DOI: 10.59560/18291155-2024.3-11

ՍԻՄՈՆ ՍԻՄՈՆՅԱՆ
Հայաստանում ֆրանսիական համալսարանի
հետազոտող դասախոս,
Ժան Մուլեն Լիոն 3 համալսարանի
իրավագիտության դոկտոր

ՄԱՍՆԱՎՈՐ ԻՐԱՎՈՒՆՔԻ ՍՈՒԲՅԵԿՏՆԵՐԻ ԿՈՂՄԻՑ ՏԵՍԱՀՍԿՄԱՆ ՄԻՋՈՑՈՎ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՄՇԱԿՄԱՆ ԵՐԱՇԽԻՔՆԵՐԸ (ՍԿԶԲՈՒՆՔՆԵՐԸ)

Ամփոփագիր

Տեսահսկման համակարգերը լայնորեն կիրառվում են անձանց կյանքի, գույքի պաշտպանության, իրավախախտումների կանխարգելման և բացահայտման, ինչպես նաև այլ օրինական շահերի պաշտպանության համար: Միևնույն ժամանակ, տեսահսկումը կարող է հանգեցնել ֆիզիկական անձանց վերաբերյալ տվյալների ապօրինի մշակման: Վերոնշյալ համատեքստում մի կողմից առաջանում է տեսահսկում իրականացնող անձի շահերի պաշտպանության անհրաժեշտությունը, մյուս կողմից՝ անձնական տվյալների պաշտպանության երաշխիքները պահպանելու հրամայականը: Եթե պետական մարմինների կողմից տեսահսկման իրականացման առանձնահատկություններն արդեն իսկ կարգավորված են օրենսդրությամբ, ապա իրավունքի մասնավոր սուբյեկտների կողմից իրականացվող տեսահսկման իրավաչափությունը, որպես կանոն, հատուկ նորմերի բացակայության պայմաններում գնահատվում է անձնական տվյալների պաշտպանության ընդհանուր կանոնների հիման վրա:

Հաշվի առնելով հայաստանյան դոկտրինայում քննարկվող հարցի վերաբերյալ ուսումնասիրությունների բացակայությունը՝ սույն հոդվածի առաջին մասը կոչված է բացահայտելու տեսահսկման միջոցով անձնական տվյալների մշակման առանձնահատկությունները: Աշխատանքի երկրորդ մասը կոչված է քննարկելու ՀՀ օրենսդրությամբ սահմանված այն երաշխիքները, որոնց վրա պետք է հիմնվի իրավունքի մասնավոր սուբյեկտների կողմից տեսահսկման միջոցով անձնական տվյալների մշակումը:

Հիմնաբառեր. տեսահսկում, անձնական տվյալ, օրինականություն, համաչափություն, թափանցիկություն:

Ներածություն

Տեսահսկման համակարգերի օգտագործումն ինչպես պետության, այնպես էլ մասնավոր իրավունքի սուբյեկտների կողմից կարող է ծառայել վերջիններիս օրինական նպատակների իրագործմանը. այժմ տեսահսկման համակարգերը լայնորեն կիրառվում են անձանց, գույքի պաշտպանության, իրավախախտումների կանխարգելման, ինչպես նաև այլ օրինական շահերի պաշտպանության համար:

Այնուամենայնիվ, տեսահսկումը կարող է բացասական ազդեցություն ունենալ մարդկանց վարքագծի վրա, քանի որ կարող է առաջացնել պարբերաբար հսկողության ներքո լինելու զգացողություն[1], ինչպես նաև հանգեցնել անձի վերաբերյալ տվյալների անհամաչափ և չհիմնավորված մշակման: Վերոնշյալ համատեքստում մի կողմից առաջանում է տեսահսկում իրականացնող անձի շահերի պաշտպանության անհրաժեշտությունը, մյուս կողմից՝ անձնական տվյալների պաշտպանության երաշխիքները պահպանելու հրամայականը:

Եթե ՀՀ-ում պետական մարմինների կողմից իրենց լիազորությունների շրջանակներում տեսահսկման միջոցով անձնական տվյալների

[1] European data protection board, Guidelines 3/2019 on processing of personal data through video devices, 2020. p. 5.

մշակումը ենթարկվել է ոլորտային կարգավորումների[1], ապա նույնը չի կարելի ասել մասնավոր իրավունքի սուբյեկտների մասով: Տեսահսկման մասով հատուկ նորմերի բացակայության պայմաններում գործում են «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով սահմանված նորմերը, որոնք չեն նախատեսում հատուկ կարգավորումներ տեսահսկման համար, սակայն նախատեսում են անձնական տվյալների մշակման սկզբունքներ ու կանոններ:

Սույն աշխատանքի նպատակն է ուսումնասիրել ՀՀ-ում մասնավոր իրավունքի սուբյեկտների կողմից տեսահսկման միջոցով անձնական տվյալների մշակման իրավակարգավորումը և, մասնավորապես, տեսահսկման իրավական հիմքերն ու դրա իրականացման այլ իրավական երաշխիքները՝ տեսահսկման վերաբերյալ ներպետական հատուկ կարգավորումների բացակայության պայմաններում: Վերոնշյալ հարցերի քննարկումը նախևառաջ պահանջում է հասկանալ տեսահսկմամբ անձնական տվյալներ մշակելու էությունն ու առանձնահատկությունները:

Հոդվածում կատարվող ուսումնասիրությունների համար որպես իրավական հիմք են ծառայում ՀՀ և ԵՄ իրավունքները: Աշխատանքում կներկայացվեն նաև տեսահսկման վերաբերյալ անձնական տվյալների պաշտպանության բնագավառում լիազոր մարմնի՝ Անձնական տվյալների պաշտպանության գործակալության (այսուհետ նաև՝ Գործակալություն) վարչական վարույթների արդյունքում ընդունված

[1] Օրինակ, «Ոստիկանության մասին» ՀՀ օրենքի 22-րդ հոդվածով նախատեսված է, որ հանցագործությունները կանխելիս կամ բացահայտելիս, հասարակական կարգի պահպանությունը (այդ թվում՝ ճանապարհային երթևեկության անվտանգությունը) ապահովելիս ոստիկանությունը կարող է հանրային վայրերում օգտագործել անշարժ տեսանկարահանող կամ լուսանկարահանող տեխնիկական միջոցներ: ՀՀ Քրեակատարողական օրենսգրքի 78-րդ հոդվածի 1-ին մասով սահմանված է տեսաձայնագրման հնարավորություն՝ դատապարտյալների կամ այլ անձանց անվտանգության ապահովման կամ այլ իրավաչափ շահերի պաշտպանության նպատակով՝ դատապարտյալների փախուստները, ինքնավնասումները, ինքնասպանությունները, պատժի կատարման սահմանված կարգի խախտումները, անկարգությունները, հանցանքները կամ այլ իրավախախտումները կանխելու կամ խափանելու նպատակով:

որոշումները, Վճռաբեկ դատարանի դիրքորոշումները, ինչպես նաև ՀՀ-ում և ԵՄ-ում ձևավորված փափուկ իրավունքը»[1]:

1. Տեսահսկումը՝ որպես անձնական տվյալների մշակման եղանակ

1.1. Անձանց նույնականացումը տեսապատկերների միջոցով

Եվրոպայի անձնական տվյալների պաշտպանության վերահսկողի (անգլ՝ European data protection supervisor) ուղեցույցներում տեսահսկումը սահմանվում է որպես տարածքի, միջոցառման, գործունեության կամ անձի տեսահսկումը էլեկտրոնային սարքավորման միջոցով[2]: Հասկանալու համար, թե ինչպես է տեսահսկմամբ իրականացվում անձնական տվյալների մշակում, անհրաժեշտ է նախևառաջ համադրել «անձնական տվյալ» եզրույթը տեսահսկման տեսադաշտում հայտնվող պատկերների հետ:

Այսպես՝ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի (այսուհետ նաև՝ Օրենք) 3-րդ հոդվածի 1-ին մասի 1-ին կետի համաձայն՝ անձնական տվյալը ֆիզիկական անձին վերաբերող ցանկացած տեղեկություն է, որը թույլ է տալիս կամ կարող է թույլ տալ ուղղակի կամ անուղղակի կերպով նույնականացնել անձի ինքնությունը: Այս դրույթից հետևում է, որ անձնական տվյալն այնպիսի տեղեկություն է, որն ունի ֆիզիկական անձին ուղղակիորեն կամ անուղղակիորեն նույնականացնելու հատկություն, այսինքն բնութագրվում է մարդուն նույնականացնելու հատկանիշով: Անձնական տվյալի վերը նշված սահմանման բովանդակությունից հետևում է, որ մարդու տեսապատկերը, այսինքն՝ այն պատկերը, որում տեսանելի է մարդու դեմքը, անձնական տվյալ է, քանի որ տեսապատկերն ունի մարդուն նույնականացնող

[1] Գործակալության՝ «փափուկ իրավունք» ձևավորելու լիազորությունը նախատեսված է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 24-րդ հոդվածի 3-րդ մասի 15-րդ կետով, որի համաձայն՝ Գործակալությունը կատարում է հետազոտություններ և մշակողների դիմումների կամ լուսաբանումների հիման վրա տալիս տվյալներ մշակելու վերաբերյալ խորհրդատվություն կամ տեղեկացնում է անձնական տվյալներ մշակելու վերաբերյալ լավագույն փորձի մասին:

[2] European data protection supervisor, Video-surveillance guidelines 2010. p. 7.

հատկություն: Մարդու պատկերի նույնականացնող հատկությունը կայանում է նրանում, որ այն ի ցույց է դնում մարդու ուրույն, միայն իրեն հատուկ դեմքի և մարմնի կառուցվածքի առանձնահատկությունները և տարբերակում է մարդուն այլ մարդկանցից:

Մարդու տեսապատկերը կամ պատկերը որակվել է որպես անձնական տվյալ Մարդու իրավունքների եվրոպական դատարանի կողմից (այսուհետ նաև՝ ՄԻԵԴ) Ֆոն Հաննովերն ընդդեմ Գերմանիայի Դաշնային Հանրապետության գործով: Այդ գործով ՄԻԵԴ-ն արձանագրել և վերահաստատել է այն դիրքորոշումը, որ անձի պատկերը հանդիսանում է իր անհատականության գլխավոր հատկանիշներից մեկը, քանի որ այն ի ցույց է դնում **անձի ուրույն հատկանիշները և տարբերակում է անձին իր նմաններից**[1]: Տեսապատկերի՝ որպես անձնական տվյալի որակմանն անդրադարձել է նաև ԵՄ անձնական տվյալների պաշտպանության վերահսկողը: Այսպես՝ ըստ EDPS-ի՝ դիմապատկերները միշտ անձնական տվյալներ են համարվում նույնիսկ այն դեպքում, երբ **տեսահսկվող անհատները ճանաչված կամ նույնականացված չեն տեսահսկում իրականացնողների կողմից**[2]: Այլ կերպ ասած՝ տեսահսկողի կողմից տեսահսկվողին անձամբ նույնականացնելը կամ չնույնականացնելը որևէ կերպ չի պայմանավորում տեսահսկվող անձի տեսապատկերի անձնական տվյալ լինելը, քանի որ տեսապատկերի՝ որպես անձնական տվյալ որակվելը որոշվում է ոչ թե տեսահսկողի կողմից տեսանյութում պատկերված անձին նույնականացնելով, այլ տեսապատկերի՝ մարդուն նույնականացնելու հատկությամբ: Մասնավորապես, թեև իրավախախտում կատարած անձը նույնականացված չէ տեսահսկում իրականացնող ընկերության կողմից, այնուամենայնիվ, վերջինիս տեսապատկերն ինքնին այնպիսի տվյալ է, որի միջոցով վերջինս կարող է նույնականացվել իրավապահ մարմինների, կամ համացանցում, հեռուստատեսությամբ հրապարակվելու դեպքում՝ այլ անձանց կողմից:

[1] ՄԻԵԴ, *Ֆոն Հաննովերն ընդդեմ Գերմանիայի* (թիվ 2), գանգատներ թիվ 40660/08 և 60641/08, կետ 96:

[2] European data protection supervisor, Video-surveillance guidelines, 2010. p. 8.

Այնուամենայնիվ, երբեմն անհրաժեշտ չէ տեսանկարահանել անձի ճանաչելի դեմքի պատկերներ, որպեսզի վերջինս նույնականացվի: Անձի ավելի քիչ տեսանելի կամ անճանաչելի դիմապատկերը նույնպես կարող է անձնական տվյալ համարվել՝ պայմանով, որ վերջինս հնարավոր լինի նույնականացնել անձի ֆիզիկական կամ վարքագծային առանձնահատկություններն այլ տվյալների հետ համադրելով[1]:

Տեսահսկման՝ որպես անձնական տվյալներ մշակելու մասին կարող են վկայել նաև այն նպատակները, որոնց իրագործման համար տվյալներ մշակողն իրականացնում է տեսահսկում: Մասնավորապես, երբ տեսախցիկները տեղադրվում են անձանց և նրանց գույքի անվտանգությունն ապահովելու, իրավախախտումները կանխելու կամ բացահայտելու նպատակով, ապա միջադեպի առկայության դեպքում անձի վերաբերյալ հավաքված տվյալները իրավապահ մարմինների կողմից ձեռքբերված այլ տվյալների հետ համադրության արդյունքում հնարավոր է նույնականացնել իրավախախտումը կատարած անձին:

Օրենքի 3-րդ հոդվածի 1-ին մասի 2-րդ կետով սահմանված է, որ անձնական տվյալների մշակումը ցանկացած գործողություն կամ գործողությունների խումբ է՝ անկախ իրականացման ձևից և եղանակից, այդ թվում՝ ավտոմատացված, տեխնիկական ցանկացած միջոցներ կիրառելու կամ առանց դրանց (...): Այս համատեքստում պետք է հիշատակել C–345/17 գործով ԵՄ Արդարադատության դատարանի դիրքորոշումը, ըստ որի՝ անձանց շարունակական տեսաձայնագրումը և տեսաձայնագրության պահպանումը համակարգչային համակարգի կոշտ սկավառակի վրա համարվում է անձնական տվյալների մշակում[2]: Մեկ այլ գործով նույն դատարանն արձանագրել է, որ տեսահսկման համակարգի միջոցով իրականացվում է անձնական տվյալների մշակում, եթե այն հնարավորություն է տալիս գրանցել և պահպանել

[1] European data protection supervisor, Video-surveillance guidelines, 2010. p. 8.

[2] CJEU, Case C-345/17, *Sergejs Buivids vs. Datu valsts inspekcija*, 14 February 2019, §34.

անձնական տվյալները, օրինակ՝ տեսապատկերները, որոնք թույլ են տալիս նույնականացնել ֆիզիկական անձանց[1]:

Հարկ է նաև նշել, որ անձնական տվյալների փաստի առկայությունը որևէ կերպ չի կարող կախվածության մեջ դրվել մշակման ձևից և եղանակից. այն փաստը, որ տվյալներ մշակողը տեսանյութերին հեռավար եղանակով իրական ռեժիմում հասանելիություն չունի, և որ այս կամ այն տեսանյութի ուսումնասիրությունը կարող է իրականացվել ըստ անհրաժեշտության՝ բողոքի դեպքում կամ ընտրանքային, որևէ ազդեցություն չունի տվյալների մշակման փաստի առկայության վրա:

1.2. Անձանց նույնականացումը կենսաչափական անձնական տվյալների միջոցով

Տեխնոլոգիաների զարգացմանը զուգընթաց վերափոխվում են նաև տեսահսկմամբ անձնական տվյալներ մշակելու եղանակները: Ներկայումս հատկապես տարածված է կենսաչափական անձնական տվյալների մշակման միջոցով անձանց նույնականացման պրակտիկան: Կենսաչափական տվյալների՝ որպես անձնական տվյալի առանձնահատուկ տեսակի մասին համապարփակ կարգավորումներ նախատեսված են ԵՄ օրենսդրությամբ: Մասնավորապես, ըստ Անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգի (այսուհետ նաև՝ GDPR կամ Կանոնակարգ) կենսաչափական են համարվում **հատուկ տեխնիկական մշակման արդյունքում ստացված անձնական տվյալները**, որոնք վերաբերում են անձի ֆիզիկական, ֆիզիոլոգիական կամ վարքագծային առանձնահատկություններին, և որոնց միջոցով իրականացվում է նրանց **եզակի նույնականացումը**, օրինակ՝ դեմքի պատկերները կամ մատնահետքը: Բովանդակային առումով կենսաչափական անձնական տվյալի նույնական սահմանում նախատեսված է Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին ԵԽ կոնվենցիայի

[1] CJUE, Case C-708/18, *TK vs. Asociaţia de Proprietari bloc M5A-ScaraA*, 11 December 2019, §35.

(առավել հայտնի անվանումը՝ 108+ կոնվենցիա) պաշտոնական պարզաբանումներով[1]:

Պրակտիկայում հաճախ առաջանում է այն հարցը, թե արդյոք անձի տեսապատկերը համարվում է կենսաչափական անձնական տվյալ: Այս առումով հարկ է նշել, որ GDPR-ի 51-րդ կետը նախատեսում է, որ տեսանկարները համարվում են կենսաչափական տվյալներ միայն այն դեպքում, երբ մշակվում են հատուկ տեխնիկական միջոցներով, որոնք թույլ են տալիս ֆիզիկական անձի եզակի նույնականացումը: Նմանատիպ նույնականացումը իրավակիրառ պրակտիկայում բնորոշվում է որպես դեմքի ճանաչում (անգլ.՝ facial recognition):

Տեսապատկերի՝ որպես կենսաչափական անձնական տվյալի միջոցով անձի եզակի նույնականացման բացահայտումը պահանջում է տեխնիկական տեսանկյունից վերլուծել այդպիսի անձնական տվյալների մշակման առանձնահատկությունները: Նախևառաջ, տեսախցիկի կամ տեսաձայնագրող սարքի միջոցով նկարահանվում է անձի տեսապատկերը, այսինքն՝ տեղի է ունենում անձնական տվյալի հավաքում: Այնուհետև, վերոնշյալ եղանակով հավաքված անձի տեսապատկերի հիման վրա ստեղծվում է հատուկ թվային մոդել, որը պարունակում է անձի արտաքին տեսքի որոշակի առանձնահատկություններ[2]: Թվային մոդելները պահպանվում են տվյալների հատուկ բազաներում: Եվ վերջապես, անձին նույնականացնելու նպատակով տեսախցիկի կամ տեսաձայնագրող սարքի միջոցով հավաքվում են տվյալներ անձի տեսապատկերի մասին, համեմատում տվյալների բազայում առկա թվային մոդելների հետ, և տեսապատկերի և վերջինիս թվային մոդելի միջև համընկման պարագայում իրականացվում է անձի ինքնաշխատ նույնականացումը: Անձի տեսապատկերի յուրաքանչյուր թվային

[1] Վերը նշված պարզաբանումների 58-րդ կետով սահմանված է, որ կենսաչափական են համարվում հատուկ տեխնիկական մշակման արդյունքում ստացված անձնական տվյալները, որոնք վերաբերում են անձի ֆիզիկական, ֆիզիոլոգիական կամ վարքագծային առանձնահատկություններին, և որոնց միջոցով իրականացվում է նրանց եզակի նույնականացումը:

[2] CNIL, Reconnaissance faciale pour un debat à la hauteur des enjeux, 2019. p. 3.

մոդելով հնարավոր է նույնականացնել միայն կոնկրետ այդ անձին, հետևաբար նմանատիպ նույնականացումը կոչվում է եզակի: Այլ կերպ ասած՝ կենսաչափական անձնական տվյալների միջոցով անձի եզակի նույնականացումը ենթադրում է տվյալներ մշակողի մոտ առկա տվյալների բազայում առկա անձի կենսաչափական տվյալների համեմատում/համադրում անձի՝ հետագայում տեսախցիկների միջոցով նույնականացման շրջանակներում ստացված տվյալների հետ:

Վերոնշյալից կարելի է բխեցնել, որ տեսահսկման կամ տեսանկարահանման արդյունքում ստացված անձի տեսապատկերը կարող է համարվել կենսաչափական անձնական տվյալ միայն այն պարագայում, երբ բավարարում է կենսաչափական անձնական տվյալի մշակման վերոնշյալ չափորոշիչներին: Մասնավորապես, տեսախցիկները, որոնք հնարավորություն են տալիս նկարահանել սահմանված տարածքում գտնվող մարդկանց և նույնիսկ նրանց դեմքերը, սակայն թույլ չեն տալիս ինքնաշխատ (ավտոմատ) կերպով վերջիններիս ուղղակիորեն նույնականացնել, չեն մշակում կենսաչափական անձնական տվյալներ:

Ինչ վերաբերում է ՀՀ իրավունքում անձանց տեսապատկերի՝ որպես կենսաչափական անձնական տվյալ որակելու հնարավորությանը, ապա Օրենքի 3-րդ հոդվածի 14-րդ կետի համաձայն՝ կենսաչափական անձնական տվյալներ են անձի ֆիզիկական, ֆիզիոլոգիական և կենսաբանական առանձնահատկությունները բնութագրող տեղեկությունները: Եթե համեմատենք վերոնշյալ սահմանումը GDPR-ով և 108+ կոնվենցիայով տրված սահմանումների հետ, ապա ակնհայտ է, որ Օրենքով տրված կենսաչափական անձնական տվյալը բովանդակային առումով ավելի լայն է, քանի որ չի պահանջում, որ կենսաչափական տվյալը լինի անձին հատուկ տեխնիկական միջոցներով եզակիորեն նույնականացնող տվյալ: Այսինքն՝ Օրենքի տեսանկյունից տեսապատկերը կամ անձի արտաքին տեսքը բնութագրող այլ տվյալներն ինքնաբերաբար կորակվեն կենսաչափական անձնական տվյալներ այնքանով, որքանով թույլ են տալիս ինքնին կամ այլ տվյալների հետ համադրության արդյունքում նույնականացնել անձին:

Տեսապատկերի՝ որպես անձնական տվյալի որակման առանձնահատկությունները բացահայտելուց հետո սույն աշխատանքը կոչված է քննարկելու տեսահսկման միջոցով անձնական տվյալներ մշակելու իրավական հիմքի հիմնախնդիրը:

2. Տեսահսկման միջոցով անձնական տվյալների մշակման իրավական երաշխիքները

Տեսահսկումը՝ որպես անձնական տվյալների մշակում, պետք է իրականացվի անձնական տվյալների պաշտպանության սկզբունքներին համապատասխան: Վերոնշյալ սկզբունքներն ամրագրված են Օրենքով: Դրանց շարքում անկյունաքարային նշանակություն ունեն օրինականության, համաչափության և թափանցիկության սկզբունքները:

2.1. Անձնական տվյալների մշակման օրինականության սկզբունքը

Անձնական տվյալների մշակումը, այդ թվում՝ տեսահսկումը պետք է լինի օրինական: Այս սկզբունքը ենթադրում է, որ տվյալներ մշակողը պարտավոր է մշակել անձնական տվյալներ՝

1. միայն օրինական և որոշակի նպատակներով,
2. համապատասխան իրավական հիմքի հիման վրա:

Այսպես՝ Օրենքի 4-րդ հոդվածի 2-րդ մասով սահմանվում է, որ անձնական տվյալները մշակվում են օրինական և որոշակի նպատակներով և առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով: Տվյալների մշակման նպատակի որոշակիությունը ենթադրում է, որ չի թույլատրվում տվյալների մշակումն անորոշ, ոչ ճշգրիտ կամ վերացական նպատակներով[1]: Օրինական նպատակի պահանջն ակնհայտ է. տվյալները չեն կարող մշակվել ապօրինի նպատակներով: Պետական մարմնի դեպքում տվյալների մշակման նպատակը պետք է լինի օրենքով սահմանված, մասնավոր սուբյեկտների դեպքում՝ օրենքով չարգելված:

[1] Explanatory Report to the Convention for the protection of individuals with regard to the processing of personal data, 2018. p. 20.

Անձնական տվյալների մշակումն օրինական է, եթե այն իրականացվում է համապատասխան իրավական հիմքի հիման վրա: Գործերից մեկով Գործակալությունն արձանագրել է, որ սեփական կամ ընտանիքի կամ գույքի անվտանգության նպատակով ընդհանուր օգտագործման կամ հանրային տարածքների հատվածներ համաչափության սկզբունքի պահպանմամբ տեսահսկելու անհրաժեշտության դեպքում պետք է ապահովել նաև տվյալների մշակման իրավական հիմքի առկայությունը[1]: Այսինքն՝ նույնիսկ օրինական և որոշակի նպատակներով իրականացված տեսահսկումը կարող է խախտել Օրենքը, եթե այն չի իրականացվել պատշաճ իրավական հիմքի հիման վրա:

Օրենքի՝ «Անձնական տվյալները մշակելու օրինականությունը» վերտառությամբ 8-րդ հոդվածի 1-ին մասի համաձայն՝ անձնական տվյալներ մշակելը օրինական է, եթե՝ 1) տվյալները մշակվել են օրենքի պահանջների պահպանմամբ, և տվյալների սուբյեկտը տվել է իր համաձայնությունը, բացառությամբ սույն օրենքով կամ այլ օրենքներով ուղղակիորեն նախատեսված դեպքերի, 2) մշակվող տվյալները ձեռք են բերվել անձնական տվյալների հանրամատչելի աղբյուրներից: Վերոնշյալ հոդվածից բխում է, որ անձնական տվյալների մշակումը կհամարվի օրինական, եթե իրականացվի կամ անձնական տվյալի սուբյեկտի ***համաձայնությամբ***, կամ համաձայնության բացակայության դեպքում մշակումն ***ուղղակիորեն նախատեսված լինի օրենքով***, կամ տվյալները ձեռք բերվեն անձնական տվյալների ***հանրամատչելի աղբյուրներից***[2]:

Որպես կանոն, մասնավոր իրավունքի սուբյեկտների համար անձնական տվյալների մշակման առավել տարածված իրավական հիմքը համաձայնությունն է: ԵՄ իրավունքում որդեգրված և ՀՀ վճռաբեկ դատարանի կողմից հաստատված դիրքորոշման համաձայն՝ «տվյալների սուբյեկտի համաձայնություն» նշանակում է որոշակի և տեղեկացված, ազատ տրված ցանկացած կամահայտնություն, որով տվյալների սուբյեկտը տալիս է իր հավանությունը՝ իր անձնական

[1] N-014/05/22 վարչական գործով Գործակալության որոշումը:

[2] N-017/09/17 վարչական գործով Գործակալության որոշումը:

տվյալները մշակելու համար[1]: Համաձայնությունը կարող է տրվել գրավոր՝ հաստատված ստորագրությամբ, բանավոր, գործողության միջոցով, որն ակնհայտ վկայում է համաձայնության մասին: Թեև համաձայնությունը կարող է տրվել ցանկացած ձևով, սակայն այն պետք է հստակ արտացոլի տվյալների սուբյեկտի կամքը իր անձնական տվյալների մշակման վերաբերյալ: Այսինքն՝ համաձայնությունը պետք է լինի «միանշանակ» և 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[2]: Վերոշարադրյալից հետևում է, որ տվյալների սուբյեկտի կողմից մինչև տեսահսկվող տարածք մտնելը տեսահսկման դաշտում տեղադրված վահանակի միջոցով տեսահսկման մասին տեղեկանալիս տեսահսկվող տարածք մտնելն ինքնին չի կարող համարվել որպես միանշանակորեն տրված համաձայնություն: Բացի այդ, միշտ չէ, որ հնարավոր է ստանալ տվյալների բոլոր սուբյեկտների (տեսահսկվող անձանց) համաձայնությունը (օրինակ՝ առևտրի կետերում՝ հաճախորդների համաձայնությունը, կրթական հաստատություններում՝ ուսանողների համաձայնությունը, բազմաբնակարան շենքերում՝ բոլոր սեփականատերերի համաձայնությունը): Ավելին, անձինք կարող են հրաժարվել իրենց անձնական տվյալները մշակելու համաձայնությունը տրամադրելուց, որի պարագայում տվյալներ մշակողը չի ունենա հնարավորություն տեսահսկման իրականացմամբ պաշտպանելու իր սեփականությունը, անվտանգությունը և այլ օրինական շահերը:

Ինչ վերաբերում է անձի դիմապատկերի և ֆիզիոլոգիական այլ առանձնահատկությունների՝ որպես հանրամատչելի տվյալ որակվելու

[1] Վճռաբեկ դատարան, գործ թիվ ԵԴ/10036/02/19, 10.03.2023 թ.:

[2] Վճռաբեկ դատարան, գործ թիվ ԵԴ/10036/02/19, 10.03.2023 թ.:

հնարավորությանը[1], ապա այն ակնհայտորեն անհիմն է, քանի որ որևէ իրավական ակտով նշված տվյալների հանրամատչելիության ռեժիմ սահմանված չէ, իսկ անձի վարքագծից հնարավոր չէ ակնհայտորեն բխեցնել, որ տեսահսկման տարածք մտնելով վերջինս հանրամատչելի է դարձնում իր տվյալները: Արդյունքում պարզ է դառնում, որ անձնական տվյալները մշակելու համաձայնության բացակայության պարագայում տեսահսկման միակ իրավական հիմքն օրենքով անձնական տվյալների մշակումն ուղղակիորեն նախատեսված լինելն է:

Օրենքի 8-րդ հոդվածով նախատեսված անձնական տվյալների մշակման՝ օրենքով ուղղակիորեն նախատեսված լինելու պահանջը ենթադրում է, որ տվյալների մշակման հնարավորությունը, ինչպես նաև դրա իրականացման պայմանները պետք է սահմանված լինեն օրենսդիր մարմնի կողմից ընդունված նորմատիվ իրավական ակտով՝ օրենքով: Վերոնշյալից բխում է, որ ՀՀ օրենսդիր մարմինը որդեգրել է այն գաղափարը, որ յուրաքանչյուր կոնկրետ դեպքում, տվյալների մշակման մյուս հիմքերի բացակայության պարագայում, անձնական տվյալների մշակման իրավական հիմք նախատեսելու հնարավորությունը վերապահված է բացառապես օրենսդիր մարմնին: Միաժամանակ, ՀՀ Սահմանադրության 6-րդ հոդվածի 2-րդ մասի համաձայն՝ «Սահմանադրության և օրենքների հիման վրա և դրանց իրականացումն ապահովելու նպատակով Սահմանադրությամբ նախատեսված մարմինները կարող են օրենքով լիազորվել ընդունելու ենթաօրենսդրական նորմատիվ իրավական ակտեր»: Այսինքն՝ օրենքով համապատասխան լիազորության առկայության դեպքում անձնական տվյալների մշակումը կարող է նախատեսվել նաև ենթաօրենսդրական ակտերով:

[1] Օրենքի 3-րդ հոդվածի 15-րդ կետը հանրամատչելի անձնական տվյալները սահմանում է որպես տեղեկություններ, որոնք տվյալների սուբյեկտի համաձայնությամբ կամ իր անձնական տվյալները հանրամատչելի դարձնելուն ուղղված գիտակցված գործողությունների կատարմամբ մատչելի են դառնում որոշակի կամ անորոշ շրջանակի անձանց համար, ինչպես նաև այն տեղեկությունները, որոնք օրենքով նախատեսված են որպես հանրամատչելի տեղեկություններ:

Մասնավոր իրավունքի սուբյեկտների կողմից անձնական տվյալներ մշակելու ուղղակիորեն նախատեսող նորմ ամրագրված է ՀՀ աշխատանքային օրենսգրքի 132-րդ հոդվածով, որը, ի թիվս այլ նպատակների, թույլատրում է գործատուին մշակել աշխատողների անձնական տվյալները՝ աշխատողների անձնական անվտանգության ապահովմանը աջակցելու, ինչպես նաև գույքի ամբողջականությունն ապահովելու նպատակով: Սակայն օրենսդրության վերլուծության արդյունքում պարզ է դառնում, որ օրենսդիր մարմինն ուղղակիորեն չի նախատեսել հանրությանը հասանելի վայրերում (առևտրի կետեր, ժամանցային վայրեր), ինչպես նաև սահմանափակ հասանելիություն ունեցող վայրերում (բազմաբնակարան շենքեր, համալսարաններ) մասնավոր իրավունքի սուբյեկտների կողմից տեսահսկում իրականացնելու իրավական հիմքերը:

Հաշվի առնելով այն փաստը, որ օրենսդիր մարմինը մի կողմից մասնավոր իրավունքի սուբյեկտների կողմից տեսահսկման միջոցով անձնական տվյալներ մշակելու համար տվյալների սուբյեկտի կողմից տրված համաձայնության բացակայության դեպքում տվյալների մշակման պատշաճ իրավական հիմք է համարել բացառապես օրենքով ուղղակիորեն նախատեսված լինելը, մյուս կողմից ձեռնպահ է մնացել մասնավոր իրավունքի որոշ սուբյեկտների համար օրենքով ուղղակիորեն տեսահսկման իրականացման հնարավորություն սահմանելուց, կարելի է արձանագրել, որ տվյալ իրավիճակում գործ ունենք օրենսդրական բացի, այսինքն՝ ինչպես բնորոշել է Սահմանադրական դատարանը, իրավակարգավորման ոլորտում գտնվող կոնկրետ հանգամանքների առնչությամբ նորմատիվ պատվիրանի բացակայություն հետ[1]:

Այսպիսով, հաշվի առնելով մասնավոր իրավունքի գերակշռող սուբյեկտների՝ բազմաբնակարան շենքերի սեփականատերերի, մասնավոր ընկերությունների, կրթական հաստատությունների կողմից տեսահսկում իրականացնելու իրավական հիմքի բացակայությունը՝ իրավակիրառ մարմինը կանգնում է երկընտրանքի առջև. առաջնորդվել

[1] Սահմանադրական դատարան, ՍԴՈ–922, 2 նոյեմբերի 2010 թ., կետ 6:

պոզիտիվ իրավունքի կարգադրագրերով՝ չնայած իրավահարաբերության կողմերից մեկի շահերի պաշտպանության անհրաժեշտությանը, թե կողմերից մյուսի լեգիտիմ շահերով՝ անտեսելով օրենսդրի կողմից անձնական տվյալների մշակմանն առաջադրված պահանջները:

Այս համատեքստում ԵՄ անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգը նախատեսում է անձնական տվյալների մշակման առավել լայն իրավական հիմքեր: Մասնավորապես, Կանոնակարգի 6-րդ հոդվածի 1-ին մասի f կետի համաձայն՝ տվյալների մշակումն օրինական է, եթե մշակումն անհրաժեշտ է տվյալներ մշակողի օրինական շահերի պաշտպանության նպատակով, բացառությամբ այն դեպքերի, երբ տվյալների սուբյեկտի հիմնարար իրավունքներն ու ազատությունները գերակայում են այդ շահերի նկատմամբ: Ընդ որում «օրինական շահ» եզրույթը ներառում է ինչպես անձի հիմնարար իրավունքներն ու ազատությունները, այնպես էլ օրենսդրությամբ ուղղակիորեն չսահմանված շահերը[1]: Կանոնակարգի հիմքում ընկած է այն գաղափարը, որ հնարավոր չէ օրենսդրական մակարդակով կարգավորել բոլոր այն դեպքերը, երբ կառաջանա տվյալների մշակման անհրաժեշտություն: Հետևաբար, տվյալների մշակման իրավաչափությունը պետք է որոշվի յուրաքանչյուր կոնկրետ իրավիճակում (case by case analysis):

Վերոնշյալ բանաձևի կիրառումը ՀՀ իրավունքում խնդրահարույց է մի շարք պատճառներով: Նախ, եթե դիտարկենք, որ ինքնին օրինական շահի առկայությունը բավարար հիմք է տվյալներ մշակելու համար՝ առանց օրինական շահի պաշտպանությունը Օրենքում որպես տվյալների մշակման հիմք նախատեսելու, ապա տեսահսկման միջոցով անձնական տվյալների մշակումը կհամարվի օրինական միայն օրենքի contra legem իրավակիրառման արդյունքում: Տվյալ պարագայում առկա կլինի օրենքի կարգավորում (քննարկվող դեպքում՝ չմշակել անձնական տվյալներ առանց օրենսդրությամբ սահմանված իրավական հիմքի), սակայն

[1] **C. Kuner** (ed), The EU Data Protection Regulation: A Commentary. «Oxford university press», 2020, p. 321.

իրավակիրառ մարմինը, տեսահսկման իրավաչափության վերաբերյալ վեճի շրջանակներում ելնելով որոշակի իրավաչափ նպատակներից (քննարկվող դեպքում՝ տեսահսկում իրականացնող անձի իրավունքների պաշտպանության անհրաժեշտությունից), կայացնում է օրենքի կարգավորմանը հակառակ որոշում (քննարկվող դեպքում՝ չի պահանջում տեսահսկում իրականացնող անձից ներկայացնել տվյալների մշակման իրավական հիմքը)[1]: Որպես contra legem իրավակիրառման դրսևորում հնարավոր է գնահատել տեսահսկման իրավաչափությունը՝ անձնական տվյալների մշակման մյուս հիմնական սկզբունքների պահպանումը ստուգելով: Այսպիսի մոտեցումը ենթադրում է, որ՝

1. տեսահսկումը պետք է ունենա օրինական և որոշակի նպատակ (Օրենքի 4-րդ հոդված),

2. տեսահսկմամբ մշակվող անձնական տվյալները պետք է լինեն համաչափ հետապնդվող նպատակին (Օրենքի 5-րդ հոդված),

3. տեսահսկումը պետք է իրականացվի թափանցիկության սկզբունքի հիման վրա, այսինքն՝ տվյալների սուբյեկտները, որոնց տեսապատկերները՝ որպես անձնական տվյալներ, հավաքվելու և այլ կերպ մշակվելու են տվյալներ մշակողների կողմից պետք է լինեն տեղեկացված տեսահսկման մասին (Օրենքի 18-րդ հոդված, 4-րդ մաս)[2]:

Միևնույն ժամանակ, տեսահսկման իրավական հիմքի բացակայությունը պրակտիկայում կարող է հանգեցնել հակասական իրավակիրառ պրակտիկայի. մասնավորապես, դատարանների դիրքորոշումը կարող է տարբերվել ոլորտի լիազոր մարմնի դիրքորոշումից: Բացի այդ, միևնույն դատարանի դատավորները կարող են ունենալ տարբեր դիրքորոշումներ քննարկվող հարցի վերաբերյալ:

Մյուս խնդիրն այն է, որ երբեմն օրինական շահի առկայությունը գնահատելիս հարկավոր է հաշվի առնել ոչ միայն կոնկրետ և օրինական

[1] **Ա. Ղամբարյան**, Contra legem իրավունքի զարգացման դոկտրինը Հայաստանի Հանրապետության անկախացման գործընթացում: «Գիտական Արցախ», № 3(10), 2021, էջ 87:

[2] Անձնական տվյալների մշակման համաչափության և թափանցիկության սկզբունքները կներկայացվեն սույն աշխատանքի հաջորդ ենթապարագրաֆներում:

նպատակի առկայությունը, այլ նաև տեսահսկմանն առարկող անձանց կամահայտնությունը: Այսպիսի իրավիճակի վառ օրինակ է բազմաբնակարան շենքերում տեսահսկման իրականացումը: Այս համատեքստում նախ պետք է պարզել, թե սեփականատերերի ձայների ինչպիսի հարաբերակցությամբ է որոշվում բազմաբնակարան շենքերի մուտքերում, ինչպես նաև ընդհանուր սեփականություն հանդիսացող տարածքներում տեսահսկում իրականացնելը: «Բազմաբնակարան շենքի կառավարման մասին» ՀՀ օրենքի 7-րդ հոդվածի 8-րդ մասը նախատեսում է միաձայն կամ ձայների կեսից ավելիի առկայության դեպքում որոշումների ընդունման պահանջներ՝ կախված քննարկվող հարցից, սակայն նշված հոդվածը որևէ կերպ չի անդրադառնում տեսահսկմանը: Գործակալության կողմից ընդունված տեսահսկման ուղեցույցով սահմանված է, որ *«տեսահսկման համակարգը տեղադրելու համար պահանջվում է ձեռք բերել բնակարանների սեփականատերերի կեսից ավելիի գրավոր համաձայնությունը: Շենքի բոլոր բնակիչները պետք է տեղեկացված լինեն տեսահսկման համակարգ տեղադրված լինելու մասին»:* Սակայն վերոնշյալ ուղեցույցի մեջ առաջարկվող լուծման նորմատիվ նշանակությունը խնդրահարույց է, քանի որ այն ոչ թե կոչված է մեկնաբանելու օրենսդրորեն ամրագրված նորմը, այլ լրացնելու բացակայող նորմը, այսինքն՝ պոզիտիվ իրավանորմի բացակայությունը լրացնել ուղեցուցային կանոնով: Նման պայմաններում տեսահսկման իրականացման համար համաձայնություն չտված անձը կարող է դատարանում վիճարկել տեսահսկման օրինականությունը, այն է՝ իրավական հիմքի բացակայությունը, իսկ դատարանների կողմից նշված հարցի վերաբերյալ կարող է ստեղծվել հակասական իրավակիրառ պրակտիկա:

Վերոգրյալը հաշվի առնելով՝ գտնում ենք, որ օրենսդրական մակարդակով տեսահսկման իրավակարգավորումը չունի ողջամիտ այլընտրանք: Օրենքի մակարդակով տեսահսկման յուրաքանչյուր դեպքի համար պետք է սահմանվեն տեսահսկման իրականացման հիմնական պայմաններ, ինչպիսիք են՝ 1) տեսահսկման թույլատրելի նպատակները,

2) անհրաժեշտության դեպքում՝ այն տարածքները, որոնց տեսահսկումը թույլատրված է, 3) եթե տեսահսկումը կարող է իրականացվել որոշակի կատեգորիայի անձանց համաձայնությամբ (օրինակ՝ բազմաբնակարան շենքի բնակիչների), ապա ձայների նվազագույն քանակը, որոնց առկայության դեպքում տեսահսկումը կհամարվի օրինական:

2.2. Անձնական տվյալների մշակման համաչափության սկզբունքը

Անձնական տվյալների մշակման համաչափության սկզբունքն ամրագրված է Օրենքի 5-րդ հոդվածի 1-ին մասով, որի համաձայն՝ տվյալների մշակումը պետք է հետապնդի օրինական նպատակ, դրան հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ և չափավոր:

Անձնական տվյալների մշակման **պիտանի** լինելը ենթադրում է, որ հետապնդվող նպատակին հասնելու տեսանկյունից տվյալների մշակումն արդյունավետ միջոց է: Այս առումով Գործակալությունն արձանագրել է, որ գույքի անձեռնմխելիության, անվտանգության, այլ անձանց կողմից միջամտությունը կանխելու կամ միջամտությունն արձանագրելու նպատակով այնպիսի տեսահսկում իրականացնելը, որը տեխնիկապես թույլ չի տալիս արձանագրել գույքի նկատմամբ միջամտությունը, թույլ չի տալիս ուղղակիորեն կամ անուղղակիորեն նույնականացնել միջամտողին, ոչ պիտանի կլինի սահմանված նպատակին հասնելու համար և ըստ այդմ խնդրահարույց կլինի անձնական տվյալների մշակման համաչափության սկզբունքի տեսանկյունից[1]:

Նպատակին հասնելու միջոցի **անհրաժեշտությունը** նշանակում է, որ պետք է մշակվեն միայն տվյալների մշակման նպատակի իրականացման համար անհրաժեշտ տվյալները և պետք է արգելվի այնպիսի անձնական տվյալների մշակումը, որոնք անհրաժեշտ չեն տվյալները մշակելու նպատակի համար կամ անհամատեղելի են դրա հետ: Տվյալների մշակման **անհրաժեշտ** լինելը ենթադրում է, որ հետապնդվող նպատակին հասնելու միջոցներից անձնական տվյալների կոնկրետ մշակումը պետք է լինի մարդու իրավունքներին և ազատություններին

[1] N-019/06/22 վարչական գործով Գործակալության որոշումը:

առավել նվազ միջամտող միջոցը, այսինքն այն պետք է լինի առկա բոլոր հնարավոր միջոցների շարքում առավել նվազ միջամտողը[1]: Միաժամանակ, «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիայի փոփոխող արձանագրության/ 108+ կոնվենցիայի 5-րդ հոդվածի 1-ին մասից բխում է, որ անձնական տվյալի մշակման միջոցի չափավոր լինելը նշանակում է, որ պետք է լինի արդար հավասարակշռություն տվյալների մշակմամբ (տեսաձայնագրմամբ) հետապնդվող նպատակի և տեսաձայնագրվող անձի հիմնարար իրավունքների և ազատությունների միջև:

Միջոցի **չափավորության** ներքո նկատի է առնվում, որ անձնական տվյալները պետք է մշակվեն այն նվազագույն քանակով, որն անհրաժեշտ է մշակման օրինական նպատակներին հասնելու համար: Վարույթներից մեկով Գործակալությունը գտել է, որ տեսախցիկով իրականացվող տեսահսկմամբ անձնական տվյալների մշակումը **չափավոր** չէ տեսախցիկով իրականացվող տեսահսկման նպատակին հասնելու համար, քանի որ տեսախցիկը կահավորված չէ այնպես, որ դրա տեսադաշտում ներառվի միայն այն նվազագույն տարածքը, որը համադրելի է անձի սեփականության անվտանգությունն ապահովելու համար, առնվազն, առանց Դիմումատուների տան պատուհանի: Ավելին, տվյալ դեպքում համաչափության սկզբունքի տեսանկյունից հիմնավորված չէ նաև տեսահսկման արդյունքում իրականացվող այնպիսի ձայնագրումը, որը կներառի Դիմումատուների տանը (ներառյալ՝ պատուհանի անմիջական հարևանությամբ տեղի ունեցող) ընդհանուր խոսակցությունները[2]: ՄԻԵԴ-ն արձանագրել է, որ սուպերմարկետում գողության կասկածների հիմքով իրականացված տեսահսկումը իրավաչափ էր և համաչափ, քանի որ սահմանափակված էր դրամարկղերի տարածքով[3]:

[1] Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. Adopted on 29 January 2020, p. 10.

[2] Ն-019/06/22 վարչական գործով Գործակալության որոշումը:

[3] ՄԻԵԴ, *Լոպեզ Ռիբալդան ընդդեմ Իսպանիայի*, գանգատներ թիվ 1874/13 և 8567/13:

Այնուամենայնիվ, հնարավոր է, որ տարածքի տեսահսկումը գերազանցի այն սահմանները, որոնց տեսահսկումն անհրաժեշտ է իրավաչափ նպատակին հասնելու համար: Այս համատեքստում տվյալներ մշակողը պետք է ձեռնարկի տեխնիկական միջոցներ, օրինակ՝ իր սեփականության շրջանակներից դուրս գտնվող տարածքների արգելափակումը կամ պիքսելավորումը[1], որի դեպքում վերոնշյալ տարածքում գտնվող անձանց հնարավոր չի լինի նույնականացնել: Վերոնշյալ միջոցառման կիրառումը բխում է Օրենքի 5-րդ հոդվածի 4-րդ մասով նախատեսված պահանջից, ըստ որի՝ արգելվում է անձնական տվյալների մշակումը, եթե տվյալները մշակելու նպատակին հնարավոր է հասնել ապանձնավորված կերպով:

Անձնական տվյալների մշակման համաչափության սկզբունքի չափանիշներից է նաև տվյալները պահպանելու ժամկետը: Այսպես՝ Օրենքի 5-րդ հոդվածի 5-րդ մասով սահմանված է, որ անձնական տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան անհրաժեշտ է դրանց նախօրոք որոշված նպատակներին հասնելու համար: Գործակալությունը տեսահսկմամբ ստացված տվյալների պահպանման ժամկետին չի անդրադարձել իր իրավակիրառ պրակտիկայում: Փոխարենը, ոլորտում ձևավորված փափուկ իրավունքը նախատեսում է, որ մարդկանց և գույքի նկատմամբ կատարված հանցանքների արձանագրումը շատ դեպքերում տեղի է ունենում դրանց իրագործմանը հաջորդող ժամերում: Ուստի հետապնդվող նպատակի տեսանկյունից 24 ժամը բավարար է տվյալների պահպանման համար, քանի դեռ այդ ժամկետում չի արձանագրվել անձանց կամ գույքին վնաս պատճառելու դեպք: Սակայն օբյեկտիվ և հիմնավոր շարժառիթների առկայության դեպքում տվյալների պահպանման ժամկետը կարող է երկարաձգվել[2]:

[1] Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. Adopted on 29 January 2020, p. 11.

[2] ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալություն, Տեսահսկման ուղեցույց: 2016, էջ 4:

2.3. Անձնական տվյալների մշակման թափանցիկության սկզբունքը

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով ամրագրված է տվյալներ մշակողի՝ իր կողմից մշակվող անձնական տվյալների մշակման, հետևաբար նաև՝ տեսահսկման մասին տվյալների սուբյեկտին տեղեկություններ տրամադրելու պարտականություն: 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[1]: Այնուամենայնիվ, ըստ ՄԻԵԴ-ի դիրքորոշման՝ որոշ դեպքերում տեսահսկման մասին չտեղեկացնելը կարող է իրավաչափ լինել: Մասնավորապես, առևտրի կենտրոնում գողությունները կանխելու և բացահայտելու հիմնավոր կասկածի առկայության դեպքում գործատուի կողմից դրամարկղի տարածքը տեսահսկելն առանց այդ մասին աշխատողներին տեղեկացնելու չի խախտում Կոնվենցիայի 8-րդ հոդվածը[2]:

Օրենքով սահմանված է տվյալներ մշակողների վերոնշյալ պարտականության կատարման երկու դեպք՝ կախված տվյալների մշակման իրավական հիմքից: *Առաջին*՝ Օրենքի 10-րդ հոդվածի 1-ին մասով նախատեսված է, որ տվյալներ մշակողը տվյալների սուբյեկտի համաձայնությունն ստանալու նպատակով ծանուցում է տվյալներ մշակելու մտադրության մասին: Նույն հոդվածի 2-րդ մասով նշվում են այն տեղեկությունները, որոնք պետք է տրամադրվեն տվյալների սուբյեկտին[3]: *Երկրորդ*՝ Օրենքի 18-րդ հոդվածի 4-րդ մասը սահմանում

[1] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, p. 6.

[2] ՄԻԵԴ, *Լոպեզ Ռիբալդան ընդդեմ Իսպանիայի*, գանգատներ թիվ 1874/13 և 8567/13:

[3] Այդ տեղեկություններն են՝ 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

է, որ եթե անձնական տվյալները ստացվել են ոչ տվյալների սուբյեկտից, բացառությամբ օրենքով նախատեսված դեպքերի, ինչպես նաև հանրամատչելի անձնական տվյալների, ապա մշակողը մինչև այդպիսի անձնական տվյալները մշակելը պարտավոր է տվյալների սուբյեկտին տրամադրել սույն հոդվածով նշված տեղեկությունները[1]: Այսպիսով, Օրենքը տվյալներ մշակողներին պարտավորեցնում է տվյալների սուբյեկտին տրամադրել տեղեկություններ՝ անկախ նրանից՝ տեսահսկումն իրականացվում է տվյալների սուբյեկտի համաձայնությամբ, թե առանց դրա:

Տվյալների սուբյեկտի համաձայնության հիման վրա մինչև տեսահսկում իրականացնելը տվյալների մշակման վերաբերյալ տեղեկությունների տրամադրումը իրավական տեսանկյունից խնդիրներ չի առաջացնում: Վճռաբեկ դատարանն արձանագրել է, որ «տեղեկացված լինելը» նշանակում է, որ 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, Օրենքի 10-րդ հոդվածով սահմանված տեղեկությունները պետք է հասանելի, հասկանալի և տեսանելի լինեն տվյալների սուբյեկտի համար, այլ ոչ թե «հասանելի ինչ-որ տեղ»[2]: Որպես օրինակ, Օրենքի

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:

[1] Այդ տեղեկություններն են՝ 1) մշակողի կամ նրա լիազորած անձի (առկայության դեպքում) անվանումը (ազգանունը, անունը, հայրանունը) և գտնվելու կամ հաշվառման (փաստացի բնակության) վայրը, 2) անձնական տվյալները մշակելու նպատակը և իրավական հիմքը, մշակվող տվյալների ցանկը, 3) անձնական տվյալների հավանական օգտագործողների շրջանակը, 4) տվյալների սուբյեկտի՝ սույն օրենքով սահմանված իրավունքները:

[2] Վճռաբեկ դատարան, գործ թիվ ԵԴ/10036/02/19, 10.03.2023 թ.:

10-րդ հոդվածում սահմանված տեղեկությունները կարող են նշված լինել այն փաստաթղթի մեջ, որը ստորագրելով անձը տալիս է իր տվյալները մշակելու համաձայնությունը, կամ կայքում, որտեղ կոնկլյուդենտ գործողություն կատարելով (վանդակի վրա սեղմելով)՝ անձը համաձայնում է, որ իր տվյալները մշակվեն:

Ինչ վերաբերում է այն դեպքերին, երբ տեսահսկումը հիմնված չէ տվյալների սուբյեկտի համաձայնության վրա, ապա Օրենքի 15-րդ հոդվածի 4-րդ հոդվածով ամրագրված է, որ մշակողի կողմից տվյալների սուբյեկտին անձնական տվյալների վերաբերյալ տեղեկությունները պետք է տրամադրվեն հասանելի ձևով և չպետք է պարունակեն տվյալների այլ սուբյեկտի վերաբերող անձնական տեղեկություններ: Այսպիսով, Օրենքը սահմանում է տվյալների սուբյեկտին տեղեկություններ տրամադրելու հիմնական, ելակետային կանոնները, իսկ տեխնիկական միջոցների ընտրության հարցը թողնված է տվյալներ մշակողներին: Գործակալության տարբեր որոշումներում արձանագրվել է, որ տեսահսկվող անձինք պետք է տեղեկացված լինեն տեսահսկման մասին նախքան տեսահսկվող տարածք մտնելը[1]: Գործակալության կողմից մշակված տեսահսկման ուղեցույցի մեջ նշված է, որ տեսահսկում իրականացնող սուբյեկտը **տեսանելի նախազգուշացման միջոցով** պետք է տեսախցիկների նկարահանման դաշտ մտնող բոլոր անձանց տեղեկացնի տեսահսկման մասին[2]:

Տվյալների սուբյեկտին տեսահսկման վերաբերյալ անհրաժեշտ տեղեկությունների փոխանցման իրագործման մասին առավել մանրակրկիտ լուծումներ են առաջարկվել Անձնական տվյալների պաշտպանության եվրոպական խորհրդի կողմից: Հաշվի առնելով տեղեկատվության ծավալը, որը պահանջվում է տրամադրել տվյալների սուբյեկտին, տվյալներ մշակողները կարող են հետևել տեղեկությունների տրամադրման աստիճանական մոտեցմանը, որի համաձայն՝

[1] Գործակալության որոշումը N-014/05/22 վարչական գործով:

[2] ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալություն, Տեսահսկման ուղեցույց: 2016, էջ 4:

տեսահսկման վերաբերյալ ամենակարևոր տեղեկատվությունը պետք է ցուցադրվի հենց նախազգուշացման նշանի վրա, իսկ մյուս տեղեկությունները կարող են տրամադրվել այլ միջոցներով: Մասնավորապես՝ նախազգուշացման նշանը կարող է հղում կատարել ինտերնետային կայքի, հեռախոսահամարի կամ պարունակել QR կոդ, որի միջոցով տվյալների սուբյեկտը հասանելիություն կստանա այդ տեղեկություններին[1]: Հետևելով ստորև նկարագրված մոդելին՝ այնպիսի առաջնային կարևորության տեղեկություններ, ինչպիսիք են մշակողի կամ նրա լիազորած անձի (առկայության դեպքում) անվանումը (ազգանունը, անունը, հայրանունը) և գտնվելու կամ հաշվառման (փաստացի բնակության) վայրը, անձնական տվյալները մշակելու նպատակը և իրավական հիմքը, մշակվող տվյալների ցանկը, պետք է նշված լինեն նախազգուշացման նշանի վրա, մինչդեռ մնացած տեղեկությունները, ինչպիսիք են անձնական տվյալների հավանական օգտագործողների շրջանակը և տվյալների սուբյեկտի՝ սույն օրենքով սահմանված իրավունքները, կարող են տրամադրվել վերոնշված այլ եղանակներով:

Եզրակացություն

Այսպիսով, ամփոփելով սույն աշխատանքում կատարված վերլուծությունները՝ կարելի է եզրակացնել, որ.

1. Տեսահսկման միջոցով իրականացվում է անձնական տվյալների մշակում, եթե դրա արդյունքում հավաքվում են ֆիզիկական անձանց վերաբերյալ այնպիսի տվյալներ, որոնց միջոցով հնարավոր է նրանց ուղղակիորեն կամ անուղղակիորեն նույնականացնել՝ ինչպես դիմապատկերի, այնպես էլ ֆիզիոլոգիական այլ հատկանիշների հիման վրա:

2. Մասնավոր իրավունքի սուբյեկտների կողմից տեսահսկման միջոցով անձնական տվյալների մշակման իրավական հիմքերը գերակշռող

[1] Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. 2020, pp. 26-27.

դեպքերում բացակայում են, քանի որ օրենսդիր մարմնի կողմից դրանք օրենքով ուղղակիորեն նախատեսված չեն: Իրավակիրառ պրակտիկայում իրավական որոշակիության հրամայականից է բխում օրենքով սահմանել մասնավոր իրավունքի սուբյեկտների կողմից տեսահսկում իրականացնելու հնարավորությունն ու պայմանները:

3. «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով ամրագրված համաչափության և թափանցիկության սկզբունքները նախատեսում են անհրաժեշտ և բավարար իրավական երաշխիքներ տեսահսկվող սուբյեկտների իրավունքների պաշտպանության, վերջիններիս և տվյալներ մշակողների շահերի հավասարակշռման համար:

Օգտագործված նորմատիվ իրավական ակտերի և գրականության ցանկ

Օրենսդրություն

1. «Անձնական տվյալների պաշտպանության մասին» ՀՕ-49-Ն ՀՀ օրենք՝ ընդունված 18.05.2015 թ.:

2. ԵՄ Անձնական տվյալների պաշտպանության մասին 2016 թվականի ապրիլի 27–ի թիվ 2016/679 ընդհանուր կանոնակարգ՝ ընդունված 27.04.2016 թ.:

3. Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին ԵԽ կոնվենցիա՝ ընդունված 28.01.1981 թ.:

Դատական և վարչական գործեր

4. ՄԻԵԴ, *Ֆոն Հաննովերն ընդդեմ Գերմանիայի* (թիվ 2), գանգատներ թիվ 40660/08 և 60641/08:

5. ՄԻԵԴ, *Լոպեզ Ռիբալդան ընդդեմ Իսպանիայի*, գանգատներ թիվ 1874/13 և 8567/13:

6. CJEU, Case C-345/17, *Sergejs Buivids vs. Datu valsts inspekcija*, 14 February 2019.

7. CJUE, Case C-708/18, *TK vs. Asociaţia de Proprietari bloc M5A-ScaraA*, 11 December 2019.

8. Վճռաբեկ դատարան, գործ թիվ ԵԴ/10036/02/19, 10.03.2023 թ.:

9. Սահմանադրական դատարան, ՍԴՈ–922, 02.11.2010 թ.:

10. N-014/05/22 վարչական գործով Գործակալության որոշումը:

11. N-017/09/17 վարչական գործով Գործակալության որոշումը:

12. N-019/06/22 վարչական գործով Գործակալության որոշումը:

Խորհրդատվական որոշումներ և կարծիքներ

13. CNIL, Reconnaissance faciale pour un debat à la hauteur des enjeux, 2019.

14. European data protection board, Guidelines 3/2019 on processing of personal data through video devices, 2020.

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

16. European data protection supervisor, Video-surveillance guidelines, 2010.

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

18. ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալություն, Տեսահսկման ուղեցույց, 2016:

Տեսական գրականություն

19. **C. Kuner** (ed), The EU General Data Protection Regulation: A Commentary. «Oxford university press», 2020, 1393 p.

20. **Ա. Ղամբարյան**, Contra legem իրավունքի զարգացման դոկտրինը Հայաստանի Հանրապետության անկախացման գործընթացում: «Գիտական Արցախ», № 3(10), 2021, էջ 86-97:

ГАРАНТИИ (ПРИНЦИПЫ) ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОСРЕДСТВОМ ВИДЕОНАБЛЮДЕНИЯ СУБЪЕКТАМИ ЧАСТНОГО ПРАВА

Аннотация

Системы видеонаблюдения широко используются для защиты жизни людей, имущества, предупреждения и раскрытия преступлений, а также защиты других законных интересов. В то же время видеонаблюдение может привести к незаконной обработке данных о физических лицах. В вышеизложенном контексте, с одной стороны, возникает необходимость защиты интересов лица, осуществляющего видеонаблюдение, а с другой – необходимость сохранения гарантий защиты персональных данных. Если особенности осуществления видеонаблюдения государственными органами уже урегулированы законодательством, то законность осуществления видеонаблюдения частными субъектами права, как правило, при отсутствии специальных норм, оценивается на основании общих правил защиты персональных данных.

Учитывая отсутствие исследований по обсуждаемому вопросу в армянской доктрине, первая часть данной статьи призвана раскрыть специфику обработки персональных данных посредством видеонаблюдения.

Вторая часть работы призвана обсудить установленные законодательством РА гарантии, на которых должна основываться обработка персональных данных частными субъектами права посредством видеонаблюдения.

Ключевые слова: видеонаблюдение, персональные данные, законность, соразмерность, прозрачность.

GUARANTEES (PRINCIPLES) OF PERSONAL DATA PROCESSING THROUGH VIDEO SURVEILLANCE CARRIED OUT BY SUBJECTS OF PRIVATE LAW

Annotation

Video surveillance systems are widely used to protect people's lives, property, prevent and detect crimes and protect other legitimate interests. At the same time, video surveillance can lead to illegal processing of data on individuals. In the above context, on the one hand, there is the need to protect the interests of the person conducting video surveillance, and on the other hand, the necessity to maintain the guarantees of personal data protection. The specifics of the implementation of video surveillance by state bodies are already regulated by legislation, but the legality of video surveillance implemented by private subjects of law, as a rule, in the absence of special norms, is assessed on the basis of the general rules of personal data protection legislation.

Taking into account the lack of studies on the issue discussed in the Armenian doctrine, the first part of this article is intended to reveal the specifics of personal data processing through video surveillance.

The second part of the work is called to discuss the guarantees established by RA legislation, on which the processing of personal data by private subjects of law through video surveillance should be based.

Keywords: video surveillance, personal data, legality, proportionality, transparency.

Հոդվածը հանձնված է խմբագրություն 07.07.2024 թ., տրվել է գրախոսության 02.08.2024 թ., ընդունվել է տպագրության 01.09.2024 թ.: