

ԼՈՒՍԻՆԵ ՄԻՆԱՍՅԱՆ

Վարչապետի աշխատակազմի տեսչական
մարմինների աշխատանքների համակարգման
գրասենյակի շուկայի վերահսկողության և
սննդամթերքի անվտանգության ոլորտների
համակարգման և մեթոդաբանության
վարչության խորհրդական

ԱՆՁԻ ՊԱՏԿԵՐԸ ՈՐՊԵՍ ԿԵՆՍԱՀԱՎԱԿԱՆ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ԱՌԱՆՁՆԱՀԱՏՈՒԿ ՏԵՍԱԿ

Հոդվածը նվիրված է անձի պատկերի՝ որպես կենսաչափական առանձնահատուկ անձնական տվյալի ուսումնասիրությանը:

Հետազոտության ընթացքում համապարփակ վերլուծության են ենթարկվել կենսաչափական անձնական տվյալների կարևորությունը և առանձնահատկությունները՝ անձնական տվյալների պաշտպանության ամբողջական համակարգում:

Այնուհետև, առանձին անդրադարձ է կատարվել անձի պատկերի անձնական տվյալին՝ որպես անձի ինքնության անբաժանելի մաս և վեր են հանվել օրենսդրական այն կարգավորումները, որով անձի պատկերը պաշտպանության է արժանանում:

Համապարփակ վերլուծության է ենթարկվել անձի պատկերի դերը, մարդու արժանապատիվ ապրելու իրավունքի լիարժեք իրականացման համար, և առաջադրվել վերջինիս պաշտպանության հատուկ կարգավիճակի կարևորությունը:

Հիմնարարներ- անձնական տվյալներ, անձնական տվյալների պաշտպանության իրավունք, կենսաչափական անձնական տվյալներ, անձի պատկեր, հիմնարար իրավունքներ:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքում հատուկ ուշադրություն է հատկացվում կենսաչափական անձնական տվյալներին¹, այսինքն՝ անձի ֆիզիկական, ֆիզիոլոգիական և կենսաբանական առանձնահատկությունները բնութագրող տեղեկություններին, որոնց հիման վրա կարելի է անձին նույնականացնել (քաշը, հասակը, մազերի գույնը, արյան խումբը, ձայնը, մատնահետքերը, ԳՆԹ անալիզի արդյունքները, դեմքի թվային պատկերը, աչքի ցանցաթաղանթը և այլն): Կենսաչափական նույնականացումը կարող է ուրվագծել անձի բոլորովին մանրակրկիտ պատկերը՝ օգտագործելով կենսաբանական պարամետրերի յուրահատկությունը, քանի որ բնության մեջ չկա միևնույն կենսաչափական նշաններով երկու մարդ: Այս փաստը կենսաչափական տեխնոլոգիաներին տալիս է հսկայական առավելություն նախկինում մշակված և այսօր լայնորեն օգտագործվող հսկողական համակարգերի նկատմամբ, որոնք են՝ PIN-կոդերը, պլաստիկ քարտերը, կրիպտոգրաֆիկական կոդերը և այլն (վերջիններս կարող են վնասվել, կորել, կրկնապատկվել կամ երրորդ անձանց կողմից անօրինական օգտագործվել): Հարկ է նշել նաև, որ տարբեր իրերի տեխնիկական բնութագրեր որոշակի պայմաններում ևս կարող են հանդես գալ, որպես անձնական տվյալ կամ դրա աղբյուր: Օրի-

նակ՝ համակարգչի IP- հասցեն², որն արդեն հանդիսանում է ոչ թե համակարգչի տեխնիկական բնութագիր, այլ՝ տեղեկատվություն, որը կարող է նույնականացնել համակարգչի տիրոջը:

Նշված հանգամանքներով է պայմանավորված պետության և մասնավոր շուկայի պարբերաբար աճող հետաքրքրությունը կենսաչափական տեխնոլոգիաների նկատմամբ, որոնք կարող են օգտագործվել սահմանային անձնագրային հսկողության, զանազան տրանսպորտային միջոցների ուղևորների գրանցման, արտաքին տեսաձայնագրման, առանձին հաստատություններ մուտքի վերահսկման (լաբորատորիաներ, թանկարժեք իրերի բանկային պահակատեղեր, պետական գաղտնիք պարունակող հիմնարկներ և այլն), հետաքննչական գործողությունների և այլնի իրականացնելու համար:

Կենսաչափական տվյալների ցանկը բացակայում է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքում, ինչպես նաև բացակայում են դրանց առանձին տեսակների, օրինակ՝ գենոմային³ տեղեկատվության մասին իրավական կարգավորումները, ինչպես դա արվում է այլ երկրներում⁴:

Կենսաչափական տվյալները օպերատիվ-հե-

տախուզական գործունեության ոլորտում մեծ դերակատարում ունեն: Այսպես, որոշ դեպքերում անձի կենսաչափական տվյալները կարող են օպերատիվ-հետախուզական միջոցառումների իրականացման հիմք հանդիսանալ, մասնավորապես՝ անձի նույնացման և օպերատիվ փորձարարության համար⁵: Բացի այդ կենսաչափական տվյալները կարող են անուղղակիորեն պատճառ կամ հիմք հանդիսանալ քրեական գործ բացելու համար, քանի որ հաճախ օգտագործվում են քննչական և դատավարական գործողությունների մեջ, սակայն ՀՀ քրեական դատավարության օրենսգրքում կենսաչափական տվյալները, որպես ապացույցի առանձին տեսակ, բացակայում են⁶:

Կենսաչափական տվյալների առանձնահատկությունը կայանում է նրանում, որ դրանցից շատերը կարող են դասակարգվել որպես «զգայուն» տվյալներ, օրինակ՝ մաշկի գույնը կարող է անձի ռասայական կամ էթնիկ պատկանելիության մասին խոսել: Սակայն օրենքը չի անդրադարձել, թե այս դեպքում անձնական տվյալներ մշակողը անձնական տվյալների տեսակներից ո՞ր մեկին պետք է տալ առաջնայնությունը: Կենսաչափական տվյալների մշակումը հնարավոր է միայն տվյալների սուբյեկտի համաձայնությամբ, բացառությամբ՝ օրենքով նախատեսված դեպքերի, և եթե միայն օրենքով հետապնդվող նպատակը հնարավոր է իրականացնել այդ կենսաչափական տվյալները մշակելու միջոցով⁷: Իսկ «հատուկ» կամ «զգայուն» կատեգորիայի անձնական տվյալների մշակումը թույլատրվում է միայն անձի համաձայնությամբ բացառությամբ, երբ տվյալի մշակումն ուղղակիորեն նախատեսված է օրենքով, ընդ որում՝ այն անհապաղ դադարեցվում է, եթե վերացել են տվյալները մշակելու հիմքերը և նպատակը⁸: Այսինքն, երկու դեպքում էլ, անհրաժեշտ է տվյալների սուբյեկտի համաձայնությունը կամ անձնական տվյալները մշակելու անհրաժեշտությունը սահմանող օրենքը, սակայն կենսաչափական տվյալների մշակման համար օրենքով հետապնդվող նպատակը հնարավոր է իրականացնել միայն այդ կենսաչափական տվյալները մշակելու միջոցով, ինչը պետք է ապացուցված լինի համապատասխան փաստական հանգամանքներով:

Մինչդեռ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը կենսաչափական տվյալների մշակման գործընթացի համար սահմանում է նույն սկզբունքները, ինչ «սովորական» անձնական տվյալների համար է՝ բացառությամբ մի քանի հատուկ սահմանված պահանջների⁹: Սա նշանակում է, որ և՛ կենսաչափական տվյալների, և՛

անձնական տվյալների այլ տեսակների անօրինական միջոցներով ձեռք բերման և օգտագործման համար օրենքը միանման սանկցիաներ է նախատեսում:

Շատ երկրներում կենսաչափական տվյալներ հավաքագրող տեխնոլոգիաների զարգացումը որպես առանձին ճյուղ ունի պետական հովանավորչություն: ԱՄՆ-ում օրինակ՝ Անվտանգության քաղաքականության խորհրդի որոշմամբ դեռևս 1995թ.-ին ստեղծվեց կառավարական ինստիտուտ՝ Կենսաչափության ասոցիացիա (Biometric Consortium (BC¹⁰)), որի անդամներն են հանդիսանում պետական, առևտրային և գիտական կազմակերպությունները: Իսկ ահա՝ Եվրոպական աշխարհամասի համար միասնական Եվրասիական տնտեսական միություն ստեղծելու անհրաժեշտությունը և ԵՄ-ի հետ վիզային ռեժիմի մատչելիության ապահովման ձգտումը, կենսաչափական անձնագրերի, նույնականացման քարտերի և սահմանը հատելիս, միասնական կենսաչափական վերահսկողության համակարգի ներդրման հիմք հանդիսացան¹¹: Միջազգային ասպարեզում ամենից զարգացած ընկերություններից են հանդիսանում՝ Միջազգային կենսաչափական ինքնության ասոցիացիան (International Biometric Identity Association (IBIA¹²)) և Կենսաչափության եվրոպական ասոցիացիան (European Association for Biometrics(EAB¹³)): ՀՀ-ում կենսաչափական տեխնոլոգիաների շուկան նոր է ձևավորվում:

Կենսաչափական տվյալների համակարգում առանձնահատուկ տեղ է զբաղեցնում քաղաքացու պատկերը՝ որպես առանձնահատուկ անձնական տվյալ դիտարկելու խնդիրը: Եթե անձնական տվյալների սահմանման նպատակը նույնականացումն է, ապա դրա առաջին նույնացուցիչներից է հանդիսանում անձի պատկերը, քանի որ մարդու պատկերից կարելի է ստանալ տեղեկատվություն անձի կենսաչափական անձնական տվյալների, անձի ֆիզիկական, ֆիզիոլոգիական և կենսաբանական առանձնահատկությունների, ազգային, կրոնական պատկանելիության և այլնի մասին: Պատահական չէ, որ ՀՀ քաղաքացուն նույնականացման քարտ տրամադրելու համար նույնականացման քարտում հայերենով և անգլերենով ամրագրվում են քաղաքացու հետևյալ անձնական տվյալները.

- 1) ազգանունը, անունը, ինչպես նաև հայրանունը՝ միայն հայերեն տարբերակում,
- 2) ծննդյան վայրը, օրը, ամիսը, տարեթիվը,
- 3) սեռը,
- 4) քաղաքացիությունը,

ԱՐԴԱՐԱԴԱՏՈՒԹՅՈՒՆ

5) ազգությունը՝ քաղաքացու կամ սույն օրենքով նախատեսված դեպքերում՝ ներկայացուցչի ցանկությամբ,

6) բնակության վայրը (նշվում է միայն երկիրը),

7) հանրային ծառայությունների համարանիշը,

8) քաղաքացու լուսանկարը,

9) քաղաքացու ստորագրությունը,

10) ինչպես նաև արյան խումբը և ռեզուսը (քաղաքացու կամ սույն օրենքով նախատեսված դեպքերում՝ ներկայացուցչի ցանկությամբ)¹⁴ :

Նույն օրենքը առանձին սահմանում է, որ նույնականացման քարտ ստանալու (փոխանակելու) համար քաղաքացին լուսանկարվում է ոստիկանության մարմնում¹⁵ : Իսկ «Նոտարիատի մասին» ՀՀ օրենքով նոտարը հաստատում է քաղաքացու նույնությունը լուսանկարում պատկերված անձի հետ¹⁶ : Այսպիսով՝ անձի նույնականացման համար լուսանկարի նշանակությունը ակնհայտ է :

Անձի պատկերի կարևորությունը երևում է նաև ձեռքակալված և կալանավորված անձանց նկատմամբ հսկողության իրականացման ժամանակ, ում, անհրաժեշտության դեպքում, նույնականացնելու համար օգտագործվում են տեխնիկական և էլեկտրոնային միջոցներ, այդ թվում՝ մատնադրոշմում, անձնական խուզարկություն և լուսանկարում¹⁷ :

Ընդ որում՝ անձի պատկերի չսանկցավորված մշակումը, տիրապետումը, օգտագործումն ու տնօրինումը մարդու անձնական և ընտանեկան կյանքի անձեռնմխելիության իրավունքի ակնհայտ խախտում է հանդիսանում: Սակայն պետք է փաստել, որ լուսանկարի՝ որպես իրավական պաշտպանության օբյեկտի, իրավական կարգավիճակը մինչ այժմ ՀՀ օրենսդրությամբ չի կարգավորվում ո՛չ քրեական, ո՛չ քաղաքացիաիրավական, ո՛չ վարչական իրավունքի շրջանակներում, ի տարբերություն ռուսական փորձի¹⁸, երբ դեռևս 2006 թվականին ռուս օրենսդիրը Ռուսաստանի Դաշնության քաղաքացիական օրենսգրքի 8-րդ գլխում՝ ոչ նյութական բարիքների ցանկում, կատարեց փոփոխություն և անձի պատվի, արժանապատվության և բարի համբավի պաշտպանության հետ մեկտեղ նախատեսեց ևս երկու դրույթ, անձի անձնական կյանքի և քաղաքացու պատկերի (այդ թվում՝ անձի լուսանկար, տեսաձայնագրություններ կամ անձին պատկերող արվեստի ստեղծագործություններ) պաշտպանության մասին:

Նման իրավական կարգավորման թերությունը այն է, որ անձի պատկերն ինքնին այդ դեպքում ոչ նյութական բարիք չի համարվում: Դա պայմանա-

վորված է այն հանգամանքով, որ պատկերը ենթադրում է անձի վիզուալ կերպարի ամրագրումը որևէ նյութական կրիչի վրա, հետևաբար օրենսդիրը պաշտպանում է նման կրիչի վրա գտնվող պատկերը, երբ այն օգտագործվում կամ հրապարակվում է երրորդ անձանց կողմից՝ առանց վերջինիս թույլտվության: Իսկ մնացած դեպքերում անձի պատկերը ինքնին, պաշտպանության ենթակա չէ:

Նմանապես անձի պատկերը ՀՀ քաղաքացիական օրենսգրքում պաշտպանություն չի ստանում: Այն պաշտպանություն կարող է ստանալ միայն երկու դեպքում՝

1. Երբ անձի պատկերը հանդիսանում է հեղինակային իրավունքի օբյեկտ¹⁹ :

2. Երբ անձի պատկերը օգտագործվել է՝ պատիվը, արժանապատվությունը կամ գործարար համբավը արատավորելու նպատակով²⁰ :

Նման կարգավորումները պարադոքսային իրավիճակներ են ստեղծում: Մասնավորապես, առաջին դեպքում՝ անձը իր սեփական պատկերը հեղինակային իրավունքի օբյեկտ ճանաչելու համար յուրաքանչյուր դեպքում լուսանկարվելիս, նախ այն պետք է համարի արվեստի գործ, այնուհետև՝ ամեն անգամ իր անունը նշի ստեղծագործության վրա կամ իր անունը գրանցի գույքային իրավունքները կոլեկտիվ հիմունքներով կառավարող համապատասխան կազմակերպությունում կամ նոտարի մոտ, կամ օրենքով համապատասխան լիազորություն ունեցող այլ կազմակերպություններում՝ լուսանկարի օրինակը ի պահ հանձնելով²¹ :

Երկրորդ դեպքում՝ անձի պատկերը պաշտպանության է ենթարկվում միայն, եթե դարձել է վիրավորանքի կամ զրպարտության օբյեկտ: Ցանկացած այլ դեպքում՝ առանց անձի թույլտվության իր պատկերի օգտագործումը դուրս է մնում քաղաքացիական օրենսդրության պաշտպանության շրջանակից:

Այսպիսով, թեև ՀՀ քաղաքացիական օրենսգրքում անձի պատկերի պաշտպանությունը առանձին հոդվածով ամրագրված չէ, սակայն անձի պատկերն անձնական տվյալ դիտարկելու դեպքում, այն պաշտպանության ավելի լայն շրջանակ է ունենում բոլոր հանգամանքներում(ոչ միայն օգտագործման և հրապարակման դեպքում), քանի որ անձնական տվյալներ մշակողը պարտավոր է հետևել և ապահովել, որ տվյալները մշակվեն օրենքի պահանջների պահպանմամբ²², օրինական և որոշակի նպատակներով և առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով²³ : Ավելին, տվյալների սուբյեկտը կարող է մշակողի գործողությունները

կամ անգործությունը, կամ որոշումները բողոքարկել անձնական տվյալների պաշտպանության լիազոր մարմին, կամ դատական կարգով, եթե համարում է, որ խախտվել է իր անձնական տվյալների պաշտպանության իրավունքը²⁴, արդյունքում ստանալով փոխհատուցում:

Այնուհանդերձ անձնական տվյալների պաշտպանության լիազոր մարմնի՝ ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության միջոցով տվյալների սուբյեկտի իրավունքների պաշտպանության գործընթացն ինքնին բարդ և երբեմն երկար ընթացակարգ է նախատեսում: Օրենքը տվյալներ մշակողին պարտադրում է անձնական տվյալների հետ իրականացվող անօրինական գործողություններ հայտնաբերելու դեպքում անհապաղ, բայց ոչ ուշ, քան երեք աշխատանքային օրվա ընթացքում վերացնել թույլ տված խախտումները²⁵, սակայն որևէ ժամկետային պարտավորություն չի սահմանում լիազոր մարմնի կողմից ստուգման գործողությունների ժամկետի համար, արդյունքում՝ անձը կարող է երկար սպասել իր իրավունքների վերականգման համար:

Անձի պատկերի կենսաչափական անձնական տվյալի դեպքում, իր իրավունքի խախտումը կարող է ճակատագրական լինել. հատկապես ներկայիս համացանցային ժամանակաշրջանում: Օրինակ, անձի պատկերի հրապարակումը առանց իր համաձայնության սեռական գործողություններ պատկերող կայքերում, կարող է վերջինիս անվան կամ բարի համբավին այնպիսի վնաս պատճառել, որի հետևանքները դժվար կլինի վերականգնել: Նույնիսկ հետագայում տվյալներ մշակողի կողմից այդ խախտման վերացումը չի կարող երաշխավորել անձի իրավունքների բացարձակ վերականգնում, քանի որ համացանցում հայտնվելիս այն կարող է ցանկացած պահի, ցանկացած վայրում ներբեռնվել այլ համակարգեր, ինչի արդյունքում՝ կփոխվի տվյալներ մշակողը: Եվ այս դեպքում՝ նոր մշակողի դեմ պետք է նոր բողոք ներկայացնել: Հետևաբար՝ պրակտիկայում նման խախտման վերացումը ամբողջ համացանցում անհնար է:

Այսօր աշխարհի ամենից հեղինակավոր լրատվամիջոցները, ինչպիսին են՝ Վաշինգտոն Փոստը (The Washington Post), Նյու Յորք Թայմսը (New York Times), Բիբիսին (BBC), Գիզմոդոն (Gizmodo) և մյուսները տեսանկյունից են այն մասին, որ անձի դեմքի և պատկերի անձնական տվյալի օգտագործումը դարձել է լայնամասշտաբ և շատ հաճախ օգտագործվում է ազգային անվտանգության և ոստիկանության կողմից՝ առանց անձի

համաձայնության²⁶: Վարորդական իրավունքների կամ անձնագրերի վրա պատկերված անձանց լուսանկարները ներբեռնվում են տվյալների ընդհանուր բազա և օգտագործվում մարդկանց նույնականացնելու համար և վերահսկելու վերջիններիս գործողությունները²⁷: ԱՄՆ-ում ոստիկանությունը օգտագործում էր տարբեր քաղաքներում տեղադրված տեսանկարահանող սարքերը նույնականացնելու «Սև կյանքերը կարևոր են» (Black lives matter) շարժման ակտիվիստներին՝ սահմանափակելով վերջիններիս ազատ արտահայտման և միավորվելու ազատության իրավունքները²⁸: Իսկ ահա Չինաստանում՝ հասարակ քաղաքացիների կյանքի վերահսկողությունը հասել է այն մակարդակի, որ պետությունը հայտարարել է ոչ միայն հանցագործությունների բացահայտման, այլև կանխման նպատակի մասին, այդպիսով ոստիկանության կողմից «կասկածելի» ընկալվող ցանկացած գործողություն արդեն իսկ կարող է ձեռքբերված հիմք հանդիսանալ, ինչը վերահսկվում է 170 միլիոն տեղակայված տեսաձայնագրող սարքերի միջոցով, որոնք նախատեսում են, որ կավելանան 400 միլիոնով²⁹:

Առավել մտահոգիչ են այնպիսի կազմակերպությունների գործունեությունը, ինչպիսիք են՝ ռուսական «Ֆայնդֆեյս» (Findface³⁰) և ամերիկյան «Քլիրվյու» (Clearview³¹) ընկերությունները: Վերջիններս գեներացնում են համացանցում, այդ թվում՝ սոցիալական ցանցերում միլիոնավոր անձանց պատկերները առանց նրանց թույլտվության, քանի որ դրանք տեսականորեն համարվում են հանրամատչելի անձնական տվյալներ, որի միջոցով կարողանում են նույնիսկ շարժման մեջ նույնականացնել աշխարհի ցանկացած կետում գտնվող ցանկացած անձի՝ վայրկյանների ընթացքում և հետևել վերջիններիս գործողություններն ամենայն մանրամասնությամբ³²: Ընդ որում՝ միաժամանակ մշակման են ենթարկվում այնպիսի հատուկ տվյալներ, ինչպիսիք են՝ անձի ռասան, մաշկի գույնը, ազգային պատկանելիությունը, հասակը, քաշը, սեռը և այլն: Այս տվյալները հավաքագրելուց հետո կարող են վաճառվել և՛ իրավապահ մարմիններին, և՛ մասնավոր ընկերություններին, և՛ անհատներին: Այս հավելվածների միջոցով նույնիսկ սովորական քաղաքացին կարող է սրճարանում նստած այլ անձի պատկերը բջջային հեռախոսով լուսանկարել, ներբեռնել ծրագիր և վայրկյանների ընթացքում այդ անձի մասին իմանալ ամբողջ տեղեկատվությունը՝ անուն, ազգանուն, հասցե, սոցիալական կայքի հասցեն, անձնական

www.ardaradutyjournal.com

ԱՐԴԱՐԱԴԱՏՈՒԹՅՈՒՆ

նկարները և այլն, քանի որ օրենսդրական որևէ կարգավորում այս ոլորտում չկա³³ :

Այսպիսով, ակնհայտ է դառնում, որ անձի պատկերը առանձնահատուկ կարգավիճակ ունեցող անձնական տվյալ է: Մյուս անձնական տվյալները կարող են կրկնվել կամ փոփոխվել, օրինակ՝ սովորական անձնական տվյալների դեպքում՝ նույն անուն, ազգանունով մարդիկ կամ հատուկ կատեգորիայի անձնական տվյալներ՝ նույն ռասայական կան էթնիկ ծագման մարդիկ կամ կենսաչափական

անձնական տվյալներ՝ նույն հասակի, քաշի կամ աչքի գույնի մարդիկ: Սակայն անձի պատկերը այնքան նույնական է անձի ինքնության հետ, այնքան հեշտ ճանաչելի և նույնականացման համար հաճախ օգտագործվող, որ այդ կենսաչափական անձնական տվյալի պաշտպանության համար անհրաժեշտ է առանձնահատուկ պաշտպանության մեխանիզմների սահմանում:

¹ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 3-րդ հոդվածի 1-ին մաս 13-րդ կետ
² IP հասցեն՝ անգլերենով Internet Protocol Address, թվային հասցեներ են, որոնք ցանցին միացած բոլոր համակարգիչները պետք է ունենան: Այդ հասցեները եզակի են՝ համացանցին միացած երկու համակարգիչ չեն կարող ունենալ միանման IP հասցե, https://hy.wikipedia.org/wiki/Այ-փի_հասցեներ:
³ Գեոմային տեղեկատվություն՝ ֆիզիկական անձի դեգոկսիրիբոնուկլիդինային թթվի (ԴՆԹ) որոշ հատվածների մասին կողավորված տեղեկատվություն պարունակող անձնական տվյալներ, համաձայն «Ռուսաստանի Դաշնությունում պետական գեոմային հաշվառման մասին» ֆեդերատիվ օրենքի 1-ին հոդվածի 1-ին մասի 3-րդ կետի:
⁴ «О государственной геномной регистрации в Российской Федерации» Федеральный закон от 03.12.2008 N 242-ФЗ.
⁵ «Օպերատիվ-հետախուզական գործունեության մասին» ՀՀ օրենքի հոդված 23-րդ և հոդված 28-րդ, 2007թ
⁶ ՀՀ քրեական դատավարության օրենսգիրք, հոդված 104-րդ
⁷ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, 2015թ. հոդված 13-րդ:
⁸ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, 2015թ. հոդված 12-րդ:
⁹ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, 2015թ. հոդված 13-րդ:
¹⁰ Biometric Consortium (BC), <https://web.archive.org/web/20060629052344/http://www.biometrics.org/> վերջին այցելություն՝ 01.02.2021:
¹¹ Վարչապետի 2009թ-ի. «Կենսաչափական կողմնորոշիչներ պարունակող էլեկտրոնային անձնագրերի և նույնականացման քարտերի համակարգի ներդրման միջոցառումների ժամանակացույցը հաստատելու մասին» N 501-Ա որոշում:
¹² International Biometric Identity Association (IBIA), <https://www.ibia.org> վերջին այցելություն՝ 01.02.2021:
¹³ European Association for Biometrics(EAB), <https://www.eab.org> վերջին այցելություն՝ 01.02.2021:
¹⁴ «Նույնականացման քարտերի մասին» ՀՀ օրենք, հոդված 4- րդ, մաս 2-րդ և մաս 3-րդ:
¹⁵ «Նույնականացման քարտերի մասին» ՀՀ օրենք, հոդված 8-րդ:
¹⁶ «Նոտարիատի մասին» ՀՀ օրենք, հոդված 71-րդ:
¹⁷ «Ձերբակալված և կալանավորված անձանց պահելու մասին» ՀՀ օրենք, հոդված 33-րդ:
¹⁸ Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. No 51-ФЗ // Российская газета. No 238-239. 08.12.1994; Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 г. No 14-ФЗ // Собрание законодательства РФ. 29.01.1996. No 5. Ст. 152.1; Гражданский кодекс Российской Федерации (часть третья) от 26 ноября 2001 г. No 146-ФЗ//Российская газета. No233. 28.11.2001.
¹⁹ ՀՀ քաղաքացիական օրենսգրքի 1112-րդ հոդվածի 10-րդ կետ:
²⁰ ՀՀ քաղաքացիական օրենսգրքի 1087.1-րդ հոդվածի 2-րդ մաս:
²¹ ՀՀ քաղաքացիական օրենսգրքի 1116-րդ հոդվածի 2-րդ մաս:
²² «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 4-րդ հոդվածի 1-ին մաս:
²³ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 4-րդ հոդվածի 2-րդ մաս:
²⁴ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 17-րդ հոդված, «Վարչական իրավախախտումների վերաբերյալ» ՀՀ օրենսգրքի 189.17-րդ հոդված:
²⁵ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 21-րդ հոդված, 3-րդ մաս:
²⁶ Gizmodo, “Leaked Document Shows Australian Police Use Creepy Clearview AI Facial Recognition Software”, Sarah Basford, February 29, 2020, <https://www.gizmodo.com.au/2020/02/australian-police-clearview-ai-facial-recognition/> վերջին այցելություն՝ 01.02.2021:
²⁷ The Perpetual Line-Up: Unregulated Police Face Recognition in America, october 18, 2016, Clare Garvie, Alvaro

Bedoya, Jonathan Frankle, Georgetown Law, Center on Privacy and Technology.

²⁸ The Washington Post “FBI, ICE find state driver’s license photos are a gold mine for facial-recognition searches” By Drew Harwell, July 7, 2019, <https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/> վերջին այցելություն՝ 01.02.2021:

²⁹ BBC News, “In Your Face: China’s all-seeing state”, Producer: Joyce Liu. Camera: Wang Xiqing, 10 December 2017, <https://www.bbc.com/news/av/world-asia-china-42248056> վերջին այցելություն՝ 01.02.2021:

³⁰ Findface Распознавание Лиц, Решения для государства и бизнеса, <https://findface.pro> վերջին այցելություն՝ 01.02.2021:

³¹ Securing our communities, Facial recognition search engine, <https://clearview.ai> վերջին այցելություն՝ 01.02.2021:

³² New York Times , “The Secretive Company That Might End Privacy as We Know It”, By Kashmir Hill, Published Jan. 18, 2020, <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> վերջին այցելություն՝ 01.02.2021:

³³ Вести, “FindFace: российская программа распознавания лиц завоевывает мир”, 22 февраля 2016, <https://www.vesti.ru/article/1656323> վերջին այցելություն՝ 01.02.2021:

ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, 18.05.2015, N ՀՕ-49-Ն օրենք
2. “О государственной геномной регистрации в Российской Федерации” Федеральный закон от 03.12.2008 N 242-ФЗ
3. «Օսլերատիվ-հետախուզական գործունեության մասին» ՀՀ օրենք, 2007թ.
4. Biometric Consortium (BC), <https://web.archive.org/web/20060629052344/http://www.biometrics.org/>
5. Վարչապետի 2009թ.-ի «Կենսաչափական կողմնորոշիչներ պարունակող էլեկտրոնային անձնագրերի և նույնականացման քարտերի համակարգի ներդրման միջոցառումների ժամանակացույցը հաստատելու մասին» N 501-Ա որոշում
6. International Biometric Identity Association (IBIA), <https://www.ibia.org>
7. European Association for Biometrics (EAB), <https://www.eab.org>
8. «Նույնականացման քարտերի մասին» ՀՀ օրենք
9. «Նոտարիատի մասին» ՀՀ օրենք
10. «Ձերբակալված և կալանավորված անձանց պահելու մասին» ՀՀ օրենք
11. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. No 51-ФЗ
12. Российская газета. No 238-239. 08.12.1994г.
13. Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 г. No 14-ФЗ
14. Собрание законодательства РФ. 29.01.1996. No 5. Ст. 152.1
15. Гражданский кодекс Российской Федерации (часть третья) от 26 ноября 2001 г. No 146-ФЗ
16. Российская газета. No233. 28.11.2001г.
17. ՀՀ քաղաքացիական օրենսգիրք
18. «Վարչական իրավախախտումների վերաբերյալ» ՀՀ օրենսգիրք
19. Gizmodo, “Leaked Document Shows Australian Police Use Creepy Clearview AI Facial Recognition Software”, Sarah Basford, February 29, 2020 <https://www.gizmodo.com.au/2020/02/australian-police-clearview-ai-facial-recognition/>
20. Clare Garvie, Alvaro Bedoya, Jonathan Frankle, The Perpetual Line-Up: Unregulated Police Face Recognition in America, october 18, 2016, Georgetown Law, Center on Privacy and Technology
21. The Washington Post , “FBI, ICE find state driver’s license photos are a gold mine for facial-recognition searches” By Drew Harwell, July 7, 2019, <https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/>
22. BBC News, “In Your Face: China’s all-seeing state”, Producer: Joyce Liu. Camera: Wang Xiqing, 10 December 2017, <https://www.bbc.com/news/av/world-asia-china-42248056>
23. Findface Распознавание Лиц, Решения для государства и бизнеса, <https://findface.pro>
24. Securing our communities, Facial recognition search engine, <https://clearview.ai>
25. New York Times, “The Secretive Company That Might End Privacy as We Know It”, By Kashmir Hill, Published Jan. 18, 2020, <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>
26. Вести, “FindFace: российская программа распознавания лиц завоевывает мир”, 22 февраля 2016, <https://www.vesti.ru/article/1656323>

Լուսինե Մինասյան

Советник департамента по координации и методологии сфер
по контролю за рынком и продовольственной безопасности
офиса по координации инспекционных органов
аппарата премьер-министра РА

РЕЗЮМЕ

Изображение человека как особый вид биометрических личных данных

Статья посвящена изучению изображения человека как особого вида биометрических личных данных. В ходе исследования были проанализированы важность и особенности биометрических персональных данных в полной системе защиты персональных данных. Отдельно были изучены изображение человека как личное данные, которое являются неотъемлемой частью личности и выявлены те законодательные регулирования, по которым образ личности удостоивается защиты.

Комплексному анализу подверглась роль защиты изображения человека для полноценного осуществления права человека на достойную жизнь и была выдвинута важность особого его статуса.

Ключевые слова: личные данные, право на защиту персональных данных, биометрические личные данные, изображение личности, основные права.

Lusine Minasyan

Adviser at the Department of Coordination and Methodology
of Areas for Market Control and Food Security of the Office of
Coordination of Inspection Bodies of the Prime Minister's Office

SUMMARY

The image of a person as a special type of biometric personal data

This article deals with issues concerning the image of a person as a special type of biometric personal data. In this study, analyzed the importance and characteristics of biometric personal data in a complete system of personal data protection. Were studied separately, the image of a person as inseparable part of the one's personality was analyzed in the light of those regulations according to which the image of a person has to be protected.

Comprehensive analysis has undergone the importance of the protection of image as an integral part of the fundamental right to a decent life and the ever-growing need of its special status in the world of biometric personal data protection.

Key words: personal data, right to personal data protection, biometric personal data, personal image, fundamental rights.

Բնագիրը ներկայացվել է 16.06.2021թ.

Ընդունվել է տպագրության 18.06.2021թ.

Հոդվածը երաշխավորել է տպագրության (գրախոսվել է)

իրավաբանական գիտությունների դոկտոր, պրոֆեսոր Ա. Խաչատրյանը