DOI: 10.59560/18291155-2025.4-238

ԵՂԵԳՆԻ ԲԱԲԱՅԱՆ

«Դը Լեգալ Լիդերս» իրավաբանական ընկերության փաստաբան, ՀԵՀ իրավագիտության ամբիոնի հայցորդ

ԹՎԱՅԻՆ ԻՆՔՆԻՇԽԱՆՈՒԹՅՈՒՆ ԵՎ ՍԱՀՄԱՆԱԴՐԱՀԻՐԱՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ. ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԱՌՋԵՎ ԾԱՌԱՑԱԾ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԸ ԳԼՈԲԱԼ ՏԵԽՆՈԼՈԳԻԱԿԱՆ ԶԱՐԳԱՑՄԱՆ ՀԱՄԱՏԵՔՍՏՈՒՄ

Ամփոփագիր

Ժամանակակից գլոբալիզացիայի և տեխնոլոգիական առաջընթացի պայմաններում պետության ինքնիշխանության դասական ըմբռնումը ենթարկվում է էական վերափոխման: Եթե նախկինում ինքնիշխանությունը սահմանափակվում էր տարածքային ամբողջականությամբ և քաղաքական անկախությամբ, ապա 21-րդ դարում այն ստանում է նոր՝ թվային չափում: **Թվային ինքնիշխանությունը** դառնում է պետության իրավական և ինստիտուցիոնալ կարողությունը՝ ինքնուրույն կերպով տնօրինելու, կարգավորելու և պաշտպանելու սեփական թվային ենթակառուցվածքները, տվյալների շրջանառությունը և տեղեկատվական անվտանգությունը:

Հայաստանի Հանրապետության համար թվային ինքնիշխանության խնդիրն ունի ռազմավարական նշանակություն, քանի որ տեղեկատվական կախվածությունը, կիբեռանվտանգության թերի համակարգը և տվյալների պաշտպանության իրավական բացերը կարող են սահմանափակել պետության սահմանադրական ինքնիշխանությունը: Այս տեսանկյունից թվային ինքնիշխանությունը դիտարկվում է ոչ միայն որպես տեխնոլոգիական, այլև սահմանադրաիրավական անվտանգության հիմնարար բաղադրիչ:

Ուսումնասիրության նպատակն է բացահայտել թվային ինքնիշխանության և սահմանադրաիրավական անվտանգության փոխկապակցվածությունը՝ առանձնացնելով այն մարտահրավերները, որոնց առջև կանգնած է Հայաստանի Հանրապետությունը գլոբալ տեխնոլոգիական միջավայրում: Աշխատության մեջ առանձնացվել են երեք հիմնական ուղղություններ՝ կիբեռանվտանգության իրավական համակարգի թերի զարգացվածությունը, տվյալների պաշտպանության

մեխանիզմների կատարելագործման անհրաժեշտությունը և թվային ենթակառուցվածքների արտաքին կախվածության ռիսկերը:

Արդյունքում հիմնավորվում է, որ թվային ինքնիշխանությունը պետք է ներառվի ազգային և սահմանադրաիրավական անվտանգության համակարգի առանցքային տարրերի շարքում: Վերջինիս ապահովման համար անհրաժեշտ է մշակել համապարփակռազմավարություն, իրականացնել օրենսդրական և ինստիտուցիոնալ բարեփոխումներ, ինչպես նաև զարգացնել թվային իրավագիտակցության մակարդակը պետական և հասարակական մակարդակներում:

Այսպիսով, թվային ինքնիշխանությունը դառնում է ժամանակակից պետականության նոր սահմանագիծ՝ պետական անկախության, տեղեկատվական պաշտպանության և սահմանադրական կայունության համադրման տիրույթում:

Հիմնաբառեր. թվային ինքնիշխանություն, սահմանադրաիրավական անվտանգություն, կիբեռանվտանգություն, տվյալների պաշտպանություն, տեխնոլոգիական կախվածություն:

Նախաբան

Ժամանակակից միջազգային հարաբերությունների և պետականության տեսության զարգացման համատեքստում ինքնիշխանության գաղափարը ենթարկվում է խորքային վերարժևորման: Եթե 20-րդ դարում պետության ինքնիշխանությունը հիմնականում գնահատվում էր տարածքային ամբողջականության, սահմանների անխախտելիության և արտաքին միջամտությունից պաշտպանվածության միջոցով, ապա 21-րդ դարում այն ստանում է բազմաչափ բնույթ՝ ընդգրկելով նաև թվային և տեղեկատվական ոլորտները:

Գիտատեխնիկական հեղափոխության և գլոբալիզացիոն գործընթացների խորացման արդյունքում ձևավորվում է նոր իրողություն, որտեղ տվյալների շրջանառությունը, տեղեկատվական հոսքերի վերահսկումը և տեխնոլոգիական ինքնաբավությունը դառնում են ոչ միայն տնտեսական մրցունակության, այլև քաղաքական անկախության և ազգային ինքնիշխանության հիմնարար բաղադրիչներ:

Այս իրողությունը հանգեցնում է իրավական նոր կատեգորիայի ձևավորմանը, այն է՝ **թվային ինքնիշխանությանը**, որը հանդես է գալիս որպես պետության ինքնիշխանության նորագույն ձևակերպում և ընդգրկում է միաժամանակ թե՛ տեխնոլոգիական, թե՛ սահմանադրաիրավական խնդիրների ամբողջություն:

Հայաստանի Հանրապետության համար թվային ինքնիշխանության հարցն ունի բացառիկ ռազմավարական նշանակություն: Մեր երկրի տեխնոլոգիական զարգացման ընթացքը, միջազգային համագործակցության ուղղությունները և տեղեկատվական միջավայրի անվտանգությունը փոխկապակցված են ազգային և սահմանադրաիրավական անվտանգության հիմնարար սկզբունքների հետ: Այս համատեքստում անհրաժեշտ է ձևավորել իրավաքաղաքական այնպիսի մոտեցումներ, որոնք կապահովեն թվային անկախության ամրապնդումը՝

միաժամանակ պահպանելով մարդու հիմնարար իրավունքների և տեղեկատվական ազատությունների հավասարակշռությունը:

«Թվային ինքնիշխանությունը» կարելի է սահմանել որպես պետության ինստիտուցիոնալ և իրավական կարողություն՝ ինքնուրույն ձևավորելու, տնօրինելու և պաշտպանելու սեփական թվային ենթակառուցվածքները, ինչպես նաև վերահսկելու տվյալների շրջանառությունն ու տեղեկատվական տարածքը: Այն ենթադրում է պետական իշխանության լիազորությունների իրացում թվային միջավայրում՝ առանց արտաքին կախվածության և միջամտության:

Այլ կերպ ասած, թվային ինքնիշխանությունը ներառում է իրավական, տեխնոլոգիական և կառավարչական գործիքակազմ, որի միջոցով պետությունը կարող է ապահովել իր տեղեկատվական միջավայրի ամբողջականությունը և կիբեռանվտանգությունը: Այն հանդիսանում է ազգային ինքնիշխանության անբաժանելի բաղադրիչ, քանի որ պետությունը, որը չի վերահսկում իր թվային ենթակառուցվածքներն ու տվյալային հոսքերը, աստիճանաբար կորցնում է նաև քաղաքական որոշումների ինքնուրույնությունը և պետականության իրական բովանդակությունը:

Այս առումով թվային ինքնիշխանությունը պետք է դիտարկվի ոչ թե որպես տեխնոլոգիական զարգացման առանձին ուղղություն, այլ՝ որպես պետական անկախության և ազգային անվտանգության հիմնարար չափում: Այն ձևավորում է նոր տեսակի ինքնիշխանություն, որի միջոցով պետությունը ոչ միայն պաշտպանում է իր թվային տարածքը, այլև երաշխավորում է սահմանադրական արժեքների պահպանությունն ու իշխանության ինքնուրույն իրացումը թվային դարաշրջանում:

1. <u>Սահմանադրաիրավական անվտանգության նշանակությունը</u>

Սահմանադրաիրավական անվտանգությունը պետության կայունության, իշխանության լեգիտիմության և պետական ինքնիշխանության իրացման հիմնասյուներից մեկն է: Այն արտահայտում է այնպիսի իրավական և ինստիտուցիոնալ պայմանների ամբողջություն, որոնք ապահովում են սահմանադրական կարգի, իշխանության բաժանման և պետական ինքնիշխանության պաշտպանությունը՝ ներառյալ նաև թվային միջավայրում:

Գլոբալ տեխնոլոգիական կախվածության խորացման պայմաններում սահմանադրական անվտանգությունը ենթարկվում է նոր՝ ոչ ավանդական սպառնալիքների: Դրանք կարող են դրսևորվել տարբեր ձևերով՝

- երբ պետական տվյալներն ու ռազմավարական տեղեկատվական ռեսուրսները պահվում են օտարերկրյա սերվերներում,
- երբ սոցիալական մեդիան դառնում է հանրային կարծիքի ձևավորման հիմնական գործիք՝ դուրս պետական վերահսկողությունից,
- կամ երբ արհեստական բանականության ալգորիթմները սկսում են ազդել ընտրական կամ քաղաքական գործընթացների վրա:

Այսպիսի զարգացումները կարող են հանգեցնել սահմանադրական ինքնիշխանության սահմանափակման՝ պետության որոշումների վրա արտաքին կամ տեխնոլոգիական ազդեցության ձևով:

Սահմանադրական ինքնիշխանությունը պետության իրավական գերակայությունն է իր տարածքում՝ հիմնված Սահմանադրության գերագույն իրավաբանական ուժի վրա, որը սահմանում է պետական իշխանության աղբյուրը, սահմանները և գործողության ձևը:

Այն արտահայտում է ժողովրդավարական պետության՝

- ինքնուրույն որոշումներ կայացնելու,
- իրավակարգ սահմանելու,
- պետական իշխանության ճյուղերի գործունեությունը կարգավորելու իրավունքը:

Հետևաբար, իրավական համակարգը պետք է ապահովի այնպիսի նորմատիվ և ինստիտուցիոնալ մեխանիզմներ, որոնք երաշխավորում են պետության՝ սեփական թվային քաղաքականությունը վարելու իրավունքը և տեխնոլոգիական անկախությունը՝ առանց մարդու հիմնարար իրավունքների և տեղեկատվական ազատությունների սահմանափակման:

Այս համատեքստում սահմանադրաիրավական անվտանգությունը վերածվում է ոչ միայն պետականության պահպանման գործիքի, այլև թվային ինքնիշխանության իրացման հիմնական երաշխիքի՝ ապահովելով իրավական համակարգի ադապտացիան նոր տեխնոլոգիական իրողություններին:

2. <u>Հետազոտական դեպք. Էդվարդ Սնոուդենն ու գլոբալ թվային վերահսկողությունը</u>

2013 թվականին ԱՄՆ Ազգային անվտանգության գործակալության (NSA) նախկին աշխատակից Էդվարդ Սնոուդենը հրապարակեց հսկայական ծավալի գաղտնի փաստաթղթեր, որոնք բացահայտում էին ԱՄՆ-ի և մի շարք դաշնակից երկրների իրականացրած զանգվածային գաղտնի հսկողության ծրագրերը: Այս բացահայտումները համարվում են ժամանակակից տեղեկատվական անվտանգության պատմության ամենահզոր իրադարձություններից մեկը:

Սնոուդենի հրապարակած փաստաթղթերը ընդգրկում էին տարբեր ծրագրեր՝

- **PRISM**՝ հնարավորություն էր տալիս NSA-ին անմիջական հասանելիություն ստանալ ամերիկյան խոշոր տեխնոլոգիական ընկերությունների՝ Google, Facebook, Apple, Microsoft սերվերներին՝ առանց օգտատերերի գիտության,
- **XKeyscore**՝ թույլ էր տալիս հավաքել և վերլուծել համաշխարհային ինտերնետային օգտատերերի առցանց գործունեության տվյալները,
- **TEMPORA**՝ Բրիտանական GCHQ-ի (Government Communications Headquarters, թարգմանաբար՝ Կառավարության հաղորդակցության գլխավոր գրասենյակ) ծրագիր, որը վերահսկում էր օվկիանոսային օպտիկական մալուխների ամբողջական տվյալահոսքը և փոխանցում ԱՄՆ-ին:

Այս ծրագրերի ծավալը և մեխանիզմները ցույց տվեցին, որ համաշխարհային ինտերնետային ենթակառուցվածքների զգալի մասը վերահսկելի է այն

պետությունների կողմից, որոնք տիրապետում են տվյալների հանգույցներին, սերվերներին և մալուխներին:

Էդվարդ Սնոուդենի բացահայտումները խոր ազդեցություն ունեցան՝

- միջազգային իրավունքի և մարդու իրավունքների ոլորտում,
- տվյալների պաշտպանության պրակտիկայում,
- ազգային թվային ինքնիշխանության ապահովման և գնահատման մոտեցումներում:

Գիտնականները նշում են, որ այս դեպքերը վկայում են այն մասին, որ տվյալների մեծածավալ կառավարման հնարավորությունը կարող է ծառայել որպես՝

- քաղաքական ազդեցության,
- տնտեսական վերահսկողության և
- ռազմական հետախուզության բարձրագույն գործիք,

և որ այդ բացահայտումները խորը ազդեցություն ունեցան միջազգային իրավունքի, մարդու իրավունքների, տվյալների պաշտպանության և ազգային ինքնիշխանության վերաբերյալ գիտական բանավեճերի վրա[1]:

Big Tech[2] ընկերությունների դերը ևս կարևոր է այս համատեքստում:

Google, Facebook, Apple, Microsoft և այլ խոշոր տեխնոլոգիական հարթակներ, որոնց սերվերներն օգտագործվել են տվյալների հավաքագրման համար, դարձել են գլոբալ թվային ենթակառուցվածքների վերահսկման հիմնական գործիքներ: Այս ընկերությունների միջոցով իրականացվող տվյալների հոսքերի վերահսկողությունը ազդեցություն է ունենում ոչ միայն օգտատերերի տվյալների գաղտնիության, այլև պետությունների թվային անկախության վրա:

«Big Brother Watch and Others v. the United Kingdom» գործը[3] վերաբերում է Միացյալ Թագավորության կողմից իրականացված **զանգվածային գաղտնալսման և ինտերնետային հաղորդակցությունների մեծածավալ հսկողության օրինականությանը:** Գանգատ ներկայացրած պետությունների, ակտիվիստների և լրագրողական կազմակերպությունների գնահատմամբ՝ Միացյալ Թագավորության (այսուհետ՝ ՄԹ) անվտանգության կառույցները (GCHQ) Սնոուդենի բացահայտումների հիման վրա գործարկում էին ծրագրեր, որոնք հնարավորություն էին տալիս՝

- իրականացնել ինտերնետային «երթևեկության» մոնիտորինգ ,
- իրականացնել մետատվյալների հավաքագրում,
- հավաքագրել հաղորդակցությունների բովանդակություններ՝

առանց անհատականացված թույլտվության և դատական վերահսկողության:

Քաղաքացիների իրավունքներով զբաղվող մի շարք կազմակերպություններ (ՄԻԵԴ դիմումները համարվում են համակցված՝ 58170/13, 62322/14, 24960/15) Մեծ

[1] *Տե՛ս* ***Greenwald, G.*** *(2014).* No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. *Metropolitan Books.*, ***Lyon, D.*** *(2015).* Surveillance after Snowden. *Polity Press:*

[2] *Տե՛ս https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/#google_vignette*

[3] *Տե՛ս European Court of Human Rights.* **Big Brother Watch and Others v. the United Kingdom,** *Applications nos. 58170/13, 62322/14, 24960/15 (Grand Chamber, May 25, 2021), https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}*

Պալատին էին դիմել այն պատճառաբանությամբ, որ նման լայնածավալ և ոչ թիրախավորված հսկողությունը խախտում է «Մարդու իրավունքների և հիմնական ազատությունների պաշտպանության մասին» կոնվենցիայով (հայտնի որպես Մարդու իրավունքների Եվրոպական կոնվենցիա (ՄԻԵԿ, անգլ. ECHR) նախատեսված ինչպես մասնավոր կյանքի (ՄԻԵԿ 8-րդ հոդված), այնպես էլ խոսքի ազատության (ՄԻԵԿ 10-րդ հոդված) իրավունքները[1]:

Դատարանի եզրակացությունը և իրավական տեսակետը հետևյալն էր՝

- Մեծ պալատը որոշեց, որ ՄԹ–ի զանգվածային հսկողության (bulk interception) ռեժիմը **խախտել է ՄԻԵԿ 8-րդ և 10-րդ հոդվածները:**
- Մասնավորապես՝ արձանագրվեց, որ տվյալ հսկողության **ռեժիմը չի ապահովել բավարար անկախ դատական/վերահսկողական երաշխիքներ,** բացակայում էր համապատասխան **end-to-end safeguards**՝ տվյալների հավաքագրումից մինչև վերլուծություն, պահպանում և ոչնչացում:
- Դատարանը նշեց, որ ցանկացած զանգվածային մոնիտորինգ պետք է լինի **օրինական, նպատակային, անհրաժեշտ և իրականացվի վերահսկողությամբ:**
- Վճիռն արձանագրվեց, որ պետությունների կողմից զանգվածային կոնտակտների գաղտնի մոնիտորինգը հնարավոր է միայն խիստ վերահսկվող և սահմանափակ պայմաններով[2]:

Մեծ պալատի վճիռը համարվում է պատմական՝ որպես առաջին ՄԻԵԴ որոշում, որն ուղղակիորեն սահմանափակում է զանգվածային մոնիտորինգի օրինականությունը և ամրապնդում է տվյալների անձնականության, խոսքի ազատության և մարդու իրավունքի պաշտպանությունը թվային միջավայրում:

Այսպիսով, վերոնշյալ գործը ցույց է տալիս, որ արտաքին հետախուզական համակարգերի կողմից իրականացվող զանգվածային տվյալահավաքը, ինչպես նաև Big Tech ընկերությունների հետ փոխազդեցության ոչ բավարար վերահսկումը կարող են էականորեն վտանգել ինչպես ազգային ինքնիշխանությունը, այնպես էլ մարդու հիմնարար իրավունքները: Եթե պետությունը չունի կանխատեսելի, իրավականորեն ամրագրված և ինստիտուցիոնալ առումով արդյունավետ վերահսկողական մեխանիզմներ, ապա տեղեկատվական միջավայրի նկատմամբ պետական ինքնավարությունը դառնում է խոցելի արտաքին ներգործությունների, տեխնոլոգիական կախվածությունների և անհամաչափ հսկողության ռեժիմների նկատմամբ:

Այս հետազոտական դեպքը հստակ ցույց է տալիս, որ թվային ինքնիշխանությունը՝ որպես ժամանակակից պետականության նորագույն չափում, չի կարող դիտարկվել միայն տեխնոլոգիական կամ տեխնիկական կարողությունների տեսանկյունից: Այն պահանջում է համադրած իրավական, ինստիտուցիոնալ և անվտանգային կառույցներ, որոնք կապահովեն պետության

[1] *Տե՛ս «Մարդու իրավունքների և հիմնական ազատությունների պաշտպանության մասին» կոնվենցիա, հոդված 8 և 10, https://www.arlis.am/hy/acts/192808*

[2] *Տե՛ս Grand Chamber confirms UK secret surveillance regime unlawful in Big Brother Watch v United Kingdom (Brick Court Chambers), https://www.brickcourt.co.uk/news/detail/grand-chamber-confirms-uk-secret-surveillance-regime-unlawful-in-big-brother-watch-v-united-kingdom*

ինքնուրույնությունը թվային միջավայրում, քաղաքացիների իրավունքների պաշտպանությունը և պետական տվյալների անվտանգ կառավարումը: Այդպիսով, թվային ինքնիշխանությունը դառնում է ոչ թե տեխնիկական ընտրություն, այլ սահմանադրաիրավական անհրաժեշտություն:

3. Հայաստանի Հանրապետության առջև ծառացած մարտահրավերները

Սնոուդենի դեպքը ցույց տվեց, որ ցանկացած երկիր, ինչպես օրինակ Հայաստանի Հանրապետությունը, որը չունի ազգային «ամպային» համակարգ և տվյալների պաշտպանված ենթակառուցվածք, փաստացի ռիսկի տակ է դնում իր պետական գաղտնիքները, քաղաքացիների տվյալները և սահմանադրական անվտանգությունը:

Հայաստանի Հանրապետությունը, գտնվելով գլոբալ տեխնոլոգիական գործընթացների անմիջական ազդեցության ներքո, կանգնած է թվային ինքնիշխանության ապահովման և պահպանման մի շարք համակարգային մարտահրավերների առջև: Այս մարտահրավերները պայմանավորված են ինչպես ներքին ինստիտուցիոնալ և իրավական անբավարարություններով, այնպես էլ արտաքին տեխնոլոգիական կախվածություններով, որոնք կարող են ազդել պետական ինքնիշխանության իրականացման վրա:

Առանձնացնենք երեք հիմնական ուղղություն.

1. Կիբեռանվտանգության ինստիտուցիոնալ և իրավական դաշտի թերի զարգացվածությունը

Չնայած վերջին տարիներին ձեռնարկված որոշակի քայլերին (օրինակ՝ 2020 թ.-ի ՀՀ Ազգային Անվտանգության ռազմավարությունում տեղ գտած 7.13 կետով նախատեսված է. «Տեղեկատվական, տեխնոլոգիական և կիբեռանվտանգության ապահովման ոլորտում մենք աշխատում ենք ինստիտուտների և գործընթացների արդյունավետության մակարդակի բարձրացման և ենթակառուցվածքների զարգացման ուղղությամբ: Հայաստանը հետամուտ է տեղեկատվական, տեխնոլոգիական և կիբեռանվտանգության պետական քաղաքականության և ռազմավարությունների մշակմանը, ինչպես նաև ոլորտի կառավարման համապետական մեխանիզմների ներդրմանը: Մենք զարգացնելու ենք կենսական նշանակության տեղեկատվական ենթակառուցվածքներ ու թվային ծառայություններ մատուցողների և պետության միջև փոխհարաբերությունների նորմատիվ-իրավական դաշտը, ինչի արդյունքում կձևավորվեն նաև կիբեռանվտանգության ազգային կենտրոն և համակարգչային պատահարների արձագանքման խմբեր»:[1])՝ Հայաստանի Հանրապետությունում դեռևս բացակայում է համապարփակ և համակարգված իրավական համակարգ, որը կապահովի պետական, ռազմավարական և մասնավոր թվային ենթակառուցվածքների լիարժեք պաշտպանությունը: Կիբեռանվտանգության ոլորտի բաշխված պատասխանատվությունը տարբեր կառույցների միջև երբեմն հանգեցնում է իրավական և

[1] *Տե՛ս ՀՀ Ազգային անվտանգության ռազմավարությունը, 2020 թ. հուլիս, էջ 31, https://www.sns.am/public/uploads/files/file-75elLZlT6j.pdf*

գործառնական հստակության պակասի, ինչը սահմանափակում է պետության կարողությունը՝ կանխարգելելու և կառավարելու կիբեռհարձակումներն ու տեղեկատվական սպառնալիքները:

Որպես օրինակ նշենք, որ **Էստոնիայի Հանրապետության «Կիբեռ գիտակից Էստոնիա» ռազմավարությունը**[1] ներկայացնում է թվային ինքնիշխանության իրականացման լավագույն միջազգային պրակտիկան՝ հիմնված պետական տվյալների լիարժեք տեղայնացման, կիբեռապահովության խիստ համակարգի, թվային ինքնության համընդհանուր մեխանիզմների և պետական-մասնավոր հատվածների սերտ համագործակցության վրա: Այն ցույց է տալիս, որ նույնիսկ փոքր պետությունները կարող են ձևավորել բարձր մակարդակի թվային ինքնիշխանություն՝ ապահովելով հստակ իրավական քաղաքականություն, կայուն ինստիտուցիոնալ համակարգ և տեխնոլոգիական ինքնաբավություն: Հայաստանի համար այս փորձը կարող է ծառայել որպես ռազմավարական ուղղություն՝ թվային ենթակառուցվածքների պաշտպանությունը, պետական տվյալների վերահսկողությունը և ազգային կիբեռանկայունությունը ապահովելու նպատակով:

2. Տվյալների պաշտպանության և գաղտնիության իրավական մեխանիզմների կատարելագործման անհրաժեշտությունը

Տվյալների պաշտպանության համակարգը Հայաստանում դեռևս գտնվում է զարգացման փուլում: Ակնհայտ է օրենսդրական դաշտի խորացման պահանջը՝ հատկապես այն ուղղությամբ, որը վերաբերում է պետական մարմինների, մասնավոր հատվածի և միջազգային հարթակների միջև տվյալների փոխանակման և պաշտպանության կանոնակարգմանը: Սա կարևոր է ոչ միայն անհատական տվյալների գաղտնիության ապահովման, այլև պետական ինստիտուտների նկատմամբ հանրային վստահության բարձրացման տեսանկյունից:

Որպես օրինակ ցանկանում ենք խոսել **2001 թ.-ին ընդունված «Կիբեռհանցագործության մասին Բուդապեշտի կոնվենցիա»-ի մասին**[2], որը կիբեռհանցագործությունների դեմ ուղղված առաջին միջազգային փաստաթուղթն է: Այն սահմանում է համակարգչային հանցագործությունների կատեգորիաներ, կիբեռհանցագործության քննության միջազգային համագործակցություն, ապացույցների պահպանման և փոխանակման ստանդարտներ: Այս փաստաթուղթը ՀՀ-ին թույլ կտա՝

- մասնակցել կիբեռհանցագործությունների դեմ համաշխարհային տեղեկատվական համագործակցությանը,
- ստանալ տեղեկատվություն այլ երկրներից,
- ապահովել սեփական թվային ենթակառուցվածքների պաշտպանությունը:

Հետևաբար Բուդապեշտի կոնվենցիան կարող է հանդիսանալ կարևոր հիմք ազգային կիբեռանվտանգության համակարգերի զարգացման համար, քանի որ այն ապահովում է կիբեռհանցագործությունների կանխարգելման և

[1] *Տե՛ս **Cyber-conscious Estonia (2024-2030)**, https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf*

[2] *Տե՛ս Budapest Convention on Cybercrime (2001), https://rm.coe.int/1680081561*

հետաքննության միասնական միջազգային մեխանիզմներ, որոնք խթանում են պետության թվային պաշտպանունակությունը:

3. Թվային ենթակառուցվածքների արտաքին կախվածության խնդիրը

Հայաստանի թվային միջավայրը զգալիորեն կախված է արտաքին տեխնոլոգիական մատակարարներից, օտարերկրյա հարթակներից և սերվերային ենթակառուցվածքներից: Այս կախվածությունը կարող է էականորեն սահմանափակել պետության վերահսկողությունը իր տեղեկատվական հոսքերի, տվյալների պահպանման և թվային գործընթացների նկատմամբ՝ առաջացնելով նաև սահմանադրաիրավական ինքնիշխանության հնարավոր խաթարման վտանգ:

Հայաստանի Հանրապետության համատեքստում Սնոուդենի բացահայտումները ընդգծում են ազգային թվային ենթակառուցվածքների ստեղծման և պաշտպանվածության կարևորությունը:

Որպես օրինակ նշենք, որ 2018 թվականին ԱՄՆ-ում ընդունվել է **Cloud Act** (Clarifying Lawful Overseas Use of Data Act)՝ նպատակ ունենալով հստակեցնել իրավական կարգավորումները, որոնք վերաբերում են արտերկրում պահվող տվյալների հասանելիությանը: Ակտի հիմնական դրույթները ընդգրկում են՝

1. ԱՄՆ-ի իրավապահ մարմինների իրավասությունը. Cloud Act-ը թույլ է տալիս ԱՄՆ-ի իրավապահ մարմիններին պահանջել ԱՄՆ-ում գրանցված տեխնոլոգիական ընկերություններից տվյալներ, նույնիսկ եթե այդ տվյալները գտնվում են արտասահմանյան սերվերներում[1]: Սա ներառում է էլեկտրոնային նամակներ, ամպային պահեստներում պահվող տվյալներ և այլ առցանց տեղեկատվություն:

2. Միջազգային իրավական համագործակցություն. ակտը թույլ է տալիս ԱՄՆ-ի կառավարությանը կնքել երկկողմ կամ բազմակողմ պայմանագրեր այլ երկրների հետ՝ հետաքննությունների և իրավապահ գործողությունների համար տվյալների փոխանակումը կարգավորելու նպատակով:

3. Ընկերությունների պաշտպանությունը. Cloud Act-ը տրամադրում է իրավական երաշխիքներ տեխնոլոգիական ընկերություններին, որպեսզի նրանք կարողանան տրամադրել տվյալներ ԱՄՆ-ի իրավապահներին:

Թվային ինքնիշխանության տեսանկյունից Cloud Act-ը առաջացնում է մի շարք մարտահրավերներ. նախ՝ այն կարող է սահմանափակել այն պետությունների իրավունքը, որոնք ցանկանում են վերահսկել իրենց քաղաքացիների տվյալները և ապահովել տվյալների տեղական անվտանգությունը: Եթե տվյալները գտնվում են արտասահմանում, ԱՄՆ-ի իրավապահների պահանջը կարող է գերակշռել ազգային օրենսդրությունը, ինչը միանշանակ ազդում է

[1] *Տե՛ս "Cloud Act and GDPR: What Implications for EU Companies' Data Protection?" LexisNexis International Legal Insights, June 20, 2025,*
https://www.lexisnexis.com/blogs/int-legal/b/insights/posts/cloud-act-gdpr-implications

տվյալների անվտանգության, պետական գաղտնիքների պաշտպանության և ազգային ինքնիշխանության վրա:

Cloud Act-ը նաև ընդգծում է այն փաստը, որ համաշխարհային թվային ենթակառուցվածքները գտնվում են բարձր մակարդակի միջազգային իրավական ու քաղաքական ազդեցության տակ, և ցանկացած պետություն, որը չունի սեփական վերահսկվող ամպային ենթակառուցվածք (cloud), փաստացի կախված է արտաքին իրավասություններից և տեխնոլոգիական ուժերից: Այս տեսանկյունից, Cloud Act-ը ծառայում է որպես ակնհայտ օրինակ այն մարտահրավերների, որոնց դիմակայելու համար Հայաստանի Հանրապետությունը պետք է զարգացնի ազգային թվային ենթակառուցվածք և ամրապնդի իրավական և ինստիտուցիոնալ մեխանիզմները իր թվային ինքնիշխանությունն ապահովելու համար:

Այս բոլոր գործոնները վկայում են, որ թվային անվտանգությունն ու թվային ինքնիշխանությունը պետք է դիտարկվեն Հայաստանի Հանրապետության ազգային և սահմանադրաիրավական անվտանգության համակարգի անբաժանելի բաղադրիչներ: Այս նպատակով անհրաժեշտ է ձևավորել ռազմավարական մոտեցում, որը կներառի իրավական, տեխնոլոգիական և ինստիտուցիոնալ բարեփոխումների համակցված քաղաքականություն՝ միտված պետական թվային ինքնիշխանության ամրապնդմանը և միջազգային տեխնոլոգիական կախվածությունների նվազեցմանը:

Եզրակացություն

21-րդ դարի գլոբալ զարգացումների համատեքստում պետության ինքնիշխանությունը վերաիմաստավորվում է՝ դուրս գալով իր դասական տարածքային և քաղաքական սահմաններից: Ժամանակակից աշխարհում ինքնիշխանության նոր չափում է ձևավորվում՝ **թվային ինքնիշխանությունը**, որը ներառում է պետության իրավունակությունը և կարողությունը՝ ինքնուրույն կերպով կարգավորելու, պաշտպանելու և տնօրինելու իր թվային միջավայրը, տվյալային հոսքերը և տեղեկատվական ենթակառուցվածքները:

Թվային ինքնիշխանությունը հանդիսանում է ազգային և սահմանադրաիրավական անվտանգության կարևորագույն բաղադրիչ, քանի որ այն ուղղակիորեն ազդում է պետական կառավարման ինքնուրույնության, տեղեկատվական անկախության և հանրային ինստիտուտների կայունության վրա: Այն պետությունները, որոնք չեն տիրապետում սեփական թվային ենթակառուցվածքների վերահսկողությանը կամ որոնց տեղեկատվական հոսքերը կախված են արտաքին կենտրոններից, փաստացիորեն կանգնում են սահմանադրական ինքնիշխանության սահմանափակման վտանգի առաջ:

Հայաստանի Հանրապետության համար թվային ինքնիշխանության ամրապնդումը ռազմավարական առաջնահերթություն է: Թեև վերջին տարիներին արձանագրվել են դրական միտումներ՝ կիբեռանվտանգության կառույցների ստեղծման, տվյալների պաշտպանության ոլորտի կարգավորման և թվային ենթակառուցվածքների զարգացման ուղղությամբ, այնուամենայնիվ առկա են մի շարք համակարգային խնդիրներ: Դրանք վերաբերում են համապարփակ

իրավական համակարգի բացակայությանը, տվյալների պաշտպանության ինստիտուտի թերի ձևավորմանը և արտաքին տեխնոլոգիական կախվածության բարձր աստիճանին:

Այս իրավիճակը պահանջում է ոչ միայն օրենսդրական բարեփոխումներ, այլև քաղաքական կամքի, ինստիտուցիոնալ համագործակցության և գիտատեխնիկական ներուժի համադրություն՝ թվային ինքնիշխանության ամրապնդման ուղղությամբ:

Թվային ինքնիշխանության ամրապնդման համար Հայաստանի Հանրապետությունը պետք է կիրառի հետևյալ ռազմավարական և պրակտիկ մոտեցումները.

1) <u>Համապարփակ պետական քաղաքականություն և ազգային թվային անվտանգության ռազմավարություն</u>

Անհրաժեշտ է մշակել և **ընդունել «ՀՀ ազգային թվային ինքնիշխանության ռազմավարություն»**, որը կներառի.

- կիբեռանվտանգության համապարփակ համակարգ,
- տվյալների պաշտպանության և անձնական տվյալների մշակման միասնական մոտեցումներ,
- պետական ամպային ենթակառուցվածքի ձևավորում,
- արտաքին տեխնոլոգիական կախվածության նվազեցման մեխանիզմներ,
- թվային կառավարման ստանդարտներ պետական մարմինների համար:

Ռազմավարությունը պետք է ունենա հստակ նպատակներ, ժամանակացույց, լիազոր մարմիններ և գնահատման ինդիկատորներ:

2) <u>Կիբեռանվտանգության միասնական կառավարման մոդելի ներդրում</u>

Առաջարկվում է ստեղծել ՀՀ Կիբեռանվտանգության ազգային կենտրոն, որը կունենա՝

- հատուկ պատրաստված մասնագիտական թիմ,
- պետություն–մասնավոր հատված համագործակցության համակարգ,
- կիրականացնի պարտադիր կիբեռանվտանգության աուդիտներ և ստուգումներ,
- կրիտիկական ենթակառուցվածքների պաշտպանություն (ռազմական, էներգետիկ, կապ, բանկային ոլորտներ):

Կենտրոնը պետք է գործի օրենսդրորեն ամրապնդված գործադիր լիազորություններով, այլ ոչ թե խորհրդատվական կարգավիճակով:

3) <u>Տվյալների պաշտպանության օրենսդրության բարեփոխում</u>

Հայաստանի Հանրապետությունը պետք է ներդնի՝

- GDPR-ի (Եվրոպական միության կողմից 2016 թ.-ին ընդունված «Տվյալների պաշտպանության հիմնական կանոնակարգի»[1]) պահանջներին համապատասխան ազգային օրենսդրության ձևավորման հստակ գործիքակազմ, որը լիովին հնարավոր է և հիմնավորված, քանի որ Հայաստանի Հանրապետության Սահմանադրությունն արդեն իսկ պարունակում է տվյալների

[10] *Տե՛ս General Data Protection Regulation (EU),https://gdpr-info.eu*

պաշտպանության և հաղորդակցության գաղտնիության հիմնարար սկզբունքների վերաբերյալ դրույթներ, որոնք համահունչ են եվրոպական ստանդարտներին. ՀՀ Սահմանադրության 33-րդ հոդվածը ապահովում է հաղորդակցության ազատությունն ու գաղտնիությունը՝ ընդգծելով, որ նամակագրության, հեռախոսազրույցների և հաղորդակցության այլ ձևերի գաղտնիությունը կարող է սահմանափակվել միայն օրենքով և միայն խիստ սահմանափակ դեպքերում, և այն, որ ՀՀ Սահմանադրության 34-րդ հոդվածը սահմանում է անձնական տվյալների պաշտպանության հիմնարար իրավունքները: Մասնավորապես՝ 34-րդ հոդվածը երաշխավորում է տվյալների պաշտպանության իրավունքը (տվյալների արդար և օրինական մշակում, անձի համաձայնության անհրաժեշտություն, տվյալների շտկման կամ վերացման իրավունք, ինչպես նաև հասանելիության սահմանափակումների իրավաչափ հիմքերը):[1]Այս սահմանադրական կարգավորումները լիովին համադրելի են GDPR-ի հիմնական դրույթների հետ և թույլ են տալիս օրենսդրական մակարդակում ներդնել եվրոպական ստանդարտներին համահունչ, առավել խիստ և արդյունավետ տվյալների պաշտպանության կարգավորումներ:

Այսպիսով, ՀՀ Սահմանադրության 33-րդ և 34-րդ հոդվածները հանդիսանում են GDPR-ին համահունչ տվյալների պաշտպանության ամբողջական օրենքի ընդունման ուժեղ իրավական հիմք, քանի որ կոնստիտուցիոնալ մակարդակում արդեն ամրագրված են այն սկզբունքները, որոնց վրա հիմնվում է եվրոպական տվյալների պաշտպանության համակարգը:

- պետական մարմինների տվյալների մշակման թափանցիկ մեխանիզմներ,
- պետական գաղտնիքներին առնչվող թվային տվյալների սահմանափակման նոր կարգ,
- պետական սեկտորի համար պարտադիր տվյալների տեղայնացման պահանջներ:

Պետք է վերաիմաստավորվի նաև Անձնական տվյալների պաշտպանության գործակալության դերը՝ այն վերածելով լիարժեք վերահսկող և անկախ կարգավորող մարմնի:

4) <u>Ազգային ամպային ենթակառուցվածքի (National Cloud) ստեղծում</u>

Որպես արտաքին կախվածության նվազեցման ամենակարևոր գործիք՝ Հայաստանի Հանրապետությունը պետք է ստեղծի.

- **պետական ամպային պլատֆորմ**, որտեղ կպահվեն
  - պետական տվյալները,
  - ռազմավարական և գաղտնի տեղեկատվությունը,
  - քաղաքացիների կենսաչափական տվյալները:

Պետական մարմինների համար անհրաժեշտ է սահմանել սահմանափակումներ՝ արգելելով ոչ անվտանգ և օտար իրավասության ներքո գործող առևտրային ամպային ծառայություններից օգտվելը (օր.՝ AWS, Microsoft Azure,

[1] *Տե՛ս ՀՀ Սահմանադրություն, հոդված 33 և 34,https://www.arlis.am/hy/acts/143723/latest*

Google Cloud)՝ բացառությամբ հատուկ համաձայնեցված անվտանգության ռեժիմների:

5) <u>Տեղական տեխնոլոգիական արդյունաբերության զարգացում</u>

Թվային ինքնիշխանության ամրապնդման կարևոր բաղադրիչ է ազգային տեխնոլոգիական ներուժի ընդլայնումը:

Անհրաժեշտ է.

- խթանել տեղական ծրագրային ապահովման, օպերացիոն համակարգերի, սերվերային լուծումների և կիբեռանվտանգության արտադրանքի ստեղծումը,
- պետական գնումների համակարգում ամրագրել «ազգային տեխնոլոգիական առաջնահերթություն» սկզբունքը,
- ապահովել հարկային և ֆինանսական խթաններ անվտանգային տեխնոլոգիաների ոլորտում գործող ընկերությունների համար:

6) <u>Սահմանադրաիրավական մակարդակում՝ թվային ինքնիշխանության ամրագրում</u>

Սահմանադրաիրավական մակարդակում նպատակահարմար է քննարկել թվային ինքնիշխանության սկզբունքի ներառումը ազգային անվտանգությանը և տեղեկատվական անվտանգությանը վերաբերող իրավական փաստաթղթերում՝ որպես պետական ինքնիշխանության բաղկացուցիչ տարր:

Դիտարկման արժանի են նաև հետևյալ սկզբունքները, որոնք կարելի է ներառել վերոնշյալ փաստաթղթերում՝

- պետական տվյալների տեղայնացում և պետական վերահսկողություն,
- ազգային թվային ենթակառուցվածքների պաշտպանություն,
- տեղեկատվական ինքնորոշման և տվյալների վերահսկողության իրավունք,
- թվային միջավայրում մարդու իրավունքների երաշխիքներ:

Այս մոտեցումը համահունչ է եվրոպական մի շարք պետությունների՝ Ֆրանսիայի, Գերմանիայի, Էստոնիայի թվային ինքնիշխանության ռազմավարություններին:

7) <u>Թվային իրավագիտակցության և մասնագիտական կարողությունների զարգացում</u>

Անհրաժեշտ է ներդնել և/կամ իրականացնել.

- պետական ծառայողների շարունակական վերապատրաստման ծրագրեր թվային իրավունքի և կիբեռանվտանգության ոլորտներում,
- դատական և իրավապահ մարմինների համար մասնագիտացված դասընթացներ,
- դպրոցական և բուհական կրթական ծրագրերում թվային իրավունք և տեղեկատվական անվտանգություն առարկաներ,
- լայնամասշտաբ հանրային իրազեկման արշավներ:

Հասարակության իրազեկվածությունը տեխնոլոգիական անվտանգության կարևորագույն օղակն է:

Այսպիսով, թվային ինքնիշխանությունը Հայաստանի Հանրապետության համար ոչ թե տեխնոլոգիական նորաձևություն է, այլ **պետականության շարունակականության, ազգային անվտանգության և ինքնիշխանության պար-**

տադիր պայման: Առանց ազգային թվային ենթակառուցվածքների, տվյալների պաշտպանության արդյունավետ մեխանիզմների, տեխնոլոգիական անկախության և բարձր իրավագիտակցության՝ պետությունը դառնում է արտաքին ուժերի, միջազգային տեխնոլոգիական կորպորացիաների և տեղեկատվական ազդեցությունների հանդեպ խոցելի:

Ուստի թվային ինքնիշխանությունը պետք է դիտարկվի որպես՝

- **ազգային անվտանգության անբաժանելի հատված,**
- **իրավաքաղաքական ռազմավարական ուղղություն,**
- **տեխնոլոգիական զարգացման հիմնասյուն,**
- **պետական կառավարման արդյունավետության նախապայման:**

Այն ապահովելու համար անհրաժեշտ է համալիր պետական քաղաքականություն, օրենսդրական ճշգրտումներ, ինստիտուցիոնալ ամրապնդում, տեխնոլոգիական արտադրության զարգացում և հանրային լայն մասնակցություն: Միայն այդ դեպքում Հայաստանի Հանրապետությունը կկարողանա լիարժեքորեն պաշտպանել սեփական ինքնիշխանությունը թվային դարաշրջանում և ձևավորել անվտանգ, անկախ և կայուն թվային միջավայր:

Օգտագործված նորմատիվ իրավական ակտերի, դատական ակտերի և գրականության ցանկ

1. ՀՀ Սահմանադրություն, 22.12.2015 թ.-ին ուժի մեջ մտած խմբագրությամբ:
2. Մարդու իրավունքների և հիմնարար ազատությունների պաշտպանության մասին կոնվենցիա (փոփոխված 11-րդ արձանագրությամբ):
3. ՀՀ Ազգային անվտանգության ռազմավարություն, 2020 թ.:
4. Council of Europe. Budapest Convention on Cybercrime, 2001.
5. European Union. General Data Protection Regulation (GDPR), 2016.
6. Cyber-conscious Estonia (2024-2030).
7. **Greenwald, G.** No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Metropolitan Books, 2014.
8. **Lyon, D.** (2015). Surveillance after Snowden. Polity Press.
9. European Court of Human Rights. *Big Brother Watch and Others v. the United Kingdom*, Applications nos. 58170/13, 62322/14, 24960/15 (Grand Chamber, May 25, 2021).

Էլեկտրոնային ռեսուրսներ

1. https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/#google_vignette
2. https://www.brickcourt.co.uk/news/detail/grand-chamber-confirms-uk-secret-surveillance-regime-unlawful-in-big-brother-watch-v-united-kingdom
3. https://www.lexisnexis.com/blogs/int-legal/b/insights/posts/cloud-act-gdpr-implications

ЦИФРОВОЙ СУВЕРЕНИТЕТ И КОНСТИТУЦИОННАЯ БЕЗОПАСНОСТЬ: ВЫЗОВЫ, СТОЯЩИЕ ПЕРЕД РЕСПУБЛИКОЙ АРМЕНИЯ В КОНТЕКСТЕ ГЛОБАЛЬНОГО ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ

Аннотация

В условиях современной глобализации и технологического прогресса классическое понимание государственного суверенитета претерпевает существенную трансформацию. Если ранее суверенитет ограничивался территориальной целостностью и политической независимостью, то в XXI веке он приобретает новое — цифровое измерение. Цифровой суверенитет становится правовой и институциональной способностью государства самостоятельно управлять, регулировать и защищать собственную цифровую инфраструктуру, потоки данных и информационную безопасность.

Для Республики Армения проблема цифрового суверенитета имеет стратегическое значение, поскольку информационная зависимость, недостаточный уровень кибербезопасности и пробелы в правовом регулировании защиты данных могут ограничивать осуществление конституционного суверенитета государства. С этой точки зрения цифровой суверенитет рассматривается не только как технологическая категория, но и как фундаментальный элемент конституционно-правовой безопасности.

Цель исследования - выявить взаимосвязь между цифровым суверенитетом и конституционно-правовой безопасностью, обозначив ключевые вызовы, с которыми сталкивается Республика Армения в условиях глобальной технологической среды. В работе выделены три основных направления: недостаточная развитость правовой системы

кибербезопасности, необходимость совершенствования механизмов защиты данных и риски внешней зависимости цифровой инфраструктуры.

В результате обосновывается необходимость включения цифрового суверенитета в число ключевых элементов национальной и конституционно-правовой безопасности. Для его обеспечения требуется разработка комплексной государственной стратегии, проведение законодательных и институциональных реформ, а также повышение уровня цифровой правовой грамотности на государственном и общественном уровнях.

Таким образом, цифровой суверенитет становится новой границей современной государственности — в сфере сочетания политической независимости, информационной защиты и конституционной стабильности.

Ключевые слова: цифровой суверенитет, конституционно-правовая безопасность, кибербезопасность, защита данных, технологическая зависимость.

DIGITAL SOVEREIGNTY AND CONSTITUTIONAL SECURITY: CHALLENGES FACING THE REPUBLIC OF ARMENIA IN THE CONTEXT OF GLOBAL TECHNOLOGICAL DEVELOPMENT

Annotation

In the context of contemporary globalization and rapid technological advancement, the classical concept of state sovereignty is undergoing substantial transformation. Whereas sovereignty was traditionally confined to territorial integrity and political independence, in the 21st century it has acquired a new dimension - digital sovereignty. **Digital sovereignty** reflects a state's legal and institutional capacity to autonomously govern, regulate, and protect its digitalinfrastructure, dataflows, and information security.

For the Republic of Armenia, the issue of digital sovereignty carries strategic significance, as informational dependence, an underdeveloped cybersecurity framework, and legal gaps in data protection may restrict the exercise of constitutional sovereignty. From this perspective, digital sovereignty is regarded not only as a technological category but also as a fundamental component of constitutional and legal security.

The purpose of this study is to examine the interrelation between digital sovereignty and constitutional security by identifying the key challenges Armenia

faces within the global technological environment. The research outlines three primary directions: the insufficient development of the cybersecurity legal system, the need to improve data protection mechanisms, and the risks associated with external dependence on digital infrastructure.

The study concludes that digital sovereignty must be incorporated into the core elements of national and constitutional security. Ensuring it requires the development of a comprehensive state strategy, the implementation of legislative and institutional reforms, and the enhancement of digital legal awareness at both governmental and societal levels.

Thus, digital sovereignty emerges as a new frontier of modern statehood - situated at the intersection of state independence, information protection, and constitutional stability.

Keywords: digital sovereignty, constitutional security, cybersecurity, data protection, technological dependence, national security.

Հոդվածը հանձնված է խմբագրություն 09.12.2025 թ., տրվել է գրախոսության 10.12.2025 թ., ընդունվել է տպագրության 15.12.2025 թ.: