2020
ԳՅՈՒՄՐԻ

ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ ՀԱՅԱՍՏԱՆՈՒՄ ԱՐՏԱԿԱՐԳ ԴՐՈՒԹՅԱՆ ՊԱՅՄԱՆՆԵՐՈՒՄ

Սույն զեկույցը պատրաստվել է՝ Ա.Դ.Սախարովի անվան մարդու իրավունքների պաշտպանության հայկական կենտրոնի աջակցությամբ

Հեղինակ՝
Վանուհի Գասպարյան

ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ ՀԱՅԱՍՏԱՆՈՒՄ ԱՐՏԱԿԱՐԳ ԴՐՈՒԹՅԱՆ ՊԱՅՄԱՆՆԵՐՈՒՄ

Բովանդակություն

ՆԱԽԱԲԱՆ 2

ՕՐԵՆՍԴՐԱԿԱՆ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ 4

ԱՐՏԱԿԱՐԳ ԴՐՈՒԹՅԱՆ ՊԱՅՄԱՆՆԵՐՈՒՄ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ԽԱԽՏՄԱՆ ԴԵՊՔԵՐԸ 11

Անձնական տվյալների խախտման դեպքեր՝ տեղեկատվական տեխնոլոգիաների կիրառմամբ 11
Հեռախոսների միջոցով տեղակայման վայրի ստուգում 11
Ինքնամեկուսացված քաղաքացիների քարտեզագրում 13

Անձնական տվյալների խախտման դեպքեր՝ սոցիալական ցանցերում արված հրապարակումներում 15
Կորոնավիրուսային վարակի տարածումը կանխելու նպատակով ՀՀ վարչապետ Նիկոլ Փաշինյանի կողմից քաղաքացիների լուսանկարների հրապարակումն իր ֆեյսբուկյան էջում 15
ՀՀ ԱԺ մարդու իրավունքների և պետաիրավական հարցերի հանձնաժողովի նախագահ, ԱԺ պատգամավոր, Նաիրա Զոհրաբյանի կողմից քաղաքացու անձնագրային տվյալների հրապարակումն իր ֆեյսբուկյան էջում։ 17

Անչափահասի անձնական տվյալների խախտում 20

Անձնական տվյալների պաշտպանության վտանգները՝ հեռավար կրթության պայմաններում 22

Պետական ինստիտուտների կողմից էլեկտրոնային փոստերի վարման քաղաքականությունը և կորոնավիրուսով վարակված քաղաքացիների անձնական տվյալների ու ընդհանուր ցանկերի արտահոսք 24

Որքանո՞վ են պահպանվում անձնական տվյալները էլեկտրոնային տեղեկատվական համակարգերում 26
ՀՀ ընտրողների ռեգիստր 26
Դատական տեղեկատվական համակարգ։ 28

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆՆԵՐ ԵՎ ԱՌԱՋԱՐԿՈՒԹՅՈՒՆՆԵՐ 30

ՎԵՐՋԱԲԱՆ 32

ՆԱԽԱԲԱՆ

Տեղեկատվական աշխարհում մարդու կյանքն անխուսափելիորեն իրեն ավելի թափանցիկ է դարձնում պետության և հասարակության համար, ուստի տեղեկատվության գաղտնիությունը պահպանելու ցանկությունը դառնում է ավելի ու ավելի շոշափելի:

Տեղեկատվական և հեռահաղորդակցական տեխնոլոգիաների զարգացումը, դրանց ներմուծումը հասարակության և պետության բոլոր ոլորտներ, բազմաթիվ քարտային ինդեքսների թվային ձևի փոխակերպումը մարդկանց ստիպեց մտածել այսօրինակ զգայուն տեղեկատվությունը պաշտպանելու անհրաժեշտության մասին: Նոր տեխնոլոգիաները, մի կողմից, զգալիորեն պարզեցրել են տվյալների հավաքումը, մշակումը, պահպանումը, փոխանցումը, իսկ մյուս կողմից՝ նրանք ստեղծել են դրանց ապօրինի շրջանառության ակնհայտ սպառնալիքներ, ինչը հանգեցնում է անձնական տվյալների իրավունքի խախտմանը:

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

Եթե անդրադառնանք համացանցին, ապա նկատելի է, որ տարբեր սոցիալական ցանցեր ու մեդիա հարթակներ օգտագործվում են ամբողջ աշխարհի մեծ թվով օգտատերերի կողմից, որոնց տրամադրվում են անձնական տվյալները որոշակի ծառայություններ մուտք գործելու և օգտագործման հնարավորության դիմաց:

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

Անձնական տվյալների պաշտպանության իրավունքի խախտումները և ոտնահարումները կարող են լուրջ սպառնալիքներ առաջացնել նաև երկրի ազգային անվտանգության համար, ուստի շատ կարևոր է, որ անձնական տվյալների պաշտպանությունը պետական հոգածության և ուշադրության ներքո լինի:

Հայաստանում ևս անձնական տվյալների պաշտպանության վիճակը խնդրահարույց է: Ընդ որում, այն խնդրահարույց է մի քանի ուղղություններով. քաղաքացիներն իրազեկված չեն իրենց իրավունքների մասին, պետությունը չի կատարում իր կողմից ստանձնած պարտավորությունները, խախտումների ուղղությամբ չեն իրականացվում վերականգնողական աշխատանքներ, դատաիրավական համակարգը քննում է փոքրաթիվ գործեր՝ չնայած ամենօրյա ակնառու և կոպիտ խախտումներին:

Այս և նմանատիպ այլ հիմնախնդիրների լուծման համար կարևոր է հանգամանորեն ուսումնասիրել անձնական տվյալների պաշտպանության իրավունքի սահմանադրական երաշխիքները և վեր հանել այն առանձնահատկությունները, որոնք ունի Հայաստանի Հանրապետությունը՝ անձնական տվյալների պաշտպանության իրավունքի իրացման հարցում:

ՕՐԵՆՍԴՐԱԿԱՆ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ

«Անձնական տվյալներ» նշանակում է՝ ինքնությունը հաստատված և ինքնությունը հաստատման ենթակա անհատների վերաբերյալ ցանկացած տեղեկատվություն: Շատ երկրների իրավական ակտերում անձնական տվյալները սահմանվում է որպես այնպիսի տեղեկատվություն, որի հիման վրա կարելի է նույնականացնել անհատին:

Անձնական տվյալների պաշտպանությունն առնչվում է կյանքի բոլոր ոլորտներին՝ կրթությունից, առողջապահությունից մինչև մարդու մուտքն ու ելքը սահմանային անցակետերով: Չկա մի ոլորտ, որտեղ անձնական տվյալների պաշտպանության խնդիրը չծագի՝ պետական, թե մասնավոր: Այս և նմանատիպ այլ խնդիրների լուծման համար պետական քաղաքականության գործունեությունն ուղղված է ինչպես այս իրավունքի մասին հանրային իրազեկմանն, այնպես էլ՝ օրենսդրական կարգավորմանը:

Ամբողջ աշխարհով ճանաչված են անձնական տվյալներ հավաքելու և մշակելու միջազգային չափանիշները: Երկրները այս ոլորտում իրենց ազգային օրենսդրությունը մշակելիս պարտադիր հաշվի են առնում անձնական տվյալներ հավաքելու և մշակելու միջազգային չափանիշները և սկզբունքները:

Մարդու իրավունքների համընդհանուր հռչակագիրը[1] մարդկության պատմության ամենակարևոր փաստաթղթերից մեկն է: Հռչակագրի 12-րդ հոդվածում ասվում է. «Ոչ ոք չի կարող ենթարկվել իր անձնական ու ընտանեկան կյանքում կամայական միջամտության, իր տան, իր նամակագրության կամ իր պատվի ու հեղինակության նկատմամբ կամայական ոտնձգությունների: Յուրաքանչյուր ոք ունի նման միջամտությունից կամ ոտնձգությունից օրենքի պաշտպանության իրավունք»:

Անձնական և ընտանեկան կյանքի հարգանքի իրավունքը պարունակում է նաև **Մարդու իրավունքների և հիմնարար ազատությունների պաշտպանության մասին կոնվենցիայում**[2], որի 8[1] հոդվածն ասում է. «Պետական մարմինների կողմից այդ իրավունքի իրականացման միջամտությունն արգելվում է, 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

[1] https://www.arlis.am/DocumentView.aspx?docID=1896
Հռչակագիրն ընդունվել է 1948 թվականի դեկտեմբերի 10-ին ՄԱԿ Գլխավոր ասամբլեայի կողմից
[2] https://www.arlis.am/documentview.aspx?docID=20870
Կոնվենցիան ընդունվել է 1950 թ. նոյեմբերի 4-ին Եվրոպայի խորհրդի կողմից

հանցագործությունների կանխման, առողջության կամ բարոյականության պաշտպանության կամ այլ անձանց իրավունքների և ազատությունների պաշտպանության նպատակով»:

Անձնական տվյալների պաշտպանության հարցի պատմությունը սկսվում է 1976 թվականից, երբ Եվրոպայի Խորհրդի նախարարների կոմիտեն ձեռնամուխ եղավ ֆիզիկական անձանց իրավունքների պաշտպանության նպատակով համապատասխան կոնվենցիայի նախապատրաստմանը: Այն արդեն 1981 թվականին պատրաստ ու բաց էր մասնակից պետությունների կողմից ստորագրվելու համար և կոչվում է **«Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիա**[3]: Դա առաջին միջազգային իրավական պարտադիր փաստաթուղթն է, որում տրված են այն ստորագրած մասնակից պետությունների քաղաքացիների պաշտպանության մեխանիզմները, որոնք կարող են խախտվել նրանց անհատական տվյալների հավաքման և մշակման գործընթացում:

Որպես եվրոպական քաղաքակրթության մաս և Եվրոպայի խորհրդի անդամ, Հայաստանն ընդունում է անձնական տվյալների պաշտպանության քաղաքականությունը՝ հիմնվելով եվրոպական չափորոշիչների և սկզբունքների վրա:

ՀՀ Սահմանադրության[4] 33, 34 և 42 հոդվածները այս կամ այն կերպ վերաբերում են տեղեկատվության անվտանգությանը: Օրինակ, Սահմանադրության 33 հոդվածը երաշխավորում է անձնական և ընտանեկան գաղտնիքների, նամակագրության, հեռախոսային խոսակցությունների, փոստային, հեռագրական և այլ հաղորդագրությունների գաղտնիության իրավունքը; 42 հոդվածը՝ տեղեկատվությունը ցանկացած իրավական ձևով ազատորեն որոնելու, ստանալու, փոխանցելու, արտադրելու և տարածելու իրավունքը:

Այս նորմատիվ իրավական ակտերի համակարգում կարևորագույն դեր է կատարում **«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը**[5] (այսուհետ՝ Օրենք), որն ընդունվել է 06.12.2015թ., իսկ ուժի մեջ է մտել 22.12.2015թ.: Հատկանշական է, որ այս օրենքի բազմաթիվ դրույթներ համահունչ են Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության

[3] https://www.arlis.am/DocumentView.aspx?DocID=80554
Կոնվենցիան վավերացվել է Հայաստանի Հանրապետության կողմից 01.09.2012թ., ՀՀԱԳՆՊՏ 2012.12.28/14(22):
[4] https://www.arlis.am/DocumentView.aspx?docID=102510
ՀՀ Սահմանադրություն
[5] https://www.arlis.am/documentview.aspx?docid=98338
ՀՀ ԱԺ-ի կողմից ընդունվել է 18.05.2015թ-ին

մասին 28.01.1981թ. կոնվենցիային: Օրենքով անձնական տվյալների պաշտպանությունը ստացել է պետական ապահովվածություն, հավասարակշռվել են անձնական տվյալների սուբյեկտների և մշակողների փոխադարձ իրավունքներն ու պարտականությունները, նաև՝ սահմանվել է անձնական տվյալների մշակման օրինականության նկատմամբ անկողմնակալ և մշտական հսկողություն իրականացնող մարմին՝ ՀՀ արդարադատության նախարարության աշխատակազմի Անձնական տվյալների պաշտպանության գործակալությունը (այսուհետ՝ Գործակալություն): Գործակալության հիմնական նպատակներն ու խնդիրներն են՝ անձնական տվյալներ մշակողների ռեեստրի վարման աշխատանքների ապահովումը, անձնական տվյալների պաշտպանության հետ կապված հարաբերությունների սուբյեկտների իրավունքների պաշտպանության ապահովումը, իր իրավասության սահմաններում անձնական տվյալների մշակման օրինականության ապահովումը:

Համապատասխան պատժամիջոցները և անձնական տվյալների պաշտպանության միջոցները անձնական տվյալների պաշտպանության օրենսդրության կիրակման հիմնական մեխանիզմներն են:

Հայաստանում, այն դեպքում, երբ քաղաքացիները համարում են, որ անձնական տվյալների պաշտպանության իրենց իրավունքը ոտնահարվել է, իրենց անձնական տվյալներն օգտագործվել կամ այլ կերպ մշակվել են օրենքի խախտմամբ, առանց իրենց համաձայնության կամ իրավական հիմքի, կարող են դիմել Գործակալությանը՝ վարչական վարույթի շրջանակներում իրենց հարցի քննության համար: Լինում են նաև դեպքեր, երբ հասարակական կազմակերպությունները կամ քաղաքացիները տեղեկացնում են Գործակալությանը այս կամ այն կազմակերպության, մարմնի կողմից մարդկանց անձնական տվյալների պաշտպանության իրավունքի խախտման մասին (ոչ թե կոնկրետ անձանց, այլ անորոշ թվով անձանց, բոլորին վերաբերող) կամ իր վերլուծությունների, ուսումնասիրությունների ընթացքում Գործակալությունը ինքն է հանդիպում անձնական տվյալների խախտում ենթադրող դեպքերի: Նման դեպքերում, երբ խոսքը չի վերաբերում կոնկրետ անձանց իրավունքի խախտմանը, Գործակալությունը վարչական վարույթ է իրականացնում սեփական նախաձեռնությամբ[6]:

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

Կիրակման պատշաճ մակարդակ ապահովելու համար Հայաստանի Հանրապետության օրենսդրության մեջ պետք է նախատեսվեն վարչական և քրեական պատասխանատվության միջոցներ: Տվյալների վերահսկիչների կողմից տվյալների հավաքագրման հարցում անփութության, կողմնակալության և/կամ տվյալների ոչ պատշաճ հավաքագրման, պահպանման և մշակման համար նրանց նկատմամբ կիրառվում են դրամական պատժամիջոցներ[7], իսկ քրեական պատժամիջոցները[8] նախատեսվում են անհատների իրավունքների կանխամտածված և գիտակցաբար թույլ տված այն խախտումների գծով, որոնք սովորաբար հանգեցնում են նյութական և բարոյական վնասների: Օրինակ, Օրենքը խախտելու համար վարչական պատասխանատվությամբ սահմանված է տուգանք, որի չափը տարբեր խախտումների դեպքում տատանվում է 50.000 ՀՀ դրամից մինչև 500.000 ՀՀ դրամ: Անձն ազատվում է վարչական պատասխանատվությունից, եթե լիազոր մարմնի որոշմամբ սահմանված ժամկետում կամ մինչև վարչական պատասխանատվության ենթարկվելու վերաբերյալ որոշում կայացնելը անձը վերացրել է թույլ տված խախտումը և լիազոր մարմին է ներկայացրել ապացույցներ այդ մասին: Սա վկայում է այն մասին, որ սահմանված պատասխանատվությունն ունի ոչ միայն պատժելու, այլ նաև անձնական տվյալների պաշտպանության իրավունքի խախտումները կանխարգելելու նպատակ:

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

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

[7] ՀՀ Վարչական իրավախախտումների վերաբերյալ ՀՀ օրենք, 189.17 հոդված
https://www.arlis.am/documentview.aspx?docid=149262
[8] ՀՀ քրեական օրենսգիրք, 144-148 հոդվածներ
https://www.arlis.am/documentview.aspx?docid=149259

Հարկ է նշել, որ վարչական պատժամիջոցները սովորաբար սահմանվում են կոնկրետ խախտումների, այլ ոչ թե ընդհանուր խախտումների համար: Եվրոպական երկրների մեծ մասում վարչական պատժամիջոցներ են նախատեսվում ծանուցման պարտականության չկատարման, տվյալների հավաքագրման, պահպանման, մշակման և ոչնչացման կանոնների խախտումների համար: Տվյալների օրինական ոչնչացման հարցը կարևորվեց ավելի ուշ, երբ էլեկտրոնային եղանակով պահվող տվյալների արժեքը բարձրացավ: Եվրոպական երկրների փորձը այդ առումով բավականին միասնական է և ենթադրում է և՛ վարչական, և՛ քրեական պատասխանատվության միջոցներ[9]:

Չնայած նրան որ անձնական տվյալների պաշտպանության ուղղությամբ խնդիրների հաղթահարման համար պետության դերն ու պարտավորությունը շատ կարևոր է, սակայն, վերջին շրջանում, նոր կորոնավիրուսային համավարակով (այսուհետ՝ Համավարակ) պայմանավորված արտակարգ դրության պայմաններում, հարկավոր է առանձնացնել պետության առանձնահատուկ դերը քաղաքացիների անձնական տվյալների պաշտպանության իրավունքի խախտման, առանց բավարար հիմնավորումների քաղաքացիների անձնական տվյալների հավաքագրման և մշակման գործում: Շատ են նաև այդ տվյալների մասսայական արտահոսքի դեպքերը: Վերջին մեկ ամսում Առողջապահության նախարարության աշխատակիցների էլեկտրոնային փոստի հասցեներից ադրբեջանական հաքերային խմբավորումները ձեռք են բերել, այնուհետև հրապարակել[10] կորոնավիրուսով վարակված քաղաքացիների սկզբում՝ 1000, հետո՝ 3500, այնուհետև, մոտ 1500 տվյալներ:

Համավարակի հետևանքով հայտարարված արտակարգ դրության ժամանակ պետությունն իրավունք ստացավ նաև միջամտել քաղաքացիների անձնական տվյալներին: Հարկ է ընդգծել, որ չնայած Համավարակի դեմ պայքարը կարող է իրավաչափ դարձնել մարդու հիմնական իրավունքներին միջամտության նպատակը՝ այդ միջամտությունը պետք է բավարարի ՀՀ Սահմանադրությամբ սահմանված պահանջներին, այն է. ընտրված միջոցի՝

1) համաչափություն (Սահմանադրության 78-րդ հոդված)

- պիտանիություն

[9]Անձնական տվյալների պաշտպանության քաղաքականության ուղեցույց:
Տարբեր երկրներում տվյալների պաշտպանության օրենսդրության խախտումների համար պատժամիջոցներ և տվյալների իրավական պաշտպանիչ միջոցներ http://www.osf.am/wp-content/uploads/2015/04/DataProPolicyGuide_arm_final.pdf

[10] Կորոնավիրուսով վարակված քաղաքացիների անձնական տվյալների արտահոսք - https://medialab.am/73315/

- անհրաժեշտություն
- համարժեքություն,

2) Սահմանադրության 80-րդ հոդվածով նախատեսված իրավունքի էության անխախտելիություն,
3) որոշակիության սկզբունք (Սահմանադրության 79-րդ հոդված):

Նշված պահանջներին չհամապատասխանող միջոցների կիրառման պարագայում անձը իրավասու է դիմել դատական պաշտպանության, այդ թվում՝ նաև ՀՀ մարդու իրավունքների վերաբերյալ միջազգային պայմանագրերի հիման վրա գործող մարմինների (մասնավորապես՝ ՄԻԵԴ[11]) :

Ուսումնասիրությունը ցույց տվեցին, որ Համաճարակի տարածման կանխարգելման նպատակով անձնական տվյալների պաշտպանության և մասնավոր կյանքի անձեռնմխելիության սահմանափակումներ Հայաստանից բացի նախատեսվել են նաև մի շարք այլ երկրներում[12]:

Այսպես.
Լեհաստանի կառավարությունը մեկուսացման մեջ գտնվող անձանց համար թողարկել է «Տնային կարանտին» հավելվածը: Մեկուսացված անձին հաղորդագրության տեսքով գալիս է ինքնանկար անելու հրահանգ: Անձը նշված հավելվածի միջոցով անում է ինքնանկար, որն օգնում է համապատասխան մարմիններին հավաստիանալու, որ անձը պահպանում է մեկուսացման պայմանները և գտնվում է մեկուսացման վայրում: Այս թվային կարանտինի ստուգմանը մասնակցելը կամավոր է, բայց այն փոխարինում է ոստիկանության սպայի վերահսկողական այցին:

Սլովակիայի խորհրդարանի կողմից ընդունվել է օրենք, որը հնարավորություն է տալիս առողջապահության նախարարությանը բջջային հեռախոսի միջոցով հետևել անձանց տեղաշարժին:

Շաբաթներ շարունակ **Գերմանիայում** քննարկումներ են ծավալվել այն մասին, թե թույլատրելի է արդյոք և ինչպես կարող են բջջային տվյալները կամ սմարթֆոնների օգտատերերի տվյալները օգտագործվեն՝ Համավարակի տարածումը կանխելու համար: Deutsche Telekom գերմանական հեռահաղորդակցման պրովայդերը իր օգտատերերի տեղաշարժի մասին

[11] Դատարանի քարտուղարության կողմից հրատարակված՝ Կոնվենցիայի 15-րդ հոդվածի վերաբերյալ ուղեցույցը (2019 թվականի դեկտեմբերի 31)
https://www.echr.coe.int/Documents/Guide_Art_15_HYE.pdf

[12] https://www.geospatialworld.net/blogs/eu-member-states-covid-19/

անանուն տվյալները փոխանցել է առողջապահական կազմակերպությանը (Ռոբերտ Կոխի Ինստիտուտ –RKI)։ Տվյալները հետազոտողներին պատկերացում կտան Համավարակի տարածման և դրա կանխման վերաբերյալ։ Սակայն, փոխանցված անանուն տվյալներով անհնարին կլինի նույնականացնել անհատ քաղաքացիներին կամ վարակված մարդկանց, ինչպես դա արվում է Ասիայի երկրներում և Իսրայելում։

ԱՄՆ կառավարությունը ակտիվ բանակցություններ է վարում Facebook-ի, Google-ի, այլ տեխնոլոգիական ընկերությունների լայն շրջանակի և առողջապահության ոլորտի փորձագետների հետ այն մասին, թե ինչպես նրանք կարող են օգտագործել Ամերիկայում բնակվողների հեռախոսներից հավաքված տվյալները կորոնավիրուսի դեմ պայքարելու համար, ներառյալ հետևելու համար, թե արդյոք մարդիկ պահպանում եմ մեկուսացման հրահանգները։ Առողջապահության ոլորտի փորձագետները հետաքրքրված են վերոհիշյալ հնարավորությամբ, որ մասնավոր հատվածի ընկերությունները կարող են հավաքագրել **անանուն տվյալներ**, որոնք նրանք կարող են օգտագործել վարակի տարածման քարտեզագրման համար[13]։

Հաջորդիվ ներկայացվում են Հայաստանում արտակարգ դրության պայմաններում անձնական տվյալներ խախտման դեպքեր, որոնց մեծամասնությունում խախտող կողմը են հանդիսանում հենց որոշում կայացնողները։

[13] https://edition.cnn.com/2020/03/18/tech/us-government-location-data-coronavirus/index.html

ԱՐՏԱԿԱՐԳ ԴՐՈՒԹՅԱՆ ՊԱՅՄԱՆՆԵՐՈՒՄ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ԽԱԽՏՄԱՆ ԴԵՊՔԵՐԸ

Անձնական տվյալների խախտման դեպքեր՝ տեղեկատվական տեխնոլոգիաների կիրառմամբ

Արտակարգ դրության պայմաններում պետության կողմից կատարվող միջոցառումները չպետք է նահանջեն ժողովրդավարության, մարդու իրավունքների և իրավունքի գերակայության սկզբունքներից:

Այդուհանդերձ, համավարակի հաղթահարման համար տեխնոլոգիաների կիրառումն օգտագործվեց վարակակիր անձանց և նրանց շփման շրջանակները դիտարկելու և բացահայտելու համար:

Հեռախոսների միջոցով տեղակայման վայրի ստուգում

Մարտի 31-ին կառավարության առաջարկով ԱԺ խորհրդարանն ընդունեց քաղաքացիների տեղաշարժը, հեռախոսազանգերի շրջանակը հասանելի դարձնելու նախագիծը: Ընդունված օրենքը[14] հեռահաղորդակցման ընկերություններից պահանջում է իշխանություններին տրամադրել իրենց հաճախորդների հեռախոսահամարները և զանգեր կատարելիս ու տեքստային հաղորդագրություններ ուղարկելիս նրանց գտնվելու վայրը, ժամը և ամսաթիվը:

Նախագիծն արժանացավ խիստ քննադատության ինչպես ԱԺ ընդդիմադիր խմբակցությունների կողմից, այնպես էլ տարբեր հասարակական և միջազգային կազմակերպությունների[15]:

Առաջին ընթերցումից հետո գործադիրն ընդունել էր որոշ մտահոգություններ և փոփոխել[16] խնդրահարույց մի քանի դրույթներ: Այդուհանդերձ, չնայած այս փոփոխություններին, նախագիծն ընդունվեց երկրորդ ընթերցմամբ, որը

---

[14] «Արտակարգ դրության իրավական ռեժիմի մասին» ՀՀ օրենքում փոփոխություններ և լրացումներ կատարելու մասին» ՀՀ օրենք https://www.arlis.am/DocumentView.aspx?docid=142124

«Էլեկտրոնային հաղորդակցության մասին» ՀՀ օրենքում լրացում կատարելու մասին ՀՀ օրենք https://www.arlis.am/documentview.aspx?docid=140751

[15] ՀՀ արդարադատության նախարար Ռուստամ Բադասյանն առաջին ընթերցմամբ քննարկման է ներկայացրել «Արտակարգ դրության իրավական ռեժիմի մասին» օրենքում լրացումներ կատարելու մասին» և «Էլեկտրոնային հաղորդակցության մասին» օրենքներում լրացում կատարելու մասին» օրենսդրական փաթեթը - http://www.parliament.am/news.php?cat_id=2&NewsID=12828&year=2020&month=03&day=30

[16] Առաջին ընթերցումից հետո կատարված փոփոխությունների մասին - http://parliament.am/draftreading_docs7/K-534_DR2.pdf?fbclid=IwAR0m9uEkM3ZLzWj7TvhTvBIJN7KT-ELRD_MDNfaQqrN3QPEEWLQimEZNvdg

պարունակում է մի շարք խնդրահարույց կարգավորումներ, որոնք անհամաչափ և ոչ անհրաժեշտ սահմանափակումներ են ստեղծում անձնական տվյալների պաշտպանության, մասնավոր և ընտանեկան կյանքի անձեռնմխելիության, հաղորդակցության ազատության և գաղտնիության իրավունքների իրացման տեսանկյունից:

Միջազգային հարթակում, Humans Right Watch-ը իր զեկույցում ներկայացնում է, որ նոր օրենքը Հայաստանում սահմանափակում է մասնավոր կյանքի իրավունքը Covid19-ի դեմ պայքարում և շեշտում, որ ցանկացած սահմանափակում պահանջում է մարդու իրավունքների պաշտպանություն. «*Հայաստանի կառավարությունը բախվել է հանրային առողջապահության ոլորտում արտակարգ իրավիճակի, և տեխնոլոգիաները կարևոր դերակատարություն ունեն հանրային առողջության վերաբերյալ ուղերձները տեղ հասցնելու և առողջապահության հասանելիությունը խթանելու գործում, բայց միաժամանակ, իշխանությունները պետք է միջոցներ ձեռնարկեն, որպեսզի զանգվածային վերահսկողության կիրառումը չխաթարի մարդու իրավունքները»* [17]:

Քաղաքացիական հասարակության ներկայացուցիչները մտահոգություն են հայտնել այս կարգավորման արդյունավետության և համաչափության կապակցությամբ: Հարտարարություններում մասնավորապես ասվում են. *«Բացակայում է կապը մշակվող անձնական տվյալների և սահմանված նպատակի միջև: Եվ հարց է ծագում, թե որքանով է նպատակահարմար վերահսկել զանգերի քանակը, տևողությունը և այն ամենը, ինչը անմիջականորեն կապ չունի տեղաշարժի հետ: Շարժական կապի տվյալների միջոցով տեղորոշման տվյալները ի տարբերություն GPS ի ունեն շատ ցածր ճշգրտություն, ուստի դրա կիրառման օգուտը շատ կասկածելի է: Այսինքն, այդ տվյալների հավաքագրումը ոչ մի օգուտ չի տա համավարակի պայքարի հետ»*[18] *«Գիտակցելով, որ բնական աղետների ու ճգնաժամային այլ իրավիճակների պայմաններում մարդու հիմնարար իրավունքներն ու ազատությունները կարող են սահմանափակվել ի շահ հասարակության անվտանգության, ցանկանում ենք շեշտել, որ նման սահմանափակումները թույլատրելի են միայն այն նվազագույն ծավալով, որն անհրաժեշտ է նպատակին հասնելու համար: Հետևաբար պետությունը պարտավոր է պահպանել համաչափության սկզբունքը, ինչպես նաև սահմանափակումները կիրառել առավելագույն թափանցիկությամբ»*[19]:

---

[17] Human Rights Watch, Free Speech, https://www.hrw.org/hy/news/2020/04/06/340302
[18] Հայ տպագրություն, https://factor.am/236357.html
[19] Հայ տպագրություն, Խոսքի ազատության և պաշտպանության կոմիտե, 02.04.2020, https://khosq.am/2020/04/02/հայ տպագրություն-55/

Հայաստանի մարդու իրավունքների պաշտպանը ևս մտահոգություն է հայտնել օրենքում մարդու իրավունքների բավարար երաշխիքների բացակայության մասին[20]:

Պետական մարմինների կողմից անձնական տվյալներ մշակելու հիմքը, տվյալների մշակում նախատեսելը, տվյալներ ստանալը պետք է համապատասխանի «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի պահանջներին:

Պետական մարմինների կողմից անձնական տվյալների մշակումը կարող է իրականացվել՝ անձնական տվյալները կարող են հավաքվել, ամրագրվել, մուտքագրվել, համակարգվել, կազմակերպվել, պահպանվել, օգտագործվել, վերափոխվել, վերականգնվել, փոխանցվել, ուղղվել, ուղեփակվել, ոչնչացվել, կամ դրանց հետ այլ գործողություն կարող է կատարվել բացառապես օրենքներով (օրենքի մակարդակում) ուղղակիորեն սահմանված դեպքերում և կարգով:

Այն պարագայում, երբ անհրաժեշտ է, որ պետական մարմինն օգտվի անձնական տվյալի մշակման համաձայնության հիմքերից, անհրաժեշտ է, որ այդ հնարավորությունը (հայեցողությունը) նույնպես նախատեսված լինի օրենքով:

Անձնական տվյալների մշակում նախատեսող օրենքներ նախագծելիս, օրենսդրական նախաձեռնություն իրականացնելիս պետական մարմինները պետք է առաջնորդվեն անձնական տվյալների մշակման համաչափության սկզբունքով: Համաչափության սկզբունքը պարտադրում է, որ նախապատվությունը տրվի նվազ միջամտող լուծումներին՝ հաշվի առնելով հետապնդվող հատուկ նպատակը: Լրացուցիչ վերահսկողական մեխանիզմների ներդնումը կարող է խաթարել մարդու իրավունքների պաշտպանության ամբողջ համակարգը և անդառնալի հետևանքներ ունենալ ժողովրդավարական ինստիտուտների գործունեության վրա:

<u>Ինքնամեկուսացված քաղաքացիների քարտեզագրում</u>

Առողջապահության նախարարության աջակցությամբ ստեղծվել է Հայաստանում նոր կորոնավիրուսային համավարակով պայմանավորված ինքնամեկուսացված քաղաքաացիների էլեկտրոնային քարտեզ[21]: Էլեկտրոնային քարտեզը ստեղծվել է «Արմեդ» էլեկտրոնային առողջապահության համակարգի[22] կողմից: Էլեկտրոնային առողջապահության համակարգն առողջապահական տվյալների կառավարման

[20]Մարդու իրավունքների պաշտպանի իրավական դիրքորոշումները հաղորդակցության գաղտնիության և մյուս իրավունքները սահմանափակող օրենքների նախագծերի վերաբերյալ https://ombuds.am/am/site/ViewNews/1137

[21] COVID-19 ինքնամեկուսացվածների քարտեզ - https://covid19-map.armed.am/

[22] ArMed էլեկտրոնային առողջապահության համակարգ - https://www.armed.am/am/auth/loginnew

միասնական համակարգ է, որտեղ մուտքագրվում և պահվում են բնակչի առողջությանը վերաբերվող ամբողջական տվյալներ: Դա հնարավորություն է տալիս բուժող բժշկին անհրաժեշտության դեպքում էլեկտրոնային եղանակով տեսնել պացիենտի առողջության պատմությունն ու նրա բուժման վերաբերյալ կայացնել տեղեկացված որոշումներ:

Ավելի ուշ նաև սկսվեցին հրապարակվել վարակակիր և ինքնամեկուսացած քաղաքացիների բնակության/գտնվելու վայրերը՝ 50 մետր շեղմամբ: Շեղումն արվում է, որպեսզի հնարավորություն չտրվի հասկանալու՝ կոնկրետ հասցեով քաղաքացու ինքնամեկուսացված լինելու հանգամանքը և դրանով չխախտվի քաղաքացու անձնական տվյալների պաշտպանության իրավունքը:

Ավելի ուշ ՀՀ Առողջապահության նախարարության տեղեկացմամբ՝ քարտեզում տեղի են ունեցել փոփոխություններ, այն ավելի ինտերակտիվ է և հագեցած լրացուցիչ տեղեկություններով: Այն թարմացվում է 1 ժամ պարբերականությամբ, ±0-100մ ճշտությամբ՝ անձնական տվյալների գաղտնիությունն ապահովելու նպատակով: Մասնավորապես, սեղմելով դեպքի վրա, կարող եք տեսնել պացիենտի կորոնավիրուսային հիվանդության հաստատման օրը, տարիքը և սեռը:

Հաշվի առնելով այն հանգամանքը, որ քարտեզը ցուցադրում է ինքնամեկուսացված քաղաքացու գտնվելու վայրը ±0-100մ ճշտությամբ, առաջանում են կասկածներ, որ առավել նոսր բնակեցված և քիչ բնակչություն ունեցող համայնքներում՝ ելնելով քարտեզի տրամադրած տվյալներից, կարելի է նույնականացնել ինքնամեկուսացված քաղաքացուն: Այս խնդիրն առավել ակնհայտ դրսևորվում է գյուղական համայնքների պարագայում, որտեղ անգամ հարյուր մետր շեղման պարագայում, հաշվի առնելով քաղաքացու տարիքը, սեռը կարելի է նույնականացնել վարակված, այնուհետև ինքնամեկուսացված քաղաքացուն:

Այսպիսով, համավարակի կանխման անհրաժեշտությունը սկսվեց գերադասվել քաղաքացիների անձնական կյանքի վարման և գաղտնիության իրավունքներից: Այսպիսի մոտեցումը միաժամանակ արժանացավ քաղաքական և հասարակական տարբեր շրջանակների քննադատությանը: Ելնելով ինտերակտիվ քարտեզի նպատակից, որը ենթադրում է բնակչության իրազեկում առ այն, որ իրենց համայնքում կան վարակված անձինք, նախարարությունը կարող էր քարտեզի միջոցով չտրամադրել հավելյալ տեղակատվություն վարակված քաղաքացու տարիքի և սեռի վերաբերյալ, որը որևէ առնչություն չունի համավարակի կանխարգելման նպատակով քաղաքացիների իրազեկվածությունը բարձրացնելու հարցում:

Կորոնավիրուսային վարակի տարածումը կանխելու նպատակով ՀՀ վարչապետ Նիկոլ Փաշինյանի կողմից քաղաքացիների լուսանկարների հրապարակումն իր ֆեյսբուկյան էջում

Արտակարգ դրության օրերին ՀՀ վարչապետ Նիկոլ Փաշինյանը սոցիալական ցանցերում տարբեր կոչերով հանրությանը դիմելիս հորդորեց համավարակի կանխարգելման դեմ սկսել պետություն-հանրություն համագործակցություն: Այսպիսի համագործակցությունը ՀՀ վարչապետը դիտարկում էր հասարակական ինքնավերահսկողության տեսանկյունից: «*Սիրելի հայրենակիցներ. Խնդրում եմ հակահամաճարակային կանոնների խախտման աղաղակող դեպքերը տեսանկարահանեք, լուսանկարահանեք եւ ուղարկեք իմ այս ֆեյսբուքյան էջին, հնարավորինս կոնկրետ եւ ճշգրիտ նշելով խախտման վայրը, ժամկետը, դրա հետ առնչություն ունեցող ֆիզիկական եւ իրավաբանական անձանց*»:

ՀՀ վարչապետի կոչերի և հորդորներին հաջորդեց հրապարակումները. հանրային և ոչ հանրային վայրերում գաղտնի՝ առանց անձից թույլտվություն ստանալու, խոշոր պլանով արված լուսանկարները՝ ուղեկցվող գրառումներով[23]: Նիկոլ Փաշինյանի էջում դրոպեների տարբերությամբ հրապարակվել են լուսանկարներ և տեսանյութեր, որտեղ քաղաքացիներն առանց դիմակների են, երբեմն՝ գրկախառնված կամ մասնակցում են բազմամարդ խնջույքների, ինչպես նաև խմբված են առևտրային բանկերի մուտքերի մոտ: Մեկ այլ դեպքում, վարչապետի մոտ էին հայտնվել քաղաքացիների վճարումների վերաբերյալ տվյալները[24]:

Վարչապետի կողմից հրապարակված լուսանկարներից մեկը[25] խնդրային էր ոչ միայն անձնական տվյալների պաշտպանության առումով, այլև բովանդակային տեսանկյունից: Լուսանկարը վարչապետը վերնագրել էր «Անթաքույց գեղեցկություն», որտեղ արձանագրված էր մետրոյում աղջկա դիմակ չկրելու փաստը (աղջկա դեմքը բաց էր): Սակայն, իրավապաշտպանների և օգտատերերի քննադատություններից հետո, Փաշինյանը լուսանկարը հեռացրեց իր էջից: Ի դեպ, սա առաջին դեպքը չէր, երբ վարչապետը անձնական լուսանկարներ էր հրապարակում և հետո, ջնջում դրանք:

[23] ՀՀ Վարչապետի հրապարակումները ֆեյսբուկում - https://factor.am/257090.html
[24] Վճարումների վերաբերյալ տվյալների փոխանցման մասին անդրադարձը - https://www.azatutyun.am/a/30587762.html
[25] Հոդված մետրոյում աղջկա լուսանկարով ուղեկցվող վարչապետի գրառման մասին- https://news.am/arm/news/583230.html

Հարկ է նշել, որ լուսանկարների հրապարակումը այդպես էլ չկանխեց համավարակի տարածումը, փոխարենը, այդպիսով որոշ քաղաքացիներ հանրայնորեն ստորացվեցին։

Լուսանկարների հրապարակումը համարվում է մարդու անձնական անձեռնմխելիության խախտում, քանի որ եթե անձը իր գործողություններով և/կամ անգործությամբ իրավախախտում է թույլ տվել, ապա ենթակա է օրենքով սահմանված պատասխանատվության, ոչ թե հրապարակավ ծաղրուծանակի, քննադատության, դրական կամ բացասական վերաբերմունքի։ Բացի այդ, լուսանկարները կարելի է տարածել միմիայն լուսանկարում պատկերված մարդու համաձայնությամբ։

Բացառված չէ, որ լուսանկարներն ու տեսագրությունները, որոնք հրապարակել է Փաշինյանն իր ֆեյսբուկյան էջում, կարող են հին լինել, այսինքն՝ նկարված լինել արտակարգ դրությունից և երկրում հակահամաճարակային խիստ կանոնների հաստատումից առաջ։ Շատ են նաև դեպքերը, երբ օգտատերն իր էջում արխիվային լուսանկար է տեղադրել, իսկ վարչապետին այն հասել է որպես արտակարգ դրության խախտման վկայություն։ Այդպիսի դեպքերի բազմաթիվ օրինակներ[26] կան։

Անգամ, եթե վարչապետի տարածած նյութերը բաժանենք բաց հասանելիություն (public) ունեցող և սահմանափակ (միայն ընկերների համար) հասանելիության նյութերի, երկու դեպքում էլ լուսանկարների և տեսագրությունների օգտագործումը կամ դրանց փոխանցումը երրորդ անձանց թույլատրվում է միայն լուսանկարում կամ տեսագրության մեջ երևացող մարդու համաձայնությամբ, էլ չենք խոսում այն դեպքերին, երբ որևէ մեկը տեսանկարահանել է առանց տվյալ անձի իմացության և համաձայնության։ Ընդ որում, միայն հրապարակման թույլտվությունը բավարար չէ. հարկ է նաև ճշտել, թե ինչ համատեքստում է օգտագործվելու այս կամ այն լուսանկարը կամ տեսագրությունը։ Նման դեպքերում, պատասխանատվություն պետք է կրի և՛ նա, ով առանց թույլտվության նկարում և ուղարկում է նման նյութերը, և՛ նա, ով դրանք հրապարակում ու տարածում է։

Գործակալությունը նման իրավիճակներում պետք է արագ արձագանքի և հայտնի իր դիրքորոշումը՝ դատապարտելով քաղաքացիների անձնական տվյալների խախտման հանգամանքը, հատկապես, երբ այդ խախտումները թույլ են տրվում որոշում կայացնողների կողմից, մասնավորապես, երկրի առաջին դեմքի մակարդակով։

[26] «Նիկոլ Փաշինյանի կողմից հրապարակված ևս մեկ կեղծ ժամանակագրությամբ լուսանկար» վերտառությամբ հոդված - https://antifake.am/am/news/2058

ՀՀ ԱԺ մարդու իրավունքների և պետաիրավական հարցերի հանձնաժողովի նախագահ, ԱԺ պատգամավոր, Նաիրա Զոհրաբյանի կողմից քաղաքացու անձնագրային տվյալների հրապարակումն իր ֆեյսբուկյան էջում:

ՀՀ Ազգային ժողովի Մարդու իրավունքների և պետաիրավական հարցերի հանձնաժողովի նախագահ, ԱԺ պատգամավոր Նաիրա Զոհրաբյանի կողմից հրապարակվեց[27] Արցախի Մարտունու շրջանի Ճարտար գյուղի բնակչի անձնագրի լուսանկարը՝ քաղաքացու լուսանկարով, որտեղ որպես անձի ծննդավայր նշված է Ադրբեջանը:

Նաիրա Զոհրաբյանն իր գրառման մեջ նշել է. «Եթե անգամ ժամանակին Արցախը դե յուրե եղել է Ադրբեջանի կազմում, որքանո՞վ է քաղաքականապես նպատակահարմար Արցախում ծնված քաղաքացիների նոր անձնագրերում ևս գրել Ադրբեջան: Պարզ է նաև, որ օրենքի տառը պահելու դեպքում պիտի գրվի Ադրբեջան: Բայց, կարծում եմ էստեղ այլ լուծում պիտի գտնել»:

ՀՀ Ոստիկանությունը պարզաբանում տարածեց և նշեց, որ քաղաքացու անձնագրում ծննդավայրը նշելիս հիմք է հանդիսանում ծննդյան վկայականում նշված ծննդավայր երկիրը:

Հարկ է նշել, որ Նաիրա Զոհրաբյանը ստանձնելով ՀՀ ԱԺ մարդու իրավունքների և հանրային հարցերի մշտական հանձնաժողովի նախագահի պաշտոնը, կոպտորեն խախտել է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը՝ հանդիսանալով երրորդ անձ և հրապարակելով անձի անձնագրային տվյալները: Այս պարագայում խախտվել է օրենքի մի քանի կետեր: Հրապարակված տվյալներում անձնական տվյալների սուբյեկտը՝ քաղաքացին, ապանձնավորված չէ, չկա քաղաքացու գրավոր թույլտվությունը, որը կապացուցեր ԱԺ պատգամավորի այդ քայլի իրավաչափությունը:

Ընդ որում, հարկավոր է նշել, որ հրապարակումն իրականացվել է Ֆեյսբուկ սոցիալական ցանցում, մինչդեռ, ԱԺ պատգամավորը՝ որպես որոշում կայացնող, ունի բավարար լծակներ հարցը ներքին առումով, թեկուզև, խորհրդարանում կարգավորելու և գործին ընթացք տալու համար:

Փաստացի, այդպես էլ պարզ չդարձավ, թե ով էր գրառման լսարանը. եթե հայ հասարակությունն էր, ապա հարկ է դիտարկել, որ հասարակությունն այդ կատեգորիայի խնդիրներ լուծող սուբյեկտ չէ, իսկ եթե լսարանը պատկան մարմիններն են, ապա Ֆեյսբո՞ւկն է այն կապող օղակը, որտեղ պետք է քննարկվեն այդ հարցերը:

[27] Նաիրա Զոհրաբյանի գրառումը ֆեյսբուկում - https://www.facebook.com/photo.php?fbid=748280022659058&set=a.102014030618997&type=3

Ավելի ուշ, Նաիրա Զոհրաբյանը հայտարարեց, որ այդ անձնագրային լուսանկարը ստացել է անձնական տվյալների սուբյեկտի ամուսնուց՝ հրապարակման և խնդրի լուծման հորդորով, մինչդեռ այս պարզաբանումը չի լուծում իրավական խնդիրը, որն առաջ է եկել, քանի որ չկա անմիջապես անձնական տվյալների սուբյեկտի գրավոր համաձայնությունը, որը փաստարկված կլիներ և խնդիրը մասնակի փակված կհամարվեր։

Այդ և մյուս փաստարկներին բերվել են իրավական հակափաստարկներ.

Փաստարկ; անձնագրի սերիան ջնջված է հրապարակել։

Հակափաստարկ; հրապարակվել են անձնական տվյալներ, ներառյալ անձնագրի լուսանկարը, ստորագրությունը, որոնք թույլ են տալիս իդենտիֆիկացնել անձին, մինչդեռ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը հստակ արձանագրում է, որ ցանկացած տվյալ, որի միջոցով հնարավոր է նույնականացնել անձին, կոչվում է անձնական տվյալ և առանց անձնական տվյալների սուբյեկտի համաձայնության դրանց տարածումը և հրապարակումը համարվում է խախտում և ենթադրում է օրենքով սահմանված կարգով վարչական պատասխանատվություն։

Փաստարկ; ՀՀ ԱԺ պատգամավորը հրապարակել է խնդրի լուծման համար։

Հակափաստարկ; այն, որ քաղաքացու անձնագրում գրված ծննդավայրը «խնդիր» է, ապացուցման կարիք ունի, որից հետո պետք է անցնել այդ «խնդրի» լուծմանը։ Եթե այս նույն հրապարակումը մեկ ուրիշն աներ, օրինակ, շարքային քաղաքացին՝ իր անձնագիրը, ապա պարզ կլիներ, որ ուզում է խնդիրը բարձրաձայնել լուծմանը հասնելու համար, բայց եթե նույն գրառումն անում է ԱԺ պատգամավորը, ով օժտված է հատուկ լիազորություններով և ունի բավարար միջոցներ խնդիրը ոչ հրապարակային կերպով և օրինական ճանապարհով լուծելու համար, ապա պարզ է դառնում, որ ճանապարհը, որով պետք է վերականգնվեր քաղաքացու խախտված իրավունքը, կրկնակի հարվածի տակ է դնում նույն այդ քաղաքացուն։

Փաստարկ; քաղաքացին է խնդրել հրապարակել։

Հակափաստարկ; ընդունենք, որ քաղաքացին է ուղարկել իր լուսանկարը ԱԺ պատգամավորին՝ հրապարակելու համար։ ԱԺ պատգամավորը, առավել ևս պետաիրավական հարցերով հանձնաժողովի նախագահը, պարտավոր էր գիտակցել, որ առանց ապանձնավորման չի կարելի հրապարակել քաղաքացու անձնական տվյալները և դրանով վտանգի տակ դնել քաղաքացուն, որովհետև նման տվյալները կարող են հիմք հանդիսանալ քաղաքացու անվամբ գործարքներ իրականացնելու համար։ «Անձնական տվյալների պաշտպանության մասին» ՀՀ

օրենքն ամրագրում է, որ անձնական տվյալները պետք է օգտագործվեն միայն այն չափով և ծավալով, որոնց արդյունքում բավարար կլինի հասնել դրանց օգտագործման համար նախատեսված նպատակին: Այսինքն, նպատակը պիտի արդարացնի միջոցները, որոնք կիրառվում են դրան հասնելու համար:

Փաստարկ; քաղաքացու ամուսինն է խնդրել հրապարակել իր կնոջ անձնագրի լուսանկարը:

Հակափաստարկ; ցանկացած քաղաքացի կարող է իր ընտանիքի կամ իր հարազատի, բարեկամի, ընկերոջ անձնական տվյալներն ուղարկել որևէ երրորդ անձի՝ ինչ-որ խնդրի լուծման նպատակով: Սա չի կարող բավարար իրավական հիմք հանդիսանալ ստացված անձնական տվյալներն օգտագործելու համար, առնվազն երկու պատճառով: Առաջին, միայն անձնական տվյալների սուբյեկտի համաձայնությամբ են օգտագործվում անձնական տվյալները, իսկ մինչև 14 տարեկան երեխայի պարագայում անձնական տվյալների օգտագործման թույլտվությունը լիազորված է օրինական ներկայացուցչին: Երկրորդ, քրեական գործերի ուսումնասիրությունը ցույց է տալիս, որ քիչ չեն դեպքերը հարազատների ու ընտանիքի անդամների կողմից խուլիգանության, խաբեության, գողության և բռնության զոհ դառնալ, և այդ իսկ հանգամանքով, անգամ հարազատի կողմից ներկայացվող տվյալները չպետք է հրապարակել մինչև տվյալների սուբյեկտից գրավոր կերպով չհաստատվեն դրանց օգտագործման թույլտվությունը և նպատակը:

Հարկ է նշել, որ Նաիրա Զոհրաբյանի հրապարակումից հետո քաղաքացու անձնագրի լուսանկարը հայտնվել է ադրբեջանական աղբյուրներում[28] և դարձել շահարկումների առիթ:

Վերջիվերջո, հարկավոր է դիտարկել «լավագույն շահի սկզբունքը», արդյո՞ք այստեղ գործել է լավագույն շահի սկզբունքը և տվյալների հրապարակումն առավել կարևոր էր, քան դրանց կորուստը, այն դեպքում, երբ հրապարակումով լուծում չի տրվում: Միանշանակ ո՛չ, լավագույն շահի սկզբունքն այստեղ չի գործում և չի գերակայում անձնական տվյալների պաշտպանության իրավունքին:

[28] В Армении вынуждены признать: Карабах - это Азербайджан - https://www.youtube.com/watch?v=1eZ3CP7KeG0

Անչափահասի անձնական տվյալների խախտում

Անձնական տվյալների պաշտպանության իրավունքի իրացման համատեքստում Հայաստանի Հանրապետությունում որպես կարգավորման ենթակա առաջնահերթ ոլորտներից է անչափահասների անձնական տվյալների պաշտպանությունը:

Այս ուղղությամբ Գործակալության կողմից քայլեր են իրականացվել, մասնավորապես.

- Խորհրդատվական որոշումներ են արձակվել, որով համապատասխան կառույցներին իրազեկել են, թե ինչպես պետք է պաշտպանվեն երեխաների իրավունքները:
- 2017 թվականին Հանրության դատին է հանձնվել անչափահասների անձնական տվյալների պաշտպանության մասին ուղեցույցը: Այն տարբեր ասպեկտներ է ներառում՝ տվյալների փոխանցում, պաշտպանություն ինտերնետում, տեսահսկում ուսումնական հաստատություններում, մոռացվելու իրավունք[29]:

Երեխաներն առավել խոցելի են, քանի որ իրենց ֆիզիկական և մտավոր զարգացման, իրավագիտակցության ձևավորման ճանապարհին կարող են ամբողջությամբ չգիտակցել իրենց անձնական տվյալների պաշտպանության կարևորությունը: Փոքր տարիքի հետևանքով հնարավոր է՝ երեխաները չկարողանան պատշաճ պաշտպանել իրենց իրավունքները, դրա համար նրանք պաշտպանված լինելու իրավունք ունեն:

Գործակալությունը մշտապես շեշտում է այն գաղափարը, որ երեխաների անձնական տվյալները մշակելիս անհրաժեշտ է հաշվի առնել **երեխայի լավագույն շահի սկզբունքը**, համաձայն որի՝ անձը, ով դեռևս չի հասել ֆիզիկական և հոգեբանական հասունության, ավելի շատ պաշտպանության կարիք ունի, քան մյուսները:

Այսուհանդերձ, անչափահասների անձնական տվյալների հրապարակման դեպքերը քիչ չեն՝ ինչպես ԶԼՄ-ների, այնպես էլ պետական պաշտոնյաների, անգամ Վարչապետի կողմից

Որպես երեխաների անձնական տվյալների պաշտպանության խախտման օրինակ ներկայացվում է 13-ամյա գյումրեցի երեխայի ծեծվելու հետևանքով հիվանդանոց

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

տեղափոխվելու վերաբերյալ իրադարձությունը[30]: Արտակարգ դրության հայտարարման օրվանից հաշված օրեր առաջ լրատվամիջոցների ոչ պրոֆեսիոնալ, հակաէթիկական և հակահիրավական լուսաբանումների և անձնական տվյալների հրապարակման հետևանքով բացահայտվեց Գյումրիում դաժան ծեծի ենթարկված 13-ամյա աղջկա ինքնությունը (ցուցադրվում է մեկ օրինակ[31]): Հրապարակվել են այնպիսի անձնական տվյալներ, որոնք թույլ են տվել նույնականացնել անձին: Դպրոցի տնօրենի և ուսուցիչների կողմից տրված հարցազրույցը ևս խախտումների շղթայի շարունակություն է: Ընդ որում, այդ հարցազրույցները ենթադրում են խախտում ոչ միայն լրատվամիջոցների կողմից, այլև դպրոցի տնօրենի և ուսուցիչների կողմից, քանի որ վերջիններս տիրապետելով անչափահասի տվյալներին, պատրաստակամություն են հայտնել այդ մասին կիսվել և հանրայնացնել: Դպրոցում մատյանի, բնակության վայրի լուսանկարները, բնակության վայրի հասցեի ներկայացումը, բնակարանի նկարահանումը և շատ այլ հիմքեր պատճառ են հանդիսացել անձի նույնականացմանը:

Ավելի ուշ, ՀՀ վարչապետը գրառում կատարեց[32]՝ տեղադրելով լուսանկար այն մասին, որ այցելել է բժշկական կենտրոնի վերակենդանացման բաժանմունքում գտնվող աղջկան (գրառման մեջ անունը, ազգանունը, տարիքը և այլ տվյալներ հրապարակված են ամբողջությամբ): Այսպիսով, վերջնականապես բացահայտվեց անձի ով լինելը, ինչն էլ իր հերթին սոցիալական և հանրային ազդեցություն ունեցավ երեխայի կյանքի անձեռնմխելիության և անձնական տվյալների պաշտպանության մի շարք հարցերում: Ավելի ուշ, բերվեց հակափաստարկ, որ վարչապետը չի խախտել երեխայի անձնական տվյալների պաշտպանության իրավունքը, քանի որ մինչ այդ հրապարակումն արդեն իսկ հրապարակվել էր բավարար քանակով անձնական տվյալներ, որոնք թույլ կտային նույնականացնել անձին: Հակափաստարկի հակահակափաստարկը առավել ակնհայտ է՝ անկախ ամեն ինչից հրապարակվել է անձնական տվյալ, ընդ որում, նոր տվյալ, որի մասին դեռ լրատվամիջոցները չունեին հրապարակված նյութեր: Հրապարակված անձնական տվյալը երեխայի անունը և ազգանունն էր և լուսանկարը: Այդուհանդերձ, եթե անգամ լրատվամիջոցների կողմից արդեն իսկ հրապարակվել էր անձի նույնականացման համար բավարար քանակով անձնական տվյալներ, ապա վարչապետի հրապարակումից հետո այդ անձնական տվյալները դարձան առավել հանրային և տեսանելի միլիոնավոր մարդկանց համար:

---

[30] Գյումրեցի աղջկա ծեծի դեպքը - https://www.azatutyun.am/a/30470519.html

[31] 13-ամյա աղջկան անձնական տվյալների պաշտպանության իրավունքը և լրագրողական էթիկան խախտող ռեպորտաժի մեկ օրինակ - https://www.shantnews.am/news/view/619577.html

[32] ՀՀ վարչապետ, Նիկոլ Փաշինյանի գրառումը ֆեյսբուկում - https://www.facebook.com/nikol.pashinyan/posts/2576082906045422

Այնպիսի տեղեկությունների հրապարակումը, որոնք թույլ են տալիս նույնականացնել (իդենտիֆիկացնել) անձի ով լինելը, արգելված են ՀՀ օրենսդրությամբ: Նման տեղեկությունների հրապարակումն ուղղակիորեն ազդում է տվյալների սուբյեկտի հետագա կյանքի ընթացքի, դրա որակի և անվտանգության վրա: Բացի այդ, եթե խոսքը անչափահասի մասին է, ով չունի օրինական ներկայացուցիչ, երեխայի իրավունքների պաշտպանությունն ու խախտված իրավունքի վնասի առավելագույն վերականգնման պարտավորությունը ստանձնում է պետությունը, մինչդեռ այս ուղղությամբ որևէ գործողություն չարվեց ո՛չ պետության, մասնավորապես Աշխատանքի և սոցիալական հարցերի նախարարության, Արդարադատության նախարարության, Գործակալության կողմից, ո՛չ էլ Մարդու իրավունքների պաշտպանի կողմից:

Անձնական տվյալների պաշտպանության վտանգները՝ հեռավար կրթության պայմաններում

Կորոնավիրուսի տարածումով պայմանավորված ճգնաժամային իրավիճակը թե՛ ամբողջ աշխարհի, թե՛ Հայաստանի կրթական համակարգի համար դարձավ իսկական մարտահրավեր: Արդյունքում՝ ՀՀ կրթության նախարար Արայիկ Հարությունյանի որոշմամբ կրթական համակարգը Հայաստանում 2020 թվականի մարտից անցավ հեռավար ուսուցման[33]:

Հեռավար կրթության անցումն իրականացվեց առանց նախապատրաստական աշխատանքների և համապատասխան տեխնիկական աջակցության: Ռեսուրսների բացակայության պայմաններում հեռավար կրթությունը ստացավ քաոսային բնույթ: Նախարարության կողմից կրթական հաստատություններին չներկայացվեց կրթության հեռավար իրականացման գործիքներ, ըստ այդմ, նաև չբերվեց հեռավար կրթության իրականացման տեխնիկական ուղեցույց, որի շնորհիվ միջնակարգ, ավագ և բարձրագույն ուսումնական հաստատությունների աշխատակիցները կկարողանային իրականացնել հեռավար կրթությունը: Չներկայացվեց նաև տեխնիկական ուղեցույց աշակերտների և ուսանողների համար, ինչի պայմաններում հեռավար կրթության գործընթացն իրականացվեց «ում՝ ինչպես հարմար է» սկզբունքով:

[33] Հայաստանի հանրապետության կրթության, գիտության, մշակույթի և սպորտի նախարարի հրաման հանրակրթական ուսումնական հաստատություններում հեռավար (դիստանցիոն) կրթության կազմակերպման կարգը հաստատելու մասին https://www.arlis.am/DocumentView.aspx?docid=142945

Ինչպես աշխարհում, այնպես էլ Հայաստանում լայն տարածում գտավ Zoom տեսակապի ծառայությունը[34]: Հարկ է նշել, որ այս ծառայությունը չունի տեխնիկական անվտանգության բարձր աստիճան, իսկ ծառայության անվճար տարբերակն առաջացրեց բազմաթիվ խնդիրներ դրանից օգտվողների համար (օրինակ, դասընթացների 40 րոպե տևողության սահմանափակում):

Տեխնիկական անհարմարություններից զատ, արտակարգ դրության օրերին հեռավար կրթության ոչ կանոնակարգված իրականացման պայմաններում տեղի ունեցավ դրանից օգտվողների անձնական տվյալների արտահոսք: Շատերն օգտվելով նման ծրագրերից մուտքի իրավունքի թույլտվություն տրամադրեցին իրենց համակարգչի և/կամ բջջային հեռախոսի ֆոտոխցիկին, միկրոֆոնին, կոնտակտներին: Արձանագրվեցին դեպքեր, երբ խմբային հեռավար դասընթացի տեխնիկական սխալ կարգավորումների պատճառով այլ անձինք մուտքի հնարավորություն ունեցան այդ դասընթացներին: Դասընթացների ընթացքում, ինչպես աշակերտների և ուսանողների, այնպես էլ մանկավարժների կողմից առանց դասընթացի մասնակիցներին ծանուցելու և համապատասխան թույլտվությունը ստանալու իրականացվեցին էկրանի պատկերների պատճենում՝ որպես լուսանկար և տարածում՝ որպես հանրային հաշվետվություն, կատարված աշխատանքի վերաբերյալ: Արձանագրվեցին դեպքեր, երբ առանց դասընթացի մասնակիցների ծանուցման և համապատասխան թույլտվության ստացման ձայնագրվեցին դասերը, այնուհետև, հանրայնորեն տարածվեցին:

Նախարարությունը՝ որպես հեռավար կրթության համակարգի ներդնող այդպես էլ չկարգավորեց ոլորտը և չանդրադարձավ անձնական տվյալների պաշտպանության հետ առնչություն ունեցող այս և մի շարք այլ խնդիրների, չկազմակերպեց դրանց զսպող մեխանիզմների ստեղծումն ու ներդնումը:

Այս խնդրին խորքային անդրադարձ տեղի չունեցավ նաև Գործակալության կողմից, որի լիազորությունների և պատասխանատվության ներքո է գտնվում ֆորս-մաժորային իրավիճակներում նման հարցերի կարգավորումն ու աջակցությունը հանրությանը՝ պատշաճ իրազեկման տեսքով:

[34] Zoom տեսակապի ծառայություն - https://zoom.us/

Պետական ինստիտուտների կողմից էլեկտրոնային փոստերի վարման քաղաքականությունը և կորոնավիրուսով վարակված քաղաքացիների անձնական տվյալների ու ընդհանուր ցանկերի արտահոսք

Նոր կորանավիրուսային համավարակի առաջին ալիքի օրերին, առողջապահության նախարարության տվյալների բազայից տեղի է ունեցել տվյալների արտահոսք, ինչի պատճառով սոցիալական ցանցերում հրապարակվել են ինչպես նոր կորոնավիրուսից մահացած քաղաքացիների անձնական տվյալները, այնպես էլ վարակված քաղաքացիների: Ցանկերում նշված է եղել քաղաքացիների անունը, ազգանունը, հայրանունը, ծննդյան տարեթիվը, ինչը հնարավորություն է տալիս նույնականացնել անձին և այդպիսով բացահայտել մարդու առողջական վիճակին վերաբերող անձնական տվյալները: Ընդ որում, այդ տվյալների ստուգումն արտակարգ դրության օրերին առավել հեշտ էր, քանի որ ՀՀ ընտրողների պետական ռեգիստրի բաց տվյալների շտեմարանը հնարավություն է տալիս հրապարակված տվյալների հաշվին գտնել քաղաքացու բնակության հասցեն, նույն հասցեում բնակվող այլ քաղաքացիների տվյալներ, որը երկրորդական հարվածի տակ է դնում նաև վարակված կամ մահացած քաղաքացու ընտանիքի անդամներին:

Հարկ է նշել, որ արտահոսքը տեղի է ունեցել ինչպես նախարարության բազայից, այնպես էլ նախարարության աշխատակիցների էլեկտրոնային փոստի հասցեներից: Ընդ որում, այստեղ հարկավոր է առանձնահատուկ ուշադրություն դարձնել այն հանգամանքի վրա, որ առողջապահական համակարգում պետական աշխատակիցները որպես հաղորդակցության և փաստաթղթերի շրջանառման միջոց կիրառում են իրենց անձնական էլեկտրոնային փոստի հաշիվները, ինչը կրկնակի վտանգի տակ է դնում տվյալների գաղտնիությունը, քանի որ աշխատակիցների անձնական էլեկտրոնային փոստերի անվտանգությունը չի մտնում նախարարության կամ որևէ այլ գերատեսչության պատասխանատվության տակ և չկան օրենսդրական մեխանիզմներ կամ լիազորություններ, որոնք կարտոնեին որևէ մարմնի հետևողականություն ցուցաբերել այս ուղղությամբ:

Առանձնահատուկ ուշադրության կարիք ունի նաև արտահոսած տվյալների հրապարակման աղբյուրները, որոնցից մեկը[35] «Զնդան» անվանումով ֆեյսբուկյան էջն է, որը ստեղծվել է 2019-ի հունիսի 20-ին, ֆեյսբուկում գրանցված է որպես

[35] Արտահոսք Առողջապահության նախարարության տվյալների բազայից. ի՞նչ խնդիր են լուծել կորոնավիրուսից մահացածների տվյալների հանրայնացմամբ. ՏԵՍԱՆՅՈՒԹ - https://factor.am/255818.html

լրատվական ընկերություն և տնօրինվում է ՌԴ-ում բնակվող օգտատիրոջ կողմից: Տվյալների արտահոսքի մյուս սկզբնաղբյուրները ադրբեջանական են և դրանց հասնելը առավել բարդ:

Ադրբեջանական աղբյուրների կողմից վարակված քաղաքացիների անձնական տվյալների արտահոսքը ենթադրում է նաև Ազգային անվտանգության ծառայության կողմից հատուկ միջոցառումներ և դրանց մասին պատշաճ իրազեկում հանրությանը: Սակայն, ԱԱԾ-ի կողմից այդպես էլ հանրությանը չներկայացվեց կատարված աշխատանքների և բացահայտված տեղեկությունների մասին որևէ իրազեկում, մինչդեռ ամեն բան սահմանափակվեց ՀՀ վարչապետի խորհրդականի անդրադարձով[36], որում բովանդակային որևէ հայտարարություն չկար:

Քաղաքացիների անձնական տվյալների արտահոսքին հաջորդեցին մի քանի դեպքեր, երբ անհայտ անձնաց կողմից ցուցաբերվել էին անհանդուրժողականության և ատելության քայլեր ուղղված վարակակիր քաղաքացիների նկատմամբ: Դրանցից մի քանիսը ստացան հանրային լայն արձագանք[37]:

Անձնական տվյալների պաշտպանությունը պետական համակարգում հաղորդակցությունն իրականացնելու գործընթացում առաջնահերթություն է, սակայն հայաստանյան պարկտիկայում հարկավոր է ընդգծել, որ ո՛չ Արդարադատության նախարարությունը, ո՛չ Անձնական տվյալների պաշտպանության գործակալությունը, ո՛չ էլ Բարձր տեխնոլոգիաների և արդյունաբերության նախարարությունը չեն առաջարկում օրենսդրական և պրակտիկ բարեփոխումներ, որոնց արդյունքում գերատեսչությունների աշխատակիցներն աշխատանքային հաղորդակցությունն իրականացնելիս կկարողանան օգտվել իրենց գերատեսչության սերվերին կցված էլեկտրոնային փոստերն ու ամպային արխիվները, որոնք կլինեն անվտանգ և մշտական վերահսկողության ներքո:

[36] Իրավապահները զբաղվում են կորոնավիրուսով վարակված քաղաքացիների տվյալների արտահոսքի մասին տեղեկության ստուգմամբ. Վարչապետի խոսնակ - https://medialab.am/73315/
[37] Մարտունիում «հարձակվել են» կորոնավիրուսով վարակված քաղաքացու տան վրա - https://www.panorama.am/am/news/2020/05/14/%D5%84%D5%A1%D6%80%D5%BF%D5%B8%D6%82%D5%B6%D5%AB-%D4%B3%D5%A5%D5%B2%D5%A1%D6%80%D6%84%D5%B8%D6%82%D5%B6%D5%AB%D6%84/2291422

Որքանո՞վ են պահպանվում անձնական տվյալները էլեկտրոնային տեղեկատվական համակարգերում

ՀՀ ընտրողների ռեգիստր

ՀՀ Կենտրոնական ընտրական հանձնաժողովի որոշմամբ[38]՝ ընտրողների սկանավորված ցուցակները տեղադրվում են ԿԸՀ կայքում (elections.am)՝ դրանցում ներառված տվյալները հասանելի դարձնելով բոլորին: Որոշման համաձայն, սկանավորված ցուցակներում տեսանելի են լինում ընտրողի հերթական համարը, ազգանունը, անունը, հայրանունը, ծննդյան ամսաթիվը, հաշվառման վայրի հասցեն, ինչպես նաև ընտրողի ստորագրությունը:

Ընդ որում, քաղաքացու հասցեի որոնման պարագայում համակարգը ցուցադրում է միևնույն հասցեում գրանցված բոլոր քաղաքացիների վերոթվարկյալ տվյալները, որն էլ այս համակարգի հաջորդ խնդիրն է:

Օրինակ, 2017թ. ապրիլի 2-ի խորհրդարանական ընտրություններից հետո Գործակալությունը ԿԸՀ-ից պահանջել էր կայքից հեռացնել 4000 ընտրողի անձնագրային տվյալները, քանի որ դրանց հրապարակումը խախտում էր Անձնական տվյալների պաշտպանության մասին օրենքը[39]:

ԿԸՀ կայքում տվյալների հրապարակումը անձնական տվյալների պաշտպանության խախտում է՝ հատկապես երկարաժամկետ տեղադրման դեպքում, երբ կարելի է ներբեռնել, պահպանել դրանք:

Անձնական տեղեկությունները խոցելի են դարձնում քաղաքացուն, հատկապես քիչ հանդիպող անուն-ազգանունով անձին: Կենսաչափական տվյալները, մասնագետների կարծիքով, հեշտությամբ կարող են այլ նպատակներով օգտագործվել պոտենցիալ հանցագործների, անձնական հաշվեհարդար ունեցողների, հաքերների և ընդհանրապես տվյալների հրապարակայնությունը շահադիտական նպատակներով կիրառել ցանկացողների կողմից:

Իհարկե, ՀՀ ընտրողների պետական ռեգիստրը մեծ նշանակություն ունի դիտորդական առաքելություն իրականցնողների համար, ինչպես նաև ընտրական գործընթացներն առավել թափանցիկ պայմաններում իրականացնելու համատեքստում, սակայն այս պարագայում ևս հարկավոր է մտածել մեխանիզմներ, որոնք առավել արդյունավետ, անվտանգ և ապահով կդարձնեն նման համահայկական բազաներում առկա տեղեկատվության պահպանումը: Օրինակ, այդ տվյալները կարող են հասանելի դառնալ ընտրական

---

[38] ԿԸՀ որոշումը, https://www.arlis.am/DocumentView.aspx?docID=111087

[39] Հոդվածը կայքում՝ https://www.panarmenian.net/arm/news/240297/

գործընթացներում՝ կոնկրետ սահմանված ժամկետներով և պայմաններով, որոնք կարող են սահմանվել ՀՀ ընտրական օրենսգրքում:

Օրինակ, Ուկրաինայում և Ռուսաստանում ընտրական հանձնաժողովների կայքերում յուրաքանչյուր ընտրողի համար առանձին բաժին է հատկացված, որտեղ տվյալները կարող է տեսնել միայն այդ տվյալների սեփականատերը: Ի տարբերություն ՀՀ ԿԸՀ կայքի, այդ երկրներում օգտատերն ինքն է մուտքագրում իր բոլոր տվյալները, որից հետո միայն սահմանափակ ժամանակով կարող է տեսնել ընտրության հետ կապված տեղեկություններ՝ իր համարը, ընտրատեղամասը: Եվրամիությունը 2018թ. մայիսին խստացրել էր ընտրություններից առաջ կուսակցությունների և ֆոնդերի կողմից ընտրողների անձնական տվյալների հավաքագրման համար նախատեսված պատժաչափը՝ դրանով կանխարգելելով նաև տվյալների հավաքագրումը[40]: Հետաքրքրական է Օբամայի երկրորդ ժամկետի ընտրությունը, երբ հատուկ ծրագրի միջոցով մի քանի ամսում յուրաքանչյուր ընտրողի վերաբերյալ հավաքվել է 800 միավոր տեղեկություն, որոնք Օբամայի վարչակազմի կողմից կրկին հաղթելու լավ միջոց են հանդիսացել: Այս երևույթն ԱՄՆ-ում արդեն լուրջ սպառնալիք է դարձել, և իշխանությունները որոշել են պայքարել քաղաքացիների անձնական տվյալների պաշտպանության համար[41]:

Ըստ մեդիա փորձագետ Սամվել Մարտիրոսյանի, ՏԻՄ և այլ ընտրությունների ժամանակ տվյալները կարելի է տրամադրել կուսակցություններին կամ բացել 10 օր առաջ՝ միայն հայկական IP-ների համար[42]:

Հայաստանում ռազմական դրության հայտարարման պահից սկսած ՀՀ ընտրողների պետական ռեգիստրը հեռացվեց ցանցից և անհասանելի դարձավ սովորական օգտատերերի համար, մինչդեռ դա լուրջ խնդիրներ էր առաջացնում նաև մինչ այդ: Ռազմական դրության դադարեցման պահից սկսած այդ բազան վերականգնվելու է ՀՀ կենտրոնական ընտրական հանձնաժողովի պաշտոնական կայքում և կրկին հասանելի է դառնալու բոլորի համար:

---

[40] Հոդված՝ https://ua.news/ru/yevrosoyuz-pidnyav-riven-kontrolyu-za-zborom-personalnih-danih/

[41] Հոդված՝ https://www.dw.com/ru/%D0%BD%D0%B0-%D1%87%D1%82%D0%BE-%D0%B8%D0%B4%D1%83%D1%82-%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8-%D0%B2-%D1%81%D1%88%D0%B0-%D1%80%D0%B0%D0%B4%D0%B8-%D0%B3%D0%BE%D0%BB%D0%BE%D1%81%D0%BE%D0%B2-%D0%B8%D0%B7%D0%B1%D0%B8%D1%80%D0%B0%D1%82%D0%B5%D0%BB%D0%B5%D0%B9/a-19041304-0

[42] Հոդված https://www.shantnews.am/news/view/274145.html

Դատական տեղեկատվական համակարգ:

Դատական նիստերը դռնբաց են[43]: Դատական վարույթը կամ դրա մի մասն օրենքով սահմանված դեպքերում և կարգով դատարանի որոշմամբ կարող է անցկացվել դռնփակ՝ վարույթի մասնակիցների մասնավոր կյանքի, անչափահասների կամ արդարադատության շահերի, ինչպես նաև պետական անվտանգության, հասարակական կարգի կամ բարոյականության պաշտպանության նպատակով: Ստացվում է, որ ցանկացած անձ իրավունք ունի հետևել դատապրոցեսին, անգամ, դատական նիստին ներկա անձն սղագրություն և ձայնագրություն կատարելու իրավունք ունի:

Դատական ատյանում վարույթը եզրափակող դատական ակտերը ենթակա են պարտադիր հրապարակման դատական իշխանության պաշտոնական կայքում՝ Դատալեքս համակարգում[44], դռնփակ անցկացվելու դեպքում դատական իշխանության կայքում հրապարակվում է եզրափակիչ դատական ակտի եզրափակիչ մասը, եթե այն չի պարունակում օրենքով պահպանվող գաղտնիք:

Ստացվում է, որ հանրային վերահսկողությանը զուգահեռ, անսահմանափակ հնարավորություն է ստեղծվում Դատալեքս կայքի միջոցով մուտք գործել ուրիշի անձնական կյանք:

Այս հարցում կարծիքները տարաբերվում են, օրինակ նախկին լրագրող Թագուհի Թովմասյանը դիմել է Բարձրագույն դատական խորհուրդի նախագահին՝ առաջարկելով դատական տեղեկատվական համակարգում առկա որոշ գործերով փակել տուժողների անձնական տվյալները[45]: Իսկ ըստ Գործակալության պետ Գևորգ Հայրապետյանի դիրքորոշման, դա ոչ թե իրավունքի խախտում է, այլ՝ իրավունքին միջամտություն. «Դատալեքսում դատական ակտերը հրապարակվում են, որովհետեւ այդ հրապարակայնությունը հնարավորություն է տալիս վերահսկելու, գլոբալ առումով ապահովելու արդարադատության իրականացումը, հնարավորություն է տալիս ունենալու վստահություն դատական իշխանության նկատմամբ, կարողանալու օգտվել դատական պրակտիկայից, զարգացնելու իրավունքը եւ այլն, եւ այլն: Այսինքն՝ հասարակությունն է օրենքի միջոցով այդպես որոշել»[46]:

Իհարկե, թափանցիկությունն ու հասանելիությունը կարևոր ու անփոխարինելի գործոններ են, բայց դրանք չպետք է դառնան մարդու իրավունքների ոտնահարման համատարած դրսևորման առիթ կամ պատճառ:

---

[43] ՀՀ դատական օրենսգիրք https://www.arlis.am/documentview.aspx?docid=146620
[44] Դատական տեղեկատվական համակարգ - http://datalex.am/
[45] Հոդվածը՝ https://hayeli.am/?p=146805&l=am
[46] Հոդվածը՝ https://armtimes.com/hy/article/179007

Հարկ է նշել, որ և՛ դատական տեղեկատվական համակարգը, և՛ ՀՀ ընտրողների պետական ռեգիստրը հասանելի են ոչ միայն Հայաստանի տարածքում, այլև Հայաստանից դուրս՝ ամբողջ աշխարհում։

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆՆԵՐ ԵՎ ԱՌԱՋԱՐԿՈՒԹՅՈՒՆՆԵՐ

Այսպիսով, անձնական տվյալների պաշտպանության վերաբերյալ իրավիճակը արտակարգ դրության պայմաններում վերլուծելուց հետո կարելի է անել հետեւյալ եզրակացությունները.

Համավարակի դեմ պայքարը կարող է իրավաչափ դարձնել մարդու հիմնական իրավունքներին միջամտությունը, սակայն այդ միջամտությունը պետք է բավարարի ՀՀ Սահմանադրությամբ սահմանված համաչափության սկզբունքին (հոդված 78):

Տվյալների պաշտպանության եվրոպական խորհուրդը նշել է, որ անձանց «հետևելը, այդ թվում՝ բջջային հեռախոսի միջոցով, կարող է բացառիկ պայմաններում լինել համաչափ: Այդ դեպքում այն պետք է ենթարկվի ուժեղացված հսկողության՝ տվյալների պաշտպանության սկզբունքների պահպանումը ապահովելու համար *(կիրառված միջոցի համաչափությունը՝ տևողության և ծավալի տեսանկյունից, տվյալների սահմանափակ պահպանումը և սահմանափակման նպատակը):*

Հայաստանի Հանրապետության կողմից վավերացված միջազգային կոնվենցիաներով սահմանված նորմերին չհամապատասխանող միջոցների կիրառման պարագայում անձը իրավասու է լինելու դիմել դատական պաշտպանության միջոցին, այդ թվում՝ նաև ՀՀ մարդու իրավունքների վերաբերյալ միջազգային պայմանագրերի հիման վրա գործող մարմինների (մասնավորապես՝ ՄԻԵԴ):

Մասշտաբային տեղեկատվության հավաքագրումը կարող է պետության կողմից կիրառվել միայն այն դեպքում, եթե գիտական վերլուծության համաձայն՝ հասարակության առողջության պաշտպանության համար այլընտրանքային արդյունավետ այլ միջոց չկա:

<u>Առաջարկվում է.</u>

Կարևոր է, որպեսզի ներկայացվեն բավարար երաշխիքներ առ այն, որ ապահովվելու է անձնական տվյալների ամբողջական պաշտպանությունը արտակարգ դրության ավարտից հետո, ինչը բավարար կերպով կարգավորված չէ Անձնական տվյալների պաշտպանության մասին ՀՀ օրենքում:

Ձեռնարկել վերահսկողական քայլեր՝ սոցիալական ցանցերում անձնական տվյալների պաշտպանության ուղղությամբ, ստեղծել հնարավորություն քաղաքացիների առցանց բողոքների ընդունման:

Ապահովել գործակալության անկախությունը՝ ձևավորելով խորհրդատվական մարմին և ընդգրկելով դրանում մարդու/քաղաքացիական իրավունքների պաշտպանության հասարակական կազմակերպությունների ներկայացուցիչների: Դա թույլ կտա զարգացնել աշխատակիցների պրոֆեսիոնալիզմը և նվաճել հանրության վստահությունը: Արմատավորել հանրությանը հաշվետվություն տալու պրակտիկան՝ Ազգային ժողովին ներկայացվող և հրապարակվող տարեկան հաշվետվության ֆորմատով:

Բարձրացնել պետական հաղորդակցական համակարգում ՏՏ գործիքների պաշտպանության և տվյալների փոխանակման գործընթացի անվտանգությունը, ներառյալ Մալբրի համակարգի անվտանգությունը:

Սահմանել առավել խիստ պատժաչափ՝ որոշում կայացնող պետական պաշտոնատար անձանց կողմից անձնական տվյալների պաշտպանության իրավունքի խախտման դեպքում:

ՎԵՐՋԱԲԱՆ

Սույն զեկույցը ներկայացնում է անձնական տվյալների իրավունքի խախտման դեպքերը Հայաստանի Հանրապետությունում արտակարգ դրության պայմաններում:

Այս զեկույցի պատրաստումը հնարավոր է դարձել Ա.Դ.Սախարովի անվան մարդու իրավունքների պաշտպանության հայկական կենտրոնի աջակցությամբ:

Զեկույցի հեղինակ՝

Բոլորը հանուն հավասր իրավունքների հիմնադրամի հիմնադիր-իրավաբան, Վանուհի Գասպարյան