edpb
European Data Protection Board

Guidelines

Իրավապահ գործունեության ոլորտում դեմքի ճանաչման տեխնոլոգիայի կիրառման վերաբերյալ 05/2022 ուղեցույց[1]

Տարբերակ 2.0

Ընդունվել է 2023 թվականի ապրիլի 26-ին

[1] Սույն թարգմանությունը Տվյալների պաշտպանության եվրոպական խորհուրդի կողմից իրականացված պաշտոնական թարգմանություն չէ: Թարգմանությունն իրականացվել է Գերմանական միջազգային համագործակցության ընկերության (GIZ) ֆինանսական աջակցությամբ Արևելյան գործընկերության տարածաշրջանային ֆոնդի շրջանակներում: Թարգմանությունն իրականացվել է Անձնական տվյալների պաշտպանության, Գերմանական միջազգային համագործակցության ընկերության և Տվյալների պաշտպանության եվրոպական խորհուրդի միջև սերտ համագործակցության արդյունքում:

Տարբերակի պատմությունը

Տարբերակ 1.0	2022 թվականի մայիսի 12	Ուղեցույցի ընդունում՝ հանրային քննարկումների համար
Տարբերակ 2.0	2023 թվականի ապրիլի 26	Ուղեցույցի ընդունում՝ հանրային քննարկումներից հետո

Բովանդակություն

ԱՄՓՈՓ ՆԿԱՐԱԳԻՐԸ

Ավելի ու ավելի շատ իրավապահ մարմիններ (ԻՄ-եր) կիրառում կամ պլանավորում են կիրառել դեմքի ճանաչման տեխնոլոգիան (ԴՃՏ)։ Այն կարող է կիրառվել ինչպես անձին **իսկորոշելու** կամ **նույնականացնելու** համար, այնպես էլ տեսանյութերի (օրինակ՝ տեսահսկման համակարգի) կամ լուսանկարների վրա։ Այն կարող է կիրառվել տարբեր նպատակներով, այդ թվում՝ ոստիկանության հետախուզման ցուցակներում գտնվող անձանց որոնելու կամ հանրային տարածքում մարդկանց տեղաշարժերը մշտադիտարկելու համար։

ԴՃՏ-ն կառուցված է **կենսաչափական տվյալների** մշակման վրա, հետևաբար, այն ներառում է հատուկ կատեգորիայի անձնական տվյալների մշակում։ Հաճախ ԴՃՏ-ում կիրառում են **արհեստական բանականության** (ԱԲ) կամ մեքենայական ուսուցման (ՄՈՒ) բաղադրիչներ։ Թեև սա հնարավորություն է տալիս մշակելու մեծածավալ տվյալներ, այնուամենայնիվ, այն նաև ներառում է խտրականության և կեղծ արդյունքների ռիսկ։ ԴՃՏ-ն կարող է կիրառվել 1-ը 1-ին վերահսկվող իրավիճակներում, ինչպես նաև մեծ թվով մարդկանց և կարևոր տրանսպորտային հանգույցների դեպքում։

ԴՃՏ-ն **առանցքային գործիք** է **ԻՄ-երի համար**։ ԻՄ-երը համարվում են գործադիր իշխանության մարմիններ և ունեն ինքնիշխան լիազորություններ։ Անձնական տվյալների պաշտպանության իրավունքից բացի ԴՃՏ-ն կարող է միջամտել նաև հիմնարար իրավունքներին և կարող է ներազդել մեր սոցիալական և ժողովրդավարական քաղաքական կայունության վրա։

Իրավապահ գործունեության համատեքստում անձնական տվյալների պաշտպանության համար պետք է բավարարվեն **Իրավունքի կիրառման հրահանգի (ԻԿՀ) պահանջները**։ ԻԿՀ-ով, մասնավորապես՝ դրա 3(13) հոդվածով («կենսաչափական տվյալներ» եզրույթ), 4-րդ հոդվածով (անձնական տվյալների մշակմանը վերաբերող սկզբունքներ), 8-րդ հոդվածով (մշակման օրինականություն), 10-րդ հոդվածով (հատուկ կատեգորիայի անձնական տվյալների մշակում) և 11-րդ հոդվածով (ավտոմատացված անհատական որոշումների կայացում) նախատեսվում է ԴՃՏ-ի կիրառման հետ կապված որոշ շրջանակ։

ԴՃՏ-ի կիրառումը կարող է բացասաբար անդրադառնալ նաև մի շարք այլ հիմնարար իրավունքների վրա։ Ուստի, **Հիմնարար իրավունքների ԵՄ խարտիան** (Խարտիա) էական նշանակություն ունի ԻԿՀ, մասնավորապես՝ Խարտիայի 8-րդ հոդվածով նախատեսված անձնական տվյալների պաշտպանության իրավունքի, ինչպես նաև Խարտիայի 7-րդ հոդվածով սահմանված անձնական կյանքի անձեռնմխելիության իրավունքի մեկնաբանման համար։

Անձնական տվյալների մշակման համար իրավական հիմք հանդիսացող **օրենսդրական միջոցներն** ուղղակիորեն միջամտում են Խարտիայի 7-րդ և 8-րդ հոդվածներով երաշխավորված իրավունքներին։ Բոլոր դեպքերում կենսաչափական տվյալների մշակումն ինքնին լուրջ միջամտություն է։ Սա կախված չէ արդյունքից, օրինակ՝ դրական համընկնումից։ Հիմնարար իրավունքների ու ազատությունների իրացման ցանկացած սահմանափակում պետք է նախատեսվի օրենքով և հարգի այդ իրավունքների ու ազատությունների էությունը։

Իրավական հիմքը պետք է լինի **բավականաչափ հստակ** ձևակերպված, որպեսզի քաղաքացիները բավարար պատկերացում ունենան այն պայմանների և հանգամանքների մասին, որոնց դեպքում մարմիններն իրավասու են դիմելու տվյալների հավաքագրման և գաղտնի հսկողության ցանկացած միջոցի: ԻԿՀ 10-րդ հոդվածի ընդհանուր դրույթի ուղղակի փոխատեղումը ներպետական իրավունքում զուրկ կլինի ճշգրտությունից և կանխատեսելիությունից:

Նախքան ազգային օրենսդրի կողմից դեմքի ճանաչման տեխնոլոգիայի կիրառման միջոցով կենսաչափական տվյալների մշակման ցանկացած եղանակի համար նոր իրավական հիմք ստեղծելը, անհրաժեշտ է **խորհրդակցել** տվյալների պաշտպանության հարցերով իրավասու վերահսկող մարմնի հետ:

Օրենսդրական միջոցները պետք է լինեն **համապատասխան**՝ խնդրո առարկա օրենսդրությամբ հետապնդվող իրավաչափ նպատակներին հասնելու համար: **Ընդհանուր հետաքրքրություն ներկայացնող նպատակը**, որքան էլ հիմնարար լինի, ինքնին չի արդարացնում հիմնարար իրավունքի սահմանափակումը: Օրենսդրական միջոցներով պետք է **տարբերակվեն** դրանց գործողության ոլորտում ընդգրկվող անձինք և պետք է ուղղված լինեն նրանց նպատակի, օրինակ՝ կոնկրետ ծանր հանցագործության դեմ պայքարին: Եթե միջոցն ընդհանուր առմամբ տարածվում է բոլոր անձանց վրա, առանց այդ տարբերակման, սահմանափակման կամ բացառության, ապա այն ուժեղացնում է միջամտությունը: Այն նաև ուժեղացնում է միջամտությունը, եթե տվյալների մշակումն ընդգրկում է բնակչության զգալի մասը:
Տվյալները պետք է մշակվեն այնպես, որպեսզի ապահովվեն տվյալների պաշտպանության ԵՄ կանոնների և սկզբունքների կիրառելիությունն ու արդյունավետությունը: Ելնելով յուրաքանչյուր իրավիճակից՝ **անհրաժեշտության և համաչափության գնահատմամբ** պետք է նաև սահմանվեն և դիտարկվեն այլ հիմնարար իրավունքների համար բոլոր հնարավոր հետևանքները: Եթե տվյալները համակարգված կերպով մշակվում են առանց տվյալների սուբյեկտների գիտության, ապա դա հավանաբար կառաջացնի **մշտական հսկողության տակ լինելու ընդհանուր զգացողություն**: Սա կարող է որոշ կամ բոլոր հիմնարար իրավունքների, ինչպիսիք են Խարտիայի 1-ին հոդվածով նախատեսված՝ մարդու արժանապատվության, Խարտիայի 10-րդ հոդվածով նախատեսված՝ մտքի, խղճի և կրոնի ազատության, Խարտիայի 11-րդ հոդվածի համաձայն արտահայտվելու ազատության, ինչպես նաև Խարտիայի 12-րդ հոդվածով նախատեսված՝ հավաքների և միավորումներ կազմելու ազատության իրավունքների առնչությամբ հանգեցնել զսպող ազդեցությունների:

Հատուկ կատեգորիայի տվյալների, օրինակ՝ կենսաչափական տվյալների մշակումը կարող է համարվել «**խիստ անհրաժեշտ**» (ԻԿՀ 10-րդ հոդված), միայն եթե անձնական տվյալների պաշտպանությանը միջամտությունը և դրա սահմանափակումները սահմանափակվում են նրանով, ինչը բացարձակ անհրաժեշտ, այսինքն՝ պարտադիր է՝ բացառելով ընդհանուր կամ համակարգված բնույթ կրող ցանկացած մշակում:

Այն փաստը, որ լուսանկարն **ակնհայտորեն հանրամատչելի է դարձվել** (ԻԿՀ 10-րդ հոդված) տվյալների սուբյեկտի կողմից, չի նշանակում, որ նրան առնչվող կենսաչափական տվյալները, որոնք կարող են առբերվել լուսանկարից հատուկ տեխնիկական միջոցներով, համարվում են ակնհայտորեն հանրամատչելի դարձված: Ծառայության կանխադրված կարգավորումները, օրինակ՝ մոդելները հանրամատչելի դարձնելը կամ ընտրության բացակայությունը, օրինակ՝ մոդելները հանրամատչելի են դարձվել առանց օգտատիրոջ կողմից այդ կարգավորումը փոխելու հնարավորության, չպետք է ոչ մի կերպ մեկնաբանվեն

որպես ակնհայտորեն հանրամատչելի դարձված տվյալներ:

ԻԿՀ 11-րդ հոդվածով սահմանվում է **ավտոմատացված անհատական որոշումների կայացման** շրջանակը: ԴՀՏ-ի կիրառումը ենթադրում է հատուկ կատեգորիայի տվյալների օգտագործում և կարող է հանգեցնել պրոֆիլավորման՝ կախված ԴՀՏ-ի կիրառման եղանակից ու նպատակից: Ամեն դեպքում, Միության իրավունքին և ԻԿՀ 11(3) հոդվածին համապատասխան, պրոֆիլավորումը, որը հանգեցնում է հատուկ կատեգորիայի անձնական տվյալների հիման վրա ֆիզիկական անձանց նկատմամբ խտրականության, արգելվում է:

ԻԿՀ 6-րդ հոդվածը վերաբերում է **տարբեր կատեգորիաների տվյալների սուբյեկտների միջև տարբերակում դնելու** անհրաժեշտությանը: Ինչ վերաբերում է տվյալների սուբյեկտներին, որոնց առնչությամբ չկա որևէ ապացույց, որը հնարավորություն կտա ենթադրելու, որ նրանց վարքագիծը կարող է նույնիսկ անուղղակի կամ հեռահար կապ ունենալ ԻԿՀ համաձայն իրավաչափ նպատակի հետ, միջամտության համար հիմնավորում, ամենայն հավանականությամբ, առկա չէ:

Տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքով (ԻԿՀ 4(1)(ե) հոդված) պահանջվում է նաև, որ մշակման նպատակի համար կարևորություն չներկայացնող ցանկացած տեսանյութ մինչև շրջանառության մեջ դրվելը պետք է միշտ հեռացվի կամ անանունացվի (օրինակ՝ մշուշապատման միջոցով՝ առանց տվյալների վերականգնման հետադարձ հնարավորության):

Հսկողը պետք է մանրամասնորեն դիտարկի, թե ինչպես (կամ եթե կարող է) բավարարի **տվյալների սուբյեկտի իրավունքներին ներկայացվող** պահանջները, նախքան որևէ ԴՀՏ-ով մշակում իրականացնելը, քանի որ ԴՀՏ-ն հաճախ ներառում է հատուկ կատեգորիայի անձնական տվյալների մշակում՝ առանց տվյալների սուբյեկտի հետ որևէ ակնհայտ փոխգործակցության:

Տվյալների սուբյեկտի իրավունքների արդյունավետ իրացումը կախված է հսկողի կողմից **տեղեկություններ տրամադրելու** իր **պարտավորությունների** կատարումից (ԻԿՀ 13-րդ հոդված): ԻԿՀ 13(2) հոդվածի համաձայն՝ «հատուկ դեպքի» առկայությունը գնահատելիս անհրաժեշտ է հաշվի առնել մի շարք գործոններ, այդ թվում, եթե անձնական տվյալները հավաքագրվում են առանց տվյալների սուբյեկտի գիտության, քանի որ դա միակ միջոցն է, որը տվյալների սուբյեկտներին տալիս է իրենց իրավունքներն արդյունավետորեն իրացնելու հնարավորություն: Եթե որոշումները կայացվեն բացառապես ԴՀՏ-ի հիման վրա, ապա տվյալների սուբյեկտները պետք է տեղեկացված լինեն ավտոմատացված որոշումների կայացման առանձնահատկությունների մասին:

Ինչ վերաբերում է **հասանելիություն ստանալու մասին դիմումներին**, երբ կենսաչափական տվյալները պահվում և կապվում են ինքնության հետ նաև տառաթվային տվյալների միջոցով՝ տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքին համապատասխան, դա պետք է հնարավորություն տա իրավասու մարմնին հաստատելու հասանելիություն ստանալու մասին դիմումը՝ հիմնվելով այդ տառաթվային տվյալներով որոնման վրա և առանց այլ անձանց կենսաչափական տվյալների ցանկացած հետագա մշակման (այսինքն՝ ԴՀՏ-ով որոնելով տվյալների շտեմարանում):

Տվյալների սուբյեկտների համար ռիսկերը հատկապես մեծ են, եթե ոստիկանության տվյալների շտեմարանում պահվում են ոչ ճշգրիտ տվյալներ, և (կամ) դրանք փոխանցվում են այլ կազմակերպություններ: Հսկողը պետք է համապատասխանաբար **ուղղի** պահված

տվյալները և ԴՁՏ համակարգերը (տե՛ս նաև ԻԿՀ 47-րդ ներածական դրույթը):

Սահմանափակման իրավունքը հատկապես կարևոր է դառնում, երբ հարցը վերաբերում է դեմքի ճանաչման տեխնոլոգիային (որը հիմնված է ալգորիթմի (ալգորիթմների) վրա և, հետևաբար, վերջնական արդյունք չի տալիս) այն դեպքերում, երբ հավաքագրվում են մեծ քանակությամբ տվյալներ, և նույնականացման ճշտությունն ու որակը կարող են տարբերվել:

Մինչև ԴՁՏ-ի կիրառումը **տվյալների պաշտպանության ազդեցության գնահատում իրականացնելը (ՏՊԱԳ)** պարտադիր պահանջ է, տե՛ս ԻԿՀ 27-րդ հոդվածը: ՏՊԵԽ-ն առաջարկում է հանրամատչելի դարձնել այդ գնահատումների արդյունքները կամ առնվազն ՏՊԱԳ-ի հիմնական արդյունքներն ու եզրահանգումները՝ որպես վստահության և թափանցիկության մակարդակի բարձրացման միջոց:

ԴՁՏ-ի գործարկման և կիրառման տարբերակերի մեծ մասի դեպքում առկա է տվյալների սուբյեկտների իրավունքների ու ազատությունների համար բարձր ռիսկ: Հետևաբար, ԴՁՏ-ն գործարկող մարմինը մինչև համակարգի գործարկումը պետք է **խորհրդակցի** իրավասու վերահսկող մարմնի հետ:

Հաշվի առնելով կենսաչափական տվյալների եզակի բնույթը՝ ԴՁՏ-ն ներդնող և (կամ) կիրառող մարմինը պետք է հատուկ ուշադրություն դարձնի **մշակման անվտանգությանը**՝ ԻԿՀ 29-րդ հոդվածին համապատասխան: Մասնավորապես, իրավապահ մարմինը պետք է ապահովի, որ համակարգը համահունչ լինի համապատասխան ստանդարտների հետ և ձեռնարկի կենսաչափական մոդելների պաշտպանության միջոցներ: Տվյալների պաշտպանության սկզբունքներն ու երաշխիքները պետք է ներկառուցված լինեն տեխնոլոգիայի մեջ՝ մինչև անձնական տվյալների մշակումն սկսելը: Հետևաբար, նույնիսկ երբ ԻՄ-ն պլանավորում է կիրառել և օգտագործել արտաքին մատակարարներից ԴՁՏ-ն, այն պետք է օրինակ՝ գնումների ընթացակարգի միջոցով ապահովի, որ գործարկվի միայն տվյալների՝ հայեցակարգային և լռելյայն պաշտպանության սկզբունքների վրա կառուցված ԴՁՏ-ն:

Գրանցամատյանի վարումը (տե՛ս ԻԿՀ 25-րդ հոդվածը) կարևոր երաշխիք է ինչպես ներքին (այսինքն՝ համապատասխան հսկողի/մշակողի կողմից ինքնամշտադիտարկում), այնպես էլ արտաքին վերահսկող մարմինների կողմից մշակման օրինականությունը ստուգելու համար: Դեմքի ճանաչման համակարգերի համատեքստում առաջարկվում է գրանցամատյանի վարում նաև վկայակոչման տվյալների շտեմարանում փոփոխությունների կատարման և նույնականացման կամ ստուգման փորձերի համար, այդ թվում՝ օգտատիրոջ, արդյունքի և վստահության գնահատականի համար: Գրանցամատյանի վարումը, այնուամենայնիվ, **հաշվետվողականության ընդհանուր սկզբունքի** մեկ էական տարրն է (տե՛ս ԻԿՀ 4(4) հոդվածը): Հսկողը պետք է կարողանա ապացուցել մշակման համապատասխանությունը ԻԿՀ 4(1)-(3) հոդվածի տվյալների պաշտպանության հիմնական սկզբունքներին:

ՏՊԵԽ-ը հիշեցնում է իր և ՏՊԵՎՄ-ի համատեղ **կոչը՝ արգելելու** որոշ տեսակի մշակումները, որոնք կապված են 1) հանրային տարածքներում անձանց հեռավար կենսաչափական նույնականացման հետ, 2) ԱԲ-ի հիման վրա աշխատող դեմքի ճանաչման համակարգերի հետ, որոնք կենսաչափական տվյալների հիման վրա դասակարգում են անձանց ըստ խմբերի՝ ելնելով էթնիկ պատկանելությունից, սեռից, ինչպես նաև քաղաքական կամ սեռական կողմնորոշումից կամ խտրականության այլ հիմքից, 3) դեմքի ճանաչման կամ

նմանատիպ տեխնոլոգիաների կիրառման հետ՝ ֆիզիկական անձի հույզերը դուրս բերելու համար և 4) իրավապահ գործունեության համատեքստում անձնական տվյալների մշակման հետ, որը հիմնված կլինի լայնամասշտաբ և ոչ ընտրողաբար անձնական տվյալների հավաքագրմամբ, օրինակ՝ առցանց հասանելի լուսանկարների ու դեմքի նկարների ներբեռնմամբ համալրված տվյալների շտեմարանի վրա:

Վտանգված հիմնարար իրավունքների հիմնական երաշխիքը տվյալների պաշտպանության իրավասու վերահսկող մարմինների կողմից **արդյունավետ վերահսկողությունն** է: Հետևաբար, անդամ պետությունները պետք է ապահովեն, որ վերահսկող մարմիններն ունենան համապատասխան և բավարար ռեսուրսներ՝ իրենց լիազորություններն իրականացնելու համար:

Այս **ուղեցույցն ուղղված է** ԵՄ և ազգային մակարդակով օրենսդիրներին, ինչպես նաև ԴՀՏ համակարգեր ներդնող և կիրառող ԻՄ-երին և դրանց ծառայողներին: Այն ֆիզիկական անձանց ուղղված է այնքանով, որքանով դա նրանց ընդհանուր առմամբ կհետաքրքրի կամ որքանով նրանք դիտարկվում են որպես տվյալների սուբյեկտ, մասնավորապես՝ կապված տվյալների սուբյեկտների իրավունքների հետ:

Ուղեցույցի նպատակն է տեղեկություններ տրամադրել իրավապահ գործունեության (մասնավորապես՝ ԻԿՀ) համատեքստում ԴՀՏ-ի որոշ հատկությունների և կիրառելի իրավական շրջանակի մասին:

- Բացի այդ, ուղեցույցը գործիք է տրամադրում՝ **տվյալ կիրառման տարբերակի** զգայունության առաջին դասակարգմանն աջակցելու համար (Հավելված I).
- ուղեցույցը նաև **գործնական ուղղորդում է տալիս ԻՄ-երին, որոնք ցանկանում են ձեռք բերել և գործարկել ԴՀՏ համակարգ** (Հավելված II).
- ուղեցույցում ներկայացվում են նաև մի շարք բնորոշ **կիրառման տարբերակներ և թվարկվում են մի շարք կարևոր դիտարկումներ**՝ հատկապես կապված անհրաժեշտության և համաչափության ստուգման հետ (Հավելված III):

1 ՆԵՐԱԾՈՒԹՅՈՒՆ

1. Դեմքի ճանաչման տեխնոլոգիան (ԴՃՏ) կարող է կիրառվել՝ անձանց իրենց դեմքով ավտոմատ ճանաչելու համար: ԴՃՏ-ն հաճախ հիմնված է արհեստական բանականության, ինչպես օրինակ՝ մեքենայական ուսուցման տեխնոլոգիաների վրա: Գնալով էլ ավելի շատ է փորձարկվում ԴՃՏ-ն և կիրառվում տարբեր ոլորտներում, սկսած անհատների կողմից կիրառվելուց մինչև մասնավոր կազմակերպությունների և պետական կառավարման մարմինների կողմից կիրառվելը: Իրավապահ մարմինները (ԻՄ-եր) նույնպես ակնկալում են առավելություններ ստանալ ԴՃՏ-ի կիրառումից: Վերջինս խոստանում է տալ ինչպես համեմատաբար նոր մարտահրավերների, օրինակ՝ հավաքագրված մեծ թվով ապացույցներով գործերի քննությունների, այնպես էլ հայտնի խնդիրների, մասնավորապես՝ դիտարկման և որոնման առաջադրանքների համար կադրերի պակասի խնդրի լուծումներ:

2. ԴՃՏ-ի նկատմամբ մեծ հետաքրքրությունը պայմանավորված է դրա արդյունավետությամբ և մասշտաբայնությամբ: Առավելությունների հետ մեկտեղ առկա են տեխնոլոգիայի և դրա կիրառության հետ կապված թերությունները, ընդ որում մեծ մասշտաբներով: Թեև կոճակի մեկ հպումով կարող են վերլուծվել հազարավոր անձնական տվյալների հավաքածուներ, այնուամենայնիվ, ալգորիթմի հետևանքով առաջացող խտրականության կամ սխալ նույնականացման նույնիսկ թեթև հետևանքները կարող են հանգեցնել նրան, որ մեծ թվով մարդիկ մեծապես կտուժվեն իրենց վարքագծում և առօրյա կյանքերում: Անձնական տվյալների, մասնավորապես կենսաչափական տվյալների մշակման մեծ մասշտաբները ԴՃՏ-ի ևս մեկ առանցքային տարրերից է, քանի որ անձնական տվյալների մշակումը Հիմնարար իրավունքների Եվրոպական միության խարտիայի (Խարտիա) 8-րդ հոդվածի համաձայն հանդիսանում է անձնական տվյալների պաշտպանության հիմնարար իրավունքին միջամտություն:

3. ԻՄ-երի կողմից ԴՃՏ-ի կիրառությունը կունենա և որոշ չափով արդեն ունի զգալի հետևանքներ անձանց և մարդկանց խմբերի, այդ թվում՝ փոքրամասնությունների վրա: Այդ հետևանքները զգալի ազդեցություններ կունենան համակեցության և մեր սոցիալական ու ժողովրդավարական քաղաքական կայունության վրա՝ բազմակարծության և քաղաքական ընդդիմության մեծ նշանակությունն արժեվորելու լույսի ներքո: Անձնական տվյալների պաշտպանության իրավունքը հաճախ մյուս հիմնարար իրավունքները երաշխավորելու կարևոր նախապայման է: ԴՃՏ-ի կիրառությունը կարող է զգալիորեն խախտել այն հիմնարար իրավունքները, որոնք դուրս են անձնական տվյալների պաշտպանության իրավունքի շրջանակից:

4. Հետևաբար, ՏՊԵԽ-ը՝ կարևորելով իրավապահ գործունեության ոլորտում ԴՃՏ-ի շարունակական ինտեգրումը, որը կարգավորվում է Իրավունքի կիրառման հրահանգով[1] և համապատասխանաբար այն փոխատեղող ազգային օրենքներով, տրամադրում է այս ուղեցույցը: Ուղեցույցը տեղեկություններ է տրամադրում ԵՄ և ազգային մակարդակով օրենսդիրներին, ինչպես նաև ԴՃՏ համակարգերի ներդրման և կիրառման ժամանակ ԻՄ-երին և դրանց ծառայողներին: Ուղեցույցի շրջանակը սահմանափակվում է ԴՃՏ-ով: Այնուամենայնիվ, ԻՄ-երի կողմից կենսաչափական տվյալների վրա հիմնված անձնական տվյալների մշակման մյուս ձևերը, հատկապես, եթե մշակվում են հեռավար կարգով, կարող են նմանատիպ կամ լրացուցիչ ռիսկեր առաջացնել անհատների, խմբերի և

հասարակության համար: Ելնելով համապատասխան հանգամանքներից՝ այս ուղեցույցի որոշ հայեցակետեր նույնպես կարող են այս դեպքերում օգտակար աղբյուր լինել: Վերջապես, անձինք, որոնք պարզապես հետաքրքրված են կամ դիտարկվում են որպես տվյալների սուբյեկտ, կարող են նույնպես գտնել կարևոր տեղեկություններ, մասնավորապես՝ կապված տվյալների սուբյեկտների իրավունքների հետ:

5. Ուղեցույցը բաղկացած է հիմնական փաստաթղթից և երեք հավելվածից: Հիմնական փաստաթղթում ներկայացված են տեխնոլոգիան և կիրառելի իրավական շրջանակը: Որպեսզի հնարավոր լինի որոշել կիրառման տվյալ ոլորտում հիմնարար իրավունքներին միջամտության լրջությունը դասակարգելու որոշ հիմնական հայեցակետերը, ձևանմուշը կարելի է գտնել I հավելվածում: ԻՄ-երը, որոնք ցանկանում են ձեռք բերել և գործարկել ԴՃՏ համակարգ, կարող են գործնական ուղղորդում գտնել II հավելվածում: Կախված ԴՃՏ-ի կիրառման ոլորտից՝ տարբեր նկատառումներ կարող են կարևոր լինել: Մի շարք հիպոթետիկ սցենարներ և կարևոր նկատառումներ կարելի է գտնել III հավելվածում:

[1] Քրեական իրավախախտումների կանխման, քննության, հայտնաբերման կամ հետապնդման կամ քրեական պատիժների կատարման նպատակներով իրավասու մարմինների կողմից անձնական տվյալների մշակման մասով ֆիզիկական անձանց պաշտպանության, ինչպես նաև այդ տվյալների ազատ տեղաշարժի մասին և Խորհրդի 2008/977/ԱՆԳ շրջանակային որոշումը չեղյալ համարող՝ Եվրոպական պառլամենտի և Խորհրդի 2016 թվականի ապրիլի 27-ի 2016/680 հրահանգ (ԵՄ):

2 ՏԵԽՆՈԼՈԳԻԱՆ

2.1 Մեկ կենսաչափական տեխնոլոգիա, երկու հստակ ֆունկցիա

6. Դեմքի ճանաչումը հավանականության վրա հիմնված տեխնոլոգիա է, որը կարող է ավտոմատ կերպով ճանաչել անձանց իրենց դեմքով՝ վերջիններիս իսկորոշելու կամ նույնականացնելու համար:

7. **ԴՃՏ-ն** դասակարգվում է կենսաչափական տեխնոլոգիաների ավելի լայն կատեգորիայի: Կենսաչափությունը ներառում է բոլոր ավտոմատացված պրոցեսները, որոնք օգտագործվում են անձին ճանաչելու համար՝ ֆիզիկական, ֆիզիոլոգիական կամ վարքային բնութագրերի քանակական գնահատման միջոցով (մատնահետքեր, ծիածանաթաղանթի կառուցվածք, ձայն, քայլվածք, արյունատար անոթների կառուցվածքներ և այլն): Այդ բնութագրերը սահմանվում են որպես «կենսաչափական տվյալներ», քանի որ դրանք թույլ են տալիս կամ հաստատում են տվյալ անձի եզակի նույնականացումը:

8. Դա վերաբերում է մարդկանց դեմքերին կամ, ավելի կոնկրետ, դեմքի ճանաչման սարքերի միջոցով դրանց տեխնիկական մշակմանը, այսինքն՝ վերցնելով դեմքի պատկերը (լուսանկարը կամ տեսանյութը), որը կոչվում է կենսաչափական նմուշ, հնարավոր է դուրս բերել այդ դեմքի հստակ բնութագրերի թվային ներկայացումը (սա կոչվում է մոդել):

9. Կենսաչափական մոդելն այն եզակի բնութագրերի թվային ներկայացումն է, որոնք դուրս են բերվել կենսաչափական նմուշից և կարող են պահվել կենսաչափական տվյալների շտեմարանում[2]: Այդ մոդելը եզակի է և հատուկ յուրաքանչյուր անձի համար և, սկզբունքորեն, ժամանակի ընթացքում չի փոփոխվում[3]: Ճանաչման փուլում սարքն այդ մոդելը համեմատում է այլ մոդելների հետ, որոնք նախկինում ստեղծվել կամ հաշվարկվել են ուղղակիորեն կենսաչափական նմուշներից, օրինակ՝ պատկերի, լուսանկարի կամ տեսանյութի մեջ երևացող դեմքերից: Հետևաբար, «դեմքի ճանաչումը» երկու քայլից բաղկացած պրոցես է՝ դեմքի պատկերի հավաքում և դրա մոդելի վերածում, որին հաջորդում է այդ դեմքի ճանաչումը՝ համապատասխան մոդելը համեմատելով մեկ կամ մի քանի այլ մոդելների հետ:

10. Ինչպես ցանկացած կենսաչափական գործընթաց, դեմքի ճանաչումը կարող է կատարել երկու հստակ ֆունկցիա՝

- անձի **իսկորոշում**, որի նպատակն է ստուգել, թե արդյոք նա այն անձն է, ում անունից ներկայանում է: Այս դեպքում համակարգը կհամեմատի նախապես ֆիքսված կենսաչափական մոդելը կամ նմուշը (օրինակ՝ սմարթ քարտում կամ կենսաչափական անձնագրում պահված մոդելը կամ նմուշը) մեկ դեմքի հետ, օրինակ՝ անցակետում գտնվող անձի դեմքի մոդելի կամ նմուշի հետ, որպեսզի ստուգի, թե արդյոք դա միևնույն անձն է: Ուստի, այս ֆունկցիոնալությունը հիմնված է երկու մոդելների համեմատության վրա: Սա նաև կոչվում է 1-ը 1-ի հետ **ստուգում.**

[2] Դեմքի ճանաչման վերաբերյալ ուղեցույց, «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» 108 կոնվենցիայի խորհրդատվական կոմիտե, Եվրոպայի խորհուրդ, 2021 թվականի հունիս:

[3] Սա կարող է կախված լինել կենսաչափության տեսակից և տվյալների սուբյեկտի տարիքից:

- անձի **նույնականացում**, որի նպատակն է գտնել անձին մի խումբ անձանց մեջ, կոնկրետ տարածքում, պատկերում կամ տվյալների շտեմարանում: Այս դեպքում համակարգը պետք է մշակի յուրաքանչյուր հավաքված դեմք, որպեսզի գեներացնի կենսաչափական մոդել և հետո ստուգի, թե արդյոք այն համընկնում է համակարգին ծանոթ անձի հետ: Այսպիսով, այս ֆունկցիոնալությունը հիմնված է մեկ մոդելի՝ մոդելների կամ նմուշների տվյալների շտեմարանի հետ համեմատության վրա (ելակետ): Սա նաև կոչվում է 1-ը շատի հետ նույնականացում: Օրինակ՝ այն կարող է տվյալների գրանցման շտեմարանը (ազգանունը, անունը) կապել դեմքի հետ, եթե համեմատությունը կատարվում է ազգանունների և անունների հետ կապված լուսանկարների շտեմարանի հետ: Այն կարող է նաև ներառել ամբոխի միջով մարդուն հետևելը, առանց անձի քաղաքացիական ինքնության հետ պարտադիր կապ ստեղծելու:

11. Երկու դեպքում էլ դեմքի ճանաչման կիրառվող տեխնիկաները հիմնված են մոդելների, այսինքն՝ համեմատվող և ելակետային մոդելի (մոդելների) միջև մոտավոր համընկնման վրա: Այս տեսակետից դրանք հիմնված են հավանականության տեսության վրա. համեմատությունը դուրս է բերում ավելի մեծ կամ ցածր հավանականություն, որ անձն իսկապես այն անձն է, որը պետք է իսկորոշվի կամ նույնականացվի. եթե այդ հավանականությունը գերազանցում է համակարգում օգտատիրոջ կամ համակարգը մշակողի կողմից սահմանված որոշակի շեմը, ապա համակարգը կենթադրի, որ կա համընկնում:

12. Թեև երկու ֆունկցիաները՝ իսկորոշումն ու նույնականացումը, հստակ են, դրանք երկուսն էլ վերաբերում են նույնականացված կամ նույնականացման ենթակա ֆիզիկական անձին առնչվող կենսաչափական տվյալների մշակմանը և, հետևաբար, կազմում են անձնական տվյալների մշակում, իսկ ավելի կոնկրետ՝ հատուկ կատեգորիայի անձնական տվյալների մշակում:

13. Դեմքի ճանաչումը տեսապատկերի մշակման տեխնիկաների ավելի լայն շրջանակի մի մասն է: Որոշ տեսախցիկներ կարող են նկարահանել մարդկանց կոնկրետ տարածքում, մասնավորապես՝ նրանց դեմքերը, սակայն դրանք որպես այդպիսին չեն կարող օգտագործվել անձանց ավտոմատ ճանաչելու համար: Նույնը վերաբերում է պարզ լուսանկարին. տեսախցիկը դեմքի ճանաչման համակարգ չէ, քանի որ մարդկանց լուսանկարները պետք է մշակվեն հատուկ եղանակով՝ կենսաչափական տվյալներ դուրս բերելու համար:

14. Այսպես կոչված սմարթ տեսախցիկներով դեմքերի զուտ հայտաբերումը նույնպես պարտադիր չէ, որ իրենից ներկայացնի դեմքի ճանաչման համակարգ: Թեև դրանք նույնպես կարևոր հարցեր են բարձրացնում էթիկայի և արդյունավետության, աննորմալ վարքագծի կամ բռնի իրադարձությունների հայտնաբերման թվային տեխնիկաների, դեմքին արտահայտված հույզերի կամ նույնիսկ ուրվանկարների ճանաչման տեսանկյունից, այնուամենայնիվ, դրանք չեն կարող համարվել հատուկ կատեգորիայի անձնական տվյալներ մշակող կենսաչափական համակարգեր՝ պայմանով, որ դրանք նպատակաուղղված չեն անձի եզակի նույնականացմանը, և որ անձնական տվյալների մշակումը չի ներառում այլ հատուկ կատեգորիայի անձնական տվյալներ: Այս օրինակները որոշ չափով առնչություն ունեն դեմքի ճանաչման հետ և ուստի կարգավորվում են անձնական տվյալների պաշտպանության կանոններով:[4] Ավելին, հայտնաբերման նմանատիպ համակարգը կարող է կիրառվել այլ համակարգերի հետ միասին, որոնք

ուղղված են անձի նույնականացմանը և ուստի համարվում են դեմքի ճանաչման տեխնոլոգիա:

15. Ի տարբերություն տեսանկարահանման և մշակման համակարգերի, որոնք, օրինակ՝ պահանջում են ֆիզիկական սարքերի տեղադրում, դեմքի ճանաչումը ծրագրային ապահովման ֆունկցիոնալություն է, որը կարող է ներդրվել գոյություն ունեցող համակարգերում (տեսախցիկներում, պատկերների շտեմարանում և այլն): Հետևաբար, այդ ֆունկցիոնալությունը կարող է միացվել կամ փոխկապակցվել բազմաթիվ համակարգերի հետ և զուգակցվել այլ ֆունկցիոնալությունների հետ: Վերջիններիս ինտեգրումն արդեն գոյություն ունեցող ենթակառուցվածքին պահանջում է հատուկ ուշադրություն, քանի որ այն պարունակում է ներհատուկ ռիսկեր՝ կապված այն փաստի հետ, որ դեմքի ճանաչման տեխնոլոգիան կարող է լինել պարզ և հեշտությամբ թաքցվել[5]:

2.2 Տարատեսակ նպատակները և կիրառությունները

16. Այս ուղեցույցի և ԻԿՀ շրջանակներից դուրս դեմքի ճանաչումը կարող է կիրառվել տարատեսակ այլ նպատակներով՝ ինչպես առևտրային օգտագործման, այնպես էլ հանրային անվտանգության կամ իրավապահ գործունեության ոլորտում խնդիրների լուծման համար: Այն կարող է կիրառվել տարբեր համատեքստերում՝ օգտատիրոջ և ծառայության միջև անձնական հարաբերություններում (հավելվածին հասանելիություն), կոնկրետ վայր մուտք գործելու համար (ֆիզիկական զտում) կամ հանրային տարածքում առանց որևէ հատուկ սահմանափակման (ուղիղ ժամանակային ռեժիմում դեմքի ճանաչում): Այն կարող է կիրառվել ցանկացած տեսակի տվյալների սուբյեկտի՝ ծառայության հաճախորդի, աշխատողի, հասարակ դիտորդի, հետախուզվող անձի կամ իրավական կամ վարչական վարույթի մասնակից որևէ անձի և այլոց նկատմամբ: Որոշ կիրառություններ արդեն սովորական և տարածված են. մյուսներն այս պահին գտնվում են փորձարկման կամ քննարկման փուլում: Թեև այս ուղեցույցի շրջանակներում անդրադարձ չի կատարվի բոլոր այդ կիրառություններին, այնուամենայնիվ, ՏՊԵԽ-ը հիշեցնում է, որ դրանք կարող են ներդրվել միայն, եթե համապատասխանում են կիրառելի իրավական շրջանակին և, մասնավորապես, ՏՊԸԿ-ին և համապատասխան ազգային օրենքներին:[6] Նույնիսկ ԻԿՀ համատեքստում, բացի իսկորոշման կամ նույնականացման ֆունկցիաներից, դեմքի ճանաչման տեխնոլոգիայի կիրառմամբ մշակված տվյալները կարող են նաև մշակվել այլ նպատակներով, օրինակ՝ դասակարգման համար:

[4] Այնուամենայնիվ, ԻԿՀ 10-րդ հոդվածը (կամ ՏՊԸԿ 9-րդ հոդվածը) կիրառելի է այն համակարգերի նկատմամբ, որոնք կիրառվում են անձանց՝ կենսաչափական տվյալների հիման վրա ըստ խմբերի դասակարգելու համար՝ ելնելով էթնիկ պատկանելությունից, ինչպես նաև քաղաքական կամ սեռական կողմնորոշումից կամ այլ հատուկ կատեգորիայի անձնական տվյալներից:

[5] Օրինակ՝ մարմնին ամրացված տեսախցիկներ, որոնք գործնականում գնալով էլ ավելի մեծ կիրառություն են ստանում:

[6] Լրացուցիչ ուղղորդման համար տե՛ս նաև Տեսանկարահանող սարքերի միջոցով անձնական տվյալների մշակման վերաբերյալ ՏՊԵԽ-ի 2020 թվականի հունվարի 29-ին ընդունված 3/2019 ուղեցույցը:

17. Առավել կոնկրետ, կարող է դիտարկվել պոտենցիալ կիրառությունների մասշտաբը՝ կախված մարդկանց կողմից իրենց անձնական տվյալների նկատմամբ հսկողության աստիճանից, այդ հսկողության իրականացման համար ունեցած արդյունավետ միջոցներից և այդ տեխնոլոգիան գործարկելու ու կիրառելու նախաձեռնության իրավունքից, դրանց հետևանքներից (ճանաչման կամ չճանաչման դեպքում) և իրականացված մշակման մասշտաբներից: Այդ անձին պատկանող անձնական սարքում (սմարթ քարտում, սմարթֆոնում և այլ սարքում) պահված մոդելի հիման վրա դեմքի ճանաչումը, որն օգտագործվում է իսկորոշման և հատուկ ինտերֆեյսի միջոցով խիստ անձնական օգտագործման համար, չի ներկայացնում նույն ռիսկերը, ինչ, օրինակ՝ նույնականացման նպատակներով օգտագործումը՝ չվերահսկվող միջավայրում, առանց տվյալների սուբյեկտների ակտիվ ներգրավվածության, որտեղ տեսահսկվող տարածք մուտք գործող յուրաքանչյուր դեմքի մոդելը համեմատվում է տվյալների շտեմարանում պահվող բնակչության լայն շրջանակի մոդելի հետ: Այս երկու ծայրահեղությունների միջև ընկած է կիրառության շատ բազմազան շրջանակ և անձնական տվյալների պաշտպանության հետ կապված հարակից խնդիրներ:

18. Լրացուցիչ ուսումնասիրելու համար այն համատեքստը, որի շրջանակներում ներկայումս քննարկվում կամ ներդրվում են դեմքի ճանաչման տեխնոլոգիաները՝ իսկորոշման կամ նույնականացման համար, ՏՊԵԽ-ը տեղին է համարում բերել մի շարք օրինակներ: Ստորև ներկայացված օրինակները բացառապես նկարագրական են և չպետք է դիտարկվեն դրանց՝ տվյալների պաշտպանության ոլորտում ԵՄ ընդհանուր օրենսդրության հետ համապատասխանության որևէ նախնական գնահատում:

<u>Դեմքի ճանաչման միջոցով իսկորոշման օրինակները</u>

19. Իսկորոշումը կարող է այնպես մշակված լինել, որ օգտատերերը լիակատար հսկողություն ունենան դրա նկատմամբ, օրինակ, որպեսզի կարողանան օգտվել ծառայություններից կամ հավելվածներից բացառապես տան պայմաններում: Որպես այդպիսին, այն լայնորեն կիրառվում է սմարթֆոնների սեփականատերերի կողմից՝ իրենց սարքն ապակողպելու համար՝ գաղտնաբառով իսկորոշման փոխարեն:

20. Դեմքի ճանաչման միջոցով իսկորոշումը կարող է նաև օգտագործվել այն անձի ինքնությունը ստուգելու համար, որն ակնկալում է օգտվել պետական կամ մասնավոր երրորդ անձի ծառայություններից: Այդպիսով, այդ պրոցեսներն առաջարկում են թվային ինքնություն ստեղծելու միջոց՝ օգտագործելով բջջային հավելվածը (սմարթֆոնը, պլանշետը և այլն), որն այնուհետ կարող է օգտագործվել առցանց վարչական ծառայություններից օգտվելու համար:

21. Ավելին, դեմքի ճանաչման միջոցով իսկորոշումը կարող է ուղղված լինել մեկ կամ մի քանի նախապես որոշված վայրեր ֆիզիկական մուտքը, օրինակ՝ շենքերի մուտքեր կամ հատուկ անցման կետեր մուտք գործելը հսկելուն: Այս ֆունկցիոնալությունը, օրինակ՝ կիրառվում է սահմանը հատելու նպատակով իրականացվող որոշ մշակման գործողություններում, որտեղ անցակետի սարքի վրա պատկերված անձի դեմքը համեմատվում է նրա անձը հաստատող փաստաթղթի (անձնագրի կամ անվտանգ կացության թույլտվության) վրա առկա անձի դեմքի հետ:

Դեմքի ճանաչման միջոցով նույնականացման օրինակները

22. Նույնականացումը կարող է կիրառվել շատ, նույնիսկ ավելի բազմազան ձևերով: Դրանք մասնավորապես ներառում են ստորև թվարկված՝ ներկայումս ԵՄ-ում դիտարկվող, փորձարկվող կամ պլանավորվող կիրառությունները, սակայն չեն սահմանափակվում դրանցով.

- լուսանկարների շտեմարանում ինքնությունը չպարզված անձի (տուժածի, կասկածյալի և այլ անձանց) ինքնության որոնում.
- հանրային տարածքում անձի տեղաշարժերի մշտադիտարկում: Նրա դեմքը համեմատվում է տեսահսկվող տարածքով անցած կամ անցնող մարդկանց կենսաչափական մոդելների հետ, օրինակ, երբ անձը թողնում է ուղերեռի մի կտորը, կամ երբ կատարվում է հանցագործություն.
- անձի ճամփորդության և այլ անձանց հետ նրա հետագա փոխգործակցությունների վերականգնում՝ նույն տարրերի ձգձգված համեմատության միջոցով, օրինակ՝ նրա շփումները պարզելու նպատակով.
- հանրային տարածքներում հետախուզվող անձանց հեռավար կենսաչափական նույնականացում: Ուղիղ ժամանակային ռեժիմում տեսապաշտպան տեսախցիկներով նկարահանված բոլոր դեմքերն իրական ժամանակում ստուգվում են անվտանգության ծառայության կողմից պահվող տվյալների շտեմարանի հետ.
- պատկերի վրա երևացող մարդկանց ավտոմատ ճանաչում, օրինակ՝ պարզելու համար այն սոցիալական ցանցում նրանց կապը, որն օգտագործում է այն: Պատկերը համեմատվում է ցանցում առկա բոլոր այն մարդկանց մոդելների հետ, որոնք համաձայնել են կիրառել այդ ֆունկցիոնալությանը՝ այդ կապի անվանական նույնականացումն առաջարկելու համար.
- հասանելիություն ծառայություններին, երբ որոշ բանկոմատներ ճանաչում են իրենց հաճախորդներին՝ համեմատելով տեսախցիկի կողմից նկարահանված դեմքը բանկի կողմից պահվող դեմքի պատկերների շտեմարանի հետ.
- ուղևորի ճամփորդության հետագծելիություն ճամփորդության որոշ փուլում: Իրական ժամանակում հաշվարկված՝ ճամփորդության որոշ փուլերում՝ նստեցման ելքերում գրանցված ցանկացած անձի դեմքի մոդելը համեմատվում է համակարգում արդեն իսկ գրանցված մարդկանց դեմքի մոդելի հետ:

23. Ի լրումն իրավապահ գործունեության ոլորտում ԴՃՏ-ի կիրառմանը, դիտարկված կիրառությունների մեծ մասը, անշուշտ, պահանջում է համապարփակ քննարկում և քաղաքական մոտեցում՝ տվյալների պաշտպանության ոլորտում ԵՄ ընդհանուր օրենսդրության հետ հետևողականություն և համապատասխանություն ապահովելու համար:

2.3 Տվյալների սուբյեկտների համար հուսալիությունը, ճշտությունը և ռիսկերը

24. Ինչպես յուրաքանչյուր տեխնոլոգիա, այնպես էլ դեմքի ճանաչման տեխնոլոգիան կարող է ունենալ խնդիրներ, երբ խոսքը վերաբերում է դրա ներդրմանը, մասնավորապես, իսկորոշման կամ նույնականացման տեսանկյունից դրա հուսալիությանն ու արդյունավետությանը, ինչպես նաև տվյալների «աղբյուրի» որակի ու ճշտության և դեմքի ճանաչման տեխնոլոգիայի մշակման արդյունքի ընդհանուր խնդրին:

25. Այդ տեխնոլոգիական մարտահրավերները կոնկրետ ռիսկեր են պարունակում համապատասխան տվյալների սուբյեկտների համար, որոնք առավել զգալի կամ լուրջ են իրավապահ գործունեության ոլորտում՝ հաշվի առնելով տվյալների սուբյեկտների համար հնարավոր՝ կա՛մ իրավական, կա՛մ մյուս հետևանքները, որոնք նույն կերպ զգալի ազդեցություն են ունենում նրանց վրա: Այս համատեքստում օգտակար է նաև ընդգծել, որ ԴՀՏ-ի փաստացի կիրառումն ինքնին ավելի անվտանգ չէ, քանի որ մարդիկ կարող են վերահսկվել ժամանակի մեջ և վայրերում: Այսպիսով, փաստացի կիրառումը նույնպես հատուկ ռիսկեր է պարունակում, որոնք պետք է գնահատվեն յուրաքանչյուր դեպքի հիման վրա:[7]

26. Ինչպես նշել է Հիմնարար իրավունքների հարցերով ԵՄ գործակալությունն իր 2019 թվականի զեկույցում, «դժվար է որոշել դեմքերը ճանաչող ծրագրային ապահովման ճշտության անհրաժեշտ մակարդակը. կան ճշտությանը գնահատական տալու և գնահատելու բազմաթիվ տարբեր եղանակներ՝ կախված նաև դրա կիրառման առաջադրանքից, նպատակից և համատեքստից: Երբ տեխնոլոգիան կիրառվում է միլիոնավոր մարդկանց կողմից այցելվող վայրերում, ինչպիսիք են երկաթուղային կայարանները կամ օդանավակայանները, սխալների համեմատաբար փոքր մասնաբաժինը (օրինակ՝ 0,01 տոկոսը)[8] դեռ նշանակում է, որ հարյուրավոր մարդիկ սխալ են նշվում: Բացի այդ, որոշ կատեգորիայի մարդկանց մոդելները կարող են սխալմամբ համընկնել, քան մյուսները, ինչպես նկարագրված է 3-րդ բաժնում: Գոյություն ունեն սխալների տոկոսը հաշվարկելու և մեկնաբանելու տարբեր եղանակներ, ուստի անհրաժեշտ է ցուցաբերել զգուշավորություն: Բացի այդ, երբ խոսքը վերաբերում է ճշտությանն ու սխալներին, հարցերը, թե ինչպես կարելի է հեշտությամբ խաբել համակարգին, օրինակ՝ կեղծ դեմքի պատկերներով (այսպես կոչված «սփուֆինգ») կարևոր են հատկապես իրավապահ նպատակներով»:[9]

[7] Տե՛ս III հավելվածում ներկայացված օրինակները:

[8] Ճշտության այս ցուցանիշը վերցված է մեջբերված զեկույցից և ավելի բարձր է, քան դեմքի ճանաչման տեխնոլոգիայի կիրառություններում ալգորիթմների ներկայիս արտադրողականությունը:

[9] Դեմքի ճանաչման տեխնոլոգիա. հիմնարար իրավունքների նկատառումներն իրավապահ գործունեության համատեքստում, Հիմնարար իրավունքների հարցերով ԵՄ գործակալություն, 2019 թվականի նոյեմբերի 21:

27. Այս համատեքստում ՏՊԵԽ-ը կարևոր է համարում հիշել, որ ԴՃՏ-ն, անկախ այն փաստից՝ օգտագործվում է իսկորոշման, թե նույնականացման նպատակով, չի ապահովում վերջնական արդյունք, այլ հիմնված է հավանականությունների վրա, որ երկու դեմքերը կամ դեմքերի պատկերները համապատասխանում են նույն մարդուն:[10] Այդ արդյունքն էլ ավելի է վատանում, երբ դեմքի ճանաչման համակարգ ներածված կենսաչափական նմուշի որակը ցածր է: Ներածված պատկերների մշուշոտությունը, տեսախցիկի ցածր լուծաչափը, շարժումը և թույլ լույսը կարող են հանդիսանալ ցածր որակի գործոններ: Արդյունքների վրա զգալի ազդեցություն ունեցող մյուս հայեցակետերը տարածվածությունը և սփուֆինգն են, օրինակ, երբ հանցագործները փորձում են կա՛մ խուսափել տեսախցիկների կողքով անցնելուց կամ խաբել ԴՃՏ-ին: Բազմաթիվ ուսումնասիրությունները նույնպես ցույց են տվել, որ ալգորիթմական մշակման այդ վիճակագրական արդյունքները կարող են նաև կողմնակալություն պարունակել, հատկապես կապված աղբյուրի տվյալների որակի, ինչպես նաև ուսուցման տվյալների շտեմարանների կամ այլ գործոնների, ինչպիսիք են գործարկման վայրի ընտրության հետ: Ավելին, պետք է նաև ընդգծել դեմքի ճանաչման տեխնոլոգիայի ազդեցությունն այլ հիմնարար իրավունքների վրա, ինչպիսիք են անձնական և ընտանեկան կյանքի նկատմամբ հարգանքը, արտահայտվելու և տեղեկատվության ազատությունը, հավաքների և միավորումներ կազմելու ազատությունը և այլն:

28. Հետևաբար, կարևոր է, որ դեմքի ճանաչման տեխնոլոգիայի հուսալիությունն ու ճշտությունը հաշվի առնվեն որպես տվյալների պաշտպանության հիմնական սկզբունքներին համապատասխանության գնահատման չափորոշիչներ՝ ԻԿՀ 4-րդ հոդվածի համաձայն, և հատկապես, երբ խոսքը վերաբերում է արդարությանն ու ճշտությանը:

29. Ընդգծելով, որ բարձրորակ տվյալները էական նշանակություն ունեն բարձրորակ ալգորիթմների համար, ՏՊԵԽ-ը նաև ընդգծում է, որ տվյալների հսկողները, որպես իրենց հաշվետվողականության պարտավորության մաս, պետք է ձեռնարկեն ալգորիթմական մշակման կանոնավոր և համակարգված գնահատում՝ մասնավորապես, այդ անձնական տվյալների մշակման արդյունքի ճշտությունը, արդարությունն ու հուսալիությունն ապահովելու համար: ԴՃՏ համակարգերի գնահատման, ուսուցման և հետագա զարգացման նպատակով օգտագործվող անձնական տվյալները կարող են մշակվել միայն բավարար իրավական հիմքի հիման վրա և տվյալների պաշտպանության ընդհանուր սկզբունքներին համապատասխան:

[10] Այս հավանականությունը կոչվում է «վստահության գնահատական»:

3 ԿԻՐԱՌԵԼԻ ԻՐԱՎԱԿԱՆ ՇՐՋԱՆԱԿԸ

30. Դեմքի ճանաչման տեխնոլոգիաների կիրառումն անքակտելիորեն կապված է անձնական տվյալների, այդ թվում՝ հատուկ կատեգորիայի տվյալների մշակման հետ: Ավելին, այն ուղղակի կամ անուղղակի ազդեցություն ունի Հիմնարար իրավունքների ԵՄ խարտիայում ամրագրված մի շարք հիմնարար իրավունքների վրա: Դա հատկապես արդիական է իրավապահ գործունեության և քրեական արդարադատության ոլորտներում: Հետևաբար, դեմքի ճանաչման տեխնոլոգիաների ցանկացած կիրառում պետք է իրականացվի կիրառելի իրավական շրջանակի խիստ պահպանմամբ:

31. Հետևյալ տեղեկությունները նախատեսված են հետագա օրենսդրական և վարչական միջոցները գնահատելիս, ինչպես նաև ԴՃՏ-ն ներառող յուրաքանչյուր դեպքում գործող օրենսդրությունը կիրառելիս հաշվի առնելու համար: Համապատասխան պահանջների արդիականությունը տարբերվում է՝ ըստ կոնկրետ հանգամանքների:Քանի որ հնարավոր չէ կանխատեսվել բոլոր ապագա հանգամանքները, այն համարվում է միայն աջակցության տրամադրում և չպետք է մեկնաբանվի որպես սպառիչ թվարկում:

3.1 Ընդհանուր իրավական շրջանակ. Հիմնարար իրավունքների ԵՄ խարտիա և Մարդու իրավունքների եվրոպական կոնվենցիա (ՄԻԵԿ)

3.1.1 Խարտիայի կիրառելիությունը

32. Հիմնարար իրավունքների ԵՄ խարտիան (այսուհետ՝ Խարտիա) հասցեագրված է Միության ինստիտուտներին, մարմիններին, գրասենյակներին ու գործակալություններին, ինչպես նաև անդամ պետություններին, երբ դրանք իրականացնում են Միության իրավունքը:

33. ԻԿՀ 1(1) հոդվածի համաձայն՝ իրավապահ նպատակով կենսաչափական տվյալների մշակման կարգավորումն անխուսափելիորեն վերհանում է հիմնարար իրավունքների, մասնավորապես՝ Խարտիայի 7-րդ հոդվածի համաձայն՝ անձնական կյանքի և նամակագրության նկատմամբ հարգանքի ու Խարտիայի 8-րդ հոդվածի համաձայն՝ անձնական տվյալների պաշտպանության իրավունքի հետ համապատասխանության հարցը:

34. Ֆիզիկական անձանց, այդ թվում՝ նրանց դեմքերի տեսանյութերի հավաքումն ու վերլուծությունը ենթադրում է անձնական տվյալների մշակում: Պատկերը տեխնիկապես մշակելիս այն ներառում է նաև կենսաչափական տվյալները: Ժամանակից և վայրից կախված ֆիզիկական անձի դեմքին վերաբերող տվյալների տեխնիկական մշակումը թույլ է տալիս եզրակացություններ կատարել համապատասխան անձանց մասնավոր կյանքի մասին: Այդ եզրակացությունները կարող են վերաբերել ռասայական կամ էթնիկ ծագմանը, առողջությանը, կրոնին, առօրյա կյանքի սովորություններին, մշտական կամ ժամանակավոր բնակության վայրերին, ամենօրյա կամ այլ տեղաշարժերին, իրականացվող գործունեություններին, այդ անձանց սոցիալական հարաբերություններին և նրանց կողմից հաճախակի այցելվող սոցիալական միջավայրերին: Տեղեկությունների մեծ շրջանակը, որը կարող է բացահայտվել ԴՃՏ-ի կիրառմամբ, հստակ ցույց է տալիս Խարտիայի 8-րդ հոդվածով սահմանված անձնական տվյալների պաշտպանության իրավունքի, ինչպես նաև Խարտիայի 7-րդ հոդվածով սահմանված անձնական կյանքի անձեռնմխելիության իրավունքի վրա հնարավոր ազդեցությունը:

35. Նման դեպքերում միանգամայն հնարավոր է նաև, որ խնդրո առարկա կենսաչափական (դեմքի) տվյալների հավաքումը, վերլուծությունը և հետագա մշակումը կարող են ներազդել

մարդկանց ազատ գործունեության վրա, նույնիսկ եթե դա լիովին գտնվում է ազատ ու բաց հասարակության պատասխանատվության շրջանակում: Դա կարող է նաև լուրջ հետևանքներ ունենալ նրանց հիմնարար իրավունքների, ինչպիսիք են նրանց՝ մտքի, խղճի և կրոնի ազատության, խաղաղ հավաքների ազատության և միավորումներ կազմելու ազատության իրավունքների իրացման վրա՝ Խարտիայի 1-ին, 10-րդ, 11-րդ և 12-րդ հոդվածների համաձայն: Այդ մշակումը ներառում է նաև այլ ռիսկեր, ինչպիսիք են անձնական տվյալներին անօրինական ճանապարհով հասանելիություն ստանալու և օգտագործելու, ինչպես նաև անվտանգության խախտման և այլնի արդյունքում համապատասխան մարմինների կողմից հավաքված անձնական տվյալների սխալ օգտագործման ռիսկը: Ռիսկերը հաճախ կախված են մշակումից և դրա հանգամանքներից, օրինակ՝ ոստիկանության ծառայողների կամ այլ չարտոնված անձանց կողմից անօրինական ճանապարհով հասանելիության և օգտագործման ռիսկից: Այնուամենայնիվ, որոշ ռիսկեր պարզապես ներհատուկ են կենսաչափական տվյալների եզակի բնույթին: Բացի հասցեից կամ հեռախոսահամարից, տվյալների սուբյեկտը չի կարող փոխել իր եզակի հատկությունները, ինչպիսիք են՝ դեմքը կամ ծիածանաթաղանթը: Կենսաչափական տվյալների չարտոնված հասանելիության կամ պատահական հրապարակման դեպքում դա կհանգեցնի նրան, որ տվյալները չեն կարող օգտագործվել որպես գաղտնաբառեր կամ կրիպտոգրաֆիկական բանալիներ կամ կարող են օգտագործվել հետագա, չարտոնված վերահսկման գործողությունների համար՝ ի վնաս տվյալների սուբյեկտի:

3.1.2 Միջամտությունը Խարտիայով սահմանված իրավունքներին

36. Բոլոր դեպքերում կենսաչափական տվյալների մշակումն ինքնին լուրջ միջամտություն է: Սա կախված չէ արդյունքից, օրինակ՝ դրական համընկնումից: Մշակումը համարվում է միջամտություն, նույնիսկ եթե կենսաչափական մոդելն անմիջապես ջնջվում է, երբ ոստիկանության տվյալների շտեմարանի հետ համընկնումը չի հանգեցնում արդյունքների:

37. Տվյալների սուբյեկտների հիմնարար իրավունքներին միջամտությունը կարող է բխել իրավունքի գործողությունից, որը կա՛մ նպատակ ունի կա՛մ կարող է սահմանափակել համապատասխան հիմնարար իրավունքը[11]: Այն կարող է բխել նաև նույն նպատակով կամ հետևանքով պետական մարմնի կամ նույնիսկ օրենքով պետական իշխանություն և հանրային լիազորություններ իրականացնելու իրավասությամբ օժտված մասնավոր սուբյեկտի գործողությունից:

38. Օրենսդրական միջոցը, որը հանդիսանում է իրավական հիմք անձնական տվյալների մշակման համար, ուղղակիորեն միջամտում է Խարտիայի 7-րդ և 8-րդ հոդվածներով երաշխավորված իրավունքներին[12]:

39. Շատ դեպքերում կենսաչափական տվյալների և մասնավորապես ԴՃՏ-ի կիրառումը նույնպես ազդում է Խարտիայի 1-ին հոդվածով երաշխավորված մարդու արժանապատվության իրավունքի վրա: Մարդու արժանապատվությունը պահանջում է, որ անձանց չպետք է վերաբերվել զուտ որպես օբյեկտ: ԴՃՏ-ն էկզիստենցիալ և խիստ անհատական հատկանիշները, դեմքի առանձնահատկությունները վերածում է մեքենայաընթեռնելի ձևի, որպեսզի այն օգտագործի որպես մարդու համարանիշ կամ նույնականացման քարտ՝ դրանով իսկ առարկայացնելով դեմքը:

40. Այդ մշակումը կարող է միջամտել նաև այլ հիմնարար իրավունքներին, ինչպիսիք են Խարտիայի 10-րդ, 11-րդ և 12-րդ հոդվածներով նախատեսված իրավունքները, քանի որ զսպող ազդեցությունները կա՛մ նախատեսված են կա՛մ առաջանում են իրավապահ մարմինների կողմից իրականացվող համապատասխան տեսահսկումից:

41. Բացի այդ, անհրաժեշտ է մանրամասն դիտարկել նաև Խարտիայի 47-րդ և 48-րդ

հոդվածների համաձայն՝ արդար դատաքննության իրավունքի և անմեղության կանխավարկածի առնչությամբ իրավապահ մարմինների կողմից դեմքի ճանաչման տեխնոլոգիաների կիրառման արդյունքում առաջացած հնարավոր ռիսկերը: ԴՃՏ-ի կիրառման արդյունքը, օրինակ՝ համընկնումը, կարող է ոչ միայն հանգեցնել նրան, որ անձը հետագայում ոստիկանության կողմից ենթարկվի հսկողության, այլ նաև վճռորոշ ապացույց հանդիսանա դատական վարույթում: ԴՃՏ-ի թերությունները, ինչպիսիք են հնարավոր կողմնակալությունը, խտրականությունը կամ սխալ նույնականացումը («կեղծ դրական»), այսպիսով, կարող են լուրջ հետևանքներ ունենալ նաև քրեական վարույթի վրա: Ավելին, ապացույցների գնահատման ժամանակ ԴՃՏ-ի կիրառման արդյունքը կարող է բարենպաստ լինել, նույնիսկ եթե կան հակասական ապացույցներ («ավտոմատացման կողմնակալություն»):

3.1.3 Միջամտության հիմնավորումը

42. Խարտիայի 52(1) հոդվածի համաձայն՝ հիմնարար իրավունքների ու ազատությունների իրացման ցանկացած սահմանափակում պետք է նախատեսված լինի օրենքով և հարգի այդ իրավունքների ու ազատությունների էությունը: Ելնելով համաչափության սկզբունքից՝ սահմանափակումները կարող են կիրառվել միայն այն դեպքում, եթե դրանք անհրաժեշտ են և իսկապես համապատասխանում են Եվրոպական միության կողմից ճանաչված ընդհանուր շահերի կամ այլ անձանց իրավունքների ու ազատությունների պաշտպանության անհրաժեշտության նպատակներին:

3.1.3.1 Օրենքով նախատեսված լինելը

43. Խարտիայի 52(1) հոդվածով սահմանվում է կոնկրետ իրավական հիմքի նկատմամբ պահանջ: Այդ իրավական հիմքը պետք է բավականաչափ հստակ ձևակերպված լինի, որպեսզի քաղաքացիները բավարար պատկերացում ունենան այն պայմանների և հանգամանքների մասին, որոնց դեպքում մարմիններն իրավասու են դիմելու տվյալների հավաքագրման ու գաղտնի հսկողության ցանկացած միջոցի[13]: Դրանով պետք է ողջամիտ հստակությամբ նշվեն պետական մարմիններին տրված համապատասխան հայեցողության շրջանակը և կիրառման եղանակը, որպեսզի մարդիկ ապահովվեն ժողովրդավարական հասարակությունում օրենքի գերակայությամբ նախատեսված նվազագույն պաշտպանությամբ[14]: Ավելին, օրինականությունը պահանջվում է համապատասխան երաշխիքներ, որոնցով ապահովվում են, որ մասնավորապես անձի՝ Խարտիայի 8-րդ հոդվածով նախատեսված իրավունքները հարգվեն: Այս սկզբունքները կիրառվում են նաև անձնական տվյալների մշակման նկատմամբ՝ ԴՃՏ համակարգերի գնահատման, ուսուցման և հետագա զարգացման նպատակով:

---

[11] ԵՄԱԴ, գործ թիվ C-219/91, *Տեր Վուուրտ* [Ter Voort], RoC 1992 I-05485, պարբերություն 36q, ԵՄԱԴ, գործ թիվ C-200/96, *Մետրոնոմ* [Metronome], RoC 1998 I-1953, պարբերություն 28:

[12] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 36, ԵՄԱԴ, գործ թիվ C-291/12, պարբերություն 23 և հետևյալը:

[13] ՄԻԵԴ, *Շիմովոլոսն ընդդեմ Ռուսաստանի գործ* [Shimovolos v. Russia], պարբերություն 68, *Վուկոտա Բոյիչն ընդդեմ Շվեյցարիայի գործ* [Vukota-Bojić v. Switzerland]:

[14] ՄԻԵԴ, *Պիեխովիչն ընդդեմ Լեհաստանի գործ* [Piechowicz v. Poland], պարբերություն 212:

44. Հաշվի առնելով այն հանգամանքը, որ ֆիզիկական անձի եզակի նույնականացման նպատակով մշակվող կենսաչափական տվյալները կազմում են ԻԿՀ 10-րդ հոդվածով թվարկված հատուկ կատեգորիայի տվյալները, ԴՀՏ-ի տարբեր կիրառությունները շատ դեպքերում կպահանջեն հատուկ օրենք, որը ճշգրիտ կնկարագրի կիրառությունը և դրա կիրառման պայմանները: Դրա մեջ մտնում են, մասնավորապես, հանցագործության տեսակները և, հարկ եղած դեպքում, այդ հանցագործությունների ծանրության համապատասխան շեմը, որպեսզի, ի թիվս այլնի, արդյունավետորեն բացառվեն ոչ մեծ հանցագործությունները:[15]

3.1.3.2 Խարտիայի 7-րդ և 8-րդ հոդվածներով սահմանված անձնական կյանքի անձեռնմխելիության և անձնական տվյալների պաշտպանության հիմնարար իրավունքի էությունը

45. Յուրաքանչյուր իրավիճակի համար անխուսափելի հիմնարար իրավունքների սահմանափակումներն այդուհանդերձ պետք է հաշվի առնեն այն կոնկրետ իրավունքի էությունը, որը պետք է հարգվի: Էությունը վերաբերում է համապատասխան հիմնարար իրավունքի բուն էությանը[16]: Մարդու արժանապատվությունը նույնպես պետք է հարգվի, նույնիսկ եթե իրավունքը սահմանափակված է[17]:

46. Անձեռնմխելի էության հնարավոր խախտման նշաններն են.

- դրույթ, որով սահմանափակումներ են կիրառվում՝ անկախ անձի վարքագծից կամ հատուկ հանգամանքներից[18].
- դատարաններ դիմելու հնարավորությունը բացակայում է կամ խոչընդոտված է[19].
- մինչև խիստ սահմանափակումը, տվյալ անձի հանգամանքներն անտեսված են[20].
- Խարտիայի 7-րդ և 8-րդ հոդվածներով նախատեսված իրավունքների հաշվառմամբ՝ մեծ թվով հաղորդակցության մետատվյալներ հավաքագրելուց բացի՝ էլեկտրոնային հաղորդակցության բովանդակության մասին տեղեկությունների ձեռքբերումը կարող է խախտել այդ իրավունքների էությունը[21].
- Խարտիայի 7-րդ, 8-րդ և 11-րդ հոդվածներով նախատեսված իրավունքների հաշվառմամբ՝ օրենսդրություն, որը պահանջում է, որ հանրային հաղորդակցության առցանց ծառայությունների հասանելիություն մատուցողները և հոսթինգ ծառայություններ մատուցողները, ընդհանուր առմամբ և առանց խտրականության, ի թիվս այլնի, պահպանեն այդ ծառայությունների հետ կապված անձնական տվյալները[22].
- Խարտիայի 8-րդ հոդվածով նախատեսված իրավունքների առնչությամբ. տվյալների պաշտպանության և տվյալների անվտանգության հիմնական սկզբունքների բացակայությունը կարող է նաև խախտել իրավունքի էությունը[23]:

[15] Տե՛ս օր.՝ Մարդու իրավունքների լիգայի թիվ C-817/19 գործերով ԵՄԱԴ-ի կողմից կայացված վճիռները, պարբերություն 151 զ, գործ թիվ C-207/16, Ministerio Fiscal, պարբերություն 56:
[16] ԵՄԱԴ, գործ թիվ C-279/09, RoC 2010 I-13849, պարբերություն 60:
[17] Հիմնարար իրավունքների խարտիայի հետ կապված բացատրություններ, բաժին I, 1-ին հոդվածի բացատրություն, ՊՏ C 303, 2007 թվականի դեկտեմբերի 14, էջեր 17-35:
[18] ԵՄԱԴ, գործ թիվ C-601/15, պարբերություն 52:
[19] ԵՄԱԴ, գործ թիվ C-400/10, RoC 2010 I-08965, պարբերություն 55:
[20] ԵՄԱԴ, գործ թիվ C-408/03, RoC 2006 I-02647, պարբերություն 68:
[21] ԵՄԱԴ, գործ թիվ 203/15, Tele2 Sverige, պարբերություն 101, ԵՄԱԴ, թիվ C-293/12 և թիվ C-594/12 գործերին հղմամբ, պարբերություն 39:
[22] ԵՄԱԴ, գործ թիվ C-512/18, La Quadrature du Net, պարբերություն 209 և հաջորդող պարբերություններ:
[23] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 40:

3.1.3.3 Իրավաչափ նպատակը

47. Ինչպես արդեն ներկայացվել է 3.1.3 կետում, հիմնարար իրավունքների սահմանափակումները պետք է իսկապես համապատասխանեն Եվրոպական միության կողմից ճանաչված ընդհանուր շահերի նպատակներին կամ այլ անձանց իրավունքների ու ազատությունների պաշտպանության անհրաժեշտությանը:

48. Միությունը ճանաչում է ինչպես «Եվրոպական միության մասին» պայմանագրի 3-րդ հոդվածում նշված նպատակները, այնպես էլ Պայմանագրերի[24] հատուկ դրույթներով պաշտպանված մյուս շահերը, օրինակ՝ ի թիվս այլնի՝ ազատության, անվտանգության և արդարադատության տարածքը, հանցագործության կանխման և դրա դեմ պայքարը: Արտաքին աշխարհի հետ հարաբերություններում Միությունը պետք է նպաստի խաղաղությանն ու անվտանգությանը և մարդու իրավունքների պաշտպանությանը:

49. Այլ անձանց իրավունքների ու ազատությունների պաշտպանության անհրաժեշտությունը վերաբերում է այն անձանց իրավունքներին, որոնք պաշտպանված են Եվրոպական միության կամ նրա անդամ պետությունների իրավունքով: Գնահատումը պետք է իրականացվի համապատասխան իրավունքների պաշտպանության պահանջները համադրելու և դրանց միջև արդար հավասարակշռություն ստեղծելու նպատակով[25]:

3.1.3.4 Անհրաժեշտության և համաչափության ստուգումը

50. Եթե խոսքը գնում է հիմնարար իրավունքներին միջամտության մասին, ապա ազգային և Միության օրենսդիրների հայեցողության շրջանակը կարող է սահմանափակ լինել: Սա պայմանավորված է մի շարք գործոններով, այդ թվում կախված է համապատասխան ոլորտից, Խարտիայով երաշխավորված տվյալ իրավունքի բնույթից, միջամտության բնույթից ու լրջությունից, ինչպես նաև միջամտությամբ հետապնդվող նպատակից[26]: Կիրառվող օրենսդրական միջոցները պետք է համապատասխան լինեն՝ խնդրո առարկա օրենսդրությամբ հետապնդվող իրավաչափ նպատակներին հասնելու համար: Ավելին, միջոցը չպետք է գերազանցի այն սահմանները, որոնք համարժեք և անհրաժեշտ են՝ այդ նպատակներին հասնելու համար[27]: Ընդհանուր շահի նպատակը, որքան էլ այն հիմնարար լինի, ինքնին չի արդարացնում հիմնարար իրավունքի սահմանափակումը[28]:

---

[24] Հիմնարար իրավունքների խարտիայի հետ կապված բացատրություններ, բաժին I, 52-րդ հոդվածի բացատրություն, ՊՏ C 303, 2007 թվականի դեկտեմբերի 14, էջեր 17-35:

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32:

[26] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 47, հետևյալ աղբյուրներով, տե՛ս անալոգիայով ՄԻԵԿ-ի 8-րդ հոդվածի առնչությամբ Մարդու իրավունքների եվրոպական դատարանի *Ս.-ն և Մարփերն ընդդեմ Միացյալ Թագավորության գործը [ՄՊ]* [S. and Marper v. the United Kingdom [GC]], Գանգատներ թիվ 30562/04 և 30566/04, պարբերություն 102, ՄԻԵԿ 2008-V:

[27] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 46, հետևյալ աղբյուրներով. գործ թիվ C-343/09 Afton Chemical EU:C:2010:419, պարբերություն 45, Volker und Markus Schecke and Eifert EU:C:2010:662, պարբերություն 74, գործեր թիվ C-581/10 և թիվ C-629/10, *Նելսոնը և այլք գործ* [Nelson and Others], EU:C:2012:657, պարբերություն 71, գործ թիվ C-283/11 Sky Österreich EU:C:2013:28, պարբերություն 50, և գործ թիվ C-101/12 Schaible EU:C:2013:661, պարբերություն 29:

[28] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 51:

51. ԵՄԱԴ-ի հաստատված նախադեպային իրավունքի համաձայն՝ անձնական տվյալների պաշտպանության առնչությամբ շեղումները և սահմանափակումները պետք է կիրառվեն միայն, եթե դրանք խիստ անհրաժեշտ են[29]: Սա նաև ենթադրում է, որ չկան նպատակին հասնելու պակաս արմատական միջոցներ: Կախված տվյալ նպատակից՝ հնարավոր այլընտրանքները, ինչպիսիք են լրացուցիչ անձնակազմով համալրումը, ոստիկանության կողմից ավելի հաճախակի իրականացվող հսկողությունը կամ փողոցների լրացուցիչ լուսավորությունը պետք է մանրամասն սահմանվեն և գնահատվեն: Օրենսդրական միջոցներով պետք է տարբերակվեն դրանց գործողության ոլորտում ընդգրկվող անձինք, և պետք է ուղղված լինեն նրանց՝ նպատակի, օրինակ՝ կոնկրետ ծանր հանցագործության դեմ պայքարի լույսի ներքո: Եթե այն ընդհանուր ձևով ընդգրկում է բոլոր անձանց՝ առանց նման տարբերակման, սահմանափակման կամ բացառության, այն սաստկացնում է միջամտությունը[30]: Այն նաև սաստկացնում է միջամտությունը, եթե տվյալների մշակումն ընդգրկում է բնակչության զգալի մասը[31]:

52. Խարտիայի 8(1) հոդվածով սահմանված կոնկրետ պարտավորությունից բխող անձնական տվյալների պաշտպանությունը հատկապես կարևոր է Խարտիայի 7-րդ հոդվածով ամրագրված անձնական կյանքի նկատմամբ հարգանքի իրավունքի առնչությամբ[32]: Օրենսդրությամբ պետք է սահմանվեն խնդրո առարկա միջոցի շրջանակն ու կիրառումը կարգավորող հստակ և ճշգրիտ կանոնները, ինչպես նաև սահմանվեն երաշխիքներ, որպեսզի այն անձինք, որոնց տվյալները մշակվել են, ունենան բավարար երաշխիքներ՝ իրենց անձնական տվյալները սխալ օգտագործման ռիսկից և ցանկացած անօրինական հասանելիությունից կամ օգտագործումից արդյունավետորեն պաշտպանելու համար[33]: Այդ երաշխիքների անհրաժեշտությունն ավելի է մեծանում, երբ անձնական տվյալները ենթարկվում են ավտոմատացված մշակման, և երբ առկա է այդ տվյալներին անօրինական հասանելիության էական ռիսկ[34]: Ավելին, ներքին կամ արտաքին, օրինակ՝ դատական կարգով ԴՀՏ-ի կիրառման թույլտվությունը նույնպես կարող է երաշխիք լինել և կարող է անհրաժեշտ լինել լուրջ միջամտության որոշ դեպքերում:[35]

---

[29] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 52, հետևյալ աղբյուրներով, գործ թիվ C-473/12IPI EU:C:2013:715, պարբերություն 39 և մեջբերված նախադեպային իրավունքը:

[30] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 57:

[31] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 56:

[32] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 53:

[33] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 54, հետևյալ աղբյուրներով, տե՛ս անալոգիայով ՄԻԵԿ-ի 8-րդ հոդվածի առնչությամբ, Մարդու իրավունքների եվրոպական դատարան, *Լիբերթին և այլք ընդդեմ Միացյալ Թագավորության գործ* [Liberty and Others v. the United Kingdom], 2008 թվականի հուլիսի 1, Գանգատ թիվ 58243/00, պարբերություն 62 և 63, *Ռոտարուն ընդդեմ Ռումինիայի գործ* [Rotaru v. Romania], պարբերություն 57-59 և *Մ.-ն և Մարփերն ընդդեմ Միացյալ Թագավորության գործ*, պարբերություն 99:

[34] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 55, հետևյալ աղբյուրներով. տե՛ս անալոգիայով ՄԻԵԿ-ի 8-րդ հոդվածի առնչությամբ Մարդու իրավունքների եվրոպական դատարանի *Մ.-ն և Մարփերն ընդդեմ Միացյալ Թագավորության գործը*, պարբերություն 103 և *Մ.-ն, Կ.-ն ընդդեմ Ֆրանսիայի գործ* [M. K. v. France], 2013 թվականի ապրիլի 18, Գանգատ թիվ 19522/09, պարբերություն 35:

[35] ՄԻԵԴ, *Սաբոն և Վիսսին ընդդեմ Հունգարիայի գործ* [Szabó and Vissy v. Hungary], պարբերություններ 73-77:

53. Սահմանված կանոնները պետք է հարմարեցվեն կոնկրետ իրավիճակին, օրինակ՝ մշակված տվյալների քանակին, տվյալների բնույթին[36] և տվյալներին անօրինական հասանելիության ռիսկին: Սա պահանջում է այնպիսի կանոնների ընդունում, որոնք, մասնավորապես հստակ և խիստ կերպով կկարգավորեն խնդրո առարկա տվյալների պաշտպանությունն ու անվտանգությունը՝ դրանց ամբողջականությունն ու գաղտնիությունն ապահովելու նպատակով[37]:

54. Ինչ վերաբերում է հսկողի և մշակողի միջև հարաբերություններին, մշակողներին չպետք է թույլատրվի անձնական տվյալների նկատմամբ կիրառվող անվտանգության մակարդակը որոշելիս հաշվի առնել միայն տնտեսական նկատառումները. դա կարող է վտանգել պաշտպանության բավական բարձր մակարդակը[38]:

55. Իրավունքի գործողությամբ պետք է սահմանվեն նյութական և դատավարական պայմաններն ու օբյեկտիվ չափանիշները, որոնց միջոցով պետք է որոշվեն իրավասու մարմինների կողմից տվյալներին հասանելիության և դրանց հետագա օգտագործման սահմանները: Կանխման, բացահայտման կամ քրեական հետապնդման նպատակներով համապատասխան իրավախախտումները պետք է համարվեն բավականաչափ լուրջ, որպեսզի հիմնավորվեն, օրինակ՝ Խարտիայի 7-րդ և 8-րդ հոդվածներով ամրագրված հիմնարար իրավունքներին այդ միջամտությունների չափն ու լրջությունը[39]:

56. Տվյալները պետք է մշակվեն այնպես, որպեսզի ապահովվեն տվյալների պաշտպանության ԵՄ, մասնավորապես՝ Խարտիայի 8-րդ հոդվածով նախատեսված կանոնների կիրառելիությունն ու ազդեցությունը, որում նշվում է, որ պաշտպանության և անվտանգության պահանջներին համապատասխանությունը ենթակա է անկախ մարմնի կողմից հսկողության: Աշխարհագրական այն վայրը, որտեղ իրականացվում է մշակումը, այդ իրավիճակում կարող է կարևոր լինել[40]:

57. Ինչ վերաբերում է անձնական տվյալների մշակման տարբեր փուլերին, անհրաժեշտ է տարբերակում մտցնել տվյալների կատեգորիաների միջև՝ հետապնդվող նպատակին հասնելու համար դրանց հնարավոր օգտակարության հիման վրա կամ ըստ շահագրգիռ անձանց կարծիքի[41]: Մշակման պայմանների, օրինակ՝ պահպանման ժամկետի սահմանումը պետք է հիմնված լինի օբյեկտիվ չափանիշների վրա՝ ապահովելու համար, որ միջամտությունը սահմանափակվի միայն նրանով, ինչը խիստ անհրաժեշտ է[42]:

58. Ելնելով յուրաքանչյուր իրավիճակից՝ անհրաժեշտության և համաչափության գնահատմամբ պետք է վերհանվեն և դիտարկվեն բոլոր այն հետևանքները, որոնք ընկնում են այլ հիմնարար իրավունքների, օրինակ՝ Խարտիայի 1-ին հոդվածի համաձայն մարդու արժանապատվության, Խարտիայի 10-րդ հոդվածի համաձայն մտքի, խղճի և կրոնի ազատության, Խարտիայի 11-րդ հոդվածի համաձայն արտահայտվելու ազատության, ինչպես նաև Խարտիայի 12-րդ հոդվածի համաձայն հավաքների և միավորումներ կազմելու ազատության իրավունքների գործողության շրջանակում:

---

[36] Տե՛ս նաև հատուկ կատեգորիայի տվյալների մշակման ժամանակ տեխնիկական և կազմակերպչական միջոցների բարձր պահանջները, հոդված 29, ԻԿՀ 1-ին պարբերություն:
[37] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 66:
[38] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 67:
[39] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություններ 60 և 61:
[40] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 68:
[41] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 63:
[42] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 64:

59. Ավելին, անհրաժեշտ է լրջորեն հաշվի առնել այն հանգամանքը, որ եթե տվյալները համակարգված կերպով մշակվում են առանց տվյալների սուբյեկտների գիտության, դա հավանաբար կառաջացնի մշտական վերահսկողության տակ գտնվելու ընդհանուր տպավորություն[43]: Սա կարող է հանգեցնել համապատասխան հիմնարար իրավունքներից որոշների կամ բոլորի առնչությամբ զսպող ազդեցությունների:

60. Իրավապահ գործունեության ոլորտում դեմքերի ճանաչման հետ կապված օրենսդրական միջոցների կիրառման հարցում անհրաժեշտության և համաչափության գնահատումը դյուրացնելու և իրագործելու նպատակով ազգային և Միության օրենսդիրները կարող են օգտվել այս առաջադրանքի համար հատուկ նախատեսված առկա գործնական գործիքներից: Մասնավորապես, կարող է օգտագործվել Տվյալների պաշտպանության եվրոպական վերահսկող մարմնի կողմից տրամադրված անհրաժեշտության և համաչափության գործիքակազմը[44]:

3.1.3.5 Խարտիայի 52(3), 53-րդ հոդվածները (պաշտպանության մակարդակը նաև ՄԻԵԿ-ի առնչությամբ)

61. Խարտիայի 52(3) և 53-րդ հոդվածների համաձայն՝ Խարտիայի այն իրավունքների իմաստը և շրջանակը, որոնք համապատասխանում են ՄԻԵԿ-ի կողմից երաշխավորված իրավունքներին, պետք է լինեն նույնը, ինչ ՄԻԵԿ-ի կողմից սահմանված իրավունքները: Սակայն ինչ վերաբերում է, մասնավորապես, Խարտիայի 7-րդ հոդվածին, դրա համարժեքը կարելի է գտնել ՄԻԵԿ-ում, մինչդեռ Խարտիայի 8-րդ հոդվածի համարժեքը՝ ոչ[45]: Խարտիայի 52(3) հոդվածը չի խոչընդոտում, որպեսզի Միության իրավունքով տրամադրի առավել ընդգրկուն պաշտպանություն: Քանի որ ՄԻԵԿ-ը չի հանդիսանում իրավական գործիք, որը պաշտոնապես ինկորպորացվել է ԵՄ իրավունքում, ԵՄ օրենսդրությունը պետք է ընդունվի Խարտիայի հիմնարար իրավունքների լույսի ներքո[46]:

62. ՄԻԵԿ-ի 8-րդ հոդվածի համաձայն՝ չի թույլատրվում պետական մարմինների միջամտությունն անձնական և ընտանեկան կյանքի նկատմամբ հարգանքի իրավունքի իրականացմանը, բացառությամբ այն դեպքերի, երբ դա նախատեսված է օրենքով և անհրաժեշտ է ժողովրդավարական հասարակությունում՝ ի շահ պետական անվտանգության, հասարակական կարգի կամ երկրի տնտեսական բարեկեցության, ինչպես նաև անկարգությունների կամ հանցագործությունների կանխման, առողջության կամ բարոյականության պաշտպանության կամ այլ անձանց իրավունքների ու ազատությունների պաշտպանության նպատակով:

---

[43] ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 37:

[44] Տվյալների պաշտպանության եվրոպական վերահսկող մարմին. անձնական տվյալների պաշտպանության հիմնարար իրավունքը սահմանափակող միջոցների անհրաժեշտության գնահատում. գործիքակազմ (2017 թվականի ապրիլի 11), Տվյալների պաշտպանության եվրոպական վերահսկող մարմին. Անձնական կյանքի անձեռնմխելիության և անձնական տվյալների պաշտպանության հիմնարար իրավունքները սահմանափակող միջոցների համաչափության գնահատման վերաբերյալ ՏՊԵՎՄ-ի ուղեցույց (2019 թվականի դեկտեմբերի 19):

[45] ԵՄԱԴ, գործ թիվ C-203/15, Tele2 Sverige, պարբերություն 129:

[46] ԵՄԱԴ, գործ թիվ C-311/18, պարբերություն 99:

63. ՄԻԵԿ-ը սահմանում է նաև ստանդարտներ՝ կապված սահմանափակումների կիրառման եղանակների հետ: Հիմնական պահանջներից մեկը, բացի օրենքի գերակայությունից, կանխատեսելիությունն է: Կանխատեսելիության պահանջը բավարարելու համար օրենքի ձևակերպումները պետք է բավականաչափ հստակ լինեն, որպեսզի անձինք բավարար պատկերացում ունենան այն հանգամանքների և պայմանների մասին, որոնց դեպքում մարմիններն իրավասու են դիմելու ցանկացած այդ միջոցին[47]: Այս պահանջը հաստատված է ԵՄԱԴ-ի և Տվյալների պաշտպանության մասին ԵՄ իրավունքով (տե՛ս 3.2.1.1 բաժինը):
64. ՄԻԵԿ-ի 8-րդ հոդվածի իրավունքներն էլ ավելի հստակեցնելով՝ Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին կոնվենցիայի դրույթները[48] նույնպես պետք է լիարժեք կերպով հարգվեն: Այնուամենայնիվ, պետք է հաշվի առնել, որ այդ դրույթները Միության գործող իրավունքի տեսանկյունից միայն նվազագույն ստանդարտներն են:

3.2 Հատուկ իրավական շրջանակը. Իրավունքի կիրառման հրահանգը

65. ԻԿՀ-ով նախատեսված է ԴՃՏ-ի կիրառման որոշ շրջանակ: Նախ՝ ԻԿՀ 3(13) հոդվածով սահմանվում է «կենսաչափական տվյալներ» եզրույթը[49]: Մանրամասների համար տե՛ս վերոնշյալ 2.1 բաժինը: Երկրորդ՝ 8(2) հոդվածով պարզաբանվում է, որ որպեսզի ցանկացած մշակում համարվի օրինական, ԻԿՀ 1(1) հոդվածում նշված նպատակների համար անհրաժեշտ լինելու հանգամանքից բացի, այն պետք է կարգավորվի ազգային իրավունքով, որն առնվազն սահմանում է մշակման խնդիրները, մշակման ենթակա անձնական տվյալները և մշակման նպատակը: Կենսաչափական տվյալների առնչությամբ հատուկ կարևորություն ունեցող մյուս դրույթները ԻԿՀ 10-րդ և 11-րդ հոդվածներն են: 10-րդ հոդվածը պետք է ընթերցվի ԻԿՀ 8-րդ հոդվածի հետ համակցությամբ[50]: ԻԿՀ 4-րդ հոդվածով սահմանված՝ անձնական տվյալների մշակման սկզբունքները պետք է միշտ պահպանվեն, և ԴՃՏ-ի միջոցով հնարավոր կենսաչափական մշակման ցանկացած գնահատման ժամանակ պետք է առաջնորդվել դրանցով:

3.2.1 Իրավապահ նպատակներով հատուկ կատեգորիայի տվյալների մշակումը

66. ԻԿՀ 10-րդ հոդվածի համաձայն՝ հատուկ կատեգորիայի տվյալների մշակումը, ինչպիսիք են կենսաչափական տվյալները, թույլատրվում է միայն, եթե դա խիստ անհրաժեշտ է, և եթե պահպանվում են տվյալների սուբյեկտի իրավունքների ու ազատությունների համապատասխան երաշխիքները: Ավելին, այն թույլատրվում է միայն, եթե Միության կամ անդամ պետության իրավունքով թույլատրվում է պաշտպանել տվյալների սուբյեկտի կամ մեկ այլ ֆիզիկական անձի կենսական շահերը, կամ երբ այդ մշակումը վերաբերում է այն տվյալներին, որոնք ակնհայտորեն հրապարակվել են տվյալների սուբյեկտի կողմից: Այս ընդհանուր դրույթն ընդգծում է հատուկ կատեգորիայի տվյալների մշակման կարևորությունը:

---

[47] Մարդու իրավունքների եվրոպական դատարան, վճիռ, *ԿՈՊԼԱՆԴ ԸՆԴԴԵՄ ՄԻԱՑՅԱԼ ԹԱԳԱՎՈՐՈՒԹՅԱՆ ԳՈՐԾ* [CASE OF COPLAND v. THE UNITED KINGDOM], 03/04/2007, Գանգատ թիվ 62617/00, պարբերություն 46:

[48] ԵՊՇ թիվ 108:

[49] ԻԿՀ 3(13) հոդվածի համաձայն՝ «կենսաչափական տվյալներ» նշանակում է ֆիզիկական անձի ֆիզիկական, ֆիզիոլոգիական կամ վարքային բնութագրերի հետ կապված հատուկ տեխնիկական մշակման արդյունքում ստացված անձնական տվյալներ, որոնք թույլ են տալիս կամ հաստատում այդ ֆիզիկական անձի եզակի նույնականացումը, օրինակ՝ դեմքի պատկերները կամ դակտիլոսկոպիկ տվյալները:

[50] WP258, Իրավունքի կիրառման հրահանգի (ԵՄ 2016/680) որոշ առանցքային հարցերի վերաբերյալ կարծիք, էջ 7:

3.2.1.1 Միության կամ անդամ պետության իրավունքով թույլատրված լինելը

67. Ինչ վերաբերում է օրենսդրական միջոցի անհրաժեշտ տեսակին, ԻԿՀ 33-րդ ներածական դրույթում նշվում է, որ «[ե]րբ սույն հրահանգով հղում է կատարվում անդամ պետությունների իրավունքին, իրավական հիմքին կամ օրենսդրական միջոցին, պարտադիր չէ, որ առկա լինի պառլամենտի կողմից ընդունված օրենսդրական ակտ՝ չհակասելով համապատասխան անդամ պետության սահմանադրական կարգի պահանջներին»[51]:

68. Խարտիայի 52(1) հոդվածի համաձայն՝ Խարտիայի կողմից ճանաչված իրավունքների ու ազատությունների իրացման ցանկացած սահմանափակում պետք է «նախատեսված լինի օրենքով»: Սա համահունչ է ՄԻԵԴ-ի 8(2) հոդվածի «օրենքին համապատասխան» արտահայտության հետ, որը նշանակում է ոչ միայն կիրառելի իրավունքին համապատասխանություն, այլև վերաբերում է այդ իրավունքի որակին՝ չհակասելով ակտի բնույթին՝ պահանջելով, որպեսզի այն համատեղելի լինի օրենքի գերակայության հետ:

69. ԻԿՀ 33-րդ հոդվածի ներածական դրույթում նշվում է, որ «[ա]յնուամենայնիվ, անդամ պետության այդ իրավունքը, իրավական հիմքը կամ օրենսդրական միջոցը պետք է լինեն հստակ և ճշգրիտ, և դրա կիրառումը պետք է Արդարադատության դատարանի և Մարդու իրավունքների եվրոպական դատարանի նախադեպային իրավունքով սահմանված կարգով կանխատեսելի լինի նրանց համար, ում վրա դրանք տարածվում են: Անդամ պետության՝ սույն հրահանգի շրջանակներում անձնական տվյալների մշակումը կարգավորող իրավունքով պետք է նշվի առնվազն մշակման խնդիրները, մշակման ենթակա անձնական տվյալները, մշակման նպատակները և անձնական տվյալների ամբողջականությունն ու գաղտնիությունը պահպանելու ընթացակարգերը և դրանց ոչնչացման ընթացակարգերը»:

70. Ազգային իրավունքի ձևակերպումները պետք է բավականաչափ հստակ լինեն, որպեսզի տվյալների սուբյեկտները բավարար պատկերացում ունենան այն հանգամանքների և պայմանների մասին, որոնց դեպքում հսկողներն իրավասու են դիմելու ցանկացած այդ միջոցին: Սա ներառում է մշակման հնարավոր նախապայմանները, ինչպիսիք են ապացույցների հատուկ տեսակները, ինչպես նաև դատական կամ ներքին թույլտվության անհրաժեշտությունը: Համապատասխան իրավունքը կարող է տեխնոլոգիական առումով չեզոք լինել այնքանով, որքանով ԴՃՏ համակարգերով անձնական տվյալների մշակման հատուկ ռիսկերն ու առանձնահատկությունները բավարար չափով հաշվի են առնված: ԻԿՀ և Եվրոպական միության Արդարադատության դատարանի (ԵՄԱԴ), ինչպես նաև Մարդու իրավունքների եվրոպական դատարանի (ՄԻԵԴ) նախադեպային իրավունքի համաձայն՝ իսկապես կարևոր է, որ օրենսդրական միջոցները, որոնք իրավական հիմք են նախատեսում դեմքի ճանաչման միջոցի համար, կանխատեսելի լինեն տվյալների սուբյեկտների համար:

71. Հնարավոր չէ օրենսդրական միջոցին հղում կատարել որպես իրավապահ նպատակներով ԴՃՏ-ի միջոցով կենսաչափական տվյալների մշակումը թույլատրող օրենք, եթե դա պարզապես ԻԿՀ 10-րդ հոդվածի ընդհանուր դրույթի պարզապես փոխատեղումն է:

---

[51] Դիտարկվող օրենսդրական միջոցի տեսակը պետք է համապատասխանի ԵՄ իրավունքին կամ ազգային իրավունքին: Կախված սահմանափակման միջամտության աստիճանից՝ ազգային մակարդակում կարող է պահանջվել կոնկրետ օրենսդրական միջոց՝ հաշվի առնելով նորմայի մակարդակը:

72. Բացի կենսաչափական տվյալներից, ԻԿՀ 10-րդ հոդվածով կարգավորվում է այլ հատուկ կատեգորիայի, ինչպիսիք են սեռական կողմնորոշման, քաղաքական կարծիքների և կրոնական համոզմունքների հետ կապված տվյալների մշակումը՝ այդպիսով ընդգրկելով մշակման լայն շրջանակ: Բացի այդ, այդ դրույթով նախատեսված չեն հատուկ պահանջներ, որոնք ցույց են տալիս այն հանգամանքները և պայմանները, որոնց դեպքում իրավապահ մարմիններն իրավասու կլինեն դիմելու դեմքի ճանաչման տեխնոլոգիայի կիրառմանը: Հղում կատարելով տվյալների այլ տեսակներին և առանց լրացուցիչ հստակեցումների հատուկ երաշխիքների բացահայտ անհրաժեշտությանը՝ ԻԿՀ 10-րդ հոդվածը ներպետական իրավունքում փոխատեղող ազգային դրույթը, նմանատիպ ընդհանուր և վերացական ձևակերպումներով, չի կարող վկայակոչվել որպես դեմքի ճանաչման տեխնոլոգիայի միջոցով կենսաչափական տվյալներ մշակելու իրավական հիմք, քանի որ այն չի ունենա ճշգրտություն և կանխատեսելիություն: ԻԿՀ 28(2) կամ 46(1)(գ) հոդվածներին համապատասխան՝ մինչև դեմքի ճանաչման տեխնոլոգիայի կիրառմամբ կենսաչափական տվյալների մշակման ցանկացած ձևի համար օրենսդրի կողմից նոր իրավական հիմք ստեղծելը, անհրաժեշտ է խորհրդակցել Տվյալների պաշտպանության վերահսկող ազգային մարմնի հետ:

3.2.1.2 Խիստ անհրաժեշտությունը

73. Մշակումը կարող է դիտարկվել «խիստ անհրաժեշտ» միայն այն դեպքում, եթե միջամտությունն անձնական տվյալների պաշտպանությանը և դրա սահմանափակումներին սահմանափակվում են նրանով, ինչը բացարձակ անհրաժեշտ է[52]: «Խիստ» եզրույթի ավելացումը նշանակում է, որ օրենսդիրը նախատեսում էր հատուկ կատեգորիայի տվյալների մշակման իրականացումը միայն անհրաժեշտության պայմաններից ավելի խիստ պայմաններում (տե՛ս վերևում 3.1.3.4 կետը): Այս պահանջը պետք է մեկնաբանվի որպես պարտադիր: Այն սահմանափակում է իրավապահ մարմնին անհրաժեշտության ստուգման ժամանակ թույլատրված հայեցողական լիազորությունների շրջանակը՝ այն հասցնելով բացարձակ նվազագույնի: ԵՄԱԴ-ի հաստատված նախադեպային իրավունքին համապատասխան՝ «խիստ անհրաժեշտության» պայմանը սերտորեն փոխկապված է նաև օբյեկտիվ չափանիշների պահանջի հետ՝ այն հանգամանքներն ու պայմանները սահմանելու համար, որոնց դեպքում կարող է ձեռնարկվել մշակումը՝ այդպիսով բացառելով ընդհանուր կամ համակարգված բնույթ կրող ցանկացած մշակում[53]:

---

[52] Անձնական կյանքի նկատմամբ հարգանքի հիմնարար իրավունքի վերաբերյալ համապատասխան նախադեպային իրավունք, տե՛ս ԵՄԱԴ-ի գործ թիվ C-73/07, պարբերություն 56 (Satakunnan Markkinapörssi and Satamedia), ԵՄԱԴ, գործեր թիվ C-92/09 և թիվ C-93/09, պարբերություն 77 (Schecke and Eifert), ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 52 (Թվային իրավունքներ), ԵՄԱԴ, գործ թիվ C-362/14, պարբերություն 92 (Schrems):

[53] ԵՄԱԴ, գործ թիվ 623/17, պարբերություն 78:

3.2.1.3 Ակնհայտորեն հանրամատչելի դարձնելը

74. Գնահատելիս, թե արդյոք մշակումը վերաբերում է այն տվյալներին, որոնք տվյալների սուբյեկտի կողմից ակնհայտորեն հանրամատչելի են դարձվել, պետք է հիշել, որ լուսանկարը, որպես այդպիսին, կանոնավոր կերպով չի համարվում կենսաչափական տվյալ[54]: Հետևաբար, այն փաստը, որ լուսանկարն ակնհայտորեն հանրամատչելի է դարձվել տվյալների սուբյեկտի կողմից, չի նշանակում, որ լուսանկարից հատուկ տեխնիկական միջոցներով առբերված համապատասխան կենսաչափական տվյալները համարվում են ակնհայտորեն հանրամատչելի դարձված:

75. Ինչ վերաբերում է ընդհանուր առմամբ անձնական տվյալներին, որպեսզի կենսաչափական տվյալները դիտվեն որպես տվյալների սուբյեկտի կողմից ակնհայտորեն հանրամատչելի դարձված, տվյալների սուբյեկտը պետք է կենսաչափական մոդելը (և ոչ միայն դեմքի պատկերը) միտումնավոր ազատ հասանելի և հանրամատչելի դարձրած լինի՝ բաց կոդի միջոցով: Եթե երրորդ անձը բացահայտում է կենսաչափական տվյալները, ապա չի կարելի համարել, որ տվյալներն ակնհայտորեն հանրամատչելի են դարձվել տվյալների սուբյեկտի կողմից:

76. Ավելին, որպեսզի կենսաչափական տվյալները համարվեն ակնհայտորեն հանրամատչելի դարձված, բավարար չէ մեկնաբանել տվյալների սուբյեկտի վարքագիծը: Օրինակ՝ սոցիալական ցանցերի կամ առցանց հարթակների դեպքում ՏՊԵԽ-ը կարծում է, որ տվյալների սուբյեկտի կողմից գաղտնիության պահպանման հատուկ ֆունկցիաները չակտիվացնելը կամ չընտրելը բավարար չէ, որպեսզի համարվի, որ տվյալների սուբյեկտն ակնհայտորեն հանրամատչելի է դարձրել իր անձնական տվյալները, և որ այդ տվյալները (օրինակ՝ լուսանկարները) կարող են վերածվել կենսաչափական մոդելների և օգտագործվել նույնականացման նպատակներով՝ առանց տվյալների սուբյեկտի համաձայնության: Առավել ընդհանուր, ծառայության կանխադրված կարգավորումները, օրինակ՝ մոդելները հանրամատչելի դարձնելը կամ ընտրության բացակայությունը, օրինակ՝ մոդելները հանրամատչելի են դարձվել առանց օգտատիրոջ կողմից այդ կարգավորումը փոխելու հնարավորության, չպետք է ոչ մի կերպ մեկնաբանվեն որպես ակնհայտորեն հանրամատչելի դարձված տվյալներ:

[54] Տե՛ս ՏՊԸԿ 51-րդ ներածական դրույթը՝ «լուսանկարների մշակումը կանոնավոր կերպով չպետք է համարվի որպես հատուկ կատեգորիայի անձնական տվյալների մշակում, քանի որ դրանք ընդգրկվում են կենսաչափական տվյալների սահմանման մեջ միայն այն դեպքում, երբ մշակվում են հատուկ տեխնիկական միջոցներով, որոնք թույլ են տալիս ֆիզիկական անձի եզակի նույնականացումը կամ իսկորոշումը:»

3.2.2 Ավտոմատացված անհատական որոշումների կայացումը, այդ թվում՝ պրոֆիլավորումը

77. ԻԿՀ 11(1) հոդվածով անդամ պետությունները պարտավորվում են ընդհանուր առմամբ արգելել բացառապես ավտոմատացված մշակման հիման վրա որոշումների կայացումը, այդ թվում՝ պրոֆիլավորումը, որն իրավական տեսանկյունից բացասական ազդեցություն ունի կամ էականորեն ազդում է տվյալների սուբյեկտի վրա: Որպես այս ընդհանուր արգելքից բացառություն՝ այդ մշակումը կարող է հնարավոր լինել միայն այն դեպքում, եթե չի արգելվում Միության կամ անդամ պետության այն իրավունքով, որով կարգավորվում է հսկողի գործունեությունը, և որը համապատասխան երաշխիքներ է տրամադրում տվյալների սուբյեկտի իրավունքների ու ազատությունների, առնվազն հսկողի կողմից մարդու միջամտություն ստանալու իրավունքի համար: Դա կարող է կիրառվել միայն սահմանափակ կերպով: Այս շեմը կիրառվում է սովորական (այսինքն՝ ոչ հատուկ) կատեգորիայի անձնական տվյալների նկատմամբ: Ավելի բարձր շեմ և առավել սահմանափակ կիրառությունը տարածվում է ԻԿՀ 11(2) հոդվածով նախատեսված բացառության վրա: Այն ևս մեկ անգամ ընդգծում է, որ առաջին պարբերությամբ նախատեսված որոշումները հիմնված չեն հատուկ կատեգորիայի տվյալների, այսինքն, մասնավորապես՝ ֆիզիկական անձին եզակի նույնականացման նպատակով օգտագործվող կենսաչափական տվյալների վրա: Բացառություն կարող է նախատեսվել միայն այն դեպքում, երբ տվյալների սուբյեկտի իրավունքներն ու ազատությունները և համապատասխան ֆիզիկական անձի օրինական շահերը պաշտպանելու համար ձեռնարկվեն համապատասխան միջոցներ: Այս բացառությունը պետք է ընթերցվի ի լրումն և վերը նշված ԻԿՀ 10-րդ հոդվածի լույսի ներքո:

78. Կախված ԴՃՏ համակարգից՝ նույնիսկ ԴՃՏ արդյունքների գնահատման գործընթացում մարդու միջամտությունը չի կարող ինքնին անձանց իրավունքները հարգելու և, մասնավորապես, անձնական տվյալների պաշտպանության իրավունքը հարգելու առումով բավարար երաշխիք լինել՝ հաշվի առնելով ինքնին մշակման գործընթացի արդյունքում առաջացող հնարավոր կողմնակալությունը և սխալը: Ավելին, մարդու կողմից միջամտությունը կարող է դիտարկվել որպես երաշխիք միայն այն դեպքում, երբ միջամտող անձը մարդու միջամտության ընթացքում կարող է քննադատորեն վիճարկել ԴՃՏ արդյունքները: Շատ կարևոր է, որ մարդուն հնարավորություն տրվի հասկանալ ԴՃՏ համակարգը և դրա սահմանները, ինչպես նաև ճիշտ մեկնաբանել դրա արդյունքները: Անհրաժեշտ է նաև ստեղծել աշխատավայր և կազմակերպություն, որը հակազդում է ավտոմատացման կողմնակալության հետևանքներին և խուսափում է արդյունքների անվերապահ ընդունումից, օրինակ՝ ժամանակի սղության, ծանրաբեռնվածության, կարիերայի համար հնարավոր վնասակար հետևանքների և այլնի պատճառով:

79. ԻԿՀ 11(3) հոդվածի համաձայն՝ պրոֆիլավորումը, որը հանգեցնում է հատուկ կատեգորիայի անձնական տվյալների, այն է՝ կենսաչափական տվյալների հիման վրա ֆիզիկական անձանց նկատմամբ խտրականության, պետք է արգելվի՝ Միության իրավունքին համապատասխան: ԻԿՀ 3(4) հոդվածի համաձայն՝ «պրոֆիլավորում» նշանակում է անձնական տվյալների ավտոմատացված մշակման ցանկացած ձև, որը ներառում է ֆիզիկական անձին վերաբերող անձնական կյանքի որոշ հայեցակետերը գնահատելու նպատակով անձնական տվյալների օգտագործում, մասնավորապես, այնպիսի հայեցակետերը վերլուծելը կամ կանխատեսելը, որոնք առնչվում են ֆիզիկական անձի աշխատանքի կատարողականին, տնտեսական վիճակին, առողջությանը, անձնական

նախասիրություններին, հետաքրքրություններին, հուսալիությանը, վարքագծին, գտնվելու վայրին կամ տեղաշարժերին: Երբ քննարկվում է, թե արդյոք համապատասխան միջոցներ նախատեսված են տվյալների սուբյեկտի իրավունքներն ու ազատությունները, ինչպես նաև համապատասխան ֆիզիկական անձի օրինական շահերը պաշտպանելու համար, անհրաժեշտ է նկատի ունենալ, որ ԴՃՏ-ի կիրառումը կարող է հանգեցնել պրոֆիլավորման՝ կախված ԴՃՏ-ի կիրառման ձևից և նպատակից: Ամեն դեպքում, Միության իրավունքին և ԻԿՀ 11(3) հոդվածին համապատասխան՝ պրոֆիլավորումը, որը հանգեցնում է հատուկ կատեգորիայի անձնական տվյալների հիման վրա ֆիզիկական անձանց նկատմամբ խտրականության, արգելվում է:

3.2.3 Տվյալների սուբյեկտների կատեգորիաները

80. ԻԿՀ 6-րդ հոդվածը վերաբերում է տվյալների սուբյեկտների տարբեր կատեգորիաների միջև տարբերակում մտցնելու անհրաժեշտությանը: Այս տարբերակումը պետք է մտցվի այնտեղ, որտեղ այն կիրառելի է և որքանով, որ այն հնարավոր է: Այն պետք է արտացոլվի տվյալների մշակման եղանակի վրա: ԻԿՀ 6-րդ հոդվածում բերված օրինակներից կարելի է եզրակացնել, որ, որպես կանոն, անձնական տվյալների մշակումը պետք է համապատասխանի անհրաժեշտության և համաչափության չափանիշներին՝ նաև կապված տվյալների սուբյեկտների կատեգորիայի հետ[55]: Կարելի է նաև եզրակացնել, որ այն տվյալների սուբյեկտների առնչությամբ, որոնց դեպքում չկա որևէ ապացույց, որը հնարավորություն կտա ենթադրելու, որ նրանց վարքագիծը կարող է նույնիսկ անուղղակի կամ հեռավար կապ ունենալ ԻԿՀ համաձայն իրավաչափ նպատակի հետ, միջամտության համար հիմնավորում, ամենայն հավանականությամբ, առկա չէ[56]: Եթե ԻԿՀ 6-րդ հոդվածի համաձայն որևէ տարբերակում կիրառելի կամ հնարավոր չէ, ապա ԻԿՀ 6-րդ հոդվածի կանոնից բացառությունը միջամտության անհրաժեշտության և համաչափության գնահատման ժամանակ պետք է մանրամասն դիտարկվի: Տվյալների սուբյեկտների տարբեր կատեգորիաների միջև տարբերակումը կարևոր պահանջ է, երբ խոսքը գնում է դեմքի ճանաչման տեխնոլոգիայի միջոցով անձնական տվյալների մշակման մասին՝ հաշվի առնելով նաև հնարավոր կեղծ դրական կամ կեղծ բացասական արդյունքները, որոնք կարող են էական ազդեցություն ունենալ տվյալների սուբյեկտների, ինչպես նաև քննության ընթացքի վրա:

81. Ինչպես նշվեց, Միության իրավունքը կիրարկելիս պետք է հարգվեն Հիմնարար իրավունքների Եվրոպական միության խարտիայի դրույթները, տե՛ս Խարտիայի 52-րդ հոդվածը: Հետևաբար, ԻԿՀ-ով նախատեսված շրջանակը և չափանիշները պետք է ընթերցվեն Խարտիայի լույսի ներքո: ԵՄ-ի և դրա անդամ պետությունների իրավունքի գործողությունները չպետք է այս միջոցից ցածր իջնեն և պետք է ապահովեն Խարտիայի ամբողջական իրավական ուժը:

[55] Տե՛ս նաև ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 56-59:
[56] Տե՛ս նաև ԵՄԱԴ, գործ թիվ C-594/12, պարբերություն 58:

3.2.4 Տվյալների սուբյեկտի իրավունքները

82. Տվյալների պաշտպանության եվրոպական խորհուրդը (այսուհետ՝ ՏՊԵԽ) Տվյալների պաշտպանության ընդհանուր կանոնակարգի (այսուհետ՝ ՏՊԸԿ) համաձայն տվյալների սուբյեկտների իրավունքների տարբեր հայեցակետերի առնչությամբ արդեն իսկ տվել է ուղղորդում[57]: ԻԿՀ-ով նախատեսվում են տվյալների սուբյեկտի համանման իրավունքներ, և դրանց առնչությամբ ընդհանուր ուղղորդումը ներկայացվել է ՏՊԵԽ-ի կողմից հաստատված՝ 29-րդ հոդվածով սահմանված աշխատանքային խմբի կարծիքում[58]: Որոշ դեպքերում ԻԿՀ-ով նախատեսվում են այդ իրավունքների որոշ սահմանափակումներ: Այդ սահմանափակումների պարամետրերի մասին առավել մանրամասն կներկայացվեն «Տվյալների սուբյեկտի իրավունքների իրավաչափ սահմանափակումներ» վերտառությամբ 3.2.4.6 բաժնում:

83. Թեև ԻԿՀ III հավելվածում թվարկված՝ տվյալների սուբյեկտի բոլոր իրավունքները բնականաբար կիրառելի են նաև դեմքի ճանաչման տեխնոլոգիայի (ԴՃՏ) միջոցով անձնական տվյալների մշակման նկատմամբ, այնուամենայնիվ, հաջորդ բաժնում շեշտը կդրվի որոշ իրավունքների և հայեցակետերի վրա, որոնք կարող են հատուկ հետաքրքրություն ներկայացնել՝ ուղղորդում ստանալու տեսանկյունից: Ավելին, այս գլուխը և դրա վերլուծությունը կախված են խնդրո առարկա ԴՃՏ-ի միջոցով մշակումից, որը բավարարել է նախորդ գլխում նկարագրված իրավական պահանջները:

84. Հաշվի առնելով ԴՃՏ-ի միջոցով անձնական տվյալների մշակման բնույթը (հատուկ կատեգորիայի անձնական տվյալների մշակումը հաճախ առանց տվյալների սուբյեկտի հետ որևէ ակնհայտ փոխգործակցության)՝ հսկողը պետք է մանրամասն դիտարկի, թե ինչպես (կամ եթե կարող է) կատարի ԻԿՀ պահանջները՝ մինչև ԴՃՏ-ի միջոցով ցանկացած մշակում սկսելը: Մասնավորապես, մանրամասն վերլուծելով հետևյալը.

- ովքեր են տվյալների սուբյեկտները (հաճախ ավելին, քան այն տվյալների սուբյեկտը, որը մշակման նպատակով հանդիսանում է հիմնական թիրախ).
- ինչպես են տվյալների սուբյեկտները տեղեկանում ԴՃՏ-ի միջոցով մշակման մասին (տե՛ս 3.2.4.1 բաժինը).
- ինչպես կարող են տվյալների սուբյեկտներն իրացնել իրենց իրավունքները (այստեղ թե՛ տեղեկություններ ստանալու, թե՛ հասանելիության իրավունքները, ինչպես նաև ուղղման կամ սահմանափակման իրավունքները կարող են հատկապես դժվար լինել պահպանել, եթե ԴՃՏ-ն օգտագործվում է բոլոր ստուգումների համար, բացառությամբ 1-ը 1-ին ստուգման՝ տվյալների սուբյեկտի հետ անմիջական շփման պայմաններում):

[57] Տե՛ս, օրինակ՝ ՏՊԵԽ-ի՝ Տվյալների սուբյեկտի իրավունքների վերաբերյալ 1/2022 ուղեցույց. հասանելիության իրավունքը և Վիդեո սարքերի միջոցով անձնական տվյալների մշակման վերաբերյալ ՏՊԵԽ-ի թիվ 3/2019 ուղեցույցը:

[58] WP258, Իրավունքի կիրառման հրահանգի (ԵՄ 2016/680) որոշ առանցքային հարցերի վերաբերյալ կարծիք:

3.2.4.1 Տվյալների սուբյեկտների համար իրավունքները և տեղեկությունները հակիրճ, հասկանալի և հեշտ հասանելի եղանակով հայտնի դարձնելը

85. ԴՃՏ-ն խնդիրներ է ստեղծում՝ տվյալների սուբյեկտներին իրենց կենսաչափական տվյալների մշակման մասին տեղեկացնելու առումով: Դա հատկապես դժվար է, երբ ԻՄ-ն ԴՃՏ-ի միջոցով վերլուծում է այն տեսանյութը, որն իրեն է փոխանցվում կամ տրամադրվում երրորդ անձի միջոցով, քանի որ քիչ հնարավորություն կա, և մեծամասամբ ընդհանրապես հնարավորություն չկա, որպեսզի ԻՄ-ն տվյալներ հավաքագրելու պահին այդ մասին ծանուցի տվյալների սուբյեկտին (օրինակ՝ տեղում որևէ նշանի միջոցով): Քննության (կամ մշակման նպատակի) համար կարևորություն չներկայացնող ցանկացած տեսանյութ մինչև կենսաչափական տվյալների ցանկացած մշակումը պետք է միշտ հեռացվի կամ անանունացվի (օրինակ՝ մշուշապատման միջոցով՝ առանց տվյալների վերականգնման հետադարձ հնարավորության), որպեսզի հնարավոր լինի խուսափել ԻԿՀ 4(1)(ե) հոդվածով նախատեսված տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքը, ինչպես նաև ԻԿՀ 13(2) հոդվածով նախատեսված տեղեկություններ տրամադրելու վերաբերյալ պարտավորությունները չկատարելու ռիսկից: Հսկողի պարտականությունն է գնահատել, թե որ տեղեկությունները կարող են կարևոր լինել տվյալների սուբյեկտի համար իր իրավունքների իրացման ժամանակ և ապահովել անհրաժեշտ տեղեկությունների տրամադրումը: Տվյալների սուբյեկտի իրավունքների արդյունավետ իրացումը կախված է հսկողի կողմից տեղեկություններ տրամադրելու պարտականությունները կատարելու հանգամանքից:

86. ԻԿՀ 13(1) հոդվածով սահմանվում են այն նվազագույն տեղեկությունները, որոնք կարող են ընդհանուր առմամբ տրամադրվել տվյալների սուբյեկտին: Այդ տեղեկությունները կարող են տրամադրվել հսկողի կայքէջի միջոցով՝ տպագիր ձևով (օրինակ՝ ըստ պահանջի հասանելի թռուցիկի միջոցով) կամ տվյալների սուբյեկտի համար հեշտ հասանելի այլ աղբյուրների միջոցով: Տվյալների հսկողը պետք է ցանկացած դեպքում ապահովի, որ տեղեկություններն արդյունավետ կերպով տրամադրվեն առնվազն հետևյալ հարցերի առնչությամբ.

- հսկողի, այդ թվում՝ տվյալների պաշտպանության պատասխանատուի ինքնությունը և կոնտակտային տվյալները.
- մշակման նպատակը և ԴՃՏ-ի միջոցով մշակված լինելու վերաբերյալ տեղեկությունները.
- վերահսկող մարմնին բողոք ներկայացնելու իրավունքը և այդ մարմնի կոնտակտային տվյալները.
- անձնական տվյալներին հասանելիություն ստանալու, դրանք ուղղելու կամ ոչնչացնելու պահանջի իրավունքը և անձնական տվյալների մշակման սահմանափակումը:

87. Բացի այդ, ազգային իրավունքով սահմանված հատուկ դեպքերում, ինչպես օրինակ՝ ԴՃՏ-ի միջոցով մշակման դեպքում, որոնք պետք է համապատասխանեն ԻԿՀ 13(2) հոդվածին[59], հետևյալ տեղեկությունները պետք է ուղղակիորեն տրամադրվեն տվյալների սուբյեկտին.

- մշակման իրավական հիմքը.
- տեղեկություններ այն մասին, թե որտեղ են հավաքվել անձնական տվյալները՝ առանց տվյալների սուբյեկտի գիտության.
- այն ժամկետը, որի ընթացքում կպահվեն անձնական տվյալները, կամ եթե դա հնարավոր չէ, այդ ժամկետը որոշելու համար կիրառվող չափանիշները.
- հարկ եղած դեպքում անձնական տվյալներ ստացողների կատեգորիաները (այդ թվում՝ երրորդ երկրները կամ միջազգային կազմակերպությունները):

88. Թեև ԻԿՀ 13(1) հոդվածը վերաբերում է հանրամատչելի դարձված ընդհանուր տեղեկություններին, ԻԿՀ 13(2) հոդվածը վերաբերում է այնպիսի հատուկ դեպքերում կոնկրետ տվյալների սուբյեկտին տրամադրվելիք լրացուցիչ տեղեկություններին, ինչպես օրինակ, երբ տվյալները հավաքվում են անմիջապես տվյալների սուբյեկտից կամ անուղղակիորեն առանց տվյալների սուբյեկտի գիտության[60]: Չկա հստակ սահմանում, թե ինչ է ԻԿՀ 13(2) հոդվածով նշանակում «առանձնահատուկ դեպքեր»: Այնուամենայնիվ, այն վերաբերում է այնպիսի իրավիճակներին, երբ տվյալների սուբյեկտները պետք է տեղեկացված լինեն կոնկրետ իրենց վերաբերող մշակման մասին, և նրանց պետք է տրամադրվեն համապատասխան տեղեկություններ՝ իրենց իրավունքներն արդյունավետորեն իրացնելու համար: ՏՊԵԽ-ը գտնում է, որ «կոնկրետ դեպքի» առկայությունը գնահատելիս անհրաժեշտ է հաշվի առնել մի քանի գործոններ, այդ թվում, եթե անձնական տվյալները հավաքվում են առանց տվյալների սուբյեկտի գիտության, քանի որ դա միակ միջոցն է, որը տվյալների սուբյեկտներին հնարավորություն է տալիս արդյունավետորեն իրացնելու իրենց իրավունքները: «Հատուկ դեպքերի» այլ օրինակներ կարող են լինել, երբ անձնական տվյալները հետագայում մշակվում են միջազգային քրեական համագործակցության ընթացակարգին համապատասխան, կամ երբ անձնական տվյալները մշակվում են գաղտնի օպերացիաների ներքո՝ ազգային իրավունքով սահմանված կարգով: Ավելին, ԻԿՀ 38-րդ հոդվածի ներածական դրույթից բխում է, որ եթե որոշումները կայացվում են բացառապես ԴՃՏ-ի հիման վրա, ապա տվյալների սուբյեկտները պետք է տեղեկացված լինեն ավտոմատացված որոշումների կայացման առանձնահատկությունների մասին: Սա նաև ցույց կտա, որ սա հատուկ դեպք է, երբ անհրաժեշտ է տվյալների սուբյեկտին տրամադրել լրացուցիչ տեղեկություններ՝ ԻԿՀ 13(2) հոդվածի համաձայն[61]:

[59] Օր.՝ «Տվյալների պաշտպանության մասին» Գերմանիայի դաշնային ակտի 56 (1) բաժնում, ի թիվս այլնի, նշվում է, թե գաղտնի գործողություններում ինչ տեղեկություններ պետք է տրամադրվեն տվյալների սուբյեկտին:

[60] Իրավունքի կիրառման հրահանգի (ԵՄ 2016/680) որոշ առանցքային հարցերի վերաբերյալ կարծիք, էջեր17-18:

[61] Ուշադրություն դարձրեք ԻԿՀ 13(1) հոդվածում նշված «տվյալների սուբյեկտին հասանելի դարձնի» եզրույթի և ԻԿՀ 13(2) հոդվածում «տվյալ սուբյեկտին տրամադրի» եզրույթների միջև տարբերությանը: ԻԿՀ 13(2) հոդվածում հսկողը պետք է ապահովի, որ տեղեկությունները հասնեն տվյալների սուբյեկտին, եթե կայքէջում հրապարակված տեղեկությունները բավարար չլինեն:

89. Ի վերջո, հարկ է նշել, որ ԻԿՀ 13(3) հոդվածի համաձայն, անդամ պետությունները կարող են ընդունել օրենսդրական միջոցներ, որոնք սահմանափակում են տեղեկություններ տրամադրելու պարտավորությունը հատուկ դեպքերում, որոշ նպատակների համար: Սա վերաբերում է այնքանով, որքանով և այնքան ժամանակ, որքանով այդ միջոցը համարվում է անհրաժեշտ և համաչափ միջոց ժողովրդավարական հասարակությունում պատշաճ կերպով հաշվի առնելով տվյալների սուբյեկտի հիմնարար իրավունքներն ու օրինական շահերը:

3.2.4.2 Հասանելիության իրավունքը

90. Ընդհանուր առմամբ, տվյալների սուբյեկտն իրավունք ունի իր անձնական տվյալների ցանկացած մշակման վերաբերյալ ստանալու դրական կամ բացասական հաստատում, իսկ դրական պատասխանի դեպքում, որպես այդպիսին անձնական տվյալներին հասանելիություն, ինչպես նաև ԻԿՀ 14-րդ հոդվածում թվարկված լրացուցիչ տեղեկությունները: ԴՃՏ-ի դեպքում, երբ կենսաչափական տվյալները պահվում և կապվում են ինքնության հետ նաև տառաթվային տվյալների միջոցով, դա պետք է հնարավորություն տա իրավասու մարմնին հաստատելու հասանելիություն ստանալու մասին դիմումը՝ հիմնվելով այդ տառաթվային տվյալներով որոնման վրա և առանց այլ անձանց կենսաչափական տվյալների ցանկացած հետագա մշակման (այսինքն՝ ԴՃՏ-ով որոնելով տվյալների շտեմարանում): Տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքը պետք է պահպանվի և չպետք է պահվեն ավելի շատ տվյալներ, քան անհրաժեշտ են մշակման նպատակի համար:

3.2.4.3 Անձնական տվյալներն ուղղելու իրավունքը

91. Քանի որ ԴՃՏ-ով հնարավոր չէ ապահովել բացարձակ ճշտություն, ուստի, հատկապես կարևոր է, որ հսկողները ուշադիր լինեն անձնական տվյալների ուղղման մասին դիմումների առնչությամբ: Սա վերաբերում է նաև այն դեպքին, երբ տվյալների սուբյեկտը ԴՃՏ-ի հիման վրա մտցվում է ոչ ճիշտ կատեգորիայում, օրինակ՝ սխալմամբ մտցվում է կասկածյալների կատեգորիայի մեջ՝ հիմնվելով տեսանյութում գործողությունների ընթացքի նախնական ենթադրության վրա: Տվյալների սուբյեկտների համար ռիսկերը հատկապես լուրջ են, եթե այդ ոչ ճշգրիտ տվյալները պահվում են ոստիկանության տվյալների շտեմարանում և (կամ) տրամադրվում այլ անձանց: Հսկողը պետք է համապատասխանաբար ուղղի պահված տվյալները և ԴՃՏ համակարգերը, տե՛ս ԻԿՀ 47-րդ ներածական դրույթը:

3.2.4.4 Ոչնչացման իրավունքը

92. Շատ դեպքերում, բացի 1-ը 1-ի ստուգման/իսկորոշման դեպքի, ԴՃՏ-ի կիրառումը հավասարազոր կլինի տվյալների սուբյեկտների մեծ թվով կենսաչափական տվյալների մշակմանը: Հետևաբար, կարևոր է, որ հսկողը նախապես նախանշի իր նպատակի և անհրաժեշտության սահմանները, որպեսզի ԻԿՀ 16-րդ հոդվածի համաձայն՝ ոչնչացման մասին դիմումը հնարավոր լինի հասցեագրել առանց անհարկի ձգձգման (քանի որ հսկողը, ի թիվս այլնի, պետք է ոչնչացնի այն անձնական տվյալները, որոնք մշակվում են 4-րդ, 8-րդ և 10-րդ հոդվածների համաձայն գործող օրենսդրությամբ անհրաժեշտ չափից ավելի):

3.2.4.5 Սահմանափակման իրավունքը

93. Այն դեպքում, երբ տվյալների ճշգրտությունը վիճարկվում է տվյալների սուբյեկտի կողմից, և տվյալների ճշգրտությունը չի կարող հաստատվել (կամ երբ անձնական տվյալները պետք է պահպանվեն հետագա ապացույցների համար), հսկողը պարտավոր է սահմանափակել այդ

տվյալների սուբյեկտի անձնական տվյալները՝ ԻԿՀ 16-րդ հոդվածին համապատասխան: Սա հատկապես կարևոր է դառնում, երբ խոսքը գնում է դեմքի ճանաչման տեխնոլոգիայի մասին (հիմնված ալգորիթմի (ալգորիթմների) վրա և, որով, երբեք վերջնական արդյունք չի ապահովվում) այն իրավիճակներում, երբ մեծ քանակությամբ տվյալներ են հավաքվում, և նույնականացման ճշգրտությունն ու որակը կարող են տարբերվել: Վատ որակի տեսանյութերի դեպքում (օրինակ՝ հանցանքի վայրից) կեղծ դրական արդյունքների վտանգը մեծանում է: Ավելին, եթե հետախուզվող անձանց ցուցակում դեմքի պատկերները կանոնավոր կերպով չեն թարմացվում, ապա դա կարող է նաև բարձրացնել կեղծ դրական կամ կեղծ բացասական արդյունքների ռիսկը: Հատուկ դեպքերում, երբ տվյալները չեն կարող ոչնչացվել այն պատճառով, որ կան հիմնավոր պատճառներ ենթադրելու, որ ոչնչացումը կարող է ազդել տվյալների սուբյեկտի օրինական շահերի վրա, այդ դեպքում տվյալները պետք է սահմանափակվեն և մշակվեն միայն այն նպատակով, որը կանխել է դրանց ոչնչացումը (տե՛ս ԻԿՀ 47-րդ ներածական դրույթը):

3.2.4.6 Տվյալների սուբյեկտների իրավունքների օրինական սահմանափակումները

94. Ինչ վերաբերում է հսկողի տեղեկություններ տրամադրելու պարտավորություններին և տվյալների սուբյեկտների հասանելիության իրավունքին, սահմանափակումները թույլատրվում են միայն, եթե դրանք սահմանված են օրենքով, ինչն իր հերթին պետք է անհրաժեշտ և համաչափ միջոց լինել ժողովրդավարական հասարակությունում պատշաճ կերպով հաշվի առնելով համապատասխան ֆիզիկական անձի հիմնարար իրավունքներն ու օրինական շահերը (տե՛ս ԻԿՀ 13(3), 13(4), 15 և 16(4) հոդվածները): Երբ ԴՃՏ-ն կիրառվում է իրավապահ նպատակներով, կարելի է ակնկալել, որ այն կկիրառվի այնպիսի հանգամանքներում, որը կվնասի հետապնդվող նպատակին՝ տեղեկացնելու տվյալների սուբյեկտին կամ ապահովելու տվյալներին հասանելիություն: Սա կիրառվում է, օրինակ՝ ոստիկանության կողմից հանցագործության քննության նկատմամբ կամ ազգային կամ հասարակական անվտանգությունը պաշտպանելու նպատակով:

95. Հասանելիության իրավունքն ավտոմատ չի նշանակում հասանելիություն բոլոր, օրինակ՝ քրեական գործով տեղեկություններին, որտեղ առկա են որևէ մեկի անձնական տվյալները: Իրավունքի սահմանափակումների կիրառման թույլտվության ցայտուն օրինակը քննության ընթացքն է:

3.2.4.7 Վերահսկող մարմնի միջոցով իրավունքների իրացումը

96. Այն դեպքերում, երբ ԻԿՀ III գլխի համաձայն կան իրավունքների իրացման օրինական սահմանափակումներ, տվյալների սուբյեկտը կարող է դիմել տվյալների պաշտպանության մարմնին խնդրանքով՝ իր անունից իրացնել իր իրավունքները՝ ստուգելով հսկողի կողմից մշակման օրինականությունը: Հսկողի պարտականությունն է տեղեկացնել տվյալների սուբյեկտին իր իրավունքներն այդ կերպ իրացնելու հնարավորության մասին (տե՛ս ԻԿՀ 17-րդ հոդվածը և ԻԿՀ 46(1)(է) հոդվածը): ԴՃՏ-ի դեպքում դա նշանակում է, որ հսկողը պետք է ապահովի, որ առկա լինեն համապատասխան միջոցներ, որպեսզի հնարավոր լինի ընթացք տալ այդ դիմումին, օրինակ՝ ձայնագրված նյութի որոնման հնարավորություն ընձեռելով՝ պայմանով, որ տվյալների սուբյեկտն իր անձնական տվյալները տեղորոշելու համար տրամադրի բավարար տեղեկություններ:

3.2.5 Այլ իրավական պահանջներն ու երաշխիքները

3.2.5.1 27-րդ հոդված. Տվյալների պաշտպանության ազդեցության գնահատումը

97. Մինչև ԴՀՏ-ի կիրառումը տվյալների պաշտպանության ազդեցության գնահատում իրականացնելը (ՏՊԱԳ) պարտադիր պահանջ է, քանի որ մշակման տեսակը, մասնավորապես՝ կիրառելով նոր տեխնոլոգիաներ, ինչպես նաև հաշվի առնելով մշակման բնույթը, շրջանակը, համատեքստը և նպատակները, ամենայն հավանականությամբ, կհանգեցնեն ֆիզիկական անձանց իրավունքների ու ազատությունների հատուկ բարձր ռիսկի: Հաշվի առնելով, որ ԴՀՏ-ի կիրառումը ենթադրում է հատուկ կատեգորիայի տվյալների պարբերաբար ավտոմատ մշակում, կարելի է ենթադրել, որ նման դեպքերում հսկողից, որպես կանոն, պահանջվում է իրականացնել ՏՊԱԳ: ՏՊԱԳ-ը պետք է առնվազն պարունակի նախատեսվող մշակման գործողությունների ընդհանուր նկարագրությունը, նպատակների առնչությամբ մշակման գործողությունների անհրաժեշտության և համաչափության գնահատումը, տվյալների սուբյեկտների իրավունքների ու ազատությունների ռիսկերի գնահատումը, այդ ռիսկերը նվազեցնելու համար նախատեսվող միջոցառումները, երաշխիքները, անվտանգության միջոցներն ու մեխանիզմները՝ անձնական տվյալների պաշտպանություն ապահովելու, ինչպես նաև դրանց համապատասխանությունն ապացուցելու համար:

ՏՊԵԽ-ն առաջարկում է հանրամատչելի դարձնել այդ գնահատումների արդյունքները կամ առնվազն ՏՊԱԳ-ի հիմնական արդյունքներն ու եզրահանգումները՝ որպես վստահության և թափանցիկության մակարդակի բարձրացման միջոց[62]:

3.2.5.2 28-րդ հոդված. վերահսկող մարմնի հետ նախնական խորհրդակցությունը

98. Համաձայն ԻԿՀ 28-րդ հոդվածի՝ հսկողը կամ մշակողը պետք է մինչև մշակումը խորհրդակցի վերահսկող մարմնի հետ, եթե. ա) տվյալների պաշտպանության ազդեցության գնահատումը ցույց է տալիս, որ մշակումը կհանգեցնի բարձր ռիսկի, եթե հսկողը ռիսկը նվազեցնելու համար միջոցներ չձեռնարկի, կամ բ) մշակման տեսակը, մասնավորապես՝ նոր տեխնոլոգիաների, մեխանիզմների կամ ընթացակարգերի կիրառմամբ մեծ ռիսկ է պարունակում տվյալների սուբյեկտների իրավունքների ու ազատությունների համար: Ինչպես արդեն ներկայացվել է սույն ուղեցույցների 2.3 բաժնում, ՏՊԵԽ-ը գտնում է, որ ԴՀՏ-ի գործարկման և կիրառման տարբերակերի մեծ մասի դեպքում առկա է տվյալների սուբյեկտների իրավունքների ու ազատությունների համար հատուկ բարձր ռիսկ: Հետևաբար, ի լրումն ՏՊԱԳ-ի, ԴՀՏ-ն գործարկող մարմինը պետք է խորհրդակցի իրավասու վերահսկող մարմնի հետ՝ նախքան համակարգի գործարկումը:

3.2.5.3 29-րդ հոդված. մշակման անվտանգությունը

99. Կենսաչափական տվյալների եզակի բնույթն անհնարին է դարձնում դրանց փոփոխումը տվյալների սուբյեկտի կողմից այն դեպքում, երբ դրանք վտանգված են, օրինակ՝ տվյալների արտահոսքի արդյունքում: Հետևաբար, ԴՀՏ-ն ներդնող և (կամ) կիրառող իրավասու մարմինը պետք է հատուկ ուշադրություն դարձնի մշակման անվտանգությանը՝ ԻԿՀ 29-րդ հոդվածին համապատասխան: Մասնավորապես, իրավապահ մարմինը պետք է ապահովի, որ համակարգը համապատասխանի համապատասխան ստանդարտներին և ձեռնարկի կենսաչափական մոդելների պաշտպանության միջոցներ[63]: Այս պարտավորությունն էլ ավելի է ակտուալ դառնում, եթե իրավապահ մարմինն օգտվում է երրորդ անձի ծառայություններ մատուցողի ծառայություններից (տվյալներ մշակողից):

3.2.5.4 20-րդ հոդված. Տվյալների՝ ներկառուցված և լռելյայն պաշտպանությունը

100. ԻԿՀ 20-րդ հոդվածի համաձայն՝ տվյալների՝ հայեցակարգային և լռելյայն պաշտպանության նպատակն է ապահովել, որպեսզի տվյալների պաշտպանության սկզբունքներն ու երաշխիքները, ինչպիսիք են տվյալների հավաքագրման ծավալները նվազագույնի հասցնելը և դրանց պահպանման սահմանափակումը, ներկառուցված լինեն տեխնոլոգիայի մեջ՝ համապատասխան տեխնիկական ու կազմակերպչական միջոցների միջոցով, ինչպիսին է կեղծանունացումը, նույնիսկ մինչև անձնական տվյալների մշակումը սկսելը և կկիրառվի դրա ողջ կենսափուլի ընթացքում: Հաշվի առնելով ֆիզիկական անձանց իրավունքներին ու ազատություններին հատուկ բարձր ռիսկը, այդ միջոցների ընտրությունը չպետք է կախված լինի բացառապես տնտեսական նկատառումներից[64], այլ պետք է ձգտի կիրառել տվյալների պաշտպանության նորագույն տեխնոլոգիաները: Նույն կերպ, եթե ԻՄ-ն պլանավորում է կիրառել և օգտագործել ԴՃՏ-ն արտաքին մատակարարներից, այն պետք է օրինակ՝ գնումների ընթացակարգի միջոցով ապահովի, որ գործարկվի միայն տվյալների՝ ներկառուցված և լռելյայն պաշտպանության սկզբունքների վրա կառուցված ԴՃՏ-ն[65]: Սա նաև ենթադրում է, որ ԴՃՏ-ի գործունեության թափանցիկությունը չի սահմանափակվում առևտրային գաղտնիքների կամ մտավոր սեփականության իրավունքի վերաբերյալ պահանջներով:

3.2.5.5 25-րդ հոդված. գրանցամատյանի վարումը

101. ԻԿՀ-ով նախատեսվում են հսկողի կամ մշակողի կողմից մշակման օրինականությունն ապացուցող և տվյալների ամբողջականությունն ու անվտանգությունն ապահովող տարբեր մեթոդներ: Այս առումով, համակարգի գրանցամատյանները շատ օգտակար գործիք են և կարևոր երաշխիք՝ ինչպես ներքին (այսինքն՝ ինքնամշտադիտարկում), այնպես էլ արտաքին վերահսկող մարմինների, ինչպես օրինակ՝ տվյալների պաշտպանության մարմինների կողմից մշակման օրինականությունն ստուգելու համար: Համաձայն ԻԿՀ 25-րդ հոդվածի՝ ավտոմատ մշակման համակարգերում պետք է պահվեն առնվազն հետևյալ մշակման գործողությունների գրանցամատյանները՝ հավաքում, փոփոխություն, քննարկում, բացահայտում, այդ թվում՝ փոխանցումներ, համադրում և ոչնչացում:

---

[62] Լրացուցիչ տեղեկությունների համար տե՛ս Տվյալների պաշտպանության ազդեցության գնահատման (ՏՊԱԳ), ինչպես նաև մշակման «բարձր ռիսկի հանգեցնելու հավանականությունը» որոշելու վերաբերյալ Տվյալների պաշտպանության ազդեցության գնահատման WP248 rev.01 ուղեցույցը:

[63] Տե՛ս օրինակ՝ ISO/IEC 24745 ստանդարտը. Տեղեկատվական անվտանգություն, կիբերանվտանգություն և գաղտնիության պաշտպանություն. կենսաչափական տեղեկությունների պաշտպանություն:

[64] Տե՛ս ԻԿՀ 53-րդ ներածական դրույթը:

[65] Լրացուցիչ տեղեկությունների համար տե՛ս Տվյալների՝ ներկառուցված և լռելյայն պաշտպանության մասին ՏՊԵԽ-ի ուղեցույցը հետևյալ հասցեով՝ https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf:

Ավելին, քննարկումների և բացահայտումների գրանցամատյանները պետք է հնարավորություն ընձեռեն պարզելու այդ գործողությունների հիմնավորումը, ամսաթիվն ու ժամը, և, հնարավորության դեպքում, նույնականացնելու այն անձին, որը քննարկել կամ բացահայտել է անձնական տվյալները, ինչպես նաև պարզել այդ անձնական տվյալներ ստացողների ինքնությունը: Ավելին, դեմքի ճանաչման համակարգերի համատեքստում առաջակվում է վարել ներքոնշյալ լրացուցիչ մշակման գործողությունների գրանցամատյան (մասամբ ԻԿՀ 25-րդ հոդվածի շրջանակներից դուրս).

- վկայակոչման տվյալների շտեմարանի փոփոխություններ (ավելացում, ջնջում կամ թարմացում): Գրանցամատյանում պետք է պահվի համապատասխան (ավելացված, ջնջված կամ թարմացված) պատկերի կրկնօրինակը, երբ այլ կերպ հնարավոր չէ ստուգել մշակման գործողությունների օրինականությունը կամ արդյունքը.

- նույնականացման կամ ստուգման փորձեր, այդ թվում՝ արդյունքի և վստահության գնահատական: Պետք է կիրառվի խիստ նվազագույնի հասցնելու սկզբունքը, որպեսզի վկայակոչման պատկերի փոխարեն գրանցամատյաններում պահվի վկայակոչման տվյալների շտեմարանից միայն պատկերի նույնականացուցիչը: Անհրաժեշտ է խուսափել մուտքային կենսաչափական տվյալների գրանցումից, եթե չկա դրա անհրաժեշտությունը (օրինակ՝ միայն համընկնման դեպքերում).

- նույնականացման կամ ստուգման փորձ կատարելու համար դիմած օգտատիրոջ նույնականացման քարտ.

- համակարգերի գրանցամատյաններում պահվող ցանկացած անձնական տվյալ ենթակա է խիստ նպատակային սահմանափակումների (օրինակ՝ աուդիտ) և չպետք է օգտագործվի այլ նպատակներով (օրինակ՝ դեռևս ճանաչում/ստուգում կատարելու նպատակով, այդ թվում՝ վկայակոչման տվյալների շտեմարաններից ջնջված պատկերի): Անհրաժեշտ է կիրառել անվտանգության միջոցներ՝ գրանցամատյանների ամբողջականությունն ապահովելու համար, միաժամանակ առաջարկվում է կիրառել ավտոմատ մշտադիտարկման համակարգեր՝ գրանցամատյանների սխալ կիրառումը հայտնաբերելու նպատակով: Վկայակոչման տվյալների շտեմարանների գրանցամատյանների դեպքում անվտանգության միջոցները պետք է համարժեք լինեն վկայակոչման տվյալների շտեմարանի անվտանգության միջոցներին՝ դեմքի պատկերների պահպանման դեպքում: Անհրաժեշտ է ներդնել նաև ավտոմատ պրոցեսներ, որոնք կապահովեն գրանցամատյաններում տվյալների պահպանման ժամկետի կատարումը:

3.2.5.6 4(4) հոդված. հաշվետվողականությունը

102. Հսկողը պետք է կարողանա ապացուցել մշակման համապատասխանությունը ԻԿՀ 4 (1)-(3) հոդվածի սկզբունքներին, տե՛ս 4(4) հոդվածը: Այս առումով չափազանց կարևոր են համակարգի կանոնակարգված ու ակտուալ փաստաթղթավորումը (այդ թվում՝ թարմացումները, արդիականացումները և ալգորիթմների ուսուցումը), տեխնիկական և կազմակերպչական միջոցները (այդ թվում՝ համակարգի աշխատանքի մշտադիտարկումը և մարդու հնարավոր միջամտությունը) և անձնական տվյալների մշակումը: Մշակման օրինականությունն ապացուցելու համար հատկապես կարևոր տարր է ԻԿՀ 25-րդ հոդվածի համաձայն (տե՛ս 3.2.5.5 բաժինը) գրանցամատյանի վարումը: Հաշվետվողականության սկզբունքը վերաբերում է ոչ միայն համակարգին ու մշակմանը, այլ նաև ընթացակարգային

երաշխիքների փաստաթղթավորմանը, ինչպիսիք են անհրաժեշտության և համաչափության գնահատումները, ՏՊԱԳ-ները, ինչպես նաև ներքին խորհրդակցությունները (օրինակ՝ ղեկավարության կողմից նախագծի կամ վստահության գնահատականի արժեքների վերաբերյալ ներքին որոշումների հաստատումը) և արտաքին խորհրդակցությունները (օրինակ՝ ՏՊՄ-ն): Այս առումով II հավելվածը ներառում է մի շարք տարրեր:

3.2.5.7 47-րդ հոդված. արդյունավետ վերահսկողությունը

103. Տվյալների պաշտպանության իրավասու մարմինների կողմից արդյունավետ վերահսկողությունը հանդիսանում է ԴՀՏ-ի կիրառման արդյունքում ազդեցություն կրած անձանց հիմնարար իրավունքների ու ազատությունների կարևորագույն երաշխիքներից մեկը: Միևնույն ժամանակ, տվյալների պաշտպանության յուրաքանչյուր իրավասու մարմնին անհրաժեշտ մարդկային, տեխնիկական և ֆինանսական ռեսուրսներ, տարածք և ենթակառուցվածքներ տրամադրելը նախապայման է իրենց առջև դրված խնդիրների արդյունավետ կատարման և լիազորությունների իրականացման համար[66]: Նույնիսկ առկա անձնակազմի թվից ավելի կարևոր են փորձագետների հմտությունները, որոնք պետք է զբաղվեն հարցերի շատ լայն շրջանակով՝ գործի քննությունից և ոստիկանության հետ համագործակցությունից մինչև մեծ տվյալների վերլուծություններ և արհեստական բանականություն: Հետևաբար, անդամ պետությունները պետք է ապահովեն, որ վերահսկող մարմինների ռեսուրսները համապատասխան և բավարար լինեն, որպեսզի վերջիններս կարողանան կատարել տվյալների սուբյեկտների իրավունքները պաշտպանելու իրենց լիազորությունը և ուշադիր հետևել այս առումով ցանկացած զարգացումների:[67]

[66] Տե՛ս «Տվյալների պաշտպանության իրավունքի կիրառման հրահանգի (ԵՄ) 2016/680 (ԻԿՀ) կիրառման և գործողության վերաբերյալ առաջին զեկույց» Հանձնաժողովի հաղորդագրությունը COM(2022) 364 վերջնական, էջ 3.4.1.

[67] Տե՛ս Եվրոպական հանձնաժողովի կողմից Տվյալների պաշտպանության օրենքի կատարման հրահանգի (ԻԿՀ) գնահատման մեջ ՏԽԵԽ-ի ներդրումը՝ 62-րդ հոդվածի համաձայն, պարբերություն 14, https://edpb.europa.eu/system/files/2021- 12/edpb contribution led review en.pdf:

4 ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ

104. Դեմքի ճանաչման տեխնոլոգիաների կիրառումն անքակտելիորեն կապված է զգալի թվով անձնական տվյալների մշակման, այդ թվում՝ հատուկ կատեգորիայի տվյալների հետ: Դեմքը և առավել լայն իմաստով կենսաչափական տվյալները մշտապես ու անվերապահորեն կապված են անձի ինքնության հետ: Հետևաբար, դեմքի ճանաչման տեխնոլոգիայի կիրառումն ուղղակի կամ անուղղակի ազդեցություն ունի Հիմնարար իրավունքների ԵՄ խարտիայում ամրագրված մի շարք հիմնարար իրավունքների ու ազատությունների վրա, որոնք կարող են դուրս գալ անձնական կյանքի անձեռնմխելիության և տվյալների պաշտպանության սահմաններից, ինչպիսիք են մարդու արժանապատվությունը, ազատ տեղաշարժը, հավաքների ազատությունը և այլն: Սա հատկապես կարևոր է իրավապահ գործունեության և քրեական արդարադատության ոլորտներում:
105. ՏՊԵԽ-ը գիտակցում է իրավապահ մարմինների կողմից հնարավոր լավագույն գործիքներից օգտվելու անհրաժեշտությունը՝ ահաբեկչական գործողություններ և այլ ծանր հանցագործություններ կատարողներին արագ բացահայտելու համար: Այնուամենայնիվ, այդ գործիքները պետք է օգտագործվեն կիրառելի իրավական շրջանակներին խիստ համապատասխան և միայն այն դեպքերում, երբ դրանք բավարարում են Խարտիայի 52(1) հոդվածով սահմանված՝ անհրաժեշտության և համաչափության պահանջները: Ավելին, թեև ժամանակակից տեխնոլոգիաները կարող են լինել լուծման մի մասը, այնուամենայնիվ, դրանք ոչ մի դեպքում միակ ճիշտ լուծումը չեն:

106. Կան դեմքի ճանաչման տեխնոլոգիաների կիրառման որոշ դեպքեր, որոնք անթույլատրելի բարձր ռիսկ են ներկայացնում անձանց և հասարակության համար («կարմիր գծեր»): Այդ պատճառով ՏՊԵԽ-ը և ՏՊԵՎՄ-ը հանդես են եկել դրանց ընդհանուր արգելքի կոչով[68]:

107. Մասնավորապես, հանրային տարածքներում անձանց հեռավար կենսաչափական նույնականացումն անձանց մասնավոր կյանք ներխուժելու մեծ ռիսկ է պարունակում և տեղ չունի ժողովրդավարական հասարակությունում, քանի որ իր բնույթով ենթադրում է զանգվածային հսկողություն: Նույն կերպ, ՏՊԵԽ-ն ԱԲ-ի հիման վրա աշխատող՝ դեմքի ճանաչման համակարգերը, որոնք կենսաչափական տվյալների հիման վրա դասակարգում են անձանց ըստ խմբերի՝ ելնելով էթնիկ պատկանելությունից, սեռից, ինչպես նաև քաղաքական կամ սեռական կողմնորոշումից, համարում է Խարտիայի հետ անհամատեղելի: Ավելին, ՏՊԵԽ-ը համոզված է, որ ֆիզիկական անձի էմոցիաները դուրս բերելու համար դեմքի ճանաչման կամ նմանատիպ տեխնոլոգիաների կիրառումը խիստ անցանկալի է և պետք է արգելվի, թերևս մի քանի պատշաճ կերպով հիմնավորված բացառություններով: Բացի այդ, ՏՊԵԽ-ը գտնում է, որ իրավապահ գործունեության համատեքստում անձնական տվյալների մշակումը, որը հիմնված է լայնամասշտաբ և ոչ ընտրողաբար անձնական տվյալների հավաքագրման վրա, օրինակ՝ առցանց հասանելի, այդ թվում՝ սոցիալական ցանցերով հանրամատչելի դարձված լուսանկարներն ու դեմքի նկարները ներբեռնելու միջոցով ձևավորված շտեմարանի վրա, որպես այդպիսին չի բավարարում Միության իրավունքով նախատեսված խիստ անհրաժեշտության պահանջը:

[68] Տե՛ս Արհեստական բանականության վերաբերյալ ներդաշնակեցված կանոններ սահմանող Եվրոպական պառլամենտի և Խորհրդի կանոնակարգի առաջարկի վերաբերյալ ՏՊԵԽ-ՏՊԵՎՄ-ի 5/2021 համատեղ կարծիքը (Արհեստական բանականության մասին ակտ), https://edpb.europa.eu/system/files/2021-06/edpb-edps joint opinion ai regulation en.pdf:

5 ՀԱՎԵԼՎԱԾՆԵՐ

Հավելված I. Աջակցության օրինակ

Հավելված II. ԻՄ-երում ԴՀՏ նախագծերի կառավարման առնչությամբ գործնական ուղղորդում

Հավելված III. Գործնական օրինակներ

ՀԱՎԵԼՎԱԾ I. ՍՑԵՆԱՐՆԵՐԻ ՆԿԱՐԱԳՐՈՒԹՅԱՆ ՁԵՎԱԹՈՒՂԹ

(**Սցենարներում հանդիպող հայեցակետերին վերաբերող տեղեկատվական աղյուսակներով**)

Մշակման նկարագրություն.

- Մշակման նկարագրություն, համատեքստ (հանցագործության հետ առնչություն), նպատակ

Տեղեկությունների աղբյուր.

- Տվյալների սուբյեկտների տեսակներ ☐ բոլոր քաղաքացիները ☐ դատապարտյալներ ☐ կասկածյալներ ☐ երեխաներ ☐ այլ խոցելի տվյալների սուբյեկտներ
- Պատկերի աղբյուր ☐ հանրային տարածքներ ☐ համացանց ☐ մասնավոր սուբյեկտ ☐ այլ անձինք ☐ այլ.....
- Հանցագործության հետ կապ ☐ ուղղակի ժամանակային ☐ անուղղակի ժամանակային ☐ ուղղակի աշխարհագրական ☐ անուղղակի աշխարհագրական ☐ պարտադիր չէ
- Տեղեկությունների հավաքագրման եղանակ ☐ հեռավար ☐ տաղավար կամ վերահսկվող միջավայր
- Այլ հիմնարար իրավունքների վրա ազդող համատեքստ
  ☐ ոչ
  այո, մասնավորապես՝ ☐ հավաքների ազատություն
  ☐ խոսքի ազատություն
  ☐ այլ.....
- Տվյալների սուբյեկտի մասին տեղեկություններ ստանալու լրացուցիչ աղբյուրների հնարավորություններ
  ☐ անձը հաստատող փաստաթուղթ ☐ հանրային հեռախոսի օգտագործում ☐ ավտոմեքենայի համարանիշ
  ☐ այլ .....

Վկայակոչման տվյալների շտեմարան (որի հետ համեմատվում են հավաքագրված տեղեկությունները).

- Կոնկրետություն ☐ ընդհանուր նշանակության տվյալների շտեմարաններ ☐ հանցանքի վայրի հետ կապված հատուկ տվյալների շտեմարաններ
- Նկարագրություն, թե ինչպես են այս վկայակոչման տվյալների շտեմարանները համալրվում (և իրավական հենքը)
- Տվյալների շտեմարանի նպատակի փոփոխություն (օր.՝ մասնավոր սեփականության անվտանգությունն առաջնային նպատակ էր)
  ☐ ԱՅՈ
  ☐ ՈՉ

Ալգորիթմ.

- Մշակման տեսակ ☐ 1-ը 1-ի հետ ստուգում (իսկորոշում)
  ☐ 1-ը շատի հետ նույնականացում
- Ճշտության նկատառումներ
- Պաշտպանության տեխնիկական միջոցներ

Արդյունք.

- Ազդեցություն ☐ ուղղակի (օրինակ՝ տվյալների սուբյեկտը կարող է ձերբակալվել, հարցաքննվել, խտրական վարքագիծ)
  ☐ անուղղակի (օգտագործվում է վիճակագրական մոդելների համար, տվյալների սուբյեկտների դեմ որևէ լուրջ իրավական հայց չի հարուցվել)
- Ավտոմատ որոշում ☐ԱՅՈ ☐ ՈՉ
- Պահպանման տևողություն

Իրավական վերլուծություն.

- Անհրաժեշտության և համաչափության վերլուծություն. նպատակ/հանցագործության ծանրություն/մշակման գործընթացում չներգրավված, սակայն դրանից ազդեցություն կրած անձանց թիվ
- Տվյալների սուբյեկտի համար նախնական տեղեկությունների տեսակ. ☐ հատուկ տարածք մուտք գործելիս
  - ☐ ԻՄ-ի կայքէջում ընդհանրապես
  - ☐ ԻՄ-ի կայքէջում՝ հատուկ մշակման համար
  - ☐ այլ.....
- Կիրառելի իրավական շրջանակ.
  - ☐ ԻԿՀ-ն մեծամասամբ փոխատեղվել է ազգային իրավունքի մեջ
  - ☐ ԻՄ-երի կողմից կենսաչափական տվյալների օգտագործման առնչությամբ ընդհանուր ազգային իրավունք
  - ☐ Այդ իրավասու մարմնի համար այդ մշակման (դեմքի ճանաչում) առնչությամբ հատուկ ազգային իրավունք
  - ☐ Այդ մշակման (ավտոմատացված որոշում) համար հատուկ ազգային իրավունք

Եզրակացություն.

Ընդհանուր նկատառումներ, թե արդյոք նկարագրված մշակումը համատեղելի է ԵՄ իրավունքի հետ (և իրավական նախադրյալների վերաբերյալ որոշ ակնարկներ)

ՀԱՎԵԼՎԱԾ II. ԻՄ-ԵՐՈՒՄ ԴՀՏ ՆԱԽԱԳԾԵՐԻ ԿԱՌԱՎԱՐՄԱՆ ԱՌՆՉՈՒԹՅԱՄԲ ԳՈՐԾՆԱԿԱՆ ՈՒՂՂՈՐԴՈՒՄ

Սույն հավելվածը որոշ լրացուցիչ գործնական ուղղորդում է տրամադրում իրավապահ մարմիններին (ԻՄ-եր), որոնք պլանավորում են նախաձեռնել Դեմքի ճանաչման տեխնոլոգիա (ԴՃՏ) ներառող նախագիծ: Այն տրամադրում է ավելի շատ տեղեկություններ կազմակերպչական և տեխնիկական միջոցների մասին, որոնք պետք է հաշվի առնել նախագծի գործարկման ընթացքում և չպետք է դիտարկվի որպես ձեռնարկվող քայլերի/միջոցառումների սպառիչ ցանկ: Այն պետք է դիտարկվի նաև Վիդեո սարքերի միջոցով անձնական տվյալների մշակման վերաբերյալ ՏՊԵՄ-ի ուղեցույցի[69] ինչպես նաև Արհեստական բանականության կիրառման վերաբերյալ ԵՄ/ԵՏՏ ցանկացած կանոնակարգի և ՏՊԵՄ-ի ուղեցույցի հետ միասին:

Սույն հավելվածն ուղղություն է տրամադրում այն ենթադրության հիման վրա, որ ԻՄ-երը կգնեն ԴՃՏ (որպես պատրաստի արտադրանք): Եթե ԻՄ-ն պլանավորում է մշակել ԴՃՏ (հետագայում ուսուցանել այն), ապա կիրառվում են լրացուցիչ պահանջներ դրա մշակման ժամանակ օգտագործվելիք՝ անհրաժեշտ ուսուցման, հսկիչ և փորձարկային տվյալների հավաքածուների և մշակման միջավայրի դերերի/միջոցների ընտրության համար: Նույն կերպ, պատրաստի արտադրանքը կարող է պահանջել լրացուցիչ հարմարեցումներ նախատեսված կիրառման համար, որի դեպքում պետք է բավարարվեն փորձարկման, հսկիչ և ուսուցողական տվյալների հավաքածուների ընտրության վերը նշված պահանջները:

Նույն ԻՄ-ի մաս լինելն ինքնին չի ապահովում կենսաչափական տվյալներին լիարժեք հասանելիություն: Ինչպես ցանկացած այլ կատեգորիայի անձնական տվյալների դեպքում, այնպես էլ հատուկ իրավական հիմքի հիման վրա իրավապահ գործունեության որոշ նպատակով հավաքագրված կենսաչափական տվյալները չեն կարող օգտագործվել առանց համապատասխան իրավական հիմքի՝ այլ իրավապահ նպատակների համար (2016/680 հրահանգի (ԵՄ) 4(2) հոդված (ԻԿՀ)): Նաև, ԴՃՏ գործիքի մշակումը/ուսուցումը համարվում է այլ նպատակ, և անհրաժեշտ է գնահատել, թե արդյոք տեխնոլոգիայի ցածր կատարողականի պատճառով տվյալների սուբյեկտների վրա ազդեցությունից խուսափելու համար դրա կատարողականը գնահատելու/տեխնոլոգիան ուսուցանելու նպատակով կենսաչափական տվյալների մշակումն անհրաժեշտ ու համաչափ է՝ հաշվի առնելով մշակման նախնական նպատակը:

1. ԴԵՐԵՐԸ ԵՎ ՊԱՐՏԱԿԱՆՈՒԹՅՈՒՆՆԵՐԸ

Երբ ԻՄ-ն կիրառում է ԴՃՏ-ն՝ ԻԿՀ գործողության շրջանակում գտնվող իր խնդիրների կատարման համար (քրեական իրավախախտումների կանխում, քննություն, բացահայտում կամ հետապնդում և այլն՝ ԻԿՀ 3-րդ հոդվածի համաձայն), այն կարող է համարվել հսկող ԴՃՏ-ի համար: Այնուամենայնիվ, ԻՄ-երը կազմված են մի քանի բաժիններից/դեպարտամենտներից, որոնք կարող են ներգրավվել այս մշակման գործընթացում՝ կա՛մ ԴՃՏ-ի կիրառման պրոցեսը սահմանելով, կա՛մ այն գործնականում կիրառելով: Ելնելով այս տեխնոլոգիայի առանձնահատկություններից՝ տարբեր բաժիններ կարող են ներգրավվել կա՛մ դրա կատարողականի գնահատումներին աջակցելու, կա՛մ դրա հետագա ուսուցման համար:

ԴՀՏ ներառող նախագծում կան ԻՄ-երից մի շարք շահագրգիռ կողմեր[70], որոնց ներգրավումը կարող է անհրաժեշտ լինել.

- բարձրագույն ղեկավարություն, որը ռիսկերը պոտենցիալ օգուտների հետ հավասարակշռելուց հետո հաստատում է նախագիծը.
- ԻՄ-ի ՏՊՊ և (կամ) իրավաբանական դեպարտամենտ, որն աջակցում է որոշ ԴՀՏ նախագծերի իրականացման օրինականությունը գնահատելու գործընթացում, աջակցում է ՏՊԱԳ-ի իրականացման հարցում, ապահովում է տվյալների սուբյեկտների իրավունքների նկատմամբ հարգանքն ու դրանց իրացումը.
- պրոցեսների պատասխանատու, որը հանդես է գալիս որպես իրավասու ԻՄ-ում նախագիծը մշակելու համար պատասխանատու հատուկ բաժին և որոշում է ԴՀՏ նախագծի մանրամասները, այդ թվում՝ համակարգի կատարողականի պահանջները, արդարության համապատասխան չափանիշը, սահմանում է վստահության գնահատականը[71], կողմնակալության ընդունելի շեմերը, բացահայտում է այն պոտենցիալ ռիսկերը, որոնք ներկայացնում է ԴՀՏ նախագիծն անձանց իրավունքների ու ազատությունների համար (խորհրդակցելով նաև ՏՊՊ-ի և ՏՏ ԱԲ-ի և (կամ) տվյալագիտության դեպարտամենտի հետ (տե՛ս ստորև), և դրանք ներկայացնում բարձրագույն ղեկավարությանը: Պրոցեսների պատասխանատուն նաև կխորհրդակցի վկայակոչման տվյալների շտեմարանի կառավարչի հետ, մինչև ԴՀՏ նախագծի մանրամասները որոշելը՝ հասկանալու համար վկայակոչման տվյալների շտեմարանի ինչպես կիրառման նպատակը, այնպես էլ դրա տեխնիկական մանրամասները: Գնված ԴՀՏ-ի վերաուսուցման դեպքում պրոցեսների պատասխանատուն նույնպես պատասխանատու կլինի ուսուցման տվյալների հավաքածուի ընտրության համար: Որպես նախագծի մանրամասները մշակելու և որոշելու գործառույթներով օժտված բաժին՝ պրոցեսների պատասխանատուն է պատասխանատու ՏՊԱԳ-ի իրականացման համար.

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal- data-through-video_en:

[70] Հետևյալ դերերը բնութագրում են ԴՀՏ նախագծի տարբեր շահագրգիռ կողմերին և նրանց պարտականությունները: Թեև այս հավելվածում դերերը նկարագրելու համար կիրառվող լեզուն հստակ չէ, այնուամենայնիվ, յուրաքանչյուր ԻՄ պետք է սահմանի և նշանակի նմանատիպ դերեր՝ ըստ իր կազմակերպության: Կարող են լինել դեպքեր, երբ բաժինը կատարում է մեկից ավելի դերեր, օրինակ՝ պրոցեսների պատասխանատուի և վկայակոչման տվյալների շտեմարանի կառավարչի կամ պրոցեսների պատասխանատու և ՏՏ ԱԲ և (կամ) տվյալագիտության դեպարտամենտի դերեր (եթե պրոցեսների պատասխանատուի բաժինն ունի բոլոր անհրաժեշտ տեխնիկական գիտելիքները):

[71] Վստահության գնահատականը կանխատեսման վստահության մակարդակն է (համընկնում) հավանականության ձևով: Օր.՝ համեմատելով երկու մոդելները՝ կա 90% վստահություն, որ դրանք պատկանում են նույն անձին: Վստահության գնահատականը տարբերվում է ԴՀՏ-ի կատարողականից, սակայն այն ազդում է կատարողականի վրա: Որքան բարձր է վստահության շեմը, այնքան քիչ են կեղծ դրական արդյունքները և ավելի շատ են կեղծ բացասականները ԴՀՏ-ի արդյունքներում:

- ՏՏ ԱԲ-ի և (կամ) տվյալագիտության դեպարտամենտ, որն աջակցում է ՏՊԱԳ-ի իրականացման հարցում, բացատրում է համակարգի արդյունավետությունը, արդարությունը[72] և պոտենցիալ կողմնակալությունը գնահատելու համար առկա չափանիշները, ներդնում է տեխնոլոգիան և պաշտպանության տեխնիկական միջոցները՝ կանխելու համար հավաքված տվյալներին չթույլատրված հասանելիությունը, կիբերհարձակումները և այլն: Գնված ԴՃՏ-ի վերաուսուցման դեպքում ՏՏ ԱԲ-ի կամ տվյալագիտության դեպարտամենտը կուսուցանի համակարգը՝ պրոցեսների պատասխանատուի կողմից տրված ուսուցման տվյալների հավաքածուի հիման վրա: Այս դեպարտամենտը պատասխանատու կլինի նաև պրոցեսների պատասխանատուների կողմից համատեղ հայտնաբերված ռիսկերը նվազեցնելուն ուղղված միջոցների մշակման համար (օր.՝ ԱԲ-ի հատուկ ռիսկերը, ինչպիսիք են մոդելի կիրառության վրա հարձակումները).

- վերջնական օգտատերեր (օրինակ՝ ոստիկանության ծառայողներ դեպքի վայրում կամ դատաբժշկական լաբորատորիաներում), որոնք իրականացնում են տվյալների շտեմարանի հետ համեմատություն, քննադատաբար վերանայում են արդյունքները՝ հաշվի առնելով նախկին ապացույցները և հետադարձ կապ տրամադրում պրոցեսների պատասխանատուին կեղծ դրական արդյունքների և հնարավոր խտրականության նշանների առնչությամբ.

- վկայակոչման տվյալների շտեմարանի կառավարիչ. իրավասու ԻՄ-ում հատուկ բաժին, որը պատասխանատու է վկայակոչման տվյալների շտեմարանի կուտակման և կառավարման համար, այսինքն՝ տվյալների շտեմարան, որի հետ համեմատվելու են պատկերները, ինչպես նաև սահմանված պահպանման ժամկետից հետո դեմքի պատկերների ջնջման համար: Այդ տվյալների շտեմարանը կարող է ստեղծվել հատուկ նախատեսված ԴՃՏ նախագծի համար կամ կարող է նախապես գոյություն ունենալ՝ համատեղելի նպատակներով: Վկայակոչման տվյալների շտեմարանի կառավարիչը պատասխանատու է որոշելու, թե երբ և ինչ հանգամանքներում կարող են պահվել դեմքի պատկերները, ինչպես նաև սահմանել դրանց պահպանման պահանջները (ըստ ժամանակի կամ այլ չափանիշների):

Քանի որ ԴՃՏ-ի գործարկման և կիրառման տարբերակների մեծ մասը պարունակում են տվյալների սուբյեկտի իրավունքների ու ազատությունների համար ներհատուկ բարձր ռիսկ, Տվյալների պաշտպանության վերահսկող մարմինը նույնպես պետք է ներգրավվի ԻԿՀ 28-րդ հոդվածով նախատեսված նախնական խորհրդակցության համատեքստում:

2. ՄԵԿՆԱՐԿ/ԴՃՏ ՀԱՄԱԿԱՐԳԻ ԳՆՈՒՄԻՑ ԱՌԱՋ

ԻՄ-ում պրոցեսների պատասխանատուն նախ պետք է հստակ պատկերացում ունենա ԴՃՏ-ի (կիրառման տարբերակ/ների) կիրառումն ապահովող պրոցեսի/ների մասին և ապահովի, որ նախատեսված կիրառման տարբերակը հիմնավորելու համար առկա է իրավական հիմք: Դրա հիման վրա այն պետք է.

- ֆորմալ առումով նկարագրի կիրառման տարբերակը: Անհրաժեշտ է նկարագրել լուծում պահանջող խնդիրը և ԴՃՏ-ի միջոցով խնդրի լուծման եղանակը, ինչպես նաև այն պրոցեսի (առաջադրանքի) ամփոփ նկարագիրը, որում այն կկիրառվի: Այս առումով ԻՄ-երը պետք է առնվազն փաստաթղթավորեն հետևյալը[73].
- պրոցեսի ընթացքում գրանցված անձնական տվյալների կատեգորիաները.
- ԴՃՏ-ի կիրառման խնդիրներն ու կոնկրետ նպատակները, այդ թվում՝

համընկնումից հետո տվյալների սուբյեկտի համար հնարավոր հետևանքները.
- դեմքի պատկերները հավաքագրելու ժամանակը և եղանակը (այդ թվում՝ այս հավաքագրման համատեքստի մասին տեղեկությունները, օրինակ՝ օդանավակայանում նստեցման ելքերի մոտ, այն խանութից դուրս անվտանգության տեսախցիկների կողմից կատարված տեսագրությունները, որտեղ կատարվել է հանցագործությունը և այլն, ինչպես նաև տվյալների սուբյեկտների կատեգորիաները, որոնց կենսաչափական տվյալները մշակվում են).
- այն տվյալների շտեմարանը, որի հետ համեմատվելու են պատկերները (վկայակոչման տվյալների շտեմարան), ինչպես նաև այն տեղեկությունները, թե ինչպես է այն ստեղծվել, դրա չափը և այն կենսաչափական տվյալների որակը, որն այն պարունակում է.
- ԻՄ դերակատարները, որոնք իրավասու կլինեն օգտագործել ԴՃՏ համակարգը և գործել դրա հիման վրա իրավապահ գործունեության համատեքստում (նրանց պրոֆիլները և հասանելիության իրավունքները պետք է սահմանվեն պրոցեսների պատասխանատուի կողմից).
- մուտքային տվյալների պահպանման նախատեսվող ժամկետը կամ այն պահը, որով կորոշի այդ ժամկետի ավարտը (օրինակ՝ քրեական վարույթի կարճումը կամ դադարեցումը՝ ազգային դատավարական իրավունքին համապատասխան, որի համար դրանք ի սկզբանե հավաքվել են), ինչպես նաև ցանկացած հետագա գործողություն (այդ տվյալների ջնջում, անանունացում և օգտագործում վիճակագրական կամ հետազոտական նպատակներով և այլն).
- գրանցամատյանների ներդնում և գրանցամատյանների ու պահվող փաստաթղթերի հասանելիություն.
- կատարողականի չափանիշներ (օր.՝ ճշտություն, ճշգրտություն, լրիվությունը, F1 չափողականություն) և դրանց նվազագույն ընդունելի շեմեր.[74]
- գնահատում այն մասին, թե որ ժամանակաշրջանում/առիթով քանի մարդու տվյալներ են մշակվելու ԴՃՏ-ով.
- <u>իրականացնի անհրաժեշտության և համաչափության գնահատում</u>[75]: Այն փաստը, որ այս տեխնոլոգիան գոյություն ունի, չպետք է լինի այն կիրառելու շարժիչ ուժը: Պրոցեսների պատասխանատուն նախ պետք է գնահատի, թե արդյոք առկա է նախատեսված մշակման համար համապատասխան իրավական հիմք: Այս նպատակով անհրաժեշտ է խորհրդակցել ՏՊՊ-ի և իրավաբանական ծառայության հետ: ԴՃՏ-ն գործարկելու շարժիչ ուժը պետք է լինի ԻՄ-երի կողմից կոնկրետ սահմանված խնդրի համար անհրաժեշտ և համաչափ լուծում լինելու հանգամանքը: Սա պետք է գնահատվի՝ ըստ հանցագործության նպատակի/ծանրության/չներգրավված, սակայն ԴՃՏ համակարգի կողմից ազդեցություն կրած անձանց թվի: Օրինականությունը գնահատելու համար առնվազն պետք է դիտարկել հետևյալ՝ ԻԿՀ-ն[76], ՏՊԸԿ-ն[77] [78], ԱԲ-ի վերաբերյալ ցանկացած գործող իրավական շրջանակ[79] և տվյալների պաշտպանության հարցերով վերահսկող մարմինների կողմից տրամադրված բոլոր ուղեկցող ուղեցույցները (ինչպես օրինակ՝ Վիդեո սարքերի միջոցով անձնական տվյալների մշակման վերաբերյալ ՏՊԵԽ-ի 3/2019 ուղեցույցը[80]): ԵՄ օրենսդրության մաս կազմող այդ ակտերը պետք է միշտ հաստատված լինեն կիրառելի ազգային պահանջներով, հատկապես քրեական դատավարության իրավունքի ոլորտում: Համաչափության գնահատմամբ պետք է բացահայտվեն տվյալների սուբյեկտների հիմնարար իրավունքները, որոնք կարող են շոշափվել (բացի անձնական կյանքի անձեռնմխելիությունից և տվյալների պաշտպանությունից): Այն պետք է նաև նկարագրի և դիտարկի ցանկացած սահմանափակում (կամ սահմանափակումների բացակայություն), որը կիրառվում է

ԴՁՏ համակարգի կիրառման տարբերակի նկատմամբ: Օրինակ, արդյոք համակարգը կաշխատի անընդհատ կամ ժամանակավորապես, և արդյոք այն կսահմանափակվի աշխարհագրական տարածքով.

- <u>իրականացնի տվյալների պաշտպանության ազդեցության գնահատում (ՏՊԱԳ)</u>[81]: Անհրաժեշտ է իրականացնել ՏՊԱԳ, քանի որ ԴՁՏ-ի գործարկումն իրավապահ գործունեության ոլորտում կարող է հանգեցնել անձանց իրավունքների ու ազատությունների բարձր ռիսկի[82]: ՏՊԱԳ-ը պետք է մասնավորապես պարունակի՝ մշակման նախատեսվող գործողությունների ընդհանուր նկարագիրը[83], տվյալների սուբյեկտների իրավունքների ու ազատությունների համար ռիսկերի գնահատումը[84], այդ ռիսկերը հասցեագրելուն ուղղված միջոցները, երաշխիքները, անվտանգության միջոցներն ու մեխանիզմները՝ անձնական տվյալների պաշտպանությունն ապահովելու և համապատասխանությունն ապացուցելու համար: ՏՊԱԳ-ը շարունակական գործընթաց է, ուստի մշակման ցանկացած նոր տարր պետք է ավելացվի, իսկ ռիսկերի գնահատումը պետք է թարմացվի նախագծի յուրաքանչյուր փուլում.
- <u>ստանա հաստատում բարձրագույն ղեկավարությունից</u>՝ բացատրելով տվյալների սուբյեկտների իրավունքների ու ազատությունների համար ռիսկերը (կիրառման տարբերակից և տեխնոլոգիայից), ինչպես նաև ռիսկերի արձագանքման համապատասխան ծրագրերը:

---

[72] Արդարությունը կարող է սահմանվել որպես անարդար, անօրինական խտրականության, ինչպիսին է գենդերային կամ ռասայական կողմնակալության բացակայություն:

[73] I հավելվածում ներկայացված է այն տարրերի ցանկը, որոնք օգնում են հսկողին նկարագրել ԴՁՏ-ի կիրառման տարբերակը:

[74] Գոյություն ունեն ԴՁՏ համակարգի կատարողականը գնահատելու տարբեր չափանիշներ: Յուրաքանչյուր չափանիշ համակարգի արդյունքների վերաբերյալ տալիս է տարբեր պատկերացում, և որպեսզի այն բավարար պատկերացում տա, թե արդյոք ԴՁՏ համակարգը լավ է կատարում իր առջև դրված խնդիրը, թե ոչ, կախված է դրա կիրառման տարբերակից: Եթե խնդիրը դեմքի ճիշտ համընկնման բարձր տոկոսներ ապահովելն է, ապա կարող են կիրառվել այնպիսի չափանիշներ, ինչպիսիք են ճշգրտությունը և լրիվությունը: Այնուամենայնիվ, այս չափանիշները չեն, որ գնահատում են, թե որքան լավ է ԴՁՏ-ն մշակում բացասական օրինակներ (քանի օրինակի դեպքում է արձանագրվել համակարգի կողմից սխալ համընկնում): Պրոցեսների պատասխանատուն SS ԱԲ-ի և տվյալագիտության դեպարտամենտի աջակցությամբ պետք է կարողանա սահմանել կատարողականի պահանջները, այնուհետև դրանք արտահայտել ամենահարմար չափանիշի մեջ՝ ըստ ԴՁՏ-ի կիրառման տարբերակի:

[75] Անհրաժեշտությունը գնահատելու հետագա քայլերը կարող են դիտարկվել՝ կապված համակարգի հարմարեցման և կիրառման հետ, ուստի կիրառման տարբերակի նկարագրությունը կարող է նաև փոքր-ինչ փոխվել անհրաժեշտության և համաչափության գնահատման ընթացքում:

[76] Քրեական իրավախախտումների կանխման, քննության, հայտնաբերման կամ հետապնդման նպատակներով իրավասու մարմինների կողմից անձնական տվյալների մշակման մասով ֆիզիկական անձանց պաշտպանության մասին Եվրոպական պառլամենտի և Խորհրդի 2016 թվականի ապրիլի 27-ի 2016/680 հրահանգ (ԵՄ):

[77] Անձնական տվյալների մշակման մասով ֆիզիկական անձանց պաշտպանության, ինչպես նաև այդ տվյալների ազատ տեղաշարժի մասին Եվրոպական պառլամենտի և Խորհրդի 2016 թվականի ապրիլի 27-ի 2016/679 կանոնակարգ (ԵՄ):

[78] Այն դեպքերում, երբ ԴՁՏ-ի կիրառությունը հետազոտելու նպատակով նախաձեռնված գիտական նախագծի շրջանակներում անհրաժեշտություն կլինի մշակել անձնական տվյալներ, սակայն այդ մշակումը չի կարգավորվի ԻԿՀ 4(3) հոդվածով, ընդհանուր առմամբ, կիրառելի կլինի

ՏՊԸԿ-ն (ԻԿՀ 9(2) հոդված): Պիլոտային նախագծերի դեպքում, որոնց կիետևեն իրավապահ մարմինների գործողությունները, դեռևս կիրառելի կլինի ԻԿՀ-ն:

[79] Օրինակ՝ կա ԱՐՀԵՍՏԱԿԱՆ ԲԱՆԱԿԱՆՈՒԹՅԱՆ ՄԱՍԻՆ ՆԵՐԴԱՇՆԱԿԵՑՎԱԾ ԿԱՆՈՆՆԵՐ ՍԱՀՄԱՆՈՂ (ԱՐՀԵՍՏԱԿԱՆ ԲԱՆԱԿԱՆՈՒԹՅԱՆ ՄԱՍԻՆ ԱԿՏ) ԵՎ ՄԻՈՒԹՅԱՆ ՕՐԵՆՍԴՐԱԿԱՆ ԱԿՏԵՐԸ ՓՈՓՈԽՈՂ ԵՎՐՈՊԱԿԱՆ ՊԱՌԼԱՄԵՆՏԻ ԵՎ ԽՈՐՀՐԴԻ ԿԱՆՈՆԱԿԱՐԳ մշակելու մասին առաջարկություն, սակայն այն դեռևս չի ընդունվել որպես կանոնակարգ:

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en:

[81] ՏՊԱԳ-ների վերաբերյալ լրացուցիչ ուղղորդում կարելի է գտնել 2016/679 կանոնակարգի նպատակներով Տվյալների պաշտպանության ազդեցության գնահատման (ՏՊԱԳ), ինչպես նաև մշակման «բարձր ռիսկի հանգեցնելու հավանականությունը» որոշելու վերաբերյալ Տվյալների պաշտպանության ազդեցության գնահատման ուղեցույցում, WP 248 rev.01, հասանելի է հետևյալ հասցեով՝ https://ec.europa.eu/newsroom/article29/items/611236 և ՏՊԵԿՄ-ի Տեղում հաշվետվողականության գործիքակազմ, մաս II, հասանելի է հետևյալ հասցեով՝ https://edps.europa.eu/node/4582 en:

[82] ԴՁՏ-ն, կախված կիրառման տարբերակից, կարող է ընկնել հետևյալ չափանիշների ներքո, որոնք հանգեցնում են բարձր ռիսկի մշակման (ՏՊԱԳ-ի վերաբերյալ ուղեցույց, WP 248 rev.01): Համակարգված մշտադիտարկում, մեծ մասշտաբով տվյալների մշակում, տվյալների հավաքածուների համապատասխանեցում կամ համակցում, նորարարական կիրառում կամ նոր տեխնոլոգիական կամ կազմակերպչական լուծումներ:

[83] Մշակման նկարագրությունը, ինչպես նաև վերևում նշված քայլերում արդեն իսկ նկարագրված անհրաժեշտության ու համաչափության գնահատումը նույնպես կազմում են ՏՊԱԳ-ի մաս՝ բացի ռիսկերի գնահատումից: Հարկ եղած դեպքում անձնական տվյալների հոսքերի առավել մանրամասն նկարագրությունը կներկայացվի ՏՊԱԳ-ում:

[84] Տվյալների սուբյեկտների համար ռիսկերի վերլուծությունը պետք է ներառի դեմքի պատկերների համեմատման վայրի հետ (տեղական/հեռավար) կապված ռիսկերը, մշակողների/ենթամշակողների հետ կապված ռիսկերը, ինչպես նաև կիրառվելու դեպքում մեքենայական ուսուցմանը հատուկ ռիսկերը (օրինակ՝ տվյալների թունավորում, հակառակորդ օրինակներ):

3. ԳՆՈՒՄՆԵՐԻ ԸՆԹԱՑՔՈՒՄ ԵՎ ՄԻՆՉԵՎ ԴՃՏ-ի ԳՈՐԾԱՐԿՈՒՄԸ

- <u>որոշի ԴՃՏ-ն (ալգորիթմն) ընտրելու չափանիշները</u>: Պրոցեսների պատասխանատուն պետք է որոշի ալգորիթմն ընտրելու չափանիշները՝ ՏՏ ԱԲ-ի և (կամ) տվյալագիտության դեպարտամենտի օգնությամբ: Գործնականում դրանք պետք է ներառեն արդարության և կատարողականի չափանիշները, որոնք որոշվել են կիրառման տարբերակի նկարագրության մեջ: Այդ չափանիշները պետք է ներառեն նաև այն տվյալներին վերաբերող տեղեկությունները, որոնցով ուսուցանվել է ալգորիթմը: Ուսուցման, փորձարկային և հսկիչ հավաքածուն պետք է բավարար չափով ներառի այն տվյալների սուբյեկտների բոլոր բնութագրերի նմուշները, որոնց տվյալները ենթակա են ԴՃՏ-ով մշակման (օրինակ՝ տարիքը, սեռը և ռասան)՝ կանխակալությունը նվազեցնելու նպատակով: ԴՃՏ մատակարարը պետք է տրամադրի տեղեկություններ և չափանիշներ ԴՃՏ-ի ուսուցման, փորձարկային և հսկիչ տվյալների հավաքածուների վերաբերյալ և նկարագրի հնարավոր անօրինական խտրականությունն ու կողմնակալությունը չափելու և մեղմելու համար ձեռնարկված միջոցները: Պրոցեսների պատասխանատուն, հնարավորության դեպքում, պետք է ստուգի, թե արդյոք առկա է մատակարարի կողմից այդ տվյալների հավաքածուն օգտագործելու համար իրավական հիմք՝ ալգորիթմների ուսուցման նպատակով (հիմնվելով մատակարարի կողմից հանրամատչելի դարձված տեղեկությունների վրա): Նաև պրոցեսների պատասխանատուն պետք է ապահովի, որ ԴՃՏ մատակարարը կիրառի կենսաչափական տվյալների հետ կապված անվտանգության ստանդարտները, ինչպես օրինակ՝ ISO/IEC 24745 ստանդարտը, որն ուղղորդում է տրամադրում կենսաչափական տեղեկությունների պաշտպանության համար՝ պահպանման և փոխանցման ընթացքում գաղտնիության, ամբողջականության և վերականգնման/հետկանչման տարբեր պահանջների, ինչպես նաև կենսաչափական տեղեկությունների անվտանգ և գաղտնիության պահանջներին համապատասխանող կառավարման և մշակման համար պահանջների և ուղեցույցի համաձայն.
- <u>վերաուսուցանի ալգորիթմը (եթե կա դրա անհրաժեշտությունը)</u>: Պրոցեսների պատասխանատուն պետք է ապահովի, որ ԴՃՏ համակարգին ճիշտ կարգավորումներ տալը, մինչև դրա կիրառումն ավելի բարձր ճշտության հասնելու համար, նույնպես կազմում է գնված ծառայությունների մաս: Այն դեպքում, երբ ձեռք բերված ԴՃՏ համակարգի լրացուցիչ ուսուցումն անհրաժեշտ է ճշտության չափանիշին համապատասխանելու համար, պրոցեսների պատասխանատուն, բացի վերաուսուցման վերաբերյալ որոշում կայացնելուց, պետք է ՏՏ ԱԲ-ի և (կամ) տվյագիտության դեպարտամենտի օգնությամբ որոշի օգտագործման ենթակա համապատասխան, ներկայացուցչական տվյալների հավաքածուն և ստուգի այդ տվյալների օգտագործման օրինականությունը.
- <u>սահմանի համապատասխան երաշխիքներ</u>՝ անվտանգության, կողմնակալության և ցածր կատարողականի հետ կապված ռիսկերին արձագանքելու համար: Սա ներառում է ԴՃՏ-ի մշտադիտարկման պրոցեսի ստեղծումը դրա կիրառումից հետո (գրանցամատյանի վարում և հետադարձ կապ՝ արդյունքների ճշտության և արդարության համար): Բացի այդ, համոզվեք, որ որոշ մեքենայական ուսուցման և ԴՃՏ համակարգերին հատուկ ռիսկերը (օրինակ՝ տվյալների թունավորում, հակառակորդ օրինակներ, մոդելի ինվերսիա, սպիտակ տուփի հարձակումներ) հայտնաբերված, գնահատված և նվազեցված են: Պրոցեսների պատասխանատուն պետք է նաև սահմանի համապատասխան երաշխիքներ՝ ապահովելու համար վերաուսուցման տվյալների հավաքածուի մեջ ներառված կենսաչափական տվյալների նկատմամբ

կիրառվող տվյալների պահպանման պահանջների կատարումը.

- <u>փաստաթղթավորի ԴՁՏ համակարգը</u>: Սա պետք է ներառի ԴՁՏ համակարգի ընդհանուր նկարագրությունը, ԴՁՏ համակարգի տարրերի և դրա ստեղծման պրոցեսի մանրամասն նկարագրությունը, ԴՁՏ համակարգի մշտադիտարկման, գործունեության և հսկողության մասին մանրամասն տեղեկություններ և դրա ռիսկերի ու դրանց նվազեցման միջոցառումների մանրամասն նկարագրությունը: Այս փաստաթղթում ներառված տարրերը կներառեն նախորդ փուլերից ԴՁՏ համակարգի նկարագրության հիմնական տարրերը (տե՛ս վերևում), սակայն դրանք կավելացվեն կատարողականի մշտադիտարկման և համակարգում փոփոխություններ կատարելու, այդ թվում՝ ցանկացած տարբերակի թարմացումների և (կամ) վերաուսուցման հետ կապված տեղեկություններով.
- <u>մշակի օգտատիրոջ ձեռնարկներ՝ բացատրելով տեխնոլոգիան և կիրառման տարբերակները:</u> Այդ ձեռնարկներում պետք է հստակ կերպով ներկայացվեն ԴՁՏ-ի կիրառման բոլոր սցենարներն ու նախապայմանները.
- <u>տեխնոլոգիայի կիրառման թեմայով դասընթացներ կազմակերպի վերջնական օգտատերերի համար</u>: Այդ դասընթացների շրջանակներում պետք է բացատրվեն տեխնոլոգիայի հնարավորություններն ու սահմանափակումները, որպեսզի օգտատերերը կարողանան հասկանալ, թե ինչ հանգամանքներում է անհրաժեշտ այն կիրառել, և այն դեպքերը, երբ այն կարող է ոչ ճշգրիտ լինել: Այդ դասընթացները կօգնեն նաև նվազեցնել ալգորիթմի արդյունքը չստուգելու/քննադատելու հետ կապված ռիսկերը:
- <u>խորհրդակցի տվյալների պաշտպանության հարցերով վերահսկող մարմնի հետ՝</u> ԻԿՀ 28(1)(բ) հոդվածի համաձայն: <u>Տրամադրեք տեղեկություններ՝</u> ԻԿՀ 13-րդ հոդվածի համաձայն՝ տվյալների սուբյեկտներին մշակման և նրանց իրավունքների մասին տեղեկացնելու համար: Այդ ծանուցումները պետք է հասցեագրված լինեն տվյալների սուբյեկտներին համապատասխան լեզվով, որպեսզի նրանք կարողանան հասկանալ մշակումը և բացատրել տեխնոլոգիայի հիմնական տարրերը, այդ թվում՝ ճշտության ցուցանիշները, ուսուցման տվյալների հավաքածուները և ձեռնարկված միջոցները՝ խտրականությունից և ալգորիթմի ցածր ճշտությունից խուսափելու համար:

4. ԱՌԱՋԱՐԿՈՒԹՅՈՒՆՆԵՐԸ ԴՁՏ-Ի ԳՈՐԾԱՐԿՈՒՄԻՑ ՀԵՏՈ

- <u>ապահովի մարդու միջամտությունը և արդյունքների նկատմամբ վերահսկողությունը</u>: Երբեք մի ձեռնարկեք որևէ միջոց անձի նկատմամբ՝ հիմնվելով բացառապես ԴՁՏ-ի արդյունքի վրա (սա կենթադրի ԻԿՀ Ավտոմատացված անհատական որոշումների կայացում վերտառությամբ 11-րդ հոդվածի խախտում, որն իրավական կամ այլ նմանատիպ հետևանքներ ունի տվյալների սուբյեկտի համար): Համոզվեք, որ ԻՄ-ի աշխատողը ստուգում է ԴՁՏ-ի արդյունքները: Նաև համոզվեք, որ ԻՄ-ի ծառայություններից օգտվողները խուսափում են ավտոմատացման կողմնակալությունից՝ ուսումնասիրելով հակասական տեղեկությունները և քննադատաբար վիճարկելով տեխնոլոգիայի արդյունքները: Դրա համար կարևոր է վերջնական օգտատերերի շարունակական վերապատրաստումը և իրազեկվածության մակարդակի բարձրացումը, սակայն բարձրաստիճան ղեկավարությունը պետք է ապահովի, որ կան համապատասխան մարդկային ռեսուրսներ՝ արդյունավետ վերահսկողություն իրականացնելու համար: Սա պահանջում է, որ յուրաքանչյուր աշխատողի տրվի բավարար ժամանակ՝ տեխնոլոգիայի արդյունքները քննադատաբար

վիճարկելու համար: Արձանագրեք, չափեք և գնահատեք այնքանով, որքանով մարդու վերահսկողությունը փոխում ԴՃՏ-ի միջոցով կայացված սկզբնական որոշումը.

- մշտադիտարկի և հասցեագրի ԴՃՏ մոդելի դրեյֆը (արտադրողականության նվազում), երբ մոդելն արտադրական շղթայում է.
- ստեղծի պրոցես, որով կվերագնահատվի ռիսկերն ու անվտանգության միջոցները պարբերաբար և ամեն անգամ, երբ տեխնոլոգիան կամ կիրառման տարբերակը կրում են որևէ փոփոխություն.
- փաստաթղթավորի համակարգի ցանկացած փոփոխություն դրա կենսափուլի ամբողջ ընթացքում (օրինակ՝ արդիականացումներ, վերաուսուցում).
- ստեղծի պրոցես, ինչպես նաև համապատասխան տեխնիկական հնարավորություններ՝ տվյալների սուբյեկտների կողմից հասանելիություն ստանալու մասին դիմումները հասցեագրելու համար: Ցանկացած դիմում ներկայացվելուց առաջ պետք է առկա լինեն տվյալների արդյունահանման տեխնիկական հնարավորությունները, եթե անհրաժեշտություն լինի դրանք տրամադրել տվյալների սուբյեկտներին.
- համոզվի, որ առկա են տվյալների խախտումները հասցեագրելու ընթացակարգեր: Եթե տեղի ունենա անձնական տվյալների խախտում, որը ներառում է կենսաչափական տվյալներ, ռիսկերը, ամենայն հավանականությամբ, բարձր կլինեն: Այս դեպքում բոլոր ներգրավված օգտատերերը պետք է տեղյակ լինեն համապատասխան ընթացակարգերի մասին, որպեսզի հետևեն դրանց, ՏՊՊ-ն պետք է անհապաղ տեղեկացվի, իսկ տվյալների սուբյեկտները տեղեկացվեն դրա մասին:

ՀԱՎԵԼՎԱԾ III. ԳՈՐԾՆԱԿԱՆ ՕՐԻՆԱԿՆԵՐ

Կան դեմքի ճանաչման համակարգի կիրառման շատ տարբեր գործնական միջավայրեր և նպատակներ, օրինակ՝ վերահսկվող միջավայրերում, ինչպիսիք են սահմանային անցակետերը, ոստիկանության տվյալների շտեմարանների կամ տվյալների սուբյեկտի կողմից ակնհայտորեն հանրամատչելի դարձված անձնական տվյալների, ուղիղ ժամանակային ռեժիմում տեսախցիկի ժապավենի (ուղիղ ժամանակային ռեժիմում դեմքի ճանաչում) և այլնի արդյունքում հավաքագրված տվյալների հետ խաչաձև ստուգումը: Արդյունքում, անձնական տվյալների և այլ հիմնարար իրավունքների ու ազատությունների պաշտպանության համար ռիսկերը զգալիորեն տարբեր են կիրառման տարբեր դեպքերում: Անհրաժեշտության և համաչափության գնահատումը դյուրացնելու համար, որին պետք է նախորդի դեմքի ճանաչման տեխնոլոգիայի հնարավոր գործարկման վերաբերյալ որոշումը, գործող ուղեցույցում ներկայացվում է իրավապահ գործունեության ոլորտում ԴՃՏ-ի հնարավոր կիրառությունների ոչ ամբողջական ցանկը:

Ներկայացված և գնահատված սցենարները հիմնված են **հիպոթետիկ** իրավիճակների վրա և նպատակ ունեն մեկնաբանելու ԴՃՏ-ի որոշ կոնկրետ կիրառման տարբերակներ և աջակցություն ցուցաբերել յուրաքանչյուր առանձին դեպքի, ինչպես նաև ընդհանուր շրջանակի սահմանման համար: Դրանք սպառիչ չեն և չեն վնասում դեմքի ճանաչման տեխնոլոգիաների նախագծման, փորձարկման կամ ներդրման հետ կապված ազգային վերահսկող մարմնի կողմից ձեռնարկվող ցանկացած ընթացիկ կամ հետագա վարույթին: Այդ սցենարները ներկայացնելու նպատակը պետք է լինի միայն սույն փաստաթղթում արդեն իսկ տրված ուղղորդումը մեկնաբանելը՝ քաղաքականություն մշակողների, օրենսդիրների և իրավապահ մարմինների համար, դեմքի ճանաչման տեխնոլոգիաները մշակելու և ներդրումը նախատեսելու գործընթացում անձնական տվյալների պաշտպանության ոլորտում ԵՄ ընդհանուր օրենսդրության հետ լիարժեք համապատասխանությունն ապահովելու համար: Այս համատեքստում պետք է նկատի ունենալ, որ նույնիսկ ԴՃՏ-ի կիրառման նմանատիպ իրավիճակներում որոշ տարրերի առկայությունը կամ բացակայությունը կարող է հանգեցնել անհրաժեշտության և համաչափության գնահատման այլ արդյունքի:

1 ՍՑԵՆԱՐ 1

1.1. Նկարագիրը

Սահմանային հսկողության ավտոմատացված համակարգ, որը թույլ է տալիս ավտոմատացնել սահմանի հատումը՝ իսկորոշելով ԵՄ քաղաքացիների և սահմանային անցումով անցնող մյուս ճանապարհորդների էլեկտրոնային ճամփորդական փաստաթղթում պահվող կենսաչափական պատկերը և հաստատելով, որ ուղևորը փաստաթղթի օրինական սեփականատերն է:

Այդ ստուգումը/իսկորոշումը ներառում է միայն մեկը մեկի դեմքի ճանաչում և իրականացվում է վերահսկվող միջավայրում (օրինակ՝ օդանավակայանի էլեկտրոնային նստեցման ելքերում): Սահմանը հատող ճանապարհորդի կենսաչափական տվյալները հավաքվում են, երբ նրան հստակ առաջարկվում է նայել տեսախցիկին էլեկտրոնային նստեցման ելքերում և համեմատվում է հատուկ տեխնիկական պահանջներին համապատասխան տրված փաստաթղթի (անձնագրի, անձը հաստատող փաստաթղթի և այլ փաստաթղթերի) տվյալների հետ:

Միևնույն ժամանակ, եթե նման դեպքերում մշակումը սկզբունքորեն դուրս է ԻԿՀ գործողության շրջանակից, ապա ստուգման արդյունքը կարող է օգտագործվել նաև անձի (տառաթվային) տվյալների՝ իրավապահ մարմինների տվյալների շտեմարանների հետ համընկնումներ որոնելու համար՝ որպես սահմանային հսկողության մաս և այդպիսով կարող է հանգեցնել տվյալների սուբյեկտի համար զգալի իրավական հետևանք ունեցող գործողությունների, օրինակ՝ ձերբակալության՝ ՀՔԾ-ում ստացված ահազանգի հիման վրա: Հատուկ հանգամանքներում կենսաչափական տվյալները կարող են օգտագործվել նաև իրավապահ մարմինների տվյալների շտեմարաններում համընկնումներ որոնելու համար (նման դեպքում այս քայլում կիրականացվի 1-ը շատի հետ նույնականացում):

Կենսաչափական պատկերի մշակման արդյունքն ուղղակի ազդեցություն ունի տվյալների սուբյեկտի վրա. միայն հաջող ստուգման դեպքում է այն թույլ տալիս հատել սահմանը: Անհաջող նույնականացման դեպքում սահմանապահները պետք է երկրորդ ստուգում իրականացնեն՝ համոզվելու համար, որ տվյալների սուբյեկտը տարբերվում է անձը հաստատող փաստաթղթում պատկերված անձից:

ՀՔԾ կամ ազգային մակարդակով ահազանգի տրման դեպքում սահմանապահները պետք է իրականացնեն երկրորդ ստուգում և անհրաժեշտ հետագա ստուգումները, այնուհետև ձեռնարկեն ցանկացած անհրաժեշտ գործողություն, օրինակ՝ ձերբակալեն անձին, տեղեկացնեն համապատասխան մարմիններին:

Տեղեկությունների աղբյուր.

- Տվյալների սուբյեկտների տեսակներ. ☒ սահմանները հատող բոլոր անձինք
- Պատկերի աղբյուր. ☒ այլ (անձը հաստատող փաստաթուղթ)
- Հանցագործության հետ կապ. ☒ պարտադիր չէ
- Տեղեկությունների հավաքագրման եղանակ. ☒ տաղավար կամ վերահսկվող միջավայր
- Այլ հիմնարար իրավունքների վրա ազդող համատեքստ. այո, մասնավորապես՝ ☒ ազատ տեղաշարժի իրավունք ☒ ապաստանի իրավունք

Վկայակոչման տվյալների շտեմարան (որի հետ համեմատվում են հավաքագրված տեղեկությունները).

- Կոնկրետություն ☒ սահմանային հսկողության հետ կապված հատուկ տվյալների շտեմարաններ

Ալգորիթմ.

- Ստուգման տեսակ: ☒ 1-ը 1-ի հետ ստուգում (իսկորոշում)

Արդյունք.

- Ազդեցություն ☒ ուղղակի (տվյալների սուբյեկտին թույլատրվել կամ մերժվել է մուտքը)
- Ավտոմատ որոշում. ☒ այո

1.2. Կիրառելի իրավական շրջանակը

2004 թվականից ի վեր, Խորհրդի թիվ 2252/2004[85] կանոնակարգի (ԵՀ) համաձայն՝ անդամ պետությունների կողմից տրված անձնագրերն ու ճամփորդական մյուս փաստաթղթերը պետք է պարունակեն դեմքի կենսաչափական պատկերը, որը պահվում է փաստաթղթում ներկառուցված էլեկտրոնային չիպի մեջ:

Շենգենյան սահմանների մասին օրենսգրքով (ՇՍՕ)[86] սահմանվում են արտաքին սահմանների վրա անձանց ստուգումների պահանջները: ԵՄ քաղաքացիների և Միության իրավունքի համաձայն ազատ տեղաշարժի իրավունքից օգտվող այլ անձանց համար նվազագույն ստուգումները պետք է ներառեն նրանց ճամփորդական փաստաթղթերի ստուգումը՝ անհրաժեշտության դեպքում օգտագործելով տեխնիկական սարքերը: ՇՍՕ-ն

հետագայում փոփոխվել է 2017/2225[87] կանոնակարգով (ԵՄ), որը, ի թիվս այլնի, ներմուծել է «էլեկտրոնային նստեցման ելքեր», «սահմանների հսկման ավտոմատացված համակարգ» և «ինքնասպասարկման համակարգ» սահմանումները, ինչպես նաև սահմանային ստուգումներ իրականացնելու համար կենսաչափական տվյալների մշակման հնարավորությունը:

Հետևաբար, կարելի է ենթադրել, որ կա անձնական տվյալների մշակման այս ձևը թույլատրող հստակ և կանխատեսելի իրավական հիմք: Ավելին, իրավական դաշտն ընդունված է Միության մակարդակով և ուղղակիորեն կիրառելի է անդամ պետությունների նկատմամբ:

1.3. Անհրաժեշտությունը և համաչափությունը. հանցագործության նպատակը/ծանրությունը

Սահմանային ավտոմատացված հսկողության ժամանակ կենսաչափական պատկերի օգտագործմամբ ԵՄ քաղաքացիների ինքնության ստուգումը հանդիսանում է ԵՄ արտաքին սահմաններում սահմանային ստուգումների տարր: Հետևաբար, այն ուղղակիորեն կապված է սահմանային անվտանգության հետ և ծառայում է Միության կողմից ճանաչված ընդհանուր շահի նպատակին: Բացի այդ, ՍԱՀ ելքերն օգնում են արագացնել ուղևորների տվյալների մշակումը և նվազեցնել մարդկային սխալների ռիսկը: Ավելին, այս սցենարում միջամտության շրջանակը, չափն ու ինտենսիվությունը շատ ավելի սահմանափակ են՝ համեմատած դեմքի ճանաչման այլ ձևերի հետ: Այնուամենայնիվ, կենսաչափական տվյալների մշակումը լրացուցիչ ռիսկեր է ստեղծում տվյալների սուբյեկտների համար, որոնք պետք է պատշաճ կերպով հասցեագրվեն և նվազեցվեն ԴՀՏ գործարկող և շահագործող իրավասու մարմնի կողմից:

1.4. Եզրակացություն

Սահմանային ավտոմատացված հսկողության համատեքստում ԵՄ քաղաքացիների ինքնության ստուգումն անհրաժեշտ և համաչափ միջոց է, եթե կան համապատասխան երաշխիքներ, և մասնավորապես եթե կիրառվում են նպատակի սահմանափակման, տվյալների որակի, թափանցիկության և անվտանգության բարձր մակարդակի սկզբունքները:

[85] «Անդամ պետությունների կողմից տրված անձնագրերում ու ճամփորդական փաստաթղթերում անվտանգության հատկանիշների և կենսաչափական տվյալների ստանդարտների մասին» ԽՈՐՀՐԴԻ 2004 թվականի դեկտեմբերի 13-ի թիվ 2252/2004 ԿԱՆՈՆԱԿԱՐԳ (ԵՀ)

[86] Անձանց միջսահմանային տեղաշարժը կարգավորող կանոնների մասին Միության օրենսգիրքը սահմանող՝ ԵՎՐՈՊԱԿԱՆ ՊԱՌԼԱՄԵՆՏԻ ԵՎ ԽՈՐՀՐԴԻ 2006 ԹՎԱԿԱՆԻ ՄԱՐՏԻ 9-Ի ԹԻՎ 2016/399 ԿԱՆՈՆԱԿԱՐԳ (ԵՄ) (Շենգենյան սահմանների մասին օրենսգիրք):

[87] Մուտքի/ելքի համակարգի կիրառման վերաբերյալ 2016/399 կանոնակարգը (ԵՄ) փոփոխող՝ Եվրոպական պառլամենտի և Խորհրդի 2017 թվականի նոյեմբերի 30-ի 2017/2225 կանոնակարգ (ԵՄ)

2 ՍՑԵՆԱՐ 2

2.1. Նկարագիրը

ԻՄ-երի կողմից ստեղծվել է երեխաների առևանգման զոհերի նույնականացման համակարգ: Ոստիկանության լիազորված ծառայողը կարող է իրականացնել առևանգման զոհ լինելու կասկածով երեխայի կենսաչափական տվյալների համեմատություն երեխաների առևանգման զոհերի շտեմարանի հետ խիստ պայմաններում՝ բացառապես նպատակ ունենալով հայտնաբերել այն անչափահասներին, որոնք կարող են համապատասխանել անհայտ կորած երեխայի նկարագրությանը, որի առնչությամբ նախաձեռնվել է քննություն և ստացվել է ահազանգ:

Մշակումն իրենից ներկայացնում է այն անձի դեմքի կամ պատկերի համեմատությունը շտեմարանում պահվող պատկերների հետ, որը կարող է համապատասխանել անհայտ կորած երեխայի նկարագրության հետ: Այդ մշակումը տեղի կունենա կոնկրետ դեպքերում և չի կրի համակարգված բնույթ:

Շտեմարանը, որի հետ կատարվում է համեմատությունը, համալրված է անհայտ կորած երեխաների նկարներով, որոնց առնչությամբ հաղորդում է ստացվել երեխայի առևանգման, երեխայի կյանքի կամ ֆիզիկական անձեռնմխելիության սպառնալիքի մասին, և դատական իշխանության կողմից հարուցվել է քրեական գործ, և երեխայի առևանգման առնչությամբ ստացվել է ահազանգ: Տվյալները հավաքվում են իրավասու իրավապահ մարմնի կողմից հաստատված ընթացակարգերի շրջանակներում, այսինքն՝ այն ոստիկանության ծառայողների կողմից, որոնք լիազորված են իրականացնելու քրեական ոստիկանության առջև դրված խնդիրները: Գրանցված անձնական տվյալների կատեգորիաներն են.

- ինքնությունը, մականունը, կեղծանունը, ծագումը, ազգությունը, հասցեները, էլ. փոստի հասցեները, հեռախոսահամարները.
- ծննդյան ամսաթիվը և վայրը.
- ծնողների վերաբերյալ տեղեկությունները.
- տեխնիկական բնութագրերով լուսանկար, որը թույլ է տալիս օգտագործել դեմքի ճանաչման սարք և այլ լուսանկարներ:

Համեմատության արդյունքները նույնպես պետք է վերանայվեն և ստուգվեն լիազորված ծառայողի կողմից՝ նախկին ապացույցները համեմատության արդյունքի հետ համադրելու և հնարավոր կեղծ դրական արդյունքները բացառելու համար:

Երեխաների նկարները և անձնական տվյալները կարող են պահպանվել միայն ահազանգի տևողության ընթացքում և պետք է ջնջվեն քրեական վարույթը կարճվելուց կամ դադարեցվելուց անմիջապես հետո՝ ազգային ընթացակարգերին համապատասխան, որոնց համար դրանք ներմուծվել են շտեմարան:

Թեև շտեմարանում կենսաչափական տվյալների պահպանման ժամկետը կարող է լինել համեմատաբար երկար և սահմանվել ազգային իրավունքի համաձայն, այնուամենայնիվ, տվյալների սուբյեկտների իրավունքների իրացումը, մասնավորապես, ուղղելու և ոչնչացնելու իրավունքն ապահովում է համապատասխան տվյալների սուբյեկտների անձնական տվյալների պաշտպանության իրավունքին միջամտությունը սահմանափակելու լրացուցիչ երաշխիք:

Տեղեկությունների աղբյուր.

- Տվյալների սուբյեկտների տեսակներ. ☒ երեխաներ
- Պատկերի աղբյուր ☒ այլ. նախապես չսահմանված, երեխայի առևանգման կասկածյալ զոհ
- Հանցագործության հետ կապ ☒ անուղղակի ժամանակային ☒ անուղղակի աշխարհագրական
- Տեղեկությունների հավաքագրման եղանակ. ☒ տաղավար կամ վերահսկվող միջավայր
- Այլ հիմնարար իրավունքների վրա ազդող համատեքստ ☒ այո, մասնավորապես՝ ☒ տարբեր

Վկայակոչման տվյալների շտեմարան (որի հետ համեմատվում են հավաքագրված տեղեկությունները).

- Կոնկրետություն ☒ կոնկրետ տվյալների շտեմարան

Ալգորիթմ.

- Ստուգման տեսակ. ☒ 1-ը շատի հետ նույնականացում

Արդյունք.

- Ազդեցություն ☒ ուղղակի
- Ավտոմատ որոշում. ☒ ՈՉ, պարտադիր գնահատում լիազորված ծառայողի կողմից

Իրավական վերլուծություն.

- Կիրառելի իրավական շրջանակ. ☒ Այս մշակման (դեմքի ճանաչում) համար հատուկ ազգային իրավունք

2.2. Կիրառելի իրավական շրջանակը

Ազգային իրավունքով նախատեսվում է տվյալների շտեմարանի ստեղծման, մշակման նպատակների որոշման, ինչպես նաև տվյալների շտեմարանի համալրման, դրան հասանելիության ապահովման և օգտագործման չափանիշների հատուկ իրավական շրջանակ: Դրա ներդրման համար անհրաժեշտ օրենսդրական միջոցներով նախատեսվում են նաև պահպանման ժամկետի որոշումը, ինչպես նաև ամբողջականության և գաղտնիության կիրառելի սկզբունքներին հղումը: Օրենսդրական միջոցներով նախատեսվում են նաև տվյալների սուբյեկտին և, տվյալ դեպքում ծնողական իրավունքներ ունեցող անձին (անձանց) տեղեկությունների տրամադրման մեթոդները, ինչպես նաև տվյալների սուբյեկտի իրավունքների իրացումն ու հարկ եղած դեպքում հնարավոր սահմանափակումները: Համապատասխան օրենսդրական միջոցի վերաբերյալ առաջարկի նախապատրաստման ժամանակ անհրաժեշտ էր խորհրդակցել ազգային վերահսկող մարմնի հետ:

2.3. Անհրաժեշտությունը և համաչափությունը. հանցագործության նպատակը/ ծանրությունը/մշակման գործընթացում չներգրավված, սակայն դրանից ազդեցություն կրած անձանց թիվը

Մշակման պայմանները և երաշխիքները

Դեմքի ճանաչման միջոցով համեմատությունը կարող է իրականացվել միայն իրավասու ծառայողի կողմից՝ որպես վերջին միջոց, եթե չկան առավել պակաս արմատական միջոցներ, և եթե դրանք խիստ անհրաժեշտ են, օրինակ՝ ճամփորդող անչափահասի անձը հաստատող փաստաթղթի իսկության վերաբերյալ կասկածի դեպքում և (կամ) նախկինում հավաքված ապացույցներն ու նյութերն ուսումնասիրելուց հետո, որոնք վկայում են անհայտ կորած երեխայի նկարագրության հետ հնարավոր համապատասխանության մասին, որի առնչությամբ իրականացվում է քննություն:

Լրացուցիչ երաշխիք է տրամադրվում նաև իրավասու ծառայողի կողմից դեմքի ճանաչման միջոցով համեմատության պարտադիր վերանայմամբ ու ստուգմամբ՝ նախկինում հավաքված ապացույցները համեմատության արդյունքի հետ համադրելու և ցանկացած հնարավոր կեղծ դրական արդյունք բացառելու նպատակով:

Հետապնդվող նպատակը

Տվյալների շտեմարանի ստեղծումը ծառայում է ընդհանուր հանրային շահի կարևոր նպատակներին, մասնավորապես՝ քրեական իրավախախտումների կանխմանը, քննությանը, հայտնաբերմանը կամ հետապնդմանը կամ քրեական պատիժների կատարմանը և այլ անձանց իրավունքների ու ազատությունների պաշտպանությանը: Տվյալների շտեմարանի ստեղծումը և նախատեսված մշակումը նպաստում են առևանգման զոհ դարձած երեխաների նույնականացմանը և, հետևաբար, կարող է դիտվել որպես այդ հանցագործության քննության ու հետապնդման իրավաչափ նպատակին աջակցող նպատակահարմար միջոց:

Տվյալների շտեմարանի նպատակն ու համալրումը

Մշակման նպատակները հստակ սահմանված են օրենքով, և տվյալների շտեմարանն օգտագործվում է միայն անհայտ կորած երեխաներին հայտնաբերելու նպատակով, որոնց առնչությամբ հաղորդում է ստացվել երեխայի առևանգման մասին և դատական մարմնի վերահսկողության ներքո հարուցվել է քննություն, և որոնց առնչությամբ երեխայի առևանգման մասին ստացվել է ահազանգ: Տվյալների շտեմարանի համալրման՝ օրենքով սահմանված պայմանները նպատակ ունեն խստորեն սահմանափակել տվյալների սուբյեկտների և տվյալների շտեմարանում ընդգրկվելիք անձնական տվյալների թիվը: Երեխայի նկատմամբ ծնողական իրավունքներ ունեցող անձը պետք է տեղյակ լինի իրականացված մշակման և նույնականացման նպատակով նախատեսված կենսաչափական տվյալների մշակման, ինչպես նաև տվյալների շտեմարանում պահվող՝ երեխայի անձնական տվյալների առնչությամբ երեխաների իրավունքների իրացման պայմանների մասին:

2.4. Եզրակացություն

Հաշվի առնելով նախատեսված մշակման անհրաժեշտությունն ու համաչափությունը, ինչպես նաև անձնական տվյալների մշակումն իրականացնելիս երեխայի լավագույն շահը և նկատի ունենալով, որ առկա են բավարար երաշխիքներ՝ հատկապես տվյալների սուբյեկտի իրավունքների իրացումն ապահովելու համար, մասնավորապես հաշվի առնելով այն փաստը, որ երեխաների տվյալները ենթակա են մշակման, դեմքի ճանաչման միջոցով մշակման կիրառումը կարող է համարվել որպես ԵՄ իրավունքի հետ համատեղելի:

Ավելին, հաշվի առնելով մշակման տեսակը և կիրառված տեխնոլոգիան, որը մեծ ռիսկ է պարունակում տվյալների սուբյեկտի իրավունքների ու ազատությունների համար, ՏՊԵԽ-ը գտնում է, որ ազգային պառլամենտի կողմից ընդունման ենթակա օրենսդրական միջոցի վերաբերյալ առաջարկության կամ այդ օրենսդրական միջոցի վրա հիմնված նորմատիվ միջոցի նախապատրաստումը, որը վերաբերում է նախատեսվող մշակմանը, պետք է իրականացվի վերահսկող մարմնի հետ նախնական խորհրդակցություն անցկացնելով՝ կիրառելի իրավական շրջանակի հետ հետևողականություն ու համապատասխանություն ապահովելու համար, տե՛ս ԻԿՀ 28.2 հոդվածը:

3 ՍՑԵՆԱՐ 3

3.1. Նկարագիրը

Անկարգություններին ոստիկանության միջամտությունների և դրանից հետո իրականացված քննության ընթացքում մի շարք անձինք ճանաչվել են կասկածյալ, օրինակ՝ նախկինում իրականացված քննությունների միջոցով՝ օգտագործելով տեսահսկման համակարգերի տեսանյութերը կամ վկաներին: Այս կասկածյալների նկարները համեմատվում են հանցանքի վայրում կամ հարակից տարածքներում տեսահսկման համակարգի կամ բջջային սարքերով տեսագրված անձանց նկարների հետ:

Ցույցի հետ կապված անկարգություններին մասնակցելու մեջ կասկածվող անձանց վերաբերյալ առավել մանրամասն ապացույցներ ձեռք բերելու համար ոստիկանությունը ստեղծում է անկարգությունների հետ տեղական և ժամանակային կապ ունեցող պատկերների տեսքով նյութերի շտեմարան: Շտեմարանը ներառում է քաղաքացիների կողմից ոստիկանության համակարգ վերբեռնված մասնավոր ձայնագրությունները, հասարակական տրանսպորտում տեսահսկման համակարգերով ձայնագրված նյութերը, ոստիկանությանը պատկանող տեսահսկման համակարգերով ձայնագրված նյութերը և լրատվամիջոցների կողմից հրապարակված նյութերը՝ առանց որևէ հատուկ սահմանափակման կամ երաշխիքի: Դաժան հանցավոր վարքագծի դրսևորումը չի հանդիսանում պարտադիր նախապայման՝ շտեմարանում ֆայլեր հավաքագրելուու համար: Հետևաբար, անկարգություններին մասնակցություն չունեցած անձինք՝ տեղի բնակչության զգալի տոկոսը, որոնք պատահաբար ցույցի պահին անցել են դրա կողքով կամ մասնակցել են ցույցին, սակայն չեն մասնակցել անկարգություններին.

– պահվում են շտեմարանում: Դրանք վիդեոներ և պատկերներ պարունակող հազարավոր ֆայլեր են:

Օգտագործելով դեմքի ճանաչման ծրագրային ապահովում՝ այդ ֆայլերում հայտնված բոլոր դեմքերին տրվում են դեմքի եզակի նույնականացուցիչներ: Առանձին կասկածյալների դեմքերն այնուհետև ավտոմատ կերպով համեմատվում են այդ դեմքերի նույնականացուցիչների հետ:

Վիդեոներ և պատկերներ պարունակող հազարավոր ֆայլերի բոլոր կենսաչափական մոդելների շտեմարանը պահպանվում է մինչև բոլոր հնարավոր քննությունների դադարեցումը: Դրական համընկնումներով զբաղվում են պատասխանատու աշխատողները, որոնք այնուհետև որոշում են հետագա գործողությունները: Սա կարող է ներառել շտեմարանում գտնված ֆայլը համապատասխան անձի քրեական գործի նյութերին կցելը, ինչպես նաև հետագա միջոցները, ինչպիսիք են այդ անձին հարցաքննելը կամ ձերբակալելը:

Ազգային իրավունքով նախատեսվում է ընդհանուր դրույթ, համաձայն որի՝ ֆիզիկական անձի եզակի նույնականացման նպատակով կենսաչափական տվյալների մշակումը թույլատրելի է, եթե խիստ անհրաժեշտ է, և եթե գործում են համապատասխան անձի իրավունքների ու ազատությունների համապատասխան երաշխիքներ:

Տեղեկությունների աղբյուր.

- Տվյալների սուբյեկտների տեսակներ. ☒ բոլոր անձինք
- Պատկերի աղբյուր. ☒ հանրային տարածքներ ☒ մասնավոր սուբյեկտ ☒ այլ անձինք ☒ այլ. լրատվամիջոցներ
- Հանցագործության հետ կապը. ☒ պարտադիր չէ, որ լինի ուղղակի աշխարհագրական կամ ժամանակային կապ
- Տեղեկությունների հավաքագրման եղանակ. ☒ հեռավար
- Այլ հիմնարար իրավունքների վրա ազդող համատեքստ ☒ այո, մասնավորապես՝
  ☒հավաքների ազատության համատեքստ
- Տվյալների սուբյեկտի մասին տեղեկությունների լրացուցիչ, հասանելի աղբյուրներ
  ☒ այլ. բացառված չէ (ինչպես օրինակ՝ ավտոմատ գանձման մեքենաների օգտագործումը կամ այցելած խանութները), քանի որ նկարների շարժառիթների նկատմամբ վերահսկողություն չի կարող իրականացվել

Վկայակոչման տվյալների շտեմարան (որի հետ համեմատվում են հավաքագրված տեղեկությունները).

- Կոնկրետություն ☒ հանցավորության ոլորտին առնչվող կոնկրետ տվյալների շտեմարան

Ալգորիթմ.

- Մշակման տեսակ. ☒1-ը շատի հետ նույնականացում

Արդյունք.

- Ազդեցություն ☒ ուղղակի (օրինակ՝ տվյալների սուբյեկտը կարող է ձերբակալվել, հարցաքննվել)
- Ավտոմատ որոշում. ☒ ՈՉ
- Պահպանման տևողություն. մինչև բոլոր հնարավոր քննությունների դադարեցումը

Իրավական վերլուծություն.

- Տվյալների սուբյեկտի համար նախնական տեղեկությունների տեսակ.
  ☒ ԻՄ-ի կայքէջում ընդհանրապես
- Կիրառելի իրավական շրջանակ. ☒ ԻԿՀ-ն մեծամասամբ փոխատեղվել է ազգային իրավունքում ☒ Ընդհանուր ազգային իրավունք ԻՄ-երի կողմից կենսաչափական տվյալների օգտագործման համար

3.2. Կիրառելի իրավական շրջանակը

Ինչպես պարզաբանվեց վերևում, ԻԿՀ 10-րդ հոդվածի ընդհանուր դրույթը պարզապես կրկնող իրավական հիմքերը բավականաչափ հստակ ձևակերպված չեն, որպեսզի անձինք բավարար պատկերացում ունենան այն պայմանների և հանգամանքների մասին, որոնց դեպքում ԻՄ-երն իրավասու են օգտագործելու հանրային տարածքներից տեսահսկման համակարգով կատարված տեսագրությունները՝ նրանց դեմքի կենսաչափական մոդելը ստեղծելու և այն ոստիկանության տվյալների շտեմարանների, տեսահսկման համակարգով կամ մասնավոր անձանց կողմից կատարված այլ հասանելի ձայնագրությունների և այլնի հետ համեմատելու համար: Այս սցենարում ներկայացված իրավական շրջանակը հետևաբար չի բավարարում նվազագույն պահանջները, որպեսզի ծառայի որպես իրավական հիմք:

3.3. Անհրաժեշտությունը և համաչափությունը

Այս օրինակում մշակումը տարբեր մտահոգությունների տեղիք է տալիս՝ կապված անհրաժեշտության և համաչափության սկզբունքների հետ՝ մի քանի պատճառներով.

Մարդիկ չեն կասկածվում ծանր հանցագործության մեջ: Դաժան հանցավոր վարքագծի դրսևորումը չի հանդիսանում նախապայման պատկերներ պարունակող շտեմարանում առկա ֆայլերի օգտագործման համար: Նաև հանցագործության հետ ուղղակի ժամանակային և աշխարհագրական կապը չի հանդիսանում նախապայման շտեմարանում առկա ֆայլերի օգտագործման համար: Սա հանգեցնում է նրան, որ տեղի բնակչության զգալի տոկոսի վերաբերյալ տվյալները պահվում են կենսաչափական տվյալների շտեմարանում պոտենցիալ մի քանի տարի տևողությամբ, մինչև բոլոր քննությունների դադարեցումը:

Հանցանքի վայրի շտեմարանը չի համալրվում միայն համաչափության պահանջները

բավարարող պատկերներով՝ այդպիսով հանգեցնելով մի իրավիճակի, երբ պետք է համեմատվեն աննսահմանափակ թվով պատկերներ: Սա հակասում է տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքին: Ավելի փոքր թվով պատկերները հնարավորություն կտան նաև դիտարկել ոչ ալգորիթմական և պակաս արմատական միջոցների, օրինակ՝ գերճանաչողների տարբերակը [super recogizer][88]:

Քանի որ օրինակը վերցված է բողոքի ցույցի վայրից, հավանական է նաև, որ պատկերներով բացահայտվեն ցույցի մասնակիցների քաղաքական հայացքները, ինչը կդառնա այս սցենարում շոշափված տվյալների երկրորդ հատուկ կատեգորիան: Այս սցենարում պարզ չէ, թե ինչպես կարելի է կանխել այդ տվյալների հավաքումը և ինչ երաշխիքներով: Ավելին, երբ տվյալների սուբյեկտները տեղեկանում են, որ ցույցին իրենց մասնակցությունը հանգեցրել է ոստիկանության կենսաչափական տվյալների շտեմարան իրենց վերաբերող տվյալների մուտքագրվելուն, դա կարող է լուրջ զսպող ազդեցություն ունենալ հավաքների իրենց իրավունքի հետագա իրացման վրա:

Տվյալների շտեմարանում առկա կենսաչափական մոդելները նույնպես կարող են համեմատվել միմյանց հետ: Սա հնարավորություն է տալիս ոստիկանությանը ոչ միայն փնտրել կոնկրետ անձի իր գործի բոլոր նյութերով, այլև մի քանի օրվա ընթացքում վերաստեղծել մարդու վարքագծի մոդելը: Այն կարող է նաև լրացուցիչ տեղեկություններ հավաքագրելու անձանց մասին, ինչպիսիք են նրանց սոցիալական շփումները և քաղաքական ներգրավվածությունը:

Միջամտությունն ավելի է ուժեղանում այն փաստով, որ տվյալները մշակվում են առանց տվյալների սուբյեկտների գիտության:

Հաշվի առնելով, որ մարդիկ մշտապես լուսանկարահանում և տեսանկարահանում են, և որ նույնիսկ ամենուր առկա տեսանկարահանումը կարող է վերլուծվել կենսաչափական եղանակով, դա կարող է հանգեցնել լուրջ զսպող ազդեցության:

Մասնավոր լուսանկարների և տեսանյութերի լայնածավալ օգտագործումը, այդ թվում՝ պոտենցիալ սխալ օգտագործումը, օրինակ՝ մատնության նպատակով, մտահոգության ևս մեկ առիթ է: Քանի որ սխալ օգտագործումը, օրինակ՝ մատնության նպատակով նաև ընդհանուր առմամբ քրեական վարույթին ներհատուկ ռիսկ է, վերջինս զգալիորեն ավելի մեծ է մշակված տվյալների մասշտաբայնության և ներգրավված անձանց թվի առումով, քանի որ մարդիկ կարող են վերբեռնել նաև իրենց կողմից չսիրված կոնկրետ անձին կամ անձանց խմբին վերաբերող նյութեր: Լուսանկարներ և տեսանյութեր վերբեռնելու ոստիկանության պահանջներն ամենայն հավանականությամբ հանգեցնում են մարդկանց կողմից նյութ տրամադրելու շատ ցածր շեմերի, հատկապես, քանի որ դա հնարավոր է անել անանուն կամ առնվազն առանց ոստիկանության բաժանմունք ներկայանալու և ինքնությունը հաստատելու անհրաժեշտության:

3.4. Եզրակացություն

Օրինակում չկա որևէ կոնկրետ դրույթ, որը կարող է իրավական հիմք հանդիսանալ: Այնուամենայնիվ, նույնիսկ եթե առկա լիներ բավարար իրավական հիմք, անհրաժեշտության և համաչափության պահանջները չէին պահպանվի, ինչի հետևանքով տեղի կունենար տվյալների սուբյեկտի՝ Խարտիայով նախատեսված անձնական կյանքի նկատմամբ հարգանքի և անձնական տվյալների պաշտպանության իրավունքներին անհամաչափ միջամտություն:

[88] Այսինքն՝ դեմքերի ճանաչման արտակարգ կարողություններով օժտված մարդիկ: Տե՛ս նաև Դեմքերի ճանաչումը Լոնդոնի քաղաքային ոստիկանության գերճանաչողների կողմից, 2016 թվականի փետրվարի 26, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/:

4 ՍՑԵՆԱՐ 4

4.1. Նկարագիրը

Ոստիկանությունը ներդնում է տեսահսկման համակարգերով ֆիքսված ծանր հանցագործություն կատարած կասկածյալների նույնականացման եղանակ՝ հետադարձ ԴՀՏ-ի միջոցով: Ծառայողը տեսանյութերից ընտրում է կասկածյալների պատկերը (պատկերները), որոնք նախնական քննության շրջանակներում հավաքվել են հանցանքի կամ այլ վայրից, և այնուհետև պատկերը (պատկերներն) ուղարկում է դատաբժշկական դեպարտամենտ: Դատաբժշկական դեպարտամենտը կիրառում է ԴՀՏ՝ այդ պատկերը (պատկերները) համապատասխանեցնելու այն անձանց նկարների հետ, որոնք նախկինում հավաքվել են ոստիկանության կողմից տվյալների շտեմարանում (այսպես կոչված նկարագրություններ պարունակող շտեմարան, որը բաղկացած է կասկածյալներից և նախկին դատապարտյալներից): Նկարագրություններ պարունակող շտեմարանը նախատեսված է այս ընթացակարգի համար՝ ժամանակավոր և մեկուսացված միջավայրում, որը վերլուծվում է ԴՀՏ-ի միջոցով, որպեսզի հնարավոր լինի իրականացնել համապատասխանեցման գործընթացը: Համապատասխանեցված անձանց իրավունքներին և շահերին միջամտությունը նվազագույնի հասցնելու համար դատաբժշկական դեպարտամենտի շատ սահմանափակ թվով աշխատողներ ունեն իրական համապատասխանեցման ընթացակարգ իրականացնելու թույլտվություն, տվյալներին հասանելիություն ունեն այն ծառայողները, որոնց վստահված է կոնկրետ ֆայլը, և արդյունքների մեխանիկական հսկողությունն իրականացվում է նախքան որևէ արդյունք քննություն իրականացնող ծառայողին ուղարկելը: Կենսաչափական տվյալները չեն փոխանցվում վերահսկվող, մեկուսացված միջավայրից դուրս: Հետագայում քննության ընթացքում օգտագործվում են միայն արդյունքը և նկարը (ոչ կենսաչափական մոդելը): Աշխատողներն անցնում են հատուկ դասընթաց այս մշակման կանոնների և ընթացակարգերի վերաբերյալ, և անձնական ու կենսաչափական տվյալների ամբողջ մշակումը մանրամասն սահմանված է ազգային իրավունքում:

Տեղեկությունների աղբյուր:

- Տվյալների սուբյեկտների տեսակներ. ☒ տեսահսկման համակարգի ձայնագրությունների միջոցով հայտնաբերված կասկածյալներ
- Պատկերի աղբյուր. ☒ հանրային տարածքներ ☒ համացանց
- Հանցագործության հետ կապ: ☒ ուղղակի ժամանակային
  ☒ ուղղակի աշխարհագրական
- Տեղեկությունների հավաքագրման եղանակ. ☒ հեռավար
- Այլ հիմնարար իրավունքների վրա ազդող համատեքստ. այո, մասնավորապես՝ ☒ հավաքների ազատություն ☒ խոսքի ազատություն ☒ այլ.

Վկայակոչման տվյալների շտեմարան (որի հետ համեմատվում են հավաքված տեղեկությունները).

- Կոնկրետություն: ☒ հանցավորության ոլորտին առնչվող կոնկրետ տվյալների շտեմարան

Ալգորիթմ.

- Մշակման տեսակ. ☒ 1-ը շատի հետ նույնականացում

Արդյունք.

- Ազդեցություն ☒ ուղղակի (տվյալների սուբյեկտը ձերբակալվել կամ հարցաքննվել է
- Ավտոմատ որոշում ☒ ՈՉ

Իրավական վերլուծություն.

- Կիրառելի իրավական շրջանակ. ☒ այդ իրավասու մարմնի համար այս մշակման (դեմքի ճանաչում) առնչությամբ հատուկ ազգային իրավունք

4.2. Կիրառելի իրավական շրջանակը

Այս սցենարում ազգային իրավունքը նշում է, որ կենսաչափական տվյալները կարող են օգտագործվել դատաբժշկական վերլուծություններ իրականացնելիս, երբ խիստ անհրաժեշտ է ծանր հանցագործություն կատարած կասկածյալների նույնականացման նպատակին հասնելու համար՝ նկարագրություններ պարունակող շտեմարանի նկարները համապատասխանեցնելու միջոցով: Ազգային իրավունքով սահմանվում են մշակման ենթակա տվյալների տեսակները, ինչպես նաև անձնական տվյալների ամբողջականության ու գաղտնիության պահպանման և դրանց ոչնչացման ընթացակարգերը՝ այդպիսով ապահովելով չարաշահումների ու կամայականությունների ռիսկի դեմ բավարար երաշխիքներ:

4.3. Անհրաժեշտությունը և համաչափությունը

Ակնհայտորեն դեմքի ճանաչման համակարգի կիրառումն առավել արդյունավետ է, քան դատաբժշկական մակարդակում մեխանիկական համապատասխանեցումը: Պատկերների մեխանիկական ընտրությունն ի սկզբանե սահմանափակում է միջամտությունը՝ համեմատած ամբողջ տեսանյութը տվյալների շտեմարանի հետ համադրելու գործընթացի և այդպիսով տարբերակում և թիրախավորում է միայն այն անձանց, որոնց առնչվում է նպատակը, այսինքն՝ ծանր հանցագործությունների դեմ պայքարը: Այնուամենայնիվ, դեռևս կարևոր է հաշվի առնել, թե արդյոք հնարավոր է իրականացնել համապատասխանեցումը ողջամիտ ժամկետում՝ կախված կոնկրետ գործից: Անձանց՝ տեխնոլոգիաներին և անձնական տվյալներին հասանելիության սահմանափակումը նվազեցնում է ազդեցությունն անձնական կյանքի անձեռնմխելիության և տվյալների պաշտպանության իրավունքների, ինչպես նաև նրա վրա, որ հետագայում կենսաչափական մոդելները չեն պահպանվում կամ օգտագործվում քննության ընթացքում: Արդյունքի մեխանիկական

հսկողությունը նշանակում է նաև ցանկացած կեղծ դրական ռիսկի նվազեցում:

4.4. Եզրակացություն

Կարևոր է, որ ազգային օրենսդրությամբ նախատեսվի համապատասխան իրավական հիմք՝ կենսաչափական տվյալների մշակման, ինչպես նաև ազգային տվյալների շտեմարանի համար, որի հետ տեղի է ունենում համապատասխանեցումը: Այս սցենարում ձեռնարկվել են մի շարք միջոցներ՝ տվյալների պաշտպանության իրավունքներին միջամտությունը սահմանափակելու համար, ինչպես օրինակ՝ իրավական հիմքում նշված ԴՀՏ-ի օգտագործման պայմանները, տեխնոլոգիաներին ու կենսաչափական տվյալներին հասանելիություն ունեցող անձանց թիվը, մեխանիկական հսկողությունները և այլն: ԴՀՏ-ն զգալիորեն բարելավում է ոստիկանության դատաբժշկական դեպարտամենտի քննչական աշխատանքի արդյունավետությունը, հիմնված է օրենքի վրա, որը թույլ է տալիս ոստիկանությանը խիստ անհրաժեշտության դեպքում մշակել կենսաչափական տվյալները և, հետևաբար, այս պարամետրերի շրջանակում կարող է դիտվել որպես անձի իրավունքների օրինական միջամտություն:

5 ՍՑԵՆԱՐ 5

5.1. Նկարագիրը

Հեռավար կենսաչափական նույնականացումն անձանց ինքնության հաստատումն է կենսաչափական նույնականացուցիչների միջոցով (դեմքի պատկեր, քայլվածք, ծիածանաթաղանթ և այլն) հեռավորության վրա, հանրային տարածքում և հընթացս կամ շարունակական ձևով՝ ստուգելով դրանք տվյալների շտեմարանում պահվող (կենսաչափական) տվյալների հետ[89]: Հեռավար կենսաչափական նույնականացումն իրականացվում է իրական ժամանակում, եթե պատկերի տեսքով նյութի հավաքումը, համեմատությունն ու նույնականացումը տեղի են ունենում առանց էական ձգձգումների:

Նախքան իրական ժամանակում յուրաքանչյուր հեռավար կենսաչափական նույնականացում իրականացնելը, ոստիկանությունը քննության շրջանակներում կազմում է հետաքրքրություն ներկայացնող՝ հետախուզման մեջ գտնվող սուբյեկտների ցուցակ: Այն համալրվում է անձանց դեմքի պատկերներով: Հիմնվելով հետախուզական տվյալների վրա, համաձայն որոնց՝ անձինք կլինեն կոնկրետ տարածքում, օրինակ՝ առևտրի կենտրոնում կամ հանրային հրապարակում, ոստիկանությունը որոշում է, թե երբ, որտեղ և որքան ժամանակ կիրառի հեռավար կենսաչափական նույնականացումը:

Օպերացիայի իրականացման օրը ոստիկանությունը տեղում կենտրոնացնում է ոստիկանական մեքենա՝ որպես կառավարման կենտրոն, ոստիկանության ավագ ծառայողի ղեկավարման ներքո: Մեքենայում տեղադրված են մոնիտորներ, որոնց վրա ցուցադրվում են մոտակայքում տեղադրված տեսախցիկների ֆիքսած կադրերը՝ տեղադրված կա՛մ ժամանակավոր կա՛մ արդեն տեղադրված տեսախցիկների տեսահոսքերին միանալու միջոցով: Երբ հետիոտներն անցնում են տեսախցիկների կողքով, տեխնոլոգիան առանձնացնում է դեմքի պատկերները, դրանք վերածում կենսաչափական մոդելների և համեմատում դրանք հետախուզվող անձանց ցուցակում գտնվող կենսաչափական մոդելների հետ:

Եթե պոտենցիալ համընկնում է հայտնաբերվում հետախուզվող անձանց ցուցակի ու տեսախցիկների կողքով անցնող անձանց միջև, ապա ահազանգ է ուղարկվում մեքենայում գտնվող ծառայողներին, որոնք այնուհետև տեղեկացնում են տեղում գտնվող ծառայողներին, եթե ահազանգը դրական է լինում, օրինակ՝ ռադիո սարքի միջոցով: Այնուհետև տեղում գտնվող ծառայողը որոշում է միջամտել, մոտենալ, թե ի վերջո բերման ենթարկել անձին: Տեղում ծառայողի ձեռնարկած միջոցները ձայնագրվում են: Գաղտնի ստուգման դեպքում հավաքված տեղեկությունները (օրինակ՝ ում հետ է այդ անձը, ինչ են նրանք կրում և ուր են գնում) պահպանվում են:

Նշված ազգային օրենսդրությամբ նախատեսվում է ընդհանուր դրույթ, համաձայն որի՝ եզակի նույնականացման նպատակով ֆիզիկական անձի կենսաչափական տվյալների մշակումը թույլատրելի է, եթե խիստ անհրաժեշտ է և պահպանվում են համապատասխան անձի իրավունքների ու ազատությունների համապատասխան երաշխիքները:

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf:

Տեղեկությունների աղբյուր.

- Տվյալների սուբյեկտների տեսակներ. ☒ բոլոր քաղաքացիները
- Պատկերի աղբյուր. ☒ հանրային տարածքներ
- Հանցագործության հետ կապ. ☒ պարտադիր չէ ուղղակի աշխարհագրական կամ ժամանակային կապ
- Տեղեկությունների հավաքագրման եղանակ. ☒ հեռավար
- Այլ հիմնարար իրավունքների վրա ազդող համատեքստ ☒ այո, մասնավորապես՝ ☒ հավաքների ազատություն ☒ խոսքի ազատություն ☒ այլ
- Տվյալների սուբյեկտի մասին տեղեկությունների լրացուցիչ հասանելի աղբյուրներ. ☒ այլ. բացառված չէ (ինչպես օրինակ՝ ավտոմատ գանձման մեքենաների օգտագործումը կամ այցելած խանութները)

Վկայակոչման տվյալների շտեմարան (որի հետ համեմատվում են հավաքված տեղեկությունները).

- Կոնկրետություն. ☒ հանցավորության ոլորտին առնչվող կոնկրետ տվյալների շտեմարան

Ալգորիթմ.

- Մշակման տեսակ. ☒1-ը շատի հետ նույնականացում

Արդյունք.

- Ազդեցություն ☒ ուղղակի (օրինակ՝ տվյալների սուբյեկտը կարող է ձերբակալվել, հարցաքննվել)
- Ավտոմատ որոշում. ☒ ՈՉ
- Պահպանման տևողություն. մինչև բոլոր հնարավոր քննությունների դադարեցումը

Իրավական վերլուծություն.

- Տվյալների սուբյեկտի համար նախնական տեղեկությունների տեսակ. ☒ ԻՄ-ի կայքէջում ընդհանրապես
- Կիրառելի իրավական շրջանակ. ☒ ԻԿՀ-ն մեծամասամբ փոխատեղվել է ազգային իրավունքում ☒ Ընդհանուր ազգային իրավունք ԻՄ-երի կողմից կենսաչափական տվյալների օգտագործման համար

5.2. Կիրառելի իրավական շրջանակը

ԻԿՀ 10-րդ հոդվածի ընդհանուր դրույթը պարզապես կրկնող իրավական հիմքերը բավականաչափ հստակ ձևակերպված չեն, որպեսզի անձինք բավարար պատկերացում ունենան այն պայմանների և հանգամանքների մասին, որոնց դեպքում ԻՄ-երն իրավասու են օգտագործելու հանրային տարածքներից տեսահսկման համակարգով կատարված տեսագրությունները՝ նրանց դեմքի կենսաչափական մոդելը ստեղծելու և այն ոստիկանության տվյալների շտեմարանների հետ համեմատելու համար: Այս սցենարում ներկայացված իրավական շրջանակը հետևաբար չի բավարարում նվազագույն պահանջները, որպեսզի ծառայի որպես իրավական հիմք:[90]

5.3. Անհրաժեշտությունը և համաչափությունը

Որքան բարձրանում է անհրաժեշտության և համաչափության նշաձողը, այնքան մեծանում է միջամտության չափը: Հանրային տարածքներում հեռավար կենսաչափական նույնականացումն ունի հիմնարար իրավունքների վրա մի շարք հետևանքներ.

[90] Այն դեպքերում, երբ ԴՀՏ-ի կիրառությունը հետազոտելու նպատակով նախաձեռնված գիտական նախագծի շրջանակներում անհրաժեշտություն կլինի մշակել անձնական տվյալներ, սակայն այդ մշակումը չի կարգավորվի ԻԿՀ 4(3) հոդվածով կամ Միության իրավունքով, կիրառելի կլինի ՏՊԸԿ-ն: Պիլոտային նախագծերի դեպքում, որոնց կհետևեն իրավապահ մարմինների գործողությունները, դեռևս կիրառելի կլինի ԻԿՀ-ն:

Սցենարները ենթադրում են համապատասխան հանրային տարածքում յուրաքանչյուր անցորդի մշտադիտարկում: Այդպիսով, դա խստորեն ներազդում է հանրային տարածքներում անանուն լինելու բնակչության ողջամիտ ակնկալիքների վրա[91]: Սա հանդիսանում է ժողովրդավարական գործընթացի շատ հայեցակետերի նախապայման, ինչպես օրինակ՝ քաղաքացիական միավորումներին միանալու որոշումը, հավաքների գնալը և բոլոր սոցիալական ու մշակութային պատկանելիություն ունեցող մարդկանց հանդիպելը, քաղաքական բողոքի ակցիաներին մասնակցելը և բոլոր տեսակի վայրեր այցելելը: Հանրային տարածքներում անանունության գաղափարը էական է՝ տեղեկություններ և գաղափարներ ազատորեն հավաքագրելու և փոխանակելու համար: Այն պահպանում է բազմակարծությունը, խաղաղ հավաքների ու միավորումներ կազմելու ազատությունը և փոքրամասնությունների պաշտպանությունը, ինչպես նաև պաշտպանում է իշխանությունների բաժանման և զսպումների ու հակակշիռների սկզբունքները: Հանրային տարածքներում անանունության հասկացության խաթարումը կարող է լուրջ զսպող ազդեցություն ունենալ քաղաքացիների վրա: Նրանք կարող են ձեռնպահ մնալ որոշ վարքագծեր դրսևորելուց, որոնք գտնվում են ազատ և բաց հասարակության պատասխանատվության շրջանակում: Սա կազդի հանրային շահի վրա, քանի որ ժողովրդավարական հասարակությունը պահանջում է ինքնորոշում և իր քաղաքացիների մասնակցությունը ժողովրդավարական գործընթացներին:
Այդ տեխնոլոգիայի կիրառման տարբերակում պարզապես փողոցով քայլելը, մետրո կամ հացաբուլկեղենի խանութ գնալը կհանգեցնի իրավապահ մարմինների կողմից անձնական, այդ թվում՝ կենսաչափական տվյալների հավաքագրմանը և, առաջին սցենարի դեպքում նաև դրանց՝ ոստիկանության տվյալների շտեմարանի հետ համապատասխանեցմանը: Այն իրավիճակը, երբ նույնը կկատարվի մատնահետքեր վերցնելով, ակնհայտորեն անհամաչափ կլինի:

Նշված իրավիճակում հայտնված տվյալների սուբյեկտների թիվը չափազանց մեծ է, քանի որ յուրաքանչյուր ոք, ով անցնում է համապատասխան հանրային վայրի կողքով, ազդեցություն է կրում: Ավելին, սցենարները ենթադրում են կենսաչափական տվյալների ավտոմատացված զանգվածային մշակում, ինչպես նաև կենսաչափական տվյալների զանգվածային համապատասխանեցում ոստիկանության տվյալների շտեմարանների հետ:
Եվրոպական նախադեպային իրավունքում զանգվածային տեսահսկումն արգելված է (օրինակ, ՄԻԵԴ-ը *Մ.-ն և Մարփերն ընդդեմ ՄԹ-ի գործում* կենսաչափական տվյալների ոչ ընտրողաբար պահպանումը համարել է անձնական կյանքի անձեռնմխելիության իրավունքին «անհամաչափ միջամտություն», քանի որ այն չի կարող համարվել «անհրաժեշտ ժողովրդավարական հասարակությունում»):
Հեռավար կենսաչափական նույնականացումն այնքան հակված է զանգվածային հսկողության, որ չկան սահմանափակման հուսալի միջոցներ: Այն, որպես այդպիսին, էապես տարբերվում է տեսահսկումից, քանի որ առանց կենսաչափական նույնականացման տեսագրությունների հնարավոր օգտագործումն արդեն իսկ լուրջ միջամտություն է, սակայն միևնույն ժամանակ սահմանափակ, մինչդեռ ԴՀՏ-ի կիրառման տարբերակում արդեն լայն տարածում գտած տեսահսկման համակարգը՝ որպես տվյալների հիմնական աղբյուր, ենթարկվելու է որակի փոփոխության: Ավելին, հատկապես ենթադրվող զսպող ազդեցությունների առումով, արդեն իսկ գոյություն ունեցող տեսահսկման համակարգերի կիրառման հնարավոր սահմանափակումները տեսանելի չեն լինի և, հետևաբար, հանրության կողմից վստահություն չեն վայելի:

[91] «Clearview AI» ընկերության կողմից մշակված՝ դեմքի ճանաչման հավելվածի վերաբերյալ ՊՏԵՀ-ի պատասխանը ԵՊԱ-ներին, 2020 թվականի հունիսի 10, Ref: OUT2020-0052:

Ոստիկանության մարմինների կողմից հեռավար կենսաչափական նույնականացումը բոլորին վերաբերվում է որպես պոտենցիալ կասկածյալի: Սակայն իրավական պետությունում քաղաքացիները համարվում են արդար, քանի դեռ չի ապացուցվել նրանց հակաիրավական վարքագիծը: Այս սկզբունքը մասամբ արտացոլված է նաև ԻԿՀ-ում, որում ընդգծվում է, որ հնարավորության դեպքում անհրաժեշտ է տարբերակում մտցնել դատապարտյալների կամ կասկածյալների նկատմամբ վերաբերմունքի միջև, որոնց դեպքում իրավապահները պետք է «*լուրջ հիմքեր ունենան ենթադրելու, որ նրանք կատարել են կամ կկատարեն քրեական իրավախախտում*» (ԻԿՀ 6(ա) հոդված), ինչպես նաև այն անձանց միջև, որոնք դատապարտված չեն կամ չեն կասկածվում հանցավոր գործունեություն կատարելու մեջ:
Տրանսպորտային համակարգի հանգուցային կետերում կամ հանրային տարածքներում կիրառումը, ինչպես նաև իրավապահ մարմինների կողմից անձանց եզակի նույնականացման հնարավորություն ունեցող տեխնոլոգիայի կիրառումը և այդ անձին հետևելը կամ գտնվելու վայրն ու տեղաշարժերը վերլուծելը կարող են բացահայտել անձի վերաբերյալ ամենազգայուն տեղեկությունները (նույնիսկ սեռական նախասիրությունները, կրոնը, առողջական խնդիրները): Այն հանգեցնում է նաև տվյալներին անօրինական հասանելիության և օգտագործման հսկայական ռիսկի:

Այնպիսի համակարգի տեղադրումը, որը հնարավորություն է տալիս բացահայտել անձի վարքագծի և առանձնահատկությունների բուն էությունը, հանգեցնում է ուժեղ զսպող ազդեցության: Դա ստիպում է մարդկանց հարց տալ իրենց, թե արդյոք արժե միանալ որևէ ցույցի՝ դրանով իսկ վնասելով ժողովրդավարական գործընթացին:
Նաև որևէ ընկերոջ հանդիպելն ու հանրության մեջ նրա հետ երևալը, որը հայտնի է, որ ոստիկանների հետ ունի խնդիրներ կամ դրսևորում է անսովոր վարքագիծ, կարող է կրիտիկական համարվել, քանի որ այս ամենը կհանգեցնի համակարգի ալգորիթմի և, հետևաբար, իրավապահ մարմինների ներգրավմանը:

Անհնար է պաշտպանել խոցելի տվյալների սուբյեկտներին, ինչպիսիք են երեխաները: Ավելին, դա ազդեցություն է թողնում այն անձանց վրա, որոնք ունեն մասնագիտական շահ, և հաճախ համապատասխան իրավական պարտավորություն գաղտնի պահելու իրենց շփումները, ինչպիսիք են լրագրողները, իրավաբանները և հոգևորականները: Սա կարող է, օրինակ՝ հանգեցնել աղբյուրի և լրագրողի, կամ այն փաստի բացահայտմանը, որ անձը խորհրդակցում է քրեական գործերով պաշտպանի հետ: Խնդիրը չի վերաբերում միայն պատահական հասարակական վայրերին, որտեղ, օրինակ՝ լրագրողներն ու իրենց աղբյուրները հանդիպում են, սակայն, բնականաբար, նաև հանրային այն տարածքներին, որոնք անհրաժեշտ են հաստատություններին կամ մասնագետներին դիմելու և այս առնչությամբ հասանելիություն ստանալու համար:

Ավելին, ԴՀՏ-ի հետ կապված մարդկանց անհարմարավետությունը կարող է դրդել նրանց փոխել իրենց վարքագիծը, խուսափել այն վայրերից, որտեղ կիրառվում է ԴՀՏ՝ այդպիսով հեռանալով հասարակական կյանքից ու մշակութային իրադարձություններից: Կախված ԴՀՏ-ի գործարկման մասշտաբներից՝ մարդկանց վրա ազդեցությունը կարող է այնքան նշանակալից լինել, որ ազդի արժանապատիվ կյանքով ապրելու նրանց կարողության վրա[92]:

[92] https://fra.europa.eu/sites/default/files/fra uploads/fra-2019-facial-recognition-technology-focus-paper- 1 en.pdf, էջ 20:

Հետևաբար, կա անձնական տվյալների պաշտպանության իրավունքի բուն էության, այն է՝ անձեռնմխելի հիմքի վրա ազդելու մեծ հավանականություն: Դրա մասին հստակ վկայում են (տե՛ս ուղեցույցի 3.1.3.2 բաժինը) մասնավորապես հետևյալը., մարդկանց եզակի կենսաբանական առանձնահատկությունները մեծ մասշտաբով ավտոմատ կերպով մշակվում են իրավապահ մարմինների կողմից արժանահավատության վրա հիմնված ալգորիթմների միջոցով՝ արդյունքների միայն սահմանափակ բացատրելիությամբ: Անձնական կյանքի անձեռնմխելիության և տվյալների պաշտպանության իրավունքների սահմանափակումները կիրառվում են՝ անկախ անձի անհատական վարքագծից կամ նրան վերաբերող հանգամանքներից: Վիճակագրորեն այս միջամտությունից ազդեցություն կրած գրեթե բոլոր տվյալների սուբյեկտներն օրինապաշտ անձինք են: Տվյալների սուբյեկտին տեղեկություններ տրամադրելու միայն սահմանափակ հնարավորություններ կան: Դատարան դիմելը մեծամասամբ հնարավոր է լինում միայն հետագայում:

Արժանահավատության վրա հիմնված և սահմանափակ բացատրելիությամբ համակարգին ապավինելը կարող է հանգեցնել պատասխանատվության ցրման (դիֆուզիայի) և իրավական պաշտպանության միջոցների բացակայության, ինչպես նաև կարող է խթան հանդիսանալ անփութության համար:

Երբ նման համակարգը, որը կարող է կիրառվել նաև գործող տեսահսկման տեսախցիկների դեպքում, գործարկվում է նվազագույն ջանքերով և անձանց համար աննկատ կերպով, այն կարող է չկիրառվել ըստ նպատակի և հնարավորություն տալ համակարգված ու արագ կերպով կազմելու մարդկանց ցուցակներ՝ ըստ էթնիկ ծագման, սեռի, կրոնական պատկանելիության և այլն: Անձնական տվյալների մշակման սկզբունքը նախապես սահմանված չափանիշներով, ինչպիսիք են անձի գտնվելու վայրը և անցած ուղին, արդեն կիրառվել է[93] և հակված է խտրականության կիրառման:

Կախված մշակված տվյալների զգայունությունից, արտահայտչականությունից ու քանակից, հանրային վայրերում դեմքի ճանաչման համակարգերը կարող են չկիրառվել ըստ նպատակի՝ վնասակար ազդեցություն ունենալով համապատասխան անձանց վրա: Այդ տվյալները կարող են նաև հեշտությամբ հավաքվել և սխալ օգտագործվել՝ զսպումների և հակակշիռների սկզբունքի հիմնական դերակատարների վրա ճնշում գործադրելու նպատակով, ինչպիսիք են՝ քաղաքական ընդդիմությունը, ծառայողներն ու լրագրողները:

Վերջապես, ԴՃՏ համակարգերը, որպես կանոն, ներառում են խիստ կողմնակալ ազդեցություն ռասայի և գենդերի առնչությամբ. կեղծ դրական արդյունքներն անհամաչափորեն ներազդում են մաշկի տարբեր գույն ունեցող մարդկանց և կանանց վրա[94]՝ հանգեցնելով խտրականության: Կեղծ դրական արդյունքից հետո ոստիկանության կողմից ձեռնարկվող միջոցները, ինչպիսիք են խուզարկությունները և ձերբակալությունները, էլ ավելի են խորացնում այս խմբերի նկատմամբ մերժողական վերաբերմունքը:

[93] Տե՛ս Ահաբեկչական հանցագործությունների և ծանր հանցագործությունների կանխման, բացահայտման, քննության և հետապնդման համար ուղևորների վերաբերյալ տվյալների գրանցման շտեմարանի (PNR) օգտագործման վերաբերյալ Եվրոպական պառլամենտի և Խորհրդի 2016 թվականի ապրիլի 27-ի 2016/681 հրահանգի (ԵՄ) 6-րդ հոդվածը և Ճամփորդական տեղեկությունների և թույլտվությունների եվրոպական համակարգ ստեղծող և թիվ 1077/2011, թիվ 515/2014 (ԵՄ), 2016/399 (ԵՄ), 2016/1624 (ԵՄ) և 2017/2226 կանոնակարգը (ԵՄ) փոփոխող՝ 2018 թվականի սեպտեմբերի 12-ի Եվրոպական պառլամենտի և Խորհրդի 2018/1240 կանոնակարգի (ԵՄ) 33-րդ հոդվածը:

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf:

5.4. Եզրակացություն

Հանրային տարածքներում նույնականացման նպատակով կենսաչափական տվյալների հեռավար մշակմանը վերաբերող վերոնշյալ սցենարներն արդար հավասարակշռություն չեն ապահովում մասնավոր և հանրային մրցակցող շահերի միջև՝ ինչն իրենից ներկայացնում է տվյալների սուբյեկտի իրավունքներին անհամաչափ միջամտություն՝ համաձայն Խարտիայի 7-րդ և 8-րդ հոդվածների:

6 ՍՑԵՆԱՐ 6

6.1. Նկարագիրը

Մասնավոր սուբյեկտը տրամադրում է հավելված, որի միջոցով համացանցից ներբեռնվում են դեմքի պատկերներ՝ տվյալների շտեմարան ստեղծելու նպատակով: Օգտատերը, օրինակ՝ ոստիկանությունը, այնուհետև կարող է վերբեռնել նկար, և օգտագործելով կենսաչափական նույնականացումը, հավելվածը կփորձի այն համապատասխանեցնել իր տվյալների շտեմարանում առկա դեմքի պատկերներին կամ կենսաչափական մոդելներին:

Տարածքային ոստիկանության բաժանմունքն իրականացնում է տեսանյութով ֆիքսված հանցագործության քննություն, որտեղ հնարավոր չէ նույնականացնել մի շարք պոտենցիալ վկաների և կասկածյալների՝ հավաքված տեղեկությունները որևէ ներքին տվյալների շտեմարանի կամ հետախուզական տվյալների հետ համապատասխանեցնելու միջոցով: Հավաքված տեղեկությունների հիման վրա անձինք գրանցված չեն ոստիկանությունում առկա որևէ տվյալների շտեմարանում: Ոստիկանությունը որոշում է կիրառել վերը նկարագրված՝ մասնավոր ընկերության կողմից տրամադրված գործիքը՝ կենսաչափական նույնականացման միջոցով անձանց նույնականացնելու համար:

Տեղեկությունների աղբյուր.

- Տվյալների սուբյեկտների տեսակներ. ☒ բոլոր քաղաքացիները (վկաներ) ☒ դատապարտյալներ ☒ կասկածյալներ
- Պատկերի աղբյուր. ☒ հանրային վայրից կամ նախնական քննության շրջանակներում այլ վայրերից հավաքագրված տեսանյութեր
- Հանցագործության հետ կապ ☒ պարտադիր չէ
- Տեղեկությունների հավաքագրման եղանակ. ☒ հեռավար
- Այլ հիմնարար իրավունքների վրա ազդող համատեքստ ☒ այո, մասնավորապես՝ ☒ հավաքների ազատություն ☒ խոսքի ազատություն ☒ այլ.

Վկայակոչման տվյալների շտեմարան (որի հետ համեմատվում են հավաքագրված տեղեկությունները).

- Կոնկրետություն. ☒ համացանցից համալրված ընդհանուր նշանակության տվյալների շտեմարաններ

Ալգորիթմ.

- Մշակման տեսակ. ☒1-ը շատի հետ նույնականացում

Արդյունք.

- Ազդեցություն ☒ ուղղակի (օրինակ՝ տվյալների սուբյեկտը ձերբակալվել, հարցաքննվել է, խտրական վերաբերմունք)

Ավտոմատ որոշում. ☒ ՈՉ

Իրավական վերլուծություն.

- Տվյալների սուբյեկտի համար նախնական տեղեկությունների տեսակ. ☒ ՈՉ

6.2. Կիրառելի իրավական շրջանակը

Երբ մասնավոր սուբյեկտը մատուցում է անձնական տվյալների մշակման ծառայություն, որի համար որոշում է դրա նպատակն ու միջոցները (այս դեպքում տվյալների շտեմարան ստեղծելու համար համացանցից նկարներ ներբեռնելը), այդ մասնավոր սուբյեկտն այդ մշակման համար պետք է ունենա իրավական հիմք: Ավելին, իրավապահ մարմինը, որը որոշում է օգտվել այս ծառայությունից իր նպատակների համար, պետք է մշակման համար ունենա իրավական հիմք, որի համար որոշում է դրա նպատակներն ու միջոցները: Որպեսզի իրավապահ մարմինը կարողանա մշակել կենսաչափական տվյալներ, պետք է առկա լինի իրավական շրջանակ, որով սահմանվում են նպատակը, մշակման ենթակա անձնական տվյալները, մշակման նպատակները և անձնական տվյալների ամբողջականության ու գաղտնիության պահպանման, ինչպես նաև դրանց ոչնչացման ընթացակարգերը:

Այս սցենարը ենթադրում է անձնական տվյալների զանգվածային հավաքագրում այն անձանցից, որոնք տեղյակ չեն իրենց տվյալների հավաքագրման մասին: Այդ մշակումը կարող է օրինական լինել միայն խիստ բացառիկ հանգամանքներում: Կախված այն հանգամանքից, թե որտեղ է տեղակայված տվյալների շտեմարանը՝ այդ ծառայությունից օգտվելը կարող է հանգեցնել անձնական տվյալների և (կամ) հատուկ կատեգորիայի անձնական տվյալների՝ Եվրոպական միությունից դուրս փոխանցման (ոստիկանության կողմից, օրինակ՝ «ուղարկելով» տեսահսկման համակարգերով ֆիքսված տեսանյութի կամ դեմքի՝ այլ կերպ հավաքագրված պատկերը), որի համար պահանջվում են հատուկ պայմաններ, տե՛ս ԻԿՀ 39-րդ հոդվածը:

Այս սցենարում չկան հատուկ կանոններ, որոնք թույլ են տալիս իրավապահ մարմնի կողմից այդ մշակումը:

6.3. Անհրաժեշտությունը և համաչափությունը

Իրավապահ մարմինների կողմից ծառայությունից օգտվելը վկայում է այն մասին, որ անձնական տվյալները փոխանցվում են տվյալների շտեմարան օգտագործող մասնավոր սուբյեկտի, որտեղ անսահմանափակ, զանգվածային կերպով հավաքագրվում են անձնական տվյալները: Ոչ մի կապ չկա հավաքագրված անձնական տվյալների և իրավապահ մարմնի կողմից հետապնդվող նպատակի միջև: Իրավապահ մարմնի կողմից մասնավոր սուբյեկտին տվյալների փոխանցումը վկայում է նաև մասնավոր սուբյեկտի կողմից մշակվող տվյալների նկատմամբ մարմնի վերահսկողության բացակայության և տվյալների սուբյեկտների կողմից իրենց իրավունքների իրացման մեծ դժվարության մասին, քանի որ նրանք տեղյակ չեն իրենց տվյալների՝ այդկերպ մշակման մասին: Սա շատ բարձր նշաձող է սահմանում այն իրավիճակների համար, երբ այդ մշակումը կարող է տեղի ունենալ: Վիճելի է, թե արդյոք որևէ նպատակ կհամապատասխանի Հրահանգով սահմանված պահանջներին, քանի որ անձնական կյանքի անձեռնմխելիության և տվյալների պաշտպանության իրավունքներից ցանկացած շեղում և դրանց ցանկացած սահմանափակում կիրառելի է միայն խիստ անհրաժեշտության դեպքում: Ծանր հանցագործությունների դեմ պայքարի արդյունավետության ընդհանուր շահն ինքնին չի կարող արդարացնել մշակումը, երբ հսկայական ծավալի տվյալները հավաքագրվում են ոչ ընտրողաբար: Հետևաբար, այդ մշակումը չի համապատասխանի անհրաժեշտության և համաչափության պահանջներին:

6.4. Եզրակացություն

Հրահանգի 4-րդ և 10-րդ հոդվածների պահանջներին համապատասխանող հստակ, ճշգրիտ և կանխատեսելի կանոնների բացակայությունը, ինչպես նաև ապացույցների բացակայությունն առ այն, որ այդ մշակումը խիստ անհրաժեշտ է նախատեսված նպատակներին հասնելու համար, հանգեցնում է այն եզրակացության, որ սույն հավելվածի օգտագործումը չի բավարարում անհրաժեշտության և համաչափության պահանջներին և նշանակում է անհամաչափ միջամտություն տվյալների սուբյեկտների անձնական կյանքի նկատմամբ հարգանքի և անձնական տվյալների՝ Խարտիային համապատասխան պաշտպանության իրավունքներին: