



DOI: 10.59560/18291155-2025.3-89

**ՄԻՄՈՆ ՄԻՄՈՆՅԱՆ**

*Հայաստանում ֆրանսիական  
համալսարանի  
հեղափոխող դասախոս,  
իրավաբանական գիտությունների  
թեկնածու*

## **ՀԱՄԱՁԱՅՆՈՒԹՅԱՆ՝ ՈՐՊԵՍ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՄՇԱԿՄԱՆ ԻՐԱՎԱԿԱՆ ՀԻՄՔԻ ՎԱՎԵՐԱՊԱՅՄԱՆՆԵՐԸ**

### **Ամփոփագիր**

Անձնական տվյալներն իրապես համարվում են արդի թվային տնտեսության հիմնասյունը: Սակայն որպեսզի անձնական տվյալների մշակումը համարվի օրինական, այն, նախևառաջ, պետք է իրականացվի համապատասխան իրավական հիմքի հիման վրա: Տնտեսվարող սուբյեկտները, իրենց հաճախորդների անձնական տվյալները մշակելիս, որպես կանոն, հիմնվում են վերջիններիս համաձայնության վրա:

Սակայն խնդիրն այն է, որ ՀՀ-ում անձնական տվյալների պաշտպանության օրենսդրությունը հարաբերականորեն նոր է, իսկ օրենսդրական նորմերը հաճախ ձևակերպված են ոչ թե հստակ կարգադրագրերի, այլ ստանդարտների տեսքով: Արդյունքում տնտեսվարող սուբյեկտներն իրենց հաճախորդների անձնական տվյալները մշակում և դրա համար վերջիններիս համաձայնությունը ստանում են՝ ելնելով սեփական պատկերացումներից և ձեռնարկատիրական նկատառումներից, որի պարագայում ֆիզիկական անձանց իրավունքների և օրինական շահերի պաշտպանությունը դառնում է խնդրահարույց:

Հաշվի առնելով հիշյալ խնդիրները՝ սույն հոդվածը կոչված է ուսումնասիրելու համաձայնության՝ որպես անձնական տվյալներ մշակելու իրավական հիմքի վավերապայմանները՝ հիմնվելով ինչպես ՀՀ իրավակարգավորումների, դատական և իրավակիրառ պրակտիկայի, այնպես էլ՝ ոլորտում առկա լավագույն ստանդարտների, մասնավորապես՝ ԵՄ օրենսդրության և «փափուկ իրավունքի» վրա:

3(120)2025

◆ ՏԵՂԵԿԴՊԵՐ

◆ ՍԱՀՄԱՆԱԴՐԱԿԱՆ ԴԱՏԱՐԱՆ

**Հիմնաբառեր.** անձնական տվյալ, համաձայնություն, տվյալներ մշակող, տվյալների սուբյեկտ:

### ՆԵՐԱԾՈՒԹՅՈՒՆ

Թվայնացման արդի դարաշրջանում տնտեսությունը հիմնված է մեծածավալ տվյալների մշակման վրա, որոնց մաս են կազմում անձնական տվյալները: Անձի մասին մանրամասն տեղեկությունների մշակումը մի կողմից թույլ է տալիս ներկայացնել թիրախավորված գովազդներ, մատուցել անձի նախընտրություններից բխող ծառայություններ, մյուս կողմից, անհրաժեշտ է տնտեսվարող սուբյեկտների իրավունքներն ու շահերը պաշտպանելու համար: Մասնավորապես, անձնական տվյալների մշակումը թույլ է տալիս ստուգել անձի վարկարժանությունը, գնահատել վերջինիս կողմից պարտավորությունների կատարման հավանականությունը և այլն:

Հաշվի առնելով, որ անձի վերաբերյալ տեղեկությունների չհիմնավորված և ոչ թափանցիկ օգտագործումը կարող է հանգեցնել վերջինիս մասնավոր կյանքի անձեռնմխելիության իրավունքի խախտման, ինչպես նաև անձնական տվյալների նկատմամբ հսկողության կորստի, ժամանակակից իրավական համակարգերը որդեգրել են այն մոտեցումը, որ անձնական տվյալները կարող են մշակվել, եթե առկա է դա անելու համար համապատասխան իրավական հիմք: ՀՀ Սահմանադրության 34-րդ հոդվածով, մասնավորապես, ամրագրվեց, որ անձնական տվյալների մշակումը պետք է կատարվի բարեխղճորեն, օրենքով սահմանված նպատակով, **անձի համաձայնությամբ կամ առանց այդ համաձայնության՝ օրենքով սահմանված այլ իրավաչափ հիմքի առկայությամբ:**

Տնտեսվարող սուբյեկտների կողմից իրենց հաճախորդների անձնական տվյալները մշակելը, որպես կանոն, հիմնված է վերջիններիս համաձայնության վրա: Մասնավորապես, ապահովագրական պայմանագիր կնքելու, մարքեթինգային ծառայություններ մատուցելու, վարկ տրամադրելու նպատակով տնտեսվարող սուբյեկտները մշակում են անձանց կյանքի տարբեր ասպեկտների վերաբերյալ տեղեկություններ՝ ստանալով վերջիններիս համաձայնությունը: Սակայն խնդիրն այն է, որ երկրում անձնական տվյալների պաշտպանության օրենսդրությունը հարաբերականորեն նոր է, իսկ ոլորտում առկա «փափուկ իրավունքը» բավականաչափ ձևավորված չէ: Բացի այդ, անձնական տվյալների պաշտպանության օրենսդրական նորմերը հաճախ ձևակերպված են ոչ թե հստակ կարգադրագրերի, այլ ստանդարտների տեսքով: Արդյունքում ՀՀ-ում համաձայնությունը, որպես անձնական տվյալների մշակման հիմք, հաճախ կիրառվում է տնտեսվարող սուբյեկտի սեփական պատկերացումներից և ձեռ-

նարկատիրական նկատառումներից ելնելով, որի պարագայում ֆիզիկական անձանց իրավունքների և օրինական շահերի պաշտպանությունը մղվում է երկրորդական պլան:

Հաշվի առնելով հիշյալ խնդիրները՝ սույն հոդվածը կոչված է **ուսումնասիրելու համաձայնության՝ որպես անձնական տվյալներ մշակելու իրավական հիմքի վավերապայմանները՝** հիմնվելով ինչպես ՀՀ իրավակարգավորումների, դատական և իրավակիրառ պրակտիկայի, այնպես էլ՝ ոլորտում առկա լավագույն ստանդարտների, մասնավորապես՝ ԵՄ օրենսդրության և «փափուկ իրավունքի» վրա: Հոդվածի տեսական նշանակությունը տվյալներ մշակելու համաձայնության հատկանիշների, վերջինիս տրամադրելու առանձնահատկությունների վերաբերյալ իրավահամեմատական ուսումնասիրության իրականացումն է: Գործնական տեսանկյունից հոդվածում առկա եզրակացություններն ու վերլուծությունները կարող են ունենալ ուղեցուցային նշանակություն՝ տնտեսվարող սուբյեկտների կողմից անձնական տվյալները մշակելու համաձայնությունը ստանալու համար:

### Ընդհանուր դրույթներ

ՀՀ-ում անձնական տվյալների մշակման իրավական հիմքերը սահմանված են «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի (այսուհետ նաև՝ ԱՏՊ օրենք) 8-րդ հոդվածով, որի համաձայն՝ անձնական տվյալներ մշակելը օրինական է, եթե դրանք մշակվել են օրենքի պահանջների պահպանմամբ, և տվյալների սուբյեկտը տվել է իր համաձայնությունը, բացառությամբ սույն օրենքով կամ այլ օրենքներով ուղղակիորեն նախատեսված դեպքերի, կամ մշակվող տվյալները ձեռք են բերվել անձնական տվյալների հանրամատչելի աղբյուրներից: Վերոնշյալից բխում է, որ անձնական տվյալների մշակումը կբավարարի իրավական հիմքի պահանջը, եթե մշակումն իրականացվի կա՛մ **անձնական տվյալի սուբյեկտի համաձայնությամբ**, կա՛մ համաձայնության բացակայության դեպքում **մշակումը նախատեսված լինի օրենքով**, կա՛մ **մշակվող տվյալները ձեռք բերվեն անձնական տվյալների հանրամատչելի աղբյուրներից**:

Ինչպես նշվեց, անձնական տվյալների մշակման առաջին **հիմքը օրենքով նախատեսված լինելն է**: Վերջինս ենթադրում է, որ անձնական տվյալներ մշակելն օրինական է, եթե դա թույլատրված է օրենքով կամ էլ օրենքով սահմանված է անձնական տվյալներ մշակելու պարտավորություն: Օրինակ, «Բանկային գաղտնիքի մասին» ՀՀ օրենքի 14-րդ հոդվածի 1-ին մասը *թույլատրում է* բանկերին իրենց գործունեության անվտանգությունը, վարկերի և այլ

ներդրումների վերադարձելիությունը ապահովելու, ինչպես նաև փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի նպատակով այլ բանկերի հետ փոխանակել միմյանց հաճախորդների վերաբերյալ անձնական տվյալներ: «Փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մասին» ՀՀ օրենքի 17-րդ հոդվածով նախատեսված է հաճախորդի եկամուտների և ունեցվածքի աղբյուրի իսկության հարցում հավաստիանալու նպատակով վերջինիս *անձնական տվյալներ մշակելու պարտավորություն*:

Անձնական տվյալներ մշակելու մյուս իրավական հիմքը **մշակվող տվյալների հանրամատչելիությունն է**: Հիշյալ հիմքով անձնական տվյալներ կարող են մշակվել, օրինակ, մարքեթինգային կազմակերպությունների կողմից, երբ վերջիններս, ուսումնասիրելով անձանց վերաբերյալ համացանցում բաց հասանելիության ռեժիմի ներքո գտնվող տվյալները, ներկայացնում են թիրախավորված գովազդներ:

Սակայն այն դեպքերում, երբ տվյալների մշակումը սահմանված չէ օրենքով կամ եթե մշակվող տվյալները հանրամատչելի չեն, ապա տնտեսվարող սուբյեկտը պարտավոր է ստանալ անձի համաձայնությունը: Թեև ԱՏԴ օրենքը սահմանում է համաձայնության մեջ պարտադիր ներառման ենթակա տեղեկությունները, համաձայնությունը տալու ձևը, այնուամենայնիվ, վերջինս չի տալիս համաձայնության հասկացությունը, և ոչ էլ համապարփակ կերպով ներկայացնում է դրա վավերապայմանները: Համաձայնության հասկացությունը տրված է ԵՄ Անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգի (այսուհետ նաև՝ Կանոնակարգ կամ GDPR) նախաբանի 32-րդ կետով, որը սահմանում է, որ համաձայնությունը պետք է տրվի հստակ հաստատական գործողությամբ, որը հանդիսանում է տվյալների սուբյեկտի ազատ կամքով տրված, կոնկրետ (որոշակի), տեղեկացված և միանշանակ հավանությունը՝ իրեն վերաբերող անձնական տվյալները մշակելու համար: Նույնական մոտեցում է որդեգրվել «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» ԵԽ կոնվենցիան փոփոխող արձանագրության (այսուհետ՝ 108+ կոնվենցիա) 5-րդ հոդվածի 2-րդ կետով: Այսպիսով, GDPR-ով և 108+ կոնվենցիայով սահմանվել է, որ անձնական տվյալներ մշակելու համաձայնությունը պետք է լինի՝

- 1) միանշանակ՝ հստակ հաստատական գործողությամբ,
- 2) տվյալների սուբյեկտի ազատ կամքով տրված,
- 3) կոնկրետ (որոշակի),
- 4) տեղեկացված:

Սույն հոդվածը կոչված է բացահայտելու համաձայնության վերը թվարկված վավերապայմաններից յուրաքանչյուրը:

### 1. Համաձայնության միանշանակ լինելը

Անձնական տվյալներ մշակելու համաձայնությունը պետք է լինի միանշանակ: Անձնական տվյալների պաշտպանության գործակալության (այսուհետ՝ Գործակալություն) կողմից իրավակիրառ պրակտիկայի շրջանակներում ձևավորված դիրքորոշման համաձայն՝ միանշանակ տրված լինելու չափանիշից բխում է, որ սկզբունքորեն չկան սահմանափակումներ, թե համաձայնությունն ինչ ձևով պետք է վերցվի, սակայն այն պետք է հստակ արտացոլի տվյալների սուբյեկտի կամքը իր անձնական տվյալների մշակման վերաբերյալ: Սա նշանակում է, որ չպետք է որևէ կասկած մնա, որ տվյալների սուբյեկտի համաձայնությունն ուղղված է հենց անձնական տվյալների մշակմանը: Այլ կերպ ասած՝ տվյալների սուբյեկտի կամահայտնությունը, որով նա տալիս է իր հավանությունն անձնական տվյալների մշակման վերաբերյալ, պետք է միանշանակորեն վկայի տվյալների սուբյեկտի մտադրության վերաբերյալ, իսկ եթե կա տվյալների սուբյեկտի մտադրության վերաբերյալ ողջամիտ կասկած, ապա համաձայնությունը չի կարող համարվել միանշանակորեն տրված<sup>1</sup>: Այս դիրքորոշումն ամբողջությամբ արտացոլում է ԵՄ իրավունքում ձևավորված այն կանոնը, ըստ որի՝ համաձայնությունը պահանջում է տվյալների սուբյեկտի կողմից կատարած հայտարարություն կամ հստակ դրական գործողություն, ինչը նշանակում է, որ այն միշտ պետք է տրվի ակտիվ գործողության կամ հայտարարության միջոցով: Տվյալ իրավիճակից պետք է ակնհայտ լինի, որ տվյալների սուբյեկտը համաձայնություն է տվել իր տվյալները մշակելու համար<sup>2</sup>:

Համաձայնությունը տրամադրելու եղանակները թվարկված են ԱՏԴ օրենքի 9-րդ հոդվածի 7-րդ մասով, որից հետևում է, որ տվյալների սուբյեկտի համաձայնությունը տրվում է՝

1) գրավոր եղանակով. այսպիսի եղանակով համաձայնություն տալու օրինակ է տվյալներ մշակելու համաձայնագրի վրա ստորագրելը, որով տվյալների սուբյեկտը հավանություն է տալիս իր անձնական տվյալների մշակմանը.

2) էլեկտրոնային եղանակով՝ հաստատված էլեկտրոնային թվային ստորագրությամբ,

<sup>1</sup> Անձնական տվյալների պաշտպանության գործակալության որոշումը N-021/12/18 վարչական գործով:

<sup>2</sup> Guidelines 05/2020 on consent under Regulation 2016/679, 2020, p. 75.

3) բանավոր եղանակով՝ այնպիսի հավաստի գործողությունների միջոցով, որոնք ակնհայտորեն կվկայեն տվյալների սուբյեկտի՝ անձնական տվյալները օգտագործելու համաձայնության մասին: Որպես օրինակ կարող է ծառայել տվյալների սուբյեկտի կողմից տրված բանավոր համաձայնությունը, որը ձայնագրվել է տվյալներ մշակողի կողմից հեռախոսային խոսակցության ընթացքում<sup>1</sup>: Միանշանակ գործողություն է համարվում նաև համաձայնության համար անհրաժեշտ տեղեկությունները պարունակող «Գաղտնիության քաղաքականությանը» հավանություն տալը՝ համապատասխան վանդակի մեջ նշում կատարելու միջոցով<sup>2</sup>:

Միևնույն ժամանակ, համաձայնություն տալը չի կարող նույնացվել պայմանագիրը կամ դրա ընդհանուր պայմանները ստորագրելու հետ, քանի որ տվյալների սուբյեկտին հնարավորություն չի ընձեռվում ուղղակիորեն արտահայտել ոչ թե պայմանագիրը կամ դրա ընդհանուր պայմաններն ընդունելու, այլ իր անձնական տվյալները մշակելուն ուղղված համաձայնությունը: Հավասարապես միայն տվյալներ մշակողի ինտերնետային կայքն այցելելը չի կարող հավասարեցվել անձնական տվյալների մշակմանը համաձայնվելուն, քանի որ անձը տվյալ պարագայում միանշանակ եղանակով չի հայտնում իր կամքը՝ ընդունելու տվյալների մշակման պայմանները, այլ ընդամենը այցելում է ինտերնետային կայք<sup>3</sup>:

Վերը նշվածը վկայում է այն մասին, որ անձնական տվյալներ մշակելու համաձայնությունը պետք է տրվի ակտիվ և միանշանակ գործողությունների միջոցով: Միևնույն ժամանակ, ԵՄ իրավունքում ընդունված է, որ օրենսդրությամբ ուղղակիորեն սահմանված դեպքերում տվյալներ մշակողը կարող է չպահանջել տվյալների սուբյեկտի՝ դրական գործողությամբ տրվող համաձայնությունը, եթե վերջինս ի սկզբանե ունեցել է տվյալների մշակումն արգելելու հնարավորություն: Այսպես, «Էլեկտրոնային հաղորդակցության բնագավառում մասնավոր կյանքի և անձնական տվյալների պաշտպանության մասին» 2002/58/EC դիրեկտիվի 13-րդ հոդվածով սահմանված է, որ մարքեթինգային նպատակներով անձնական տվյալներ մշակելիս տվյալներ մշակողը կարող է չստանալ հաճախորդի ակտիվ գործողությամբ տրվող համաձայնությունը, եթե մինչև հաճախորդի հետ գործարար հարաբերություններ սկսելը տվյալներ մշակողը հաճախորդին ընձեռել է մարքեթինգային նպատակներով անձնական

<sup>1</sup> Guidelines 05/2020 on consent under Regulation 2016/679, 2020, p. 79.

<sup>2</sup> Անձնական տվյալների պաշտպանության գործակալության որոշումը N-021/12/18 վարչական գործով:

<sup>3</sup> Անձնական տվյալների պաշտպանության գործակալության որոշումը N-040/08/23 վարչական գործով:

տվյալներ մշակելն արգելելու պարզ և մատչելի հնարավորություն, պայմանով, որ այդ նպատակներով անձնական տվյալների մշակումը վերաբերելու է բացառապես տվյալներ մշակողի կողմից մատուցվող ծառայություններին, և հաճախորդը չի օգտվել այդ նպատակներով անձնական տվյալներ մշակելն արգելելու հնարավորությունից: Նշվածից հետևում է, որ Դիրեկտիվը նախատեսել է տվյալներ մշակողի կողմից մատուցվող ծառայություններ առաջարկելու նպատակով հաճախորդների անձնական տվյալները մշակելու համաձայնությունը ստանալու երկու եղանակ՝ opt-in, երբ հաճախորդը համաձայնություն է տալիս ակտիվ գործողությամբ, և opt-out, երբ հաճախորդի համաձայնությունը համարվում է տրված, քանի դեռ վերջինս չի արգելել իր անձնական տվյալների մշակումը՝ առանց ակտիվ գործողություններ կատարելու անհրաժեշտության:

ՀՀ օրենսդրության վերլուծությունը ցույց է տալիս, որ ՀՀ-ում նախատեսված չէ opt-out եղանակով համաձայնություն տալու հնարավորությունը: ԱՏՊ օրենքով սահմանված՝ համաձայնության տրամադրման եղանակների ցանկը վկայում է այն մասին, որ ՀՀ իրավունքում համաձայնությունն ընկալվում է որպես բացառապես ակտիվ գործողությամբ արտահայտվող կամահայտնություն:

## **2. Համաձայնության՝ տվյալների սուբյեկտի ազատ կամքով տրված լինելը**

### **2.1. Համաձայնության՝ տվյալների սուբյեկտի ազատ կամքով տրված լինելու չափանիշները**

Համաձայնության՝ «ազատ կամքով» տրված լինելու վավերապայմանը ենթադրում է տվյալների սուբյեկտի համար վերջինիս անձնական տվյալները մշակելը թույլատրելու իրական ընտրության հնարավորություն: Ըստ Վճռաբեկ դատարանի դիրքորոշման՝ համաձայնությունը կամային ակտ է, և պետք է տրված լինի տվյալների սուբյեկտի «իրական ընտրությամբ (ազատ, կամավոր որոշմամբ), առանց խաբեության, սպառնալիքի, հարկադրանքի կամ համաձայնություն չտալու դեպքում իր համար բացասական հետևանքի»<sup>1</sup>: GDPR-ը սահմանում է, որ եթե տվյալների սուբյեկտն իրական ընտրություն չունի, ստիպված է տալիս իր համաձայնությունը կամ համաձայնությունը չտալու դեպքում կկրի բացասական հետևանքներ, ապա համաձայնությունը չի համարվի վավեր<sup>2</sup>:

<sup>1</sup> Տե՛ս ՀՀ Վճռաբեկ դատարան քաղաքացիական գործ թիվ ԵԴ/25649/02/20; ՀՀ Վճռաբեկ դատարան քաղաքացիական գործ թիվ ԵԴ/5278/02/19:

<sup>2</sup> Opinion 15/2011 on the definition of consent (WP187), 2011, p. 12.

Համաձայնության ազատ տրված լինելը նաև ենթադրում է, որ արգելվում է տվյալների սուբյեկտի համաձայնությունը ստանալու նպատակով տվյալների սուբյեկտի փոխարեն նախապես ընտրություն կատարելը: Օրինակ՝ տնտեսվարող սուբյեկտները հաճախ ինտերնետային կայքում կամ ծրագրային հավելվածում համաձայնություն տալու համար նախատեսված վանդակում տվյալների սուբյեկտի փոխարեն կատարում են նշում, իսկ համաձայնությունը տալու վահանակն ակտիվացնում է տվյալների սուբյեկտը: Նույնիսկ եթե տվյալների սուբյեկտին տրված է իր տվյալները մշակելու համաձայնությունը չտալու հնարավորություն (օրինակ՝ վանդակում կատարած նշումն ապահովող հնարավորություն), ապա այնուամենայնիվ համաձայնությունը չի կարող համարվել ազատորեն տրված, քանի որ տվյալներ մշակողն արդեն իսկ ընտրություն է կատարել անձի փոխարեն:

Համաձայնության ազատ տրված լինելու վավերապայմանի պահպանման անհրաժեշտությունը հատկապես կարևորվում է այն իրավիճակներում, երբ անձնական տվյալները մշակվում են մի քանի նպատակներով, որոնցից ոչ բոլորն են անհրաժեշտ տնտեսվարող սուբյեկտի՝ պայմանագրից բխող իրավունքներն ու օրինական շահերը պաշտպանելու համար: Օրինակ՝ հաճախորդի տվյալները կարող են մշակվել ինչպես նրա ֆինանսական վիճակը գնահատելու, այնպես էլ՝ վերջինիս նախասիրությունների հիման վրա այլ ծառայություն առաջարկելու, այսինքն՝ մարքեթինգային նպատակով: Այս դեպքում տվյալներ մշակողը պետք է ապահովի, որ տվյալների սուբյեկտը հնարավորություն ունենա համաձայնություն տալու/չտալու վերը նշված համաձայնություններից յուրաքանչյուրին և զերծ մնա անուղղակի եղանակով տվյալների սուբյեկտի ընտրությունը սահմանափակելուց<sup>1</sup>: Հակառակ դեպքում, եթե անձը զրկված է այն հնարավորությունից, ապա համաձայնությունը չի համարվի ազատ տրված:

Համաձայնության ազատ տրված լինելու վավերապայմանը ենթադրում է նաև համաձայնությունը ցանկացած պահի հետ կանչելու հնարավորություն<sup>2</sup>: Ավելին, եթե տվյալներ մշակողը ստացել է անձի համաձայնությունը մի քանի նպատակներով անձնական տվյալներ մշակելու համար, ապա պետք է ապահովի ինչպես դրանց յուրաքանչյուրին համաձայնելու, այնպես էլ տրված համաձայնությունը հետ կանչելու հնարավորություն: Օրինակ, քննարկվող օրինակում համաձայնությունը կհամարվի ազատորեն տրված, եթե

<sup>1</sup> Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին ԵԵՄ կոնվենցիայի պաշտոնական պարզաբանումներ, 2018, կետ 42:

<sup>2</sup> Տե՛ս նույն տեղում:



հաճախորդն ունենա ինչպես ֆինանսական վիճակը գնահատելու, այնպես էլ՝ վերջինիս նախասիրությունների հիման վրա այլ ծառայություն առաջարկելու, այսինքն՝ մարքեթինգային նպատակով անձնական տվյալներ մշակելու արդեն իսկ տրված համաձայնությունը հետ կանչելու իրական հնարավորություն:

## **2.2. Համաձայնության՝ տվյալների սուբյեկտի ազատ կամքով տրված լինելու պահանջի սահմանափակումները ՀՀ իրավունքում**

Ինչպես նշվեց, անձնական տվյալներ մշակելու համաձայնությունը համարվում է ազատորեն տրված, եթե տվյալների սուբյեկտն ունի իր անձնական տվյալները մշակելը թույլատրելու/չթույլատրելու իրական ընտրության հնարավորություն, իսկ նման համաձայնություն չտալու դեպքում վերջինս չի կրի իր համար անբարենպաստ բացասական հետևանքներ: Համաձայնության հիշյալ վավերապայմանի պահպանումը հատկապես խնդրահարույց է ֆինանսական ծառայությունների դեպքում. ֆինանսական կազմակերպությունները, իրենց իրավունքների և օրինական շահերի պաշտպանությունից ելնելով, հաճախ ստանում են հաճախորդների անձնական տվյալները մշակելու թույլտվություն: Օրինակ՝ բանկերը և վարկային կազմակերպությունները, վարկի մոնիթորինգի, այսինքն, վարկառուի կողմից իր պարտավորությունները կատարելու և դրա հավանականությունը ստուգելու նպատակով կատարում են հարցումներ վարկային բյուրոյին: Ընդ որում, «Վարկային տեղեկատվության շրջանառության և վարկային բյուրոների գործունեության մասին» ՀՀ օրենքի 16-րդ հոդվածի 1-ին մասը սահմանում է, որ վարկային զեկույցների և վարկային տեղեկատվության սուբյեկտին նույնականացնող տվյալներ պարունակող այլ ծառայությունների ստացումը վարկային բյուրոյից իրականացվում է վարկային տեղեկատվության սուբյեկտի գրավոր (այդ թվում՝ էլեկտրոնային) համաձայնությամբ: Սակայն նման համաձայնություն չտրամադրելու դեպքում ֆինանսական կազմակերպությունները հրաժարվում են հաճախորդներին տրամադրել վարկեր, քանի որ չեն կարող վերահսկել վարկային պայմանագրից բխող պարտավորությունների կատարումը, ինչպես նաև գնահատել անձի վարկարժանությունը: Ստացվում է, որ որոշ դեպքերում համաձայնություն տրամադրելը կրում է պարտադիր բնույթ, քանի որ առանց դրա առհասարակ չեն առաջանում պայմանագրային հարաբերություններ տվյալներ մշակողի, այսինքն՝ ֆինանսական կազմակերպության, և տվյալների սուբյեկտի, այսինքն՝ հնարավոր հաճախորդի միջև:

Քննարկվող առանձնահատկությունը պայմանավորված է այն հանգամանքով, որ ԱՏՊ օրենքը, ինչպես նշեցինք, սահմանում է անձնական տվյալներ

մշակելու ընդամենը երեք հիմք. տվյալներ մշակողը կարող է առանց տվյալների սուբյեկտի համաձայնության մշակել վերջինիս անձնական տվյալները, եթե դա նախատեսված կամ թույլատրված է օրենքով կամ էլ մշակվող տվյալները հանրամատչելի են: Ստացվում է, որ անձնական տվյալներ մշակելու իրավական հիմքն ապահովելու նպատակով տնտեսվարող սուբյեկտներն ապավինում են համաձայնությանը՝ չունենալով տվյալներ մշակելու այլ իրավական հիմքեր:

Հատկանշական է, որ ԵՄ իրավունքում նախատեսված են անձնական տվյալներ մշակելու այլ իրավական հիմքեր ևս: Մասնավորապես, GDPR-ի 6-րդ հոդվածի 1-ին մասի b կետով սահմանվում է, որ տվյալներ մշակողը կարող է մշակել այն անձնական տվյալները, որոնք անհրաժեշտ են տվյալների սուբյեկտի հետ կնքված պայմանագիրը կատարելու համար: Միևնույն իրավադրույթի f կետի համաձայն՝ տվյալներ մշակելն օրինական է, եթե դա անհրաժեշտ է տվյալներ մշակողի կամ երրորդ անձի օրինական շահերը պաշտպանելու նպատակով, եթե չեն խախտվում տվյալների սուբյեկտի իրավունքները<sup>1</sup>: Հետևաբար, քննարկվող օրինակում, երբ ֆինանսական կազմակերպությունն իրականացնում է վարկային հարցումներ վարկի մոնիթորինգի նպատակով, ապա այդ իրավիճակին համապատասխանում են GDPR-ի՝ վերը հիշատակված իրավական հիմքերը, մինչդեռ տվյալների սուբյեկտի համաձայնության հիման վրա անձնական տվյալները կարող են մշակվել այն դեպքերում, երբ տվյալներ մշակողը կարող է պաշտպանել իր իրավունքներն ու օրինական շահերը առանց անձի համաձայնության:

Վերը հիշատակված փաստարկները վերաբերելի են նաև անձնական տվյալներ մշակելու համաձայնությունը հետ կանչելու դեպքերին: Մասնավորապես, ԱՏՊ օրենքի 9-րդ հոդվածի 3-րդ մասը սահմանում է, որ տվյալների սուբյեկտն իրավունք ունի հետ կանչելու իր համաձայնությունը սույն օրենքով, ինչպես նաև այլ օրենքներով նախատեսված դեպքերում և կարգով: Խորհրդի ուղեցուցային կանոնները նախատեսում են, որ համաձայնությունը համարվում է ազատորեն տրված, եթե հնարավոր է այն յուրաքանչյուր պահի հետ կանչել՝ առանց տվյալների սուբյեկտի համար բացասական հետևանքների<sup>2</sup>: Մինչդեռ եթե փորձենք կիրառել հիշյալ նորմը

<sup>1</sup> Հիշյալ կետով, մասնավորապես, սահմանված է, որ տվյալներ մշակելն ունի համապատասխան իրավական հիմք, եթե դա անհրաժեշտ է տվյալներ մշակողի կամ երրորդ անձի օրինական շահերը պաշտպանելու նպատակով, բացառությամբ այն դեպքերի, երբ տվյալների սուբյեկտի շահերը կամ իրավունքներն ու հիմնարար ազատությունները գերակայում են այդ անձանց իրավունքների և շահերի նկատմամբ:

<sup>2</sup> Guidelines 05/2020 on consent under Regulation 2016/679, 2020, p. 46.

հայաստանյան իրականությունում, կստացվի հետևյալ իրավիճակը. տնտեսվարող սուբյեկտը ստանում է իր հաճախորդի համաձայնությունը պայմանագրից բխող պարտավորությունները կատարելու և հաճախորդի կողմից նրա պարտավորությունները չկատարելու դեպքում իր իրավունքներն ու օրինական շահերը պաշտպանելու նպատակով (օրինակ՝ պարտքի հավաքագրման, վարկի մոնիթորինգի), սակայն հաճախորդը պայմանագրային հարաբերությունների ընթացքում հետ է կանչում իր համաձայնությունը՝ օգտվելով ԱՏՊ օրենքով ընձեռված հնարավորությունից: Իրավունքի նորմերի տառացի մեկնաբանությունը կհանգեցնի մի թյուր իրավիճակի, որի պարագայում տվյալներ մշակողի իրավունքների և օրինական շահերի պաշտպանությունը կախվածության մեջ է դրվում տվյալների սուբյեկտի հայեցողությունից: Մինչդեռ տվյալ դեպքում տվյալների մշակմանը նույնպես համապատասխանում են GDPR-ի 6-րդ հոդվածի 1-ին մասի b և f կետով սահմանված իրավական հիմքերը, որոնց պարագայում անհրաժեշտ չէ ստանալ տվյալների սուբյեկտի համաձայնությունը:

Բերված օրինակները վկայում են այն իրողության մասին, որ ՀՀ օրենսդրությամբ նախատեսված անձնական տվյալները մշակելու իրավական հիմքերը սահմանափակ են և չեն համապատասխանում առկա հասարակական և տնտեսական պահանջներին, որի պայմաններում համաձայնությունը, լինելով դիսպոզիտիվ բնույթի ակտ, երբեմն կրում է պարտադիր, այսինքն՝ իմպերատիվ բնույթ: Մասնավորապես, համաձայնություն տալը կարող է համարվել պարտադիր պայման տվյալներ մշակողի կողմից մատուցվող ծառայությունից օգտվելու համար, եթե դա օբյեկտիվորեն անհրաժեշտ է հաճախորդի հետ պայմանագրի կնքելու, պայմանագրով նախատեսված պարտավորությունները կատարելու համար (օրինակ՝ վարկ տրամադրելու և գործող վարկի մոնիթորինգի նպատակներով վարկային բյուրո հարցումներ կատարելը):

Ինչ վերաբերում է համաձայնությունը հետ կանչելուն, ապա ԱՏՊ օրենքով գործող իրավական հիմքերի առկայության պայմաններում տվյալներ մշակողը պետք է հնարավորություն ունենա մերժել անձնական տվյալներ մշակելու համաձայնությունը հետ կանչելու դիմումը, եթե օրինակ, հաճախորդի անձնական տվյալներ մշակելն անհրաժեշտ է հաճախորդի և տվյալներ մշակողի միջև կնքված պայմանագրից բխող պարտավորությունները կատարելու համար, կամ առանց հաճախորդի անձնական տվյալները մշակելու տվյալներ մշակողը չի կարող իրականացնել հաճախորդի հետ հարաբերություններում իր իրավունքների և օրինական շահերի պաշտպանությունը,

այդ թվում նաև այն ժամանակ, երբ հաճախորդն ունի չկատարած պարտավորություններ տվյալներ մշակողի նկատմամբ: Այնուամենայնիվ, առաջացած խնդիրների երկարաժամկետ լուծումը ենթադրում է ԱՏՊ օրենքով վերանայել անձնական տվյալներ մշակելու իրավական հիմքերի շրջանակը:

### 3. Համաձայնության որոշակի լինելը

Համաձայնության որոշակի լինելու չափանիշը մեկնաբանվել է Վճռաբեկ դատարանի կողմից: Այսպես, «որոշակի» լինելու չափանիշը վերաբերում է ինչպես փոխանցման ենթակա անձնական տվյալների, այնպես էլ՝ այն նպատակների հստակ սահմանմանը, ի իրագործումն որոնց՝ պետք է մշակվեն այդ անձնական տվյալները: Այսինքն՝ համաձայնությունից պետք է հստակ լինի և՛ մշակման ենթակա անձնական տվյալների ցանկը, և՛ դրանց մշակման նպատակների շրջանակը<sup>1</sup>: Սույն վերլուծությունը բխում է ԱՏՊ օրենքի 10-րդ հոդվածի 2-րդ մասի բովանդակությունից, որից հետևում է, որ տվյալների սուբյեկտի համար, իր համաձայնությունը տալիս, պետք է ակնհայտ լինեն անձնական տվյալների մշակման նպատակները, ինչպես նաև մշակման ենթակա անձնական տվյալների ցանկը:

Համաձայնության որոշակի լինելու պահանջի չափապանման հետևանքներն ակներև են հատկապես ապահովագրական ոլորտում: Այսպես, Հայաստանի ավտոապահովագրողների բյուրոյի RL 1-001 (ԱՊՊԱ ընդհանուր պայմաններ) կանոնների 17-րդ կետով սահմանված է, որ ԱՊՊԱ պայմանագրի կնքմամբ ապահովադիրները թույլատրում են ապահովագրողներին և Ավտոապահովագրողների բյուրոյին ինչպես տվյալ պայմանագրի կնքման և գործողության ընթացքում, այնպես էլ պայմանագրի գործողության ավարտից հետո միմյանց միջև կամ երրորդ անձանց հետ ցանկացած եղանակով և կրիչի վրա շրջանառել (ստանալ և տրամադրել) իրենց վերաբերյալ ցանկացած փաստաթուղթ, տեղեկություն, տեսանյութ, լուսանկար կամ այլ նյութ՝ ԱՊՊԱ պայմանագրում անհրաժեշտ տվյալների արտացոլման կամ արտացոլված տեղեկությունների ստուգման, ԱՊՊԱ պատահարի և դրա գծով իրականացվող հատուցման գործընթացի կարգավորման՝ ներառյալ փորձաքննությունների իրականացման, ինչպես նաև հատուցման վճարմամբ պայմանավորված հետադարձ պահանջի իրավունքի արդյունավետ իրականացման և ԱՊՊԱ ոլորտում անհրաժեշտ այլ գործողություններ իրականացնելու համար: Բերված օրինակում նկատելի է համաձայնության որոշակիության պահանջի միաժամանակ երկու խախտում. նախ,

<sup>1</sup> Վճռաբեկ դատարանի որոշումը թիվ ԵԴ/25649/02/20 քաղաքացիական գործով:

ապահովադիրների, այսինքն՝ տվյալների սուբյեկտների համար հիշյալ թույլտվությունը, այսինքն՝ տվյալներ մշակելու համաձայնությունը տրամադրելիս, պարզ չէ, թե որոնք են լինելու մշակվող անձնական տվյալները, քանի որ ապահովագրողները և բյուրոն, որպես տվյալներ մշակողներ, կարող են մշակել նրանց վերաբերյալ ցանկացած տեսակի անձնական տվյալ. *այնուհետև*, ապահովագրողները և բյուրոն նախապես չեն սահմանել ապահովադիրների անձնական տվյալները մշակելու բոլոր նպատակները, քանի որ ըստ հիշյալ կանոնի՝ տվյալները կարող են օգտագործվել ԱՊՊԱ ոլորտում անհրաժեշտ այլ գործողություններ իրականացնելու համար: Նման դեպքում տվյալների սուբյեկտները կորցնում են իրենց անձնական տվյալների մշակման նկատմամբ հսկողությունը, իսկ նպատակների և մշակվող տվյալների անսահմանափակ լինելը կարող է խնդրահարույց լինել անձնական տվյալների մշակման սկզբունքների պահպանման տեսանկյունից: Այսպես, նախ, խախտվում է ԱՏՊ օրենքի 4-րդ հոդվածով ամրագրված տվյալների մշակման օրինականության սկզբունքը, ըստ որի՝ անձնական տվյալները մշակվում են օրինական և որոշակի նպատակներով և առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով, քանի որ «ԱՊՊԱ ոլորտում անհրաժեշտ այլ գործողություններ իրականացնելու համար» ձևակերպումն իր բովանդակությամբ որոշակի չէ: Նման ձևակերպումը խնդրահարույց է նաև տվյալների մշակման համաչափության սկզբունքի տեսանկյունից, որի համաձայն՝ տվյալների մշակումը պետք է հետապնդի օրինական նպատակ, իսկ դրան հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ և չափավոր<sup>1</sup>: Խնդիրն այն է, որ քննարկվող օրինակում պարզ չեն տվյալների մշակման բոլոր նպատակները, ինչպես նաև դրանց հասնելու համար օգտագործվող միջոցները, հետևաբար դրանց համաչափությունը ստուգելն առհասարակ անհնարին է:

Համաձայնության որոշակի լինելու քննարկված կանոններն ընդունված են նաև ԵՄ իրավունքում: Միևնույն ժամանակ, GDPR-ով նախատեսված են համաձայնության որոշակիության առավել խիստ պահանջներ: Մասնավորապես, Անձնական տվյալների պաշտպանության եվրոպական խորհուրդը (անգլ.<sup>1</sup> European data protection board, այսուհետ՝ Խորհուրդ), մեկնաբանելով GDPR-ի 7-րդ հոդվածը, եկել է այն եզրակացության, որ համաձայնության որոշակիությունը ենթադրում է, որ տվյալների սուբյեկտի համար պետք է

<sup>1</sup> Համաչափության սկզբունքը սահմանված է ԱՏՊ օրենքի 5-րդ հոդվածով, ինչպես նաև GDPR-ի 5-րդ հոդվածի 1-ին մասի c կետով:

պարզ լինի, թե որ անձնական տվյալը որ նպատակի կամ նպատակների իրագործման համար է մշակվում<sup>1</sup>: Այսինքն, տնտեսվարող սուբյեկտները չեն կարող պարզապես տվյալներ մշակելու համաձայնագրերի մեջ նշել մշակվող տվյալների և դրանց նպատակների սպառիչ ցանկ, այլ նաև պետք է պարզ և մատչելի ձևով ներկայացնեն, թե որ տվյալը որ նպատակի իրագործման համար է մշակվում: Հիշյալ պահանջը վերաբերում է նաև անձնական տվյալները մշակելու ժամկետին: ԱՏՊ օրենքի 10-րդ հոդվածի 2-րդ մասում նշված է, որ տվյալների մշակման համաձայնագիրը պետք է պարունակի համաձայնության գործողության ժամկետը: Նման կարգավորումից բխում է, որ տվյալներ մշակողը պետք է սահմանի մեկ միասնական ժամկետ, մինչդեռ անձնական տվյալները, կախված նպատակից, կարող են մշակվել տարբեր ժամկետներով: Գտնում ենք, որ հիշյալ իրավադրույթը պետք է սահմաներ ոչ թե համաձայնության գործողության ժամկետը, այլ անձնական տվյալները մշակելու ժամկետները, որի դեպքում տվյալներ մշակողները կսահմանեն, թե որ անձնական տվյալը որ նպատակի համար և ինչ ժամկետով է մշակվում, այդ թվում՝ պահպանվում:

#### 4. Համաձայնության տեղեկացված լինելը

Անձնական տվյալներ մշակելու համաձայնությունը պետք է լինի տեղեկացված: Այս պահանջը հիմնված է տվյալների մշակման թափանցիկության սկզբունքի վրա, համաձայն որի՝ տվյալների սուբյեկտները պետք է հասանելի և հասկանալի եղանակով տեղեկացված լինեն, թե ինչպես է իրականացվում նրանց անձնական տվյալների մշակումը<sup>2</sup>: Խորհուրդը, անդրադառնալով համաձայնության «տեղեկացված» լինելու չափանիշին, նշել է, որ անձնական տվյալների սուբյեկտի համաձայնությունը պետք է հիմնված լինի անձնական տվյալների մշակման հանգամանքները և հետևանքները գիտակցելու և հասկանալու, անձնական տվյալների մշակման (մշակվող տվյալների, մշակման նպատակի, այլ անձանց հնարավոր փոխանցման, տվյալների սուբյեկտի իրավունքների և այլնի) վերաբերյալ ճշգրիտ և լիարժեք տեղեկությունների վրա: Ընդ որում, այդ տեղեկությունները պետք է հասանելի, հասկանալի և տեսանելի լինեն տվյալների սուբյեկտի համար<sup>3</sup>:

Ի կատարումն համաձայնության՝ տեղեկացված լինելու պահանջի, ԱՏՊ օրենքի 10-րդ հոդվածի 1-ին մասով սահմանվում է, որ տվյալներ մշակողը

<sup>1</sup> Guidelines 05/2020 on consent under Regulation 2016/679, 2020, p. 61.

<sup>2</sup> Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, p. 6.

<sup>3</sup> Opinion 15/2011 on the definition of consent (WP187), 2011, p. 14.

տվյալների սուբյեկտի համաձայնությունը ստանալու նպատակով ծանուցում է տվյալներ մշակելու մտադրության մասին: Նույն հոդվածի 2-րդ մասի համաձայն՝ ծանուցումը պետք է պարունակի հետևյալ տեղեկությունները՝ 1) տվյալների սուբյեկտի ազգանունը, անունը, հայրանունը, 2) անձնական տվյալների մշակման իրավական հիմքերը և նպատակը, 3) մշակման ենթակա անձնական տվյալների ցանկը, 4) անձնական տվյալների հետ կատարման ենթակա գործողությունների ցանկը, որոնց համար հայցվում է տվյալների սուբյեկտի համաձայնությունը, 5) այն անձանց շրջանակը, որոնց կարող են փոխանցվել անձնական տվյալները, 6) անձնական տվյալների սուբյեկտի համաձայնությունը հայցող մշակողի կամ նրա ներկայացուցչի անվանումը (ազգանունը, անունը, հայրանունը, պաշտոնը) և գտնվելու կամ հաշվառման (փաստացի բնակության) վայրը, 7) տվյալների սուբյեկտի կողմից անձնական տվյալների ուղղում, ոչնչացում, տվյալների մշակման դադարեցում պահանջելու կամ մշակման հետ կապված այլ գործողություն կատարելու վերաբերյալ տեղեկություններ, 8) հայցվող համաձայնության գործողության ժամկետը, ինչպես նաև համաձայնությունը հետ կանչելու կարգը և դրա հետևանքները:

Տվյալների սուբյեկտների համաձայնությունը ստանալուց առաջ նրանց անձնական տվյալների մշակման վերաբերյալ տեղեկատվություն տրամադրելը կարևոր է, որպեսզի վերջիններս կարողանան իրենց տվյալների վերաբերյալ տեղեկացված որոշումներ կայացնել, տեղեկացված լինեն, թե ինչպիսի պայմաններով անձնական տվյալների մշակման համար են տրամադրում իրենց համաձայնությունը: Եթե տվյալներ մշակողը տվյալների սուբյեկտին չի տրամադրում հասանելի և անհրաժեշտ տեղեկատվություն, ապա տվյալների սուբյեկտի տրված համաձայնությունը դառնում է պատրանքային<sup>1</sup>: Վճռաբեկ դատարանը գործերից մեկով նշել է, որ համաձայնությունը միշտ ենթադրում է անձնական տվյալի մշակման վերաբերյալ անձնական տվյալների սուբյեկտների իրազեկվածություն: Հենց այս նպատակով օրենսդիրը սահմանել է անձնական տվյալներ մշակողի կողմից տվյալների սուբյեկտի համաձայնությունն ստանալու նպատակով ծանուցման կառուցակարգ, որը կոչված է ապահովելու համաձայնության՝ «տեղեկացված» լինելու չափանիշին համապատասխանությունը<sup>2</sup>:

Տեղեկացվածության վերաբերյալ վերը հիշատակված ստանդարտներից հետևում է, որ վերջինս ենթադրում է բովանդակային և ձևական պահանջների պահպանում: *Բովանդակային առումով* տեղեկացված լինելու պահանջը ենթադրում է տվյալների մշակման վերաբերյալ էական տեղեկությունների

<sup>1</sup> Guidelines 05/2020 on consent under Regulation 2016/679, 2020, p. 62.

<sup>2</sup> Վճռաբեկ դատարանի որոշումը թիվ ԵԴ/25649/02/20 քաղաքացիական գործով:

տրամադրում<sup>1</sup>, որոնց հիման վրա տվյալների սուբյեկտը կայացնում է իր անձնական տվյալները մշակելու համաձայնություն տալու/չտալու մասին որոշում: *Ձևական առումով* այդ տեղեկությունները պետք է հասանելի և մատչելի լինեն տվյալների սուբյեկտի համար: Դա ապահովելու նպատակով տվյալներ մշակողը պետք է տվյալների սուբյեկտին ընձեռի անձնական տվյալների մշակման պայմաններին ծանոթանալու իրական հնարավորություն: Մասնավորապես, համաձայնության տեղեկացված լինելու պահանջը պահպանված չէ այն դեպքում, երբ տվյալներ մշակողը, տվյալների սուբյեկտի համաձայնությունը ստանալու համար, վերջինիս տեղեկացնում է, որ անձնական տվյալների մշակման՝ ԱՏՊ օրենքի 10-րդ հոդվածով սահմանված տեղեկությունները տեղադրված են իր ինտերնետային կայքում<sup>2</sup>: Դրա փոխարեն, տվյալներ մշակողը պետք է ակտիվ գործողությամբ տվյալների սուբյեկտին ներկայացնի պահանջվող տեղեկությունները, այլ ոչ թե դա թողնի տվյալների սուբյեկտի հայեցողությանը: Պրակտիկ տեսանկյունից այդ պարտականությունը կարող է կատարվել անհրաժեշտ տեղեկությունները տվյալների սուբյեկտի էլեկտրոնային հասցեին ուղարկելով, անձնական տվյալներ մշակելու համաձայնագրի մեջ ներառելով և այլն:

### Եզրակացություն

Այսպիսով, սույն աշխատանքի մեջ կատարված վերլուծությունները թույլ են տալիս կատարել հետևյալ եզրահանգումները.

1. Թեև անձնական տվյալներ մշակելու համաձայնության վավերապայմանները գրեթե սահմանված չեն ՀՀ օրենսդրությամբ, այնուամենայնիվ, դրանք բխեցվում են օրենսդրական նորմերից իրավակիրառ և դատական պրակտիկայի շրջանակներում կայացված որոշումների միջոցով:
2. ՀՀ իրավունքում ձևավորված անձնական տվյալներ մշակելու համաձայնության վավերապայմանները, որոշ առանձին վերապահումներով հանդերձ, համարժեք են ԵՄ իրավունքում ձևավորված ստանդարտներին: Այնուամենայնիվ, դրանք ունեն զարգացման և հստակեցման կարիք:
3. ՀՀ-ում անձնական տվյալների մշակման իրավական հիմքերը սակավ են, որի պայմաններում համաձայնություն տալը կարող է համարվել տվյալներ մշակողի կողմից մատուցվող ծառայություններից օգտվելու պարտադիր

<sup>1</sup> Խոսքը գնում է ԱՏՊ օրենքի 10-րդ հոդվածի 2-րդ մասով թվարկված տեղեկությունների մասին:

<sup>2</sup> Անձնական տվյալների պաշտպանության գործակալության որոշումը N-040/08/23 վարչական գործով:



նախապայման, իսկ արդեն տրված համաձայնությունը հետ կանչելու պահանջը միշտ չէ, որ իրատեսական է՝ ելնելով տվյալներ մշակողի իրավունքների և օրինական շահերի պաշտպանության անհրաժեշտությունից: Նման պայմաններում պրակտիկայում միշտ չէ, որ պահպանվում է համաձայնության՝ ազատ տրված լինելու պահանջը:

## **Օգտագործված նորմատիվ իրավական ակտերի և գրականության ցանկ**

### **Օրենսդրություն**

1. ՀՀ Սահմանադրություն՝ 06.12.2015 թ. փոփոխություններով:
2. «Անձնական տվյալների պաշտպանության մասին» ՀՕ-49-Ն ՀՀ օրենք՝ ընդունված 18.05.2015 թ.:
3. «Վարկային տեղեկատվության շրջանառության և վարկային բյուրոների գործունեության մասին» ՀՕ-185-Ն ՀՀ օրենք՝ ընդունված 22.10.2008 թ.:
4. «Անձնական տվյալների պաշտպանության մասին» 2016 թվականի ապրիլի 27-ի թիվ 2016/679 ԵՄ ընդհանուր կանոնակարգ՝ ընդունված 27.04.2016 թ.:
5. «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» ԵԽ կոնվենցիան փոփոխող արձանագրություն՝ ընդունված 18.05.2018 թ.:
5. «Էլեկտրոնային հաղորդակցության բնագավառում մասնավոր կյանքի և անձնական տվյալների պաշտպանության մասին» 2002/58/EC դիրեկտիվ՝ ընդունված 12.07.2002 թ.:
6. Հայաստանի ավտոապահովագրողների բյուրոյի RL 1-001 կանոններ (ԱՊՊԱ ընդհանուր պայմաններ):

### **Դատական և վարչական գործեր**

7. Վճռաբեկ դատարանի որոշումը թիվ ԵԴ/25649/02/20 քաղաքացիական գործով:
8. Վճռաբեկ դատարանի որոշումը թիվ ԵԴ/5278/02/19 քաղաքացիական գործով:
9. Անձնական տվյալների պաշտպանության գործակալության որոշումը N-021/12/18 վարչական գործով:
10. Անձնական տվյալների պաշտպանության գործակալության որոշումը N-040/08/23 վարչական գործով:

### Խորհրդատվական որոշումներ և կարծիքներ

11. Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին ԵԽ կոնվենցիայի պաշտոնական պարզաբանումներ, 2018:

12. Article 29 Working Party, Guidelines on transparency under Regulation 2016/679.

13. European data protection board, Guidelines 05/2020 on consent under Regulation 2016/679, 2020.

14. Working Party 187, Opinion 15/2011 on the definition of consent, 2011.

## УСЛОВИЯ ДЕЙСТВИТЕЛЬНОСТИ СОГЛАСИЯ КАК ПРАВОВОГО ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

### Аннотация

Персональные данные фактически являются краеугольным камнем современной цифровой экономики. Однако для того чтобы обработка персональных данных считалась законной, она, прежде всего, должна осуществляться на соответствующем правовом основании. Обработывая персональные данные своих клиентов, хозяйствующие субъекты, как правило, полагаются на согласие последних. Для заключения договоров страхования, предоставления маркетинговых услуг, выдачи кредитов хозяйствующие субъекты обрабатывают информацию о различных аспектах жизни физических лиц, получая их согласие.

Однако проблема заключается в том, что законодательство о защите персональных данных в стране относительно новое, а правовые нормы часто формулируются не в виде четких предписаний, а в виде стандартов. В результате хозяйствующие субъекты обрабатывают персональные данные своих клиентов, исходя из собственных представлений и предпринимательских соображений, что делает защиту прав и законных интересов физических лиц проблематичной.

Учитывая эти проблемы, данная статья призвана изучить условия действительности согласия как правового основания обработки персональных данных, опираясь как на правовые регулирования Республики Армения, судебную и правоприменительную практику, так и на существующие лучшие стандарты в этой области, в частности на законодательство ЕС и “мягкое право”.

## VALIDITY REQUIREMENTS OF CONSENT AS A LEGAL BASIS FOR PERSONAL DATA PROCESSING

Personal data is truly considered the cornerstone of the modern digital economy. However, for personal data processing to be considered lawful, it must first and foremost be carried out on an appropriate legal basis. When processing their customers' personal data, economic entities typically rely on the latter's consent. For purposes such as entering into insurance contracts, providing marketing services, or granting loans, economic entities process information about various aspects of individuals' lives with their consent.

The problem, however, is that personal data protection legislation in the country is relatively new, and legal norms are often formulated not as clear directives but as standards. As a result, economic entities process their customers' personal data based on their own perceptions and entrepreneurial considerations, which makes the protection of individuals' rights and legitimate interests problematic.

Considering these issues, this article aims to examine the validity requirements for consent as a legal basis for processing personal data, drawing upon both Armenian legal regulations, judicial and law enforcement practices, as well as the best existing standards in the field, particularly EU legislation.

**Keywords:** personal data, consent, data controller, data subject.

Հոդվածը հանձնված է խմբագրություն 07.07.2025 թ., տրվել է գրախոսության 10.07.2025 թ., ընդունվել է տպագրության 25.07.2025 թ.:

юридических лиц Уголовного кодекса РА еще не стал предметом комплексного исследования и практического применения и многочисленные вопросы по теме требуют разъяснения, можно констатировать, что выбранная тема остается актуальной.

**Ключевые слова:** преюдиция, юридическое лицо, внутреннее убеждение судьи, пределы преюдиции, неопровержимая преюдиция, предмет доказывания.

## 1. Введение

На современном этапе уголовного судопроизводства вопрос применения преюдиции в уголовно-процессуальных правоотношениях приобретает особую актуальность в условиях динамично развивающихся экономических отношений. Значимость данного института объясняется тем, что обстоятельства, установленные ранее и обладающие юридическим значением, позволяют существенно упростить процесс доказывания, повысить эффективность расследования и оптимизировать судебное разбирательство. Особенно актуально это в нынешних условиях, когда юридические лица, вовлечённые в сложные экономические отношения, уже признаны полноправными участниками уголовного процесса. Таким образом, преюдиция становится важнейшим средством обеспечения процессуальной экономии, укрепления правовой определенности и формирования единообразной судебной практики при привлечении организаций к уголовной ответственности.

Как справедливо отмечает Г.М. Резник, разрешение сложнейших экономических споров требовало применения арбитражными судами норм корпоративного, финансового, банковского, налогового, таможенного права - причем не только отечественного, но и иностранного. В уголовном же судопроизводстве все более распространённый характер стали приобретать заведение в коррупционных целях уголовных дел в отношении предпринимателей, их обвинение и последующее осуждение по статьям о мошенничестве, присвоении и легализации (отмывании) полученных преступным путем денежных средств или иного имущества<sup>1</sup>.

<sup>1</sup> Резник Г.М. Стандарты доказанности и межотраслевая преюдиция [Электронный ресурс]. URL: <http://www.iuaj.net/node/625>

## 2. Основное исследование

Следует подчеркнуть, что за последние пятнадцать лет институт преюдиции неоднократно становился предметом рассмотрения не только законодателя, но и Конституционного Суда РА, что свидетельствует о его особой значимости в целях доказывания и функционирования уголовного судопроизводства в целом. Сама концепция преюдиции отражает характер соотношения различных видов судопроизводства в государстве, уровень доверия к судебным актам, а также выявляет как сходство, так и различие стандартов доказывания в уголовном, гражданском, арбитражном и административном процессах. В этом контексте преюдициальный аспект выступает не только как законодательная или правоприменительная категория, но и как явление политико-правового характера, поскольку в его рамках преломляются ключевые проблемы уголовно-правовой политики и формирования единого правового пространства.

Правильное разрешение на нормативном уровне вопросов преюдиции обеспечивает стабильность судебных решений и единство судебной системы, позволяет снизить стоимость судопроизводства, обеспечить быстрое рассмотрение дел в разумные сроки. Однако наряду с этим верно подчеркивается проблемность преюдиции, заключающаяся «в том, что при ее применении могут вступать в коллизию два процессуальных принципа: общеобязательная сила судебных постановлений и внутреннее судебское убеждение при оценке доказательств»<sup>1</sup>.

Термин «преюдиция» имеет латинское происхождение (от лат. praepjudicialis) и означает «относящийся к предыдущему судебному решению»<sup>2</sup>. Одно из первых упоминаний о преюдиции содержится во фрагменте таблицы, являвшейся источником римского права. Также к ранним источникам относятся труды Цицерона, Цезаря, Сенеки, Павла и Ульпиана. Наиболее полное значение, которое римские граждане придавали преюдиции, раскрыто в Институциях Гая и в Своде римского права<sup>3</sup>.

В Древнем Риме институт преюдиции не имел абсолютного и неопровержимого характера. При рассмотрении побочного, второстепенного

<sup>1</sup> См. там же.

<sup>2</sup> Арутюнян А. А., Брусницын Л. В., Васильев О. Л., Головки Л. В. и др. Курс уголовного процесса / Под ред. Л. В. Головки. – М.: Статут, 2016. – 1278 с.

<sup>3</sup> Бартошек М. Римское право: понятия, термины, определения / М. Бартошек. – М., 1989.

вопроса ответчик мог возражать против применения преюдиции, если её использование способно было нанести ему ущерб в последующем процессе по основному спору. Так, например, разбирательству уголовного дела о преступлении, наказуемом смертной казнью, могло предшествовать рассмотрение имущественного спора, и в таком случае сторона имела право оспаривать преюдициальное значение ранее вынесенного решения. Данные положения основывались на норме, закреплённой в Кодексе Юстиниана, где подчёркивалось: “Решение, принятое по спору двоих, никому не должно причинять вред”<sup>1</sup>.

В юридической литературе существует понятие преюдициальности (от лат. *praejudicio* – предрешение) – в процессуальном праве обязательность для всех судов, рассматривающих дело, принять без проверки и доказательств факты, ранее установленные вступившим в законную силу решением или приговором по какому-либо другому делу<sup>2</sup>.

Следует заметить, что понятие преюдиции исторически изменчиво. Интересно, насколько оно изменчиво с “географической” точки зрения. Так, обращаясь к американскому праву, мы можем констатировать, что по их законодательству преюдиция не относится к доказательному праву, а регулируется правилами о процедуре. *Res judicata* означает эффект предыдущего судебного решения, который не подчиняется логическим правилам, а регламентируется правилами судопроизводства. *Res judicata* включает в себя: 1) предотвращение иска (*claim preclusion*) и 2) предотвращение вопроса (*issue preclusion*).

Предотвращение иска означает, что истец вправе лишь один раз предъявить иск, вытекающий из одних и тех же действий или происшествий. Например, предъявлен иск о возмещении вреда, причиненного вследствие дорожно-транспортного происшествия, где истец настаивает на небрежных действиях ответчика. После вынесения решения по этому делу тот же истец не вправе предъявить иск к тому же ответчику в связи с тем же происшествием, даже если на этот раз он ссылается не на небрежность, а на правило об ответственности без вины. Предотвращение вопроса означает, что

<sup>1</sup> Дигесты Юстиниана [Электронный ресурс]. – URL: <http://www.digestaiust.narod.ru/03.html>

<sup>2</sup> Постановление Конституционного Суда РФ от 17 марта 2009 г. №5-П “По делу о проверке конституционности положения, содержащегося в абзацах четвертом и пятом пункта 10 статьи 89 Налогового кодекса Российской Федерации, в связи с жалобой общества с ограниченной ответственностью “Варм”. URL: [www.ksrf.ru](http://www.ksrf.ru)