ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ

ՊԵՏԱԿԱՆ ԿԱՌԱՎԱՐՄԱՆ ԱԿԱԴԵՄԻԱ

Առկա ուսուցում 1622 թողարկում

Իրավագիտության ամբիոն

Անձնական տվյալների պաշտպանության իրավունքը և դրա սահմանադրական երաշխիքները

ՄԱԳԻՍՏՐՈՍԱԿԱՆ ԹԵԶ

«Իրավագիտություն» մասնագիտությամբ իրավագիտության մագիստրոսի որակավորման աստիճան հայցելու համար

Մագիստրանտ՝ Ավանեսյան Դիանա Արտակի

Ղեկավար՝ Հակոբյան Լիլիա Արեգի
իրավ.գիտ.թեկնածու, դոցենտ

Ամբիոնի վարիչ՝ Եզեկյան Արմեն Ռևիկի
իրավ. գիտ. թեկնածու, դոցենտ

Երևան 2018

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

ՆԵՐԱԾՈՒԹՅՈՒՆ **3**

ԳԼՈՒԽ 1.ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ԻՐԱՎՈՒՆՔԸ ՍԱՀՄԱՆԱԴՐԱԿԱՆ ԻՐԱՎՈՒՆՔԻ ՀԱՄԱԿԱՐԳՈՒՄ **8**

1.1 Անձնական տվյալների պաշտպանության իրավական հիմքերը 8

1.2 Մասնավոր կյանքի անձեռնմխելիության իրավունքի և անձնական տվյալների պաշտպանության իրավունքի հարաբերակցության առանձնահատկությունները Հայաստանի Հանրապետությունում 22

1.3 Անձնական տվյալների պաշտպանության իրավունքի իրացման միջազգային փորձը 29

ԳԼՈՒԽ 2. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ԻՐԱՎՈՒՆՔԻ ԻՐԱՑՄԱՆ ԿԱՌՈՒՑՎԱԿԱՐԳԵՐԸ 41

2.1.Անձնական տվյալների պաշտպանության իրավունքի իրացման կառուցակարգերը ՀՀ-ում 41

2.2.Անձնական տվյալների պաշտպանության իրավունքի իրացումը ՀՀ տեսախցիկներով նկարահանումների դեպքում 51

2.3.Անձնական տվյալների պաշտպանության իրավունքի իրացումը ՀՀ հանրային իշխանության մարմինների կողմից անձնական տվյալների տիրապետմանը և օգտագործմանն ուղղված լիազորությունների իրականացման շրջանակներում 61

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ **71**

ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ **75**

ՆԵՐԱԾՈՒԹՅՈՒՆ

Թեմայի արդիականությունը: Հասարակության զարգացման ներկա պայմաններում անձնական տվյալների պաշտպանության իրավունքի, դրա սահմանադրական երքշխիքների մասին հետազոտություններն ու ուսումնասիրությունները ձեռք են բերել առանձնակի կարևորություն և արդիականություն: Տվյալների պաշտպանության պահանջներին համապատասխանող օրենսդրությունը երկրի քաղաքականության և կայուն զարգացման, կառավարման արդյունավետության ապահովման առանցքային տարրերն են: Անձնական տվյալների պաշտպանության իրավունքի սահմանադրական հիմքերի ուսումնասիրումը մշտապես զարգացում ապրող իրավունքի ոլորտ է: Տեղեկատվահաղորդակցական տեխնոլոգիաների ամենօրյա զարգացումներով պայամանավորված՝ անձնական տվյալների պաշտպանության հիմնահարցն ամեն օր ձեռք է բերում ավելի մեծ կարևորություն: Անձնական տվյալների պաշտպանության իրավունքի խախտումները և ոտնահարումները կարող են լուծջ սպառնալիքներ հանգեցնել երկրի ազգային անվտանգությանը, ուստի այս իրավունքի ամրապնդման, հուալի պաշտպանության, Սահմանադրորեն երաշխիքների ապահովման հարցը Հայաստանի Հանրապետության պետական կառավարման ուշադրության կենտոնում է և մեր երկրում գործուն քայլեր են արվում դրանք ապահովելու համար:

Ամբողջ աշխարհով ճանաչված են անձնական տվյալներ հավաքելու և մշակելու միջազգային չափանիշները: Երկրները այս ոլորտում իրենց ազգային օրենսդրությունը մշակելիս պարտադիր հաշվի են առնում անձնական տվյալներ հավաքելու և մշակելու միջազգային չափանիշները և սկզբունքները: Եվրոպայի խորհրդի՝ «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիան այն ամենաարդյունավետ գործիքն է, որը կարող է ներդաշնակեցնել անձնական տվյալների պաշտպանության օրենսդրությունները: Որպես եվրոպական քաղաքակրթության մաս և Եվրոպայի խորհրդի անդամ, Հայաստանը ընդունում է անձնական տվյալների պաշտպանության քաղաքականությունը՝ հիմնվելով եվրոպական չափորոշիչների և սկզբունքների վրա:

Անձնական տվյալների պաշտպանության պատշաճ մակարդակի ապահովումն անհրաժեշտ է հանրային ծառայությունների արդիականացման, էլեկտրոնային կառավարման գործիքների ներդրման համար՝ նպաստելով կոռուպցիայի հետ կապված ռիսկերի և վարչական իրավասությունների չարաշահումների կրճատմանը: Անձնական տվյալների պաշտպանության կարևոր պատճառներից է նաև անհատների անձնական կյանքի նկատմամբ հարգանքը, որը մարդու իրավունքների համաձայնագրերով պաշտպանված հիմնարար իրավունք է: Անձնական տվյալների պաշտպանության մասին համապարփակ օրենսդրության ընդունումը երաշխիք է հանդիսանում ՀՀ-ում անձնական տվյալների պաշտպանության իրավաքան հիմքերի ապահովման համար: «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով անձնական տվյալների պաշտպանությունը ստացել է պետական ապահովվածություն, հավասարակշռվել են անձնական տվյալների սուբյեկտների և մշակողների փոխադարձ իրավունքներն ու պարտականությունները, նաև՝ սահմանվել է անձնական տվյալների մշակման օրինականության նկատմամբ անկողմնակալ և մշտական հսկողություն իրականացնող մարմին՝ ՀՀ արդարադատության նախարարության աշխատակազմի Անձնական տվյալների պաշտպանության գործակալությունը:

Անձնական տվյալների պաշտպանության անհրաժեշտությունը հարցը մնում է արդիական հատկապես այն կազմակերպություններում, որոնք անձնական տվյալների հետ կապված իրենց գործառույթները իրականացնում են նորագույն տեղեկատվական տեխնոլոգիաների միջոցով, ինչպես նաև այն կազմակերպությունները, որոնք օրենքով սահմանված նպատակով և կարգով ձեռք բերելով որոշակի անձնական տվյալներ, դրանք կարողանում են օգտագործել այլ առևտրային նշանակության նպատակներով: Օրինակ՝ բանկերը, վարկային և ապահովագրական կազմակերպությունները, տուրիստական ընկերությունները, կապի օպերատորները, խանութների ցանցերը և այլն: Այս և նմանատիպ այլ հիմնախնդիրների լուծման համար կարևոր ենք համարում հանգամանորեն ուսումնասիրել անձնական տվյալների պաշտպանության իրավունքի սահմանադրական երաշխիքները և վեր հանել այն առանձնահատկությունները, որ

ունի Հայաստանի հանրապետությունը անձնական տվյալների պաշպանության իրավունքի իրացման հարցում:

Թեմայի նպատակը և խնդիրները. Մագիստրոսական թեզի հիմնական նպատակն է ուսումնասիրել և վերլուծել Հայաստանի Հանրապետությունում անձնական տվյալների պաշտպանության իրավունքը, պարզաբանել՝ դրա սահմանադրական երաշխիքները, շեշտադրել այն ուղղությունները, որոնք կարող են էական ազդեցություն ունենալ անձնական տվյալների պաշտպանության իրավունքի ամրապնդման գործում: Նշված նպատակին հասնելու համար առաջադրվել են հետևյալ հիմնական խնդիրները.

1. **Ուսումնասիրել** անձնական տվյալների պաշտպանության իրավական հիմքերը.
2. **Ցույց տալ** անձնական տվյալների պաշտպանության դերն ու կարևորությունը երկրի ազգային անվտանգության ապահովման գործում.
3. **Մատնանշել** մասնավոր կյանքի անձեռնմխելիության իրավունքի և անձնական տվյալների պաշտպանության իրավունքի հարաբերակցության առանձնահատկությունները Հայաստանի Հանրապետությունում.
4. **Վերլուծել** անձնական տվյալների պաշտպանության իրավունքի իրացման միջազգային հաջողված փորձը.
5. **Կարևորել** անձնական տվյալների պաշտպանության իրավունքի իրացման կառուցակարգերի անհրաժեշտ դերակատարությունը ՀՀ-ում.
6. **Բացահայտել** անձնական տվյալների պաշտպանության իրավունքի իրացումը ՀՀ տեսախցիկներով նկարահանումների պարագայում,
7. **Քննարկել** ՀՀ հանրային իշխանության մարմինների դերը անձնական տվյալների հավաքագրման, մշակման և պաշտպանության գործընթացներում:

Հետազոտության օբյեկտը և առարկան: Մագիստրոսական թեզի հետազոտության օբեյկտն ու առարկան անձնական տվյալների պաշտպանությունն է

և այն սահմանադրական երաշխիքները, որոնք ապահովում են այդ իրավունքի արդյունավետ իրացումը:

Գրականության տեսություն: Մագիստրոսական թեզի տեսական հիմքն են դարձել տվյալ հարցի վերաբերյալ մասնագիտական գրականությունը: Տեղեկատվություններ են ստացվել նաև օրենքներից և ենթաօրենսդրական ակտերից, իսկ անձնական տվյալների պաշտպանության սահմանադրական երաշխիքների ներկա իրավիճակի բնութագրման համար հիմք է հանդիսացել Հայաստանի Հանրապետության Սահմանադրությունը, «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը: Այս ամենը հնարավորություն է տվել համակարգված ուսումնասիրել անձնական տվյալների պաշտպանության իրավունքի ինստիտուտը և դրա սահմանադրակա երաշխիքների մեխանիզմները:

Մագիստրոսական թեզի հետազոտության մեթոդաբանական հիմքերը: Պայմանավորված մագիստրոսական թեզի առանձնահատկություններով և հաշվի առնելով առաջադրված խնդիրները՝ օգտագործվել են հետազոտության ինչպես ընդհանուր՝ համակարգային, այնպես էլ մասնավոր՝ տրամաբանական-իրավաբանական, պատմահրավական, իրավահամեմատական, իրավիճակային մոտեցման, համեմատական վերլուծության մեթոդները:

Հետազոտության տեսական և գործնական նշանակությունը: Մագիստրոսական թեզի տեսական նշանակությունը դրսևորվում է Սահմանադրական իրավունքի համակարգում անձնական տվյալների պաշտպանության իրավունքի տեղին ու դերին վերաբերող խնդիրների քննարկումներում կատարված ընդհանրացումներում, ինչպես նաև հետազոտման արդյունքում ներկայացված տեսական եզրահանգումներում: Մագիստրոսական թեզի հետազոտության արդյունքում ձևավորված հիմնական դրույթներն ու եզրահանգումները կարող են կիրառվել ՀՀ անձնական տվյալների պաշտպանության իրավունքի համակարգի կատարելագործման և կարգավորման նորմատիվ համակարգում առկա բացթողումների լրացման համար:

Մագիստրոսական թեզի կառուցվածքը: Մագիստրոսական թեզը բաղկացած է ներածությունից, երկու գլուխներից, եզրակացությունից, օգտագործված գրականության ցանկից:

ԳԼՈՒԽ 1.ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ԻՐԱՎՈՒՆՔԸ ՍԱՀՄԱՆԱԴՐԱԿԱՆ ԻՐԱՎՈՒՆՔԻ ՀԱՄԱԿԱՐԳՈՒՄ

1.1 Անձնական տվյալների պաշտպանության իրավական հիմքերը

Տվյալների պաշտպանությունը մշտապես զարգացում ապրող իրավունքի ոլորտ է: Դա պայմանավորված է մասնավոր կյանքի անձեռնմխելիությանն առնչվող մտահոգություններով, որը սերտորեն կապված է տեղեկատվական տեխնոլոգիաների արագ աճի, ինչպես նաև այն փաստի հետ, որը տվյալները հնարավոր է թվային եղանակներով փոխանցել և դրանք հեշտությամբ հասանելի են: Տվյալների գողության, տվյալների կորստի և չթույլատրված կամ ոչ պատշաճ օգտագործման, ինչպես նաև անհատական տվյալների բացահայտման հետզհետե ավելացող դեպքերը օրենքների և քաղաքականության արդյունավետ իրականացման հետ կապված հարցեր են առաջացնում: Այդ մտահոգություններն էլ ավելի են խորանում այնպիսի իրավիճակներում, երբ տվյալների ոչ միտումնավոր բացահայտումը կարող է հանգեցնել անհատների անվտանգությանը վնաս հասցնելուն կամ դրա սպառնալիքին: Անձնական տվյալներ հավաքելու և մշակելու միջազգային չափանիշները ճանաչված են ամբողջ աշխարհով: Այնուամենայնիվ, պարտադիր բնույթ ունեցող մեկ միջազգային փաստաթղթի բացակայությունը բազմաթիվ քննարկումների տեղիք է տվել:

Տվյալների պաշտպանության և մասնավոր կյանքի անձեռնմխելիության հարցերով հանձնակատարների 31րդ միջազգային խորհրդաժողովի ընթացքում մի շարք պետությունների կողմից ընդունվեց որոշում, որով կոչ էր արվում ընդունել մեկ միասնական կոնվենցիա և ճանաչել, որ տվյալների պաշտպանությունը և մասնավոր կյանքի անձեռնմխելիու թյունը հիմնարար իրավունքներ են, որոնք վերաբերում են բոլոր անհատներին՝ անկախ քաղաքացիությունից կամ բնակությունից[1]:

Ակնհայտ է, որ տվյալների պաշտպանության պահանջներին համապատասխանող օրենսդրությունը պետական քաղաքականության առանցքային

[1] Տվյալների պաշտպանության և մասնավոր կյանքի անձեռնմխելիության հարցերով հանձնակատարների միջազգային խորհրդաժողով, 2009 թվականի նոյեմբերի 5, հասանելի է հետևյալ կայքէջում՝ http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_ resolucion_madrid_en.pdf

տարրն է և պետք է ձևավորվի միջազգային գործելակերպերին հնարավորինս մոտ լինելու սկզբունքով: Եվրոպայի խորհրդի՝ Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին կոնվենցիան այն ամենաարդյունավետ գործիքն է, որը կարող է ներդաշնակեցնել եվրոպական երկրներում անձնական տվյալների պաշտպանության օրենսդրությունները: Որպես եվրոպական քաղաքակրթության մաս և Եվրոպայի խորհրդի անդամ, Հայաստանը պետք է ընդունի անձնական տվյալների պաշտպանության քաղաքականությունը՝ հիմնվելով եվրոպական չափորոշիչների վրա:

Տվյալների հուսալի պաշտպանության օրենսդրության գլխավոր հիմնավորումը տնտեսական է. անձնական տվյալների պատշաճ պաշտպանությունը գիտելիքահեն տնտեսության հիմքն է, որը ժամանակակից համաշխարհային տնտեսությանը ինտեգրվելու հնարավորություններից է: Բացի այդ, անձնական տվյալների պաշտպանության պատշաճ մակարդակի ապահովումն անհրաժեշտ է հանրային ծառայությունների արդիականացման, էլեկտրոնային կառավարման գործիքների ներդրման համար՝ նպաստելով կոռուպցիայի հետ կապված ռիսկերի և վարչական իրավասությունների չարաշահումների կրճատմանը: Եվ վերջին, բայց ոչ նվազ կարևոր պատճառը անհատների անձնական կյանքի նկատմամբ հարգանքն է, որը մարդու իրավունքների համաձայնագրերով պաշտպանված հիմնարար իրավունք է:

Հարկ է նշել, որ Եվրոպայի խորհրդի կոնվենցիայով սահմանված չափորոշիչներին հետևելը երաշխավորում է համապատասխանության ապահովման նվազագույն պահանջների բավարարումը, այն է՝ որպես հասարակության արդիականացման կարևոր մաս արագորեն աճող տեղեկատվական տեխնոլոգիաների շուկայի և էլեկտրոնային կառավարման գործիքների առկայությունը: Այդ չափորոշիչները կարելի է ներկայացնել հինգ հայեցակարգային սկզբունքների միջոցով[2]:

[2] «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիա (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), 1981 թվական, Եվրոպայի խորհուրդ (ընդունվել է 1981 թվականի հունվարի 28-ին) [ETS No. 108, Strasbourg, 28.1.1981], հասանելի է հետևյալ կայքէջում՝ http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

1. Անձնական տվյալները պետք է ստացվեն օրինական ճանապարհով և անաչառորեն մշակվեն: Չնայած նրան, որ «օրինականություն» հասկացությունը լայնորեն կիրառվում է Հայաստանի իրավական համակարգում, «անաչառություն» հասկացությունը այդքան էլ մեծ տարածում չունի և բացատրության կարիք ունի: Անձնական տվյալների պաշտպանության համատեքստում այն նշանակում է, որ տվյալների վերահսկիչները և տվյալներ մշակողները պետք է անձնական տվյալները ազնիվ ճանապարհով ստանան՝ կամ տվյալների սուբյեկտի համաձայնությամբ կամ օրենքի տառին խիստ համապատասխան: Սա նաև նշանակում է, որ տվյալների վերահսկիչը /տվյալներ մշակողը չպետք է պարզապես ապահովի օրենքներին և կանոնակարգերին ֆորմալ համապատասխանություն, նա նաև պետք է խուսափի ֆորմալ ընթացակարգի ցանկացած չարաշահումից, որը չնայած ֆորմալ համապատասխանությանը, չի բխում տվյալների սուբյեկտի շահերից կամ համապատասխան կանոնակարգի նպատակներից:

2. Անձնական տվալները պետք է պահվեն որոշակի և օրինական նպատակների համար և չպետք է օգտագործվեն այդ նպատակների հետ անհամատեղելի ձևով: Անձնական տվյալների օրինական և պատշաճ օգտագործման սկզբունքը լավ հայտնի է, այդ մասին միշտ խոսվում է, սակայն համաձայն Մարդու իրավունքների դատարանի գործելակերպերի, միշտ չէ, որ այն պատշաճ կերպով կիրարկվում է նույնիսկ ավանդաբար ժողովրդավարական երկրներում: Նույնիսկ օրինական ճանապարհով ստացված տվյալները կարող են օգտագործվել այն նպատակների համար, որոնք տարբերվում են դրանց սկզբնական հավաքագրման նպատակներից: Նույնիսկ դա անելիս տվյալների վերահսկիչը կարծելով, որ անաչոռորեն է գործում, կարող է խախտել նշված սկզբունքը:

3. Համարժեք, համապատասխան և ոչ ավելորդ այն նպատակների առումով, որոնց համար դրանք պահպանվել են: Նույնիսկ օրինական ճանապարհով հավաքված տվյալները չպետք է ավելին լինեն, քան պահանջվում է: Սակայն նշված սկզբունքը չի բացառում տվյալների պահպանման տարբերակը ավելի լայն նպատակների համար, եթե դա նախատեսվում է օրենքով կամ համաձայնեցված է տվյալների սուբյեկտի հետ: Ինչևէ, ընդհանուր, ավելի լայն նպատակը չի նշանակում

«հենց այնպես, ամեն դեպքի համար», այլ անհատների կամ հանրության շահերի համար, ինչպիսիք են քաղաքացիների ընդհանուր ռեգիստրը կամ հեռախոսահամարների տեղեկատուն (սպիտակ գիրքը): Առաջին դեպքում սա ընդհանուր նպատակ է, որը նախատեսվում է օրենքով, երկրորդը տվյալների հենք է, որը ստեղծվում է հանրային օգտագործման նպատակներով՝ տվյալների սուբյեկտների համաձայնությամբ:

4. Ճշգրտվում են և, անհրաժեշտության դեպքում, թարմացվում: Այս սկզբունքով սահմանվում է անհատների սուբյեկտիվ իրավունքը, որով նրանք իրավասու են պահանջելու իրենց վերաբերող տեղեկությունների կանոնավոր ճշգրտումը և թարմացումը, ինչպես նաև համապատասխան իրավական գործիքներ ներդնելու պետության պարտավորությունը: Պետության նշված պարտավորությունը կատարում է, ընդունելով հանրային տվյալների հենքերի վարչարարման ոլորտում համապատասխան կանոններ և կանոնակարգեր (տվյալների կանոնավոր թարմացման և ճշգրտման միջոցառումներ), ինչպես նաև առանձին պահվող տվյալների գծով նվազագույն պահանջներ, սահմանելով հատուկ ռեժիմներ տվյալների այն առանձնահատուկ հենքերի համար, որոնք ունեն պետական կարևորություն (նոտարական գրասենյակներ, կոմունալ ծառայություններ և հանրության համար կարևոր մասնավոր ընկերությունների կողմից մատուցվող ծառայություններ):

5. Պահպանվում են այնպես, որ հնարավոր լինի նույնականացնել տվյալների սուբյեկտներին այն ժամանակահատվածի սահմաններում, որի համար դրանք պահվում են՝ առանց գերազանցելու նշված ժամկետները: Տվյալների անաչառ օգտագործումը անձնական տվյալների մշակման քաղաքականության հիմնարար արժեքներից է: Չօգտագործվող տվյալների ոչնչացումը այդ մոտեցման մասն է կազմում և պետք է պարտադիր լինի տվյալների հենքերի հանրային և մասնավոր սեփականատետերի (տվյալների վերահսկիչների) համար: Ինչպես արդեն նշվեց, թե՛ օրենքում և թե՛ տվյալների սեփականատիրոջ համաձայնությամբ կարելի է սահմանել ոչ կոնկրետ նպատակ, ինչպիսիք են քաղաքացիների տվյալների ռեգիստրի, քրեական գործերի մասին գրանցումների կամ հեռախոսագրքի վարումը:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով անձնական տվյալների պաշտպանությունը ստացել է պետական ապահովվածություն, հավասարակշռվել են անձնական տվյալների սուբյեկտների և մշակողների փոխադարձ իրավունքներն ու պարտականությունները, նաև՝ սահմանվել է անձնական տվյալների մշակման օրինականության նկատմամբ անկողմնակալ և մշտական հսկողություն իրականացնող մարմին՝ Անձնական տվյալների պաշտպանության գործակալությունը[3]:

Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին Եվրոպայի խորհրդի կոնվենցիան, որը Հայաստանը վավերացրել է 2012 թվականին, այսօր դեռևս այս ոլորտում միակ պարտադիր միջազգային փաստաթուղթն է: Այն բաց է բոլոր երկրների համար և կարող է դառնալ համաշխարհային չափանիշ: Փաստաթղթով սահմանված են մի շարք սկզբունքներ, որոնք պետությունները պետք է ներառեն իրենց ներպետական օրենսդրության մեջ՝ ապահովելով, մասնավորապես, տվյալների արդար և օրինական մշակումը[4]:

Քաղաքացին, ամենօրյա կյանքի հասարակական հարաբերությունների տարբեր ոլորտներում՝ ֆինանսական, հարկային, կենսաթոշակային, սոցիալական, բժշկության և այլն, կոնկրետ նպատակներով տեղեկություններ է հայտնում իր անուն-ազգանվան, հասցեի, աշխատավայրի, բնակավայրի, ընտանիքի կազմի, հեռախոսահամարի և այլնի մասին:

Անձնական տվյալների յուրահատկությունը կայանում է նրանում, որ դրանք պատկանում են ֆիզիկական անձին, օտարման ենթակա չեն և քաղաքացիական շրջանառության օբյեկտներ լինել չեն կարող: Այլ խոսքերով, մարդկանց վերաբերյալ տվյալներն առուվաճառքի առարկա չեն կարող դառնալ: Սակայն դա չի բացառում

[3] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

[4] «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիա (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), 1981 թվական, Եվրոպայի խորհուրդ (ընդունվել է 1981 թվականի հունվարի 28-ին) [ETS No. 108, Strasbourg, 28.1.1981], հասանելի է հետևյալ կայքէջում՝ http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

օրենքով սահմանված կարգով կամ անձի համաձայնությամբ նրա անձնական տվյալների օգտագործումը:

Անձնական տվյալների պաշտպանության հարցի պատմությունն սկսվում է 1976 թվականից, երբ Եվրոպայի Խորհրդի նախարարների կոմիտեն ձեռնամուխ եղավ ֆիզիկական անձանց իրավունքների պաշտպանության նպատակով համապատասխան կոնվենցիայի նախապատրաստմանը: Այն արդեն 1981 թվականին պատրաստ ու բաց էր մասնակից պետությունների կողմից ստորագրվելու համար և կոչվում է 'Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին' կոնվենցիա[5]: Դա առաջին միջազգային իրավական պարտադիր փաստաթուղթն է, որում տրված են այն ստորագրած մասնակից պետությունների քաղաքացիների պաշտպանության մեխանիզմները, որոնք կարող են խախտվել նրանց անհատական տվյալների հավաքման և մշակման գործընթացում:

Կոնվենցիան արձանագրում է, որ անձնական տվյալները, որոնք բացահայտում են ռասայական ծագումը, քաղաքական կարծիքները, կրոնական կամ այլ համոզմունքները, ինչպես նաև առողջությանը կամ սեռական կյանքին առնչվող անձնական տվյալները, չեն կարող մշակվել ավտոմատ կերպով, եթե ներպետական իրավունքը չի ապահովում համապատասխան երաշխիքներ: Նույնը կարող է կիրառվել դատվածությանն առնչվող անձնական տվյալների նկատմամբ:

Արգելվում են անձի վերաբերյալ տեղեկությունների օգտագործումը և տարածումը, եթե դրանք հակասում են տեղեկությունների հավաքման նպատակներին: Սահմանադրությունը յուրաքանչյուրին իրավունք է վերապահում ծանոթանալու իր վերաբերյալ պետական և տեղական ինքնակառավարման մարմիններում առկա տեղեկություններին և պահանջել դրանց ճշգրտում կամ վերացում՝ օրենքով նախատեսված դեպքերում:

[5] «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիա (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), 1981 թվական, Եվրոպայի խորհուրդ (ընդունվել է 1981 թվականի հունվարի 28-ին) [ETS No. 108, Strasbourg, 28.1.1981], հասանելի է հետևյալ կայքէջում՝ http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Անձնական տվյալների պաշտպանության մասին համապարփակ օրենսդրության ընդունումը երաշխիք է հանդիսանում ՀՀ-ում անձնական տվյալների պաշտպանության իրավաքան հիմքերի ապահովման համար: «Անձնական տվյալների պաշտպանության մասին» նոր ՀՀ օրենքն ընդունվել է Ազգային ժողովի կողմից 2015 թվականի մայիսի 18-ին և ուժի մեջ մտել 2015 թվականի հուլիսի 1-ին: Օրենքով սահմանվում է պետական և մասնավոր կազմակերպությունների կողմից անձնական տվյալների շրջանառության կարգը, ինչպես նաև անձնական տվյալների հետ աշխատող կազմակերպությունների և այդ տվյալների սուբյեկտների իրավունքներն ու պարտականությունները:

Օրենքով սահմանվում են նաև որոշակի ընթացակարգեր, այդ թվում՝ անձնական տվյալները շրջանառության մեջ առնելու մասին ծանուցման և տվյալները երկրի սահմաններից դուրս փոխանցելու կարգը, ինչպես նաև անձնական տվյալների պաշտպանության համար լիազորված պետական մարմնի լիազորությունների շրջանակները:

Անձնական տվյալների պաշտպանության մասին այս նոր օրենքի պահանջների կիրարկումն ապահովելու համար, ՀՀ «Վարչական իրավախախտումների վերաբերյալ» օրենսգրքում կատարվել են համապատասխան փոփոխություններ ու լրացումներ:

Ներկա դրությամբ անձնական տվյալների պաշտպանության մասին Հայաստանի Հանրապետության օրենսդրությունը բավարարում է «Ավտոմատացված համակարգերում անձնական տվյալների շրջանառման առնչությամբ անհատների իրավունքների պաշտպանության մասին» Եվրոպայի Խորհրդի կոնվենցիայով սահմանված բոլոր հիմնական պահանջները: Այդուհանդերձ, մի շարք հարցեր, ինչպես օրինակ՝ արտաքին հսկման (փողոցային) տեսախցիկների և իրավական կարգավորման չենթարկվող էլեկտրոնային հեռահաղորդակցության սարքերի տեղադրման և դրանց միջոցով ստացված տվյալների օգտագործման հետ կապված հարաբերությունները դուրս են մնացել օրենքի կարգավորման հարթությունից:

Անձնական տվյալների պաշտպանության մասին օրենսդրության արդյունավետ կիրարկումը համար անհրաժեշտ բոլոր օրենսդրական և ենթաօրենսդրական

ակտերը, ինչպես օրինակ՝ «Անձնական տվյալների պաշտպանության հարցերով լիազորված պետական մարմնի կանոնադրությունը»[6] և «Վարչական իրավախախտումների վերաբերյալ ՀՀ օրենսգրքում կատարված փոփոխություններն ու լրացումները» ընդունվել և ուժի մեջ են մտել 2016 թվականի հունվարից[7]: Այդուհանդերձ, կա մի կարևոր իրավական ակտ՝ «Անձնական տվյալների պաշտպանության բավարար մակարդակ ունեցող երկրների ցանկը», որը ընդունվել է ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալության որոշման համաձայն 2017 թվականի փետրվարի 17-ին[8]: Այդ ցանկը իրավական բազա է ապահովում տվյալների միջսահմանային փոխանցման համար:

Նման ցանկի բացակայությունը բարդացնում և դանդաղեցնում էր տվյալների շրջանառություն իրականացնող կազմակերպությունների և տեղեկատվական տեխնոլոգիաների ոլորտում աշխատող ընկերությունների գործունեությունը:

ՀՀ-ում անձնական տվյալների պաշտպանության իրավական հիմքերի ապահովման հաջորդ կարևոր երաշխիքը տվյալների պաշտպանության հարցերով անկախ գործակալության ստեղծումն է: «Անձնական տվյալների պաշտպանության մասին» օրենքի համաձայն 2015 թվականին ստեղծվել է անձնական տվյալների պաշտպանության գործակալությունը: Այն հիմնադրվել է որպես ՀՀ արդարադատության նախարարության առանձին ստորաբաժանում[9]:

Անձնական տվյալների պաշտպանության գործակալության գործունեության նպատակների մեջ է մտնում՝

---

[6] Անձնական տվյալների պաշտպանության գործակալության կանոնադրությունը տես ՀՀ արդարադատության նախարարության կայքէջում՝ http://www.justice.am/structures/view/structure/32

[7] «Վարչական իրավախախտումների վերաբերյալ ՀՀ օրենսգրքում կատարված փոփոխություններն ու լրացումները», ուժի մեջ է մտել 11.01.2016թ.: Հասանելի է http://www.arlis.am/DocumentView.aspx?docid=102854

[8] Անձնական տվյալների պաշտպանության բավարար մակարդակ ունեցող երկրների ցանկը» հաստատելու մասին ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալության որոշում, 17.01.2017թ., Հասանելի է http://moj.am/storage/uploads/002_Cucak-final.pdf

[9] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

- անձնական տվյալների շրջանառություն իրականացնող կազմակերպությունների («անձնական տվյալներ մշակողների») ռեեստրի վարումը,
- անձնական տվյալների շրջանառության հետ կապված հարաբերություններում տվյալների սուբյեկտների իրավունքների պաշտպանության ապահովումը,
- ինչպես նաև իր լիազորությունների շրջանակներում անձնական տվյալների շրջանառության օրինականության ապահովումը:

Գործակալությունն իրավասու է՝ «Անձնական տվյալների պաշտպանության մասին» օրենքի պահանջների խախտման դեպքերում կիրառել օրենքով սահմանված վարչական պատժամիջոցներ, իսկ օրենքով սահմանված դեպքերում դիմել դատարան: Գործակալության որոշումները կարող են բողոքարկվել դատական կարգով:

Գործակալության պետը նշանակվում է նշանակվում է հինգ տարի ժամկետով Հայաստանի Հանրապետության վարչապետի կողմից՝ Հայաստանի Հանրապետության արդարադատության նախարարի ներկայացմամբ՝ իրավապաշտպան գործունեություն իրականացնող առնվազն հինգ հասարակական կազմակերպությունների համատեղ առաջարկությունների հիման վրա[10]:

Օրենքով սահմանվում է, որ անձնական տվյալների պաշտպանության հարցերով լիազոր մարմինը գործում է անկախ: Միևնույն ժամանակ, անձնական տվյալների պաշտպանության գործակալության կանոնադրության համաձայն, գործակալությունը «կառավարում է» արդարադատության նախարարը, իսկ «անմիջական ղեկավարումն» իրականացնում է գործակալության պետը[11]:

Գործակալության պետը հաշվետու է Հայաստանի Հանրապետության վարչապետին, արդարադատության նախարարին, ինչպես նաև նախարարի այն

[10] Անձնական տվյալների պաշտպանության գործակալության կանոնադրությունը տես ՀՀ արդարադատության նախարարության կայքէջում՝ http://www.justice.am/structures/view/structure/32

[11] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, հոդված 24. ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

տեղակալին, ում լիազորությունների մեջ մտնում է գործակալության գործունեության համակարգումը[12]:

Միջազգային առաջադեմ փորձը ցույց է տալիս, որ անհրաժեշտ է լիազոր մարմնի «բացարձակ» անկախություն, ինչպես ֆունկցիոնալ, այնպես էլ ֆինանսական, ինչը ենթադրում է պետական բյուջեից բավարար միջոցների հատկացումը: Իրականում գործակալությունը բավարար ֆինանսական անկախություն չունի:

«Անձնական տվյալների պաշտպանության մասին» օրենքում չկան գործակալության ֆինանսական անկախությունը երաշխավորող դրույթներ: Ներկայումս գործակալությունը ֆինանսավորվում է արդարադատության նախարարության բյուջեի միջոցով, ինչը հնարավորություն է տալիս նախարարությանը որոշակի ազդեցություն ունենալ գործակալության գործունեության վրա: Գործակալության գործունեության ֆինանսավորման համար 2016 թվականի պետական բյուջեով նախատեսված գումարը կազմում է 22,215,000 դրամ (մոտ 46,100 ԱՄՆ դոլար)[13]:

Տվյալների պաշտպանության անկախ գործակալության արդյունավետ աշխատանքը Գործակալության աշխատանքի արդյունավետության բարելավմանը հիմնականում խանգարում է ռեսուրսների, այդ թվում՝ կադրային, տեխնիկական և մեթոդական, պակասը, ինչը թույլ չի տալիս գործակալությանը լիարժեքորեն և ամբողջ մասշտաբով իրականացնել իր ֆունկցիաները: Չնայած գործակալության նորանշանակ պետի էնտուզիազմին և աշխատակազմի անդամների նվիրվածությանը, կազմակերպությունն ընդհանուր առմամբ ունի գործավարության բավարար փորձ ունեցող կադրերի պակաս, ինչը թույլ չի տալիս նրան միաժամանակ իրականացնել մի քանի վարչական վարույթներ: Ավելին, գործակալությունը չունի բավարար փորձագիտական ռեսուրսներ անձնական տվյալների պաշտպանության

[12] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, հոդված 25, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

[13]ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության 2016 թ. գործունեության հանրային հաշվետվություն , հասանելի է՝ http://www.moj.am/storage/uploads/002Annual-report-2016_ARM.pdf

հետ կապված գործերի հետաքննության, ինչպես նաև իր լիազորությունների նեղ շրջանակներից դուրս գտնվող հարցերի կարգավորման համար: Օրինակ, վերջերս գործակալությունը բարձրացրեց ուղղակի մարքեթինգի հարցը, որը կարգավորվում է «Տվյալների պաշտպանության մասին» Եվրոպական Միության դիրեկտիվով, սակայն չի մտնում «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի կարգավորման հարթության մեջ, բացառությամբ այն դեպքերի, երբ մարքեթինգի համար անձնական տվյալների օգտագործումը կատարվել է սահմանված կարգի խախտմամբ:

Չնայած այն բանին, որ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը տալիս է բավականին հստակ սահմանումներ, այն, ինչպես և իրավական ակտերից շատերը, պարունակում է դրույթներ, որոնք կարիք ունեն լրացուցիչ պարզաբանումների և պաշտոնական բացատրությունների: Անձնական տվյալների պաշտպանության գործակալության հիմնական գործառույթներից մեկն ի սկզբանե պետք է լիներ հանրային քննարկումների կազմակերպումը օրենքի հիմնական հասկացություններն ու դրույթները ներկայացնելու և մեկնաբանելու նպատակով: Օրինակ, գործակալությունը կարող էր բացել տվյալների «մշակման» կամ «փոխանցման» վերաբերյալ ծանուցում տալու հասկացությունը՝ բացատրելով, թե ո՞վ պետք է տա ծանուցումը, ի՞նչ ֆորմատով և ո՞ր դեպքերում: Բնականաբար, գործակալության դերն այս առումով պետք լիներ ավելի շուտ մասնավոր և հանրային կազմակերպություններին նոր ուժի մեջ մտած օրենքի պահանջները ներկայացնելը, քան փողոցային տեսախցիկների և իրավական կարգավորման չենթարկվող էլեկտրոնային հեռահաղորդակցության սարքերի հետ կապված հակասական (գործակալության լիազորությունների և օրենքի կարգավորման շրջանակների առումով) խնդիրների լուծումը:

Հայաստանի Հանրապետությունը վավերացրել է «Ավտոմատացված համակարգերում անձնական տվյալների շրջանառման առնչությամբ անհատների իրավունքների պաշտպանության մասին» Եվրոպայի Խորհրդի կոնվենցիան 2012 թվականին: Ընդհանուր առմամբ կարելի է ասել, որ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը և դրա կիրարկման նպատակով ընդունված

օրենսդրական («Վարչական իրավախախտումների վերաբերյալ» օրենսգրքում կատարված փոփոխություններն ու լրացումները) և ենթաօրենսդրական ակտերը համապատասխանում են կոնվենցիայի հիմնական սկզբունքներին: Օրենքով տրված սահմանումները հիմնականում համընկնում են կոնվենցիայում սահմանված հասկացությունների հետ:

Մասնավորապես, օրենքով սահմանվում է «տվյալների հատուկ կատեգորիաներ» (քաղաքական, կրոնական, առողջապահական և սեռական բնույթի տվյալներ) հասկացությունը, ինչը ենթադրում է այդ տվյալների ավելի խիստ պահպանում և դրանց օգտագործում միայն օրենքով սահմանված կարգով: Այդուհանդերձ, ոչ օրենսդրական և ոչ էլ ենթաօրենսդրական ակտերով չի սահմանվում նման հատուկ կատեգորիայի տվյալների պահպանման ընթացակարգը:

Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը չի սահմանում պատժամիջոցներ, այլ հղում է կատարում «Վարչական իրավախախտումների վերաբերյալ» օրենսգրքին, որում կատարվել են համապատասխան լրացումներ ու փոփոխություններ. մասնավորապես, ավելացվել է նոր հոդված որով տույժեր են սահմանվում «Անձնական տվյալների պաշտպանության մասին» օրենքի ֆունդամենտալ դրույթների խախտման (ինչպես օրինակ՝ անձնական տվյալները շրջանառության վերցնելու մասին ծանուցում չտալու կամ դրանք առանց թույլտվության կամ սահմանված կարգի խախտմամբ երկրի սահմաններից դուրս փոխանցելու) համար: Այդուհանդերձ, նախատեսված տույժերի չափը, որը տատանվում է 100,000-ից 500,000 դրամ, բավարար չէ խոշոր ընկերությունների կողմից խախտումները կանխելու համար[14]:

«Ավտոմատացված համակարգերում անձնական տվյալների շրջանառման առնչությամբ անհատների իրավունքների պաշտպանության մասին» եվրոպական կոնվենցիայի արդյունավետ կիրարկումը կարևոր նախապայման է անձնական տվյալների պաշտպանության իրավունքի կայացման և արմատավորման համար:

[14] «Վարչական իրավախախտումների վերաբերյալ» օրենսգիրք, http://www.arlis.am/DocumentView.aspx?docid=73129

Բոլոր անհրաժեշտ իրավական ակտերն ընդունվել են ու թեկուզև որոշ ուշացմամբ, բայց ուժի մեջ են մտել ու գործում են սկսած 2016 թվականի հունվարից: Կոնվենցիայի Արդյունավետ կիրարկմանը հիմնականում խանգարում է այն, որ անձնական տվյալների պաշտպանության գործակալությունը չունի բավարար վարչարարական փորձ և մասնագիտական (մասնավորապես՝ իրավաբանական) պոտենցիալ և հաճախ ծախսում է իր ռեսուրսները այնպիսի վարույթների վրա, որոնք անմիջական առնչություն չունեն գործող օրենսդրությամբ նախանշած ոլորտներում (ուղղակի մարքեթինգ, փողոցային կամ արտաքին անվտանգության տեսախցիկներ) տվյալների պաշտպանության հետ:

Ներկայացնենք նաև «Ավտոմատացված համակարգերում անձնական տվյալների շրջանառման առնչությամբ անհատների իրավունքների պաշտպանության մասին» եվրոպական կոնվենցիայի՝ «Վերահսկող գերատեսչությունների և միջազգային տեղեկատվական հոսքեր իրականացնող կազմակերպությունների ներկայացուցիչների վերաբերյալ» 2001 թվականի լրացում-արձանագրությունը:

Հայաստանի Հանրապետությունը վավերացրել է «Ավտոմատացված համակարգերում անձնական տվյալների շրջանառման առնչությամբ անհատների իրավունքների պաշտպանության մասին» ԵԽ-ի կոնվենցիայի վերոհիշյալ լրացում-արձանագրությունը 2012 թվականին: Կոնվենցիայի պահանջներին լրացում-արձանագրությամբ ավելացված երկու ֆունդամենտալ հասկացություններն էլ սահմանված են «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով, և այդ սահմանումները համապատասխանում են լրացում-արձանագրության պահանջներին:

«Ավտոմատացված համակարգերում անձնական տվյալների շրջանառման առնչությամբ անհատների իրավունքների պաշտպանության մասին» եվրոպական կոնվենցիայի՝ «Վերահսկող գերատեսչությունների և միջազգային տեղեկատվական հոսքեր իրականացնող կազմակերպությունների ներկայացուցիչների վերաբերյալ» լրացում-արձանագրության առանցքային պահանջներից մեկը՝ անկախ վերահսկող մարմնի ստեղծումը, կատարվել է աննշան ուշացմամբ: Չնայած այն բանին, որ օրենքն ընդհանուր առմամբ ամուր հիմքեր է ապահովում անձնական տվյալների

պաշտպանության գործակալության ինստիտուցիոնալ անկախության համար, գործակալությունն իրականում չունի բավարար ֆինանսական անկախություն: Անհրաժեշտ է համապատասխան փոփոխություններ ու լրացումներ կատարել օրենքում՝ գործակալության փաստացի ֆինանսական անկախությունն ապահովելու և իր գործառույթներն արդյունավետորեն իրականացնելու նպատակով բավարար ռեսուրսներ տրամադրելու համար:

Այս համատեքստում անհրաժեշտ է իրականացնել.

- Ապահովել տվյալների պաշտպանության հարցերով համապատասխան լիազորություններ,պարտականություններ և ֆինանսավորում ունեցող անկախ մարմնի գործունեությունը:
- Գործակալության արդյունավետ աշխատանքն ապահովելու նպատակով համալրել այն բավարար փորձառություն և գիտելիքներ ունեցող կադրերով, մասնագիտական սարքերով և մեթոդաբանությամբ:
- Անձնական տվյալների պաշտպանության հարցերով մարմնի ֆինանսական անկախությունն ավելի նպատակահարմար է սահմանել օրենսդրական մակարդակով՝ կառավարության կողմից հնարավոր ճնշումը և ազդեցությունը բացառելու համար: Դրա համար անհրաժեշտ է բավարար միջոցներ հատկացնել պետբյուջեի առանձնացված հոդվածով:
- Հատուկ ընթացակարգեր մշակել զգայուն տվյալների հատուկ կատեգորիայի տվյալների պահպանման համար:
- Ապահովել գործակալության անկախությունը՝ ձևավորելով խորհրդատվական մարմին և ընդգրկելով դրանում մարդու/քաղաքացիական իրավունքների պաշտպանության հասարակական կազմակերպությունների ներկայացուցիչների: Դա թույլ կտա զարգացնել աշխատակիցների պրոֆեսիոնալիզմը և նվաճել հանրության վստահությունը:
- Արմատավորել հանրությանը հաշվետվություն տալու պրակտիկան՝ Ազգային ժողովին ներկայացվող և հրապարակվող տարեկան հաշվետվության ֆորմատով:

Այսպիսով՝ Հայաստանի Հանրապետությունումմ անձնական տվյալների պաշտպանության ոլորտի կարգավորումը սաղմնային փուլում է: Հայաստանի Արդարադատության նախարարությունում վերջերս ստեղծված Անձնական տվյալների պաշտպանության գործակալության երեք հոգանոց աշխատակազմի գործունեության այս սկզբնական փուլը կարևոր է այն առումով, որ ցանկացած որոշում, օրենսդրական փոփոխության առաջարկ՝ դառնալու է նախադեպ և որոշիչ է լինելու տվյալների շտեմարանների մատչելիության առումով:

Անձական տվյալների թեման ներկայում շատ հրատապ է, քանի որ այն ոչ շատ լավ հետազոտված ոլորտ է:

Մեր օրերում անձնական տվյալների պաշտպանությունը էլ ավելի լուրջ խնդիր է դառնում, որովհետև գոյություն ունի համացանց, որտեղ գրեթե անվերահսկելի իրավիճակ է տիրում: Շատ կարևոր է, որ պետական կառավարման ինստիտուտները և առհասարակ պետությունը հոգ տանի անձնական տվյալների գաղտնիությունը ապահովելու, անձնական կյանքի անձեռնմխելիության իրավունքը պաշտպանելու վերաբերյալ:

Սկսած անուն ազգանունից, անձնագրի տվյալներից, ապրելու վայրից, հեռախոսահամարից, մինչև ընտանիքի անդամների տվյալները, պետք է անձի համաձայնությամբ տարածվեն և օգտագործվեն: Սակայն երբեմն անվերահսկելի է դառնում իրավիճակը և անձնական տվյալները օգտագործվում են ոչ ճիշտ նպատակով:

1.2 Մասնավոր կյանքի անձեռնմխելիության իրավունքի և անձնական տվյալների պաշտպանության իրավունքի հարաբերակցության առանձնահատկությունները Հայաստանի Հանրապետությունում

Մասնավոր կյանքի անձեռնամխելիության իրավունքը քաղաքակիրթ հասարակությունների արժեհամակարգերի այն կարևորագույն տարրերից է, որը իր ամրագրումն է գտել բազմաթիվ պետությունների սահմանադրություններում կամ նման նշանակության օրենքներում: Մասնավոր կյանքի անձեռնամխելիության իրավունքի՝ որպես սահմանադրական իրավունքի արժևորումը, ներկա ժամանակում առավել քան անհրաժեշտություն է, որը պայմանավորված է տեխնիկայի և

տեղեկատվական տեխնոլոգիաների զարգացման արդի աստիճանով: Անձի մասնավոր կյանքն ուղղակիորեն առնչվում է անձի անձնական տվյալների հետ, որոնց անձեռնամխելիության և գաղտնիության ապահովումն է, որ իրական պայմաններ է ստեղծում անձի մասնավոր կյանքի անձեռնամխելիությունն իրական դարձնելու համար: Անձնական տվյալների հետ անմիջականորեն առընչվում են բոլոր իրավաբանական անձինք և անհատ ձեռնարկատերերը, ինչպես նաև պետական և տեղական ինքնակառավարման մարմինները:

«Մասնավոր կյանք» և «անձնական տվյալներ» հասկացությունները մեկ ընդհանրական սահմանում չունեն: Դրանք կարելի է սահմանել որպես.

- մարդու կյանքի այնպիսի ոլորտ, որը նա չի ցանկանում հասնաելի դարձնել ուրիշներին (ֆիզիկական և իրավաբանական անձանց, պետական կառավարման ինստիտուտներին և լիազոր անձանց),
- «սեփական հայեցողություն»՝ անկախություն արտաքին կառավարչական և պետության վերահսկողությունից, հասարակական կազմակերպություններից[15]:

Մասնավոր կյանքը տանելով իրավական դաշտ՝ այն ձեռք է բերում մասնավոր կայնքի իրավունքի կարգավիճակ, որը «թույլ է տալիս մարդուն իրեն մարդ զգալ»[16]:

Չնայած «մասնավոր կայնք» հասկացությունը չունի իրավական ձևակերպում, իրավական կարագավորումները սահմանում են դրա անձեռնամխելիության սահմանները և համապատասխան ոտնձգությունների պատժելիության մակարդակները[17]:

---

[15] Шахов Н. (2008) Отношения по охране частной жизни и информации о частной жизни как объект теоретико-правового исследования. Ростов-на Дону. С. 7

[16] Bygrave L.A. Privacy and Data Protection in an International Perspective. In: Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010. p.165-200 Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf (date of visit: 19.02.2013); Назаров, Б.Л. (1995) Права человека История, теория и практика: Учебное пособие – Москва:.: Русспит

[17] Авдеев, М.Ю. (2013) Законодательство Российской Федерации о неприкосновенности частной жизни: к вопросу о заимствовании зарубежного опыта. Доступно через: http://cyberleninka.ru/article/n/zakonodatelstvo-rossiyskoy-federatsii-o-neprikosnovennosti-chastnoy-zhizni-k-voprosu-o-zaimstvovanii-zarubezhnogo-opyta

Մասնավոր կյանքի իրավունքը ենթադրում է, որ մարդը ինքնուրույն պետք է որոշի թե իր մասին ինչպիսի և ինչ քանակով տեղեկատվություն պետք է դարձնել հրապարակային և տրամադրել համապատասխան ինստիտուտներին: Այսինքն մարդն ինքն է տնօրինում իր մասին տեղեկատվության տարածման սահմանները[18]:

Անձնական տվյալները շատ երկրների իրավական ակտերում սահմանվում է որպես այնպիսի տեղեկատվություն, որի հիման վրա կարելի է նույնականացնել անհատին (personally identifiable information)[19]:

Իսկ ինչո՞ւ է անհրաժեշտ պաշտպանել անձնական տվյալները: Անձնական տվյալների անձեռնամխելիության վտանգները բազմազան են: Դրանք հատկապես մեծ կարևորություն և նոր նշանակություն են ստանում տեղեկատվահաղորդակցական մեխանիզմների և տեխնոլոգիաների սրընթաց զարգացման պայմաններում՝ կապած տեղեկատվության հավաքման, մշակման և պահպանման հետ: Այդ սպառնալիքներն են.

- տեղեկատվության հավաքագրման անհամապատասխան միջոցների կիրառումը (զանգվածային համատարած հետևումը, հաղորդագրությունների կորզումը, հարցումները, հարցաթերթիկները և այլն),
- տեղեկատվության մշակման գործընթացում անհրաժեշտ պաշտպանական կանոներին չհետևելը:
- տեղեկատվության տարածման անընդունելի միջոցների կիրառումը (տեղեկատվության գաղտնիության խախտումը, առանց տեղեկացնելու հրապարակումը, հասանելիության տրամադրումը, յուրացուը, խեղաթյուրումը և այլն),
- Միջամտությունը անձի վարքագծին[20]:

[18] Вайхерт,Г. (2011) Защита персональных данных в рамках серии дискуссий «Настоящее будущего» Доступно через: https://www.datenschutzzentrum.de/vortraege/20110224-weichert-datenschutz-moskau-ru.pdf.

[19] Gellman, R. (2014) Fair Information Practices: A Basic Histor». Доступно через: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[20] Солоув, Д. «Мне нечего скрывать» и другие ошибочные толкования приватности. Доступно через: https://www.pgpru.com/biblioteka/statji/nothingtohide.

Նոր տեղեկատվահաղորդակցական տեխնոլոգիաները անսահմանափակ հնարավորություն են տալիս գիտակցաբար կամ անգիտակցաբար խախտել անձնական տվյալների և մասնավոր կյանքի անձեռնամխելիության իրավունքը:

Անձնական տվյալների պաշտպանության անհրաժեշտությունը առավել կարևորվում է այն կազմակերպություններում, որոնք անձնական տվյալների հետ կապված իրենց գործառույթները իրականացնում են նորագույն տեղեկատվական տեխնոլոգիաների միջոցով, ինչպես նաև այն կազմակերպությունները, որոնք օրենքով սահմանված նպատակով և կարգով ձեռք բերելով որոշակի անձնական տվյալներ, դրանք կարողանում են օգտագործել այլ առևտրային նշանակության նպատակներով: Օրինակ՝ բանկերը, վարկային և ապահովագրական կազմակերպությունները, տուրիստական ընկերությունները, կապի օպերատորները, խանութների ցանցերը և այլն:

Վերոգրյալ պետությունների շարքին է դասվում նաև Հայաստանի Հանրապետությունը, որի Սահմանադրության 31-րդ հոդվածի 1-ին մասի համաձայն՝ «Յուրաքանչյուր ոք ունի իր մասնավոր և ընտանեկան կյանքի, պատվի ու բարի համբավի անձեռնմխելիության իրավունք»[21]: Այս իրավունքի իրացման ապահովմանն է ուղղված ՀՀ Սահմանադրության 34-րդ հոդվածը[22], որը, սակայն, կարող էր առավելապես ունենալ հռչակագրային բնույթ, եթե ՀՀ օրենսդիր մարմնի կողմից չընդունվեին մի շարք օրենքներ, որոնց դրույթների մի մասը կամ օրենքն ամբողջությամբ ուղղված են հասարակական հարաբերություններում հիշյալ իրավունքի իրացման իրական հնարավորության ստեղծմանը և ամրագում են գործնական երաշխիքներ և մեխանիզմներ մարդու մասնավոր կյանքի անձեռնամխելիության իրավունքի պաշտպանության համար:

Այդ նորմատիվ իրավական ակտերի համակարգում կարևորագույն դեր է կատարում «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը, որը

[21] ՀՀ Սահմանադրություն, փոփոխություններով, 06.12.2015թ. , Հոդված 31, մաս 1-ին: Հասանելի է http://www.arlis.am/DocumentView.aspx?docID=102510

[22] ՀՀ Սահմանադրություն, փոփոխություններով, 06.12.2015թ. , Հոդված 34: Հասանելի է http://www.arlis.am/DocumentView.aspx?docID=102510

ընդունվել է 06.12.2015թ., իսկ ուժի մեջ է մտել 22.12.2015թ.[23]: Հատկանշական է, որ այս օրենքի բազմաթիվ դրույթներ համահունչ են Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին 28.01.1981թ. կոնվենցիային[24]:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 3-րդ հոդվածի 1-ին մասի 1-ին կետի դրույթը սահմանում է, որ **անձնական տվյալը** ֆիզիկական անձին վերաբերող ցանկացած տեղեկությունն է, որը թույլ է տալիս կամ կարող է թույլ տալ ուղղակի կամ անուղղակի կերպով նույնականացնել անձի ինքնությունը.»[25]: «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի նույն հոդվածի 1-ին մասի 12-րդ, 13-րդ, 14-րդ և 15-րդ կետերը դասակարգում են անձնական տվյալների տեսակները, որոնց պաշտպանության ռեժիմը այս կամ այն չափով տարբերվում է՝ կապված անձի համար դրանց կարևորության աստիճանով, ինչպես նաև դրանց՝ երրորդ անձանց հասանելի դառնալու ռիսկերի բարձր մակարդակով[26]:

Նշված դրույթների համաձայն անձնական տվյալները բաժանվում են հետևյալ տեսակների՝

- անձնական կյանքի տվյալներ,
- կենսաչափական անձնական տվյալներ,
- հատուկ կատեգորիայի անձնական տվյալներ,
- հանրամատչելի անձնական տվյալներ:

Այդ տեսակներից յուրաքանչյուրը ընդգրկում է որոշակի խումբ տվյալներ, որոնք կոնկրետ հատկանիշով ընդհանրանում են և առաջացնում առանձին մեկ ռեժիմով կարգավորվելու անհրաժեշտություն:

---

[23] ՀՀ Սահմանադրություն, փոփոխություններով, 06.12.2015թ. : Հասանելի է http://www.arlis.am/DocumentView.aspx?docID=102510

[24] «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիա (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), 1981 թվական, Եվրոպայի խորհուրդ (ընդունվել է 1981 թվականի հունվարի 28-ին) [ETS No. 108, Strasbourg, 28.1.1981], հասանելի է հետևյալ կայքէջում՝ http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[25] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, հոդված 3, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

[26] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, հոդված12.13.14.15, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

- **Անձնական կյանքի տվյալներն են՝** անձի անձնական կյանքի, ընտանեկան կյանքի, ֆիզիկական, ֆիզիոլոգիական, մտավոր, սոցիալական վիճակի վերաբերյալ կամ նման այլ տեղեկություններ:
- **Կենսաչափական անձնական տվյալներն են՝** անձի ֆիզիկական, ֆիզիոլոգիական և կենսաբանական առանձնահատկությունները բնութագրող տեղեկություններ:
- **Հատուկ կատեգորիայի անձնական տվյալներն են՝** անձի ռասայական, ազգային պատկանելությանը կամ էթնիկ ծագմանը, քաղաքական հայացքներին, կրոնական կամ փիլիսոփայական համոզմունքներին, արհեստակցական միությանն անդամակցությանը, առողջական վիճակին ու սեռական կյանքին վերաբերող տեղեկություններ:
- **Հանրամատչելի անձնական տվյալներն են՝** 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:

Միաժամանակ, «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի նույն հոդվածի 2-րդ և 4-րդ կետերը սահմանում են անձնական տվյալների մշակման և օգտագործման հասկացությունները[27]:

Անձնական տվյալների մշակում է համարվում անկախ իրականացման ձևից և եղանակից (այդ թվում՝ ավտոմատացված, տեխնիկական ցանկացած միջոցներ կիրառելու կամ առանց դրանց) ցանկացած գործողություն կամ գործողությունների խումբը, որը կապված է անձնական տվյալները հավաքելու կամ ամրագրելու կամ մուտքագրելու կամ համակարգելու կամ կազմակերպելու կամ պահպանելու կամ օգտագործելու կամ վերափոխելու կամ վերականգնելու կամ փոխանցելու կամ

[27] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, հոդված 2,4: ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

ուղղելու կամ ուղեփակելու կամ ոչնչացնելու կամ այլ գործողություններ կատարելու հետ:

Իսկ անձնական տվյալների օգտագործումը անձնական տվյալների հետ կատարվող գործողությունն է, որի ուղղակի կամ անուղղակի նպատակը կարող է լինել որոշումներ ընդունելը կամ կարծիք ձևավորելը կամ իրավունքներ ձեռք բերելը կամ իրավունքներ կամ արտոնություններ տրամադրելը կամ իրավունքները սահմանափակելը կամ զրկելը կամ այլ նպատակի իրագործումը, որոնք տվյալների սուբյեկտի կամ երրորդ անձանց համար առաջացնում կամ կարող են առաջացնել իրավական հետևանքներ կամ այլ կերպ առնչվել նրանց իրավունքներին ու ազատություններին:

Վերը ներկայացված իրավական հասկացությունների բովանդակությունների բացահայտումը հնարավորություն է տալիս պարզելու, թե վերոգրյալ կազմակերպություններից որոնք ինչ չափով են իրենց գործունեության ընթացքում մշակում և օգտագործում անձնական տվյալներ, ինչը անհրաժեշտաբար առաջացնում է նրանց կողմից անձնական տվյալների մշակման և օգտագործման ընթացքում այդ տվյալների համար «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով սահմանված ռեժիմի ապահովման անհրաժեշտություն:

Ենթադրենք ապահովագրական կազմակերպությունը ապահովագրում է անձի առողջությունը, բնականաբար ապահովագրողը պետք է ապահովադրից պահանջի վերջինիս կամ շահառուի (կախված նրանից, թե ում առողջությունն է ապահովագրվում) առողջության վերաբերյալ հավաստի և ամբողջական տվյալներ, որոնք հանդիսանում են հատուկ կատեգորիայի անձնական տվյալ և դրանց մշակումն ու օգտագործումը ապահովագրական կազմակերպությունը պարտավոր է իրականացնել այդ տեսակի անձնական տվյալին վերաբերող օրենքի պահանջներին համահունչ՝ չհաշված ապահովագրական գաղտնիքի ռեժիմով դրանց պաշտպանության հնարավորությունը, քանի որ այն, քննարկվող տվյալի վերաբերմամբ, ունի դիսպոզիտիվ բնույթ:

Բանկերի և վարկային կազմակերպությունների դեպքում, օրինակ՝ վարկ տրամադրելիս վերջիններս վարկառուից պահանջում են նրա, օրինակ՝ անձնագրային

տվյալները, հեռախոսահամարը, էլեկտրոնային փոստի հասցեն, որոնք ևս անձնական տվյալներ են և «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջն է, որպեսզի ապահովվի դրանց պաշտպանվածությունը՝ անկախ նրանից, որ դրանց պաշտպանությունը, ինչ-որ չափով, կարող է ապահովվել նաև բանկային գաղտնիքի պաշտպանության շրջանակներում: Կամ, օրինակ՝ կապի օպերատորները կամ տուրիստական կազմակերպությունները ուղղակի մարկետինգ իրականացնելիս (direct marketing):

Այդ ռեժիմների չապահովումը առաջացնում է վարչական, ավելին, անգամ քրեական պատասխանատվություն:

Հաշվի առնելով այն, որ անձնական տվյալների պաշտպանության ինստիտուտը ներկայիս կարգավորմամբ նորություն է ՀՀ իրավական համակարգի համար, որը նոր իրավական մշակույթ է ՀՀ իրավական կյանքում և ուղղված է սահմանադրորեն և միջազգային փաստաթղթերով արժևորված արժեքի՝ անձի մասնավոր կյանքի անձեռնմխելիության իրավունքի պաշտպանությանը, ուստի անհրաժեշտ է, որ անձնական տվյալներ մշակող ցանկացած սուբյեկտ մանրամասն և ամբողջությամբ տեղեկացված լինի հիշյալ իրավադրույթներին՝ դրանց խախտման համար սահմանված պատասխանատվության միջոցներից խուսափելու և որ ամենակարևորն է՝ նպաստելու այս նոր իրավական մշակույթի ձևավորմանն ու կայացմանը ՀՀ-ում:

1.3 Անձնական տվյալների պաշտպանության իրավունքի իրացման միջազգային փորձը

Անձնական տվյալների պաշտպանության իրավունքի իրացման միջազգային փորձի ուսումնասիրումը հնարավորություն է տալիս հետազոտել աշխարհում Հայաստանի հանրապետությաը մոտ առանձնահատկություններով երկրիների առաջադեմ և հաջողված փորձը այս ոլորտում և կիրառել նրանց փորձը մեր երկրում առկա խնդիրների լուծման համար: Մագիստրոսական թեզի այս մասում հատկանծական ենք համարել ուսումնասիրել մեր հարևան Վրաստանի փորձը

անձնական տվյալների պաշտպանության գործում: Ուսումնասիրվել և ներկայացվել են նաև այլ երկրների հաջողված օրինակներ: Միջազգային փորձագետների գնահատմամբ՝ Վրաստանի Անձնական տվյալների պաշտպանության գործակալությունը ճանաչվել է ամենաարդյունավետ մարմինը, որը նշանակալի արդյունքի է հասել կարճ ժամկետում:

Վրաստանում «Անձնական տվյալների պաշտպանության մասին» օրենքն ընդունվել է 2012-ին Եվրամիության ասոցացման պայմանագրի շրջանակներում: Երկու տարվա ընթացքում կատարվել են փոփոխություններ ոլորտին առնչվող օրենսդրության մեջ, հաստատվել է Անձնական տվյալների պաշտպանության տեսուչի կարգավիճակը, որը նշանակվել է 2013-ին[28]:

Վրացական օրենքը կարգավորում է տեսահսկումը, բիոմետրիկ տվյալների պաշտպանությունը, ուղիղ մարքեթինգը, անդրսահմանային տվյալների փոխանցումը: Սահմանում է վերահսկող մարմնի իշխանությունը և ապահովում է անկախությունը: Վարչական պատասխանատվություն է սահմանում օրենքը խախտողների համար:

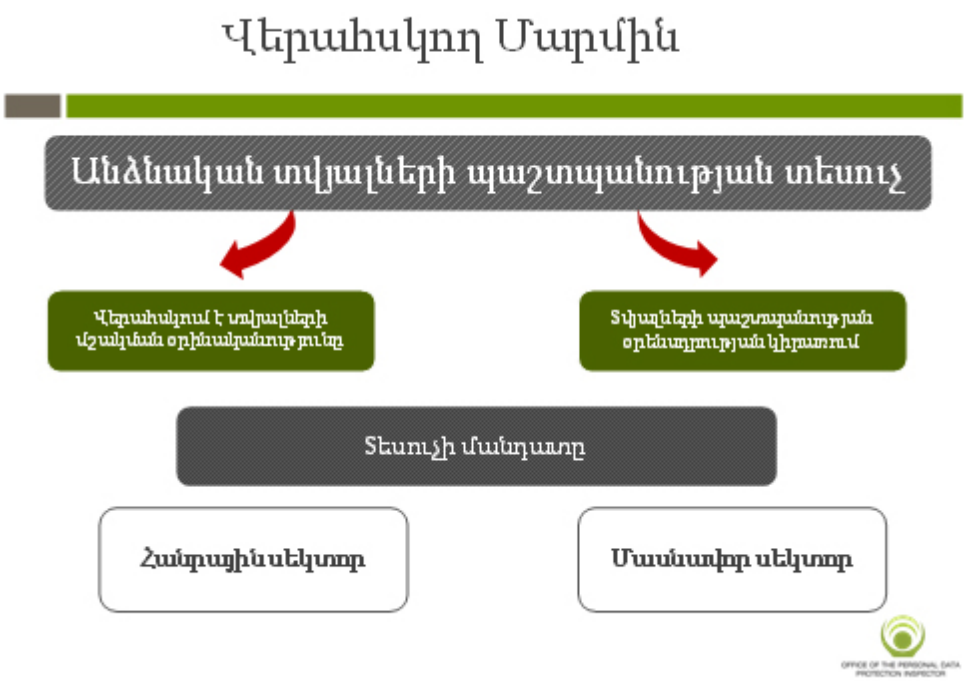
Ի տարբերություն Հայաստանի, որտեղ Անձնական տվյալների պաշտպանության գործակալությունը ՀՀ Արդարադատության նախարարության առանձնացված ստորաբաժանում է, Վրաստանի Անձնական տվյալների պաշտպանության տեսուչի գրասենյակը անկախ մարմին է[29]:

Տեսուչին նշանակում է Հատուկ հանձնաժողովը՝ բաղկացած 5 հոգուց, որոնք ներկայացնում են Օմբուդսմենին, խորհրդարանը, կառավարությունը, քաղաքացիական հասարակությունը: Հանձնաժողովը 2-5 թեկնածու է ընտրում և ներկայացնում վարչապետին, վերջինս նրանցից երկուսին է ընտրում և

[28] «Անձնական տվյալների պաշտպանության մասին» Վրաստանի օրենք, https://personaldata.ge/manage/res/docs/unofficial%20translations/ENG%20Statute%20Unofficial%20Translation.pdf

[29] https://personaldata.ge/en/about-us/inspector

ներկայացնում խորհրդարանին, որն էլ վերջնական ընտրությունն է կատարում: Տեսուչը նշանակվում է 3 տարի ժամկետով, ունի անձեռնմխելիություն[30]:

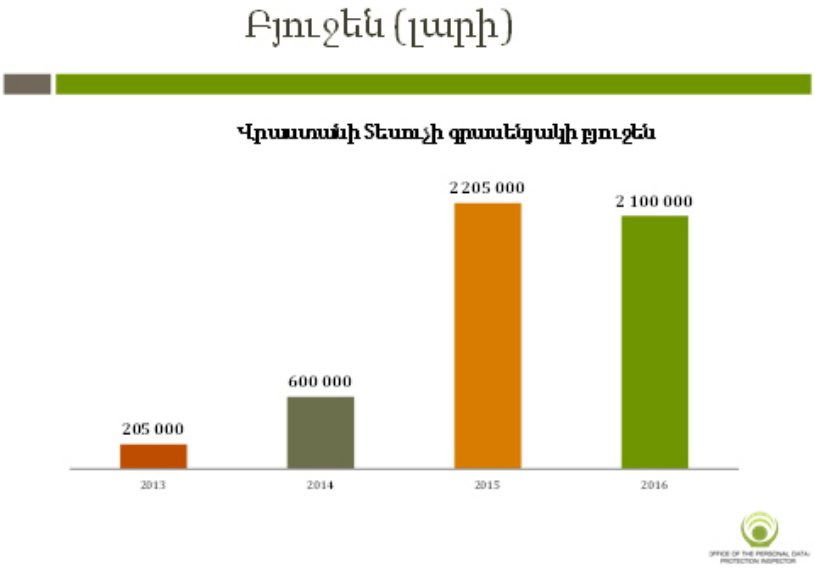


ՀՀ օրենսդրությամբ էլ Անձնական տվյալների պաշտպանության գործակալության անկախությունը երաշխավորված է, որի հավաստումն է գործակալության պետի նշանակման կարգը. Ըստ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի՝ թեկնածուներին ներկայացնում է քաղաքացիական հասարակության կոնսորցիումը: Առնվազն 5 հասարակական կազմակերպություն պետք է միավորվի մեկ թեկնածուի առաջադրելիս: Առաջադրված թեկնածուներից ՀՀ վարչապետը նշանակում է կատարում: Եվ նա կաշկանդված է քաղհասարակության կարծիքով[31]:

[30] «Անձնական տվյալների պաշտպանության մասին» Վրաստանի օրենք, հոդված 12, https://personaldata.ge/manage/res/docs/unofficial%20translations/ENG%20Statute%20Unofficial%20Translation.pdf

[31] [31] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք,. ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

Վրաստանի Տեսուչի գրասենյակը հաշվետու է միայն խորհրդարանին, պետբյուջեից հատուկ տողով է ֆինանսավորվում, ինչն էլ երաշխավորում է նրա անկախությունը: Երեք տարվա ընթացքում տեսուչի գրասենյակի բյուջեն շեշտակի աճել է (մոտ 700,000 եվրո տարեկան), ընդլայնվել է նաև աշխատակազմը՝ 43 մարդ[32]:



Համեմատության համար Հայաստանի Անձնական տվյալների պաշտպանության գործակալության բյուջեն մոտ 21 մլն դրամ է (մոտ 41.000 եվրո)[33], որը զուտ 6 աշխատակցի աշխատավարձի ծախսն է: Թեև Հայաստանի համապատասխան կառույցը ԱՆ առանձնացված ստորաբաժանում է, սակայն գործակալության բյուջեն ներառված չէ Արդարադատության նախարարության բյուջեում և պետբյուջեում նշվում է առանձին տողով[34]:

Վրացական օրենսդրությունն անձնական տվյալների պաշտպանության ոլորտում առանձնանում է նրանով, որ նախատեսում է՝

- Դատական վերահսկողություն

[32] «Անձնական տվյալների պաշտպանության մասին» Վրաստանի օրենք, հոդված 11,12 https://personaldata.ge/manage/res/docs/unofficial%20translations/ENG%20Statute%20Unofficial%20Translation.pdf

[33] https://personaldata.ge/en/about-us/budget

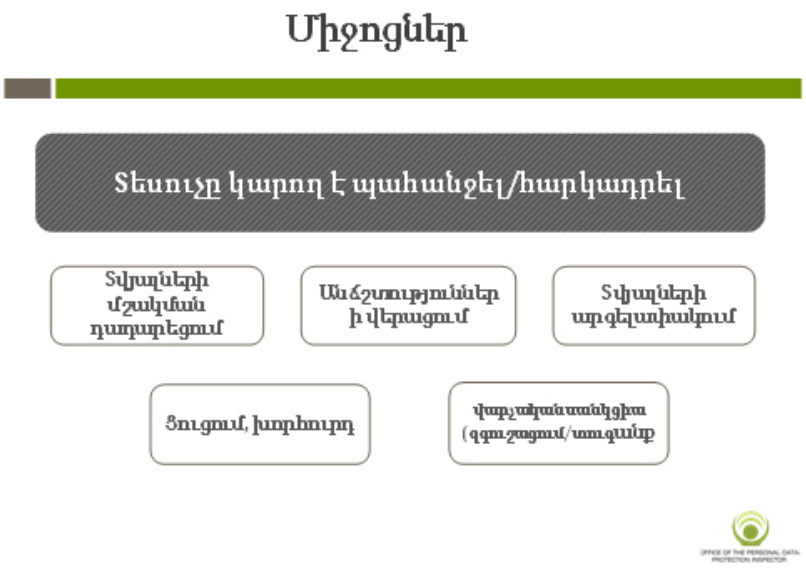
[34] «Հայաստանի Հանրապետության 2017 թվականի պետական բյուջեի մասին» ՀՀ օրենք, Ընդունված է 2016 թվականի դեկտեմբերի 8-ին, Հասանելի է՝ http://www.gov.am/files/docs/2014.pdf

- Գաղտնի գործունեության սահմանափակ օգտագործում
- Հիմնավորման բարձր չափանիշ
- Բողոքարկման իրավունք[35]:

Գաղտնի քննչական գործողությունների նկատմամբ Տեսուչի համար արտաքին վերահսկման մեխանիզմներ են սահմանված, մասնավորապես՝ գաղտնալսելու նկատմամբ նախնական և հետագա վերահսկողություն: Այս մեխանիզմները ներդրվեցին Վրաստանում տեղի ունեցած մեծ սկանդալից հետո, երբ պարզվեց, որ իրավապահները հարյուրավոր տեսագրություններ ունեն մարդկանց մասին: Փոփոխություններ կատարվեցին Քրեական դատավարության օրենգրքում, որոնցով սահմանվեցին՝ որևէ մարմին չի կարող տեսագրություն կատարել առանց դատարանի որոշման: Ինչ վերաբերում է հանրային նշանակության մասնագիտությունների տեր մարդկանց՝ փաստաբաններ, լրագրողներ, քաղաքական գործիչներ տեսահսկմանը, ապա դատախազությունը պիտի հիմնավորի, որ չկա այլ միջոց հետաքննություն կատարելու համար: Տեսուչն այս պարագայում արտաքին վերահսկողության իշխանություն ունի: Օրինակ՝ դատարանը կարող է որոշել 1 ամսով թույլատրել գաղտնալսում, բայց իրավապահները շարունակեն ավելի երկար, այս պարագայում տեսչական մարմինը վերահսկողության իր գործառույթն է իրականացնում՝ ստուգելու դատական որոշման կիրառումը:

Միջոցները, որ կարող է կիրառել Տեսչական մարմինը

[35] Անձնական տվյալների պաշտպանության մասին» Վրաստանի օրենք, հոդված 11,12 https://personaldata.ge/manage/res/docs/unofficial%20translations/ENG%20Statute%20Unofficial%20Translation.pdf



Տեսուչի գրասենյակը հաջող փորձ ունի անդրսահմանային տվյալների փոխանցման ոլորտում: Նրանք արձանագրել էին հետևյալ խախտումները սահմանային անցակետերում ՝

- լուսանկարահանում առանց օրինական նպատակի,
- տվյալների պահպանման կանոնների բացակայություն,
- տեսահսկում՝ առանց դրա մասին զգուշացման[36]:

Ձեռնարկված միջոցառումները հանգեցրել էին դրական արդունքի՝

- լուսանկարահանման սահմանափակում՝ բացառիկ դեպքերում,
- տվյալների պահպանման կանոնների սահմանում,
- Տեսահսկման մասին զգուշացնող ցուցանակներ:

Բարեփոխումներ են իրականացրել քրեակատարողական համակարգում, առողջապահության ոլորտում (դեղատներ), կրթական հաստատություններում (դպրոցներ), հանրային և մասնավոր կառույցներում:

Ստեղծվել է մոբայլ հավելված, որով մարդիկ հեշտորեն կարող են տեսուչին հայտնել իրենց անձնական տվյալի պաշտպանության իրավունքի խախտման մասին:

[36] https://personaldata.ge/en/home

Միջազգային փորձագետների գնահատմամբ՝ Վրաստանի Անձնական տվյալների պաշտպանության գործակալությունը ճանաչվել է ամենաարդյունավետ մարմինը, որը նշանակալի արդյունքի է հասել կարճ ժամկետում:

Միջազգային փորձի ուսումնասիրման արդյունքում անձնական տվյալների պաշտպանության համատեքստում հետաքրքրություն է ներկայացնում ԵՄ արդարադատության դատարանի դատական պրակտիկան կապված մոռացվելու իրավունքի հետ: Վերջինս անձնական կյանքի անձեռնմխելիության հետ կապված նոր հասկացություն է թվային աշխարհում: Այն կյանքի է կոչվել Եվրոպական Միությունում («Տվյալների պաշտպանության» դիրեկտիվի շրջանակներում) և Արգենտինայում: ԱՄՆ-ում խոսքի ազատության ջատագովները նշված սկզբունքի մեջ տեսնում են պոտենցիալ վտանգ խոսքի ազատությանը, մանավանդ, եթե այն կիրառվի հասարակական գործիչների նկատմամբ: Այս հարցն ըստ ամենայն հավանականության դեռ ակտուալ չէ Հայաստանում, բայց մի օր վստահաբար մարդիկ կհարցնեն՝ «չունի՞ արդյոք անձը մոռացվելու իրավունք»: Սա կարող է նույնիսկ գիտական հետազոտությունների և ապագա քաղաքական բանավեճերի նյութ դառնալ: Մոռացվելու իրավունքի հասկացությունը լայն քննարկումների առարկա է դարձել սկսած 2005 թվականից, երբ մի շարք անհատներ դատական կարգով պահանջեցին հեռացնել իրենց մասին տվյալները որոնողական կայքերի բազաներից և այլ տվյալների բազաներից՝ պնդելով, որ տվյալների պահպանումը հակառակ իրենց կամքի վիրավորական է, անտեղի և (կամ) անցանկալի:[37]

Պատմության մեջ առաջինը նման հայցով դիմել է Իսպանիայի քաղաքացի Մարիո Կոստեխա Գոնսալեսը, ով բողոքել է «Google Spain»-ի, «Google Inc.»-ի և իսպանական մի լրագրի դեմ տվյալների պաշտպանության ազգային գործակալությանը («Google Spain»-ը և «Google Inc.»-ը ընդդեմ Մարիո Կոստեխա Գոնսալեսի շահերը ներկայացնող Իսպանիայի տվյալների պաշտպանության գործակալությանը): Քաղաքացու բողոքը կայանում էր նրանում, որ «Google»-ի որոնողական համակարգը շարունակում էր տվյալներ ներկայացնել ժամանակին

[37] Шишлов А.А. Правовое регулирование защиты персональных данных в рамках Европейского Союза // Закон и право. - М.: ЮНИТИ-ДАНА, 2010, № 1. - С. 32-33.

պարտքերի դիմաց աճուրդի հանված իր տան վերաբերյալ, այն պարագայում, երբ համապատասխան վարույթը արդեն մի քանի տարի է ինչ փակվել էր և հետևաբար ներկայացված տվյալները, բացի իր անձնական կյանքի անձեռնմխելիությունը ոտնահարելուց, ուրիշ ոչ մի բանի պիտանի չէին: Քաղաքացին պահանջում էր, որ նախ լրագիրը հեռացնի կամ ճշտի ներկայացված տվյալները այնպես, որ իր անձին վերաբերող տեղեկությունները այլևս չերևան, և երկրորդը, որ «Google Spain»-ը կամ «Google Inc.»-ը միջոցներ ձեռնարկեն, որ իրեն վերաբերող անձնական տվյալները այլևս չհայտնվեն որոնման արդյունքներում[38]:

Հարկ է նշել, որ գործող եվրոպական օրենսդրությունը ունիվերսալ լուծում չի տալիս «մոռացվելու իրավունքի» հետ կապված բոլոր հարցերին: Եվրոպական հանձնաժողովի թիվ 95/48/EC դիրեկտիվի համաձայն անդամ պետությունները պետք է երաշխավորեն տվյալների սուբյեկտներին տվյալներն օգտագործող (տնօրինող) կազմակերպություններից իրենց վերաբերող տվյալներն արգելափակելու, ճշտելու կամ ջնջելու պահանջ ներկայացնելու իրավունքը, այն դեպքերում, երբ այդ տվյալները չեն համապատասխանում դիրեկտիվի պահանջներին, մասնավորապես՝ թերի են կամ սխալ[39]: Որոշ անդամ պետություններ այդ իրավունքն ամրագրել են դիրեկտիվի կիրարկման նպատակով ընդունված տվյալների պաշտպանության մասին նեղ ճյուղային օրենքներում: Օրինակ, Միացյալ Թագավորությունում տվյալների սուբյեկտը կարող է դատական կարգով ներկայացնել տվյալներն արգելափակելու, ճշտելու կամ ջնջելու պահանջ միայն այն դեպքերում, երբ կարող է ապացուցել, որ այդ տվյալները ճշգրիտ չեն:

Նիդեռլանդները ԵՄ անդամ այն պետություններից է, որը կառուցել է տվյալների պաշտպանության կայուն և արդյունավետ համակարգ: Այս երկրում

---

[38] Хачатурян Ю.А. Право работника на защиту персональных данных // Современное право. - М.: Новый Индекс, 2006, № 1. - С. 43-51

[39] Անձնական տվյալների մշակման և այդ տվյալների ազատ տեղաշարժի առնչությամբ անհատների պաշտպանության մասին հրահանգ 95/48/ԵՀ (Directive 95/48/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data) (ընդունվել է Եվրոպական պառլամենտի և Խորհրդի կողմից 1995 թվականի հոկտեմբերի 24-ին) [Official Journal L 281, 23-11-1995, P. 0031 – 0050], հասանելի է հետևյալ կայքէջում՝ http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-48_part1_en.pdf

անձնական տվյալների պաշտպանության մարմինը՝ Տվյալների պաշտպանության հանձնաժողովը, կազմված է նախագահից և երկու անդամներից: Նախագահը նշանակվում է թագավորի հրամանով վարչապետի ներկայացմամբ, վեց տարի ժամկետով: Երկու անդամները նշանակվում են նույն ընթացակարգով չորս տարի ժամկետով: Ի լրումն, Հանձնաժողովը կից փորձագետների խորհուրդ ունի, որը խորհրդատվություն է տրամադրում անձնական տվյալների պաշտպանության ընդհանուր հարցերի առնչությամբ: Ոլորտը կանոնակարգող իրավական ակտերի շրջանակում առանձնանում է Անձնական տվյալների պաշտպանության մասին ակտը, որում մանրամասն սահմանված են բոլոր ընթացակարգերը, ինչպես նաև պատասխանատվության ենթակա սուբյեկտների շրջանակը:

Լատվիայում Տվյալների պետական տեսչությունը կառավարվում է տնօրենի կողմից, ով նշանակվում և ազատվում է Կառավարության կողմից՝ Արդարադատության նախարարի ներկայացմամբ: Նույնը Լիտվիայի տվյալների պաշտպանության մարմինը՝ Տվյալների պաշտպանության տեսչությունը, կառավարվում է տնօրենի կողմից, ով նշանակվում է հինգ տարի ժամկետով և պաշտոնից ազատվում կառավարության կողմից, Կառավարության մասին օրենքով նախատեսված ընթացակարգին համապատասխան[40]:

Նմանատիպ ընթացակարգ նախատեսված է նաև Էստոբիայում: Տարբերությունը այն է, որ տնօրենի թեկնածությունը առաջադրում է Ներքին գործերի նախարարությունը: Էստոնիայի օրենքով սահմանվում են Տեսչության ղեկավարի աշխատանքից ազատման հետևյալ դեպքերը՝ ղեկավարի դիմումի համաձայն, նշանակման ժամկետի լրանալու, կարգապահական խախտման, երկարատև անգործունակության, նրա նկատմամբ մեղադրական դատավճիռը օրինական ուժի մեջ մտնելու, եթե հայտնի են դարձել փաստեր, որոնք օրենքի համաձայն արգելում են տվյալ անձի նշանակումը որպես տնօրեն:

Այս երեք երկրների փորձի ուսումնասիրությունը վկայում է, որ Էստոնիայի պարագայում անկախության մակարդակը ավելի բարձր է:

[40] Անձնական տվյալների պաշտպանության քաղաքականության ուղեցույց, http://www.osf.am/wp-content/uploads/2015/04/DataProPolicyGuide_arm_final.pdf

«Համայնքի ինստիտուտների և մարմինների կողմից անձնական տվյալների մշակման և ազատ տեղաշարժման ընթացքում անձանց իրավունքների պաշտպանության մասին» 45/2001 Եվրոպական պառլամենտի և խորհրդի կոմղից ընդունված ռեգլամենտը, որն առավելապես ուղղված էր 1995 թվականի դիրկետիվի կատարումն ապահովելուն և իր հիմքում ուներ այն հիմնական գաղափարները, որոնք ամրագրված էին դիրեկտիվում:

2012 թվականի հունվարին ԵՄ հանձնաժողովը նպատակ ունենալով ստեղծել տվյալների պաշտպանության համակողմանի համակարգ, նախաձեռնեց ԵՄ անձնական տվյալների պաշտպանության ոլորտի բարեփոխումները:

Արդյունքում 2016 թվականի մայիսի 7-ին համապատասխան դիրեկտիվի և ռեգլմենտի պաշտոնական տեքստերը հրապարակվեցին ԵՄ պաշտոնական լրագրում ԵՄ պաշտոնական լեզուներով: Չնայած որ ռեգլամենտը իրավաբանորեն ուժի մեջ է մտնում 2016 թվականի մայիսի 24-ից, սակայն այն սկսելու է կիրառվել 2018 թվականի մայիսի 25-ից: Դիրեկտիվը նույնպես ուժի մեջ է մտել 2016 թվականի մայիսի 5-ից, սակայն կսկսի կիրառվել 2018 թվականի մայիսի 6-ից[41]:

Նոր կանոնների մշակումը օբյեկտիվորեն պայմանավորված է անձնաց հետադարձ վերահսկողություն ապահովելու իրավունքի տրամադրմամբ, ինչպես նաև օրենսդրությունը բիզնես միջավայրին համապատասխանեցնելու նպատակով: Բարեփոխումները նպաստելու են ԵՄ քաղաքացիներին և բիզնես ոլորտի ներկայացուցիչներին առավելագույնս օգտվել թվային տնտեսության հնարավորություններից: ԵՄ չորս ազատությունները՝ ապրանքների, ծառայությունների, կապիտալի և աշխատուժի տեղաշարժը առանց սահմանափակումների, ուղղակիորեն առնչվում է նաև անձնական տվյալների ազատ տեղաշարժին, ինչը համապարփակ և միասնական իրավակարգավում է պահանջում:

Նոր ռեգլամենտը իրավակարգավումների տեսանկյունից նախատեսում է հետևյալ հայեցակարգային փոփոխությունները՝

[41] Անձնական տվյալների պաշտպանության քաղաքականության ուղեցույց, http://www.osf.am/wp-content/uploads/2015/04/DataProPolicyGuide_arm_final.pdf

1) Տարածքային իրավասության ընդլայնում: Քննարկվող ռեգլամենտը իր իրավասությունը տարածում է նաև ԵՄ-ից դուրս գտնվող կազմակերպությունների վրա: Նպատակը մեկն է տվյալների սուբյկենտների կողմից ԵՄ մատակարարվող ապրանքների և ծառայությունների պատշաճ վերահսկողությունը: Այդ կազմակերպությունները իրավասու են իրենց ներկայացուցիչները նշանակել ԵՄ-ում:

2) Հաշվետվողականությունը և գաղտնիությունը: Տվյալների վերահսկիչները ծանրաբեռնված են հետևյալ պարտականություններով՝ իրականացնելու պատշաճ վարչարարություն, գնահատական տալ տվյալների մշակման ընթացքում տվյալների սուբյեկտի իրավունքների խախտման հնարավոր ռիսկայնության մասին, տվյալների պաշտպանությունը իրականացնել կառուցողական և արդյունավետ եղանակով:

3) Տվյալների պաշտպանության տեսուչի պաշտոնի ստեղծումը: Վերջինս պետք է լինի որակավորված փորձագետ տվյալների պաշտպանության ոլորտում: Տվյալներ մշակողները և տվյալների վերստուգիչները հաշվետու են այս պաշտոնյային:

4) Տվյալների արտահոսքի վերաբերյալ ծանուցումը: Տվյալների վերահսկիչները տվյալների մեծ արտահոսքի պարագայում այդ մասին պարտավոր են 72 ժամվա ընթացքում տեղյակ պահել Տվյալների պաշտպանության տեսուչին: Որոշ պարագաներում այդպիսի ծանուցում ստանալու իրավունք ունի նաև տվյալների սուբյեկտը:

5) Տվյալների պաշտպանության տեսուչի կողմից տույժերի նշանակման հնարավորությունը: Ռեգլամենտը նախատեսում է բազմատեսակ սանկցիաների կիրառման հնարավորություն տվյալների պաշտպանության մասին օրենսդրությունը խախտելու պարագայում: Օրինակ՝ 20 միլիոն եվրո առանց տվայլների սուբյեկտի համաձայնության վերջինիս տվյալները մշակելու համար:

6) Մեկ պատուհանի սկզբունքի կիրառումը, որը հանդիսանում է այս ռեգլամենտի առանցքային կետերից մեկը: Ենթադրվում է, որ այս սկզբունքը հնարավորությունն կընձեռի այն կազմակերպություններին, որոնք գործունեություն են իրականացնում ԵՄ մի քանի պետություններում վերահսկվել միայն մեկ պետության իրավասու մարմնի կողմից: Սակայն կանոնակարգի համատեքստում հստակ մոտեցում չկա այն

կազմակերպությունների հետ փոխհարաբերությունների մասին, որոնք դուրս են ԵՄ սահմաններից:

7) Տվյալների պաշտպանության նոր Եվրոպական խորհուրդը, որը կազմված է լինելու խորհրդի ղեկավարությունից և ԵՄ-ում Տվյալների պաշտպանության ներկայացուցիչներից: Խորհուրդը իր առանցքային դերակատարությունն է ունենալու մեկ պատուհանի սկզբունքի կենսագործման համար:

8) Տվյալների միջազգային փոխանցումը: Այս ոլորտում ավելացել է այնպիսի հասկացություն ինչպիսին հանդիսանում է օրինական շահեր եզրույթը, վերջինս ենթադրում է, որ այդպիսի տվյալները կարող են փոխանցվել, եթե վերաբերվում են մի քանի սուբյեկտների և Տվյալների պաշտպանության տեսուչը տվել է իր համաձայնությունը[42]:

[42] Անձնական տվյալների պաշտպանության քաղաքականության ուղեցույց, http://www.osf.am/wp-content/uploads/2015/04/DataProPolicyGuide_arm_final.pdf

ԳԼՈՒԽ 2. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ԻՐԱՎՈՒՆՔԻ ԻՐԱՑՄԱՆ ԿԱՌՈՒՑՎԱԿԱՐԳԵՐԸ

2.1.Անձնական տվյալների պաշտպանության իրավունքի իրացման կառուցակարգերը ՀՀ-ում

Անձնական տվյալների պաշտպանությունն առնչվում է կյանքի բոլոր ոլորտներին՝ կրթությունից, առողջապահությունից մինչև մարդու մուտքն ու ելքը սահմանային անցակետերով: Չկա մի ոլորտ, որտեղ անձնական տվյալների պաշտպանության խնդիրը չծագի՝ պետական, թե մասնավոր: Այս և նմանատիպ այլ խնդիրների լուծման համար պետական քաղաքականության գործունեությունն ուղղված է ինչպես այս իրավունքի մասին հանրային իրազեկմանը, այնպես էլ օրենսդրական կարգավորմանը: Անձնական տվյալների պաշտպանության իրավունքի իրացման համար Հայաստանի Հանրապետությունում իրականացվել և շարունակվում են իրականցվել բազում գործնական քայլեր: Մասնավորապես, այս ոլորտի կարգավորման համար 2015 թվականին ստեղծվեծ Անձնական տվյալների պաշտպանության գործակալությունը՝ որպես ՀՀ Արդարադատության նախարարության առանձնացված ստորաբաժանում, որի հիմնական նպատակներն ու խնդիրներն են՝ անձնական տվյալների մշակողների ռեեստրի վարման աշխատանքների ապահովումը, անձնական տվյալների պաշտպանության հետ կապված հարաբերությունների սուբյեկտների իրավունքների պաշտպանության ապահովումը, իր իրավասության սահմաններում անձնական տվյալների մշակման օրինականության ապահովումը[43]:

Անձնական տվյալների պաշտպանության իրավունքի իրացման համատեքստում ՀՀ-ում որպես կարգավորման ենթակա առաջնահերթ ոլորտներ ընտրվել են տեսահսկումը, որը թե՛ պետական, թե՛ մասնավոր ընկերությունների կողմից իրականացվում է օրենքի համատարած խախտումներով, անցանկալի առևտրային հաղորդագրությունները, որոնք բջջային հեռախոս ունեցողները

[43] Անձնական տվյալների պաշտպանության գործակալության կանոնադրությունը տես ՀՀ արդարադատության նախարարության կայքէջում՝ http://www.justice.am/structures/view/structure/32

ստանում են՝ առանց նախնական համաձայնության, և անչափահասների անձնական տվյալների պաշտպանությունը:

Այս ուղղություններով Հայաստանի Հանրապետությունում իրականացվել են մի շարք գործուն քայլեր: Մասնավորապես.

- Տեսահսկման ուղեցույցը[44], որը մշակվել է Վրաստանի նմանատիպ ուղեցույցի հիման վրա, արդեն ընդունվել է:
- Խորհրդատվական որոշումներ են արձակվել, որով համապատասխան կառույցներին իրազեկել են, թե ինչպես պետք է պաշտպանվեն երեխաների իրավունքները: Անչափահասների իրավունքներին առնչվող գործերով վարույթներից առանձնացնենք մեկը, որը հարուցվել է Երևանի ավագանու «Բարև Երևան» խմբակցության անդամ Անահիտ Բախշյանի դիմումի հիման վրա հարուցված վարչական վարույթի արդունքում: Ըստ Բախշյանի՝ Երևանի 16 դպրոցների դասասենյակներում և ուսուցչանոցներում իրականացվում է տեսահսկում[45]: Վարչական վարույթը հարուցվել է՝ պարզելու համար, թե որքանով է դա իրավաչափ, որն է եղել նպատակը, արդյոք իրականացվում է օրենքի դրույթներին համապատասխան: Գործը հիմա վարչական լսումների փուլում է:
- 2017 թվականին Հանրության դատին է հանձնվել անչափահասների անձնական տվյալների պաշտպանության մասին ուղեցույցը: Այն տարբեր ասպեկտներ է ներառում՝ տվյալների փոխանցում, պաշտպանություն ինտերնետում, տեսահսկում ուսումնական հաստատություններում, մոռացվելու իրավունք[46]:

[44] Տեսահսկման ուղեցույց, ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալություն, 2016թ. Հասնելի է՝ http://www.foi.am/u_files/file/Manual_Video.pdf

[45] ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության 2015 հոկտեմբերից 2016 հունվար ընկած ժամանակահատվածի հանրային հաշվետվություն http://moj.am/storage/files/legal_acts/legal_acts_5389572924341_Annual-report-PDPA.pdf

[46] Երեխաների անձնական տվյալների պաշտպանության մասին ուղեցույց, ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալություն, 2017թ., Հասանելի է՝ http://iravaban.net/wp-content/uploads/2017/02/001.Ughecuyc-erexaneri_andznakan_tvyalner.pdf

- Անցանկալի առևտրային հաղորդագրությունների հարցը փորձ է արվել լուծել օրենսդրական ճանապարհով. օրենքի նախագիծն արդեն կառավարությունում է, շուտով կուղարկվի ԱԺ: Այն սահմանում է, թե ինչ է անցանկալի հաղորդագրությունը (երբ մարդն առանց իր համաձայնության իր հեռախոսահամարին ստանում է առևտրային բնույթի հաղորդագրություն, ինչն անթույլատրելի է և նախատեսում է վարչական պատասխանատվություն), երկրորդ՝ եթե մարդը մի օր մի տեղ շփոթվել է և համաձայնություն է տվել, պիտի հնարավորություն ունենա այդ համաձայնությունը հետ կանչելու: Ընդունման դեպքում այս երկու նորմերն օրենքի ուժ կստանան և կդառնան պարտադիր:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը նոր է. Ընդ որում, Օրենքով սահմանված են անձնական տվյալների պաշտպանության նոր կառուցակարգեր, անձնական տվյալների հետ վարվելու նոր կանոններ: Հետևաբար, բազմաթիվ քաղաքացիներ, անձնական տվյալներ մշակող կազմակերպություններ և պետական մարմիններ դեռ բավարար չափով տեղյակ չեն, թե Օրենքի կարգավորումներն ինչ իրավունքներ ու պարտականություններ են սահմանում իրենց համար, ուստի, 2016թ.-ի ընթացքում շատ քաղաքացիներ, կազմակերպություններ դիմել են Գործակալությանը՝ Օրենքի վերաբերյալ խորհրդատվություն ստանալու համար: 2016թ.-ին Գործակալությունը 343 անձի և կազմակերպության տրամադրել է խորհրդատվություն, որից 40 քաղաքացի, 187 իրավաբանական անձ, 82 պետական մարմին (այդ թվում՝ ՏԻՄ-եր և պետական հիմնարկներ), 22 լրագրող, 5 ՀԿ և 7 փաստաբան:

Դիմողների մեծ մասը՝ 66%-ը, խնդրել է խորհրդատվություն կենսաչափական և հատուկ կատեգորիայի անձնական տվյալների մշակման ընթացակարգերի և այդ մասին ծանուցման վերաբերյալ:

Դիմողների 8%-ը խնդրել է խորհրդատվություն անձնական տվյալների անվտանգության ապահովման վերաբերյալ, իսկ 7%-ը՝ անձնական տվյալներն այլ երկիր փոխանցելու վերաբերյալ: Դիմողների մնացած 19%-ը Գործակալությունից խորհրդատվություն է խնդրել տարբեր՝ երեխաների անձնական տվյալների

պաշտպանության, անցանկալի հաղորդագրությունների (ուղղակի մարքեթինգ), տեսահսկման և այլ հարցերի վերաբերյալ[47]:

Համապատասխան պատժամիջոցները և անձնական տվյալների պաշտպանության միջոցները անձնական տվյալների պաշտպանության օրենսդրության իրացման հիմնական մեխանիզմն են: Եվրոպայի խորհրդի կոնվենցիան չի որոշակիացնում այն պատժամիջոցները, որոնք պետք է ներդրվեն կոնվենցիան ստորագրած երկրների կողմից, հիմնվելով անդամ-պետությունների օրենսդրական ավանդույթների և հանրային շահերի բավարարման պահանջների վրա: Եվրոպական երկրներում ընդհանուր մոտեցումը հետևյալն է.

- ֆինանսական, սովորաբար վարչական պատժամիջոցները կիրառվում են տվյալների հավաքագրման, պահպանման և մշակման նկատմամբ անփութության, կողմնակալ և/կամ անպատշաճ վերաբերմունքի դեպքում, և
- քրեական տուգանքները և տույժերը կիրառվում են անհատների իրավունքների կանխամտածված և գիտակցաբար թույլ տված այն խախտումների համար, որոնք սովորաբար պատճառում են նյութական կամ բարոյական վնաս:

Հարկ է նշել, որ վարչական պատժամիջոցները սովորաբար սահմանվում են կոնկրետ խախտումների, այլ ոչ թե ընդհանուր խախտումների համար: Եվրոպական երկրների մեծ մասում վարչական պատժամիջոցներ են նախատեսվում ծանուցման պարտականության չկատարման, տվյալների հավաքագրման, պահպանման, մշակման և ոչնչացման կանոնների խախտումների համար: Տվյալների օրինական ոչնչացման հարցը կարևորվեց ավելի ուշ, երբ էլեկտրոնային եղանակով պահվող տվյալների արժեքը բարձրացավ:

Եվրոպական երկրների փորձը այդ առումով բավականին միասնական է և ենթադրում է և վարչական, և քրեական պատասխանատվության միջոցներ:

[47] ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության 2016 թ. գործունեության հանրային հաշվետվություն, Հասանելի է՝ http://moj.am/storage/files/legal_acts/legal_acts_8577044455541_Annual-report-2017_ARM.pdf

Այն բոլոր դեպքերում, երբ քաղաքացիները համարում են, որ անձնական տվյալների պաշտպանության իրենց իրավունքը ոտնահարվել է, իրենց անձնական տվյալներն օգտագործվել կամ այլ կերպ մշակվել են օրենքի խախտմամբ, առանց իրենց համաձայնության կամ իրավական հիմքի, կարող են դիմել Անձնական տվյալների պաշտպանության գործակալությանը՝ վարչական վարույթի շրջանակներում իրենց հարցի քննության համար:

Լինում են նաև դեպքեր, երբ հասարակական կազմակերպությունները կամ քաղաքացիները տեղեկացնում են Անձնական տվյալների պաշտպանության գործակալությանը այս կամ այն կազմակերպության, մարմնի կողմից մարդկանց անձնական տվյալների պաշտպանության իրավունքի խախտման մասին (ոչ թե կոնկրետ անձանց, այլ անորոշ թվով անձանց, բոլորին վերաբերող) կամ իր վերլուծությունների, ուսումնասիրությունների ընթացքում Անձնական տվյալների պաշտպանության գործակալությունն ինքն է հանդիպում անձնական տվյալների խախտում ենթադրող դեպքերի: Նման դեպքերում, երբ խոսքը չի վերաբերում կոնկրետ անձանց իրավունքի խախտմանը, Գործակալությունը վարչական վարույթ է իրականացնում սեփական նախաձեռնությամբ:

2016թ.-ի ընթացքում Անձնական տվյալների պաշտպանության գործակալությունում քաղաքացիների դիմումների հիման վրա կամ Գործակալության նախաձեռնությամբ հարուցվել է 11 վարչական վարույթ, որոնցից 9-ով կայացվել է որոշում, իսկ 2-ը դեռ քննության ընթացքում են: Ստորև վարչական վարույթներով կոնկրետ գործերի ամփոփ նկարագրությունն է՝ ներկայացված ըստ վարույթի հարուցման ժամանակագրության[48]:

Անձնական տվյալների պաշտպանության գործակալությունն այս գործով որոշել էր բավարարել դիմումատուի պահանջը՝ Իրավաբանական անձանց պետական ռեգիստրի գործակալությունից պահանջելով իրավաբանական անձանց պետական գրանցամատյանից երեք աշխատանքային օրվա ընթացքում ոչնչացնել

[48] ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության 2016 թ. գործունեության հանրային հաշվետվություն, Հասանելի է՝ http://moj.am/storage/files/legal_acts/legal_acts_8577044455541_Annual-report-2017_ARM.pdf

«Կոնցեռն-Դիալոգ» ՓԲԸ-ի մասնակիցների (բաժնետերերի) կազմի, նրանց մասնակից դառնալու, մասնակցության չափերի և դրանց փոփոխության վերաբերյալ տեղեկատվությունը:

2016թ.-ի մարտի 1-ին Գործակալությունը վարույթ էր հարուցել՝ պարզելու, թե արդյոք թմրադեղ ստացող հիվանդների բժշկական անձնական տվյալները և նրանց օգնող անձանց մասին տեղեկությունները բժշկական հաստատությունների կողմից ՀՀ ոստիկանությանը փոխանցելը համապատասխանու՞մ է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջներին: Վարույթը հիմնված էր Human Rights Watch միջազգային ՀԿ-ի կողմից Գործակալությանն ուղղված գրության վրա: Գործակալությունը հաշվի էր առել «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջները, և վարույթի հիմքում ընկած տեղեկությունների բնույթը՝ որպես «բժշկական գաղտնիք»:

Գործակալությունն իր որոշմամբ հաստատել էր, որ բժշկական բնույթի տեղեկությունները գաղտնի պահելը մարդու իրավունքն է, իսկ գաղտնիության ապահովումը՝ բժշկական օգնություն և սպասարկում իրականացնողների պարտականությունը:

Գործակալությունը որոշեց, որ թեև թմրադեղ ստացող հիվանդների անձնական տվյալները, ինչպես նաև եթե հիվանդն ընդունակ չէ ինքնուրույն ընդունել թմրադեղը, այն անձի անձնական տվյալները, ով վերցնում է թմրադեղը և օգնում հիվանդին ընդունել այն, ՀՀ ոստիկանության կողմից ստանալու հնարավորությունը նախատեսված է օրենքով, սակայն որևէ իրավական ակտով սահմանված չեն նշված անձնական տվյալների փոխանցման կարգը և պայմանները, և այս պարագայում ապահովված չէ անձնական տվյալների մշակման համաչափության սկզբունքը:

Ի կատարումն Գործակալության որոշման՝ ՀՀ առողջապահության նախարարությունը շրջաբերականներով դիմել էր իր ենթակայության տակ գտնվող բժշկական հաստատություններին՝ պահանջելով ապահովել բժշկական անձնական տվյալների գաղտնիությունը, դրանք այլ անձանց փոխանցել միայն օրենքով սահմանված դեպքերում և կարգով:

Նախարարությունը շրջաբերականով դիմել էր նաև Երևանի քաղաքապետարանին և ՀՀ մարզպետարաններին՝ նրանց ենթակայությամբ գործող բժշկական հաստատություններին՝ համապատասխան պահանջով դիմելու համար:

2016թ.-ի մարտի 1-ին Գործակալությունը վարույթ է հարուցել՝ պարզելու, թե արդյոք Երևանի քաղաքապետարանի («Փարքինգ Սիթի Սերվիս» ՓԲԸ-ի) կողմից Երևան քաղաքի վճարովի ավտոկայանատեղերում (կարմիր գծեր) տեղադրված տեսախցիկներով արվող տեսագրությունը համապատասխանու՞մ է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջներին: Վարույթի շրջանակներում Գործակալությունը արձանագրեց, որ տեսագրության միջոցով անձնական տվյալները պետք է հավաքվեն և օգտագործվեն բացառապես ավտոկայանատեղի տուրքի վճարման նկատմամբ հսկողության իրականացման նպատակով և այն նվազագույն քանակով, որն անհրաժեշտ է այդ նպատակին հասնելու համար, իսկ այն անձնական տվյալները, որոնք անհրաժեշտ չեն այդ նպատակի համար կամ անհամատեղելի են դրա հետ, չպետք է մշակվեն: Գործակալությունը որոշեց, որ տեսագրման իրականացումը, ինչպես նաև Երևանի քաղաքապետարանի կողմից վարչական իրավախախտումը ապացուցելու համար տեսագրությունը վարչական ակտի հասցեատիրոջը հասանելի դարձնելը, բողոքարկման դեպքում նրան ուղարկելը՝ առանց դրանում առկա այլ անձանց անձնական տվյալների ապանձնավորման, հակասում է անձնական տվյալների մշակման համաչափության սկզբունքին: Ի կատարումն Գործակալության որոշման՝ «Փարքինգ Սիթի Սերվիս» ՓԲԸ-ն ներկայացրել էր վարչական ակտի հասցեատիրոջն ուղարկվող տեսագրության նոր ֆորմատը, որի համաձայն՝ այդուհետ տեսագրության որակն իջեցնելու միջոցով ապանձնավորվելու են վարչական ակտի հասցեատերերին ուղարկվող տեսագրությունների մեջ առկա այլ անձինք և մեքենաների համարանիշները:

2016թ.-ի մայիսի 25-ին Գործակալությունը քաղաքացու դիմումի հիման վրա վարույթ էր հարուցել՝ ստուգելու, թե արդյոք ՔԿԱԳ ԵՀՍ տարածքային բաժնի կողմից անձի մահվան ակտի գրանցման վերաբերյալ տեղեկանքը տրամադրելու միջոցով նաև անձի առողջական վիճակի մասին տեղեկությունները այլ անձի (տվյալ դեպքում՝

փաստաբանի) տրամադրելը և փաստաբանի կողմից այդ տեղեկություններն օգտագործելը համապատասխանու՞մ է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջներին: Ուսումնասիրելով ոլորտը կարգավորող օրենսդրությունը՝ Գործակալությունը որոշեց, որ քաղաքացու մահվան պատճառ հանդիսացած հիվանդությունների մասին տեղեկություններ (առողջական տվյալներ) պարունակող տեղեկանքը փաստաբան Վանիկ Մարգարյանին ՔԿԱԳ ԵՀՍ տարածքային բաժնի կողմից տրամադրելը չի հակասում «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքին, քանի որ նախատեսված է օրենքով: 2016թ.-ի օգոստոսի 30-ին քաղաքացին բողոք էր ներկայացրել Գործակալությանը՝ խնդրելով վերանայել իր որոշումը: Քաղաքացու բողոքի հիման վրա Գործակալությունը ևս մեկ անգամ ստուգել է ՔԿԱԳ-ի գործողությունների համապատասխանությունն «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջներին և որոշել, որ նախորդիվ կայացրած իր որոշումը պետք է թողնել անփոփոխ[49]:

2016թ.-ի հունիսի 10-ին Գործակալությունը վարույթ է հարուցել՝ ստուգելու թե արդյոք nutcall.com կայքի միջոցով ՌԴ քաղաքացիների անձնական տվյալների հրապարակումը համապատասխանու՞մ է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջներին: Վարույթը հարուցվել է Գործակալության նախաձեռնությամբ՝ ՌԴ Կապի և զանգվածային հաղորդակցությունների նախարարության հաղորդակցության, տեղեկատվական տեխնոլոգիաների և զանգվածային հաղորդակցությունների վերահսկողության դաշնային ծառայության գրության հիման վրա: Ծառայությունն իր գրությամբ հայտնել էր, որ nutcall.com դոմեյնի ադմինիստրատորը Stark Industries (Սթարք Ինդասթրիզ) հայկական կազմակերպությունն է:

Վարույթի ընթացքում պարզվել էր, որ Սթարք Ինդասթրիզ կազմակերպությունը nutcall.com կայքին միայն տեխնիկական օժանդակություն է ցուցաբերում և որևէ կերպ չի առնչվում nutcall.com-ի գործունեությանը, կայքի

[49] ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության 2016 թ. գործունեության հանրային հաշվետվություն, Հասանելի է՝ http://moj.am/storage/files/legal_acts/legal_acts_8577044455541_Annual-report-2017_ARM.pdf

սեփականատերը կամ գործարկողը չէ, այսինքն՝ «Սթարք Ինդասթրիզ» ՍՊԸ-ն այս վարույթի արդյունքում կայացվելիք վարչական ակտի հասցեատեր չէ: Արդյունքում, վարչական վարույթը կարճվել է: Սակայն, վարույթի ընթացքում Գործակալության միջամտությամբ nutcall.com կայքը խմբագրել է կայքի բովանդակությունը և ապահովել, որ այնտեղ առկա այն անձանց անձնական տվյալները, ում համաձայնությունն առկա չէ, կայքից հեռացվեն: Բացի այդ, nutcall.am կայքում առանձին բաժնով տրվել է հետադարձ կապի հնարավորություն, որի միջոցով առաջարկել է հայտնել առանց համաձայնության անձնական տվյալների մշակման մասին և պարտավորվել միջոցներ ձեռնարկել:

Դպրոցներում տեսահսկման իրականացման վերաբերյալ 2016թ. նոյեմբերին Գործակալությունը 2 վարչական վարույթ էր հարուցել Երևանի 20 դպրոցներում տեսահսկման իրականացման համապատասխանությունն «Անձնական տվյալների մասին» ՀՀ օրենքին պարզելու նպատակով: Մի շարք դեպքերում գործակալությունը հայտնաբերել է անձնական տվյալների մշակման համաչափության, օրինականության սկզբունքների, ինչպես նաև անձնական տվյալների մշակման անվտանգության ապահովման խախտումներ: Որոշ դպրոցներում երեխաների տեսահսկումն իրականացվել է առանց նպատակը նախապես սահմանելու, այսինքն՝ թե կոնկրետ որ օրինական նպատակին հասնելու համար է իրականացվում երեխաների տեսահսկումը: Օրինական նպատակ այս դեպքում կարող է լինել անձանց և գույքը, ինչպես նաև անչափահասներին վնասակար ազդեցություններից պաշտպանելը[50]:

Խախտումների հաջորդ խումբը շեղումն է համաչափության սկզբունքից, երբ նպատակը չի համապատասխանում մշակվող տվյալների ծավալին: Այսինքն՝ մշակվում են անձնական տվյալներ, որոնք անհրաժեշտ չեն տվյալները մշակելու նպատակի համար, կամ անձնական տվյալները մշակվում են ավելի մեծ քանակով, քան անհրաժեշտ է սահմանված նպատակներին հասնելու համար: Ինչպես նաև որոշ դպրոցներում տեսահսկվող տարածքների տեսանելի հատվածներում չկան

[50] ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության 2016 թ. գործունեության հանրային հաշվետվություն, Հասանելի է՝ http://moj.am/storage/files/legal_acts/legal_acts_8577044455541_Annual-report-2017_ARM.pdf

նախազգուշացնող նշաններ՝ տեսախցիկների նկարահանման դաշտ մտնող բոլոր անձանց տեղեկացնելու տեսահսկման մասին: Գործակալությունը հաշվի է առել, որ ուսումնական հաստատություններում տեսախցիկների առկայությունը պետք է բխի երեխայի լավագույն շահից: Դպրոցներում տեսահսկման համակարգերը պետք է տեղադրվեն միայն այն բացառիկ դեպքերում, երբ այլ միջոցներով հնարավոր չէ հասնել հետապնդվող նպատակին:

Տեսախցիկների տեղադրման վայրերի ընտրությունը միշտ պետք է լինի հետապնդվող նպատակին համապատասխան և համարժեք: Գործակալությունը հատուկ ընդգծել է այն գաղափարը, որ տեսահսկումը հակակշռվում է աշակերտների, ուսուցիչների և այլ աշխատողների անձնական կյանքը հարգելու իրավունքով և կարող է միջամտել և խոչընդոտել մի կողմից աշակերտների կրթություն ստանալու և խոսքի ազատությանը:

Այսպիսով՝ Հայաստանի Հանրապետությունում անձնական տվյալների պաշտպանության իրավունքի ոլորտի ներկա քաղաքականության հիմնական հարցերը և դրան լուծման ուղիները սահմանելու համար կարելի է կատարել մի քանի գործնական առաջարկություն: Նախ, անձնական տվյալների պաշտպանության մարմնի գործունեության անկախությունը և թափանցիկությունը ապահովելու համար կարելի է ընտրել փորձագիտական խորհր հիմնելու մոդելը: Երկար՝ օրինակ տասը տարուց ոչ պակաս՝ փորձ ունեցող և մարդու/քաղաքացիական հասարակության իրավունքների պաշտպանության գծով հասարակական կազմակերպություններից կազմված փորձագետների խորհուրդը այն արդյունավետ գործիքը կարող է դառնալ, որը կապահովի տվյալ մարմնի հանրային վստահությունը և խորհրդի մասնագիտական փորձը: Այնուամենայնիվ, օրենքը պետք է նախատեսի մեխանիզմներ, երաշխավորելով մարդու/քաղաքացիական իրավունքների պաշտպանության ոլորտում հանրության և հասարակական կազմակերպությունների կողմից հարգված և իրական փորձ ունեցող անձի նշանակումը:

Տվյալների պաշտպանության մարմնի ֆինանսական անկախությունը նպատակահարմար է սահմանել օրենքով, դրանով իսկ բացառելով հնարավոր ճնշումները և կառավարության ազդեցությունը: Նման երաշխիք կարող է լինել

որոշակի դրույթ, որը կնախատեսի տվյալ մարմնի բյուջեն մեկ աշխատակցի հաշվով, սահմանելով այն ոչ պակաս, քան մարդու իրավունքների պաշտպանի գրասենյակի մեկ աշխատակցի համար նախատեսված բյուջետային գումարը:

Տվյալների պաշտպանության մարմնի արդյունավետ գործունեության համար պետք է ներդրվի հրապարակային հաշվետվողականություն հասկացությունը՝ Ազգային ժողովին ներկայացվող տարեկան զեկույցի և պաշտոնական հրապարակման ձևով: Ի լրումն, փորձագետների խորհրդի ձևավորման դեպքում այն կարող է իր կարծիքը ներկայացնել տվյալ մարմնի հաշվետվության/գործունեության առնչությամբ:

2.2.Անձնական տվյալների պաշտպանության իրավունքի իրացումը ՀՀ տեսախցիկներով նկարահանումների դեպքում

Անձնական տվյալների պաշտպանության իրավունքի իրացման գործում Հայաստանի Հանրապետությունում գերակա ոլորտ է տեսախցիկներով նկարահանումների գործընթացում անձնական տվյալների պաշտպանության հարցը: Այս ուղղությամբ կարատվել են մի շարք գործնական քայլեր: Այդ քայլերից հատկանշական է հատկապես 2016 թվականին ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալության կողմից մշակված և հրատարակված տեսահսկման ուղեցույցը[51]:

Այդ ուղեցույցը Հայաստանի Հանրապետությունում համակարգված փաստաթուղթ է, որի հիմնական նպատակն է ներկայացնել տեսահսկման հիմնական կանոններն ու սկզբունքները՝ ապահովելով մարդկանց անձնական տվյալների պաշտպանությունը: Այս ուղեցույցի միջոցով ցանկացած ոք կարող է իրազեկվել տեսահսկամն ժամանակ անձնական տվյալների պաշտպանության իր իրավունքի իրացման մասին: Իսկ տեսահսկում իրականացնող յուրաքանչյուր անձ կամ

[51] Տեսահսկման ուղեցույց, ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալություն, Երևան 2016թ. http://www.foi.am/u_files/file/Manual_Video.pdf

կազմակերպություն պետք է առաջնորդվի «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով և այս ուղեցույցով: Ուղեցույցը մշակվել է՝ առաջնորդվելով «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջներով և տեսահսկման կարգավորման միջազգային չափանիշներով:

Մարդու տեսանկարը անձնական տվյալ է, որը թույլ է տալիս ուղղակի կամ անուղղակի նույնականացնել անձին: Հետևաբար, տեսախցիկի միջոցով իրականացվող տեսանկարահանումը և հսկողությունը, որպես անձնական տվյալի մշակում, նախատեսում է անձնական տվյալի մշակման, օգտագործման և պաշտպանության պահանջների և սկզբունքների ապահովում:

Տեսահսկման համակարգը տարածքի, միջոցառման, գործունեության կամ անձի տեսա/ձայնահսկումն է էլեկտրոնային սարքավորման միջոցով: Համակարգը կարող է աշխատել տեսագրման ռեժիմով (երբ տեսագրվում է) և իրական ժամանակում տվյալների փոխանցման եղանակով[52]:

Տեսահսկումը պետք է իրականացվի միայն օրենքով նախատեսված նպատակներով և առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով:

Օրինակ, կրթական հաստատությունում գույքի պաշտպանությունը ապահովելու նպատակով տեղադրված տեսահսկման համակարգը արգելվում է օգտագործել վերահսկելու ուսումնական գործընթացը: Տեսահսկման համակարգի տեղադրումը կարող է հետապնդել մեկից ավելի օրինական նպատակ: Օրինակ՝ առաջին օրինական նպատակը կարող է լինել հանցագործությունների հայտնաբերումը և կանխումը, իսկ երկրորդը՝ ճանապարհային երթևեկության անվտանգության ապահովումը:

Տվյալներ մշակողը պետք է տեսահսկման համակարգը օգտագործի միայն այն դեպքերում, երբ այլ եղանակներով անհնար է հասնել հետապնդվող նպատակին կամ պահանջվում է անհամաչափ ջանքեր: Պետք է հավասարակշռություն լինի

[52] Տեսահսկման ուղեցույց, ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալություն, Երևան 2016թ. http://www.foi.am/u_files/file/Manual_Video.pdf

հետապնդվող նպատակի և նկարահանվող անձի մասնավոր կյանքի պաշտպանության միջև (արդյո՞ք անհրաժեշտ է տեսախցիկ տեղադրել բժշկական հաստատության սպասասրահներում): Տեսահսկողը պարտավոր է տեսանկարները մշակել այն նվազագույն ծավալով, որն անհրաժեշտ է օրինական նպատակներին հասնելու համար:

Տեսախցիկը պետք է տեղադրվի այնպես, որ նրա տեսադաշտ ճշգրտորեն մտնեն միայն այն պատկերները, որոնք համապատասխանում են հսկողության նպատակին (համաչափության սկզբունք): Օրինակ, բնակելի շենքի տեսահսկման դեպքում պետք է անհնար լինի տեսնել, թե ով որ բնակարանն է մտնում:

Տեսաձայնագրում իրականացնելիս տեսահսկողը պարտավոր է հիմնավորել տեսաձայնագրման անհրաժեշտությունը: Միաժամանակ, տեսաձայնային հսկողություն իրականացնող համակարգերի օգտագործման դեպքում տվյալներ մշակողը համաչափության սկզբունքին համապատասխան պարտավոր է հիմնավորել ձայնային վերահսկման անհրաժեշտությունը: Տեսահսկման արդյունքում հավաքված տվյալները (ներառյալ տեսագրությունները և նկարները) պետք է պահպանվեն հետապնդվող նպատակին հասնելու համար անհրաժեշտ ժամկետով: Տեսախցիկով գրանցված անձնական տվյալները պետք է ջնջվեն որոշակի ժամկետում: 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 կարևոր շարժառիթների առկայության դեպքում տվյալների պահպանման ժամկետը կարող է երկարաձգվել (համաչափության սկզբունք): Որքան տվյալներն ավելի երկար ժամկետով են պահվում, այդքան դրանց անվտանգության պահանջները պետք է խիստ լիննեն:

Թափանցիկության սկզբունքը ներառում է մի կողմից տեսահսկում իրականացնողի պարտականությունը տեսահսկվող անձանց տեղեկացնելու տեսահսկման իրականացման վերաբերյալ (բարեխղճության սկզբունք), իսկ մյուս կողմից՝ տեսահսկվող անձանց իրենց անձնական տվյալների վերաբերյալ

տեղեկություններ ստանալու իրավունքը (տեղեկատվության մատչելիության սկզբունքը):

Տեսահսկում իրականացնող սուբյեկտը տեսանելի նախազգուշացման միջոցով պետք է տեսախցիկների նկարահանման դաշտ մտնող բոլոր անձանց տեղեկացնի տեսահսկման մասին: Այն դեպքում, երբ այդ պատկերները ցանկացած ձևով տեսաձայնագրվում են, տեսանելի ծանուցումը պետք է պարունակի նաև տեղեկություն, թե նկարահանված մարդիկ ումից կարող են ստանալ իրենց վերաբերյալ տեսագրությունը: Օրինակ, բնակելի շենքում պետք է տեսահսկման վերաբերյալ նախազգուշացումն ակնհայտորոն տեսանելի լինի շենք մտնող յուրաքանչյուր անձի համար: Եթե տեսահսկման տարածքն ընդարձակ է, տեսահսկողը կարող է ունենալ մի քանի նախազգուշացնող նշաններ կամ մեկ նշան՝ մուտքի դռան մոտ:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը սահմանում է, որ յուրաքանչյուրն ունի իր անձնական տվյալների մշակման մասին տեղեկություն ստանալու իրավունք[53]: Սա վերաբերում է նաև տեսահսկման միջոցով անձնական տվյալներ մշակելուն: Օրենքի 15-րդ հոդվածի համաձայն՝ անձն իրավունք ունի ստանալ տեղեկություն իրեն տեսահսկելու եղանակների (օրինակ՝ տեսագրում կամ տեսաձայնագրում), հիմքերի և նպատակների, տեսահսկվող տվյալների ցանկի (սահմանների) և տեսագրությունը ձեռք բերելու աղբյուրների մասին, ինպես նաև այն անձանց շրջանակը, որոնց կարող է փոխանցվել իր տեսագրությունը[54]: Յուրաքանչյուր անձնական տվյալ մշակող՝ տեսահսկում իրականացնող պետական կամ մասնավոր մարմին պարտավոր է տեսահսկման սուբյեկտին հնարավորություն ընձեռել անվճար ծանոթանալու տեսահսկման սուբյեկտին վերաբերող տեսագրությանը (տեսաձայնագրությանը), իսկ եթե տեսահսկում իրականացնողը պահպանում է տեսագրությունը (այսինքն կա տեսագրությունը ձեռք բերելու աղբյուր),

[53] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

[54] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, հոդված 15, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

ապա տեսահսկման սուբյեկտն իրավունք ունի նաև ստանալ տեսագրության կրկնօրինակը (ձեռք բերել տեսագրությունը):

Տեսահսկում իրականացնողը տեղեկությունները պետք է տրամադրի հասանելի ձևով, իսկ այդ տեղեկությունները չպետք է պարունակեն այլ սուբյեկտների անձնական տվյալներ: Հարկ է նշել, որ տեղեկությունները պետք է տրամադրվեն անվճար, եթե օրենքով այլ բան նախատեսված չէ: Տեսահսկման սուբյեկտը տեսագրությունը կարող է ստանալ նաև իր ներկայացրած կրիչով՝ կրկին անվճար: Եթե տեսահսկման սուբյեկտը չի նշել, թե ինչ կրիչով է ցանկանում ստանալ տեսագրությունը, ապա այն տրամադրվում է տեսահսկում իրականացնողի համար առավել ընդունելի կրիչով: Կարևորագույն սկզբունք է, որ անձի մասին տեղեկությունները չպետք է վաճառվեն նրան, իսկ վճարելու անհրաժեշտությունը պետք է կապված լինի միմիայն տեսագրության տրամադրման համար տեսահսկողի կատարած ծախսերը փոխհատուցելու հետ:

Ուղեցույցում սահմանվում են, որ տարբեր վայրերում տեսահսկում կարելի իրականացնել տարբեր նպատակներով: Կան նաև վայրեր որտեղ տեսահսկումն արգելվում է:

Հասարակական վայրը ներառում է փողոցները, մայթերը, հրապարակները, խաղահրապարակները, պուրակները, զբոսայգիները, մարզադաշտերը և այլ հասարակական վայրերը: Հասարակական վայրում տեսահսկում կարող է իրականացվել հետևյալ նպատակներով.

- հանցագործությունները կանխելու,
- անձանց անվտանգության և գույքի պաշտպանության,
- հասարակական կարգի պահպանության,
- անչափահասների վրա վնասակար ազդեցությունը կանխելու[55]:

[55] Տեսահսկման ուղեցույց, ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալություն, Երևան 2016թ. http://www.foi.am/u_files/file/Manual_Video.pdf

Փողոցների տեսահսկումն իրականցվում է նաև ճանապարհային երթևեկության անվտանգությունն ապահովելու նպատակով, որի շրջանակներում տեսագրությունները կամ տեսանկարները դրվում են վարորդներին վարչական պատասխանատվության ենթարկելու վարչական վարույթների հիմքում[56]:

Թանգարաններում, ռեստորաններում, մարզադահլիճներում, սրճարաններում, առևտրի կենտրոններում, խանութներում, տեսահսկումը կարող է իրականացվել անվտանգության ապահովման նկատառումով, հանցագործությունները կանխելու, անձանց անվտանգությունը, գույքը, ինչպես նաև գաղտնի տեղեկատվությունը պաշտպանելու նպատակով: Տեսահսկումն արգելվում է հասարակական վայրերի հանդերձարաններում և սանհանգույցներում:

Պետական կամ մասնավոր կազմակերպությունների տեսահսկումն արվում է անվտանգության ապահովման, անձանց անվտանգությունը և գույքը վնասներից պաշտպանելու, գաղտնի տեղեկատվության պաշտպանության նպատակով: Տեսախցիկը տեղադրվում է շենքերի մուտքի մոտ: Շենքերի ներսում՝ աշխատավայրում տեսահսկման համակարգը տեղադրվում է բացառիկ դեպքերում, եթե դա անհրաժեշտ է անձանց անվտանգությունը և գույքը վնասներից պաշտպանելու, ինչպես նաև գաղտնի տեղեկատվությունը պաշտպանելու նպատակով, եթե այլ միջոցներով հնարավոր չէ հասնել այդ նպատակներին:

Տեսահսկումն արգելվում է հանդերձարաններում, սանհանգույցներում, հանգստի սենյակներում, լողասենյակներում և մասնավոր պահարաններում: Աշխատավայրում տեսահսկման համակարգ տեղադրելուց առաջ տեսահսկողը պարտավոր է աշխատակազմին գրավոր տեղեկացնել համակարգի և աշխատողների իրավունքների մասին: Աշխատակիցներին անհրաժեշտ է բացատրել տեսահսկման անհրաժեշտությունը, նպատակը և նրանց իրավունքները:

Տեսահսկման ուղեցույցով սահմանվում են նաև այն սկզբունքները, որո պետք է շահագործվեն տեսահսկման համակարգերը: Այդ սկզբունքներն են՝

[56] «Տեսանկարահանող կամ լուսանկարահանող սարքերով հայտնաբերված ճանապարհային երթևեկության կանոնների խախտումների վերաբերյալ գործերով իրականացվող վարչական վարույթի առանձնահատկությունների մասին» ՀՀ օրենք, ուժի մեջ է մտել 01.01.2009թ. Հասանելի՝ http://www.arlis.am/DocumentView.aspx?docid=48761

- Օրինականության սկզբունք: Անձնական տվյալները մշակվում են օրինական և որոշակի նպատակներով և առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով: Տեսահսկման համակարգի տեղադրումը կարող է հետապնդել մեկից ավելի օրինական նպատակ: Օրինակ՝ առաջին օրինական նպատակը կարող է լինել հանցագործությունների հայտնաբերումը և կանխումը, իսկ երկրորդը՝ ճանապարհային երթևեկության անվտանգության ապահովումը:
- Համաչափության սկզբունք: Տեսահսկողը պետք է գնահատի տեսախցիկի հնարավոր ազդեցությունը նկարահանման սուբյեկտների վրա, ինչպես նաև համոզված լինի, որ նպատակին հասնելու համար ուրիշ առավել հարմար միջոց գոյություն չունի: Տեսահսկողը պարտավոր է տեսանկարները մշակել այն նվազագույն ծավալով, որն անհրաժեշտ է օրինական նպատակներին հասնելու համար: Տեսախցիկը պետք է տեղադրվի այնպես, որ դրա տեսադաշտ ճշգրտորեն մտնեն միայն այն պատկերները, որոնք համապատասխանում են տեսահսկման նպատակին: Տեսաձայնագրում իրականացնելիս տեսահսկողը պարտավոր է հիմնավորել տեսաձայնագրման անհրաժեշտությունը: Տեսանկարահանման և տեսաձայնագրման նյութերը պահվում են որոշակի ժամկետով: Հետապնդվող նպատակներին հասնելուն պես անհրաժեշտ է ուղեփակել կամ ոչնչացնել տեսանկարները և տեսաձայնագրությունները: Որքան տվյալներն ավելի երկար ժամկետով են պահպանվում, այնքան դրանց պահպանությանն ուղղված պահանջները խստացվում են:
- Հավաստիության սկզբունքը: Տեսանկարահանման տվյալները պետք է լինեն ամբողջական, ճշգրիտ, պարզ և հնարավորինս թարմացված: Այս սկզբունքը նշանակում է, որ մի կողմից պետք է ապահովել անձնական տվյալների ճշգրտությունը (օրինակ, անձի անունը և ազգանունը, ծննդյան տարեթիվը ճիշտ գրանցվեն), որպեսզի անձի նույնականացումը

ծառայի իր նպատակին: Մյուս կողմից՝ այս սկզբունքը նշանակում է, որ արդեն հնացած տվյալները պետք է թարմացվեն (օրինակ, վավերականությունը կորցրած անձնագրային տվյալները փոխարինվեն նոր տվյալներով, կամ բժշկական հաստատությունը պետք է հիվանդի առողջական վիճակի մասին տվյալները թարմացնի, հակառակ դեպքում չի կարողանա պատշաճ բժշկական սպասարկում իրականացնել):

- Տեղեկատվություն ստանալու սկզբունքը: Այս իրավունքը երկու մաս ունի. մի կողմից, տեսանկարահանման սուբյեկտը պետք է նախապես իրազեկված լինի տվյալ վայրում տեսանկարահանման համակարգերի առկայության մասին: Մյուս կողմից, տեսանկարահանման սուբյեկտն իրավունք ունի ստանալ իր անձնական տվյալների վերաբերյալ տեղեկություններ:
- Անվտանգության սկզբունքը: Տեսահսկողի կողմից լիազորված անձանց կամ կազմակերպությունների համար պետք է սահմանել տեսանկարների անվտանգության ապահովման կանոններ և ընթացակարգեր: Տեսանկարների անվտանգությունն ապահովելու կարևոր պայմաններից է լավ պաշտպանված օպերացիոն կամ տեխնիկական, կազմակերպչական և ֆիզիկական համակարգերը: Համակարգերը լավ են պաշտպանված, եթե լիազորված աշխատակազմից բացի ուրիշ որևէ մեկը մուտք չունի համակարգ: Անհրաժեշտ է պարբերաբար ստուգել օպերացիոն համակարգերը, երաշխավորել տեսանկարների անվտանգությունը և գաղտնիությունը, կանխել դրանց կորուստը և անօրինական ձեռքբերումը:
- Գաղտնիության սկզբունքը: Տեսահսկողը պետք է հարգի անձանց մասնավոր կյանքի իրավունքը և ապահովի տեսանկարահանման և տեսաձայնագրման գաղտնիությունը: Լիազորված անձանցից բացի ոչ ոք իրավունք չունի ծանոթանալ տեսանկարահանման/տեսաձայնագրման նյութերին, եթե նման

անհրաժշտությունը պայմանավորված չէ Հայաստանի Հանրապետության օրենսդրությամբ[57]:

Անձնական տվյալների պաշտպանույթան մասին ՀՀ օրենքը խախտելու, այդ թվում անձնական տվյալ մշակելու (այդ թվում տեսահսկման միջոցով) օրենքով սահմանված կարգը խախտելու կամ տեսահսկման սուբյեկտի պահանջով մշակողի կողմից տեղեկատվություն չտրամադրելու կամ տրամադրման կարգը խախտելու համար սահմանված է վարչական պատասխանատվություն: Քանի որ տեսահսկումը նույնպես անձնական տվյալների մշակում է, վարչական պատասխանատությունը վրա կհասնի նաև տեսահսկումն առանց օրենքով սահմանված հիմքերի, առանց օրինական նպատակի կամ օրենքով սահմանված կարգի խախտմամբ իրականացնելու դեպքում: Օրենքը խախտելու համար սահմանված է տուգանք, որի չափը տարբեր խախտումների դեպքում տատանվում է 50.000 ՀՀ դրամից մինչև 500.000 ՀՀ դրամ: Անձն ազատվում է վարչական պատասխանատվությունից, եթե լիազոր մարմնի որոշմամբ սահմանված ժամկետում կամ մինչև վարչական պատասխանատվության ենթարկվելու վերաբերյալ որոշում կայացնելը անձը վերացրել է թույլ տված խախտումը և լիազոր մարմին է ներկայացրել ապացույցներ այդ մասին: Սա վկայում է այն մասին, որ սահմանված պատասխանատվությունն ունի ոչ միայն պատժելու, այլ նաև անձնական տվյալների պաշտպանության իրավունքի խախտումները կանխարգելելու նպատակ:

ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության կողմից քննվում են մի շարք դեպքեր, երբ ոտնահարվել են քաղաքացիների անձնական տվյալների պաշտպանության մասին օրենքը հենց տեսահսկման կանոների խախտման մասով: Մասնավորապես ՝ դպրոցներում տեսահսկման իրականացման վերաբերյալ 2016թ. նոյեմբերին Գործակալությունը 2 վարչական վարույթ էր հարուցել Երևանի 20 դպրոցներում

[57] Տեսահսկման ուղեցույց, ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալություն, Երևան 2016թ. http://www.foi.am/u_files/file/Manual_Video.pdf

տեսահսկման իրականացման համապատասխանությունն «Անձնական տվյալների մասին» ՀՀ օրենքին պարզելու նպատակով58:

Մի շարք դեպքերում գործակալությունը հայտնաբերել է անձնական տվյալների մշակման համաչափության, օրինականության սկզբունքների, ինչպես նաև անձնական տվյալների մշակման անվտանգության ապահովման խախտումներ: Որոշ դպրոցներում երեխաների տեսահսկումն իրականացվել է առանց նպատակը նախապես սահմանելու, այսինքն՝ թե կոնկրետ որ օրինական նպատակին հասնելու համար է իրականացվում երեխաների տեսահսկումը: Օրինական նպատակ այս դեպքում կարող է լինել անձանց և գույքը, ինչպես նաև անչափահասներին վնասակար ազդեցություններից պաշտպանելը: Խախտումների հաջորդ խումբը շեղումն է համաչափության սկզբունքից, երբ նպատակը չի համապատասխանում մշակվող տվյալների ծավալին: Այսինքն՝ մշակվում են անձնական տվյալներ, որոնք անհրաժեշտ չեն տվյալները մշակելու նպատակի համար, կամ անձնական տվյալները մշակվում են ավելի մեծ քանակով, քան անհրաժեշտ է սահմանված նպատակներին հասնելու համար: Ինչպես նաև որոշ դպրոցներում տեսահսկվող տարածքների տեսանելի հատվածներում չկան նախազգուշացնող նշաններ՝ տեսախցիկների նկարահանման դաշտ մտնող բոլոր անձանց տեղեկացնելու տեսահսկման մասին:

Գործակալությունը հաշվի է առել, որ ուսումնական հաստատություններում տեսախցիկների առկայությունը պետք է բխի երեխայի լավագույն շահից: Դպրոցներում տեսահսկման համակարգերը պետք է տեղադրվեն միայն այն բացառիկ դեպքերում, երբ այլ միջոցներով հնարավոր չէ հասնել հետապնդվող նպատակին: Տեսախցիկների տեղադրման վայրերի ընտրությունը միշտ պետք է լինի հետապնդվող նպատակին համապատասխան և համարժեք: Գործակալությունը հատուկ ընդգծել է այն գաղափարը, որ տեսահսկումը հակակշռվում է աշակերտների, ուսուցիչների և այլ աշխատողների անձնական կյանքը հարգելու իրավունքով և կարող է միջամտել և խոչընդոտել մի կողմից աշակերտների կրթություն ստանալու և խոսքի ազատությանը, իսկ մյուս կողմից՝ ուսուցիչների համար դասավանդման

[58] Հանրային հաշվետվություն, ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալություն, 2016թ. Հասանելի է՝ http://moj.am/storage/files/legal_acts/legal_acts_8577044455541_Annual-report-2017_ARM.pdf

ազատությանը: Պետք է հաշվի առնել նաև երեխայի՝ իր անհատականությունը զարգացնելու իրավունքը: Անշուշտ, երեխայի՝ իր անհատականությունը աստիճանաբար զարգացնելու իրավունքը խեղաթյուրվում է, եթե վաղ հասակից սկսած երեխան բնականոն երևույթ համարի իրեն տեսահսկելը: Ինչպես նաև, անվտանգության նպատակով իրականացվող տեսահսկումը չի կարող կիրառվել աշակերտների կարգապահության, ուսուցիչների աշխատանքի կամ ուսումնական գործընթացի որակի վերահսկողության կամ այլ նպատակով: Վարչական վարույթով կայացրած իր որոշմամբ Գործակալությունը պարտավորեցրել է Երևանի 20 դպրոցներին իրականացնել համապատասխան միջոցառումներ՝ երեխաների և ուսուցիչների տեսահսկումը «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով սահմանված սկզբունքներին և կանոններին համապատասխան իրականացնելու նպատակով:

Ամփոփելով կարող ենք նշել, որ տեսահսկման իրականացման գործընթացը Հայատասանի Հանրապետությունում ունի իրավական կարգավորում, սակայն շատ են տեսահսկման միջոցով անձնական տվյալների պաշտպանության իրավունքի ոտնահրաման դեպքերը: Քաղաքացինրը երբեմն չեն տիրապետում իրենց իրավունքներին և պահանջատեր չեն, ուստի իրավունքների ոտնահարման դեպքերն էլ չեն հասնում համապատասխան մարմիններին: Հայաստանի Հանրապետությունը՝ հանձինս ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության, հետևողական է այս հարցում և գործուն քայլեր է ձեռնարկում այս ոլորտում հասրակության իրավագիտակցության մակարդակի բարձրացման և հնարավոր ոտնձգությունների դեպքերի բացահայտման և կանխարգելիչ միջոցառումների իրականացման ուղղությամբ:

2.3.Անձնական տվյալների պաշտպանության իրավունքի իրացումը ՀՀ հանրային իշխանության մարմինների կողմից անձնական տվյալների

տիրապետմանը և օգտագործմանն ուղղված լիազորությունների իրականացման շրջանակներում

ՀՀ հանրային իշխանության մարմինները անձնական տվյալների հավաքագրման, մշակման և պաշտպանության գործընթացում անձնական տվյալների տիրապետմանը և օգտագործմանն ուղղված իրենց լիազորությունների իրականացման շրջանակներում առաջնորդվում են «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով: Համաձայն այս օրենքի 18-րդ հոդվածի պետական իշխանության մարմինները, որպես անձնական տվյալների մշակող ունեն հետևյալ պարտականությունները անձնական տվյալները հավաքելու ընթացքում.

- Անձնական տվյալները մշակելու ընթացքում պարտավոր են տվյալների սուբյեկտի պահանջով նրան տրամադրել օրենքի նախատեսված տեղեկատվությունը:
- Ոչ ամբողջական, ոչ ճշգրիտ, հնացած, անօրինական ճանապարհով ձեռք բերված կամ մշակելու նպատակներին հասնելու համար ոչ անհրաժեշտ անձնական տվյալների դեպքում պարտավոր են անհրաժեշտ գործողություններ իրականացնել դրանք ամբողջացնելու, թարմացնելու, ուղղելու կամ ոչնչացնելու ուղղությամբ:
- պարտավոր են տվյալների սուբյեկտին գրավոր պարզաբանել անձնական տվյալները չտրամադրելու հետևանքները, այդ թվում՝ անձնական տվյալների սուբյեկտի իրավունքները:
- Եթե անձնական տվյալներն ստացվել են ոչ տվյալների սուբյեկտից, բացառությամբ օրենքով նախատեսված դեպքերի, ինչպես նաև հանրամատչելի անձնական տվյալների, ապա պետական իշխանության մարմինները մինչև այդպիսի անձնական տվյալները մշակելը պարտավոր են տվյալների սուբյեկտին տրամադրել հետևյալ տեղեկատվությունը.
    - 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.
- անձնական տվյալների հավանական օգտագործողների շրջանակը.
- տվյալների սուբյեկտի՝ սույն օրենքով սահմանված իրավունքները[59]:

ՀՀ հանրային իշխանության մարմինները ունեն հետևյալ պարտականությունները Անձնական տվյալներ մշակելու անվտանգության ապահովման նկատառումներով՝

- նրանք պարտավոր են ոչնչացնել կամ ուղեփակել անձնական այն տվյալները, որոնք անհրաժեշտ չեն օրինական նպատակին հասնելու համար:
- Անձնական տվյալները մշակելու ընթացքում պարտավոր են օգտագործել գաղտնագրման միջոցներ՝ անձնական տվյալներ պարունակող տեղեկատվական համակարգերի պաշտպանվածությունը պատահական կորստից, տեղեկատվական համակարգեր անօրինական մուտք գործելուց, անձնական տվյալների անօրինական օգտագործումից, ձայնագրումից, ոչնչացումից, վերափոխումից, ուղեփակումից, կրկնօրինակումից, տարածումից և այլ միջամտությունից ապահովելու համար:
- ՀՀ հանրային իշխանության մարմինները պարտավոր են կանխել անձնական տվյալների մշակման համապատասխան տեխնոլոգիաների մատչելիությունը դրա իրավունքը չունեցող անձանց համար և ապահովել, որ այդ համակարգերի օրինական օգտագործողի համար հասանելի լինեն միայն իրենց կողմից մշակման ենթակա տվյալները և այն տվյալները, որոնցից թույլատրված է օգտվել:
- Տեղեկատվական համակարգերում անձնական տվյալները մշակելու անվտանգությունն ապահովելուն ներկայացվող պահանջները, կենսաչափական անձնական տվյալների նյութական կրիչներին և տեղեկատվական համակարգերից դուրս այդ անձնական տվյալները

[59] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, հոդված 18, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

պահպանելու տեխնոլոգիաներին ներկայացվող պահանջները սահմանվում են Հայաստանի Հանրապետության կառավարության որոշմամբ:

«Անձնական տվյալների պաշտպանության» մասին ՀՀ օրենքով հսկողություն իրականացնող այլ մարմին սահմանված լինելու դեպքում այդ մարմինը օրենքով իրեն վերապահված լիազորությունների շրջանակներում կարող է սահմանել օրենքով նախատեսված՝ Հայաստանի Հանրապետության կառավարության որոշմամբ սահմանված պահանջներից ավելի բարձր պահանջներ:

Տեղեկատվական համակարգերից դուրս կենսաչափական անձնական տվյալների օգտագործումն ու պահպանումը կարող են իրականացվել միայն այնպիսի նյութական կրիչների միջոցով, տեխնոլոգիաների կիրառմամբ կամ ձևերով, որոնք ապահովում են այդ տվյալների պաշտպանվածությունը դրանց անօրինական մուտք գործելուց, անձնական տվյալների անօրինական օգտագործումից, ոչնչացումից, վերափոխումից, ուղեփակումից, կրկնօրինակումից, տարածումից և այլն:

ՀՀ հանրային իշխանության մարմինները պարտավոր են պահպանել անձնական տվյալների գաղտնիությունը ինչպես անձնական տվյալները մշակելու հետ առնչվող ծառայողական կամ աշխատանքային պարտականությունները կատարելու ընթացքում, այնպես էլ դրա ավարտից հետո:

ՀՀ հանրային իշխանության մարմինները իրենց տիրապետման տակ գտնվող անձնական տվյալներ մշակող էլեկտրոնային համակարգերը բավարար պաշտպանության մակարդակ ունեցող ճանաչելու և ռեեստրում ընդգրկելու նպատակով կարող են դիմել անձնական տվյալների պաշտպանության լիազոր մարմին:

ՀՀ հանրային իշխանության մարմինները պարտավոր են օրենքով սահմանված կարգով տվյալների սուբյեկտին և լիազոր մարմնին տեղեկատվություն տրամադրել տվյալների սուբյեկտի վերաբերյալ անձնական տվյալների առկայության մասին կամ հնարավորություն ընձեռել ծանոթանալու դրանց գրավոր հարցումը ստանալուց հետո՝ հինգ օրվա ընթացքում:

ՀՀ հանրային իշխանության մարմինները պարտավոր են տվյալների սուբյեկտին հնարավորություն ընձեռել անվճար ծանոթանալու տվյալների սուբյեկտին

վերաբերող անձնական տվյալներին: Եթե տվյալների սուբյեկտի անձնական տվյալներն ամբողջական կամ ճշգրիտ չեն կամ հնացած են կամ ձեռք են բերվել անօրինական ճանապարհով կամ անհրաժեշտ չեն մշակելու նպատակներին հասնելու համար, ապա մշակողի կամ լիազորված անձի կողմից դրանք հայտնաբերվելու կամ տվյալների սուբյեկտի կամ օրինական ներկայացուցչի (կամ լիազորված անձի) կողմից դիմում ստանալուց հետո մշակողը պարտավոր է անհապաղ կամ նման հնարավորության բացակայության դեպքում երեք աշխատանքային օրվա ընթացքում անհրաժեշտ գործողություններ իրականացնել դրանք ամբողջացնելու, թարմացնելու, ուղղելու, ուղեփակելու կամ ոչնչացնելու ուղղությամբ[60]:

ՀՀ հանրային իշխանության մարմինները պարտավոր են անձնական տվյալների պաշտպանության լիազոր մարմնի գրավոր հարցման հիման վրա նրա գործունեության իրականացման համար անհրաժեշտ տեղեկատվությունը տրամադրել հարցումն ստանալու օրվանից հինգ օրվա ընթացքում:

Տվյալների սուբյեկտի գրավոր պահանջի հիման վրա տվյալների սուբյեկտի անձնական տվյալները տրամադրելը, ուղղելը, ուղեփակելը կամ ոչնչացնելը մերժելու դեպքում մշակողը պարտավոր է տվյալների սուբյեկտին և լիազոր մարմնին հարցումն ստանալու օրվանից հինգ օրվա ընթացքում տրամադրել պատճառաբանված գրավոր որոշում՝ հղում կատարելով այն օրենքի դրույթներին, որոնք հիմք են հանդիսացել որոշում ընդունելու համար:

Անձնական տվյալները տրամադրելը, ուղղելը, ուղեփակելը կամ ոչնչացնելը մերժելու հիմքերը լիազոր մարմնի կողմից հիմնավորված չհամարվելու դեպքում ՀՀ հանրային իշխանության մարմինները պարտավոր են անհապաղ տրամադրել, ուղղել, ուղեփակել կամ ոչնչացնել տվյալների սուբյեկտի անձնական տվյալները կամ լիազոր մարմնի որոշումը բողոքարկել դատական կարգով:

Առանց անձնական տվյալների սուբյեկտի համաձայնության ՀՀ հանրային իշխանության մարմինները կարող են անձնական տվյալները փոխանցել երրորդ

[60] «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, հոդված 18,19, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338

անձանց կամ տվյալներից օգտվելու հնարավորություն տրամադրել, եթե դա նախատեսված է օրենքով և ունի բավարար պաշտպանության մակարդակ:

Առանց անձնական տվյալների սուբյեկտի համաձայնության ՀՀ հանրային իշխանության մարմինները կարող են հատուկ կատեգորիայի անձնական տվյալներ փոխանցել երրորդ անձանց կամ տվյալներից օգտվելու հնարավորություն տրամադրել, եթե՝

- ՀՀ հանրային իշխանության մարմինները հանդիսանում են օրենքով կամ միջպետական պայմանագրով սահմանված հատուկ կատեգորիայի անձնական տվյալներ մշակող, այդ տեղեկության փոխանցումը ուղղակիորեն նախատեսված է օրենքով և ունի բավարար պաշտպանության մակարդակ.
- օրենքով նախատեսված բացառիկ դեպքերում հատուկ կատեգորիայի անձնական տվյալները կարող են փոխանցվել տվյալների սուբյեկտի կյանքի, առողջության կամ ազատության պաշտպանության համար:

Անձնական տվյալները կարող են այլ երկիր փոխանցվել տվյալների սուբյեկտի համաձայնությամբ, կամ եթե տվյալների փոխանցումը բխում է անձնական տվյալների մշակման նպատակներից և (կամ) անհրաժեշտ է այդ նպատակների իրագործման համար:

Առանց լիազոր մարմնի թույլտվության անձնական տվյալները կարող են փոխանցվել այլ պետություն, եթե այդ պետությունում ապահովված է անձնական տվյալների պաշտպանության բավարար մակարդակ: Անձնական տվյալների պաշտպանության բավարար մակարդակը համարվում է ապահովված, եթե՝

- անձնական տվյալները փոխանցվում են միջազգային պայմանագրերին համապատասխան.
- անձնական տվյալները փոխանցվում են լիազոր մարմնի կողմից պաշտոնական հրապարակված ցուցակում ընդգրկված որևէ երկիր:

Անձնական տվյալները կարող են փոխանցվել բավարար պաշտպանության մակարդակ չապահովող պետության տարածք միայն լիազոր մարմնի թույլտվությամբ, եթե անձնական տվյալները փոխանցվում են պայմանագրի հիման

վրա, և պայմանագրով նախատեսված են անձնական տվյալների պաշտպանության այնպիսի երաշխիքներ, որոնք լիազոր մարմնի կողմից հաստատվել են որպես բավարար պաշտպանություն ապահովող:

Օրենքով նախատեսված դեպքերում ՀՀ հանրային իշխանության մարմինները պարտավոր են նախքան այլ երկիր տվյալներ փոխանցելը գրավոր դիմել լիազոր մարմին՝ թույլտվություն ստանալու հայտով: Հայտում ՀՀ հանրային իշխանության մարմինները պարտավոր են նշել այն երկիրը, որտեղ փոխանցվում են անձնական տվյալները, անձնական տվյալներն ստացող սուբյեկտի նկարագրությունը (անվանումը, իրավակազմակերպչական ձևը), անհատական տվյալների նկարագրությունը (պարունակությունը), անձնական տվյալների մշակման, անձնական տվյալները փոխանցելու նպատակը և պայմանագիրը կամ դրա նախագիծը: Լիազոր մարմինը 30 օրվա ընթացքում պարտավոր է թույլատրել կամ մերժել հայտը: Լիազոր մարմինը կարող է ՀՀ հանրային իշխանության մարմիններից պահանջել լրացուցիչ տեղեկություններ՝ պահպանելով հայտը դիտարկելու ժամկետը: Այն դեպքում, երբ լիազոր մարմինը կգտնի, որ պայմանագրային երաշխիքները բավարար չեն, պարտավոր է նշել այն անհրաժեշտ փոփոխությունները, որոնք կապահովեն անձնական տվյալների պաշտպանության երաշխիքներ:

Անձնական տվյալների պաշտպանության լիազոր մարմինը պարբերաբար, սակայն ոչ պակաս, քան տարին մեկ անգամ, պարտավոր է վերանայել անձնական տվյալների պաշտպանության բավարար մակարդակն ապահովող երկրների ցուցակը[61] և հրապարակել փոփոխությունները պաշտոնական տեղեկագրում և իր պաշտոնական ինտերնետային կայքում:

Պետական մարմինների տնօրինության տակ գտնվող անձնական տվյալները կարող են փոխանցվել օտարերկրյա պետական մարմիններին միայն միջպետական պայմանագրերի շրջանակներում, իսկ ոչ պետական մարմիններին՝ օրենքի նորմերին համապատասխան:

[61] Անձնական տվյալների պաշտպանության բավարար մակարդակ ունեցող երկրների ցանկը» հաստատելու մասին ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալության որոշում, 17.01.2017թ., Հասանելի է http://moj.am/storage/uploads/002_Cucak-final.pdf

Անձնական տվյալների պաշտպանությունն իրականացնում է լիազոր մարմինը, որը գործում է Հայաստանի Հանրապետության կառավարության որոշմամբ սահմանված կառուցվածքով: ՀՀ արդարադատության նախարարության աշխատակազմի Անձնական տվյալների պաշտպանության գործակալությունը ՀՀ կառավարության՝ 2015թ.-ի հուլիսի 2-ի 734-Ն որոշմամբ ճանաչվել է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով նախատեսված լիազոր մարմին[62]:

Անձնական տվյալների պաշտպանության գործակալությունը իր գործունեությունը իրականացնում է ՀՀ Սահմանադրության, «Անձնական տվյալների պաշտպանության» մասին ՀՀ օրենքի, իր կանոնադրության և այլ իրավական ակտերի հիման վրա[63]: «Անձնական տվյալների պաշտպանության» մասին ՀՀ օրենքով սահմանվում է Անձնական տվյալների պաշտպանության գործակալության՝ որպես լիազոր մարմնի լիազորությունները և գործունեության շրջանակները:

Համաձայն «Անձնական տվյալների պաշտպանության» մասին ՀՀ օրենքի Անձնական տվյալների պաշտպանության գործակալությունը ՝

- ստուգում է իր նախաձեռնությամբ կամ համապատասխան դիմումի հիման վրա անձնական տվյալների մշակման համապատասխանությունը «Անձնական տվյալների պաշտպանության» մասին ՀՀ օրենքի պահանջներին.
- «Անձնական տվյալների պաշտպանության» մասին ՀՀ օրենքի պահանջների խախտման դեպքում կիրառում է օրենքով սահմանված վարչական պատասխանատվության միջոցներ.

[62] «ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալություն ստեղծելու, ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալությունը լիազոր մարմին ճանաչելու, ՀՀ կառավարության 2002 թվականի նոյեմբերի 28-ի n 1917-ն որոշման մեջ լրացումներ կատարելու և ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության կանոնադրությունը և կառուցվածքը հաստատելու մասին» ՀՀ կառավարության 2015թ.-ի հուլիսի 2-ի 734-Ն որոշում, հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docid=98941

[63] http://www.moj.am/structures/view/structure/32

- պահանջում է արգելափակել, կասեցնել կամ դադարեցնել «Անձնական տվյալների պաշտպանության» մասին ՀՀ օրենքի պահանջները խախտող անձնական տվյալների մշակումը.
- օրենքով նախատեսված հիմքերի առկայության դեպքում մշակողից պահանջում է անձնական տվյալների ուղղում, փոփոխում, ուղեփակում կամ ոչնչացում.
- անձնական տվյալներ մշակելու վերաբերյալ մշակողի ծանուցման ուսումնասիրության արդյունքում ամբողջությամբ կամ մասամբ արգելում է անձնական տվյալների մշակումը.
- վարում է անձնական տվյալներ մշակողների ռեեստր.
- իրավաբանական անձանց անձնական տվյալներ մշակող էլեկտրոնային համակարգերը ճանաչում է բավարար պաշտպանության մակարդակ ունեցող և դրանք ներառում է ռեեստրում.
- ստուգում է տվյալներ մշակելու համար օգտագործվող սարքերը և փաստաթղթերը, այդ թվում՝ առկա տվյալները և համակարգչային ծրագրերը.
- օրենքով նախատեսված դեպքերում դիմում է դատարան.
- իրականացնում է օրենքով սահմանված այլ լիազորություններ.
- պահպանում է իր գործունեության ընթացքում իրեն վստահված կամ հայտնի դարձած անձնական տվյալների գաղտնիությունը.
- ապահովում է տվյալների սուբյեկտի իրավունքների պաշտպանությունը.
- քննում է անձնական տվյալների մշակմանը վերաբերող հարցերով ֆիզիկական անձանց դիմումները և իր լիազորությունների սահմաններում ընդունում որոշումներ.
- տարեկան մեկ անգամ ներկայացնում է հրապարակային հաշվետվություն՝ անձնական տվյալների պաշտպանության բնագավառում առկա իրավիճակի և նախորդ տարվա գործունեության վերաբերյալ.

- 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.
- իրավապահ մարմիններին հաղորդում է ներկայացնում իր գործունեության ընթացքում քրեաիրավական բնույթի խախտումների վերաբերյալ կասկածներ ի հայտ գալու դեպքում:

ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալության որոշումները կարող են բողոքարկվել դատական կարգով: Նրա գործունեությունը ֆինանսավորվում է պետական բյուջեի միջոցների հաշվին՝ առանձին տողով:

ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալությանը կից կարող է հասարակական հիմունքներով գործել խորհրդատվական մարմին, որի ձևավորման ու գործունեության կարգը սահմանվում է անձնական տվյալների պաշտպանության լիազոր մարմնի ղեկավարի հրամանով:

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ

Հետազոտելով անձնական տվյալների պաշտպանության իրավունքը Սահմանադրական երաշխիքների համատեքստում, օգտագործելով Անձնական տվյալների պաշտպանության, սահմանադրական իրավունքի վելուծության և իրավական համակարգի արդիականացման գիտամեթոդական մոտեցումները՝ կազմվել է մագիստրոսական թեզի կառուցվածքը, որը հնարավորություն է տալիս վեր հանել անձնական տվյալների պաշտպանության իրավական համակարգի առանձնահատկությունները Հայաստանի Հանրապետությունում: Մագիստրական թեզի եզրակացություններն ու առաջարկությունները բխում են այդ առանձնահատկություններից: Այսպիսով ամփոփելով մագիստրական թեզի հետազոտություններն ու վերլուծությունները՝ հանգել ենք հետևյալ եզրակացություններն ու համապատասխան առաջարկությունները.

1. Անձնական տվյալների պաշտպանությունն առնչվում է կյանքի բոլոր ոլորտներին՝ կրթությունից, առողջապահությունից մինչև մարդու մուտքն ու ելքը սահմանային անցակետերով: Չկա մի ոլորտ, որտեղ անձնական տվյալների պաշտպանության խնդիրը չծագի՝ պետական, թե մասնավոր: Այս և նմանատիպ այլ խնդիրների լուծման համար պետական քաղաքականության գործունեությունն ուղղված է ինչպես այս իրավունքի մասին հանրային իրազեկմանը, այնպես էլ օրենսդրական կարգավորմանը: Անձնական տվյալների պաշտպանության իրավունքի իրացման համար Հայաստանի Հանրապեությունում իրականացվել և շարունակվում են իրականցվել բազում գործնական քայլեր: Մասնավորապես, այս ոլորտի կարգավորման համար 2015 թվականին ստեղծվեծ Անձնական տվյալների պաշտպանության գործակալությունը՝ որպես ՀՀ Արդարադատության նախարարության աշխատակազմի առանձնացված ստորաբաժանում, որի հիմնական նպատակներն ու խնդիրներն են՝ անձնական տվյալների պաշտպանության հետ կապված հարաբերությունների սուբյեկտների իրավունքների պաշտպանության

ապահովումը, իր իրավասության սահմաններում անձնական տվյալների մշակման օրինականության ապահովումը:

2. ՀՀ-ումանձնական տվյալների պաշտպանության իրավական համակարգը դեռ ձևավորման և զարգացման սաղմնային փուլում է: Հայաստանի Արդարադատության նախարարությունում վերջերս ստեղծված Անձնական տվյալների պաշտպանության գործակալության փոքրաթիվ աշխատակազմի գործունեության այս սկզբնական փուլը կարևոր է այն առումով, որ ցանկացած որոշում, օրենսդրական փոփոխության առաջարկ՝ դառնալու է նախադեպ և որոշիչ է լինելու տվյալների շտեմարանների մատչելիության առումով:
3. Հասարակության զարգացման ներկա՝ հետարդիական, փուլում անձնական տվյալների պաշտպանությունը էլ ավելի լուրջ հիմնախնդիր է, որովհետև հասրակության կեսագործունեության բոլոր ոլորտներ է ներթափանցել համացանցը, որտեղ գրեթե անվերահսկելի իրավիճակ է տիրում: Շատ կարևոր է, որ պետական կառավարման ինստիտուտները և առհասարակ պետությունը հոգ տանի անձնական տվյալների գաղտնիությունը ապահովելու, անձնական կյանքի անձեռնմխելիության իրավունքը պաշտպանելու վերաբերյալ:
4. Անձնական տվյալների պաշտպանության իրավունքի իրացման համատեքստում ՀՀ-ում որպես կարգավորման ենթակա առաջնահերթ ոլորտներ ընտրվել են տեսահսկումը, որը թե՛ պետական, թե՛ մասնավոր ընկերությունների կողմից իրականացվում է օրենքի համատարած խախտումներով, անցանկալի առևտրային հաղորդագրությունները, որոնք բջջային հեռախոս ունեցողները ստանում են՝ առանց նախնական համաձայնության, և անչափահասների անձնական տվյալների պաշտպանությունը:
5. Համապատասխան պատժամիջոցները և անձնական տվյալների պաշտպանության միջոցները անձնական տվյալների պաշտպանության օրենսդրության իրացման հիմնական մեխանիզմն են: Եվրոպայի

խորհրդի կոնվենցիան չի որոշակիացնում այն պատժամիջոցները, որոնք պետք է ներդրվեն կոնվենցիան ստորագրած երկրների կողմից, հիմնվելով անդամ-պետությունների օրենսդրական ավանդույթների և հանրային շահերի բավարարման պահանջների վրա: Եվրոպական երկրներում ընդհանուր մոտեցումը հետևյալն է.

6. Ամփոփելով կարող ենք նշել, որ տեսահսկման իրականացման գործընթացը Հայատասանի Հանրապետությունում ունի իրավական կարգավորում, սակայն շատ են տեսահսկման միջոցով անձնական տվյալների պաշտպանության իրավունքի ոտնահրաման դեպքերը: Քաղաքացինրը երբեմն չեն տիրապետում իրենց իրավունքներին և պահանջատեր չեն, ուստի իրավունքների ոտնահարման դեպքերն էլ չեն հասնում համապատասխան մարմիններին: Հայաստանի Հանրապետությունը՝ հանձինս ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության, հետևողական է այս հարցում և գործուն քայլեր է ձեռնարկում այս ոլորտում հասրակության իրավագիտակցության մակարդակի բարձրացման և հնարավոր ոտնձգությունների դեպքերի բացահայտման և կանխարգելիչ միջոցառումների իրականացման ուղղությամբ:
7. Հաշվի առնելով այն, որ անձնական տվյալների պաշտպանության ինստիտուտը ներկայիս կարգավորմամբ նորություն է ՀՀ իրավական համակարգի համար, որը նոր իրավական մշակույթ է ՀՀ իրավական կյանքում և ուղղված է սահմանադրորեն և միջազգային փաստաթղթերով արժևորված արժեքի՝ անձի մասնավոր կյանքի անձեռանմխելիության իրավունքի պաշտպանությանը, ուստի անհրաժեշտ է, որ անձնական տվյալներ մշակող ցանկացած սուբյեկտ մանրամասն և ամբողջությամբ տեղեկացված լինի հիշյալ իրավադրույթներին՝ դրանց խախտման համար սահմանված պատասխանատվության միջոցներից խուսափելու

և որ ամենակարևորն է՝ նպաստելու այս նոր իրավական մշակույթի ձևավորմանն ու կայացմանը ՀՀ-ում:

8. անձնական տվյալների պաշտպանության մարմնի գործունեության անկախությունը և թափանցիկությունը ապահովելու համար կարելի է ընտրել փորձագիտական խորհուրդ հիմնելու մոդելը: Երկար՝ օրինակ տսասը տարուց ոչ պակաս՝ փորձ ունեցող և մարդու/քաղաքացիական հասարակության իրավունքների պաշտպանության գծով հասարակական կազմակերպություններից կազմված փորձագետների խորհուրդը այն արդյունավետ գործիքը կարող է դառնալ, որը կապահովի տվյալ մարմնի հանրային վստահությունը և խորհրդի մասնագիտական փորձը: Այնուամենայնիվ, օրենքը պետք է նախատեսի մեխանիզմներ, երաշխավորելով մարդու/քաղաքացիական իրավունքների պաշտպանության ոլորտում հանրության և հասարակական կազմակերպությունների կողմից հարգված և իրական փորձ ունեցող անձի նշանակումը:
9. Տվյալների պաշտպանության մարմնի ֆինանսական անկախությունը նպատակահարմար է սահմանել օրենքով, դրանով իսկ բացառելով հնարավոր ճնշումները և կառավարության ազդեցությունը: Նման երաշխիք կարող է լինել որոշակի դրույթ, որը կնախատեսի տվյալ մարմնի բյուջեն մեկ աշխատակցի հաշվով, սահմանելով այն ոչ պակաս, քան մարդու իրավունքների պաշտպանի գրասենյակի մեկ աշխատակցի համար նախատեսված բյուջետային գումարը:

ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

Օրենքներ և այլ իրավական ակտեր

1. ՀՀ Սահմանադրություն, փոփոխություններով, 06.12.2015թ. Հասանելի է http://www.arlis.am/DocumentView.aspx?docID=102510
2. «**Անձնական տվյալների պաշտպանության մասին**» ՀՀ օրենք, ուժի մեջ է մտել 01.07.2015թ.: Հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docID=98338
3. «Անձնական տվյալների պաշտպանության մասին» Վրաստանի օրենք, https://personaldata.ge/manage/res/docs/unofficial%20translations/ENG%20Statute%20Unofficial%20Translation.pdf
4. «Վարչական իրավախախտումների վերաբերյալ» օրենսգիրք, http://www.arlis.am/DocumentView.aspx?docid=73129
5. «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիա (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), 1981 թվական, Եվրոպայի խորհուրդ (ընդունվել է 1981 թվականի հունվարի 28-ին) [ETS No. 108, Strasbourg, 28.1.1981], հասանելի է հետևյալ կայքէջում՝ http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
6. «Հայաստանի Հանրապետության 2017 թվականի պետական բյուջեի մասին» ՀՀ օրենք, Ընդունված՝ 2016 թվականի դեկտեմբերի 8-ին, Հասանելի է՝ http://www.gov.am/files/docs/2014.pdf
7. «ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալություն ստեղծելու, ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալությունը լիազոր մարմին ճանաչելու, ՀՀ կառավարության 2002 թվականի նոյեմբերի 28-ի n 1917-ն որոշման մեջ լրացումներ կատարելու և ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության կանոնադրությունը և կառուցվածքը հաստատելու մասին» ՀՀ

կառավարության 2015թ.-ի հուլիսի 2-ի 734-Ն որոշում, հասանելի է՝ http://www.arlis.am/DocumentView.aspx?docid=98941

8. «Վարչական իրավախախտումների վերաբերյալ ՀՀ օրենսգրքում կատարված փոփոխություններն ու լրացումները», ուժի մեջ է մտել 11.01.2016թ.: Հասանելի է http://www.arlis.am/DocumentView.aspx?docid=102854
9. «Տեսանկարահանող կամ լուսանկարահանող սարքերով հայտնաբերված ճանապարհային երթևեկության կանոնների խախտումների վերաբերյալ գործերով իրականացվող վարչական վարույթի առանձնահատկությունների մասին» ՀՀ օրենք, ուժի մեջ է մտել 01.01.2009թ. Հասանելի ՝ http://www.arlis.am/DocumentView.aspx?docid=48761content/uploads/2015/04/ DataProPolicyGuide_arm_final.pdf
10. Անձնական տվյալների մշակման և այդ տվյալների ազատ տեղաշարժի առնչությամբ անհատների պաշտպանության մասին հրահանգ 95/48/ԵՀ (Directive 95/48/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data) (ընդունվել է Եվրոպական պառլամենտի և Խորհրդի կողմից 1995 թվականի հոկտեմբերի 24-ին) [Official Journal L 281, 23-11-1995, P. 0031 – 0050], հասանելի է հետևյալ կայքէջում՝ http://ec.europa.eu/justice/policies/privacy/docs/95-48-ce/ dir1995-48_part1_en.pdf
11. Անձնական տվյալների պաշտպանության բավարար մակարդակ ունեցող երկրների ցանկը» հաստատելու մասին ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալության որոշում, 17.01.2017թ., Հասանելի է http://moj.am/storage/uploads/002_Cucak-final.pdf
12. Անձնական տվյալների պաշտպանության գործակալության կանոնադրությունը տես ՀՀ արդարադատության նախարարության կայքէջում՝ http://www.justice.am/structures/view/structure/32

13. «Անձնական տվյալների պաշտպանության մասին» Վրաստանի օրենք, https://personaldata.ge/manage/res/docs/unofficial%20translations/ENG%20Statute%20Unofficial%20Translation.pdf
14. Հանրային հաշվետվություն, ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալություն, 2016թ. Հասանելի է՝ http://moj.am/storage/files/legal_acts/legal_acts_8577044455541_Annual-report-2017_ARM.pdf
15. ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության 2015 հոկտեմբերից 2016 հունվար ընկած ժամանակահատվածի հանրային հաշվետվություն http://moj.am/storage/files/legal_acts/legal_acts_5389572924341_Annual-report-PDPA.pdf

Գրականություն

16. Անձնական տվյալների պաշտպանության քաղաքականության ուղեցույց, http://www.osf.am/wp-content/uploads/2015/04/DataProPolicyGuide_arm_final.pdf
17. Երեխաների անձնական տվյալների պաշտպանության մասին ուղեցույց, ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալություն, 2017թ., Հասանելի է՝ http://iravaban.net/wp-content/uploads/2017/02/001.Ughecuyc-erexaneri_andznakan_tvyalner.pdf
18. Տեսահսկման ուղեցույց, ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալություն, 2016թ. Հասնելի է՝ http://www.foi.am/u_files/file/Manual_Video.pdf
19. Տեսահսկման ուղեցույց, ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության

գործակալություն, Երևան 2016թ. http://www.foi.am/u_files/file/Manual_Video.pdf

20. Bygrave L.A. Privacy and Data Protection in an International Perspective. In: Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010. p.165-200 Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf (date of visit: 19.02.2013);
21. Gellman, R. (2014) Fair Information Practices: A Basic Histor». Доступно через: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf.
22. **Авдеев, М.Ю.** (2013) Законодательство Российской Федерации о неприкосновенности частной жизни: к вопросу о заимствовании зарубежного опыта. Доступно через: http://cyberleninka.ru/article/n/zakonodatelstvo-rossiyskoy-federatsii-o-neprikosnovennosti-chastnoy-zhizni-k-voprosu-o-zaimstvovanii-zarubezhnogo-opyta
23. **Вайхерт,Г.** (2011) Защита персональных данных в рамках серии дискуссий «Настоящее будущего» Доступно через: https://www.datenschutzzentrum.de/vortraege/20110224-weichert-datenschutz-moskau-ru.pdf.
24. **Назаров, Б.Л.** (1995) Права человека История, теория и практика: Учебное пособие – Москва:.: Русспит
25. **Солоув, Д.** «Мне нечего скрывать» и другие ошибочные толкования приватности. Доступно через: https://www.pgpru.com/biblioteka/statji/nothingtohide.
26. **Хачатурян Ю.А**. Право работника на защиту персональных данных // Современное право. - М.: Новый Индекс, 2006, № 1. - С. 43-51

27. **Шахов Н.** (2008) Отношения по охране частной жизни и информации о частной жизни как объект теоретико-правового исследования. Ростов-на Дону. С. 7
28. **Шишлов А.А.** Правовое регулирование защиты персональных данных в рамках Европейского Союза // Закон и право. - М.: ЮНИТИ-ДАНА, 2010, № 1. - С. 32-33.

Համացանցային կայքեր

29. www.e-gov.am
30. www.parliament.am
31. www.arlis.am
32. www.mjo.am
33. http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf
34. https://personaldata.ge/en/home
35. https://personaldata.ge/en/about-us/budget
36. http://www.moj.am/structures/view/structure/32
37. https://personaldata.ge/en/about-us/inspector