანონმდებლო ხელისუფლების, ასევე ექსპერტთა ჯგუფების ჩართულობით.[198]

► *<u>ისეთი სტრატეგიულ ფარულ ღონისძიებებზე წინასაწარი ნებართვის გაცემა, რომელიც სრულად ქვეყნის ფარგლებს გარეთ ხორციელდება</u>*

უკანასკნელი რეფორმის პროცესში, გერმანიამ ცვლილება შეიტანა კანონმდებლობაში, მათ შორის სრულად ქვეყნის ფარგლებს გარეთ განხორციელებული ფარული ღონისძიებების რეგულირებისთვის და ამისთვის შექმნა ახალი კვაზი სასამართლო ექსპერტთა ჯგუფი (დამოუკიდებელი კომიტეტი, იხილეთ ქვეთავები 3.1. და 3.2) ფარულ ღონისძიებებზე ნებართვის გაცემის და ზედამხედველობის ექსკლუზიური მანდატით. BND ღონისძიებების მოთხოვნის შუამდგომლობით მიმართავს კანცლერს, რომელიც განიხილავს და ნებართვის მოსაპოვებლად მას დამოუკიდებელ კომიტეტს გადასცემს. ორი მოსამართლისგან და პროკურორისგან შემდგარი ეს კვაზი სასამართლო ორგანო იკრიბება სამ თვეში ერთხელ, და შემოთავაზებულ საძიებო სიტყვებზე შეზღუდული წვდომით, განიხილავს ფარული ღონისძიებების შესახებ შუამდგომლობას. სრულად ქვეყნის ფარგლებს გარეთ განხორციელებული კომუნიკაციის ფარული მიყურადება მხოლოდ კომიტეტის მიერ ნებართვის გაცემის შემდგომ არის დასაშვები.[199]

გერმანიას ამ დრომდე არ დაუნერგავს სპეციალური სამსახურების მიერ შემოწმებული ადვოკატის სისტემა რომელიმე კვაზი სასამართლო ორგანოში, თუმცა სამოქალაქო საზოგადოება აღნიშნულს აქტიურად ითხოვდა.[200]

<u>მიმდინარე და შემდგომი ზედამხედველობა კვაზისასამართლო ორგანოების მიერ</u>

გერმანიაში ორივე კვაზი სასამართლო ორგანოს (G-10 კომისია და დამოუკიდებელი კომიტეტი) აქვს BfV-ს და BND-ს საქმიანობის მიმდინარე და შემდგომი შემოწმების განხორციელების მანდატი. G-10 კომისიის საზედამხედველო ფუნქციები ეხება ინფორმაციის შეგროვების, დამუშავებისა და გამოყენების სრულ ფარგლებს. საეთაშორისო საუკეთესო პრაქტიკებთან შესაბამისობაში, G-10 კომისიას, შემოწმების ნებისმიერ ეტაპზე, აქვს იმ ფარული ღონისძიებების დაუყოვნებლივ შეწყვეტაზე გადაწყვეტილების მიღების უფლებამოსილება, რომლებსაც ის უკანონოდ და არასაჭიროდ მიიჩნევს.[201]

G-10 კანონი შეიცავს დეტალურ რეგულირებას პერსონალური მონაცემების წაშლასთან დაკავშირებით. BfV ვალდებულია 6 თვეში ერთხელ გადახედოს მის მიერ შენახული პერსონალური ინფორმაციის სისწორეს და რელევანტურობას. თუ პერსონალური მონაცემები არაზუსტი ან არარელევანტურია, მისი წაშლა უნდა მოხდეს სამსახურის თანამშრომლის ზედამხედველობით, რომელსაც მოსამართლის პოზიციისთვის განსაზღვრული კვალიფიკაცია გააჩნია. წაშლილი ინფორმაცია უნდა აღირიცხოს

196 EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.99
197 Council of Europe, Democratic and Effective Oversight of National Security Services, (2015), p.57
198 For more information, see Thorsten Wetzling, Germany's Intelligence Reform: More surveillance, modest restraints and inefficient controls' SNV Policy Brief (2017), p.8
199 Ibid.
200 Thorsten Wetzling, SNV Policy Brief: 'The Key to Intelligence Reform in Germany- Strengthening the G-10 Commission's role to authorize strategic surveillance' 2016, p.3
201 G-10 Law, articles 3-5

და აღრიცხული ინფორმაცია გამოყენებული შეიძლება იყოს მხოლოდ ზედამხედველების მიერ დათვალიერებისას (მუხლი 3ბ). პერსონალური ინფორმაციის წაშლაზე ზედამხედველობის ასეთი დეტალური რეგულირება საუკეთესო პრაქტიკის მაგალითია.

სასამართლოსა და კვაზისასმაართლო ორგანოს მიერ საჩივრების განხილვა

გერმანიაში, პირებს, რომლებსაც სამსახურების წინააღმდეგ პრეტენზია გააჩნიათ, შეუძლიათ საჩივრით მიმართონ კვაზი სასამართლო ორგანოებს (რომლებსაც საგამოძიებო უფლებამოსილებები გააჩნიათ და რომელთა გადაწყვეტილებებიც შესასრულებლად სავალდებულოა), ან სასამართლოებს. სასამართლო სისტემის ფარგლებში, ფარული ღონისძიებების შესახებ საჩივრები უმაღლესი ადმინისტრაციული სასამართლოს მიერ განიხილება, რაც საერთაშორისო სტანდარტებთან შესაბამისობაშია. სამსახურების შესახებ ყველა სხვა საჩივრის განხილვა ადგილობრივი ადმინისტრაციული სასამართლოს კომპეტენციაში შედის.[202]

202 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.20

ბელგია კიდევ ერთი ქვეყანაა, სადაც სასამართლო ზედამხედველობას ჩვეულებრივი სასამართლოს ნაცვლად ძირითადად კვაზი სასამართლო ექსპერტთა ჯგუფები ახორციელებენ. ამის მიუხედავად, სასამართლოები გადამწყვეტ როლს თამაშობენ პირადი ცხოვრების უფლებასთან/ფარულ ღონისძიებებთან დაკავშირებული საქმეების გადაწყვეტაში და შესაბამისად სტანდარტების დადგენაში.

მიზანმიმართულ ფარულ ღონისძიებებზე წინასაწარი ნებართვის გაცემა: როგორც პირველ თავშიც აღინიშნა, ფარული ღონისძიებების მარეგულირებელი ბელგიური სამართლებრივი მოდელის პროგრესული მახასიათებელია კანონით სპეციფიკური და საგამონაკლისო ფარული ღონისძიებების განსხვავებაა. სპეციფიკური ფარული ღონისძიებები ნაკლებად ინტენსიურია და მაგალითად მდგომარეობს კომუნიკაციების ოპერატორის თანამშრომლობის მოთხოვნა, მაიდენტიფიცირებელი პერსონალური ინფორმაციის შემოწმება, ლოკალიზაცია და ელექტრონული კომუნიკაციების საშუალებების გამოყენებით განხორციელებული ზარის მონაცემების მოპოვება. უსაფრთხოების სამსახურის ხელმძღვანელი იძლევა ნებართვას ასეთ ღონისძიებებზე; თუმცა, სამსახური ვალდებულია ექსპერტთა საზედამხედველო ორგანოებს რეგულარულად წარუდგინოს ანგარიში ამ ღონისძიებების განხორციელების შესახებ.[203]

საგამონაკლისო ფარული ღონისძიებები ჩარევის უფრო ინტენსიური ფორმებია, რომელიც მოიცავს არა მარტო კომუნიკაციების მიყურადებას, არამედ პირადი სადგომის დათვალიერებასა და ჩხრეკას; ჰაკერობა ელექტრონულ სისტემებში; ფარული აგენტების გამოყენება მათ შორის შენიღბული იდენტობის შექმნით. საგამანაკლისო ფარულ ღონისძიებებზე ნებართვის მოპოვებისთვის, უსაფრთხოების სამსახური უშუალოდ ადმინისტრაციულ კომისიას, კვაზი სასამართლო ექსპერტთან საზედამხედველო ჯგუფს წარუდგენს წერილობით მოთხოვნას (იხ. თავი 3.2). კომისია განიხილავს მოთხოვნას, და 4 დღეში წყვეტს მოთხოვნის დაკმაყოფილების საკითხს. საგამონაკლისო ღონისძიებების განხორციელება მხოლოდ ნებართვის გაცემის შემდეგ დაიშვება. თუმცა, მათ შორის დადებითი გადაწყვეტილების გამოტანისას, ადმინისტრაციული კომისია ინფორმაციას აწვდის მუდმივმოქმედ კომიტეტ I-ს (მეორე კვაზი სასამართლო ექსპერტთა ორგანო ბელგიაში, იხილეთ თავი 3.2); რომელსაც შეუძლია კომისიის ნებართვის დაძლევა და ფარული ღონისძიებების დაუყოვნებლივი შეწყვეტის მოთხოვნა.[204]

საერთაშორისო სტანდარტებთან შესაბამისობაში, გადაუდებელი აუცილებლობის შემთხვევაში, უსაფრთხოების სამსახურს, ადმინისტრაციული კომისიის ხელმძღვანელის თანხმობით საგამონაკლისო ღონისძიებების განხორციელება შეუძლია 48 საათის განმავლობაში, და იმ პირობით, რომ გადაუდებელი აუცილებლობის დასაბუთება კომისიას ამის შემდგომ დაუყოვნებლივ წარედგინება.[205]

საჩივრების განხილვა და გადაწყვეტა:

სამოქალაქო სამართლის თანახმად, ჩვეულებრივ სასამართლოებს აქვთ უსაფრთხოების სამსახურების მიერ ადამიანის უფლებების დარღვევის შესახებ წარდგენილი საჩივრების განხილვის უფლებამოსილება. თუმცა, ასეთ სასამართლოებს არ აქვთ საკმარისი სპეციალური ცოდნა და ასევე შესაძლებელია შეზღუდული წვდომა ჰქონდეთ ინფორმაციაზე. ამის ნაცვლად, მუდმივმოქმედი კომიტეტი I, რომელსაც სრული წვდომა აქვს კონფიდენციალურ ინფორმაციაზე და გააჩნია საჩივრების მიღების და განხილვის უფლებამოსილება, ფართო საგამოძიებო ფუნქციებით და ტექნიკურ ფარულ

203 EU FRA Surveillance by Intelligence Services (2015), p.69
204 EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.94
205 Ibid. p.98

ღონისძიებებზე სპეციალური ცოდნით, საჩივრების განხილვისთვის უფრო შესაბამისი ორგანოა. იმის მიუხედავად, რომ მას სასამართლოებისგან განსხვავებით არ შეუძლია უფლების აღმდგენი სამართლებრივი საშუალების მინიჭება, მას შეუძლია მოსარჩელის იმ ორგანოსთან ან სამსახურთან გადამისამართება, რომელსაც ამ საკითხის გადაწყვეტის კომპეტენცია გააჩნია.[206]

ინდივიდუალური საჩივრების განხილვის გარდა, ბელგიის საკონსტიტუციო სასამართლო კრიტიკულ როლს თამაშობს, ფარულ ღონისძიებებთან დაკავშირებული საქმეების გადაწყვეტაში. ცოტა ხნის წინ სასამართლომ მონაცემთა შენახვის შესახებ კანონი არაკონსტიტუციურად ცნო. შედეგად, მთავრობამ შეიმუშავა ახალი კანონპროექტი მკაცრი გარანტიებით საკონსტიტუციო სასამართლოს მიერ მიღებული გადაწყვეტილების შესასრულებლად.[207]

3.4. ზედამხედველობა სამოქალაქო საზოგადოების მხრიდან

დემოკრატიულ საზოგადოებაში ანგარიშვალდებულების სისტემის კონტექსტში, სამოქალაქო საზოგადოება არაპირდაპირ, თუმცა მნიშვნელოვან როლს თამაშობს. სხვა ზედამხედველობის ორგანოებთან შედარებით, როგორიცაა სასამართლო, საკანონმდებლო ხელისუფლება, დამოუკიდებელი ზედამხედველობის ორგანოები და ომბუდსმენის ინსტიტუციები; მას არ აქვს ფორმალური მანდატი ნებართვის გაცემასთან, საქმიანობის შემოწმებასთან ან უსაფრთხოების სამსახურების საქმიანობის გამოძიებასთან კავშირში. თუმცა, სამოქალაქო საზოგადოებრივი ორგანიზაციები რამდენიმე მნიშვნელოვან ფუნქციას ასრულებენ და მნიშვნელოვანი წვლილი შეაქვთ უსაფრთხოების სამსახურების ანგარიშვალდებულების უზრუნველყოფაში.

სამოქალაქო საზოგადოებრივი ორგანიზაციების ძირითადი ფუნქციები უსაფრთხოების სამსახურების ზედამხედველობაში:[208]

- **საკანონმდებლო პროცესის მონიტორინგი:** სამოქალაქო საზოგადოებრივი ორგანიზაციები (CSOs) აანალიზებენ უსაფრთხოების სამსახურების მართვისა და ზედამხედველობის შესახებ კანონმდებლობას, ახდენენ საკანონმდებლო ხარვეზების იდენტიფიცირებას, და შეიმუშავებენ რეკომენდაციებს მათი გაუმჯობესებისთვის. ზოგიერთ ქვეყანაში, ისინი მოწვეული არიან საპარლამენტო კომიტეტების მიერ კანონპროექტების შესახებ მათი ექსპერტული დასკვნის წარსადგენად. ეს არის ძირითადი შესაძლებლობა სამოქალაქო საზოგადოებისთვის, რომ წვლილი შეიტანოს საკანონმდებლო ჩარჩოს ჩამოყალიბებაში, თუმცა უმეტეს ქვეყნებში, ამას არ აქვს ინსტიტუციონალიზებული სახე. მას შემდგომ, რაც კანონი ძალაში შედის, სამოქალაქო საზოგადოებრივი ორგანიზაციები განაგრძობენ მათი აღსრულების მონიტორინგს, რათა მოხდეს კანონსა და პრაქტიკას შორის შეუსაბამობების იდენტიფიცირება.

- **უსაფრთხოების სამსახურების საქმიანობის მონიტორინგი და სტრატეგიული საქმეების წარმოება:** იმის გათვალისწინებით, რომ უსაფრთხოების სამსახურები საიდუმლოების პირობებში ოპერირებენ, ხშირად საზოგადოებრივი ორგანიზაციებისთვის შეუძლებელია მათი საქმიანობის პროაქტიული მონიტორინგი, თუმცა ისინი, როგორც წესი, რეაგირებენ მედია საშუალებებით უკანონო საქმიანობის შესახებ გავრცელებულ სკანდალებსა და ბრალდებებზე. საკანონმდებლო ჩარჩოს და საქმიანობის მონიტორინგის საშუალებით, საზოგადოებრივი ორგანიზაციები მნიშვნელოვან როლს თამაშობენ, პრობლემურ კანონმდებლობასთან და უსაფრთხოების სამსახურების პრაქტიკასთან

206 EU FRA Surveillance by Intelligence Services (2015), P.69

207 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), pp1-2

208 For more details, see *EU FRA, Surveillance by Intelligence Services Vol 2. (2017)* p.69

დაკავშირებით სამართალწარმოებაში როგორც ეროვნულ, ისე ევროპულ სასამართლოში. მაგალითის სახით, ოთხმა ფრანგულმა საზოგადოებრივმა ორგანიზაციამ წარადგინა სარჩელი რადიო გადამცემი ხაზებით მიყურადების ღონისძიების შესახებ. საკონსტიტუციო სასამართლომ აღნიშნულ ფარულ ღონისძიებაზე რეგულირება საფრანგეთის კონსტიტუციასთან შეუსაბამოდ გამოაცხადა. შესაბამისად, შიდა უსაფრთხოების კოდექსის მუხლი L.811-5 ძალადაკარგულად იქნა გამოცხადებული.[209]

- **კვლევის და ადვოკატირების საშუალებით ინფორმირებული საჯარო დებატები:** უსაფრთხოების სამსახურების მარეგულირებელი კანონმდებლობა და პოლიტიკის დოკუმენტები ხშირად ჩვეულებრივი მოქალაქეებისთვის საკმაოდ ტექნიკური და კომპლექსურია. თუმცა, ეს კანონები და პოლიტიკის დოკუმენტები მნიშვნელოვან გავლენას ახდენენ ძირითად ადამიანის უფლებებზე, განსაკუთრებით პირადი ცხოვრების უფლებაზე. მნიშვნელოვანია, საზოგადოებამ გაიაზროს უსაფრთხოების სამსახურების უფლებამოსილებების და საქმიანობის ფარგლები, ისევე როგორც ყოველდღიურ ცხოვრებაზე მათი გავლენა. საზოგადოებრივი ორგანიზაციები კრიტიკულ როლს თამაშობენ საზოგადოებაზე ორიენტირებული კვლევების, სტატიების, ასევე ადვოკატირების კამპანიების საშუალებით ფარული ღონისძიებების, პირადი ცხოვრების უფლების და უსაფრთხოების სამსახურების ანგარიშვალდებულების საკითხებზე ცნობიერების ამაღლების კუთხით. მართალია, ეს ზედამხედველობის პირდაპირ ფორმას არ წარმოადგენს, თუმცა ამ საკითხებზე ხილვადი საჯარო კამპანიები და ინფორმირებული საზოგადოებრივი აზრის ხელშეწყობა ზეწოლას ახდენს კანონის და პოლიტიკის განმსაზღვრელ პირებზე მათი საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანის კუთხით.
- **საერთაშორისო სტანდარტების შექმნაში წვლილის შეტანა:** ბოლო რამდენიმე ათწლეულის განმავლობაში, საერთაშორისო საზოგადოებამ მზარდი ინტერესი და ძალისხმევა გამოიჩინა უსაფრთხოების სამსახურების მართვისა და ზედამხედველობისთვის ნორმებისა და პრინციპების ჩამოყალიბების კუთხით. მართალია ისინი სავალდებულოდ შესასრულებელ ნორმებს არ წარმოადგენენ, თუმცა მათ წვლილი შეაქვთ სტანდარტის დადგენასა და საუკეთესო პრაქტიკებთან შესაბამისობის უზრუნველყოფის კუთხით სახელმწიფოების ხელშეწყობაში. ასეთი ნორმატიული ინსტრუმენტების მაგალითია გლობალური პრინციპები ეროვნული. უსაფრთხოებისა და ინფორმაციაზე დაშვების უფლების შესახებ (Tshwane Principles) და ანტიტერორიზმისა და ადამიანის უფლებების შესახებ ოტოვას პრინციპები (Ottowa Principles). ამ ინსტრუმენტების განვითარებაში წვლილი შეიტანეს სამოქალაქო საზოგადოებრივი ორგანიზაციების ექსპერტებმა მთელი მსოფლიოს მასშტაბით.

ეს არ არის ამომწურავი სია, არამედ არასამთავრობო ორგანიზაციების იმ ძირითადი ფუნქციების მოკლე მიმოხილვაა, რომლებსაც უსაფრთხოების სამსახურების ზედამხედველობაში წვლილი შეაქვთ. სამოქალაქო საზოგადოებრივი ორგანიზაციების ეფექტიანობა და ფარგლები დიდწილად დამოკიდებულია პოლიტიკურ კულტურაზე, რომელიც მოიცავს ხელისუფლების თანამშრომლობისთვის მზაობას, უსაფრთხოების სამსახურების გამჭვირვალობას, საზოგადოების ჩართულობასა და ინტერესს ამ საკითხებზე, ისევე როგორც მათზე ექსპერტული ცოდნის რესურსს.

209 *France, Constitutional Court, Decision n. 2016-590 QPC, 21 October 2016*

შერჩეული ქვეყნების საუკეთესო პრაქტიკები:

გერმანია

გერმანია ერთ-ერთი ის ქვეყანაა, სადაც მოსახლეობა და სამოქალაქო საზოგადოება საკმაოდ მგრძნობიარეა ამ თემების მიმართ და ჩართულია ფარული მეთვალყურეობის, პერსონალური ინფორმაციის, პირად ცხოვრების დაცვასთან დაკავშირებულ პროცესებში, ნაწილობრივ ქვეყნის ისტორიული კონტექსტის გათვალისწინებით. კონკრეტულად ამ საკითხებზე მუშაობს რამდენიმე საზოგადოებრივი ორგანიზაცია, მათ შორის გამორჩეულია Stiftung f□r Neue Verwaltung (SNV), Netzpolitik, Digitale Gesellschaft და საზოგადოება სამოქალაქო უფლებებისთვის.

კვლევის და ადვოკატირების საშუალებით ინფორმირებული საჯარო დებატების ხელშეწყობა: SNV აქვს სპეციფიური პროგრამა 'ციფრული ძირითადი უფლებები, ფარული მეთვალყურეობა და გამჭვირვალობა', რომელიც ატარებს კვლევას და ანალიზს სპეციალურ სამსახურებთან დაკავშირებულ კანონმდებლობასა და პრაქტიკაზე, ასევე შეიმუშავებს რეკომენდაციებს. პროგრამა ექსპერტთა წრეებისთვის განკუთვნილ კვლევებს აქვეყნებს, ასევე მედიაში ავრცელებს უფრო მოკლე სტატიებსა და თვალსაზრისებს, სადაც უბრალო, გასაგები ენით აღწერს სპეციალური სამსახურების პრობლემებსა და პირადი ცხოვრების უფლებასთან დაკავშირებულ რისკებს.[210]

სტრატეგიული სამართალწარმოება: მათი ევროპელი კოლეგების მსგავსად, არასამთავრობო ორგანიზაციები გერმანიაში აქტიურები არიან სასამართლოებში ფარულ ღონისძიებებთან დაკავშირებული კანონმდებლობის გასაჩივრების კუთხით. 2013 წელს, რეპორტიორები საზღვრების გარეშე გერმანიის წარმომადგენლობამ (RWB) BND-ს (გერმანიის სადაზვერვო სამსახური) წინააღდეგ საერთაშორისო კომუნიკაციების სტრატეგიული მიყურადების ღონისძიების შესახებ სარჩელი შეიტანა. რამდენიმეწლიანი სამართლებრივი დავის შემდგომ, 2017 წელს, საქმე წარედგინა გერმანიის ფედერალურ საკონსტიტუციო სასამართლოს, სადაც მათ შორის სტრატეგიული მეთვალყურეობის შემთხვევაში უფლების აღმდგენი სამართლებრივი საშუალების არარსებობა იყო სადავოდ გამხდარი.[211]

---

210 Publications (including those in English), and information on activities of SNV can be accessed at: https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency

211 EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.70

საკანონმდებლო პროცესის მონიტორინგი: სპეციალური სამსახურების საქმიანობისა და ადამიანის უფლებების საკითხებზე მომუშავე არასამთავრობო ორგანიზაციები ბელგიაში ყურადღებით აკვირდებიან საკანონმდებლო პროცესს. ცოტა ხნის წინ, რამდენიმე საზოგადოებრივმა ორგანიზაციამ გამოაქვეყნა საერთო საჯარო განცხადება მეტადატის შეგროვების შესახებ კანონპროექტის შესახებ.[212]

სტრატეგიული სამართალწარმოება: არასამთავრობო ორგანიზაციამ OBFG და სხვა ადამიანის უფლებებზე მომუშავე არასამთავრობო ორგანიზაციებმა კანონი პერსონალური ინფორმაციის შენახვის შესახებ ბელგიის საკონსტიტუციო სასამართლოში გაასაჩივრეს, იმ არგუმენტით, რომ კანონი საკმარისზე მეტ დისკრეციას განსაზღვრავს, და არაპროპორციული ღონისძიებების გამოყენების რისკებს ქმნის. საბოლოოდ, სასამართლომ კანონი გააუქმა და განმარტა, რომ კანონის ფარგლები ყველა ბელგიის მოქალაქის პერსონალურ მონაცემებს ეხებოდა, და არ იყო შეზღუდული იმ პირებით, რომელთა მიმართ არსებობს ეჭვი საზოგადოებრივი უსაფრთხოებისთვის საფრთხის შექმნის ან სერიოზული და კონკრეტული დანაშაულის ჩადენის შესახებ.[213]

212 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.3

213 Ibid. Also see (Belgium constitutional court, Case No. 84/2015, 11 June 2015.

ხორვატიამ მიიღო პროგრესული კანონმდებლობა სამოქალაქო საზოგადოების უსაფრთხოების სამსახურების ზედამხედველობაში ჩართულობის უზრუნველსაყოფად. ექსპერტთა ორგანოს 'უსაფრთოხებისა და დაზვერვის სამსახურების ზედამხედველობის სამოქალაქო საბჭო' სამართლებრივი საფუძველი, იძლევა აკადემიური წრეების წარმომადგენლების, ადამიანის უფლებების ექსპერტების და ადვოკატების, საბჭოში წევრად ჩართვის შესაძლებლობას.[214] საბჭოს ყოფილი წევრები იყვნენ კიდეც საზოგადოებრივი ორგანიზაციების წარმომადგენლები.[215]

კიდევ ერთი ახალი საუკეთესო პრაქტიკის მაგალითია, 2014 წლიდან უსაფრთხოებისა და დაზვერვის სააგენტოს (SOA) მიერ ყოველწლიური ანგარიშების საჯაროდ გამოქვეყნების პრაქტიკა. ამ გზით, SOA ანგარიშს წარუდგენს საზოგადოებრივ ორგანიზაციებს და მასზე მოსაზრებების გამოთქმის საშუალებას იძლევა.[216]

უსაფრთხოების სამსახურების სამართლებრივი საფუძვლის და საქმიანობის შესწავლა: ზოგიერთი არასამათავრობო ორგანიზაცია ხორვატიაში აქტიურად არის ჩართული სამსახურების საქმიანობის მონიტორინგში. ცოტა ხნის წინ, მშვიდობის კვლევების ცენტრმა და აქტივისტურმა ორგანიზაციამ 'Are You Syrius?', გამოაქვეყნა ანგარიში, რომელიც უსაფრთხოების სამსახურის (SOA) როლს იკვლევს უცხოელების და თავშესაფრის მაძიებელი პირების სპეციალურ შემოწმებაში. ინდვიდუალური საქმის მასალების და კანონმდებლობის შესწავლის შედეგად, არასამათავრობო ორგანიზაციებმა რამდენიმე პრობლემური პრაქტიკის იდენტიფიცირება მოახდინეს და შესაბამისი რეკომენდაციები შეიმუშავეს.[217]

214 Article 110 of the SOA Law https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf
215 Council of Europe, Democratic and Effective Oversight of National Security Services, (2015), p.48
216 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016)
217 The report can be accessed: http://www.asylumineurope.org/news/04-05-2017/croatia-increasing-rejections-asylum-claims-based-classified-security-reasons

საკანონმდებლო პროცესის მონიტორინგი და ინფორმირებული საჯარო დებატების ხელშეწყობა:

კანადას აქტიური სამოქალაქო საზოგადოება ჰყავს, განსაკუთრებით უსაფრთხოების და ადამიანის უფლებების დაცვის სფეროში. მთავრობის ღიაობა და ინსტიტუციური მექანიზმების არსებობა, რომლებიც კანონმდებლობაზე არასამთავრობო ორგანიზაციების დასკვნების თავმოყრას გულისხმობს, დამატებით აძლიერებენ სამოქალაქო საზოგადოების ჩართულობას საკანონმდებლო პროცესში. უკანასკნელ პერიოდში, მთავრობამ 2015 წლის ანტიტერორისტულ კანონზე საზოგადოებრივი აზრის შესასწავლად საჯარო კონსულტაციის პროცესი წამოიწყო. რამდენიმე საზოგადოებრივმა ორგანიზაციამ (მათ შორის Openmedia, კანადელი ჟურნალისტები თავისუფალი გამოხატვისთვის (CJFA)) წარმოადგინეს მათი მოსაზრებები მასობრივ ფარულ ღონისძიებებთან დაკავშირებული საკითხების შესახებ და წამოიწყეს მასშტაბური საჯარო კამპანიები კანონის ყველაზე პრობლემური ნაწილების შესახებ საზოგადოების ინფორმირებისთვის, და მთავრობისთვის მათი პოზიციის გაზიარებისთვის საზოგადოებას პირდაპირი, ხელმისაწვდომი ონლაინ საშუალებებით უზრუნველყვეს.[218]

218 See http://www.cbc.ca/news/politics/liberal-security-bill-opposition-1.4297316 , http://www.cjfe.org/6_reasons_why_you_should_participate_in_the_national_security_consultation and https://act.openmedia.org/security

გასაიდუმლოებასა და გამჭვირვალობას შორის ბალანსის შენარჩუნება არის უსაფრთხოების სამსახურის მართვის შესახებ დებატების ერთ-ერთი მთავარი სამსჯელო საკითხი. მაშინ როცა გასაგებია მიზიზები, თუ რატომ თან სდევს საიდუმლოების გარკვეული ხარისხი უსაფრთხოების სამსახურის საქმიანობას, საკმარისი ინფორმაციის გარეშე, ზედამხედველობის ორგანოებისთვის შეუძლებელი იქნებოდა უსაფრთხოების სამსახურის პოლიტიკისა და საქმიანობის კანონიერებასა და ეფექტიანობაზე დაკვირვება. უკანასკნელი ათწლეულების განმავლობაში საერთაშორისო დონეზე შემუშავდა გამჭვირვალობის შესახებ სტანდარტები, განსაკუთრებით აღსანიშანავია გლობალური პრინციპები ეროვნული უსაფრთხოებისა და ინფორმაციაზე უფლების შესახებ (The Tshwane Principles)[219] და გაეროს საუკეთესო პრაქტიკების მიმოხილვა. ეს თავი შეეხება უსაფრთხოების სამსახურების გამჭვირვალობის ზოგად სტანდარტებსა და საკუთარ პერსონალურ მონაცემებზე ხელმისაწვდომობის უფლებასთან დაკავშირებულ საკითხებს.

4.1. ზოგადი სტანდარტები გამჭვირვალობისა და ინფორმაციის ხელმისაწვდომობის შესახებ

- ***საჯაროდ ხელმისაწვდომი კანონები:*** გამჭვირვალობის ყველაზე ფუნდამენტური სტანდარტის თანახმად, უსაფრთხოების სამსახურები უნდა შეიქმნას საჯაროდ ხელმისაწვდომი კანონების საფუძველზე. გაეროს საუკეთესო პრაქტიკების მიმოხილვის მე–4 პრაქტიკის თანახმად: *„ყველა სადაზვერვო სამსახური შექმნილია/ჩამოყალბებულია და მოქმედებს საჯაროდ ხელმისაწვდომი კანონებით, რომლებიც შეესაბამება კონსტიტუციას და ადამიანის უფლებათა საერთაშორისო სამართალს. სპეციალურ სამსახურებს შეუძლიათ განახორციელონ ან მათ შესაძლოა მიეცეთ მითითება განახორციელონ მხოლოდ ის საქმიანობა, რომლიც დადგენილია ეროვნული კანონმდებლობით და რომელიც შეესაბამება აღნიშნულ კანონმდებლობას.“*

- ***საიდუმლო რეგულაციები:*** ზოგადად აღიარებული ფაქტია, რომ საჯაროდ ხელმისაწვდომი კანონების გარდა, უსაფრთხოების სამსახურების საქმიანობა რეგულირდება საიდუმლო კანონქვემდებარე აქტებით (მინისტრის ბრძანებები და სხვა), რომელთა გასაჯაროებაც აკრძალულია. ასეთი რეგულაციები ხშირად მოიცავს უსაფრთხოების სამსახურების სამოქმედო პროცედურებისა და საქმიანობის მეთოდების აღწერას, რომელთა გამჟღავნებითაც შესაძლოა საფრთხე შეექმნას უსაფრთხოების სამსახურის ღონისძიებათა მიმდინარეობას.[220] თუმცა, გაეროს სახელმძღვანელო დოკუმენტის თანახმად, აღნიშნული კანონქვემდებარე აქტების გამოყენება მკაცრად უნდა იყოს შეზღუდული და ასეთი საიდუმლო სამართლებრივი აქტები არ უნდა იქნეს გამოყენებული ნებისმიერი ისეთი ღონისძიების განხორციელების საფუძვლად, რომელიც ზღუდავს ადამიანის უფლებებს.[221] მაგალითად, აღნიშნული სამსახურების მიერ ჩატარებული მეთვალყურეობის ფარგლები უნდა რეგულირდებოდეს კანონით და არა საიდუმლო დირექტივებით.

- ***ინფორმაციაზე წვდომის მარეგულირები კანონმდებლობის და შეზღუდვები:*** დემოკრატიულ

219 The Tshwane Principles, available from https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles

220 Aidan Wills, Understanding Intelligence Oversight,(DCAF.2010) p.14

221 UN Compilation of Good Practices, Practice 4.

საზოგადოებაში ინფორმაციის თავისუფლების კანონები ქმნიან გამჭვირვალობის პრინციპის დანერგვის საფუძველს. თუმცა ასეთ კანონებს, ჩვეულებრივ, თან ახლავს გარკვეული შეზღუდვები. საუკეთესო პრაქტიკად მიიჩნევა ისეთი რეგულაციები, რომლის თანახმადაც უსაფრთხოების სამსახურები სრულად არ თავისუფლდებიან ამ კანონების მოთხოვნებისგან, არამედ ამის სანაცვლოდ უფლება ეძლევათ ეროვნული უსაფრთხოების დაცვის მიზნებიდან გამომდინარე ისარგებლონ საკანონმდებლო დონეზე ზუსტად განსაზღვრული გამონაკლისებითა და შეზღუდვებით.[222] ევროკავშირის ყველა წევრი ქვეყნის კანონმდებლობა შეიცავს ეროვნული უსაფრთხოების წინაშე არსებული გამოწვევებიდან ან/და უსაფრთხოების სამსახურების მიზნების შეუსრულებლობის საფრთხიდან გამომდინარე ინფორმაციაზე ხელმისაწვდომობის უფლების გარკვეული დოზით შეზღუდვის მექანიზმს.[223]

- ***შეზღუდვები ინფორმაციის ხელმისაწვდომობაზე:*** სასიცოცხლოდ მნიშვნელოვანია, თუ რა ფორმით და როგორ ადგენს აღნიშნულ შეზღუდვებს კანონი. ეროვნული უსაფრთხოებისა და ინფორმაციაზე უფლების შესახებ გლობალური პრინციპებმა დაადგინა ყოვლისმომცველი სტანდარტი ასეთი შეზღუდვების შესახებ. მე–3 პრინციპი ადგენს, რომ: „ეროვნული უსაფრთხოების ინტერესებიდან გამომდინარე ინფორმაციაზე უფლების შეზღუდვა არ შეიძლება დაწესდეს, გარდა იმ შემთხვევისა როდესაც მთავრობას შეუძლია დაამტკიცოს, რომ: (1) შეზღუდვა (ა) კანონითაა დადგენილი და (ბ) აუცილებელია დემოკრატიულ საზოგადოებაში (გ) ეროვნული უსაფრთხოების ლეგიტიმური ინტერესის დასაცავად; და (2) კანონი ითვალისწინებს შესაბამის დაცვის გარანტიებს აღნიშნულის ბოროტად გამოყენების თავიდან ასაცილებლად, რაც მოიცავს დამოუკიდებელი ზედამხედველობის ორგანოს მიერ შეზღუდვის კანონიერების სწრაფი, სრული, ხელმისაწვდომი და ეფექტიანი შემოწმების მექანიზმის არსებობას და სასამართლოების მხრიდან ყოველმხრივი და სრული განხილვის წარმოებას.“ ეს სტანდარტი შეზღუდვის აუცილებლობის დასაბუთების ტვირთს მთავრობას აკისრებს, ხაზს უსვამს ეროვნული უსაფრთხოების ინტერესების ლეგიტიმაციას და საჭიროდ მიიჩნევს ამგვარი შეზღუდვების ეფექტური გარე და სასამართლო ზედამხედველობის მექანიზმის დანერგვას.

- ***ლეგიტიმურად გასაიდუმლოებული ინფორმაცია:*** მაშინ როცა ინფორმაციის ხელმისაწვდომობის შეზღუდვა უმეტეს შემთხვევაში ეფუძნება „ეროვნული უსაფრთხოების“ დაცვის ინტერესებს, საერთაშორისო დონეზე არ არსებობს სავალდებულო და სრულყოფილი ჩამონათვალი თუ რა სახის ინფორმაცია უნდა იქნეს გასაიდუმლოებული. მიუხედავად ამისა, ექსპერტების მოსაზრებებისა და საერთაშორისო საუკეთესო პრაქტიკის საფუძველზე, ეროვნული უსაფრთხოებისა და ინფორმაციაზე უფლების შესახებ გლობალური პრინციპებმა დაადგინა ისეთი ინფორმაციის ჩამონათვალი, რომელზე წვდომაც საზოგადოებას კანონიერად შეიძლება შეეზღუდოს, კერძოდ:[224]

  - ინფორმაცია მიმდინარე თავდაცვის გეგმების, ოპერაციებისა და შესაძლებლობების შესახებ იმ დროის ხანგრძლივობით, როცა აღნიშნული ინფორმაცია უსაფრთხოების მიზნებისთვის გამოყენებადია.

  - ინფორმაცია იარაღისა და სხვა სამხედრო სისტემების (მათ შორის საკომუნიკაციო სისტემების) წარმოების, მათი შესაძლებლობების ან გამოყენების შესახებ.

  - ინფორმაცია სახელმწიფოს ტერიტორიის, კრიტიკული ინფრასტრუქტურის ან კრიტიკული ეროვნული ინსტიტუტების არსებული საფრთხეებისაგან, ძალის გამოყენების ან საბოტაჟისაგან

222 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005), p.,.44

223 *EU FRA Surveillance by Intelligence Services (2015)*, p.62

224 Tshwane Principles, Part II, Principle 9

დაცვის სპეციალური ღონისძიებების შესახებ, რომელთა ეფექტიანობა მათ გასაიდუმლოებაზეა დამოკიდებული;

- ინფორმაცია რომელიც სადაზვერვო სამსახურების მიერ მოპოვებულია შესაბამისი ღონისძიების, წყაროს ან/და რომელიმე სადაზვერვო მეთოდის გამოყენებით ან უკავშირდება მათ, თუ აღნიშნული ინფორმაცია შეეხება ეროვნული უსაფრთხოების საკითხებს; და

- ინფორმაცია ეროვნული უსაფრთხოების საკითხებთან დაკავშირებით, რომელიც კონფიდენციალურობის დაცვის მოლოდინით მოწოდებულ იქნა უცხო ქვეყნის ან სამთავრობოთაშორისი ორგანოს მიერ, ასევე დიპლომატიური კომუნიკაციის გზით მიღებული სხვა ინფორმაცია, რომლებიც ეხება ეროვნული უსაფრთხოების საკითხებს.

► ***ინფორმაციის გასაიდუმლოება:*** შეთანხმების პირობებში, რომ გარკვეული ინფორმაცია შეიძლება არ იქნეს გასაჯაროებული, არსებობს სტანდარტები იმის შესახებ, თუ როგორ უნდა ცნოს სახელმწიფომ ასეთი ინფორმაცია საიდუმლოდ. პირველ რიგში, ჩამონათვალი თუ რა უნდა იქნეს გასაიდუმლოებული უნდა შეეხებოდეს ინფორმაციის ტიპს და არა დოკუმენტებს. ამ მიდგომით შესაძლებელი იქნება დოკუმენტების გასაჯაროება საიდუმლო ინფორმაციის შემცველი ნაწილის რედაქტირებითა და დოკუმენტის დანარჩენი ნაწილის საზოგადოებისათვის ხელმისაწვდომობით.[225] ეროვნული უსაფრთხოებისა და ინფორმაციაზე უფლების შესახებ გლობალური პრინციპები მოიცავს გასაიდუმლოების შემდეგ გასატარებელი ღონისძიებების დეტალურ აღწერას, მათ შორის, მთავრობის ვალდებულებას, დაასაბუთოს გასაიდუმლოების საჭიროება (პრინციპი მე-11), მონაცემების გასაიდუმლოების მართვის პროცედურებში საზოგადოების ჩართულობას (პრინციპი მე–12), გასაიდუმლოების ვადების შეზღუდვის შესახებ ინფორმაციის და გასაიდუმლოების შესახებ გადაწყვეტილებების პერიოდული განხილვის/გადასინჯვის მექანიზმს (პრინციპი 16).

► ***უსაფრთხოების სამსახურების ყოველწლიური საჯარო ანგარიშები:*** მიუხედავად იმისა, რომ არ არსებობს საერთაშორისოდ აღიარებული სტანდარტი მომსახურების წლიური ანგარიშების შინაარსსა და მოცულობაზე, საუკეთესო პრაქტიკა მოიაზრებს, რომ ის უნდა მოიცავდეს:[226]

- უსაფრთხოების სამსახურების საქმიანობის ძირითად პრიორიტეტებს;

- უსაფრთხოებისათვის რისკის შემქმნელი ძირითადი ფაქტორების მიმოხილვას;

- უსაფრთხოების/დაზვერვის პოლიტიკასთან დაკავშირებულ მნიშვნელოვანი ცვლილებებს;

- ინფორმაციასა და სტატისტიკას ანგარიშვალდებულების ფუნქციების შესახებ, მათ შორის რეაგირების ღონისძიებების აღწერას ინფორმაციის წვდომის შესახებ მოთხოვნებზე.

4.2. სტანდარტები საკუთარ პერსონალურ მონაცემებზე ხელმისაწვდომობის უფლების შესახებ

გამჭვირვალობის შეფასების ძირითადი ასპექტია უსაფრთხოების სამსახურებში შენახულ პირის საკუთარ მონაცემებზე წვდომის უფლება. პერსონალური მონაცემების ავტომატური დამუშავებისაგან პირთა დაცვის შესახებ ევროპის საბჭოს კონვენცია[227] პირადი მონაცემების ავტომატური დამუშავების

225 Laurie Nathan, 'Intelligence Transparency, Secrecy and Oversight in a Democracy', p.55 in Born and Wills (ed.) *Overseeing Intelligence Services: A Toolkit* (DCAF: 2012)
226 Ibid, p.57
227 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

თვალსაზრისით წარმოადგენს პირველ სავალდებულო იურიდიულ ინსტრუმენტს, რომელიც ადგენს მონაცემთა შეგროვებისა და დამუშავების სტანდარტებს და რომელიც აშკარად აღიარებს მონაცემთა სუბიექტების უფლებებს (რომელთა შესახებ ხდება მონაცემების შეგროვება). კონვენციის მე-8 მუხლი ადგენს, რომ:

„ნებისმიერი პირი უფლებამოსილი უნდა იყოს:

ა) დაადგინოს/შეამოწმოს ავტომატური პერსონალური მონაცემების ფაილის არსებობა, მისი ძირითადი მიზნები, აგრეთვე ფაილის დამმუშავებლის ვინაობა, მისი საცხოვრებელი ადგილი ან საქმიანობის ძირითადი ადგილი;

ბ) გონივრულ ვადაში, გადამეტებული დაყოვნების ან ხარჯების გარეშე მიიღოს ინფორმაცია, ინახება თუ არა მისი პერსონალური მონაცემები ავტომატური დამუშავების ფაილებში, მიიღოს ამ მონაცემების შესახებ ინფორმაცია მისთვის გასაგები ფორმით;

გ) მოითხოვოს ცვლილებების შეტანა მონაცემებში ან მათი წაშლა თუ მონაცემების დამუშავების პროცესი (მიღება, გასწორება ან/და ამოღება) ეწინააღმდეგება შიდა კანონმდებლობით დადგენილ რეგულაციებს კონვენციის მე-5 და მე-6 მუხლებით გათვალისწინებულ ძირითად პრინციპებთან კავშირში;

დ) ისარგებლოს უფლების აღმდგენი საშუალებით, თუ მისი მოთხოვნა დადასტურების ან, საჭიროების შემთხვევაში, მონაცემების გასწორების ან წაშლის შესახებ, წინამდებარე მუხლის “ბ” და “გ” ქვეპუნქტებთან საპირისპიროდ შეუსრულებელი იქნება’

ამ სამართლებრივად მბოჭავი ძალის მქონე კონვენციის დებულებები ითვალისწინებს უსაფრთხოების სამსახურების მკაფიო ვალდებულებებს, მოახდინონ რეაგირება პირადი მონაცემების შესახებ მოთხოვნებზე, გააცნოს ინფორმაცია მონაცემების სუბიექტს, უკანონო შეგროვების/დამუშავების შემთხვევაში უზრუნველყოს შეგროვებული პერსონალური მონაცემების შესწორება ან წაშლა. თუმცა, კონვენციის მე-9 მუხლი უფლებას იძლევა, რომ უსაფრთხოების სამსახურებმა გადაუხვიონ მსგავს ვალდებულებებს “სახელმწიფო დაცვის, საზოგადოებრივი უსაფრთხოების, სახელმწიფოს მონეტარული ინტერესების ან სისხლის სამართლის დანაშაულთან ბრძოლის ინტერესების გათვალისწინებით”, აგრეთვე “მონაცემთა სუბიექტის ან სხვათა უფლებებისა და თავისუფლებების დაცვის მიზნით“.

ეს სტანდარტები არა მხოლოდ ევროპის საბჭოს კონვენციითაა აღიარებული, არამედ საერთაშორისო სამართლის სარეკომენდაციო ხასიათის მექანიზმებითაც, როგორიცაა გაეროს სახელმძღვანელო პრინციპები კომპიუტერული პერსონალური მონაცემების ფაილების რეგულირების შესახებ (პრინციპი 4)[228], ეროვნული უსაფრთხოებისა და ინფორმაციაზე უფლების შესახებ გლობალური პრინციპები (III ნაწილი), ასევე გაეროს საუკეთესო პრაქტიკების მიმოხილვა (პრაქტიკა 26). ამ ევროპული და საერთაშორისო სტანდარტების შესაბამისად, დემოკრატიული ქვეყნების უდიდესმა ნაწილმა მიიღო შესაბამისი კანონები ეროვნულ დონეზე და დაადგინა მექანიზმები საკუთარი მონაცემების მიღების უფლების დაცვისა და რეალიზების მიზნით. ამ საკითხთან მიმართებით სამი ძირითადი მიდგომა არსებობს:

მონაცემთა სუბიექტის მიერ ინფორმაციაზე პირდაპირი წვდომა: ბევრ ქვეყანას აქვს კანონები, რომლებიც საშუალებას აძლევს მონაცემთა სუბიექტს უშუალოდ მიმართოს უსაფრთხოების სამსახურს და მოითხოვოს წვდომა მისივე პერსონალურ მონაცემებზე. თუმცა ასეთი კანონები გარკვეულ შეზღუდვებსაც ითვალისწინებს, რაც საშუალებას აძლევს უსაფრთხოების სამსახურებს არ მიაწოდონ

228 General Assembly Resolution 45/95 (1990), available from : http://www.refworld.org/pdfid/3ddcafaac.pdf

პირს მის შესახებ არსებული ინფორმაცია თუ არსებობს საფრთხე იმისა, რომ აღნიშნულმა ხელი შეუშალოს მიმდინარე გამოძიების პროცესს, ასევე უსაფრთხოების სამსახურების წყაროებისა და მეთოდების დაცვას.[229] ამ თვალსაზრისით მნიშვნელოვანი სტანდარტია ის, რომ ასეთი გამონაკლისი შემთხვევები კანონით უნდა იყოს დადგენილი და კანონი უნდა შეიცავდეს მონაცემთა სუბიექტის მიერ ამ გადაწყვეტილების სასამართლოში გასაჩივრების უფლებას.[230]

არაპირდაპირი წვდომა საექსპერტო ზედამხედველობის ორგანოს ან პერსონალური ინფორმაციის დაცვის სააგენტოს (DPA) მეშვეობით: სუბიექტის მონაცემებზე წვდომის შეზღუდვების დასაბალანსებლად, ზოგიერთი სახელმწიფო აღნიშნულ ინფორმაციაზე წვდომის უფლებას მათი სახელით ანიჭებს მონაცემთა დაცვის ან/და საექსპერტო ზედამხედველობის ორგანოებს. ამ თვალსაზრისით, საუკეთესო პრაქტიკის მაგალითია, როდესაც ამ ორგანოებს უფლება აქვთ შეამოწმონ იყო თუ არა დასაბუთებული მონაცემთა სუბიექტის ხელმისაწვდომობის შეზღუდვა, განიხილონ აღნიშნული მონაცემები იყო თუ არა კანონიერად შეგროვებული/მოპოვებული და დაადგინონ მონაცემთა განადგურების საჭიროება თუ აღმოჩენილ იქნა რაიმე კანონის დარღვევა.[231] ეს მიდგომა მიღებულია ევროკავშირის 12 წევრ ქვეყანაში, მათ შორის ავსტრიაში, ბელგიაში, ბულგარეთში, კვიპროსში, ფინეთში, საფრანგეთში, უნგრეთში, ირლანდიაში, იტალიაში, ლუქსემბურგში, პორტუგალიასა და შვედეთში.[232]

უსაფრთხოების სამსახურის მიერ მონაცემთა სუბიექტისათვის შეტყობინების გაგზავნა: ბოლოს, განვითარებული, თუმცა ჯერჯერობით არა ფართოდ გავრცელებული მიდგომა არის უსაფრთხოების სამსახურების დავალდებულება შეატყობინოს მონაცემთა სუბიექტს მას შემდეგ რაც მის მიმართ დასრულდება ფარული მეთვალყურეობის ღონისძიებები, მონაცემთა სუბიექტის ან/და საექსპერტო ზედამხედველობის ორგანოს მოთხოვნის მიუხედავად.

ზემოთ მოყვანილი მიდგომები არ არის ურთიერთგამომრიცხავი და ქვეყანას შეუძლია ისინი ერთობლივად გამოიყენოს.

229 UN Compilation, para 40.

230 Laurie Nathan, 'Intelligence Transparency, Secrecy and Oversight in a Democracy', p.55 in Born and Wills (ed.) Overseeing Intelligence Services: A Toolkit (DCAF: 2012)

231 EU FRA, Surveillance by Intelligence Services ,Vol 2, (2017), p.110, Also see Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, (DCAF: 2005)

232 EU FRA, Surveillance by Intelligence Services Vol 2, (2017), p.126

ხორვატია

საჯაროდ ხელმისაწვდომი კანონები და საიდუმლო რეგულაციები: ხორვატიის უსაფრთხოების სამსახური (SOA) საქმიანობას ახორციელებს საჯაროდ ხელმისაწვდომი კანონის საფუძველზე. საერთაშორისო სტანდარტების შესაბამისად, კანონი პირდაპირ განსაზღვრავს სტანდარტებს მეთვალყურეობისა და ინფორმაციის შეგროვების სხვა ისეთი ფარული ღონისძიებების და ინფორმაციის მოპოვების ფარული ღონისძიებების შესახებ, რომლებიც შესაძლოა არღვევდეს ადამიანის უფლებებსა და თავისუფლებებს (SOA-ს კანონის 33-37 მუხლები), ასევე ადგენს ავტორიზაციისა და ზედამხედველობის პროცედურებს. თუმცა, ქვემოთ ჩამოთვლილი საკითხების შესახებ არსებული რეგულაციები გასაიდუმლოებულია და შესაბამისად საზოგადოებისათვის არაა ხელმისაწვდომი (კანონის 62-65 მუხლები):

- უსაფრთხოების სამსახურის შიდა სტრუქტურა, საქმიანობის სფერო/ფარგლები და შიდა დანაყოფების მართვა,
- თანამშრომლების საჭირო რაოდენობა, მათი სამუშაო მოთხოვნები, ფუნქციები და ამოცანები,
- უსაფრთხოების/სადაზვერვო ღონისძიებები, პროცედურები და საშუალებები, რომლებსაც იყენებსს SOA საქმიანობის განხორციელებისას.

ინფორმაციის ხელმისაწვდომობა და მასთან დაკავშირებული შეზღუდვები: ხორვატიაში ინფორმაციის ხელმისაწვდომობა რეგულირდება კანონით ინფორმაციის ხელმისაწვდომობის უფლების შესახებ.[233] კანონის მე-15 მუხლი შეიცავს ფართო ჩამონათვალს იმ პირობებისა, რომლის საფუძველზეც შესაძლებელია შეიზღუდოს ინფორმაციის ხელმისაწვდომობა, რომელთაგან ერთ-ერთი საფუძველია „საჯარო დაწესებულებების მიერ ინფორმაციის გასაიდუმლოება“.

ინფორმაციის გასაიდუმლოება: „მონაცემთა საიდუმლოების შესახებ აქტით“[234], რომელიც არეგულირებს ინფორმაციის გასაიდუმლოების პროცედურებს, დადგენილია, რომ SOA-ს დირექტორი არის უფლებამოსილი განსაზღვროს ის ინფორმაცია, რომლის გამჟღავნება ზიანს მიაყენებს სახელმწიფო უშიშროებას ან სახელმწიფო ხელისუფლების ორგანოების ფუნქციონირებას (6-9 მუხლები). ამ თვალსაზრისით, მეთვალყურეობის ღონისძიებებთან დაკავშირებული პირადი მონაცემები მიზნის მიხედვით შესაძლოა დაიყოს, როგორც სრულიად საიდუმლო, საიდუმლო, კონფიდენციალურ ან შეზღუდული სარგებლობის ინფორმაციად.[235] ინფორმაციის გასაიდუმლოების პროცესში SOA-ს ფართო უფლებამოსილებების გათვალისწინებით, არსებობს საფრთხე, რომ პრაქტიკაში საზოგადოების დაშვება ინფორმაციაზე მნიშვნელოვნად შეზღუდული იყოს.

ხორვატია მისდევს „ინფორმაციაზე მონაცემთა სუბიექტის პირდაპირი წვდომის“ მიდგომას. SOA-ს კანონის მე-40 მუხლი ადგენს, რომ SOA ვალდებულია მოთხოვნიდან 15 დღის განმავლობაში

233 http://www.revizija.hr/en/access-to-information/law-on-the-right-to-access-information
234 http://europam.eu/data/mechanisms/FOI/FOI%20Laws/Croatia/Croatia_Data%20Secrecy%20Act_2007.pdf
235 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.7

აცნობოს მონაცემთა სუბიექტს საიდუმლო ინფორმაციის შეგროვებისას მის მიმართ გამოყენებული ღონისძიებები და მათი მოთხოვნის შემთხვევაში უზრუნველყოს მონაცემთა სუბიექტის დაშვება შეგროვებულ ინფორმაციასთან. თუმცა ამავე მუხლის თანახმად, დაწესებულია ფართო შეზღუდვები ამ უფლებას გამოყენებაზე, რომელიც აძლევს შესაძლებლობას SOA-ს არ გაასაჯაროს მონაცემები, თუ ინფორმაციის გამჟღავნებამ შესაძლოა (i) საფრთხე შეუქმნას სააგენტოს მიერ მასზე დაკისრებული ამოცანების შესრულებას, (ii) სხვა პირის უსაფრთხოებას ან/და (iii) გამოიწვიოს ისეთი შედეგები,რომლებიცსაზიანოა ეროვნული უსაფრთხოებისა და ხორვატიის რესპუბლიკის ეროვნული ინტერესებისათვის. იმ შემთხვევაში, თუ მონაცემთა სუბიექტს სურს ინფორმაციის გასაჯაროებაზე უარის თქმის შესახებ SOA-ს გადაწყვეტილების გასაჩივრება, მას შეუძლია მიმართოს ინფორმაციის კომისარს, რომელსაც აქვს უფლება იმსჯელოს იმაზე გამოიყენა თუ არა SOA- მ „პროპორციულობის“ ტესტი ინფორმაციის გასაიდუმლოებამდე. უსაფრთხოების და სადაზვერვო სააგენტოების სამოქალაქო ზედამხედველობის საბჭო (ექსპერტთა საზედამხედველობ ორგანო) ასევე უფლებამოსილია გააკონტროლოს SOA-ს მიერ ინფორმაციის გასაიდუმლოების პროცედურის კანონმდებლობასთან შესაბამისობა, მაგრამ ჯერჯერობით საბჭოს მიერ აღნიშნული უფლებამოსილება არასდროს ყოფილა გამოყენებული. საზედამხედველო ორგანოების ეს სამართლებრივი შეზღუდვები პრაქტიკულად შეუძლებელს ხდის პირის მიერ საკუთარ პერსონალურ მონაცემებზე წვდომას.[236]

SOA-ს წლიური ანგარიშები: SOA აქვეყნებს ყოველწლიურ ანგარიშს, რომელიც ხელმისაწვდომია ვებ-გვერდზე. ანგარიშები დაახლოებით 30 გვერდია და მოიცავს უსაფრთხოების ძირითადი გამოწვევებისა და SOA-ს მიერ სპეციალური შემოწმების ღონისძიებების მიმოხილვას, ასევე საერთაშორისო თანამშრომლობის შესახებ ინფორმაციასა და ბიუჯეტთან დაკავშირებულ ძირითად საკითხებს.

236 Ibid.

საჯაროდ ხელმისაწვდომი კანონები და საიდუმლო რეგულაციები: კანადის უსაფრთხოების სამსახური (CSIS) საქმიანობას ახორციელებს საჯაროდ, კანადის ორივე ოფიციალურ სახელმწიფო ენაზე ხელმისაწვდომი კანონის საფუძველზე. კანონი დეტალურად ადგენს ინფორმაციის შეგროვების ისეთ პროცედურებს, რომლის დროსაც არსებობს ადამიანის უფლებების დარღვევის საფრთხე. აღნშნული ნორმები სრულად შეესაბამება საერთაშორისო სტანდარტებს. მიუხედავად იმისა, რომ მინისტრის ბრძანებები საჯარო არ არის, კანადა იზიარებს საუკეთესო საერთაშორისო პრაქტიკას, რადგანაც დადგენილია CSIS-ის ვალდებულება, რომ ყველა ბრძანება გაეგზავნოს საზედამხედველო კომიტეტს (იხ. მე-2 თავი გარე კონტროლის შესახებ).

ინფორმაციის ხელმისაწვდომობა: კანადას აქვს ერთ-ერთი ყველაზე სრულყოფილი კანონმდებლობა ინფორმაციის თავისუფლების უზრუნველყოფის კუთხით. ინფორმაციის ხელმისაწვდომობის აქტის[237] 13-16 მუხლები ითვალისწინებს გამონაკლისს მთავრობის ვალდებულებისაგან საჯარო გახადოს ინფორმაცია. თუმცა, ამავე კანონით დეტალურად არის წარმოდგენილი ინფორმაციის ხელმისაწვდომობაზე უარის თქმის შესახებ საჯარო დაწესებულების გადაწყვეტილების გასაჩივრების პროცედურა. საინფორმაციო კომისარს უფლება აქვს მიიღოს, განიხილოს და გამოიძიოს სამთავრობო დაწესებულებების მიერ ინფორმაციის გასაჯაროებაზე უარის თქმის შესახებ შემოსული განცხადებები/საჩივრები (მუხლი 30-36). გამოძიების შედეგებზე დაყრდნობით, კომისარი სახელმწიფო დაწესებულებას უწევს რეკომენდაციას შესაბამისი ღონისძიებების განხორციელების თაობაზე (მუხლი 37). თუ სახელმწიფო დაწესებულება ინფორმაციის კომისარის რეკომენდაციის მიუხედავად მაინც უარს აცხადებს ინფორმაციის გაცემაზე, მომჩივანს აქვს უფლება მიმართოს ფედერალურ სასამართლოს (მუხლი 41). ამდენად, საერთაშორისო სტანდარტების შესაბამისად, კანადის კანონი ინფორმაციის ხელმისაწვდომობაზე უარის შემთხვევაში სამართლებრივი დაცვის მყარ მექანიზმებს ითვალისწინებს.

საკუთარ პერსონალურ მონაცემებზე წვდომა: პირადი ცხოვრების დაცვის აქტი[238] არეგულირებს სამთავრობო დაწესებულებაში დაცულ პერსონალურ ინფორმაციაზე წვდომის პროცედურებს. აქტი განსაზღვრავს თუ რა იგულისხმება ტერმინში - „პერსონალური მონაცემი“, პერსონალურ მონაცემებზე წვდომის პროცედურებს, ასევე პირის მიერ საკუთარ პერსონალურ მონაცემებზე წვდომის უფლების შეზღუდვის საფუძვლებს. თუ პირს უარი ეთქვა საკუთარ პერსონალურ მონაცემებთან დაშვებაზე, მას შეუძლია საჩივარი შეიტანოს პირადი ცხოვრების დაცვის კომისართან. ამ დროს, მოქმედებს ინფორმაციაზე წვდომის შესახებ კანონით გათვალისწინებული მსგავსი უფლების აღმდგენი ღონისძიება, როგორიცაა ფედერალური სასამართლოს მიერ შემოწმება (პირადი ცხოვრების დაცვის აქტის მუხლი 41).

საუკეთესო საერთაშორისო პრაქტიკის დანერგვის მიზნით, კანადის უსაფრთხოების სამსახურმა CSIS-მა შექმნა „ინფორმაციაზე წვდომისა და კონფიდენციალურობის დაცვის“ უზრუნველყოფაზე პასუხისმგებელი სპეციალური სტრუქტურული დანაყოფი. ეს სტრუქტურული დანაყოფი იღებს და ამუშავებს ინფორმაციის ხელმისაწვდომობასა და კონფიდენციალურობაზე შემოსულ ყველა მოთხოვნას და სხვა ამოცანებთან ერთად ხელს უწყობს პირებს მათი მოთხოვნის ფორმულირებაში. აღნიშნული დანაყოფი ყოველწლიურად აქვეყნებს მათი მუშაობის შესახებ სრულყოფილ ინფორმაციას, რომელიც მოიცავს დეტალურ სტატისტიკურ მონაცემებს ინფორმაციის მიღებასთან დაკავშირებული მოთხოვნების შესახებ, გაცემული/გასაჯაროებული დოკუმენტების რაოდენობას, საგამონაკლისო წესების გამოყენების შემთხვევებს და ა.შ. ეს სპეციალური სამსახურების მიერ ინფორმაციასა და

237 http://laws-lois.justice.gc.ca/eng/acts/A-1/FullText.html
238 http://laws-lois.justice.gc.ca/PDF/P-21.pdf

პერსონალურ მონაცემებზე პირის წვდომის მოპოვებისა, ასევე მათ მიერ შესაბამისი მოთხოვნების დაყენების ხელშეწყობის მაგალითია.[239]

CSIS-ის ყოველწლიური ანგარიშები: CSIS-ის ყოველწლიური მოხსენებები სამაგალითოა, რადგან ის შეიცავს უსაფრთხოების სამსახურის შესახებ სრულ ინფორმაციას, მათ შორის საჯაროვდება თანამშრომელთა რაოდენობა, ჩაშლილი სტატისტიკა პერსონალის შესახებ (უმცირესობების, ქალების, შეზღუდული შესაძლებლობების მქონე პირთა რაოდენობა პერსონალის შემადგენლობაში); ასევე ბიუჯეტის შესახებ ინფორმაცია (ჩაშლილია თუ რა თანხები ხმარდება ბიუჯეტიდან ხელფასებს და რა ნაწილი ღონისძიებების ჩასატარებლად აუცილებელ ხარჯებს). გარდა ამისა, ანგარიშში წარმოდგენილია ინფორმაცია მიღებული საჩივრებისა და SIRC-ის (ექსპერტთა ზედამხედველობის ორგანო) ან/და სხვა საზედამხედველო ორგანოს მიერ მათი განხილვის შესახებ. ანგარიში არის ძალიან ინტერაქციული, ვიდეოებით, ინფოგრაფიკებითა და მკითხველზე მორგებული ტექსტებით გაჯერებული.[240]

239 The report of the unit can be accessed at: https://www.csis-scrs.gc.ca/tp/pblctns/2015-2016/nnlrprt-tp20152016-en.php

240 The report can be accessed at: https://www.csis-scrs.gc.ca/pblctns/nnlrprt/2014-2016/index-en.php#Unique

საჯაროდ ხელმისაწვდომი კანონები: ორივე BfV და BND მოქმედებენ საჯაროდ ხელმისაწვდომი კანონების საფუძველზე, რომლებიც დეტალურად განსაზღვრავენ ინფორმაციის შეგროვების ღონისძიებებს.

ინფორმაციაზე წვდომა: ფედერალურ დონეზე ინფორმაციის ხელმისაწვდომობის უფლება რეგულირდება ინფორმაციის თავისუფლების კანონით[241]. კანონი შეიცავს იმ გამონაკლისების ფართო ჩამონათვალს, რომელთა საფუძველზეც ფედერალურმა სახელმწიფო უწყებებმა შეიძლება უარი უთხრას პირს ინფორმაციასთან წვდომაზე. ეს გარემოებები მოიცავს იმ შემთხვევებს, როდესაც:

► ინფორმაციის გასაიდუმლოებას აქვს საზიანო შედეგები:

ა) საერთაშორისო ურთიერთობებზე,

ბ) ფედერალური შეიარაღებული ძალების სამხედრო და სხვა უსაფრთხოებისათვის მნიშვნელოვან ინტერესებზე,

გ) შიდა ან გარე უსაფრთხოების ინტერესებზე,

დ) ფინანსური, კონკურენციისა და მარეგულირებელი ორგანოების მონიტორინგისა და ზედამხედველობის ამოცანებზე,

ე) გარე ფინანსური კონტროლის საკითხებზე,

ვ) უკანონო საგარეო ვაჭრობის პრევენციის ზომებზე,

ზ) მიმდინარე სასამართლო პროცესის მსვლელობაზე,

- ინფორმაცია ექვემდებარება ოფიციალურ გასაიდუმლოებას,
- ინფორმაცია დაკავშირებულია უსაფრთხოების/სადაზვერვო სამსახურების მიერ სპეციალური შემოწმების ღონისძიებების განხორციელებასთან (აქტის მე-3 ნაწილი).

კანონით დადგენილი საუკეთესო პრაქტიკის მაგალითია ჩანაწერი, რომლის საფუძველზეც საჯარო დაწესებულება ინფორმაციასთან დაშვებაზე უარის გადაწვეტილების მიღებისას ვალდებულია აცნობოს პიროვნებას იმის შესახებ, თუ რამდენად და როდის ექნება პირს ამ ინფორმაციასთან ნაწილობრივი ან სრული დაშვების შესაძლებლობა მომავალში (ნაწილი 9 (2)). კანადის მოდელის მსგავსად, გერმანიის კანონი ითვალისწინებს უფლების აღდგენის/დაცვის მყარ სამართლებრივ საშუალებებს. ინფორმაციის გაცემაზე უარის თქმის შესახებ გადაწყვეტილება შეიძლება გასაჩივრდეს ადმინისტრაციულ სასამართლოში (მუხლი 9 (3)). გარდა ამისა, თუ პირს მიაჩნია, რომ დაირღვა მისი ინფორმაციის ხელმისაწვდომობის უფლება, შესაძლებლობა აქვს სასამართლოს ნაცვლად მიმართოს მონაცემთა დაცვის ფედერალურ კომისარს (ნაწილი 12 (1)).

საკუთარ მონაცემებზე წვდომა: პირის უფლება მოითხოვოს უსაფრთხოების სამსახურების ხელთ არსებული მის შესახებ პერსონალური ინფორმაცია, დარეგულირებულია კონსტიტუციის დაცვის შესახებ[242] და დაზვერვის სამსახურის შესახებ (BND Act) ფედერალური აქტებით. რაც შეეხება BfV–ს (შიდასახელმწიფოებრივი უსაფრთხოების სამსახური), მიუხედავად იმისა, რომ კანონი აღიარებს

241 https://www.gesetze-im-internet.de/englisch_ifg/englisch_ifg.html#p0021
242 https://www.gesetze-im-internet.de/bverfschg/

პირადი მონაცემების ხელმისაწვდომობის უფლება-პრინციპს, უფლების განხორციელების ფარგლები პრაქტიკაში მაინც ძალიან ვიწროდ განიმარტება. მონაცემთა სუბიექტმა უნდა მიუთითოს „სპეციფიური გარემოებების არსებობაზე“ და დაადასტუროს ინფორმაციაზე წვდომის მოთხოვნის “განსაკუთრებული ინტერესი”. მაშინაც კი როცა ეს პირობები შესრულებულია, BfV უფლებამოსილია პირს არ მისცეს არსებულ ინფორმაციაზე წვდომა, თუ ინფორმაციის გასაჯაროება: „ა) საფრთხეს შეუქმნის მისი ამოცანების განხორციელებას, ბ) რისკის ქვეშ აყენებს ინფორმაციის წყაროს ან არსებობს შიშის საფუძველი, რომ მოთხოვნა მიზნად ისახავს BfV-ის ცოდნის ან საოპერაციო მეთოდების მდგომარეობის შესწავლას, გ) შეიძლება საფრთხე შეუქმნას საზოგადოებრივ უსაფრთხოებას ან საზიანო გავლენა იქონიოს ფედერაციის ან გერმანიის სახელმწიფოს კეთილდღეობაზე, ან დ) წინააღმდეგობაში მოდის სამსახურის საიდუმლო სამართლებრივ სტატუსთან ან ინფორმაციის საიდუმლო შინაარსთან ან მესამე მხარის კანონიერ ინტერესებთან“.[243] მეტ-ნაკლებად ანალოგიური წესები ვრცელდება BND-ისაგან ინფორმაციის მოთხოვნაზე.

პირს შეუძლია ინფორმაციაზე დაშვების მოთხოვნით მიმართოს მონაცემთა დაცვის ფედერალურ კომისარს, როდესაც მისი მოთხოვნა არ არის დაკმაყოფილებული, რომელსაც თავის მხრივ შეუძლია მიმართოს უსაფრთხოების სამსახურს მონაცემთა სუბიექტის სახელით. თუმცა, კანადის მოდელისგან განსხვავებით, აღმასრულებელი ხელისუფლების ორგანოებს/წარმომადგენლებს (BfV - სთვის შინაგან საქმეთა სამინისტრო, ან BND-სთვის ფედერალური კანცლერი) შეუძლიათ დაბლოკონ მონაცემთა კომისრის გამოძიება, ეროვნული უსაფრთხოების მიზნებიდან გამომდინარე[244], რაც ვერ ჩაითვლება ყველაზე ოპტიმალურ პრაქტიკად მაგალითად კანადურ მოდელთან შედარებით.

მეთვალყურეობის სუბიექტის შეტყობინება: გერმანიამ დანერგა ინოვაციური მექანიზმი, რომლის თანახმადაც უსაფრთხოების სამსახურებს აქვთ ვადებულება შეატყობინონ მეთვალყურეობის სუბიექტებს მას შემდეგ, რაც მათ მიმართ მიმდინარე ფარული ღონისძიებები დასრულდება.[245] თუმცა აღნიშნულზე ვრცელდება გარკვეული დათქმები:

- მიზანმიმართული მეთვალყურეობის შესახებ მონაცემთა სუბიექტებს ინფორმაცია უნდა მიეწოდოთ ზედამხედველობის ღონისძიებების დასრულებიდან 12 თვის განმავლობაში, გარდა იმ შემთხვევისა თუ აღნიშნული ინფორმაციის გამჟღავნება საფრთხეს შეუქმნის ფარული მეთვალყურეობის ღონისძიებების მიზანს ან ზიანს მიაყენებს ქვეყნის ინტერესებს (G-10 კანონის მუხლი 12 (1)).

- თუ უსაფრთხოების სამსახურის მიერ იქნება მიღებული გადაწვეტილება, რომ 12 თვის შემდეგ არ აცნობონ მონაცემთა სუბიექტს, საქმე უნდა იქნეს განიხილული G-10 კომისიის მიერ, რომელიც იღებს გადაწყვეტილებას იმის შესახებ, თუ კიდევ რამდენ ხანს დარჩება აღნიშნული ინფორმაცია გასაიდუმლოებული.

- თუ G-10 კომისია ერთხმად მიიჩნევს, რომ ამ ინფორმაციის გამჟღავნება ღონისძების დასრულებიდან 5 წლის განმავლობაშიც იქნება საფრთხის შემცველი ღონისძიების მიზნის მიღწევის ან ქვეყნის ინტერესების დარღვევის კუთხით, მაშინ შეტყობინება მომავალშიც არ იქნება საჭირო. ევროკავშირის FRA-ის სტატისტიკის მიხედვით, 2013 წელს 1,944 ადამიანიდან ან დაწესებულებიდან, რომელთა მიმართაც შეწყდა მეთვალყურეობის ღონისძიებები, ინფორმირებული იყო 650 მათგანი. G10-ის გადაწვეტილებით აღნიშნული 1,944 პირიდან 1,079 ადამიანისათვის/დაწესებულებისთვის ინფორმაცია არსებული

243 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.14
244 Ibid.
245 G-10 Law Section 12

მდგომარეობით მიწოდებული არ იყო (თუმცა შესაძლოა მომავალში განხორციელებულიყო მათი ინფორმირება), ხოლო 260 პირის შემთხვევაში ერთსულოვნად იქნა მიღებული გადაწყვეტილება, რომ მათ ინფორმაცია მომავალშიც არ მიეწოდებოდათ.[246]

- სტრატეგიული მეთვალყურეობის შემთხვევაში შეტყობინების იგივე წესები ვრცელდება იმ პერსონალურ მონაცემებზე, რომელიც დამუშავდა ღონისძიების მიმდინარეობისას, მაგრამ ეს წესები არ ვრცელდება იმ მონაცემებზე, რომლებიც დაუყოვნებლივ წაიშალა შეგროვების შემდეგ. სრულად ქვეყნის ფარგლებს გარეთ განხორციელებული სტრატეგიული მეთვალყურეობის შემთხვევაში შეტყობინების ვალდებულებისაგან უსაფრთხოების სამსახურები სრულად არიან გათავისუფლებულნი.[247]

როგორც ზემოაღნიშნულიდან იკვეთება, გერმანიამ გაიზიარა სამივე მიდგომა: მონაცემთა სუბიექტის პირდაპირი წვდომა, DPA-ს მეშვეობით არაპირდაპირი წვდომა და უსაფრთხოების სამსახურების მიერ შეტყობინების სისტემა.

უსაფრთხოების სამსახურების წლიური ანგარიშები: მიუხედავად იმისა, რომ შიდა უსაფრთხოების სამსახურის BFV-ის წლიური ანგარიში არის მოცულობითი (335 გვერდი), ანგარიშის უმრავლესობა ეძღვნება იმ ორგანიზაციების/მოძრაობების დეტალურ აღწერას, რომელიც საფრთხეს უქმნის ეროვნულ უსაფრთხოებას. მხოლოდ რამდენიმე გვერდი ეძღვნება BfV-ს ზედამხედველობას და კანადის მაგალითისგან განსხვავებით, არ შეიცავს საჩივრების შესახებ სტატისტიკურ მონაცემებს. BND-ის წლიური ანგარიში არ არის ხელმისაწვდომი მის ვებ-გვერდზე.

246 EU FRA Surveillance by Intelligence Services (2015) p.64
247 EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.126

საჯაროდ ხელმისაწვდომი კანონები: ბელგიის უსაფრთხოების სამსახურები შექმნილია და მოქმედებს საჯაროდ ხელმისაწვდომი კანონების საფუძველზე.[248] მუდმივმოქმედი კომიტეტი I თავის ვებ-გვერდზე აქვეყნებს არა მხოლოდ კანონებს, არამედ მინისტრის ყველა რელევანტურ ბრძანებას, რომელიც განსაზღვრავს ინფორმაციის გასაიდუმლოებასა და საერთო მონაცემთა ბაზების შექმნას. აღნიშნული წარმოადგენს საუკეთესო პრაქტიკას.

ინფორმაციასა და საკუთარ პერსონალურ მონაცემებზე წვდომა: ბელგიაში, უსაფრთხოების სამსახურების მიერ შენახულ ინფორმაციაზე წვდომის პროცედურები, ასევე პერსონალური მონაცემების საკითხები რეგულირდება ადმინისტრაციის გამჭვირვალობის შესახებ კანონით.[249] კანონი საშუალებას იძლევა პირს ჰქონდეს პირდაპირ წვდომა საკუთარ პერსონალურ მონაცემებზე, თუმცა აღნიშნული წესი ექვემდებარება გარკვეულ შეზღუდვებს. უსაფრთხოების სამსახური არაა ვალდებული გაამჟღავნოს მონაცემები, თუ იგი მიიჩნევს, რომ კონკრეტულ შემთხვევაში საზოგადოებრივი წესრიგის და უსაფრთხოების, ეროვნული თავდაცვისა და მოსახლეობის უსაფრთხოების დაცვის ინტერესი აღემატება, გამჭვირვალობის დაცვის ინტერესს (გამჭვირვალობის კანონის მე-6 მუხლი). თუმცა პრაქტიკაში, ასეთი ფართო გამონაკლისების არსებობა თითქმის ყველა მოთხოვნაზე უარის თქმას იწვევს. უფრო მეტიც, კანადის მოდელისგან განსხვავებით, უსაფრთხოების სამსახური არ აქვეყნებს სტატისტიკას, თუ რამდენი განცხადება იქნა მიღებული ინფორმაციაზე დაშვების შესახებ.[250]

ინფორმაციაზე არაპირდაპირი წვდომა: როდესაც მონაცემთა სუბიექტის პირდაპირი წვდომა საკუთარ მონაცემებზე ეფექტიანად არ არის უზრუნველყოფილი, ბელგიის პირადი ცხოვრების დაცვის შესახებ კანონი ითვალისწინებს არაპირდაპირ წვდომას იმ პირად მონაცემებზე, რომლებიც შეგროვებულ იქნა ეროვნული უსაფრთხოების, სახელმწიფო უსაფრთხოებისა და ეროვნული თავდაცვის მიზნებისათვის. ასეთ შემთხვევებში მონაცემთა სუბიექტს უფლება აქვს მოთხოვნა წარადგინოს პირადი ცხოვრების დაცვის კომისიაში, რომელიც განიხილავს იყო თუ არა უსაფრთხოების სამსახურის მიერ პერსონალური ინფორმაციის დამუშავებასთან დაკავშირებული ღონისძიებები კანონმდებლობის შესაბამისი. თუ დადგინდა გარკვეული ხარვეზი, კონფიდენციალურობის კომისიას შეუძლია გასცეს რეკომენდაცია მონაცემების შეცვლასთან დაკავშირებით. განხილვის დასრულების შემდეგ, კომისია მონაცემთა სუბიექტს აღნიშნულის შესახებ აცნობებს, თუმცა სამსახურის მიერ დამუშავებულ მონაცემებს არ ასაჯაროებს.[251]

მონაცემზე არაპირდაპირი წვდომა შესაძლებელია მოპოვებულ იქნეს ასევე მუდმივმოქმედი კომიტეტის I-ის მეშვეობით, როდესაც მონაცემთა სუბიექტი წარადგენს მოთხოვნას კომიტეტში და სუბიექტს აქვს ამის ლეგიტიმური და პირადი ინტერესი.[252]

უსაფრთხოების სამსახურების მიერ შეტყობინება: 2011 წელს ბელგიის საკონსტიტუციო სასამართლომ დაადგინა, რომ უსაფრთხოების სამსახურებმა „აქტიურად უნდა მოახდინონ მეთვალყურეობის სუბიექტის ინფორმირება იმ მომენტიდან, როდესაც აღნიშნული შეტყობინების განხორციელება შესაძლებელია სპეციალური სამსახურების საქმიანობის მიზნებისთვის საფრთხის

248 Organic Law on Security and Intelligence Services (1998).
249 Loi relative à la publicité de l'administration, 11 April 1994
250 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.16
251 Belgium, Belgian Privacy Commission (Commission vie privée/ Privacycommissie), 'La protection des données à caractère personnel en Belgique', Brussels, Privacy Commission, p. 20
252 Organic Law on the intelligence and security services Art 43 (4).

შექმნის გარეშე“.[253] თუმცა, კანონმდებლობა ამ გადაწყვეტილებასთან შესაბამისობაში ჯერ კიდევ არ არის მოყვანილი.

სამსახურის წლიური ანგარიშები: ბელგიური უსაფრთხოების სამსახურის წლიური ანგარიშები არ არის ხელმისაწვდომი მათ ვებ-გვერდზე.

253 Judgement No. 145/2011, 22 September 2011, paras 88 to 92.

ბიბლიოგრაფია

Aidan Wills and Benjamin Buckland, *Access to Information by Intelligence and Security Service Oversight Bodies*, (DCAF/OSF, 2012), http://www.dcaf.ch/sites/default/files/publications/documents/Access_information_oversight_bodies_draft.02.12.pdf

Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2010), http://www.dcaf.ch/guidebook-understanding-intelligence-oversight

Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2456151

Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015): https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Canadian Security Intelligence Agency, Annual Report 2016: https://www.csis-scrs.gc.ca/pblctns/nnlrprt/2014-2016/index-en.php#Unique

Croatian Council for Civilian Oversight of Security and Intelligence Agencies, Fact Sheet, available from http://www.sabor.hr/0060

Committee I, Activity Report 2014-2015, http://www.comiteri.be/images/pdf/Jaarverslagen/Activity_Report_2014_15.pdf

DCAF, Parliamentary Brief: Safeguards in Electronic Surveillance, available from: https://dcaf.ch/resources?type=publications

European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks,* (Luxembourg, 2015), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU*- - Volume II: field perspectives and legal update (Luxembourg, 2017), http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and/publications

German Federal Ministry of the Interior, Report on the Protection of the Constitution (2016),: https://www.verfassungsschutz.de/en/about-the-bfv

German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),: http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

Global Principles on National Security and the Right to Information (Tshwane Principles), available from: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016): http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005), p., available from: http://www.dcaf.ch/making-intelligence-accountable

Hans Born and Aidan Wills (ed.) *Overseeing Intelligence Services: A Toolkit* (DCAF: 2012) http://www.dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf

Hans de With and Erhard Kathmann, 'Annex A- Country Case Studies - Germany', in Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011)

Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

Lauren Hutton, 'Overseeing Information Collection', Tool 5, in Born and Wills, *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012)

The Paris Principles, http://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx

Thorsten Wetzling, 'Germany's Intelligence Reform: More surveillance, modest restraints and inefficient controls' SNV Policy Brief (2017), available from: https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency/publikationen

Thorsten Wetzling, SNV Policy Brief: 'The Key to Intelligence Reform in Germany- Strengthening the G-10 Commission's role to authorize strategic surveillance' 2016, https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency/publikationen

UNODC, 'Current practices in electronic surveillance in the investigation of serious and organized crime' (New York, 2009) https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

UN General Assembly Resolution 45/95 (1990), http://www.refworld.org/pdfid/3ddcafaac.pdf

UN Human Rights Council, *Compilation Of Good Practices On Legal And Institutional Frameworks And Measures That Ensure Respect For Human Rights By Intelligence Agencies While Countering Terrorism, Including On Their Oversight* (*UN Compilation of Good Practices*), A/HRC/14/46 para , http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf

Venice Commission, *Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session* (2007), http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx

Venice Commission , *Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session,* CDL-AD (2015) 011: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e,

Wauter Van Laetham, The Belgian Civil Intelligence Service: Roles, Powers, Organisation and Supervision , EJIS, Volume 2, (2008) http://www.comiteri.be/index.php/en/publications/specialized-literature

ეროვნული კანონმდებლობა

ბელგია

Act on Security and Intelligence Services, (Loi Organique des Services de Renseignement et de Securite) (18 decembre 1988), available from : http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032

Loi relative à la publicité de l'administration, 11 April 1994, http://www.mumm.ac.be/Downloads/bmdc_LOI-WET_11_04_1994.pdf

კანადა

Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23) available from: http://laws-lois.justice.gc.ca/eng/acts/c-23/index.html

National Security and Intelligence Committee of Parliamentarians Act (S.C. 2017, c. 15),: http://laws.justice.gc.ca/eng/AnnualStatutes/2017_15/page-1.html

Security of Information Act (R.S.C., 1985, c. O-5), available from http://laws-lois.justice.gc.ca/eng/acts/O-5/

Access to Information Act http://laws-lois.justice.gc.ca/eng/acts/A-1/FullText.html

Privacy Act http://laws-lois.justice.gc.ca/PDF/P-21.pdf

ხორვატია

Act on the Security Intelligence System of the Republic of Croatia https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

Data Secrecy Act: **http://europam.eu/data/mechanisms/FOI/FOI%20Laws/Croatia/Croatia_Data%20Secrecy%20Act_2007.pdf**

Decree on the Right of Security and Intelligence Agency Officials to Bear and Use Firearms, available from: https://www.soa.hr/UserFiles/File/Decree_bear_and_use_firearms.pdf

Act on the Right to Access to Information: , http://www.revizija.hr/en/access-to-information/law-on-the-right-to-access-information

გერმანია

Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution https://www.gesetze-im-internet.de/bverfschg/

Act on the Federal Intelligence Service, https://www.gesetze-im-internet.de/bndg/

Code of Criminal Procedure, as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410) https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

Act on the Parliamentary Control of Federal Intelligence Services Art.4.1, http://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html

G-10 Act, https://www.gesetze-im-internet.de/g10_2001/index.html

Freedom of Information Act, https://www.gesetze-im-internet.de/englisch_ifg/englisch_ifg.html#p0021

ევროპული სასამართლოს საქმეები

Klass and Others v. Germany, No.5029/71, 6 September 1978.

Leander v. Sweden, Application No.9248/81, 26 March 1987.

Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016,

Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015,*

United Communist Party of Turkey and Others v. Turkey, 19392/92, 30 January 1998

Zana v. Turkey, 18954/91, 25 November 1997