



Բազմակողմանի
տեղեկատվության ինստիտուտ

ՏՎՅԱԼՆԵՐԻ ԿԱՌԱՎԱՐՈՒՄԸ ՀՀ ՊԵՏԱԿԱՆ ՄԱՐՄԻՆՆԵՐՈՒՄ

Գեորգ Զայրապետյան

ԵՐԵՎԱՆ
2024

ՏՎՅԱԼՆԵՐԻ ԿԱՌԱՎԱՐՈՒՄԸ ՀՀ ՊԵՏԱԿԱՆ ՄԱՐՄԻՆՆԵՐՈՒՄ

Գեորգ Չալոյան

Չեկոյցի հեղինակային իրավունքները պատկանում են
Բազմակողմանի տեղեկատվության ինստիտուտին:
Առանց նախնական թույլտվության զեկոյցի ամբողջական կամ մասնակի
վերահրատարակումը կամ այլ ձևով օգտագործելը արգելվում է:

© Բազմակողմանի տեղեկատվության ինստիտուտ

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

Ներածություն	4
Մեթոդաբանություն	6
Նախնական տեղեկություններ	7
Տվյալները ստանալու կամ ձեռավորելու փուլ Եզրահանգում	10 13
Տվյալների մշակման փուլ Եզրահանգում	14 17
Տվյալներից ազատվելու փուլ Եզրահանգում	18 21
Առաջարկություններ/խորհրդատվականներ	23
Հավելված	25

Ներածություն

Այս վերլուծությունում «պետական մարմիններ» եզրույթի շրջանակում նկատի ունենք իշխանության բոլոր ճյուղերը՝ պետական բոլոր ինստիտուտները եւ մարմինները, այդ թվում՝ պետական կառավարման եւ տեղական ինքնակառավարման մարմինները, պետական կամ համայնքային հիմնարկները եւ կազմակերպությունները:

Գիտության եւ տեխնոլոգիական առաջընթացի պայմաններում մեծանում է նաեւ պետության (պետական մարմինների, տեղական ինքնակառավարման մարմինների, պետական ցանկացած կազմակերպություն) տնօրինության տակ գտնվող եւ մշակվող տվյալների ծավալը: Ընդ որում, խոսքը ոչ թե տեղեկատվության ազատության համատեքստում որեւէ պաշտոնական փաստաթղթի կամ դրվագային մի տեղեկության մասին է, այլ, որպես կանոն, համակարգված, տեւական ժամանակ կամ պարբերաբար մշակվող, ծավալուն տվյալների վերաբերյալ: Պարզ ասած՝ շատանում են.

- տվյալների բազաները՝ որոշակի հատկանիշներով համակարգված տվյալների ամբողջությունը, որը հաճախ կոչվում է նաեւ տվյալների շտեմարան,
- տեղեկատվական համակարգերը՝ տվյալների բազայում ներառված տվյալների, դրանց էլեկտրոնային կամ ոչ էլեկտրոնային եղանակով մշակելու համար կիրառվող տեղեկատվական տեխնոլոգիաների կամ տեխնիկական միջոցների ամբողջությունը:

Պետության կողմից օգտագործվող եւ գրեթե յուրաքանչյուրին հայտնի նման տեղեկատվական համակարգերի եւ տվյալների բազաների օրինակներ են Դատալեքս (DataLex) դատական տեղեկատվական համակարգը, տարբեր պետական մարմիններում իրականացվող տեսահսկման համակարգերը, էլեկտրոնային առողջապահության համակարգը (e-health (Armed)), Ներքին գործերի նախարարության տնօրինության տակ գտնվող շտեմարանները եւ այլն:

Միեւնույն ժամանակ, մի կողմից տվյալների բազաներում եւ/կամ տեղեկատվական համակարգերում մշակվող տվյալներն իրենց ծավալի, մարդկանց այս կամ այն իրավունքին առնչությամբ լրացուցիչ զգայունություն են ձեռք բերում, մյուս կողմից՝ ամերեւույթ (նախնական տպավորությամբ) շատ հաճախ նման տվյալները պատշաճ չեն կառավարվում, եւ տվյալների ոչ պատշաճ կառավարման մասին նշելով՝ նկատի ունենք, որ առկա է լինում որեւէ ինդիք՝

- տվյալները ստանալու կամ ձեւավորելու փուլում,
- տվյալների մշակման, ներառյալ՝ դրանք օգտագործելու փուլում,
- տվյալներից ազատվելու՝ տվյալների մշակումը դադարեցնելու կամ դրանք ոչնչացնելու փուլում:

Ըստ այդմ, սույն վերլուծության հիմքում հետեւյալ երեք պնդումներն են՝

1. պետության կողմից տվյալները ստացվում կամ ձեւավորվում են առանց պատշաճ իրավական հիմքի, ըստ էության՝ անօրինական,
2. եթե անգամ տվյալները ստացվում կամ ձեւավորվում են պատշաճ իրավական հիմքով, ապա չկան դրանց հետ վարվելու կանոններ, ըստ այդմ նաեւ՝ չկա պատշաճ անվտանգության ապահովում,
3. եթե անգամ տվյալները ստացվում կամ ձեւավորվում են պատշաճ իրավական հիմքով, եւ չկան դրանց հետ վարվելու կանոններ եւ ապահովված է դրանց որոշակի անվտանգությունը, ապա կարգավորված չէ, թե վերջում ինչ պետք է լինի այդ տվյալների հետ:

Այս վերլուծության արդյունքում

- կհաստատենք, մասամբ կհաստատենք, մասամբ կհերքենք կամ ամբողջությամբ կհերքենք վերոնշյալ պնդումներից յուրաքանչյուրը,
- կձեւավորենք ամփոփ եզրահանգում պետության կողմից տվյալի կառավարման, այն է՝ տվյալի ամբողջ «կյանքի» կարգավորվածության վերաբերյալ (տվյալի կյանք ասելով՝ նկատի ունենք տվյալի հայտնվելը (ստացվելը կամ ձեւավորվելը) պետության մոտ, տվյալի գոյություն ունենալու ընթացքում դրա հետ կատարվող գործողությունները եւ տվյալից ազատվելը),
- եզրահանգման հիման վրա կներկայացնենք համապատասխան խորհրդատվականներ/առաջարկություններ:

Մեթոդաբանություն

Նախ պետք է փաստել, որ Հայաստանը չունի տվյալների կառավարումը կարգավորող համապարփակ՝ ամբողջական օրենսդրություն: Մասնավորապես, մշակվել եւ այս վերլուծության իրականացման ընթացքում հանրային քննարկման են դրվել «Կիբեռանվտանգության մասին» եւ «Հանրային տեղեկությունների մասին» օրենքների նախագծեր՝ հարակից իրավական ակտերի նախագծերի փաթեթներով: Հենց այս նախագծերով է ակնկալվում կարգավորել մի կողմից Հայաստանում կենսական նշանակության ծառայությունների մատուցման համար կիրառվող տեղեկատվական համակարգերով և/կամ կրիտիկական տեղեկատվական ենթակառուցվածքների անխափան շահագործման, դրանցում մշակվող, շրջանառվող, պահպանվող, փոխանցվող և հրապարակվող տեղեկության հասանելիության, ամբողջականության, գաղտնիության ապահովման, կիբեռմիջադեպերի մասին ծանուցելու, դրանք կանխարգելելու և լուծելու, կիբեռանվտանգության ապահովման ծառայություն մատուցողներին ներկայացվող պահանջների, համապատասխանության գնահատման կամ աուդիտի ինչպես նաև սույն օրենքի պահանջների պահպանման նկատմամբ հսկողության և վերահսկողության իրականացման հետ կապված հարաբերությունները, մյուս կողմից՝ տեղեկությունների հավաքագրման, մշակման, օգտագործման, տվյալների շտեմարանների ստեղծման, դրանց կառավարման, տեղեկությունները հասանելի դարձնելու հետ կապված հարաբերությունները (որոշ բացառություններով):

Այս նախագծերը դեռևս վերջնական չեն, գտնվում են հանրային քննարկումների փուլում, կարող են էականորեն փոփոխվել, ուստի՝ դրանք դեռ չեն կարող այս վերլուծության համար պատշաճ հիմք լինել: Նման պայմաններում ռացիոնալ չի լինի այս վերլուծությամբ ՀՀ պետական մարմիններում տվյալների կառավարման օրենսդրության խորքային եւ համապարփակ ուսումնասիրություն իրականացնել:

Այդուհանդերձ, կան օրենքներ, որոնք նախանշում են պետական մարմինների կողմից տվյալների կառավարման որոշ կանոններ: Այսպես, «Տեղեկատվության ազատության մասին» օրենքը, առարկայացնելով տեղեկատվության ազատության յուրաքանչյուրի սահմանադրական իրավունքը, ի թիվս այլնի՝ պետական մարմինների համար սահմանում է տվյալների մատչելիության, հանրամատչելիության, ինչպես նաև տվյալների մատչելիության սահմանափակման ընդհանուր կանոններ, որոնք անդրադառնում են տվյալների կառավարմանը: Տվյալների կառավարմանն առնչվող դրույթներ նախատեսող մեկ այլ օրենք է «Անձնական տվյալների պաշտպանության մասին» օրենքը, որը կարգավորում է տվյալների առանձին տեսակի՝ անձնական տվյալների մշակման, դրանց նկատմամբ պետական հսկողություն իրականացնելու կարգն ու պայմանները:

Արդյունքում, այս վերլուծությունն իրականացվել է հիմնականում տվյալների կառավարման գործնական օրինակների ուսումնասիրությամբ՝ տվյալների կառավարման պատշաճությունը (ըստ ներածությունում նշված երեք պնդումների) գնահատելով գործող օրենսդրությամբ, հիմնականում՝ «Տեղեկատվության ազատության մասին» եւ «Անձնական տվյալների պաշտպանության մասին» օրենքներով, ըստ անհրաժեշտության նաև՝ ոլորտային այլ իրավական ակտերով:

Գործնական օրինակներն ընտրվել են այնպես, որ մի կողմից լինեն արդիական՝ գործեն եւ կիրառելի լինեն այժմ, լինեն ոչ թե դիպվածային, այլ վերաբերեն անորոշ կամ որոշակի, բայց շատ թվով անձանց, համադրելի լինեն նմանատիպ այլ դեպքերի (օրնիակների) հետ, մյուս կողմից՝ հնարավորություն տան անդրադառնալ տվյալների կառավարման պատշաճությանը տվյալների կյանքի տարբեր փուլերում՝ տվյալները ստանալու կամ ձեւավորելու փուլում, տվյալների մշակման՝ դրանց հետ կատարվող գործողությունների փուլում, տվյալներից ազատվելու՝ դրանք ոչնչացնելու փուլում:

Նախնական տեղեկություններ

Մինչև գործնական օրինակներին անցնելը նախ նշենք որոշ հասկացություններ եւ կանոններ, որոնք անհրաժեշտ են լինելու տվյալների կառավարման պատշաճությունը գնահատելիս:

Սահմանադրության 6-րդ հոդվածը սահմանում է, որ պետական և տեղական ինքնակառավարման մարմիններն ու պաշտոնատար անձինք իրավասու են կատարելու միայն այնպիսի գործողություններ, որոնց համար լիազորված են Սահմանադրությամբ կամ օրենքներով: Սահմանադրական այս կանոնն ունիվերսալ է, եւ, ըստ այդմ, բացառվում է «ինքնագործունեությունը», այն է՝ օրենքով չսահմանված գործողություններ, նաեւ՝ տվյալների կառավարման, տվյալների հետ վարվելու դեպքերում: Սահմանադրական այս կանոնը պետք է մտապահել, քանի որ այն կարմիր գծով անցնելու է այս վերլուծությունում քննարկվող օրինակներով:

«Տեղեկատվության ազատության մասին» օրենքը սահմանում է, որ տեղեկություն են համարվում անձի, առարկայի, փաստի, հանգամանքի, իրադարձության, եղելության, երեւոյթի վերաբերյալ օրենսդրությամբ սահմանված կարգով ստացված եւ ձևավորված տվյալներ՝ անկախ դրանց տնօրինման ձևից կամ նյութական կրիչից (տեքստային, էլեկտրոնային փաստաթղթեր, ձայնագրություններ, տեսագրություններ, լուսաժապավեններ, գծագրեր, սխեմաներ, նոտաներ, քարտեզներ): «Տեղեկատվության» հասկացությունից բխում է, որ պետական մարմիններում ըստ էության պետք է խոսք գնա միայն **օրենսդրությամբ սահմանված կարգով ստացված կամ ձեւավորված** տվյալների մասին, այսինքն, պետական մարմնում առհասարակ չպետք է լինեն տվյալներ, որոնք պետական մարմնում ստացվել կամ ձեւավորվել են օրենսդրությամբ չսահմանված կարգով: Սա պետական մարմիններում տվյալների կառավարման որակը, մասնավորապես՝ տվյալները ստանալու կամ ձեւավորելու փուլի պատշաճությունը գնահատելու չափանիշ է:

«Տեղեկատվության ազատության մասին» օրենքը նախանշում է պետական մարմիններում ձեւավորված կամ ստացված տվյալների ռեժիմի հարցերը: Այսպես,

- տվյալները (տեղեկությունները) ի սկզբանե բաց են, քանի դեռ որեւէ օրենքով չի սահմանվել այդ տվյալների որեւէ գաղտնիք լինելու կարգավիճակը (6-րդ հոդված),
- տվյալի մատչելիությունը (տեղեկության տրամադրումը) կարող է մերժվել միայն տեղեկության՝ գաղտնիք լինելու հիմքով (8-րդ եւ 12-րդ հոդվածներ),
- այն տվյալները, որոնք օրենքով չեն սահմանվել որպես որեւէ գաղտնիք, բաց են եւ հասանելի կամ հարցման հիման վրա (9-րդ հոդված), կամ տեղեկություն տնօրինող պետական մարմնի սեփական նախաձեռնությամբ հրապարակված լինելու միջոցով (7-րդ հոդված):

Վերոնշյալ կանոնները նույնպես պետական մարմիններում տվյալների կառավարման որակը, մասնավորապես՝ տվյալների մշակման՝ դրանց հետ կատարվող գործողությունների փուլի պատշաճությունը գնահատելու չափանիշներ են:

«Անձնական տվյալների պաշտպանության մասին» օրենքը սահմանում է ի թիվս այլնի պետական կառավարման կամ տեղական ինքնակառավարման մարմինների, պետական կամ համայնքային հիմնարկների կամ կազմակերպությունների, կողմից տվյալների մի առանձին տեսակի՝ անձնական տվյալների հետ վարվելու՝ անձնական տվյալներ մշակելու կանոնները: Այս օրենքի համաձայն՝ **անձնական տվյալ է** ֆիզիկական անձին վերաբերող ցանկացած տեղեկություն, որը թույլ է տալիս կամ կարող է թույլ տալ ուղղակի կամ անուղղակի կերպով նույնականացնել անձի ինքնությունը:

Նույն օրենքի համաձայն՝ **անձնական տվյալի մշակում է** համարվում տվյալների հետ կատարվող ցանկացած գործողություն կամ գործողությունների խումբ: Օրենքով սահմանված է նաեւ անձնական տվյալների պաշտպանությունն իրականացնող լիազոր մարմինը (անձնական տվյալների պաշտպանության լիազոր մարմինն Անձնական տվյալների պաշտպանության գործակալությունն է):

«Անձնական տվյալների պաշտպանության մասին» օրենքը սահմանում է անձնական տվյալների մշակման ընդհանուր սկզբունքները եւ կանոնները, որոնք վերաբերում են նաեւ պետական մարմինների կողմից անձնական տվյալների մշակմանը: Դրանք նույնպես տվյալների կառավարման որակը գնահատելու չափանիշներ են: Այդ կանոններից այս վերլուծության համատեքստում մասնավորապես ուշադրության են արժանի հետեւյալները.

- Անձնական տվյալները պետք է մշակվեն օրինական (օրենքով սահմանված կամ օրենքին չհակասող) եւ որոշակի (կոնկրետ) նպատակներով (4-րդ հոդված, օրինականության սկզբունք): Առանց օրինական եւ որոշակի նպատակի անձնական տվյալների մշակումն իրավաչափ չէ:
- Տվյալների մշակման նպատակին հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ եւ չափավոր, տվյալները պետք է մշակվեն օրինական նպատակներին հասնելու համար նվազագույն քանակով եւ ժամկետով, նաեւ տվյալների մշակումն արգելվում է, եթե նպատակին հնարավոր է հասնել ապանձնավորված կերպով (5-րդ հոդված, համաչափության սկզբունք):
- Տվյալների մշակումը պետք է ունենա իրավական հիմք (8-րդ հոդված, անձնական տվյալներ մշակելու օրինականությունը): Առհասարակ, օրենքն անձնական տվյալներն օրինական մշակելու երեք հիմք է նախատեսում՝ անձի **համաձայնությունը**, կամ համաձայնության բացակայության դեպքում տվյալների մշակումն **օրենքով ուղղակիորեն նախատեսված լինելը**, կամ տվյալները անձնական տվյալների **հանրամատչելի աղբյուրներից ձեռք բերված լինելը**: Սակայն, պետական եւ տեղական ինքնակառավարման մարմինների կողմից անձնական տվյալի մշակման հիմքերից որեւէ մեկն ընտրելու հայեցողությունը պետք է մեկնաբանել հնարավորինս նեղ. այն պարագայում, երբ անհրաժեշտ է, որ պետական մարմինն օգտվի անձնական տվյալի մշակման համաձայնության կամ հանրամատչելի աղբյուրից ձեռք բերված լինելու հիմքերից, անհրաժեշտ է, որ այդ հնարավորությունը (հայեցողությունը) նույնպես արտացոլված լինի օրենքով: Նման դիրքորոշում Անձնական տվյալների պաշտպանության գործակալությունը հայտնել է թիվ N-017/09/17 վարչական գործով կայացված որոշմամբ եւ հետագայում վերահաստատել է իր այդ դիրքորոշումը այլ վարչական գործերով կայացրած որոշումներով՝ հաշվի առնելով ՀՀ Սահմանադրության 6-րդ հոդվածը, որի 1-ին մասի համաձայն՝ «Պետական և տեղական ինքնակառավարման մարմիններն ու պաշտոնատար անձինք իրավասու են կատարելու միայն այնպիսի գործողություններ, որոնց համար լիազորված են Սահմանադրությամբ կամ օրենքներով»: Արդյունքում, պետական մարմինների դեպքում անձնական տվյալների մշակումը պետք է այսպես թե այնպես նախատեսված լինի օրենքով:
- Անձնական տվյալները պետք է մշակվեն օրենքի պահանջների պահպանմամբ (4-րդ հոդված, օրինականության սկզբունք): Այլ կերպ ասած՝ անձնական տվյալները պետք է մշակվեն այնպես (այն ձեւով), ինչպես նախատեսված է օրենսդրությամբ:
- Անձնական տվյալներ մշակելու ընթացքում պետք է կիրառվեն գաղտնագրման (անվտանգության ապահովման կազմակերպչական եւ տեխնիկական) միջոցներ՝ անձնական տվյալներ պարունակող տեղեկատվական համակարգերի պաշտպանվածությունը եւ անձնական տվյալներն անօրինական միջամտություններից ապահովելու համար:

Անձնական տվյալների մշակման բոլոր դեպքերում, այդ թվում՝ պետական մարմինների կողմից անձնական տվյալների մշակման դեպքերում, պարտադիր է վերոնշյալ կանոնների միաժամանակյա պահպանումը, իսկ դրանցից որեւէ մեկի խախտումն ինքնին կհանգեցնի անձնական տվյալների պաշտպանության իրավունքի խախտման:

«Անձնական տվյալների պաշտպանության մասին» օրենքն առանձնացրել է անձնական տվյալների որոշ տեսակներ՝ հաշվի առնելով դրանց օբյեկտիվ զգայունությունը եւ մարդու այս կամ այն իրավունքին միջամտության ռիսկը:

- Կենսաչափական անձնական տվյալներ - անձի ֆիզիկական, ֆիզիոլոգիական և կենսաբանական առանձնահատկությունները բնութագրող տեղեկություններ:
Սրանք բիոմետրիկ տվյալներն են, որպես կանոն կարող են ստացվել միայն անմիջականորեն մարդուց, վերաբերում են միայն այդ մարդուն, ինչպես նաեւ սովորաբար թույլ են տալիս մարդուն անսխալական նույնականացնել: Այս առանձնահատկությունների պատճառով կենսաչափական անձնական տվյալները մեծացնում են մարդու ինքնության գողության (identity theft, кража личности) հավանականությունը: Կենսաչափական են, օրինակ, մարդու մատնահետքը, ստորագրությունը, լուսանկարը:
- Հատուկ կատեգորիայի անձնական տվյալներ - անձի ռասայական, ազգային պատկանելությանը կամ էթնիկ ծագմանը, քաղաքական հայացքներին, կրոնական կամ փիլիսոփայական համոզմունքներին, արհեստակցական միությանն անդամակցությանը, առողջական վիճակին ու սեռական կյանքին վերաբերող տեղեկություններ:
Այս տվյալների զգայունությունը հիմնականում պայմանավորված է նրանով, որ հատուկ կատեգորիայի անձնական տվյալները մեծացնում են մարդուն խտրականության ենթարկելու ռիսկը:
- Անձնական կյանքի տվյալներ - անձի անձնական կյանքի, ընտանեկան կյանքի, ֆիզիկական, ֆիզիոլոգիական, մտավոր, սոցիալական վիճակի վերաբերյալ կամ նման այլ տեղեկությունները:
Այս տվյալները հիմնականում արտացոլում են մարդու կյանքի այն մասը, որին մարդը սովորաբար չի ցանկանում հաղորդակից դարձնել ուրիշներին: Անձնական կյանքի տվյալների օբյեկտիվ զգայունությունը պայմանավորված է հենց մարդու մասնավոր եւ ընտանեկան կյանքի անձեռնմխելիությանը միջամտության ռիսկով:

«Անձնական տվյալների պաշտպանության մասին» օրենքը 23-րդ հոդվածով սահմանել է, որ անձնական տվյալներ մշակողը մինչև կենսաչափական կամ հատուկ կատեգորիայի անձնական տվյալներ մշակելը պարտավոր է անձնական տվյալների պաշտպանության լիազոր մարմինն ծանուցել տվյալներ մշակելու մտադրության մասին: Ծանուցումն տվյալների մշակման վերաբերյալ 8 խումբ տեղեկություններ պարունակող փաստաթուղթ է (տե՛ս <https://www.moj.am/storage/uploads/Tsanucman-nmush.pdf>), եւ նման ծանուցում ներկայացնելու պարտականություն ունեն նաեւ այն պետական մարմինները, որոնք կենսաչափական կամ հատուկ կատեգորիայի անձնական տվյալներ մշակելու մտադրություն ունեն:

Տվյալները ստանալու կամ ձեւավորելու փուլ

➤ Օրինակ 1

2023 թվականի փետրվարի 27-ին Արդարադատության նախարարության կայքում <https://moj.am/article/3513> հղմամբ հրապարակվել է «Պրոբացիայի ծառայությունում տեղադրվել է մատնահետքի եւ տեսապատկերի միջոցով անձին նույնականացնելու սարքավորում, կիրառվում է տնային կալանք և վարչական հսկողություն խափանման միջոցը. Արդարադատության նախարար Գրիգոր Մինասյանն այցելել է Պրոբացիայի ծառայություն՝ 2023թ.-ին նախատեսված աշխատանքները քննարկելու նպատակով» վերտառությամբ տեղեկատվական կյուբ, որում, ի թիվս այլնի, նշվում է, որ Պրոբացիայի ծառայության անցակետում տեղադրվել է մատնահետքի եւ տեսապատկերի միջոցով անձին նույնականացնելու սարքավորում, որը հնարավորություն է տալիս նույնականացնել շահառուին եւ արձանագրել վերջինիս՝ Պրոբացիայի ծառայություն ներկայանալու փաստը: Նյութում նշված է, որ այդ սարքավորման միջոցով ապահովվում է պրոբացիայի ծառայողների ժամանակի եւ ռեսուրսների խնայողություն, ինչպես նաեւ նվազեցվում են կոռուպցիոն ռիսկերը:

«Անձնական տվյալների պաշտպանության մասին» օրենքի իմաստով անձի մատնահետքը եւ տեսապատկերը կենսաչափական անձնական տվյալներ են: Ըստ այդմ, Պրոբացիայի ծառայությունը մատնահետքի եւ տեսապատկերի միջոցով անձին նույնականացնող սարքերով իրականացնում է կենսաչափական անձնական տվյալների մշակում: Սակայն հարց է, թե որքանով է Պրոբացիայի ծառայությունը կենսաչափական տվյալների մշակումն իրականացնում օրենսդրությանը համապատասխան:

Ոչ պրոբացիայի «Պրոբացիայի մասին» օրենքում, ոչ էլ Պրոբացիայի ծառայության գործունեությունը կարգավորող այլ օրենքներում չկա որեւէ դրույթ, որը նման կենսաչափական տվյալներ ձեւավորելու, դրանք մշակելու իրավունք է սահմանվել Պրոբացիայի ծառայության համար:

Արդյունքում, Պրոբացիայի ծառայությունում մարդու մատնահետքը եւ տեսապատկերը մշակվում են առանց պատշաճ իրավական հիմքի, ըստ էության՝ անօրինական, իսկ այդ տվյալների մշակմամբ տեղեկությունները չեն ստացվում կամ ձեւավորվում օրենսդրությամբ սահմանված կարգով:

Այս օրինակը պատկերավոր ներկայացնում է, թե ինչպես են տվյալների հետ գործողությունները հենց ամենասկզբից՝ տվյալների ստացման կամ ձեւավորման պահից, իրականացվում օրենսդրության խախտմամբ:

➤ Օրինակ 2

2023 թվականի հուլիսի 13-ին «Իրազեկ քաղաքացիների միավորում» հասարակական կազմակերպության փաստերի ստուգման fip.am հարթակում՝ <https://fip.am/23087> հղմամբ հրապարակվել է ««Սառը» ավտոբուսից Փաշինյանի տեսագրությունը ապօրինաբար է տարածվել» վերտառությամբ կյուբը, որտեղ բարձրացվել է Երեւանի քաղաքային ավտոբուսում տեղադրված տեսախցիկով իրականացված տեսագրությունը համացանցում տարածելու իրավաչափությունը (տվյալների արտահոսքի): Այս հրապարակումը Անձնական տվյալների պաշտպանության լիազոր մարմնում վարույթի առիթ է դարձել, որով քննարկվել է Երեւան քաղաքի հանրային տրանսպորտում իրականացվող տեսահսկման (անձնական տվյալների մշակման)

համապատասխանությունն «Անձնական տվյալների պաշտպանության մասին» օրենքի պահանջներին:

Վարույթի արդյունքում 2023 թվականի օգոստոսի 17-ին կայացրած որոշմամբ Անձնական տվյալների պաշտպանության գործակալությունը որոշել է, որ Երեւանի քաղաքային տրանսպորտում տեղադրված տեսախցիկով մարդկանց տեսապատկերը մշակվում է առանց պատշաճ իրավական հիմքի՝ «Անձնական տվյալների պաշտպանության մասին» օրենքի խախտմամբ: Եւ իսկապես, «Երեւան քաղաքում տեղական ինքնակառավարման մասին» օրենքում կամ Երեւան համայնքի գործունեությանն առնչվող այլ օրենքներում հնարավոր չի եղել գտնել Երեւանի հանրային տրանսպորտում տեսախցիկներով անձանց տվյալների մշակման պատշաճ իրավական հիմք:

Արդյունքում, Երեւանի քաղաքապետարանը հանրային տրանսպորտում տեղադրված տեսախցիկներով մարդկանց տեսապատկերը մշակում է առանց պատշաճ իրավական հիմքի, ըստ Էուռլայն՝ անօրինական, իսկ այդ տվյալների մշակմամբ տեղեկությունները չեն ստացվում կամ ձեւավորվում օրենսդրությամբ սահմանված կարգով:

Պետք է նշել, որ Երեւանի քաղաքապետարանը Վարչական դատարանում բողոքարկել է անձնական տվյալների պաշտպանության լիազոր մարմնի վերոնշյալ որոշումը: Դատարանի որոշման հրապարակման օր է նշանակվել 2024 թվականի մայիսի 2-ը (տե՛ս https://datalex.am:443/?app=AppCaseSearch&case_id=38562071809988339):

➤ **Օրինակ 3**

2017 թվականին «Իրազեկ քաղաքացիների միավորում» հասարակական կազմակերպության գրության առիթով Անձնական տվյալների պաշտպանության լիազոր մարմինն անդրադարձել էր Ոստիկանության ծառայողների համազգեստի վրա առկա անհատական տեսախցիկներով իրականացվող տեսահսկմամբ մշակվող տվյալների, մասնավորապես՝ տեսագրությունների հրապարակման իրավաչափությանը:

Վարույթով կայացրած որոշմամբ Անձնական տվյալների պաշտպանության գործակալությունը պարզել էր, որ առկա էին միայն ճանապարհապարեկային ծառայության արդյունավետության բարձրացման, ոստիկանության ծառայողների գործունեության օրինականության նկատմամբ պատշաճ հսկողություն ապահովելու նպատակով տեսաձայնագրում իրականացնելու իրավական հիմքեր, այնինչ ոստիկանության ծառայողների կողմից իրենց համազգեստներին ամրացված տեսախցիկներով իրենց հետ հաղորդակցվող անձանց տեսաձայնագրելու պատշաճ իրավական հիմքեր չկային:

Արդյունքում, Ոստիկանությունը ծառայողների համազգեստներին ամրացված տեսախցիկներով մարդկանց տեսապատկերը մշակում էր առանց պատշաճ իրավական հիմքի, ըստ Էուռլայն՝ անօրինական, իսկ այդ տվյալների մշակմամբ տեղեկությունները չեն ստացվում կամ ձեւավորվում օրենսդրությամբ սահմանված կարգով: Նշված վարույթով կայացված որոշումը օրենսդրական փոփոխությունների առիթ դարձավ, մասնավորապես, «Ոստիկանության մասին» օրենքի 22-րդ հոդվածով սահմանվեց շարժական (ծառայողի համազգեստին ամրացվող, ծառայողի ձեռքում կամ տրանսպորտային միջոցում գտնվող) տեսաձայնագրող կամ լուսանկարահանող սարքեր օգտագործելու իրավունքը, նման տեսահսկմամբ ձեւավորված տվյալների մշակման նպատակները, տվյալների մշակման պայմանները, այդ թվում՝ պահպանման ժամկետները, հրապարակայնությունը, տվյալներին հասանելիությունը եւ այլն:

➤ **Օրինակ 4**

2018 թվականին արդեն մշակված եւ պատրաստ էր Էլեկտրոնային առողջապահության e-health համակարգը (ArMed): Ակնկալվում էր, որ համակարգը պետք է փոխկապակցվի տվյալների պետական այլ շտեմարանների, այդ թվում՝ բնակչության պետական ռեգիստրին՝ պացիենտների անձնագրային տվյալները թվային եղանակով ինքնաշխատ ստանալու եւ ըստ այդմ մշակվող տվյալների արդիականության եւ հավաստիության պայմաններում անձին (բուժառուի) ճիշտ նույնականացնելու համար:

Այդուհանդերձ, նախ համակարգի ներդրման կապակցությամբ իրականացվող հանրային քննարկումների ընթացքում, ապա նաեւ առանձին որոշմամբ Անձնական տվյալների պաշտպանության լիազոր մարմինն առարկեց Էլեկտրոնային առողջապահության e-health համակարգում տվյալների նման մշակման դեմ՝ ի թիվս այլնի համարելով, որ տվյալների նման մշակումը նկարագրված չէ որեւէ օրենքով:

Այստեղ կարող էր հարց առաջանալ, թե ինչպե՞ս է ստացվում, որ բժշկական հաստատությունները բուժառուի ամբուլատոր քարտի վարման շրջանակներում ունեն նման տվյալներ մշակելու իրավասություն, բայց Էլեկտրոնային առողջապահության համակարգի շրջանակներում ոչ: Խնդիրն այն էր, որ Էլեկտրոնային առողջապահության համակարգի շրջանակներում տվյալների մշակման ձեւն այնպես էր փոխվում, որ փոխվում էին նաեւ տվյալների մշակման պայմանները: Այսպես, թղթային տարբերակով ամբուլատոր քարտերի վարման շրջանակում մշակվող տվյալներին վերաբերելի չէին համացանցային ռիսկերը (կիբեռ ռիսկերը), թղթային տարբերակով մշակվող տվյալները ունեին դրանց հասանելիության այլ հնարավորություններ, քան առկա էր Էլեկտրոնային եղանակով եւ այլն: Իսկ այդ պահին գործող վերաբերելի օրենսդրությամբ հենց Էլեկտրոնային եղանակով (Էլեկտրոնային առողջապահական համակարգի միջոցով) անձնական տվյալների մշակումը կարգավորված չէր:

Արդյունքում, Էլեկտրոնային առողջապահության e-health համակարգում տվյալների մշակումն ակնկալվում էր իրականացնել օրենքով չնախատեսված ձեւով՝ առանց տվյալների նման մշակման պատշաճ իրավական հիմքի, ըստ էության՝ անօրինական: Անձնական տվյալների պաշտպանության գործակալության որոշումն օրենսդրական փոփոխությունների առիթ դարձավ, մասնավորապես, «Բնակչության բժշկական օգնության եւ սպասարկման մասին» օրենքը 2020 թվականի մայիսին շարադրվեց նոր խմբագրությամբ՝ ի թիվս այլնի սահմանելով նաեւ Էլեկտրոնային առողջապահության համակարգը եւ դրանում տվյալների մշակման կանոնները:

➤ **Օրինակ 5**

2022 թվականի մարտի 18-ին Արդարադատության նախարարության կայքում <https://moj.am/article/3107> հղմամբ հրապարակվել էր ««Արմավիր» ԶԿԶ-ում ներդրվել է ավելի քան 400 տեսախցիկից բաղկացած ամբողջական տեսահսկման համակարգ» վերտառությամբ տեղեկատվական նյութ, որում նկարագրվում էր «Արմավիր» քրեակատարողական հիմնարկում Զրեակատարողական ծառայության ղեկավարի եւ միջազգային գործընկերների հետ միասին Արդարադատության նախարարի եւ փոխնախարարի կատարած շրջայցը եւ ծանոթացումը գործարկված տեսահսկման համակարգին եւ, ի թիվս այլնի, նշվում էր, որ տեսահսկման համակարգի տեղադրման նպատակն է ապահովել քրեակատարողական հիմնարկի թափանցիկ աշխատանքը:

«Անձնական տվյալների պաշտպանության մասին» օրենքի իմաստով անձի տեսապատկերը կենսաչափական անձնական տվյալ է. իսկ այնպիսի տեսահսկումը, որի տեսադաշտում հայտնվում են մարդիկ՝ անձնական տվյալների մշակում է: Ըստ այդմ,

Նախարարության հրապարակած կյուրթում խոսվում էր ըստ էության Քրեակատարողական ծառայության կողմից տեսահսկման միջոցով անձնական տվյալների մշակման մասին:

Տվյալների նման մշակման կապակցությամբ Անձնական տվյալների պաշտպանության լիազոր մարմնի նախաձեռնությամբ իրականացված որոշ աշխատանքային քննարկումների արդյունքում պարզվեց, որ քրեակատարողական հիմնարկում իրականացվող տեսահսկման միջոցով անձնական տվյալների մշակումն իրականացվում էր առանց պատշաճ իրավական հիմքի, ըստ էության՝ անօրինական, իսկ այդ տվյալների մշակմամբ տեղեկությունները չեն ստացվում կամ ձեւավորվում օրենսդրությամբ սահմանված կարգով: Նույն ժամանակահատվածում՝ 2022 թվականին, ընթանում էին Քրեակատարողական նոր օրենսգրքի մշակման աշխատանքները: Արդյունքում, քրեակատարողական հիմնարկում էլեկտրոնային հսկողության (տեսահսկման) համակարգի եւ դրա արդյունքում տվյալների մշակման հարցերը ներառվեցին մշակվող օրենսդրությունում, մասնավորապես, 2022 թվականի հուլիսի 1-ին ուժի մեջ մտած Քրեակատարողական նոր օրենսգրքի 72-րդ հոդվածով սահմանվեց քրեակատարողական հիմնարկներում էլեկտրոնային հսկողությունը եւ կարգավորվեց էլեկտրոնային հսկողության ընթացքում տվյալների կառավարման ամբողջ ընթացքը՝ տվյալների մշակման նպատակները, պայմանները, այդ թվում՝ պահպանման ժամկետները, իսկ օրենսգրքի հիման վրա Կառավարության՝ 2023 թվականի մարտին ընդունված որոշմամբ սահմանվեցին նաեւ էլեկտրոնային հսկողություն իրականացնող անձանց ցանկը, դրա արդյունքով ստացված տվյալների օգտագործման, պահպանման եւ ոչնչացման պայմանները, ստացված տվյալներին ծանոթանալու իրավունք ունեցող պաշտոնատար անձանց ցանկը, տեսանկարահանող, լուսանկարահանող, տեսաձայնագրող տեխնիկական միջոցների ցանկն ու դրանց կիրառման կարգը:

Եզրահանգում

Տվյալներ ստանալը կամ դրանք ձեւավորելն օրենսդրությամբ սահմանված կարգով եւ պատշաճ իրավական հիմքով իրականացնելու պահանջն ինքնանպատակ չէ. բացի օրինականության ապահովումը, դրանով է պայմանավորված նաեւ տվյալների կառավարման հաջորդ փուլերի պատշաճությունը: Մասնավորապես, վերելում նկարագրված օրինակներում տվյալների ձեւավորման կամ ստացման իրավական հիմքի ու առհասարակ կարգավորման բացակայության պայմաններում բազմաթիվ հարցեր են առաջանում այդ տվյալների կարգավիճակի, այլ անձանց հասանելիության, դրանց պահպանման:

Վերոնշյալ օրինակները վկայում են, որ պետությունը ստացվող կամ ձեւավորվող տվյալների դեպքում հաճախ չի ապահովում պատշաճ իրավական հիմքեր, բազմաթիվ եւ ծավալուն տվյալներ ստացվում կամ ձեւավորվում, եւ հետագայում մշակվում են իներցիայով, առանց պատշաճ իրավական կարգավորման: Վերոնշյալ օրինակները նաեւ վկայում են, որ երբեմն պետական մարմիններում ստացվող կամ ձեւավորվող տվյալների համար պետությունը պատշաճ իրավական հիմք ապահովել է ոչ թե նախապես՝ մինչեւ տվյալները ստանալը կամ ձեւավորելը, այլ հետահայաց (post factum)՝ քաղաքացիական հասարակության եւ լիազոր մարմնի մասնագիտական «հուշումներից» հետո: Ըստ այդմ, **պետությունը չունի տվյալների կառավարման՝ տվյալներ ստանալու կամ ձեւավորելու փուլին վերաբերելի այնպիսի ընդհանուր քաղաքականություն, որը կապահովի յուրաքանչյուր նոր տվյալի ստացման կամ ձեւավորման պատշաճ իրավական հիմք՝ անկախ նրանից, թե որ պետական մարմնի մասին է խոսքը եւ անկախ պետական մարմիններում որոշում կայացնող անձանց փոփոխություններից:**

Տվյալների մշակման փուլ

➤ Օրինակ 1

Այս վերլուծության «Տվյալները ստանալու կամ ձեւավորելու փուլ» բաժնի 1-ին օրինակում նշեցինք Պրոբացիայի ծառայությունում մարդու մատնահետքը եւ տեսապատկերը մշակելու մասին: Այդ օրինակը խնդիրներ ունի ոչ միայն նման տվյալներ ստանալու կամ ձեւավորելու իրավական հիմքերի բացակայության առումով, այն նաեւ այն համատեքստում, թե **փաստացի** ինչպես է իրականացվել տվյալների նման մշակումը:

Այսպես, այս վերլուծության «Նախնական տեղեկություններ» բաժնում նշեցինք, որ «Անձնական տվյալների պաշտպանության մասին» օրենքը 23-րդ հոդվածով սահմանել է, որ անձնական տվյալներ մշակողը մինչև կենսաչափական կամ հատուկ կատեգորիայի անձնական տվյալներ մշակելը պարտավոր է անձնական տվյալների պաշտպանության լիազոր մարմինն ծանուցել տվյալներ մշակելու մտադրության մասին: Միաժամանակ նշեցինք, որ «Անձնական տվյալների պաշտպանության մասին» օրենքի իմաստով անձի եւ՛ մատնահետքը, եւ՛ տեսապատկերը կենսաչափական անձնական տվյալներ են: Չեղարկվելով, եթե անգամ նման տվյալների մշակումն ունենա իրավական պատշաճ հիմք, միեւնույն է, օրենսդրության իմպերատիվ պահանջն է, որ մինչև կենսաչափական տվյալների մշակումն իրականացնելը՝ տվյալներ մշակողը պետք է ներկայացրած լինել օրենքով սահմանված համապատասխան ծանուցում՝ նման մտադրության մասին:

Պրոբացիայի ծառայությունում մատնահետքի եւ տեսապատկերի միջոցով անձին նույնականացնելու մասին տեղեկությունը հրապարակվել է 2023 թվականի փետրվարի 27-ին, հետեւաբար, «Անձնական տվյալների պաշտպանության մասին» օրենքին համապատասխան եւ ըստ այդմ, տվյալների մշակումն օրենսդրությամբ սահմանված պահանջների պահպանմամբ իրականացրած լինելու համար համապատասխան ծանուցումն Անձնական տվյալների պաշտպանության լիազոր մարմինին պետք է ներկայացվեր առնվազն մինչ այդ: Այդուհանդերձ, նման ծանուցում օրենքով սահմանված ժամկետում Անձնական տվյալների պաշտպանության գործակալությունը չի ստացել:

Արդյունքում, անգամ եթե առկա լինել Պրոբացիայի ծառայությունում մարդու մատնահետքը եւ տեսապատկերը մշակելու պատշաճ իրավական հիմք, միեւնույն է, տվյալների կառավարումը տվյալների մշակման փուլում պատշաճ չի իրականացվել, մասնավորապես, տվյալների մշակման կապակցությամբ չեն իրականացվել այն գործողությունները, որոնք պետք է իրականացվեին:

➤ Օրինակ 2

Ծավալուն տվյալներ ստացվում եւ ձեւավորվում են դատավարությունների ընթացքում դատավարական իրավական ակտերի հիման վրա, դատական գործերի քննության ընթացքում: Դատական ակտերը կարող են պարունակել բազմաթիվ եւ անորոշ շրջանակի տեղեկություններ՝ անձնական եւ ոչ անձնական տվյալներ, տեղեկություններ մարդկանց, կազմակերպությունների, առարկայի, փաստի, հանգամանքների, հրադարձությունների, եղելությունների, երեւույթների վերաբերյալ: Միաժամանակ, որպես արդար դատաքննության իրավունքի մաս եւ երաշխիք՝ ՀՀ օրենսդրությամբ սահմանված է դատական վարույթի հրապարակայնությունը: Այդ համատեքստում ՀՀ դատական օրենսգիրքը դատական վարույթի հրապարակայնությանը վերաբերող 11-րդ

հողվածով սահմանել է, որ դատական ատյանում վարույթը եզրափակող դատական ակտերը, իսկ օրենքով կամ Բարձրագույն դատական խորհրդի որոշմամբ նախատեսված դեպքերում նաեւ այլ դատական ակտերը ենթակա են պարտադիր հրապարակման դատական իշխանության պաշտոնական կայքում: Դատական վարույթը կամ դրա մասը դռնփակ անցկացվելու դեպքում դատական իշխանության կայքում հրապարակվում է եզրափակիչ դատական ակտի եզրափակիչ մասը, եթե այն չի պարունակում օրենքով պահպանվող գաղտնիք: Դատական իշխանության պաշտոնական կայքում հրապարակվում են նաեւ գործի եւ դրա ընթացքի վերաբերյալ տեղեկություններ: Այսպես, ՀՀ դատական օրենսգրքի 11-րդ հոդվածը պատշաճ հրավական հիմք է ստեղծում դատական վարույթի վերաբերյալ տարբեր տվյալների հրապարակման համար:

Այժմ անդրադառնանք Դատական օրենսգրքով նախատեսված տվյալների հրապարակման պայմաններից մեկին՝ այն հարթակին, որտեղ դրանք հրապարակվում են: Դատական օրենսգրքի սահմանում է այդ տվյալների պետք է հրապարակվեն դատական իշխանության պաշտոնական կայքում: Հասարակությունում որպես «Դատական տեղեկատվական համակարգ» ընկալվում է www.datalex.am հղմամբ գործող հարթակը, որտեղ հասանելի են դատական վարույթի վերաբերյալ Դատական օրենսգրքով սահմանված տեղեկությունները: Անհրաժեշտ է Է արձանագրել, որ www.datalex.am հղմամբ գործող «Դատական տեղեկատվական համակարգ»-ը ՀՀ կառավարության www.e-gov.am կայքի բաժին է (տե՛ս ՀՀ կառավարության՝ 2012 թվականի օգոստոսի 30 -ի N 1104-Ն որոշում), այնինչ ՀՀ դատական օրենսգրքի 18-րդ հոդվածի համաձայն՝ դատական իշխանության պաշտոնական կայքը ոչ թե www.datalex.am-ն է, այլ www.court.am կայքն է:

Պետք է նշել, որ դատական իշխանության կայքում <http://acts.court.am/> հղմամբ գործում է www.datalex.am հարթակին նույնական հարթակ, որտեղ նույնությամբ արտագրված է www.datalex.am-ի բովանդակությունը: Այդուհանդերձ, անկախ նրանից, թե էլ որ հարթակներում են հրապարակված Դատական օրենսգրքով նախատեսված տվյալները՝ փաստ է, որ այդ տվյալները հրապարակվում են www.datalex.am-ում եւ փաստ է, որ www.datalex.am-ը Դատական օրենսգրքով այդ տվյալների հրապարակման համար նախատեսված հարթակ չէ: www.datalex.am տվյալների մշակման խնդրին արձանագրել է նաեւ Անձնական տվյալների պաշտպանության գործակալությունը՝ «Իրավական հետազոտությունների հայկական կենտրոն» հասարակական կազմակերպության ղեկավարի առիթով հարուցված վարույթի արդյունքում 2019 թվականին կայացրած որոշմամբ:

Այդուհանդերձ, այս վերլուծությունը հրապարակելու պահին խնդիրը դեռեւս վերացված չէ:

Արդյունքում, տվյալ դեպքում թե՛եւ առկա է դատական վարույթի հրապարակայնության շրջանակներում տվյալների հրապարակման պատշաճ հրավական հիմք, սակայն տվյալների կառավարումը տվյալների մշակման փուլում պատշաճ չի իրականացվել, մասնավորապես, տվյալները հրապարակվում են այնպիսի հարթակում (տվյալների հետ կատարվում են այնպիսի գործողություններ), որը նախատեսված չէ Դատական օրենսգրքով:

➤ **Օրինակ 3**

Հաճախ տվյալների մշակման խնդիրները կարող են կապված լինել նոր տեխնոլոգիաների եւ գործիքների ինտեգրիցիոն կիրառմամբ, երբ նման գործիքները

կիրառվում են առանց պատշաճ կարգավորման կամ երբ նման գործիքների կիրառում տվյալների մշակման փուլում առհասարակ նախատեսված չէ: Նման մի դեպք Անձնական տվյալների պաշտպանության լիազոր մարմնում քննարկման առարկա դարձավ 2021 թվականի սկզբում եւ կապված էր սոցիալական ցանցերի եւ կայքերի օգտագործման հետ:

Այսպես, 2020 թվականի դեկտեմբերին Լոռու մարզի Սպիտակի համայնքապետարանն իր ֆեյսբուքյան էջում գրառում էր կատարել Սպիտակի բնակիչներից երկուսի մասին՝ ներկայացնելով աղետի գոտու (խոսքը 1988 թվականի երկրաշարժի մասին է) քաղաքային բնակավայրերում պետական աջակցությամբ իրականացվող բնակարանային ապահովման ծրագրի շրջանակներում այդ բնակիչներին տների հատկացնելու մասին տեղեկություններ:

Տեղական ինքնակառավարման մարմնի կողմից համացանցում նման տվյալներ հրապարակելու իրավաչափությունը քննարկելիս՝ Սպիտակի համայնքապետարանն ի թիվս այլնի կշեղ էր, որ քաղաքացիներին բնակարան հատկացնելու մասին տեղեկությունները հրապարակվում են նաեւ ՀՀ քաղաքաշինության կոմիտեի կայքում: Միաժամանակ պարզվեց, որ նման տվյալների հրապարակման իրավական միակ հիմքը ՀՀ կառավարության՝ 1999 թվականի հունիսի 10-ի թիվ 432-Ն որոշմամբ հաստատված կարգի 15-րդ կետն է, որի համաձայն՝ բնակարանների բաշխման հրապարակայնությունն ապահովելու նպատակով քաղաքացիներին բնակարան հատկացնելու մասին որոշումները հրապարակվում են տեղական մամուլում:

Արդյունքում, ստացվում էր, որ մի կողմից Սպիտակի համայնքապետարանը վերահրապարակել էր այն, ինչն արդեն իսկ հրապարակված էր Քաղաքաշինության կոմիտեի կայքում, մյուս կողմից Կառավարության որոշմամբ սահմանված էր այդ տեղեկությունների հրապարակման կանոնը: Սակայն, միեւնույն է առկա էր խնդիր. բանն այն է, որ մի կողմից այս դեպքում հստակ սահմանված էր տվյալների հրապարակման ձեւը՝ տեղական մամուլում, եւ կառավարության որոշման մեջ որեւէ խոսք չկար համացանցում պետական մարմնի կայքում այդ տեղեկությունների հրապարակման մասին: Մյուս կողմից, համացանցում բոլորի համար որոնողական համակարգերով մշտապես հասանելի եղանակով տվյալների հրապարակման պայմանները էականորեն տարբերվում են համայնքային թերթում նույն տեղեկության հրապարակման պայմաններից՝ համացանցում հրապարակված տվյալներին վերաբերելի է կիբեռհարձակման ռիսկը, տվյալները հասանելի են անորոշ թվով անձանց համար եւ առանց ժամկետի սահմանափակման եւ այլն: Որպես հետեւան՝ Քաղաքաշինության կոմիտեն իր կայքից հեռացրեց անձանց մասին տվյալները:

Արդյունքում, տվյալ դեպքում թեեւ առկա էր տվյալների հրապարակման իրավական հիմք, սակայն տվյալների կառավարումը տվյալների մշակման փուլում պատշաճ չէր իրականացվել, տվյալները հրապարակվում են այնպիսի հարթակում (տվյալների հետ կատարվում են այնպիսի գործողություններ), որը նախատեսված չէր օրենսդրությամբ: Իր հերթին՝ պաշտոնական կայքերի ստեղծմանը եւ սոցիալական ցանցերում պետական մարմինների ներկայացվածությանը զուգահեռ՝ օրենսդրությունը չէր փոխվել եւ չէր նախատեսել այդ հարթակներում տվյալների հրապարակայնեցման առանձնահատկությունները:

Եզրահանգում

Ինչպես նշեցինք այս վերլուծության «Նախնական տեղեկություններ» բաժնում օրինականության սկզբունքի պահանջ է, որ տվյալները մշակվեն օրենքի պահանջների պահպանմամբ, այսինքն այնպես (այն ձեռով), ինչպես նախատեսված է օրենսդրությամբ: Նման կանոնը ինքնանպատակ չէ, այն հնարավորություն է տալիս ապահովել, որ տվյալների հետ կատարվում են կառավարվող, այլ ոչ թե անվերահսկելի գործողություններ, եւ ըստ այդմ անվերահսկելի չեն տվյալների մշակմամբ անձանց իրավունքներին միջամտության ռիսկերը, ներառյալ՝ տվյալների անվտանգությունը:

Վերոնշյալ օրինակները վկայում են, որ որոշ դեպքերում, հատկապես նոր տեխնոլոգիաներն իներցիայով կիրառելու արդյունքում պետությունը կարող է շեղվել այս կամ այն տվյալի հետ վարվելու՝ օրենսդրությամբ սահմանված կարգերից, անգամ եթե առկա է նման տվյալների մշակման պատշաճ իրավական հիմք: Ըստ այդմ, **պետությունը չունի տվյալների կառավարման՝ տվյալների մշակման, ներառյալ՝ դրանք օգտագործելու փուլին վերաբերելի այնպիսի ընդհանուր քաղաքականություն, որը կապահովի յուրաքանչյուր տվյալի մշակում, ներառյալ՝ դրա օգտագործում բացառապես օրենսդրությամբ սահմանված կարգով, իսկ անհրաժեշտության դեպքում տվյալների մշակման, ներառյալ՝ դրանք օգտագործելու նոր ձեւերի եւ միջոցների, ըստ այդմ նաեւ անվտանգության միջոցների պատշաճ եւ ժամանակին ամրագրում վերաբերելի օրենսդրությունում՝ անկախ նրանից, թե որ պետական մարմնի մասին է խոսքը եւ անկախ պետական մարմիններում որոշում կայացնող անձանց փոփոխություններից:**

Տվյալներից ազատվելու փուլ

➤ Օրինակ 1

2023 թվականի փետրվարին Յեյսինկյան քաղաքացիական ասամբլեայի Վանաձորի գրասենյակն ի թիվս այլոց դիմելով նաեւ Անձնական տվյալների պաշտպանության լիազոր մարմինն՝ բարձրացրել էր տեղական ինքնակառավարման մարմինների որոշումներում երեխաների անձնական տվյալների եւ մասնավոր կյանքին վերաբերող տեղեկությունների ներառման եւ հրապարակման հարցը: Կազմակերպությունն ուշադրություն էր դարձրել, որ Շիրակի մարզի համայնքներից մեկի կայքում համայնքի ղեկավարի որոշումներում հասանելի էին երեխաների վերաբերյալ տեղեկություններ, այդ թվում՝ երեխաների անձնական կյանքի՝ ընտանիքների հետ վերամիավորման, խնամքի, դաստիարակության հետ կապված եւ նմանատիպ այլ հարցեր՝ երեխաներին նույնականացնող տվյալներով:

Պարզվել էր, որ երեխաներին նույնականացման, ինչպես նաեւ երեխաների եւ նրանց ընտանիքի այլ անդամների անձնական եւ ընտանեկան կյանքի, սոցիալական վիճակի վերաբերյալ, ինչպես նաեւ այլ զգայուն անձնական տվյալներ տեղական ինքնակառավարման մարմնի ղեկավարների կամ ավագանու որոշումների շրջանակում հրապարակված են տեղական ինքնակառավարման տարբեր մարմինների կայքերում:

Այս դեպքում համայնքի ղեկավարի եւ ավագանու ընդունած նորմատիվ իրավական ակտերի հրապարակումն ուղղակիորեն նախատեսված է «Տեղական ինքնակառավարման մասին» ՀՀ օրենքի 11-րդ հոդվածով: Այսինքն, առկա է տվյալների հրապարակման պատշաճ իրավական հիմք: Միաժամանակ, պահպանված էր նաեւ նման տվյալների հրապարակման կարգը: Մասնավորապես, «Տեղական ինքնակառավարման մասին» ՀՀ օրենքի 11-րդ հոդվածը նաեւ սահմանել է, որ ընդունած նորմատիվ իրավական ակտերը պետք է հրապարակվեն համայնքի պաշտոնական կայքում, ինչպես նաեւ օրենքը չի նախատեսել նշված իրավական ակտերը մասնակի կամ խմբագրված (օրինակ, զգայուն տվյալները ապանձնավորած՝ սեւացրած, ծածկած կամ ջնջած) հրապարակելու իրավունք: Կարելու է նաեւ, որ օրենքը չի նախատեսել նաեւ նման զգայուն տվյալներ պարունակող իրավական ակտերը հրապարակված մնալու ժամկետ, այսինքն, զգայուն տվյալներ պարունակող որոշումները պետք է հրապարակված մնան միշտ: Այս համատեքստում հարց է առաջանում՝ ինչու՞ է անհրաժեշտ նման զգայուն տվյալները հրապարակել, ընդ որում՝ առանց հրապարակված մնալու ժամկետի սահմանափակման:

Տվյալ դեպքում առկա էր եւ՝ տվյալների հրապարակման իրավական հիմք, եւ՝ տվյալները հրապարակվել էին օրենսդրության պահանջների պահպանմամբ, սակայն տվյալների մշակման նման պայմաններ սահմանելիս առերեւոյթ չի գնահատվել, թե նման զգայուն տվյալներ անսահմանափակ ժամկետով հրապարակելու անհրաժեշտությունը եւ ըստ այդմ չի նախատեսվել այդ տվյալների հրապարակայնությունը դադարեցնելու պայման: Արդյունքում, տվյալ դեպքում պետությունը նման կարգավորումներ սահմանելիս հաշվի չի առել տվյալների մշակման համաչափության սկզբունքը:

Սա խնդիր էր համարել նաեւ Անձնական տվյալների պաշտպանության լիազոր մարմինը եւ Արդարադատության, Աշխատանքի եւ սոցիալական հարցերի եւ Տարածքային կառավարման եւ ենթակառուցվածքների նախարարություններին ուղղված գրությամբ առաջարկել էր «Տեղական ինքնակառավարման մասին» օրենքով սահմանել, որ համայնքի ղեկավարի եւ ավագանու ընդունած այն նորմատիվ իրավական ակտերը, որոնք կպարունակեն անձնական կյանքի տվյալներ, կենսաչափական անձնական

տվյալներ կամ հատուկ կատեգորիայի անձնական տվյալներ (զգայուն տվյալներ) կամ երեխայի ցանկացած անձնական տվյալ, պետք է հրապարակվեն այդ տվյալներն ապանձնավորված եղանակով: Այսպիսով թեև նշված տեղեկությունները չէին սահմանվի որպես գաղտնիք եւ, օրինակ, տրամադրման ենթակա կլինեին «Տեղեկատվության ազատության մասին» օրենքով սահմանված կարգով տեղեկություն ստանալու հարցմամբ դիմած անձանց, սակայն կդադարեցվեր նման զգայուն տվյալների անսահմանափակ ժամկետով հրապարակումը:

Այս վերլուծությունը հրապարակելու պահին խնդիրը դեռեւս առկա է, «Տեղական ինքնակառավարման մասին» օրենքում փոփոխություն չի իրականացվել, եւ շարունակում է գործել համայնքի ղեկավարի կամ ավագանու որոշումների շրջանակում զգայուն անձնական տվյալները, ինչպես նաեւ երեխաների ցանկացած անձնական տվյալ անժամկետ հրապարակելու կանոնը:

➤ **Օրինակ 2**

Վերելի օրինակում նկարագրված խնդրին համադրելի խնդիր առկա էր նաեւ դատական ակտերի հրապարակման դեպքում: Ինչպես նշեցինք, դատական ակտերը կարող են պարունակել բազմաթիվ եւ անորոշ շրջանակի տեղեկություններ, այդ թվում՝ մարդկանց վերաբերյալ:

Նախկինում հրապարակվող դատական ակտերը պարունակում էին նաեւ զգայուն տվյալներ, ինչպես նաեւ երեխաների տվյալներ, իսկ դատական ակտերը խմբագրված (օրինակ, զգայուն տվյալները ապանձնավորած՝ սեւացրած, ծածկած կամ ջնջած) հրապարակելու կամ դատական ակտերը հրապարակված մնալու ժամկետ սահմանված չէր: 2015 թվականին «Անձնական տվյալների պաշտպանության մասին» օրենքի ընդունումից հետո մինչեւ 2018 թվականին Դատական նոր օրենսգրքի ընդունումը ընկած ժամանակահատվածում հրապարակված դատական գործերից երեխաների կամ մարդկանց զգայուն տվյալների վերահրապարակման, այլ հարթակներում տարածման փաստացի տեղի ունեցած մի քանի դեպքերի առիթով քննարկման առարկա դարձավ դատական ակտերի շրջանակում զգայուն անձնական տվյալներ, ինչպես նաեւ երեխաների ցանկացած անձնական տվյալ հրապարակելու համաչափության (համաչափության սկզբունքի մասին տե՛ս այս վերլուծության «Նախնական տեղեկություններ» բաժնում), այդ թվում՝ անժամկետ հրապարակելու հարցը:

Արդյունքում, 2018 թվականի ապրիլի 9-ին ուժի մեջ մտած Դատական նոր օրենսգրքի 11-րդ հոդվածի 10-րդ մասով նախատեսվեց, որ դատական իշխանության պաշտոնական կայքում անձնական կյանքի տվյալներ, կենսաչափական եւ հատուկ կատեգորիայի անձնական տվյալներ, երեխայի անձնական տվյալներ պարունակող դատական ակտերը հրապարակվում են ապանձնավորված կարգով: Ապանձնավորման կարգը սահմանում է Բարձրագույն դատական խորհուրդը: Ըստ այդմ, Դատական օրենսգրքով դադարեցվեց դատական ակտերի շրջանակում զգայուն անձնական տվյալների, ինչպես նաեւ երեխաների ցանկացած անձնական տվյալի անժամկետ հրապարակումը: Այդուհանդերձ, պետք է ընդգծել, որ գործնականում դատական օրենսգրքի այս պահանջը պատշաճ չի կատարվում. որոշ դեպքերում զգայուն եւ երեխաների անձնական տվյալներ պարունակող դատական ակտերը հրապարակվում են առանց այդ տվյալներն ապանձնավորելու:

➤ **Օրինակ 3**

Պարբերաբար հանրային բանավեճի առիթ է դառնում ընտրությունների հրապարակայնության շրջանակում ընտրողների գուցակների հրապարակայնության, հատկապես՝ առցանց հասանելիության հանգամանքը եւ հատկապես, ընտրողների ստորագրված գուցակների հրապարակայնությունը: Այսպես, Ընտրական օրենսգրքը սահմանադրական օրենքի 73-րդ հոդվածի 3.1 մասի որի համաձայն՝ «3.1. Ազգային ժողովի ընտրությունների ժամանակ տարածքային ընտրական հանձնաժողովը քվեարկության հաջորդ օրը՝ ժամը 12.00-ից սկսած, իրականացնում է ընտրողների գուցակների սկանավորում, (...) Ընտրողների գուցակները սկանավորվում են Կենտրոնական ընտրական հանձնաժողովի սահմանած կարգով և չափորոշիչներին համապատասխան՝ այնպես, որ տվյալ ընտրական տեղամասի ընտրողների գուցակում ընտրողի հերթական համարը, ազգանունը, անունը, հայրանունը, ծննդյան ամսաթիվը, հաշվառման վայրի հասցեն, ինչպես նաև ընտրողի ստորագրության, ընտրողների գրանցման համար պատասխանատու հանձնաժողովի անդամի անհատական կնիքի համար նախատեսված սյունակները լինեն տեսանելի: Ընտրողների սկանավորված գուցակները ոչ ուշ, քան սկանավորման աշխատանքներն սկսվելուց 24 ժամ հետո պաշտոնապես հրապարակվում ու ներբեռնելու և, ըստ ընտրական տեղամասերի, որոնման հնարավորությամբ տեղադրվում են Կենտրոնական ընտրական հանձնաժողովի համացանցային կայքում»: Այս կանոնը գործում է 2016 թվականից:

Թեև ընտրողների ստորագրված գուցակների առցանց հրապարակայնությունը ուղղակիորեն սահմանված է Ընտրական օրենսգրքով, սակայն այդ տվյալների հրապարակման համաչափության հարց է առկա՝ ի թիվս այլև նաև այդ գուցակների հրապարակման պայմանների առումով: Այսպես, մի կողմից Ընտրական օրենսգրքը չի սահմանել ընտրողների ստորագրված գուցակները համացանցից հեռացնելու ժամկետ, մյուս կողմից պարզ չէ, թե ինչու է անհրաժեշտ, որ ՀՀ ազգային ժողովի ընտրությունների արդյունքում հրապարակված գուցակները հասանելի լինեն համացանցում անժամկետ, օրինակ, նախորդ ընտրությունների ստորագրված գուցակները հասանելի լինեն Ազգային ժողովի հաջորդ ընտրություններից հետո նույնպես: Ավելին, առաջին հայացքից ընտրողների ստորագրված գուցակների հրապարակումն այլևս պետք է անհրաժեշտ չլինի ընտրությունների արդյունքների բողոքարկման հնարավորությունների/ժամկետների ավարտից հետո:

Այս դեպքում պետք է նկատի ունենայ, որ մի կողմից առերեւոյթ առկա չէ ընտրողների ստորագրված գուցակները համացանցում անժամկետ հրապարակելու որեւէ հիմնավորվածություն, մյուս կողմից՝ տվյալ դեպքում հրապարակվում են տասնյակ հազարավոր մարդկանց այնպիսի տվյալներ (ազգանուն, անուն, հայրանուն, ծննդյան ամսաթիվ, հաշվառման վայրի հասցե, ստորագրություն (ստորագրությունը կենսաչափական անձնական տվյալ է), որոշ դեպքերում նաև՝ անձնագրի սերիա եւ համար), որոնք էականորեն մեծացնում են, օրինակ, անձի ինքնության գողության հավանականությունը (կենսաչափական անձնական տվյալների եւ ինքնության գողության մասին տե՛ս այս վերլուծության «Նախնական տեղեկություններ» բաժնում):

Տվյալ դեպքում ընտրողների ստորագրված գուցակների հրապարակայնությունը նախատեսելիս առերեւոյթ չի գնահատվել նման տվյալներ, այդ թվում՝ կենսաչափական տվյալ համարվող ստորագրությունը սկանավորված տարբերակով անսահմանափակ ժամկետով հրապարակելու անհրաժեշտությունը եւ ըստ այդմ չի նախատեսվել այդ տվյալների հրապարակայնությունը դադարեցնելու պայման: Արդյունքում, տվյալ դեպքում պետությունը նման կարգավորումներ սահմանելիս հաշվի չի առել տվյալների մշակման համաչափության սկզբունքը:

➤ **Օրինակ 4**

Գրեթե բոլոր պետական մարմիններն ունեն պաշտոնական կայքեր, ինչպես նաև գրեթե բոլոր պետական մարմիններն ունեն «պաշտոնական» կոչվող օգտահաշիվներ սոցիալական տարբեր հարթակներում, հատկապես տարածված է ներկայությունը Facebook (Ֆեյսբուք) սոցիալական ցանցում: Բնականաբար, ինչպես պաշտոնական կայքերում, այնպես էլ սոցիալական ցանցերում պետական մարմինները տարածում են ծավալուն տեղեկություններ՝ տվյալներ իրենց գործունեությանն առնչվող անձանց, առարկաների, փաստերի, հանգամանքների, իրադարձությունների, եղելությունների եւ երեւույթների վերաբերյալ (կայքերի եւ համացանցում այլ հարթակների ինտեգրոն կիրառման ինտրի մասին տե՛ս այս վերլուծության «Տվյալների մշակման փուլ» բաժնում ներկայացված 3-րդ օրինակը եւ նույն բաժնի եզրահանգումը):

Թե՛ւ այս վերլուծության ընթացքում կոնկրետ պետական մարմնի պաշտոնական կայքի կամ սոցիալական ցանցում օգտահաշիվի խորթային վերլուծությունը չենք իրականացրել, սակայն հանրամատչելի աղբյուրներում, այդ թվում՝ իրավական ակտերի իրավական տեղեկատվական պաշտոնական համակարգերում հնարավոր չի եղել գտնել պետական մարմինների կողմից առցանց հարթակներում հրապարակվող տեղեկությունների արխիվացման, որոնողական համակարգերի միջոցով որոնման հասանելիության սահմանափակման կամ այս կամ այն տվյալը առցանց հասանելիությունից հանելու (հրապարակումը դադարեցնելու) կանոններ (այդպիսի կանոններին հաճախ նախատեսվում են առցանց հարթակների գաղտնիության քաղաքականություններով կամ կայքերի օգտագործման պայմաններով (privacy policy, terms of use)):

Նման պայմաններում առերեւույթ (նախնական տպավորությամբ) այն տվյալները, որոնք հայտնվում են պետական մարմնի կայքում կամ սոցիալական ցանցի օգտահաշիվում կամ առցանց այլ հարթակներում, մտում են այնտեղ միշտ՝ առանց ժամկետի սահմանափակման:

Եզրահանգում

Այս վերլուծության «Նախնական տեղեկություններ» բաժնում անդրադարձել էինք տվյալների մշակման համաչափության սկզբունքին, որի համաձայն չափավոր, տվյալները պետք է մշակվեն օրինական նպատակներին հասնելու համար նվազագույն քանակով եւ ժամկետով, երբ հնարավոր է՝ ապանձնավորված: Համաչափության սկզբունքի համատեքստում տվյալներից ճիշտ ժամանակին ազատվելը, առանց նպատակի ծավալուն տվյալներ չպահպանելը, նպատակին հասնելուց հետո այլևս ոչ անհրաժեշտ տվյալների մշակումը (ներառյալ՝ հրապարակումը) դադարեցնելը, հատկապես՝ տվյալների առցանց մշակման պայմաններում, ի թիվս այլնի նաեւ նվազեցնում են տվյալների ոչ պատշաճ կառավարման արդյունքում՝ անձանց իրավունքներին միջամտության ռիսկերը եւ ապահովում են տվյալների անվտանգությունը:

Վերոնշյալ օրինակները վկայում են, որ պետությունը, հատկապես նոր կարգավորումներ մշակելիս, անգամ եթե պատշաճ սահմանում է տվյալների ստացման կամ ձեւավորման իրավական հիմք, անգամ եթե սահմանում է տվյալների հետ վարվելու ընթացակարգեր, միեւնույն է որոշ դեպքերում «մոռանում» է գնահատել մշակվելիք տվյալների համաչափությունը, կարգավորել տվյալների «կյանքի» ամբողջ ընթացքը եւ ըստ այդմ նախատեսել այն պահը, երբ պետք է «ազատվել» նպատակին այլևս չծառայող տվյալներից: Ըստ այդմ, **պետությունը չունի տվյալների կառավարման՝**

տվյալներից ազատվելու փուլին վերաբերելի այնպիսի ընդհանուր քաղաքականություն, որը կապահովի, որ ստացված կամ ձեւավորված յուրաքանչյուր տվյալ մշակվի սահմանված նպատակին հասնելու համար համաչափորեն՝ նվազագույն ժամկետով, եւ սահմանված լինեն նպատակին հասնելու համար պիտանելիությունը եւ անհրաժեշտությունը սպառած տվյալների մշակումը դադարեցնելու կանոններ՝ անկախ նրանից, թե որ պետական մարմնի մասին է խոսքը եւ անկախ պետական մարմիններում որոշում կայացնող անձանց փոփոխություններից:

Առաջարկություններ/խորհրդատվականներ

Այս վերլուծությամբ ներկայացված օրինակները վկայում են, որ **տվյալների ոչ պատշաճ կառավարման խնդիրը ոչ թե դիպվածային է, այլ համակարգային**, վերաբերում է ոչ թե կոնկրետ պետական մարմնի, այլ բնորոշ է տարբեր պետական մարմինների եւ տարբեր ոլորտների՝ սկսած գործադիր իշխանության տարբեր մարմիններից, տեղական ինքնակառավարման մարմիններից եւ վերջացրած դատավարություններում օգտագործվող տվյալներով:

Ուստի, համակարգային խնդիրն անհրաժեշտ է համակարգային լուծում: Այս առումով առաջարկում ենք.

➤ իրականացնել տվյալների նախնական քարտեզագրում հետեւյալ քայլերով՝

- ցուցակագրել պետական մարմնի կողմից ստացվող կամ ձեւավորվող տվյալները,
- պարզել տվյալներից յուրաքանչյուրի մշակման իրավական հիմքը, գնահատել իրավական հիմքի պատշաճությունը կամ արձանագրել պատշաճ իրավական հիմքի բացակայությունը,
- պատշաճ իրավական հիմք ունեցող տվյալներից յուրաքանչյուրի համար պարզել դրա կարգավիճակը (դասակարգված է որպես որեւէ գաղտնիք, թե՛ ոչ), եւ եթե դասակարգված է, ապա պարզել նաեւ դասակարգման իրավական հիմքը (այն օրենքը, որով սահմանված է տվյալի գաղտնիությունը),
- եթե տվյալը դասակարգված չէ, կամ եթե դասակարգման իրավական հիմքը պատշաճ չէ, ապա պարզել այդ տվյալների զգայունությունը, գնահատել տվյալի մատչելիությամբ պայմանավորված միջամտությունը մարդու իրավունքներին, տվյալի հրապարակայնությունը սահմանափակելու նպատակահարմարությունը եւ մարդու իրավունքներին անհամաչափորեն միջամտող տվյալներ վերհանելու դեպքում՝ համապատասխան հիմնավորմամբ ձեւավորել տվյալների դասակարգման պատշաճ իրավական հիմք,
- պատշաճ իրավական հիմք չունեցող տվյալների վերհանման դեպքում կամ դադարեցնել այդ տվյալների մշակումը, կամ ձեւավորել տվյալների մշակման պատշաճ իրավական հիմք՝ նկարագրելով տվյալի «կյանքի» ամբողջ ընթացքը, այդ թվում՝ անդրադառնալով տվյալի կարգավիճակին (տե՛ս վերելի կետերը):

Այս վերլուծությամբ ներկայացված օրինակները եւ մասնավորապես այն, որ որոշ դեպքերում քաղաքացիական հասարակության եւ Անձնական տվյալների պաշտպանության լիազոր մարմնի մասնագիտական «հուշումներից» հետո պետությունը շտկել է այս կամ այն ոլորտում տվյալների մշակման իր գործողությունները՝ մասնավոր դեպքերում էականորեն բարելավելով տվյալների կառավարման իր մոդելը, վկայում են, որ տվյալների կառավարման շատ խնդիրների հիմքում հաճախ ոչ թե դիտավորությունն է, այլ իրազեկման եւ համապատասխան հմտությունների պակասը: Այս խնդիրն արձանագրվել է նաեւ ՀՀ կառավարության 2021-2026 թվականների գործունեության միջոցառումներում, մասնավորապես Կառավարության 2021-2026 թվականների գործունեության միջոցառումների ծրագիրը հաստատելու մասին ՀՀ կառավարության՝ 2021 թվականի նոյեմբերի 18-ի N-1902-Լ որոշման 1-ին հավելվածով ի թիվս այլնի նախատեսված է Անձնական տվյալների պաշտպանության լիազոր մարմնի կարողությունների (մարդկային ռեսուրսների, մասնագիտական, տեխնիկական) հզորացումը: Իսկ նույն որոշման 2-րդ հավելվածը որպես նշված միջոցառման հիմնավորում ի թիվս այլնի շեշտվում է, որ իրազեկման և գիտելիքի պակասի խնդիրն

անդրադառնում է ոչ միայն մասնավոր կյանքում մարդու անձնական տվյալների պաշտպանության հմտությունների բացակայությանը, այլ նաև անձնական տվյալների պաշտպանության վերաբերյալ **պետական մարմիններում անձնական տվյալների մշակման հետ առնչվող անձանց իրազեկման և գիտելիքի բարձրացմանը:**

Այս առումով առաջարկում ենք

- շեշտադրել տվյալների կառավարման, ներառյալ՝ անձնական տվյալների պաշտպանության, կիրառական տեղեկատվության, տեղեկատվության ազատության եւ համադրելի այլ թեմաներով ուսուցումները/վերապատրաստումները պետական մարմինների հնարավորինս լայն շրջանակի ներկայացուցիչների համար՝ դրանցում ներգրավելով քաղաքացիական հասարակությանը, ինչպես նաև հնարավոր ծրագրերում եւ նախաձեռնություններում նախատեսել նման ուսուցումների շարունակականության համար բավարար ռեսուրսներ:

Հավելված

2023 թվականի փետրվարի 27-ին Արդարադատության նախարարության կայքում <https://moj.am/article/3513> հղմամբ հրապարակված կյուրթի լուսապատճենը:



2022 թվականի մարտի 18-ին Արդարադատության նախարարության կայքում <https://moj.am/article/3107> հղմամբ հրապարակված կյուրթի լուսապատճենը:





Բազմակողմանի տեղեկատվության ինստիտուտ
www.mdi.am