ՊԱՇՏԱՆ ԿԱՌԱՎԱՐՄԱՆ ՈՒՂԵՑՈՒՅՑԵՐ

թիվ 06

Թափանցիկության և գաղտնիության հավասարակշռումը պաշտպանության ոլորտում. միջազգային առաջատար փորձից ստացված դասեր

Centre for Integrity in the Defence Sector

Norwegian Ministry of Defence

ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՈԼՈՐՏՈՒՄ ԲԱՐԵՎԱՐՔՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Պաշտպանության ոլորտում բարեվարքության կենտրոնը (CIDS) խթանում է բարեվարքությունը, հակակոռուպցիոն միջոցառումների իրականացումը և պատշաճ կառավարումը պաշտպանության ոլորտում: Համագործակցելով Նորվեգիայի և միջազգային այլ գործընկերների հետ՝ կենտրոնը ձգտում է զարգացնել կարողությունները, բարձրացնել իրազեկվածությունը և տրամադրել գործնական միջոցներ՝ կոռուպցիոն ռիսկերը նվազեցնելու համար: CIDS-ը ստեղծվել է 2012 թվականին Նորվեգիայի պաշտպանության նախարարության կողմից:

ՀԵՂԻՆԱԿԻ ՄԱՍԻՆ

Ֆրանցիսկո Կարդոնա կրտսեր միջազգային փորձագետ է CIDS-ում: Կարդոնան ճանաչված մասնագետ է քաղաքացիական ծառայության և պետական կառավարման բարեփոխումների, վարչական իրավունքի և արդարադատության, հակակոռուպցիոն քաղաքականության և ինստիտուցիոնալ զարգացման ձևավորման և գնահատման ոլորտում: Իր մասնագիտական կարիերայի ընթացքում նա աշխատել է ինչպես իր հայրենիքում՝ Իսպանիայում, որտեղ գործունեություն է ծավալել քաղաքացիական ծառայության ոլորտում, այնպես էլ միջազգային կազմակերպություններում, մասնավորապես՝ Տնտեսական համագործակցության և զարգացման կազմակերպության (ՏՀԶԿ) ՍԻԳՄԱ ծրագրում, որտեղ 15 տարի աշխատել է որպես պետական կառավարման ոլորտի քաղաքականության ավագ վերլուծաբան: ՍԻԳՄԱ-ում նա խորհրդատվություն է տրամադրել Արևելյան Եվրոպայի, Աֆրիկայի, Լատինական Ամերիկայի և Կարիբյան տարածաշրջանի անցումային տնտեսությամբ և զարգացող շուրջ 25 երկրների: Նա իրավաբանական կրթություն ունի (ավարտել է Վալենսիայի համալսարանը 1976 թ. -ին) և ստացել է մագիստրոսի մի քանի կոչում պետական կառավարման ոլորտում:

ԱՌԱՋԱԲԱՆ

CIDS-ի կողմից հրատարակվող «Պատշաճ կառավարման ուղեցույցներ»-ի առաջնային նպատակն է՝ լայն լսարանին ներկայացնել պատշաճ կառավարման ոլորտի հիմնական խնդիրները: Ուղեցույցներում հարցերը ներկայացված են հակիրճ՝ առանց չափազանց պարզեցնելու:

Վեցերորդ «Պատշաճ կառավարման ուղեցույց»-ում հեղինակի նպատակն է՝ կատարել պաշտպանության ոլորտում գաղտնիության հասկացության քննադատական վերլուծություն: Այդ նպատակով հեղինակը կատարում է հետևյալ հարցադրումը. «(...) ինչպե՞ս պետք է (...) «բաց կառավարություն» ունեցող ժողովրդավարական հասարակություններում ապահովել հավասարակշռությունը տեղեկատվության ազատ մատչելիության և այդ նույն տեղեկատվության որոշակի սահմանափակման միջև»: Բացի այդ, ե՞րբ է անհրաժեշտ սահմանափակել տեղեկատվությունը՝ ելնելով ազգային անվտանգության շահերից: Դիտարկվում է քաղաքացիների՝ պետական պաշտպանության իրավունքը:

Ուղեցույցը մշակել է CIDS-ի ավագ միջազգային փորձագետ Ֆրանցիսկո Կարդոնան: Ցանկանում եմ շնորհակալություն հայտնել նրան՝ պատշաճ կառավարման ոլորտում այսպիսի կարևոր թեմայի անդրադառնալու համար: Վերջին տարիներին այս թեման արդիական է եղել հասարակական քննարկումների ընթացքում և, հավանաբար, կշարունակի այդպիսին լինել նաև գալիք տարիներին:

Ցանկանում եմ իմ շնորհակալության խոսքն ուղղել նաև կենտրոնի խմբագիր Բորդ Բրեդրուպ Կնուդսենին և մեր հրատակությունների համակարգող Ասե Մարի Ֆոսումին՝ այս ուղեցույցի պատրաստման մեջ ներդրված իրենց ջանքերի համար:

Հուսով ենք՝ այս ուղեցույցը կօգտագործվի լայն լսարանի կողմից ինչպես պետական հատվածում, ներառյալ պաշտպանության ոլորտը, այնպես էլ դրանից դուրս: Տեղեկատվության հասանելիությունն ու գաղտնիությունը հավասարակշռելը չափազանց կարևոր է ժողովրդավարական հասարակության արդյունավետության համար:

CIDS-ը ողջունում է բոլոր արձագանքները այս ուղեցույցի վերաբերյալ:

Օսլո, 24 ապրիլի 2018 թ.

Պեր Քրիստենսեն
Տնօրեն

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

Ներածություն

Պատշաճ կառավարման սույն ուղեցույցում համառոտ ներկայացված է ԵՄ և ՏՀՋԿ երկրներում կիրառվող միջազգային առաջատար փորձը՝ ուղղված պաշտպանության և ազգային անվտանգության ոլորտում հանրային տեղեկատվության գաղտնիությունը պահպանելուն՝ միևնույն ժամանակ ապահովելով հանրության համար պետական հաստատությունների կողմից պահվող տեղեկատվության հասանելիության ընդհանուր իրավունքը: Սույն ուղեցույցի նպատակն է ներկայացնել այն քաղաքականությունը, որը նպաստում է բաց կառավարմանը, տեղեկատվության մատչելիությանը և կառավարության գործունեության վերաբերյալ քաղաքացիների կողմից տեղեկացված որոշումներ կայացնելու կարողության զարգացմանը: Միևնույն ժամանակ հստակեցվում են պետական գաղտնիքների պատշաճ պաշտպանության հետ կապված հարցեր՝ ազգային անվտանգության, պաշտպանության և հետախուզության, ինչպես նաև կոռուպցիայի և հանցավորության դեմ պայքարի համատեքստում:

Թափանցիկությունն ու հրապարակայնությունը գերազանց կանխարգելիչ միջոցներ են՝ ուղղված կոռուպցիայի, անբարեխիղճ և անարդյունավետ կառավարման դեմ: Ժողովրդավարությունը չի կարող պատշաճ կերպով գործել գաղտնիության պայմաններում, ինչը պայմանավորված է նրանով, որ գաղտնիության գերակայման պարագայում քաղաքական ռեժիմը պարզապես դադարում է ժողովրդավարական լինելուց, քանի որ բացառվում է քաղաքացիների մասնակցությունը քաղաքական գործընթացներին: Դա նշանակում է, որ լիազորությունների իրականացումը կարող է դուրս գալ վերահսկողությունից, իսկ ժողովրդավարական հաշվետվողականությունը՝ տեղի չունենալ: Այնուամենայնիվ, տեղեկատվության հանրային մատչելիությունը կարող է նաև սահմանափակվել՝ արդյունավետ կառավարվող երկրում ժողովրդավարության պատշաճ իրացումն ապահովելու համար: Հետևաբար, ինչպես հանրային տեղեկատվության բացահայտումը, այնպես էլ այդպիսի բացահայտման որոշակի սահմանափակումները պետք է հավասարապես ծառայեն հանրային շահերին:

Հայեցակարգային շրջանակ. ազգային անվտանգությունը՝ որպես գաղտնիության հիմնավորում

Հիմնական հայեցակարգային ենթադրությունն այն է, որ բաց կառավարումը և տեղեկատվության ազատ հասանելիությունը՝ մի կողմից, և այդ հասանելիության համար որոշակի սահմանափակումների հաստատումը՝ մյուս կողմից, բխում են հանրային շահերից: Միջազգայնորեն ընդունված ընդհանուր սկզբունքն այն է, որ կառավարությունը պետք է խթանի «տեղեկացված լինելու իրավունքը»՝ միևնույն ժամանակ սահմանելով ողջամիտ սահմանափակումներ՝ որոշակի հանրային տեղեկատվության գաղտնիությունը պաշտպանելու համար: Վերջինս անհրաժեշտ է՝ որոշ տիրույթներում, մասնավորապես՝ ազգային անվտանգության և պաշտպանության ոլորտում պետության գործունեության արդյունավետությունն ապահովելու համար:

Նման գաղտնիության հետ կապված հիմնական խնդիրը կայանում է նրանում, որ անհրաժեշտ է պարզել, թե երբ և որքանով են արդարացված տեղեկատվության հանրային մատչելիության սահմանափակումները: Առողջ ժողովրդավարական պետությունների հավակնոտ նպատակն է՝ հանրության համար ապահովել տեղեկատվության պատշաճ հասանելիություն՝ միևնույն ժամանակ սահմանելով այդպիսի հասանելիության որոշակի օրինական սահմաններ: Այդ երկու մոտեցումների միջև հավասարակշռություն հաստատելը մեծապես կախված է երկրի պատմությունից, սոցիալական արժեքներից և մշակութային այլ գործոններից: Այդ պատճառով դժվար է պարզել, թե արդյոք գոյություն ունեն միջազգային ստանդարտներ, որոնք կօգնեն հասնել ճիշտ հավասարակշռության (Թրանսփարենսի ինթերնեշնլ ՄԹ, 2014թ.): Գործնականում ճշգրիտ միջազգային ստանդարտներ գոյություն չունեն, թեև վերջին տարիներին եղել են բազմաթիվ տեսական քննարկումներ և որոշ ընդհանուր սկզբունքներ հաստատելու փորձեր[1]:

Հսկողության բացակայության պարագայում գաղտնիության պահպանման պրակտիկան հեշտությամբ կընդարձակվի և կծավալվի: Ազգային անվտանգության, պաշտպանության, քրեական հետաքննության, հետախուզական տվյալների հավաքագրման կամ ահաբեկչության դեմ պայքարի հարցերով զբաղվող որոշ պետական ծառայություններ

1 **Տե՛ս Ցվանեի սկզբունքները** (2013)՝ https://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points

հակված են գաղտնիություն կիրառել իրենց յուրաքանչյուր գործողության նկատմամբ, նույնիսկ եթե արդյունքում քաղաքացիները զրկվում են կառավարության գործունեության մասին տեղեկացված լինելու իրավունքից: «Գաղտնիության մեխանիզմի» պահպանման մեծ ծախսերից զատ, գաղտնիության էական և համատարած կիրառումը հակված է խարխլել հասարակության վստահությունը պետական ինստիտուտների նկատմամբ և, ի վերջո, թուլացնել ժողովրդավարական լեգիտիմությունը: Գաղտնիության չափից բարձր մակարդակը սովորաբար նաև ավելի շատ սխալների և խախտումների է հանգեցնում, քան թափանցիկությունը և հանրային վերահսկողությունը, քանի որ թափանցիկության բացակայությունը դժվարացնում է հանրային վերահսկողությունը և սխալ գործելակերպերի շտկումը: Արդյունքում, երկարաժամկետ կտրվածքով բարձր աստիճանի գաղտնիությունը կարող է ավելի մեծ վնաս հասցնել ազգային անվտանգությանը, քան բաց տեղեկատվության առկայությունը:

Ինչպես պնդում են որոշ պետական պաշտոնյաներ, օրինակ՝ Միացյալ Նահանգներում, չափից շատ գաղտնիությունը «դարձել է անհիմն խոչընդոտ տեղեկատվության փոխանակման համար՝ ինչպես կառավարության ներսում, այնպես էլ դրանից դուրս, ինչը վնասում է պետական քաղաքականությանը» (Aftergood, 2008թ . , էջ 400): Դա վկայում է չափից ավելի գաղտնիության խնդրի մասին, այսինքն՝ տեղեկատվությունը տիրապետող ծառայությունները հակված են գաղտնի դասակարգել տեղեկատվությունը՝ գերազանցելով այդպիսի դասակարգման փաստացի անհրաժեշտությունը:

Դասակարգման ցանկացած համակարգի նպատակն է կանխել տեղեկատվության բացահայտումը, որը կարող է վտանգել ազգային անվտանգությունը, սակայն «ազգային անվտանգություն», «անվտանգության սպառնալիքներ» և այլ համանման հասկացությունների անորոշությունը ստեղծում է ավելորդ գաղտնիության կիրառման հնարավորություն: Փաստացի և սուբյեկտիվ տեղեկատվությունը տարբերակելու բարդությունը դժվարացնում է տեղեկատվությունը որպես գաղտնի դասակարգելու չափանիշների հստակ սահմանումը:

Տեղեկատվության պատշաճ դասակարգումը՝ գաղտնիության տեսանկյունից, ինքնին շատ բարդ է, բայց տեսականորեն կարող ենք ընդունել, որ գաղտնիությունը համարվում է «ողջամիտ», երբ այն նպատակահարմար է և հնարավորինս քիչ է հեռանում բաց կառավարման, թափանցիկության և տեղեկատվության ազատ հասանելիության ժողովրդավարական արժեքներից: Այլ կերպ ասած՝ կարող ենք համաձայնել, որ թափանցիկության սահմանափակումը ողջամիտ է, երբ այն. ա) բացառություն է, բ) ուղղված է ազգային անվտանգության կարևոր շահերի պաշտպանությանը: Այս եզրակացությամբ ընդունվում է պաշտպանության և ազգային անվտանգության ոլորտում այնպիսի տեղեկատվության առկայությունը, որի քողարկումն էական չէ ազգային անվտանգության համար, և, հետևաբար, այն կարող է անվտանգ բացահայտվել՝ ամբողջությամբ կամ մասամբ:

Որոշ ժողովրդավարական երկրներում դեռևս գերակշռում է այն ավանդական մոտեցումը, ըստ որի թափանցիկությունը պարզապես ներկայացնում է քաղաքացու պահանջը, իսկ գաղտնիությունն ազգային անվտանգության հարց է՝ կապված հանրային շահերի պաշտպանության հետ: Օրինակ, Ֆրանսիայի պետական խորհրդի փոխնախագահ պարոն Ժան Մարկ Սովեն 2011 թվականի հուլիսի 5-ին Ֆրանսիայի խորհրդարանի ստորին

պալատին՝ Ազգային ժողովին, ուղղված իր ելույթում ասել է. «*Դա է գաղտնիություն պահանջող օրինական պետական շահերի և քաղաքացիների կողմից պահանջվող թափանցիկության միջև բաժանարար գիծ հաստատելու ճանապարհը*» (Sauvé, 2011թ., էջ 6): Այս հայտարարությունը հիմնված է այն ենթադրության վրա, որ գաղտնիության պահպանումն ուղղված է հանրային շահերի պաշտպանությանը, մինչդեռ թափանցիկությունը չի բխում հանրային շահերից, այլ միայն քաղաքացիների և լրագրողների հետաքրքրասիրությունից առաջացող պահանջ է: Սա տարակուսելի ենթադրություն է: Փորձը ցույց է տալիս, որ թափանցիկության խթանումը հանրային շահերը պաշտպանելու լավագույն միջոցներից է, քանի որ այն նպաստում է պետական մարմինների հաշվետվողականությանը քաղաքացիների և վերահսկման այլ ժողովրդավարական մեխանիզմների առջև: Ուստի, թափանցիկությունը, այլ ոչ թե գաղտնիությունը, կարող է դիտվել որպես «պետության և հասարակության միջև բնականոն կերպով առաջացող բացը» *կամրջելու* միջոց (Fenster, 2010թ., էջ 619):

Առկա է միջազգային լայն կոնսենսուս այն մասին, որ պետական մարմինների քաղաքականության և գործողությունների թափանցիկությունը պետք է լինի ընդհանուր կանոն, իսկ գաղտնիությունը՝ բացառություն: Ավելին, նման բացառությունները պետք է արդարացված լինեն. դրանք կարող են հիմնավորվել միայն օրինական լինելու դեպքում, իսկ օրինական են միայն այն դեպքում, եթե հնարավոր է ապացուցել, որ դրանք գոյություն ունեն՝ հանուն ազգային անվտանգության իրական շահերի պաշտպանության:

Օրինական և ոչ օրինական գաղտնիությունը տարբերակելու անհրաժեշտությունը պահանջում է որոշակի վերահսկողություն իշխանությունների կողմից, որոնք պետք է լինեն գաղտնիություն կիրառող մարմնից անկախ: Նման անկախ հսկողության մեխանիզմները կարող են իրականացվել դատարանների կամ ավելի մասնագիտացված պետական մարմինների կողմից, և նրանց դերն է՝ պարզել, թե արդյոք ազգային անվտանգության շահերը, որոնք նշվում են որպես տեղեկատվությունը գաղտնի դասակարգելու հիմնավորում, իրական են և տվյալ իրավիճակի համար բավականաչափ կարևոր: Առանց արտաքին հսկողության մեխանիզմների՝ տեղեկատվության գաղտնիության վերաբերյալ որոշումները դառնում են չափազանց հայեցողական և, ամենայն հավանականությամբ, կամայական: Սակայն, ինչպես կտեսնենք ստորև, պատմականորեն դատարաններն ունեցել են, և առ այսօր ունեն, այնպիսի դերակատարում, որը չափազանց նպաստավոր է անվտանգության ծառայությունների կամ հետախուզական մարմինների կողմից տեղեկատվության չբացահայտման համար:

Տեսականորեն լիարժեք թափանցիկությունն անցանկալի է և, թերևս, անհնար, ինչպես նշվեց ավելի վաղ: Ավելին, պետությունը մշտապես ունենալու է գործունեության որոշակի ոլորտներ, որոնք գաղտնի են կամ բացահայտման ոչ ենթակա: Ինչպես նշում է Ֆենսթերը (2010թ., էջ 623), գաղտնիության և թափանցիկության միջև հաճախ կա տիրույթ, ինչը նշանակում է, որ պարտադիր չէ, որ գաղտնիությունը միանշանակորեն հակադրվի թափանցիկությանը: Գործնականում գաղտնիությունն ու թափանցիկությունը միանգամայն հակադիր իրողություններ չեն, քանի որ և՛ գաղտնիությունը, և՛ թափանցիկությունը պահանջում են առանձին ինստիտուցիոնալ հիմքեր, որոնք կառուցվածքային առումով տարբեր են (Riese, 2014թ., էջ 14):

Առավել թափանցիկությունը միշտ չէ, որ ենթադրում է նվազ գաղտնիություն, սակայն որակյալ թափանցիկությունը կնպաստի գաղտնիության պահպանմանը: Առավել թափանցիկություն նշանակում է, որ պաշտպանվում են գաղտնիության միայն իրական պահանջները: Թափանցիկության քաղաքականության ինստիտուցիոնալացումը երկրների մեծ մասում համեմատաբար նոր է, մինչդեռ գաղտնիության ինստիտուցիոնալացումը բխում է վաղուց հաստատված ավանդույթներից: Այդ ավանդույթներից յուրաքանչյուրի հիմքում ընկած արժեքներն ու շահերը տարատեսակ են և ինչ-որ չափով հակասական: Խնդիրը կապված է տեղեկացված լինելու իրավունքի և գաղտնիության իրական կարիքների պաշտպանության ինստիտուցիոնալացումն աստիճանաբար ներդաշնակեցնելու հետ՝ ինչպես դրանցով զբաղվող կազմակերպական կառույցներում, այնպես էլ կառավարման պրակտիկայում: Այդ երկու տեսակի քաղաքականության միջև ներդաշնակություն որոնելը տեսականորեն պետք է հանգեցնի միասնական, ինտեգրված քաղաքականության և ազգային կառավարման կառույցներում տեղեկատվության հասանելիության առավել հետեվողական ինստիտուցիոնալացման՝ ազգային անվտանգության կարիքներին համապատասխան:

Այնուամենայնիվ, «ազգային անվտանգություն» հասկացությունը բավականին անհստակ է, քանի որ կարող է ունենալ տարբեր իմաստներ տարբեր ազգային համատեքստերում, ինչն է՛լ ավելի է բարդացնում խնդիրը: Յակոբսենի կողմից ուսումնասիրված (2013թ.) եվրոպական երկրների մեծ մասում ազգային անվտանգությունը այս կամ այն չափով ներառում է միջազգային հարաբերությունները, ինչպես նաև ներքին անվտանգության սպառնալիքները: Այլ կերպ ասած, պարտադիր չէ, որ ակնհայտ սահմանագիծ լինի:

Պետական գաղտնիքի իրավաչափ լինելը պարզելու համար Աֆթերվուդը (2009թ., էջ 402-403) առաջարկում է գաղտնիության երեք գործնական կատեգորիաներ՝ միևնույն ժամանակ ընդունելով, որ պետական քաղաքականության մեջ կա օրինաչափ գաղտնիքն անօրինաչափից տարանջատելու, ինչպես նաև առաջինը պահպանելու, իսկ վերջինը՝ բացահայտելու խնդիր.

1. **Իրական ազգային անվտանգության գաղտնիություն.** կիրառվում է այնպիսի տեղեկատվության պաշտպանության համար, որի բացահայտումը կարող է որոշակի սպառնալիք առաջացնել ազգային անվտանգության համար՝ վտանգելով պաշտպանության կամ միջազգային հարաբերությունների հաստատման ընթացքը: Նման տեղեկատվությունը գաղտնի պահելը վիճելի չէ, քանի որ այն ընկած է գաղտնիության բոլոր համակարգերի հիմնավորման հիմքում, և հանրային շահը լավագույնս սպասարկվում է, երբ այս տեսակի տեղեկատվությունը մնում է գաղտնի:

2. **Բյուրոկրատական գաղտնիություն.** արտացոլում է բյուրոկրատների կողմից տեղեկատվությունը պաշտպանելու միտումը՝ ելնելով հարմարավետության նկատառումներից կամ այն ենթադրությունից, որ դրա բացահայտումը կարող է ավելի ռիսկային լինել, քան գաղտնի պահելը: Այս բյուրոկրատական միտումը սովորաբար բերում է պահանջվող մակարդակը գերազանցող գաղտնիության, ինչի արդյունքում ստեղծվում է գաղտնի դասակարգված տեղեկատվության անհարկի մեծ քանակ: Սա նաև մեծացնում է բյուջեի՝ գաղտնիության ապահովման հետ կապված ծախսերը և հաճախ ազդում է բյուրոկրատների՝ սեփական կարևորությունն ընդգծելու և որոշակի պետական

գերատեսչությունների աշխատանքի վերաբերյալ տեղեկատվությունը չբացահայտելու նրանց ցանկության վրա:

3. **Քաղաքական գաղտնիություն.** արտացոլում է քաղաքական առավելություն ապահովելու համար գաղտնիությունն օգտագործելու միտումը: Գաղտնիության այս ձևն ամենավիճարկելին է, քանի որ այն իրացնելիս չարաշահվում է ազգային անվտանգության իրական շահերի համընդհանուր ճանաչված օրինականությունը՝ սեփական շահերից բխող օրակարգն առաջ տանելու, քաղաքական հակասություններից խուսափելու կամ հանրային հաշվետվողականությունը շրջանցելու համար: Ծայրահեղ դեպքերում քաղաքական գաղտնիությամբ քողարկվում են օրենքի խախտման, մարդու իրավունքների ոտնահարման, կոռուպցիայի կամ չարաշահումների դեպքեր: Այն նաև սպառնալիք է օրինական քաղաքական գործընթացի համար:

ԴԱՏԱԿԱՆ ՄԱՐՄԻՆՆԵՐԻ ԸՆԴՀԱՆՈՒՐ ԹՈՒՅԼ ԴԵՐԱԿԱՏԱՐՈՒՄԸ ԴԱՍԱԿԱՐԳՄԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ՎԵՐԱՀՍԿՄԱՆ ԳՈՐԾՈՒՄ

Ինչպես արդեն նշվեց, դատարաններն ավանդաբար ցուցաբերել են, և առ այսօր ցուցաբերում են, բավականին նպաստավոր վերաբերմունք տեղեկատվությունը գաղտնի դասակարգող մարմինների գործողությունների և նրանց, այսպես կոչված, «*պետական գաղտնիք պարունակող հարցերում գործադիր արտոնության*» նկատմամբ: Դատական համակարգի ներկայացուցիչների նման նպաստավոր վերաբերմունքն օգնել է ամրապնդել այն համոզմունքը, որ ազգային անվտանգության հետ կապված հարցերը չափազանց զգայուն են՝ նույնիսկ դատարանում բացահայտելու համար (Setty, 2012բ .): ԱՄՆ-ից վերցված լավ օրինակ է հանդիսանում սառը պատերազմի ժամանակաշրջանում կայացած «*Միացյալ Նահանգներն ընդդեմ Ռեյնոլդսի*»[2] նշանավոր դատավարությունը:

Դատարանների նպաստավոր վերաբերմունքը գործադիր իշխանության նկատմամբ է՛լ ավելի ամրապնդվեց ԱՄՆ-ում սեպտեմբերի 11-ին տեղի ունեցած (հաճախ «9/11» անվանվող) ահաբեկչությունից հետո: Դատավարությունների ընթացքում ազգային անվտանգությունը պաշտպանելու մասին կառավարության պնդումները մշտապես գերկշռում են այնպիսի սկզբունքների նկատմամբ, ինչպիսիք են՝ հաշվետվողականությունը, թափանցիկությունը և բաց կառավարումը: ԱՄՆ-ում, ՄԹ-ում, Ֆրանսիայում և ժողովրդավարական աշխարհի այլ երկրներում, առավել ևս՝ պակաս ժողովրդավարական երկրներում կայացած բազմաթիվ գործեր ընդգծում են դատական իշխանության սահմանափակ դերը անվտանգության հետ կապված գործադիր մարմնի որոշումների վերանայման գործընթացում: Ցավոք, սա կարող է գործել ի վնաս օրենքի գերակայության, հիմնարար իրավունքների և անվտանգության իրական շահերի պաշտպանության:

ԱՄՆ-ում «*պետական գաղտնիք պարունակող հարցերում գործադիր արտոնությունը*», ՄԹ-ում՝ «*հանրային շահերի անձեռնմխելիության հավաստագիրը*», իսկ Ֆրանսիայում՝ «*պաշտպանության ոլորտի գաղտնիությունը*» գաղտնի տեղեկատվության հետ առնչվող գործադիր մարմինները շատ հաճախ օգտագործում են դատական վերանայումը կանխելու կամ այն պակաս արդյունավետ դարձնելու համար: Տվյալների թափանցիկության բացառությունները, որոնք հիմնված են վերոհիշյալ երեք տերմիններից բխող պնդումների վրա, սովորաբար ընդունվում են դատարանների

2 https://supreme.justia.com/cases/federal/us/345/1/case.html

կողմից, նույնիսկ եթե երբեմն դատարանները անորոշ կերպով նշում են, որ այդ արտոնությունը պետք է սահմանափակվի միայն իրական ազգային անվտանգության հարցերին առնչվող գործերով: Այս բավականին տարածված դատական դիրքորոշումը, ընդհանուր առմամբ, բացահայտում է «դատարանների կողմից զսպումների և հակակշիռների հասկացության անտեսումը, դատական պատասխանատվությունից հրաժարումը և պետական մարմինների կողմից չարաշահումների դեպքում դատական հայց ներկայացնելու համակարգի ապահովման կառուցվածքային անհրաժեշտության արհամարհումը» (Setty, 2012 թ . , էջ 1573):

Դատարանների դերի մասին իր նշանավոր աշխատության մեջ (2006թ . , էջ 168) Ֆուքսը նշում է, որ «հաշվի առնելով կառավարության տեղեկատվության մատչելիության իրավունքով պայմանավորված կարևոր արժեքները՝ այդ իրավունքը կարող է անտեսվել միայն այն դեպքում, երբ կա գաղտնիության օրինաչափ անհրաժեշտություն... Ո՛չ խորհրդարանները, ո՛չ հասարակությունն ինքնին ի վիճակի չեն վիճարկել չափազանց գաղտնիությունը: Անկախ վերանայումը դատական համակարգի պատասխանատվության մի մասն է, որի միջոցով ապահովվում է կառավարության գործողությունների պատշաճ լիազորումը»: Միայն դատարաններն են բավականաչափ անկախ՝ չափազանց գաղտնիությունը վիճարկելու դերը ստանձնելու համար, սակայն, ըստ էության, ինչպես նշում է Ֆուքսը, նրանք հրաժարվել են կատարել այդ դերը»:

Յակոբսենի ուսումնասիրած (2013թ .) եվրոպական գրեթե բոլոր երկրներում դատարանները լիազորված են ուսումնասիրել գաղտնի դասակարգված տեղեկատվությունը, որը կառավարությունը փորձում է գաղտնի պահել՝ ազգային անվտանգության նկատառումներից ելնելով: Սակայն ուշագրավ է այն, որ կան երկրներ, որտեղ գաղտնի դասակարգված տեղեկատվությունը կարող են ուսումնասիրել միայն հատուկ թույլտվություն ունեցող որոշակի դատարաններ կամ դատավորներ: Գերմանիայում միայն դաշնային վարչական դատարանը կարող է ուսումնասիրել գաղտնի դասակարգված որևէ տեղեկատվություն: Իսպանիայում, չնայած ծառայողական գաղտնիքի մասին օրենքը չի նախատեսում դատավորների համար մատչելիության իրավունք, ինչպես դա արվում է Կոնգրեսի և Սենատի դեպքում, գերագույն դատարանը որոշում է կայացրել այն մասին, որ միայն ինքն իրավունք ունի ծանոթանալ կառավարության տրամադրության տակ գտնվող գաղտնի տեղեկատվությանը: Ֆրանսիան միակ երկիրն է, որտեղ դատարանները չունեն գաղտնի դասակարգված տեղեկատվությունն ուսումնասիրելու ոչ մի լիազորություն (Սարտր և Ֆերլե, 2010թ .): Ֆրանսիական դատավորի համար գրեթե անհնար է ստանալ գաղտնի դասակարգված տեղեկատվությունն անմիջականորեն ուսումնասիրելու թույլտվություն: Այս արգելքի գործողությունը սահմանափակելու համար 1998 թ. ընդունված օրենքով ստեղծվեց անկախ մարմին հանդիսացող Ֆրանսիայի *Ազգային պաշտպանության գաղտնիության հարցերով հանձնաժողովը* (*Commission du secret défense nationale*, CSDN), որը դատավորի պահանջով կարող է ստանալ գաղտնի տեղեկատվության հասանելիության իրավունք՝ գնահատելու, թե արդյոք ողջամիտ է գաղտնազերծել այդ տեղեկատվությունը[3]: Ինչ վերաբերում է ԵՄ-ին, եվրոպական երկրների դատական իշխանությունների մեծ մասը հիմնականում ապավինում է պետական մարմնի այն եզրակացությանը, որ տեղեկատվության բացահայտումը կարող է վնասել ազգային անվտանգության շահերին (Jacobsen, 2013թ .):

3 http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense

ԳԱՂՏՆԻՈՒԹՅԱՆ ԴԱՍԱԿԱՐԳՄԱՆ ՉԱՓԱՆԻՇՆԵՐ ԵՎ ՄԱԿԱՐԴԱԿՆԵՐ

Գաղտնիության դասակարգման մակարդակները ստանդարտացված են, և ՏՀՋԿ շատ երկրներում կարելի է գտնել դասակարգման միևնույն համակարգը: ՏՀՋԿ երկրների շարքում Նոր Զելանդիան լավ օրինակ է, թե ինչպես է իրականացվում պետական գաղտնիք պարունակող տեղեկատվության հետ աշխատանքը: Նոր Զելանդիայում ծառայողական տեղեկատվությունը պաշտպանվում է ըստ չափանիշների, որոնք հիմնված են ծառայողական տեղեկատվությունը պաշտպանելու անհրաժեշտության հստակ սահմանման վրա՝ տեղեկատվությունը պետք է պաշտպանված լինի այնքանով, որքանով դա բխում է հանրային շահերից և գաղտնիությունը պահպանելու նպատակահարմարությունից: Տեղեկատվության գաղտնիությունը որոշելիս փորձ է արվում տվյալ տեղեկատվությունը դասակարգել՝ հաշվի առնելով այն վնասը, որը կարող է առաջանալ դրա չարտոնված բացահայտման արդյունքում, և հստակեցվում են այն պաշտպանական միջոցները, որոնք անհրաժեշտ է կիրառել[4]: Ըստ Նոր Զելանդիայի ուղեցույցների՝ գաղտնիության մակարդակներով դասակարգումն ինքնին չի նշանակում, որ ծառայողական տեղեկատվությունը պետք է թաքցնել, այլ միայն այն, որ տեղեկատվությունը պետք է դիտարկել ըստ էության՝ կիրառելով օրենքով սահմանված չափանիշներ[5]: Ավստրալիայի գաղտնիության գնահատման համակարգը հետաքրքիր է նրանով, որ այն սահմանում է հստակ ուղեցույցներ տվյալների գաղտնիության հաստատման և դրանց գաղտնազերծման վերաբերյալ[6]:

Նոր Զելանդիայում գաղտնիության մակարդակները, որոնք համահունչ են լայնորեն կիրառվող միջազգային պրակտիկային, սահմանվում են հետևյալ կերպ՝ կախված պաշտպանվող հանրային շահերից.

- Ազգային անվտանգության հետ կապված տվյալներ. տեղեկատվության բացահայտումը կարող է վտանգել երկրի կամ բարեկամական կառավարությունների անվտանգությունը, պաշտպանությունը կամ միջազգային հարաբերությունները.

- Կառավարության քաղաքականության և (կամ) գաղտնիության հետ կապված տվյալներ. տեղեկատվության Ազգային անվտանգության տեղեկատվությունն ունի պաշտպանության տարբեր մակարդակներ, որոնք որոշվում են՝ հաշվի առնելով հետևյալ չափանիշները.

1. **Չույժ գաղտնի.** տվյալների բացահայտումը կարող է հատկապես ծանր վնաս հասցնել ազգային շահերին .

    - Ուղղակի սպառնալիք հանդիսանալ Նոր Զելանդիայի կամ բարեկամ երկրների ներքին կայունության համար
    - Ուղղակիորեն հանգեցնել մարդկային կյանքի զանգվածային կորստի
    - Ծայրաստիճան վնաս հասցնել Նոր Զելանդիայի կամ դաշնակիցների ուժերի անվտանգությանը
    - Ծայրաստիճան վնաս հասցնել Նոր Զելանդիայի ուժերի կամ բարեկամական ուժերի գործառնական արդյունավետությանը
    - Ծայրաստիճան վնաս հասցնել հատկապես արժեքավոր անվտանգության կամ հետախուզական գործողությունների շարունակական արդյունավետությանը

4 Նոր Զելանդիայի «Պաշտոնական տեղեկատվության մասին» ակտ 1982թ . :

5 Նոր Զելանդիայի «Պաշտոնական տեղեկատվության պաշտպանության ուղեցույցներ»: Տե՛ս https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/

6 Ավստրալիա (2014թ .) . Տեղեկատվական անվտանգության կառավարման ուղեցույցներ: Ավստրալիայի կառավարության գաղտնիության դասակարգման համակարգ: Հասանելի է՝ https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf

- Ծայրաստիճան վնաս հասցնել այլ կառավարությունների հետ հարաբերություններին
- Երկարաժամկետ լուրջ վնաս հասցնել կարևոր ազգային ենթակառուցվածքներին

2. Գաղտնի. տվյալների բացահայտումը կարող է լուրջ վնաս հասցնել ազգային շահերին.

- Առաջացնել միջազգային լարվածություն
- Լրջորեն վնասել հարաբերությունները բարեկամական կառավարությունների հետ
- Լուրջ վնաս հասցնել Նոր Զելանդիայի կամ բարեկամական ուժերի անվտանգությանը
- Լուրջ վնաս հասցնել Նոր Զելանդիայի կամ բարեկամական ուժերի գործառնական արդյունավետությանը
- Լուրջ վնաս հասցնել արժեքավոր անվտանգության կամ հետախուզական գործողությունների արդյունավետությանը
- Լուրջ վնաս հասցնել Նոր Զելանդիայի կամ բարեկամ երկրների ներքին կայունությանը
- Արգելափակել կամ խաթարել կարևոր ազգային ենթակառուցվածքների աշխատանքը

3. Կոնֆիդենցիալ. տվյալների բացահայտումը կարող է զգալի վնաս հասցնել ազգային շահերին.

- Էական վնաս հասցնել դիվանագիտական հարաբերություններին՝ հանգեցնելով պաշտոնական բողոքի ներկայացման կամ այլ պատժամիջոցների կիրառման
- Վնաս հասցնել Նոր Զելանդիայի կամ բարեկամական ուժերի գործառնական արդյունավետությանը
- Վնաս հասցնել Նոր Զելանդիայի կամ բարեկամական ուժերի անվտանգությանը
- Վնաս հասցնել արժեքավոր անվտանգության կամ հետախուզական գործողությունների արդյունավետությանը
- Վնաս հասցնել Նոր Զելանդիայի կամ բարեկամ երկրների ներքին կայունությանը
- Խաթարել կարևոր ազգային ենթակառուցվածքների աշխատանքը

4. Ծառայողական (սահմանափակ) օգտագործման համար. տվյալների բացահայտումը կարող է բացասաբար ազդել ազգային շահերի վրա.

- Բացասաբար ազդել դիվանագիտական հարաբերությունների վրա
- Խոչընդոտել Նոր Զելանդիայի կամ բարեկամական ուժերի գործառնական արդյունավետությանը
- Խոչընդոտել Նոր Զելանդիայի կամ բարեկամական ուժերի անվտանգությանը
- Բացասաբար ազդել Նոր Զելանդիայի կամ բարեկամ երկրների ներքին կայունության վրա
- Բացասաբար ազդել Նոր Զելանդիայի կամ բարեկամ երկրների տնտեսական բարեկեցության վրա

Պետական քաղաքականության և անհատների անձնական տվյալների համար սահմանվում են տարբեր մակարդակներ՝ ելնելով հետևյալ չափանիշներից.

1. Սահմանափակ հասանելիությամբ մասնավոր տվյալներ. տվյալների բացահայտումը կարող է վնաս հասցնել պետական շահերին կամ վտանգի ենթարկել քաղաքացիներին.

- Վտանգել որևէ անձի անվտանգությունը
- Լուրջ վնաս հասցնել Նոր Զելանդիայի տնտեսությանը
- Խոչընդոտել կառավարության բանակցություններին

2. **Կոնֆիդենցիալ հիմքով տրամադրված.** տվյալների բացահայտումը կարող է վնասել օրենքի և հանրային կարգի պահպանմանը, միջամտել պետական գործերի վարմանը, ազդել քաղաքացիների մասնավոր կյանքի անձեռնմխելիության վրա.

- Վնաս հասցնել օրենքների պահպանմանը
- Բացասաբար ազդել անհատի մասնավոր կյանքի անձեռնմխելիության վրա
- Վնաս հասցնել քաղաքացու առևտրային տեղեկատվությանը
- Վնաս հասցնել՝ կոնֆիդենցիալ տեղեկատվության չբացահայտման պարտավորության խախտման հետևանքով
- Վնասել քաղաքացիների առողջության կամ անվտանգության պաշտպանության միջոցառումների իրականացմանը
- Վնասել Նոր Զելանդիայի տնտեսական շահերին
- Վնասել հասարակության համար նյութական կորուստները կանխող կամ մեղմացնող միջոցառումների իրականացմանը
- Հանգեցնել սահմանադրական դրույթների խախտման
- Խոչընդոտել պետական գործերի արդյունավետ վարմանը
- Հանգեցնել օրինական մասնագիտական արտոնությունների խախտման
- Խոչընդոտել կառավարության առևտրային գործունեությանը
- Հանգեցնել անիրավաչափ շահույթ կամ առավելություն ստանալու նպատակով տեղեկատվության բացահայտման կամ օգտագործման

Ինչպես արդեն նշվեց, ՏՀԶԿ շատ երկրներում կարելի է գտնել դասակարգման համանման նշումներ և չափանիշներ: Նույնիսկ Թուրքիայում, որտեղ գաղտնիության կանոնները հրապարակավ մատչելի չեն, հայտնի է գաղտնիության որոշակի մակարդակների առկայության մասին (Jacobsen 2013թ.): Շվեդիան Յակոբսենի ուսումնասիրությանը (2013թ.) մասնակցած միակ երկիրն էր, որտեղ օրենքը չի սահմանում տեղեկատվության գաղտնիության մակարդակներ, քանի որ այդ երկրում գաղտնիությունը միայն վարչարարական գործառույթ է կատարում: Տեղեկատվության գաղտնիության հետ կապված այլ ասպեկտները (օրինակ՝ դասակարգման ընթացակարգեր, մակագրման պահանջներ, գաղտնիության իրավասություններ, գաղտնիությունը հիմնավորելու պարտավորություններ, սխալ դասակարգման համար պատասխանատվություն, վերահսկող մարմիններ և այլն) զգալիորեն տարբերվում են եվրոպական տարբեր երկրներում (տե՛ս Jacobsen 2013թ. և Թրանսփարենսի ինթերնեշնլ ՄԹ 2014թ.):

ԳԱՂՏՆԱԶԵՐԾՄԱՆ ՉԱՓԱՆԻՇՆԵՐ

Եվրոպական երկրներում տեղեկատվության գաղտնազերծման համար սահմանված են երեք հիմնական չափանիշներ՝ ժամկետներ, շրջադարձային իրադարձություն կամ պարտադիր վերանայման ժամանակահատված: Հիմնական նպատակն է կանխել տեղեկատվության մշտապես գաղտնի դասակարգված լինելը: Այնուամենայնիվ, քչաթիվ չեն այն երկրները, որտեղ օրենսդրական կամ վարչարարական պրակտիկայում դասակարգված տեղեկատվության գաղտնազերծման որևէ չափանիշ նախատեսված չէ: Յակոբսենի (2013թ.) կողմից կատարված հաշվարկի համաձայն՝ եվրոպական երկրներում գաղտնի դասակարգելու ժամկետի միջին տևողությունը 30

տարի է. մասնավորապես, Նիդեռլանդներում այդ ժամկետը կազմում է 10 տարի, Ռումինիայում՝ 100 տարի, Իսպանիայում և Թուրքիայում գաղտնագրումն անժամկետ է: Վերջինս, սակայն, գրեթե բացառություն է Եվրոպայում:

Որպես գաղտնի դասակարգված տեղեկատվության ամենատարածված պարտադիր վերանայման ժամանակահատվածը 5 տարի է: Շվեդիայում չկա նախապես սահմանված պարտադիր վերանայման ժամկետ, սակայն տեղեկատվության գաղտնիությունը վերանայվում է յուրաքանչյուր անգամ, երբ ներկայացվում է բացահայտման հայց: Ինքնաբերական գաղտնագերծման (շրջադարձային իրադարձություն) պրակտիկան տարբեր երկրներում տարբերվում է, սակայն դրանց մեծ մասում հիմնական ասպեկտը տարբեր դասակարգում ունեցող տեղեկատվության գաղտնագերծման մասին կառավարության հայեցողական որոշումն է: Նման որոշումը կարող է կայացվել նաև քաղաքացու կամ քաղաքացիական կազմակերպության կողմից «Տեղեկատվության մատչելիության մասին» օրենքի համաձայն ձեռնարկված ընթացակարգի շրջանակներում:

ԳԱՂՏՆԻՈՒԹՅԱՆ ՎԵՐԱՀՍԿՄԱՆ ԹԵՍՏԵՐԻ ԿԻՐԱՌՈՒՄ. ՀՆԱՐԱՎՈՐ ՎՆԱՍԻ ԹԵՍՏ ԵՎ ՀԱՆՐԱՅԻՆ ՇԱՀԵՐԻ ՀԱՎԱՍԱՐԱԿՇՌՄԱՆ ԹԵՍՏ

Ըստ *Right2INFO.org*-ի՝ (հասարակական կազմակերպություն, որը նպաստում է պատշաճ օրենսդրության ու պրակտիկայի ձևավորմանը), այսպես կոչված, «հնարավոր վնասի թեստը» և «հանրային շահերի թեստը» բխում են այն պահանջից, որ տեղեկատվություն ստանալու իրավունքի սահմանափակումները պետք է լինեն համաչափ և անհրաժեշտ[7]: Այդ թեստերի հիմքում ընկած հասկացությունների համար ՏՀԶԿ ՍԻԳՄԱ-ն (2010թ.) առաջարկում է լայնածավալ և մանրամասն հայեցակարգային մոտեցում, որում տարբերակվում են տեղեկատվության մատչելիության բացարձակ և հարաբերական սահմանափակումները: Առաջինների թվում, ընդհանուր առմամբ, ընդգրկված են պաշտպանության և ազգային անվտանգության հետ կապված սահմանափակումները:

ՀՆԱՐԱՎՈՐ ՎՆԱՍԻ ԹԵՍՏ

Հնարավոր վնասի թեստի համաձայն՝ պետական մարմինը պետք է հիմնավորի, որ որոշակի տեղեկատվության բացահայտումը պարունակում է պաշտպանված շահերի վնասման սպառնալիք: Հետևաբար, այն չպետք է բացահայտվի: Հնարավոր վնասի թեստը պահանջում է, որ պետությունը հիմնավորի տվյալ օրինական շահերի համար զգալի և ակնհայտ վնասի ռիսկի առկայությունը: Պետք է ցույց տրվի, որ սահմանափակումը կապված է որոշակի օրինական շահերի հետ, և տեղեկատվության բացահայտումը էականորեն կվնասի այդ շահերին: Նման հնարավոր վնասը պետք է լինի բավականաչափ հստակ, որոշակի, սպառնացող և անմիջական, այլ ոչ թե ենթադրվող կամ հեռավոր:

ՀԱՆՐԱՅԻՆ ՇԱՀԵՐԻ ՀԱՎԱՍԱՐԱԿՇՌՄԱՆ ԹԵՍՏ

Հանրային շահերի հավասարակշռման թեստը վերաբերում է համաչափությանը: Թեստը պահանջում է կատարել հաշվեկշռման գնահատում, որում տվյալների բացահայտումից վնասը համադրվում է բացահայտման միջոցով սպասարկվող հանրային շահի հետ: Պայմանները, որոնց դեպքում հստակ և կոնկրետ հանրային շահը կարող է գերազանցել գաղտնիության պահանջը, որոշվում են ազգային օրենսդրությամբ: Գաղտնիության դասակարգման շատ ազգային մոդելների հա-

7 http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test

մածայն՝ ներառյալ միջամերիկյան և աֆրիկյան, հանրային շահը դառնում է պարտադիր և գերակշիռ է մյուս շահերի նկատմամբ, եթե տեղեկատվությունը վերաբերում է մարդու իրավունքների խախտմանը կամ մարդկության դեմ հանցագործությանը: Հավասարակշռման թեստը պահանջում է, որ հանրային մարմինը կամ վերահսկող մարմինը գնահատեն այն վնասը, որը բացահայտումը կարող է պատճառել որոշակի պաշտպանված շահի՝ այն համադրելով տեղեկատվության բացահայտմամբ սպասարկվող հանրային շահի հետ:

Հանրային շահը տարբեր երկրներում ունի տարբեր սահմանումներ և հաճախ յուրաքանչյուր առանձին դեպքի համար պահանջում է առանձին գնահատում: Ընդհանուր առմամբ, բացահայտմանը նպաստող հանրային շահերը սովորաբար կապված են հանրային բանավեճի, քաղաքական բանավեճին հասարակության մասնակցության, պետական միջոցների բաշխման և ծախսման համար հաշվետվողականության և հանրային անվտանգության հարցերի հետ: Հանրային անվտանգության և շրջակա միջավայրի, առողջությանը սպառնացող էական վտանգների հետ կապված հարցերը և մարդու իրավունքների կոպիտ խախտումների վերաբերյալ տեղեկատվությունը սովորաբար դիտվում են որպես տեղեկատվության բացահայտմամբ սպասարկվող հանրային շահի պարտադիր գերակայությունն արդարացնող:

Որոշ երկրներ հրապարակել են քաղծառայողների վարչարարական ընթացակարգերի ուղեցույցներ: Օրինակ՝ Ավստրալիայի Նոր Հարավային Ուելս նահանգում տեղեկատվություն բացահայտելու որոշում կայացնելիս պետական ծառայողները պետք է կիրառեն հանրային շահերի հավասարակշռման թեստը: Դա նշանակում է, որ նրանք պետք է համադրեն բացահայտման նպատակահարմարության մասին վկայող գործոնները չբացահայտմամբ սպասարկվող հանրային շահի գործոնների հետ[8]: Տվյալ ուղեցույցի համաձայն՝ հանրային շահերի հավասարակշռման թեստը ներառում է երեք փուլ.

1. Սահմանել տեղեկատվության բացահայտմամբ սպասարկվող հանրային շահը:

2. Սահմանել տեղեկատվության չբացահայտմամբ սպասարկվող հանրային շահը:

3. Գնահատել տեղեկատվության բացահայտմամբ և չբացահայտմամբ սպասարկվող հանրային շահի հարաբերական կշիռը և որոշել, թե որտեղ է այդ շահերի միջև հավասարակշռությունը:

Չնայած տեղեկատվության բացահայտման օգտին Ավստրալիայի օրենսդրության հստակ դիրքորոշմանը, տեղեկատվության հասանելիության նահանգային օրենքները սահմանում են մի շարք իրավիճակներ, երբ նախապատվությունը տրվում է տեղեկատվությունը չբացահայտելուն և գաղտնիությունը պաշտպանելուն: Առավել ակնառու է այն տեղեկատվությունը, որի վրա տարածվում է գաղտնիության մասին օրենքի գործողությունը, որի հետ կապված սահմանված են 26 օրենսդրական ակտեր: Այն համահունչ է ՏՀՋԿ շատ երկրների վրա տարածվող ընդհանուր միտմանը, ըստ որի տեղեկատվության ազատության մասին օրենքները (FOIAs) գործնականում դադարեցին լինել արդիական՝ հատվելով պետական գաղտնիքների մասին ավանդական օրենսդրությանը: Պետական գաղտնիքները հաճախ պահվում են տեղեկատվության ազատ հասանելիության մասին օրենսդրության շրջանակներից դուրս: Ավելին, շատ երկրներում, ընդհանուր առմամբ, քիչ ջանքեր են գործադրվում՝ պետական գաղտնիքի մասին ավան-

8 http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

դական օրենսդրությունը հանրային տեղեկատվության ազատ մատչելիության մասին նոր օրենսդրությանը համապատասխանեցնելու համար:

Այն փաստը, որ տեղեկատվության ազատության մասին շատ օրենքներ գրեթե չեն անդրադառնում ազգային անվտանգության հետ կապված գաղտնիությանը, նշանակում է, որ օրենսդրությանն ապավինելը ու դատարաններին դիմելը մինչ այժմ բավականաչափ արդյունավետ չեն եղել՝ անվտանգության մարմինների և հետախուզական գործակալությունների աշխատանքում անվտանգությունն ու գաղտնիությունն օգտագործելու համընդհանուր միտումը նվազեցնելու համար: Նման հաստատությունները՝ գաղտնի տեղեկատվության հետ գործ ունենալու իրենց ավանդական և հաճախ անթափանց գործելակերպով, հիմնականում մնում են տեղեկատվության ազատության մասին օրենքների ազդեցությունից դուրս, չնայած հանրային թափանցիկությանը նպաստող ընդհանուր միջազգային միտումներին և «տեղեկացված լինելու իրավունքը» իրացնելու քաղաքացիական հասարակության պահանջներին:

Այս ամենը վկայում է այն մասին, որ գաղտնիությունն ու հրապարակայնությունն արդյունավետորեն հավասարակշռող ընդհանուր օրենսդրության ընդունումը մարտահրավեր է ինչպես տեսական, այնպես էլ գործնական առումով: Պատճառներից մեկն այն է, որ պետական մարմինները կամ գործակալությունները, որոնք առավել շատ են միտված գաղտնագրել տեղեկատվությունը, իրենց աշխատանքում և գործելակերպում հաճախ ունենում են բոլորովին այլ նպատակներ և դրդապատճառներ: Դա հանգեցնում է անվտանգության հետ կապված տարբեր վարչական մշակույթների ձևավորմանը: Օրինակ՝ ռազմական իշխանությունները հիմնականում ուշադրություն են դարձնում գենքի տեխնոլոգիայի և օպերատիվ պլանների անվտանգությանը, հետախուզական գործակալությունները՝ աղբյուրների և աշխատանքի մեթոդների պաշտպանությանը, դիվանագետները մտահոգված են դիվանագիտական տեղեկատվության գաղտնագրման և հանրայնացման միջազգային հետևանքներով, իսկ ոստիկանությունը փորձում է պաշտպանել իր տեղեկատուներին և օպերատիվ պլանները: Արդյունքում, յուրաքանչյուր մարմին կամ գերատեսչություն մշակում է իր սեփական ուղեցույցները, ընթացակարգերն ու արձանագրությունները, որոնք սովորաբար ուժի մեջ են մնում երկար տարիներ՝ առանց մանրակրկիտ վերլուծության և լուրջ վերանայման: Ավելին, հասկանալի է, որ վերը թվարկված գերատեսչություններում աշխատակիցները նախընտրում են գործել անվտանգ՝ ավելորդ խնդիրներից խուսափելու համար, ինչը հաճախ հանգեցնում է ավելորդ գաղտնիության (Aftergood, 2009թ.):

Արդյունքում, իրազեկ դիտորդներն ու պրակտիկ մասնագետները ենթադրում են, որ նույնիսկ եթե կոնկրետ գերատեսչություն պետք է կատարի տեղեկատվության գաղտնիության դասակարգում, ապա գաղտնազերծում կատարող մարմինն ու համապատասխան լիագորությունը պետք է լինի այդ գերատեսչությունից դուրս: Դա այդպիսի գերատեսչության կողմից սեփական շահերը հետապնդելու միտումը չեզոքացնելու և չափազանց գաղտնիությունը բացառելու լավագույն միջոցն է (Aftergood, 2009թ., էջ 412): Դա իրականացնելու մի քանի հաջող փորձեր արվել են ԱՄՆ-ում, մասնավորապես՝ *Գաղտնիության բողոքարկման միջգերատեսչական խորհրդի* (ISCAP)[9] և *Գաղտնիության քաղաքականության հիմնարար վերլուծության* (FCPR)

9 https://www.archives.gov/declassification/iscap

միջոցով[10]: Մեկ այլ օրինակ է վերոհիշյալ Ազգային պաշտպանության գաղտնիության հարցերով հանձնաժողովը (CSDN) Ֆրանսիայում: Աֆթերգուդի (2009թ.) նկարագրած ամերիկյան փորձը, ըստ էության, ցույց է տալիս, որ «եթե մի գերատեսչություն չի կարող հաջողությամբ բացատրել և համոզել որևէ բարձրաստիճան պաշտոնյայի կամ այլ գերատեսչությունների խորհրդի, թե ինչու է անհրաժեշտ, ելնելով ազգային անվտանգության շահերից, գաղտնի դասակարգել որևէ տեղեկատվություն, ապա հիմքեր կան՝ կասկածի տակ դնելու այն մշտապես գաղտնի պահելու անհրաժեշտությունը»:

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆՆԵՐ

1. Անհրաժեշտ է մշակել անվտանգության և պաշտպանության ոլորտներում տեղեկատվության գաղտնիության օրենսդրություն, որը պետք է լինի հնարավորինս հստակ: Այդպիսի օրենսդրությունը պետք է չափանիշներ սահմանի տեղեկատվության՝ որպես գաղտնի դասակարգման և գաղտնազերծման համար՝ միաժամանակ նկատի ունենալով, որ օրենսդրությունը սովորաբար ունի ընդհանուր բնույթ, և, հետևաբար, նշված չափանիշները նույնպես կլինեն ընդհանուր: Գաղտնիությունը կարգավորող օրենսդրությունը, որը շատ երկրներում գերակայում է տեղեկատվության ազատ հասանելիությանն առնչվող օրենսդրության նկատմամբ, պետք է համապատասխանեցվի վերջինիս հետ՝ տվյալ երկրի իրավական դաշտում հակասություններից խուսափելու համար:

2. Պատշաճ իրավական դաշտի հետ մեկտեղ՝ անհրաժեշտ է գերատեսչության մակարդակով հմուտ և փորձառու ղեկավարության առկայություն, որը գաղտնիության դասակարգման իրավական չափանիշները կկիրառի ողջամիտ և շրջահայաց ձևով՝ հնարավորինս մեծ չափով նպաստելով ժողովրդավարական արժեքների և հասարակության առջև թափանցիկության սկզբունքների ապահովմանը: Տարբեր նկատառումները հավասարակշռելու անհրաժեշտության գիտակցված ըմբռնումը պետք է կազմակերպական մշակույթի մաս կազմի: Համապատասխան մարմինների ղեկավարները պետք է իրենց առջև խնդիր դնեն՝ հավասարակշռված մոտեցում ապահովել օրինական գաղտնիության և օրինական թափանցիկության պահանջների միջև:

3. Անհիմն և ավելորդ գաղտնիության նվազեցումը և տեղեկացված լինելու հանրային իրավունքի ու ազգային անվտանգության պահանջների, ինչպես նաև գաղտնիության այլ օրինական հիմնավորումների հավասարակշռումը բարդ խնդիր է ներկայացնում: ԵՄ և ՏՀՋԿ երկրների մեծ մասում պաշտպանության ոլորտի գաղտնիության մշակույթի վերածումը թափանցիկության մշակույթի, ըստ երևույթին, անիրագործելի խնդիր է տեսանելի ապագայում[11]:

4. Անվտանգության և պաշտպանության ոլորտի աշխատակիցներից և այլ գործընկերներից պահանջվում է դրսևորել հավատարմություն, հարգանք և շրջահայացություն հաստատված ընթացակարգերի նկատմամբ: Այդ որակները, անշուշտ, անհրաժեշտություն են, սակայն պետք է խրախուսել նաև որոշակի աստիճանի նորարարություն և նոր գաղափարներ, նույնիսկ եթե հնարավոր փոփոխությունների շրջանակը մեծ չլինի: Ըստ այդմ, պետք է

10 https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/ODNI%20FY2017%20FCGR.pdf : **Տե՛ս նաև 1994թ.** Էներգիայի դեպարտամենտի առաջատար գեկույցը՝ https://www.osti.gov/opennet/forms.jsp?formurl=od/fcprsum.html

11 Նույնիսկ եթե թվում է, որ Ռումինիային դա հաջողվել է իրագործել (Matei, 2007թ.):

քննադատական մոտեցում ցուցաբերել այն հարցին, թե ինչպես ձեռք բերել օպտիմալ հավասարակշռություն, մի կողմից՝ օրինական գաղտնիության, և մյուս կողմից՝ տեղեկատվության օրինական հասանելիության միջև:

5. Գաղտնիության մասին օրենքների կամ քաղաքականության իրականացման համար պատասխանատու անձնակազմը պետք է հատուկ վերապատրաստված լինի, որպեսզի կարողանա համապատասխան կարևորություն տալ կառավարությունից պահանջվող բաց և թափանցիկ կառավարման ժողովրդավարական պահանջին՝ միևնույն ժամանակ օրենսդրության հիման վրա հստակ տարբերակի տեղեկատվության այն տեսակները, որոնք պետք է թաքցվեն հանրային հասանելիությունից: Տվյալների ոչ խտրական բացահայտումը չի հանդիսանում ոչ խտրական գաղտնիության այլընտրանքը: Անվտանգության և պաշտպանության ոլորտում աշխատող անձնակազմի որակավորումն ու կարողությունները մեծ նշանակություն ունեն, քանի որ դրանք ուղղակիորեն ազդում են ժողովրդավարական հասարակության և անվտանգության մարմինների ու քաղաքացիական հասարակության միջև հարաբերությունների վրա:

6. Անկախ գործող որևէ հաստատություն, օրինակ՝ միջզերատեսչական գաղտնազերծման հանձնաժողով, որը դուրս է գտնվում տեղեկատվությունը գաղտնի դասակարգող հիմնական մարմինների բացառիկ լիազորությունների սահմաններից, օր.՝ ռազմական, հետախուզական և ոստիկանության մարմիններ, պետք է լիազորություն ունենա վերանայել և պարբերաբար գաղտնազերծել կոնկրետ մարմինների կողմից գաղտնի պահվող տեղեկատվությունը: Ընդհանուր առմամբ, դատարանները սովորաբար չափազանց նպաստավոր վերաբերմունք են ցուցաբերել պետական գաղտնիք պարունակող հարցերում գործադիր արտոնությանը, և այս առումով փոփոխություններ ակնկալելու բավարար հիմքեր չկան:

7. Ներկայումս կարծես թե ձևավորվում են նոր գործելակերպեր, որոնք ենթադրում են հայեցողական լիազորությունների նվազեցում՝ ի տարբերություն գաղտնիության դասակարգման ավանդական մոտեցումների: Դրանց էությունը կայանում է նրանում, որ տեղեկատվության դասակարգման և գաղտնազերծման վերաբերյալ որոշումը պետք է կայացվի ոչ թե որևէ անհատի, այլ անկախ կոմիտեի կամ հանձնաժողովի կողմից, որն իրավասու է անկողմնակալ որոշում ընդունել ցանկացած տեղեկատվության ամբողջական կամ մասնակի դասակարգման կամ գաղտնազերծման անհրաժեշտության վերաբերյալ: Նմանատիպ մասնագիտացված մարմինը պետք է առաջնորդվի իրավականորեն հաստատված չափանիշներով, որպեսզի որոշի վնասի չափը և իրականացնի հավասարակշռման թեստեր: Այս անկախ կոմիտեի կամ հանձնաժողովի անդամների թիվը պետք է սահմանափակ լինի, օրինակ՝ 5-7 անդամ, և կարող է ներառել անվտանգության ոլորտի փորձագետներ, որոնք ներկայացնում են գործադիր իշխանությունը, խորհրդարանը, պատգամավորներին և օմբուդսմենին և դատական իշխանությունը:

ՏԵՂԵԿԱՏՎԱԿԱՆ ՌԵՍՈՒՐՍՆԵՐ

Aftergood, Steven (2009):"*Reducing Government Secrecy: Finding What Works,*" in Yale Law & Policy Review Հատոր 27, թիվ 2 (գարուն, 2009թ.), էջ 399-416: Հասանելի է՝ https://www.jstor.org/stable/40239716?seq=1#page_scan_tab_contents

Fenster, Mark (2010): *Seeing the State: Transparency as Metaphor*, in Administrative Law Review, էջ 617-672, Հասանելի է՝ http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1571&context=facultypub

Fuchs, Meredith (2006): *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, in Administrative Law Review, Հատոր 58, թիվ 1, ձմեռ 2006թ., էջ 131-176

Jacobsen, Amanda L. (2013): *National Security and the Right to Information in Europe*. Հասանելի է՝ http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

Matei, Florina Cristiana (2007): *Reconciling Intelligence Effectiveness and Transparency: The Case of Romania*, in Strategic Insights, Հատոր VI, հրատարակություն 3 (մայիս 2007թ.): Հասանելի է՝ https://calhoun.nps.edu/bitstream/handle/10945/11297/mateiMay07.pdf?sequence=1

OECD (2010), "*The Right to Open Public Administrations in Europe: Emerging Legal Standards*", SIGMA Papers, թիվ 46, OECD Publishing, Paris. Հասանելի է՝ http://dx.doi.org/10.1787/5km4g0zfqt27-en

Riese, Dorothée (2014): *Secrecy and Transparency*, 2014թ. սեպտեմբերի 3-6-ը Գլազգոյում՝ ECPR համաժողովի ընթացքում, ներկայացված զեկույց: Հասանելի է՝ https://ecpr.eu/Filestore/PaperProposal/2cedead9-5191-42de-ae36-7d320a28a304.pdf

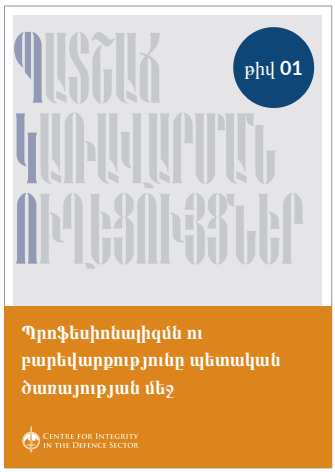
Sartre, Patrice & Ferlet, Philippe (2010): *Le secret de défense en France* in Revue Études 2010/2, Հատոր 412, փետրվար, էջ 165-175: Հասանելի է՝ https://www.cairn.info/revue-etudes-2010-2-page-165.htm

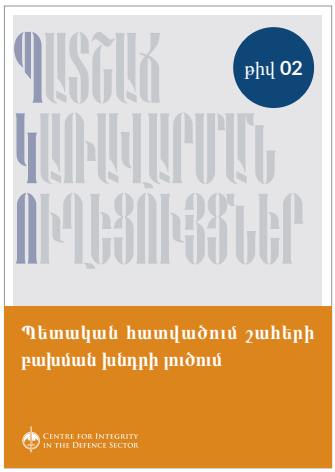
Sauvé, Jean-Marc (2011): *Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ? Transparence, valeurs de l'action publique et intérêt général,* Թրանսպարենսի ինթերնեշնլ Ֆրանսիայի կողմից 2011թ. հուլիսի 5-ին՝ երեքշաբթի, կազմակերպված սիմպոզիումի ընթացքում Ազգային Ժողովում ներկայացված ելույթ: Հասանելի է՝ http://www.conseil-etat.fr/content/download/2597/7819/version/1/file/discours-transparence-international.pdf

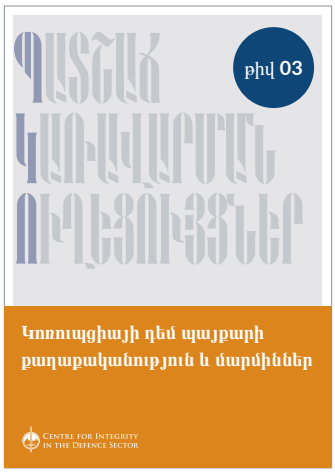
Setty, Sudha (2012): *The Rise of National Security Secrets,* in Connecticut Law Review, հատոր 44, թիվ 5, հուլիս 2012թ., էջ 1563-1582

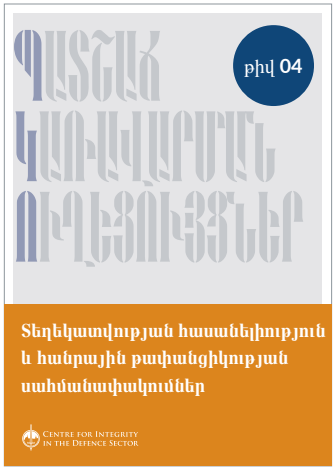
Թրանսպարենսի ինթերնեշնլ ՄԹ (2014թ.). Գաղտնի տեղեկատվություն. 15 երկրների վերլուծություն: Հասանելի է՝ http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

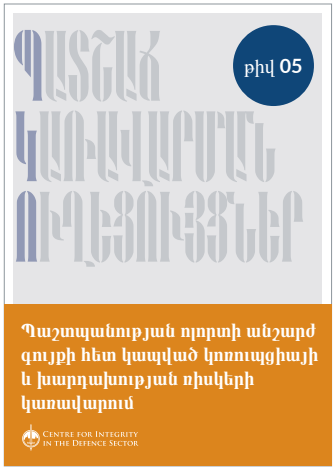
Պատշաճ կառավարման ուղեցույցներ








ՊԱՏՇԱՌ
ԿՈՌՈՒՊՑԻԱՆ
ՈՒՍՈՒՄՆԱՍԻՐՈՒԹՅՈՒՆՆԵՐ
թիվ 04
Տեղեկատվության հասանելիություն և հաերային թափանցիկության սահմանափակումներ
Centre for Integrity in the Defence Sector


ՊԱՏՇԱՌ
ԿՈՌՈՒՊՑԻԱՆ
ՈՒՍՈՒՄՆԱՍԻՐՈՒԹՅՈՒՆՆԵՐ
թիվ 05
Պաշտպանության ոլորտի անշարժ գույքի հետ կապված կոռուպցիայի և խարդախության ռիսկերի կառավարում
Centre for Integrity in the Defence Sector

«Պատշաճ կառավարման ուղեցույցները» իրենցից ներկայացնում են ոչ ծավալուն գրքույկների շարք, որոնցից յուրաքանչյուրի մեջ քննարկվում է պաշտպանության ոլորտում պատշաճ կառավարման կարևորությանն առնչվող որոշակի թեմա: Ուղեցույցները նախատեսված են այն անձանց համար, ովքեր ցանկանում են ավելին իմանալ պաշտպանության ոլորտում, կամ ընդհանուր առմամբ՝ պետական հատվածում, պատշաճ կառավարմանն ուղղակիորեն առնչվող մեկ կամ մի քանի թեմաների մասին, ինչպես նաև կարող են օգտագործվել կրթական նպատակներով:

Հրատարակությունը՝ Պաշտպանության ոլորտում բարեվարքության կենտրոն
Դիզայնը՝ www.melkeveien.no
Տպագրությունը՝ Նորվեգիայի կառավարության անվտանգության և սպասարկման կազմակերպություն
Մայիս/2018թ . : Տպաքանակ՝ 100 օրինակ

Centre for Integrity in the Defence Sector
www.cids.no

NATO OTAN

Անգլերեն բնօրինակի թարգմանությունը հայերեն լեզվի կատարվել է Հյուսիսատլանտյան դաշինքի կազմակերպության հովանու ներքո: