«ԴատաԼեքս» դատական տեղեկատվական համակարգում անձնական տվյալների պաշտպանության և ապաանձնավորման խնդրի վերաբերյալ ՀՔԱ Վանաձորի գրասենյակի դիրքորոշումը

Թեև «ԴատաԼեքս» դատական տեղեկատվական համակարգի միջոցով որոշակի առումով ապահովվում է դատավորների հաշվետվողականությունը և դատական ակտերը հանրությանը հասանելի դարձնելը երաշխավորում է դատավորների գործունեության թափանցիկությունը, սակայն դատական համակարգի գործունեության հանրային հաշվետվողականության բարձրացումը չի կարող իրականացվել անձի մասնավոր և ընտանեկան կյանքի գաղտնիության, ինչպես նաև անձնական տվյալների պաշտպանության իրավունքների խախտմամբ:

«ԴատաԼեքս» դատական տեղեկատվական համակարգում ամեն օր հրապարակվում են հարյուրավոր դատական ակտեր, որոնցով բացահայտվում են անձնական՝ կենսաչափական, հատուկ կատեգորիայի անձնական տվյալներ, անձի անձնական և ընտանեկան կյանքին առնչվող տեղեկություններ: Ընդ որում, նշված տվյալների՝ «ԴատաԼեքս» դատական տեղեկատվական համակարգում հրապարակվելուց հետո հեռացման կամ ոչնչացման կարգ նախատեսված չէ, ինչը ենթադրում է անձի անձնական տվյալների հասանելիություն այլ անձանց համար: Հատկապես մտահոգիչ է այնպիսի զգայունության անձնական տվյալների հրապարակումը, որոնք առնչվում են անձի ֆիզիկական և հոգեկան առողջությանը[1], մարդու իմունային անբավարարության հարուցիչով (ՄԻԱՎ) վարակված լինելու հանգամանքին[2]: Հազարավոր դատական ակտերում նշվում են կողմերի անձնագրային տվյալները[3], հաշվառման հասցեները: Որոշ դեպքերում համակարգում ձևական առումով գործադրվում են միջոցներ անձնական տվյալները «փակելու» ուղղությամբ, սակայն դատական ակտի ուսումնասիրությունից անձի ինքնությունը բացահայտվում է: Մասնավորապես, անձին հարկադիր հոսպիտալացման ենթարկելու վերաբերյալ մի շարք դատական գործերով թեև «Պատասխանող» դաշտը դատարկ է թողնվում, այնուամենայնիվ «Պահանջ» դաշտում և դատական ակտում լրացվում է անձի անուն-ազգանունը, որով բացահայտվում է անձի ինքնությունը[4]:

«ԴատաԼեքս» դատական տեղեկատվական համակարգում անձնական տվյալների պաշտպանության խնդրի մասին բարձրաձայնվել է 2012 թվականից: Դատական ակտերի որոնման համակարգում դատավարության մասնակիցների անձնական տվյալների

[1] Տե՛ս օրինակ՝ http://www.datalex.am/?app=AppCaseSearch&case_id=35465847065588578 http://www.datalex.am/?app=AppCaseSearch&case_id=15481123719153742:

[2] Տե՛ս օրինակ՝ http://www.datalex.am/?app=AppCaseSearch&case_id=30962247438248444, http://www.datalex.am/?app=AppCaseSearch&case_id=33495522228627017:

[3] Տե՛ս օրինակ՝ http://www.datalex.am/?app=AppCaseSearch&case_id=14355223812313214:

[4] Տե՛ս օրինակ՝ http://www.datalex.am/?app=AppCaseSearch&case_id=45880421204151333 http://www.datalex.am/?app=AppCaseSearch&case_id=27303072741064902 http://www.datalex.am/?app=AppCaseSearch&case_id=14355223812351407 http://www.datalex.am/?app=AppCaseSearch&case_id=45880421204119901:

պաշտպանության ուղղությամբ միջոցառումների ձեռնարկումը դեռևս նախատեսված էր ՀՀ իրավական և դատական բարեփոխումների 2012-2016 թվականների ռազմավարական ծրագրից բխող միջոցառումների ծրագրով: Թեև գործողությունը չի կատարվել, սակայն վերջինս ՀՀ իրավական և դատական բարեփոխումների 2012-2016 թվականների ռազմավարական ծրագրից բխող միջոցառումների 2016 թվականին կատարման վիճակի վերաբերյալ հաշվետվությամբ նշվել է որպես ամբողջությամբ կատարված՝ մանրամասնելով, որ «ԴատաԼեքս» դատական տեղեկատվական համակարգում անձնական տվյալները «փակվել» են 2015 թվականի մայիսի 18-ին ընդունված և 2015 թվականի հուլիսի 1-ին ուժի մեջ մտած՝ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջների հիման վրա, որոնք սահմանում են պետական կառավարման կամ տեղական ինքնակառավարման մարմինների, պետական կամ համայնքային հիմնարկների կամ կազմակերպությունների, իրավաբանական կամ ֆիզիկական անձանց կողմից անձնական տվյալները մշակելու, դրանց նկատմամբ պետական հսկողություն իրականացնելու կարգն ու պայմանները:

Անձնական տվյալների պաշտպանության խնդրին դատական ակտերի հրապարակման համատեքստում անդրադարձել է նաև Մարդու իրավունքների պաշտպանը մարդու իրավունքների և ազատությունների պաշտպանության վիճակի մասին իր 2019[5] և 2020[6] թվականների հաղորդումներում:

Անձնական տվյալների հրապարակման նշված պրակտիկան խնդրահարույց է անձնական տվյալների պաշտպանության միջազգային իրավական և ներպետական օրենսդրության կարգավորումների տեսանկյունից:

Անձնական տվյալների պաշտպանությունը երաշխավորված է «Մարդու իրավունքների և հիմնարար ազատությունների պաշտպանության մասին» եվրոպական կոնվենցիայի (այսուհետ նաև՝ ՄԻԵԿ)՝ անձնական և ընտանեկան կյանքը հարգելու իրավունքն ամրագրող 8-րդ հոդվածով, որի իրացումը կարող է սահմանափակվել այն դեպքերում, 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 և ազատությունների պաշտպանության նպատակով:

Դատական վարույթի հրապարակայնությանը և դատական համակարգի հաշվետվողականությանը՝ որպես Կոնվենցիայի 8-րդ հոդվածով ամրագրված իրավունքը սահմանափակող նպատակի, անդրադարձել է Մարդու իրավունքների եվրոպական դատարանը (այսուհետ նաև՝ Դատարան)՝ սահմանելով, որ գնահատման սահման պետք է թողնել իրավասու ազգային մարմիններին՝ ելնելով դատական վարույթի

[5] Մարդու իրավունքների և ազատությունների պաշտպանության վիճակի մասին ՄԻՊ 2019 թ. հաղորդում՝ https://ombuds.am/images/files/15b2661f76d10eb07746d7d4d4dec84f.pdf, էջ. 268-269:
[6] Մարդու իրավունքների և ազատությունների պաշտպանության վիճակի մասին ՄԻՊ 2020 թ. հաղորդում՝ https://ombuds.am/images/files/883f55af65e3c33553139031c7ac0ce6.pdf, էջ. 421-423:

հրապարակայնության շահերից, մի կողմից, և երաշխավորել կողմի կամ երրորդ անձի շահերը նման տվյալների գաղտնիությունը պահպանելու հարցում: Այս լուսանցքի շրջանակը կախված կլինի այնպիսի գործոններից, ինչպիսիք են քննարկվող շահերի բնույթն ու լրջությունը և միջամտության աստիճանը[7]:

Դատարանը ընդգծել է, որ միջամտությունը կհամարվի «անհրաժեշտ ժողովրդավարական հասարակությունում» օրինական նպատակի համար, եթե այն համապատասխանի «անհետաձգելի հասարակական պահանջի» (“pressing social need”), և, մասնավորապես, եթե այն համարժեք է հետապնդվող օրինական նպատակին և եթե ազգային իշխանությունների ներկայացրած պատճառները դա հիմնավորելու համար «համապատասխան և բավարար» են: Անձի անձնական տվյալների բացահայտմանը միտված ցանկացած միջոց, անկախ անձի դատավարական կարգավիճակից, պետք է բավարարի գերակա սոցիալական կարիքը[8] և պետք է հնարավորինս սահմանափակվի այն ամենով, ինչ խիստ անհրաժեշտ է՝ ելնելով վարույթի հատուկ բնույթից[9]:

Վերոնշյալ նկատառումները հատկապես կարևոր են անձի՝ ՄԻԱՎ-ով ապրելու վերաբերյալ տեղեկատվության գաղտնիության պաշտպանության հարցում: Նման տվյալների բացահայտումը կարող է էապես ազդել անհատի անձնական և ընտանեկան կյանքի, ինչպես նաև սոցիալական և զբաղվածության վիճակի վրա՝ ենթարկելով նրան դատապարտման և օստրակիզմի վտանգի: Այդ պատճառով այն կարող է նաև հուսալքել անձանց ախտորոշում կամ բուժում փնտրել և դրանով իսկ խարխլել վարակի տարածումը զսպելու համայնքի ցանկացած կանխարգելիչ ջանքը: Այսպիսով, նման տեղեկատվության գաղտնիությունը պաշտպանելու շահերը կարևոր կլինեն որոշելու համար, թե արդյոք միջամտությունը համաչափ էր հետապնդվող օրինական նպատակին: Նման միջամտությունը չի կարող համատեղելի լինել Կոնվենցիայի 8 -րդ հոդվածի հետ, եթե այն հիմնավորված չէ հանրային շահերից բխող հիմնարար պահանջով[10]:

Կոնվենցիայի բոլոր Պայմանավորվող կողմերի իրավական համակարգերում առողջության տվյալների գաղտնիության պահպանումը կենսական սկզբունք է: Պարտադիր է ոչ միայն հարգել պացիենտի գաղտնիության զգացումը, այլև պահպանել նրա վստահությունը բժշկական մասնագիտության և առհասարակ առողջապահական ծառայությունների նկատմամբ: Առանց այդպիսի պաշտպանության, բժշկական օգնության կարիք ունեցող անձինք կարող են զերծ մնալ այնպիսի անձնական և մտերիմ տեղեկատվության բացահայտումից, որոնք կարող են անհրաժեշտ լինել համապատասխան բուժում ստանալու համար, և նույնիսկ նման օգնության դիմելուց՝ դրանով իսկ վտանգելով սեփական առողջությունը, իսկ վարակիչ հիվանդությունների դեպքում՝ համայնքի առողջությունը: ՄԻԵԴ-ը սահմանել է, որ ներքին օրենսդրությունը պետք է ապահովի

[7]Guide to the Case-Law of the European Court of Human Rights, Data protection, para. 240.
[8] Վիսենտ Դել Կամպոն ընդդեմ Իսպանիայի, 2018 թ., պարբ. 46:
[9] L.L. v. France, 2006, para. 45.
[10] Z. v. Finland, 9/1996/627/811, Council of Europe: European Court of Human Rights, 25 February 1997, available at: https://www.refworld.org/cases,ECHR,3ae6b71d0.html [accessed 20 August 2021], para. 96.

համապատասխան երաշխիքներ՝ կանխելու առողջության անձնական տվյալների ցանկացած հրապարակում կամ բացահայտում, որը կարող է չհամապատասխանել Կոնվենցիայի 8 -րդ հոդվածով սահմանված երաշխիքներին[11]:

Զ-ն ընդդեմ Ֆինլանդիայի գործով ՄԻԵԴ-ը արձանագրել է Կոնվենցիայի 8-րդ հոդվածի խախտում առ այն, որ դիմումատուի բժշկական անձնական տվյալները դեռևս 2002թ. հանրությանը հասանելի են դարձվել՝ կապված Վերաքննիչ դատարանի վճռում դիմողի ինքնության և առողջական վիճակի հրապարակման հետ: Ներպետական դատարանները 10 տարով սահմանափակել էին գործի նյութերի փաստաթղթերի գաղտնիության ժամկետը, որոնք բացահայտում էին դիմումատուի ինքնությունը և ՄԻԱՎ-դրական վիճակը: Դատարանը 8-րդ հոդվածի խախտում է արձանագրել՝ հիմնավորելով, որ դատական իշխանությունները անբավարար կշիռ են հաղորդել կողմերի և երրորդ անձանց անձնական տվյալների պաշտպանության շահերին: Անձնական կյանքի նկատմամբ հարգանքի իրավունքի լուրջ միջամտությունը, որն առաջացել է դատական գործընթացներում, առանց դիմումատուի համաձայնության իր առողջական վիճակի վերաբերյալ տեղեկատվության հրապարակմամբ, ավելի կսրվեր, եթե տվյալ բժշկական տեղեկատվությունը հանրությանը հասանելի դառնա տասը տարի անց[12]:

Որպեսզի պարզվի, թե առկա են բավարար հիմքեր անձի ինքնությունը և այլ անձնական տվյալները դատական ակտում բացահայտելու համար, կարևորագույն հարց է, թե արդյո՞ք նվազ չանհատականացնող միջոցներ սահմանված են եղել ներպետական իրավունքում և պրակտիկայում: Նշվածը ընդգրկում է դատարանի հնարավորությունը ապաանձնավորել վճիռը՝ չհիշատակելով անուններ, վճռի պատճառաբանական մասը գաղտնի պահելը որոշակի ժամանակահատվածում և դրա փոխարեն պատճառաբանական մասի կրճատված տարբերակի հրապարակումը[13], կամ կրճատել վճռի տեքստը կամ դրանում որոշ հարցերը[14]: Դատարանը հաստատել է, որ այդպիսի միջոցներն ընդհանուր առմամբ ունակ են նվազեցնելու դատավարության ազդեցությունը տվյալների սուբյեկտի անձնական կյանքի պաշտպանության իրավունքի վրա[15]:

Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին Կոնվենցիայի (1981 թվականի հունվարի 28-ի «Կոնվենցիա 108») 5-րդ հոդվածի համաձայն՝ տվյալների մշակումը պետք է համաչափ լինի հետապնդվող օրինական նպատակին, արտացոլի մշակման բոլոր փուլերում արդար հավասարակշռություն՝ շահագրգիռ շահերի՝ պետական և մասնավոր, և իրավունքների ու ազատությունների միջև: Յուրաքանչյուր Կողմ ապահովում է, որ տվյալների մշակումը

[11] Z v. Finland, 1997, § 95.
[12] Z v. Finland, 1997, §§ 111-112.
[13] Z v. Finland, 1997,1997, § 113.
[14] Vicente del Campo v. Spain, 2018, § 50.
[15] Guide to the Case-Law of the European Court of Human Rights, Data protection, para. 241.

կարող է իրականացվել տվյալների սուբյեկտի ազատ, հստակ, գիտակցված և միանշանակ համաձայնության կամ օրենքով սահմանված այլ օրինական հիմունքների հիման վրա (...)[16]:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 5-րդ հոդվածի համաձայն՝ «1. Տվյալների մշակումը պետք է հետապնդի օրինական նպատակ, դրան հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ և չափավոր: (…) 4. Արգելվում է անձնական տվյալների մշակումը, եթե տվյալները մշակելու նպատակին հնարավոր է հասնել ապանձնավորված կերպով:

5. Անձնական տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան անհրաժեշտ է դրանց նախօրոք որոշված նպատակներին հասնելու համար:»:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 26-րդ հոդվածի համաձայն՝ «1. Առանց անձնական տվյալների սուբյեկտի համաձայնության՝ մշակողը կարող է անձնական տվյալները փոխանցել երրորդ անձանց կամ տվյալներից օգտվելու հնարավորություն տրամադրել, եթե դա նախատեսված է օրենքով և ունի բավարար պաշտպանության մակարդակ: 2. Առանց անձնական տվյալների սուբյեկտի համաձայնության՝ մշակողը կարող է հատուկ կատեգորիայի անձնական տվյալներ փոխանցել երրորդ անձանց կամ տվյալներից օգտվելու հնարավորություն տրամադրել, եթե՝ 1) տվյալներ մշակողը հանդիսանում է օրենքով կամ վավերացված միջազգային պայմանագրով սահմանված հատուկ կատեգորիայի անձնական տվյալներ մշակող, այդ տեղեկության փոխանցումը ուղղակիորեն նախատեսված է օրենքով և ունի բավարար պաշտպանության մակարդակ. 2) օրենքով նախատեսված բացառիկ դեպքերում հատուկ կատեգորիայի անձնական տվյալները կարող են փոխանցվել տվյալների սուբյեկտի կյանքի, առողջության կամ ազատության պաշտպանության համար»:

Այսպիսով, որպես դատական համակարգի գործունեության հաշվետվողականության և անձնական տվյալների պաշտպանության միաժամանակյա ապահովման իրավաչափ և ողջամիտ տարբերակ է դատական ակտերի ապաանձնավորումը, որն ուղղակիորեն բխում է նաև «Անձնական տվյալների պաշտպանության մասին» օրենքի 5-րդ հոդվածի 4-րդ մասից:

Անձնական կյանքի տվյալներ, կենսաչափական և հատուկ կատեգորիայի անձնական տվյալներ, երեխայի անձնական տվյալներ պարունակող դատական ակտերի հրապարակման ապաանձնավորված կարգի վերաբերյալ դրույթ նախատեսում է «ՀՀ դատական օրենսգիրք» սահմանադրական օրենքը, որի 11-րդ հոդվածի 10-րդ մասի համաձայն. «Դատական իշխանության պաշտոնական կայքում անձնական կյանքի տվյալներ, կենսաչափական և հատուկ կատեգորիայի անձնական տվյալներ, երեխայի անձնական տվյալներ պարունակող դատական ակտերը հրապարակվում են ապանձնավորված կարգով: Բարձրագույն դատական խորհուրդը կարող է սահմանել

[16] Հասանելի է՝ https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=W0JaOjG2

անձնական տվյալների ապանձնավորման այլ դեպքեր: Ապանձնավորման կարգը սահմանում է Բարձրագույն դատական խորհուրդը»:

Հարկ է նկատել, որ նշված կարգը վերաբերում է միայն դատական իշխանության պաշտոնական կայքին, այն է՝ «court.am»-ին, մինչդեռ վերջինում հրապարակվում են միայն Դատավորին կարգապահական պատասխանատվության ենթարկելու մասին Բարձրագույն դատական խորհրդի որոշումները, իսկ մյուս դատական ակտերը հրապարակվում են «ԴատաԼեքս» դատական տեղեկատվական համակարգում:

Ի ապահովումն «ՀՀ դատական օրենսգիրք» սահմանադրական օրենքի 11-րդ հոդվածի՝ Բարձրագույն դատական խորհուրդը 2018 թվականի սեպտեմբերի 27-ին կայացված թիվ ԲԴԽ-40-Ո-105 որոշմամբ (այսուհետ՝ Որոշում) սահմանել է դատական իշխանության պաշտոնական կայքում հրապարակվող դատական ակտերում անձնական տվյալների ապանձնավորման կարգը և անձնական տվյալների ապանձնավորման այլ դեպքերը: Նշված որոշմամբ, սակայն, Բարձրագույն դատական խորհուրդը անդրադարձել է ոչ միայն դատական իշխանության պաշտոնական կայքում, այլ նաև «դատական համակարգ»-ում անձնական տվյալների ապաանձնավորմանը: Մասնավորապես, Որոշման 1-ին Հավելվածի 5-րդ կետի համաձայն. «Դատական համակարգ» համակարգչային ծրագիրն ավտոմատ կերպով դատական ակտի տեքստում նույնականացնում և ապանձնավորում է սույն կարգում նշված ապանձնավորման ենթակա անձնական տվյալները՝ պահպանելով ապանձնավորման գործընթացին ձեռքով միջամտելու հնարավորությունը: Նշված ծրագրի միջոցով ապահովվում է նաև ավտոմատացված եղանակով դատական իշխանության պաշտոնական կայքում ապանձնավորված կերպով դատական գործի և դրա ընթացքի հրապարակումը»:

Որոշման 1-ին Հավելվածի 12-րդ կետի համաձայն. «Դատական ակտում առկա Անձնական տվյալների ապանձնավորման նկատմամբ հսկողությունն իրականացնում է տվյալ ակտն ընդունող դատավորը»:

Որոշման 2-րդ հավելվածի 3-րդ կետի համաձայն. «Դատական ակտում առկա բոլոր անձնական տվյալների ապանձնավորումն իրականացվում է համապատասխան համակարգչային ծրագրի միջոցով՝ ձեռքով ապանձնավորելու (տվյալները փակելու կամ փոխարինելու) եղանակով՝ մինչև ապանձնավորման ծրագրային միասնական համակարգի ներդրումը, որից հետո ապանձնավորումն իրականացվելու է ավտոմատացված եղանակով»:

Որոշման 1-ին Հավելվածի 3-րդ կետի համաձայն. «ՀՀ դատական օրենսգիրք» սահմանադրական օրենքի և «Անձնական տվյալների պաշտպանության մասին» օրենքի պահանջների շրջանակում սույն կարգին համապատասխան ապանձնավորվում են ֆիզիկական անձանց վերաբերյալ հետևյալ անձնական տվյալները՝ 1) անձնագրի, նույնականացման քարտի կամ անձի ինքնությունը հաստատող այլ փաստաթղթի, ինչպես նաև անձի վերաբերյալ առևտրային, հարկային, բանկային, ապահովագրական, ծառայողական, կրոնական, կուսակցական, էթնիկ, ռասայական, կրթական և բժշկական տվյալներ պարունակող փաստաթղթի համարը և սերիան, 2) հաշվառման և/կամ բնակության վայրի հասցեները, 3) հեռախոսի, ֆաքսի և էլեկտրոնային փոստի համարները և

հասցեները, 4) բանկային, ապահովագրական և այլ հաշվեհամարները, 5) անշարժ գույքի գտնվելու հասցեն, կադաստրային ծածկագիրը, անշարժ գույքի նկատմամբ իրավունքի պետական գրանցման վկայականի համարը և սերիան, 6) ավտոմեքենայի համարանիշը, տրանսպորտային միջոցի նկատմամբ իրավունքի պետական գրանցման (հաշվառման) վկայականի (վկայագրի) համարը և սերիան, 7) քրեական գործերով՝ տուժողի, վկայի և ընթերակայի անունը, ազգանունը, հայրանունը, 8) քաղաքացիական, վարչական և սնանկության գործերով՝ վկայի անունը, ազգանունը, հայրանունը:

Որոշման 2-րդ Հավելվածի 1-ին մասի համաձայն. «Հայաստանի Հանրապետության դատական օրենսգիրք» սահմանադրական օրենքով սահմանված դեպքերից բացի, հրապարակման ենթակա դատական ակտերի ապանձնավորումն իրականացվում է նաև այն դեպքերում, երբ դրանք պարունակում են հետևյալ անձնական տվյալները. 1) օրենքով սահմանված պարտադիր զինվորական ծառայության զորակոչի միջոցով իրականացվող շարքային կազմի պարտադիր զինվորական ծառայության և հանրային ծառայության վերաբերյալ այնպիսի տեղեկություններ, որոնք կարող են թույլ տալ նույնականացնելու վերը նշված ծառայություն իրականացնող զինծառայողին կամ հանրային ծառայողին: 2) ֆիզիկական անձին պատկանող գույքի վերաբերյալ այնպիսի տեղեկություններ, որոնք կարող են թույլ տալ նույնականացնելու տվյալ ֆիզիկական անձին»:

Այսպիսով, թեև «ՀՀ դատական օրենսգիրք» սահմանադրական օրենքը ուղղակիորեն նախատեսում է միայն դատական իշխանության պաշտոնական էջում առկա անձնական տվյալների ապաանձնավորման դրույթ, այնուամենայնիվ, Բարձրագույն դատական խորհուրդը սահմանել է նաև ապաանձնավորման պարտավորություն «դատական համակարգում» հրապարակվող դատական ակտերի հետ կապված՝ պատվիրակելով ներդնել ապանձնավորման ծրագիր և անձնական տվյալների պաշտպանության պարտականությունը յուրաքաչյուր գործով դնելով տվյալ գործով նախագահող դատավորի վրա: Դատական ակտերի ապաանձնավորման ծրագիրը, սակայն, մինչ օրս ներդրված չէ, իսկ դատավորների ներկայիս ծանրաբեռնվածության և մշակվող անձնական տվյալների ծավալի պայմաններում առանց ծրագրային ապահովման անհնար է իրականացնել դատական ակտերի ապաանձնավորումը: Ընդ որում, բացի ապաանձնավորման ծրագրի ներդրումից, հարկ է լուծել նաև դատական տեղեկատվական համակարգում արդեն իսկ առկա և հանրությանը հասանելի անձնական տվյալների հեռացման խնդիրը, քանի որ այն նպատակը, որը հետապնդում է «Դատական համակարգում» տվյալների հրապարակումը՝ դատական իշխանության գործունեության թափանցիկությունը և հանրային իրազեկվածությունը, քննված և ավարտված գործերով այլևս առկա չէ, ուստի նման տեղեկատվությունը նույնպես ենթակա է հեռացման: Նշված մոտեցումը համահունչ է անձնական տվյալների պաշտպանության միջազգային իրավական ոլորտում անձնական տվյալների հեռացման իրավունքի («մոռացվելու իրավունք») կարգավորումներին: Նշված տվյալների պահպանման ժամանակային սահմանափակում սահմանված չէ և նման կարգավորման բացակայության

պայմաններում անձը կախված է այն ջանասիրությունից, որով իշխանությունները կկիրառեն սահմանված երաշխիքները[17]:

Այսպիսով, դատական տեղեկատվական համակարգում անձնական տվյալները պետք է մշակվեն այն նվազագույն չափով, որն անհրաժեշտ է դատավարական որոշումների ու ժամկետների, ինչպես նաև դատական ակտերի հրապարակայնության ապահովման համար՝ երաշխավորելով սահմանված տվյալների ապաանձնավորումը:

Հաշվի առնելով վերոգրյալը՝ առաջարկում ենք.

1. <u>«ՀՀ դատական օրենսգիրք» սահմանադրական օրենքում նախատեսել «ԴատաԼեքս» դատական տեղեկատվական համակարգում տեղադրվող ակտերի ապաանձնավորման վերաբերյալ դրույթ:</u>
2. <u>«ԴատաԼեքս» դատական տեղեկատվական համակարգում ներդնել ապաանձնավորման ծրագիր՝ այդ թվում ապահովելով արդեն իսկ առկա անձնական տվյալների հեռացումը:</u>

[17] Guide to the Case-Law of the European Court of Human Rights, Data protection, p. 62.