ՀՀ ԱՐԴԱՐԱԴԱՏՈՒԹՅԱՆ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ
ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ
ԳՈՐԾԱԿԱԼՈՒԹՅՈՒՆ

ՏԵՍԱՀՍԿՄԱՆ ՈՒՂԵՑՈՒՅՑ

ԵՐԵՎԱՆ, 2016

ՏԵՍԱՀՍԿՄԱՆ ՈՒՂԵՑՈՒՅՑ

Տեսահսկման ուղեցույցը մշակվել է Հայաստանի Հանրապետության Արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության կողմից: Ուղեցույցի նպատակն է ներկայացնել տեսահսկման հիմնական կանոններն ու սկզբունքները՝ ապահովելով մարդկանց անձնական տվյալների պաշտպանությունը:

Ուղեցույցը մշակվել է՝ առաջնորդվելով <<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքի պահանջներով և տեսահսկման կարգավորման միջազգային չափանիշներով: Տեսահսկում իրականացնող յուրաքանչյուր անձ կամ կազմակերպություն պետք է առաջնորդվի <<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքով և այս ուղեցույցով:

1. Ի՞նչ է տեսահսկումը

Մարդու տեսանկարը անձնական տվյալ է, որը թույլ է տալիս ուղղակի կամ անուղղակի նույնականացնել անձին: Հետևաբար, տեսախցիկի միջոցով իրականացվող տեսանկարահանումը և հսկողությունը (այսուհետ՝ տեսահսկում), 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 ուղիղ, իրական ժամանակի ռեժիմով տվյալների փոխանցմամբ:

Քանի որ տեսահսկմամբ խախտվում է անձի անձնական կյանքի գաղտնիության իրավունքը, այդ իսկ պատճառով տեսահսկողը պետք է տեսահսկման համակարգ տեղադրելուց առաջ գնահատի տեսահսկման իրական կարիքն ու նպատակը, համակարգի ազդեցությունը անձի անձնական տվյալների պաշտպանության իրավունքի վրա, և համոզված լինի, որ մեկ այլ միջոցով հնարավոր չէ հասնել հետապնդվող նպատակին:

1.1 Տեսահսկում հասարակական վայրերում

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:

Փողոցների տեսահսկումն իրականցվում է նաև ճանապարհային երթևեկության անվտանգությունն ապահովելու նպատակով, որի շրջանակներում տեսագրությունները կամ տեսանկարները դրվում են վարորդներին վարչական պատասխանատվության ենթարկելու վարչական վարույթների հիմքում (տես՝ <<Տեսանկարահանող կամ լուսանկարահանող սարքերով հայտնաբերված ճանապարհային երթևեկության կանոնների խախտումների վերաբերյալ գործերով իրականացվող վարչական վարույթի առանձնահատկությունների մասին>> ՀՀ օրենքը):

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:

1.2 Պետական և մասնավոր կազմակերպությունների շենքերի տեսահսկում

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:

1.3 Բնակելի շենքերի, մասնավոր տների և դրանց մերձակայքում իրականացվող տեսահսկում

Բնակելի շենքերում տեսահսկման համակարգը ներդրվում է անվտանգության, անձանց անվտանգությունը և գույքը վնասներից պաշտպանելու համար: Համակարգը տեղադրելուց առաջ բազմաբնակարան շենքի բոլոր բնակիչները պետք է տեղյակ լինեն

տեսահսկման մասին, ինչպես նաև պետք է առկա լինի բազմաբնակարան շենքի սեփականատերերի առնվազն կեսից ավելիի գրավոր համաձայնությունը:

Բնակելի շենքերում պետք է տեսահսկման վերաբերյալ նախազգուշացումն ակնհայտորեն տեսանելի լինի շենք մտնող յուրաքանչյուր անձի համար:

Տեսախցիկները թույլատրվում է տեղադրել միայն մուտքի դռների մոտ և ընդհանուր տարածքներում: Բնակիչների բնակարանները տեսահսկելն արգելվում է: Բնակարանի սեփականատերը կամ վարձակալը կարող է նկարահանել միայն իր բնակարանը և պատշգամբը:

Մասնավոր նպատակով իրականացվող տեսահսկումը հնարավոր է միայն սեփական տարածքում: Առանձնատան սեփականատերն իրավունք ունի տեսահսկել իր առանձնատունը և դրա այգին, բայց չի կարող իր հողամասի սահմաններից դուրս նկարահանել, եթե չունի համապատասխան հարևանի համաձայնությունը:

2. Տեսահսկման համակարգի շահագործման սկզբունքները

Տեսանկարահանման համակարգի շահագործման ընթացքում անհրաժեշտ է պահպանել հետևյալ սկզբունքները.

2.1 ***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:

2.2 ***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:

2.3 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):

2.4 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:

2.4.1 ***Նախազգուշացնող նշաններ***

Տեսահսկողը պարտավոր է տեսանելի վայրում ունենալ նախազգուշացնող նշան, որը տեսանկարահանվող սուբյեկտին կիրազեկի տեսահսկման համակարգի առկայության մասին: Հասարակական, պետական և մասնավոր վայրերում տեսահսկման համակարգեր տեղադրելիս անհրաժեշտ է տեսանելի վայրում ունենալ նախազգուշացնող նշան, որը տեսանկարահանվող սուբյեկտին կիրազեկի տեսանկարահանման մասին: Նախազգուշացնող նշաններ կարող են չտեղադրվել միայն այն տարածքներում, որտեղ տեսանկարահանումը սահմանված է օրենքով կամ առկա է ազգային անվտանգության խնդիր: Տեսաձայնագրման դեպքում անհրաժեշտ է ունենալ նաև նախազգուշացնող նշան տեսաձայնագրման մասին:

Եթե տեսահսկման տարածքն ընդարձակ է, տեսահսկողը կարող է ունենալ մի քանի նախազգուշացնող նշաններ կամ մեկ նշան՝ մուտքի դռան մոտ:

2.4.2 Տեղեկատվության մատչելիություն

<<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքը սահմանում է, որ յուրաքանչյուրն ունի իր անձնական տվյալների մշակման մասին տեղեկություն ստանալու իրավունք: 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, ինչպես նաև այն անձանց շրջանակը, որոնց կարող է փոխանցվել իր տեսագրությունը:

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), ապա տեսահսկման սուբյեկտը 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: Համաձայն <<Տեղեկատվության ազատության մասին>> ՀՀ օրենքի կարգավորումների՝ եթե տեսագրությունը տրամադրվում է էլեկտրոնային փոստով, ապա դա պետք է արվի անվճար, կամ եթե տեսագրության նյութերը պատճենվում են թղթային տարբերակով տրամադրելու համար, ապա մինչև 10 էջ տեղեկությունը պետք է տրամադրվի անվճար, իսկ 11-րդ էջից սկսած տեղեկությունը պետք է տրամադրվի այնպիսի վճարով, որը չի գերազանցում տեղեկության տրամադրման իրական ծախսերը: 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:

Օրենքը սահմանել է, որ տեղեկությունները պետք է տրամադրվեն գրավոր հարցումը ստանալուց հետո՝ հինգ օրվա ընթացքում (օրենքի 20-րդ հոդված, 1-ին մաս):

Կարևոր է, որ տեսահսկում իրականացնողը սահմանի տեսահսկման և տեղեկությունների տրամադրման ներքին ընթացակարգեր, որվհետև այդպիսով տեսահսկվողի համար պարզ են դառնում տեսահսկման կանոնները, այն պայմանները, թե ինչպես, պատասխանատու որ անձի միջոցով տեսահսկվողը կարող է ստանալ իրեն հետաքրքրող հարցերի պատասխանը, ում և ինչպես պետք է դիմի իր տեսագրության մասին տեղեկություններ կամ տեսագրության կրկնօրինակը ստանալու համար, ինչպես կարող է ծանոթանալ իր տեսագրությունը մշակելու պայմաններին, ում և ինչպես պետք է դիմի իր տեսահսկվողի մոտ պահվող տեսագրության անվտանգության ապահովման հարցերով և այլն: Ընթացակարգեր ունենալը խրախուսելի է, որը պետք է համապատասխանի <<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքին:

Տեսահսկողը պետք է ունենա նաև բողոքարկման ընթացակարգեր, ներքին վերանայման մեխանիզմներ, բողոքարկմանը լուծում տալու ժամկետներ և այլն

2.5 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:

Տեղեկատվական համակարգերում անձնական տվյալները մշակելու անվտանգությունն ապահովելուն ներկայացվող պահանջները, կենսաչափական անձնական տվյալների նյութական կրիչներին և տեղեկատվական համակարգերից դուրս այդ անձնական տվյալները պահպանելու տեխնոլոգիաներին ներկայացվող պահանջները սահմանվում են Հայաստանի Հանրապետության կառավարության 2015 թվականի հոկտեմբերի 15-ի N 1175-Ն որոշմամբ:

Մշակողները կարող են կիրառել նաև <<Տեղեկատվության անվտանգության կառավարման>> ՀՍՏ ԻՍՈ/ԻԷԿ 27000 շարքի միջազգային չափանիշներն այնքանով, որքանով դրանք իրենց էությամբ կիրառելի են կենսաչափական անձնական տվյալների նյութական կրիչների և տեղեկատվական համակարգերից դուրս այդ անձնական տվյալների պահպանման տեխնոլոգիաների նկատմամբ:

Երբ տեսահսկողը վարձում է տեխնիկական անվտանգությամբ զբաղվող կազմակերպություն տեսահսկման համակարգ ներդնելու կամ տվյալներ մշակելու նպատակով, այդ կազմակերպությունը դառնում է համակարգող և պատասխանատու անձնական տվյալների պաշտպանության համար: Տեսահսկողը պայմանագիր է կնքում մշակող կողմի հետ և պայմագրի ժամկետի ավարտին պես սահմանափակում է տվյալների հասանելիությունը երրորդ կողմին:

Ցանկացած տեսահսկման համակարգի նյութական կրիչ (օրինակ տեսախցիկ) պետք է ունենա եզակի նույնականացման համար և հաշվառված լինի մշակողի կողմից (ՀՀ կառավարության N 1175-Ն որոշում):

2.6 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:

3. Տեսահսկման չափանիշները

Տեսահսկման համակարգերը պետք է համապատասխանեն հետապնդվող նպատակին և բխեն համաչափության սկզբունքից: Այս առումով տեսահսկողը պետք է հաշվի առնի հետևյալը՝

Տեսախցիկների քանակը, դրանց գտնվելու վայրը և կետայնությունը (resolution) պետք է համապատասխանեն տեսահսկման նպատակին, կազմակերպության գործունեության առանձնահատկություններին, տարածքի ընդհանուր մակերեսին, սենյակի կառուցվածքին և այլն: Տեսահսկման համակարգը պետք է տեղադրվի այնպես, որ հնարավորինս քիչ տարածք վերահսկելով հնարավոր լինի հասնել հետապնդվող նպատակին: Եթե նպատակին կարելի է հասնել ավելի ցածր կետայնությամբ տեսախցիկների օգնությամբ, ապա պետք է օգտագործել դրանք՝ խուսափելով ավելորդ անձնական տվյալներ մշակելուց:

Տեսանկարներից պետք է պարզ լինի տեսահսկման ժամը, ամսաթիվը, և վայրը:

Ուղիղ, իրական ժամանակում/ռեժիմում տվյալների փոխանցմամբ աշխատող տեսահսկումը կարող են իրականացնել միայն հատուկ թույլատվություն ունեցող անձինք (օրինակ, անվտագության աշխատակիցները): Այս ռեժիմում աշխատող տեսահսկման համակարգի էկրանները պետք է այնպես շրջված լինեն, որ միայն թույլատրված/լիազորված անձը կարողանա տեսնել տեսապատկերները: Հանրային էկրաններն արգելվում են: Օրինակ, խանութի տվյալ բաժնում գտնվող անձը էկրանին պետք է տեսնի միայն այդ բաժնի տեսանկարները:

4. Պատասխանատվություն

<<Անձնական տվյալների պաշտպանության 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: