2. ՈՒՂԵՆԻՇԱՅԻՆ ԳՈՐԾԵՐԻ ՀԱՄԱՌՈՏԱԳՐԵՐ

2.1. Զանգվածային հսկողություն

«Big Brother Watch-ը և այլք» ընդդեմ Միացյալ Թագավորության (Big Brother Watch and others v. the United Kingdom [GC], application nos *58170/13, 62322/14* and *24960/15*, judgment of 25 May 2021)

Հաղորդակցությունների զանգվածային գաղտնալսման համապատասխանությունը կոնվենցիոն պահանջներին. ***խախտում***

Վերաբերելի նախադեպային իրավունք

1) **Weber and Saravia v. Germany,** *application no. 54934/00, decision of 29 June 2006*
2) **Liberty and Others v. the United Kingdom,** *application no. 58243/00, judgment of 1 July 2008*
3) **Roman Zakharov v. Russia [GC],** *application no. 47143/06, judgment of 4 December 2015*

HUDOC համակարգում որոնման համար բանալի բառեր

Art 8 • Private life • Convention compliance of secret surveillance regime including bulk interception of communications and intelligence sharing • Need to develop case-law in light of important differences between targeted interception and bulk interception • Adapted test for examining bulk interception regimes through global

assessment • Focus on "end-to-end safeguards" to take into account the increasing degree of intrusion with privacy rights as the bulk interception process moves through different stages • Fundamental deficiencies present in bulk interception regime, through absence of independent authorisation, failure to include categories of selectors in the application for a warrant, and failure to subject selectors linked to an individual to prior internal authorisation • Sufficient foreseeability and safeguards in regime for receipt of intelligence from foreign intelligence services • Regime for acquisition of communications data from communications service providers not "in accordance with law"

Art 10 • Freedom of expression • Insufficient protection of confidential journalist material under electronic surveillance schemes

Փաստական հանգամանքները

Դիմումատուները մի շարք կազմակերպություններ և անհատներ են, որոնք բողոք են ներկայացրել Միացյալ Թագավորության կառավարության կողմից գործարկվող էլեկտրոնային հսկողության համակարգի ծավալի և շրջանակների վերաբերյալ: Դիմումատուների կարծիքով իրենց գործունեության բնույթը ենթադրում էր, որ իրենց էլեկտրոնային հաղորդակցությունը և/կամ հաղորդակցության տվյալները գաղտնալսվել են Միացյալ Թագավորության հատուկ ծառայությունների կողմից, կամ դրանց բովանդակությունը ձեռք է բերվել հեռահաղորդակցման ծառայություններ մատուցողներից կամ օտարերկրյա հատուկ ծառայություններից:

2018 թվականի սեպտեմբերի 13-ի վճռով Եվրոպական դատարանը գտավ, որ ներպետական օրենսդրությամբ նախատեսված կառուցակարգերով տեխնիկական հաղորդակցության ուղիներից տեղեկատվության զանգվածային դուրսբերմամբ խախտվել են Եվրոպական կոնվենցիայի 8-րդ և 10-րդ հոդվածները: Սակայն Եվրոպական դատարանը համարեց, որ 8-րդ հոդվածի խախտում առկա չէ հետախուզական տեղեկատվության տարածման ռեժիմի

համատեքստում: Դիմումատուների պահանջով գործը հանձնվել է Մեծ պալատի քննությանը:

Մեծ պալատի եզրահանգումները

1. Տեխնիկական հաղորդակցությանուղիներից տեղեկատվության զանգվածային դուրսբերումը *Կոնվենցիայի 8-րդ հոդված*

Միջամտություն: Կոնվենցիայի 8-րդ հոդվածը տարածվում է տեխնիկական հաղորդակցության ուղիներից տեղեկատվության զանգվածային դուրսբերման բոլոր փուլերի վրա, որոնք ներառում են՝ 1. հաղորդակցության և հարակից տվյալների գաղտնալսումը և նախնական հավաքումը, 2. հատուկ զտիչ մեխանիզմների կիրառումը գաղտնալսված հաղորդակցության հարակից տվյալների նկատմամբ, 3. ընտրված հեռահաղորդակցության և հարակից տվյալների հետազոտությունը, 4. տվյալների հետագա պահպանումը և «վերջնական արտադրանքի» օգտագործումը, այդ թվում՝ փոխանցումը երրորդ կողմերին:

Նախադեպային իրավունքի զարգացման անհրաժեշտությունը: Տեխնոլոգիաների զարգացման համատեքստում անհրաժեշտ էր զարգացնել նախադեպային իրավունքը, քանի որ նախկինում Դատարանը հստակ տարբերակում չէր մտցրել **թիրախավորված գաղտնալսումների** և **զանգվածային գաղտնալսումների** միջև, որոնք էապես տարբերվում են մի շարք ասպեկտներով (օրինակ՝ ի տարբերություն թիրախավորված գաղտնալսման, զանգվածային գաղտնալսումը հիմնականում ուղղված է միջազգային հաղորդակցություններին և առավելապես օգտագործվում է օտարերկրյա հաղորդակցություններ տվյալների հավաքմանը և հայտնի և անհայտ դերակատարներից սպառնացող վտանգի բացահայտմանը):

Զանգվածային գաղտնալսումների ռեժիմի նկատմամբ կիրառելի թեստը: Գնահատելու համար գործարկվող գաղտնալսումների համակարգի «համաձայն օրենքի» և «անհրաժեշտության» չափանիշներին համապատասխանությունը՝ Դատարանը պետք է ուսումնասիրի՝ որքանով է ազգային օրենսդրությունը հստակորեն սահմանել հետևյալ հանգամանքը.

- *Զանգվածային գաղտնալսումների թույլատրման հիմքերը:*

Որքան լայն են նախատեսված հիմքերը, այնքան մեծ է իրավունքների խախտման ռիսկը: Սակայն ավելի նեղ և հստակ սահմանված հիմքերն արդյունավետ երաշխիք կլինեն խախտումների դեմ այն դեպքում, երբ այլ բավարար երաշխիքներ ևս լինեն նախատեսված, որոնք կապահովեն, որ զանգվածային գաղտնալսումները թույլատրվեն միայն թույլատրելի հիմքերի առկայության դեպքում, և որ դա անհրաժեշտ էր և համաչափ նպատակին հասնելու տեսանկյունից: Հետևաբար, Դատարանի կարծիքով, ռեժիմը, որը թույլատրում էր զանգվածային գաղտնալսումները համեմատաբար լայն հիմքերով, դեռևս կարող է բավարարել 8-րդ հոդվածի պահանջները, եթե, ամբողջական վերցրած, համակարգն ունեցել է խախտումների դեմ բավարար այլ երաշխիքներ ևս.

- *Հանգամանքները, որոնցում անձի հաղորդակցությունը կարող է գաղտնալսվել:*
- *Գաղտնալսման թույլտվություն տալու ընթացակարգը:*

Զանգվածային գաղտնալսման թույլտվությունը պետք է տա գործադիր իշխանությունից անկախ մի մարմին (ընդ որում՝ պարտադիր չէ, որ այն լինի դատական): Այս մարմինը պետք է տեղեկացվի գաղտնալսման նպատակի, ինչպես նաև հաղորդակցության «կրողների» մասին, ինչը հնարավորություն կտա գնահատելու ինչպես գաղտնալսման գործողության անհրաժեշտությունը

և համաչափությունը, այնպես էլ հաղորդակցության «կրողների» ընտրությունը.

- *Գաղտնալսված նյութի ընտրության, հետազոտման և օգտագործման ընթացակարգը*:
- *Գաղտնալսված նյութն այլ կողմերին փոխանցելու ընթացակարգը:*

Ազգային օրենսդրությունը պետք է հստակ սահմանի այն հանգամանքները, որոնց պայմաններում կարող է տեղի ունենալ գաղտնալսված նյութի փոխանցում այլ կողմերի, տեղեկատվությունը փոխանցող պետությունը պետք է երաշխավորի, որ ստացող պետությունն ունի անհրաժեշտ կանխարգելիչ երաշխիքներ խախտումների և անհամաչափ միջամտության դեմ, առավել խիստ երաշխիքներ են անհրաժեշտ, երբ փոխանցվող նյութը պահանջում է հատուկ գաղտնիություն (օրինակ՝ լրագրողական գաղտնի նյութը), օտարերկրյա գաղտնի ծառայություններին փոխանցող նյութը պետք է լինի անկախ հսկողության ներքո.

- *Գաղտնալսման տևողության սահմանափակումները, գաղտնալսված նյութի պահպանությունը, այն հանգամանքները, որոնց պարագայում այսպիսի նյութը պետք է ջնջել և ոչնչացնել:*
- *Ex post facto վերանայման արդյունավետ համակարգի առկայությունը:*

Վերոնշյալ պայմանների լույսի ներքո դիտարկելով քննարկման առարկա գանգատներում բարձրացված հարցերը՝ Դատարանը գտավ, որ ամբողջությամբ վերցրած Միացյալ Թագավորության կառավարության կողմից գործարկվող գաղտնալսման ռեժիմը, չնայած նախատեսված երաշխիքներին, չի ունեցել կամայականությունների և խախտման ռիսկերի դեմ բավարար

երաշխիքներ: Մասնավորապես, արձանագրվեցին հետևյալ հիմնարար բացթողումները.

1. անկախ թույլտվության տրամադրման մեխանիզմի բացակայությունը.
2. թույլտվության տրամադրման դիմումի մեջ որոնման պայմանները («զտիչների») չներառելը.
3. կոնկրետ անձի հետ կապված որոնման պայմանների (այն է՝ հատուկ նույնականացման այնպիսի գործիք, ինչպիսին է էլ. փոստի հասցեն) ներքին թույլտվության բացակայությունը:

Այսպիսով՝ **Դատարանը գտավ, որ չնայած նախատեսված երաշխիքներին՝ ազգային օրենսդրությունը չի բավարարում «օրենքի որակին» ներկայացվող պայմանները, և այսպիսով քաղաքացիների անձնական կյանքի իրավունքին միջամտությունը չի կարող համարվել «անհրաժեշտ ժողովրդավարական հասարակությունում»:**

2. Օտարերկրյա կառավարություններից և/կամ հատուկ ծառայություններից գաղտնալսված նյութի ստացումը

Դատարանը եզրահանգեց, որ Միացյալ Թագավորության ազգային օրենքը հստակ և մանրամասն սահմանում է այն դեպքերը, երբ հատուկ ծառայություններն իրավասու են օտարերկրյա հատուկ ծառայություններից հայցելու գաղտնալսված տեղեկատվություն, և թե ինչպես պետք է ստացված տեղեկատվությունը հետազոտվի, օգտագործվի և պահվի: Դատարանին բավարարել են նաև գաղտնալսված տեղեկատվության հայցման և ստացման նկատմամբ պատշաճ հսկողության առկայությունը և կատարված գործողությունների նկատմամբ *ex post facto* արդյունավետ վերահսկողությունը: Հետևաբար Դատարանը գտավ, որ օտարերկրյա գաղտնի ծառայություններից գաղտնալսված տեղեկատվության ստացման մասով գործարկվող ռեժիմը չի խախտում Կոնվենցիայի 8-րդ հոդվածը:

3. Տեղեկատվության ստացումը հեռահաղորդակցության օպերատորներից

Այս առումով Դատարանը վերահաստատել է Պալատի այն եզրահանգումները, ըստ որոնց՝ առկա է Կոնվենցիայի 8-րդ հոդվածի խախտում առ այն, որ գործարկվող ռեժիմը չի բավարարել «համաձայն օրենքի» չափանիշը:

Կոնվենցիայի 10-րդ հոդված

Դատարանը վերահաստատեց, որ լրագրողական աղբյուրի պաշտպանությունը մամուլի ազատության անկյունաքարերից մեկն է: Այս պաշտպանությունը խարխլելը կարող է վնասակար ազդեցություն ունենալ մամուլի՝ որպես հանրային հսկողական գործառույթ իրականացնողի դերի, ինչպես նաև վստահելի և ճշգրիտ տեղեկատվություն տրամադրելու կարողության վրա:

Համաձայն զանգվածային գաղտնալսման համակարգի՝ լրագրողական գաղտնի նյութը կարող է ձեռք բերվել գաղտնի ծառայությունների կողմից՝ լրագրողի կամ լրատվական կազմակերպության հետ կապված զտիչների կամ որոնման պայմանների կիրառման արդյունքում: Այսպիսի միջամտությունը համարժեք է լրագրողի տան կամ աշխատավայրի խուզարկությանը: Այսպիսով՝ մինչև գաղտնի ծառայությունների կողմից լրագրողների հետ կապված զտիչների կամ որոնման պայմանների սահմանումը, որոնք ենթադրաբար կարող են հանգեցնել գաղտնի լրագրողական նյութերի զննությանը, այսպիսի զտիչների կամ որոնման պայմանների սահմանումը պետք է նախապես թույլատրվի դատավորի կամ անկախ և անկողմնակալ մարմնի կողմից, որը կկարողանա գնահատել այդ միջամտության «հիմնավորվածությունը հանրային շահի պահանջի տեսանկյունից»: Այսպիսով՝ կիրառվող ռեժիմը, որը միջամտում է լրագրողների արտահայտվելու ազատությանը, չի բավարարել վերոնշյալ պահանջը:

Այսպիսով՝ Դատարանը.

1. ***միաձայն գտավ, որ խախտվել են Կոնվենցիայի 8-րդ և 10-րդ հոդվածները,***
2. ***փաստերկու կողմ և հինգ դեմ ձայների հարաբերակցությամբ գտավ, որ Կոնվենցիայի 8-րդ և 10-րդ հոդվածների խախտում տեղի չի ունեցել օտարերկրյա հետախուզական ծառայություններից հետախուզական տեղեկատվության ստացման մասով:***