# ՀԻՄՆԱՎՈՐՈՒՄ

## «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՔՐԵԱԿԱՆ ՕՐԵՆՍԳՐՔՈՒՄ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ», «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՔՐԵԱԿԱՆ ԴԱՏԱՎԱՐՈՒԹՅԱՆ ՕՐԵՆՍԳՐՔՈՒՄ ԼՐԱՑՈՒՄՆԵՐ ԵՎ ՓՈՓՈԽՈՒԹՅՈՒՆՆԵՐ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ», «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՔԱՂԱՔԱՑԻԱԿԱՆ ՕՐԵՆՍԳՐՔՈՒՄ ԼՐԱՑՈՒՄՆԵՐ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ», «ԱՆԿԱՆԽԻԿ ԳՈՐԾԱՌՆՈՒԹՅՈՒՆՆԵՐԻ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ», «ԱՊՕՐԻՆԻ ԾԱԳՈՒՄ ՈՒՆԵՑՈՂ ԳՈՒՅՔԻ ԲՌՆԱԳԱՆՁՄԱՆ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆՆԵՐ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ», «ՀԱՆՐԱՅԻՆ ԾԱՌԱՅՈՒԹՅԱՆ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ», «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԴԱՏԱԿԱՆ ՕՐԵՆՍԳԻՐՔ» ՍԱՀՄԱՆԱԴՐԱԿԱՆ ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» ԵՎ «ՍԱՀՄԱՆԱԴՐԱԿԱՆ ԴԱՏԱՐԱՆԻ ՄԱՍԻՆ» ՍԱՀՄԱՆԱԴՐԱԿԱՆ ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» ՕՐԵՆՔՆԵՐԻ ՆԱԽԱԳԾԵՐԻ ԸՆԴՈՒՆՄԱՆ

1. **<u>Ընթացիկ իրավիճակը և իրավական ակտի ընդունման անհրաժեշտությունը</u>.**

Տեղեկատվական տեխնոլոգիաների զարգացումն ամբողջ աշխարհում ուղիղ համեմատական է կյանքի որակի բարձրացմանը, քանի որ այն նախադրյալներ է ստեղծում դրական առումով աննախադեպ տնտեսական և սոցիալական փոփոխությունների համար: Այդ զարգացումներն, այնումենայնիվ, իրենց հետ առաջ են բերում նաև նոր խնդիրներ՝ նոր մարտահրավերների առջև կանգնեցնելով թե միջազգային հանրությանը, և թե ներպետական իրավաստեղծ և իրավակիրառ գործունեություն իրականացնող մարմիններին: Ի թիվս այլնի՝ այդպիսի լրջագույն խնդիր է տեղեկատվական տեխնոլոգիաների կիրառմամբ կատարվող նոր հանցատեսակների տարածումը, ինչպես նաև ավանդական համարվող հանցանքների կատարումը այդ միջոցների լայն շրջանակի օգտագործման եղանակներով: Այս ուղղությամբ վերջին զարգացումներից է նաև կրիպտոակտիվների շուկայի ձևավորումը:

Դեռևս Հայաստանի Հանրապետության նախագահի՝ 2011 թվականի դեկտեմբերի 29-ին ընդունված՝ «Հայաստանի Հանրապետությունում կազմակերպված հանցավորության դեմ պայքարի արդյունավետության բարձրացման ազգային ծրագիրը հաստատելու մասին» N ՆԿ-232-Ն կարգադրության համաձայն՝ *«Կիբեռանվտանգության հզորացումը և կիբեռհանցագործությունների դեմ պայքարը ՀՀ համար ռազմավարական նշանակության խնդիրներ են: Կիբեռհանցագործությունները նոր երևույթ չեն: Դրանց կատարման մեխանիզմները մշտապես փոփոխվում և կատարելագործվում են: Գաղտնիք չէ, որ հանցագործներին հաջողվում է ոչ միայն օգտվել կիբեռտեխնոլոգիական նորույթներից, այլև մշակել և ներդնել դրանք՝ հետապնդելով ինչպես համակարգչային ցանցի օգնությամբ կամ դրա դեմ հանցանք կատարելու, այնպես էլ հանցագործության հետքերը թաքցնելու նպատակ: Նկատի ունենալով ողջ աշխարհում ահագնացող թափերով զարգացող ահաբեկչության նոր տեսակի զարգացումը՝ խիստ կարևոր է կիբեռահաբեկչությանը վերաբերող այնպիսի խնդիրներին լուծում տալը, ինչպիսիք են կիբեռտարածության մեջ և համացանցում ահաբեկչական գաղափարախոսության քարոզման, ահաբեկչական կազմակերպությունների կողմից անդամների հավաքագրման կանխումն ու բացահայտումը, ահաբեկչության դեմ պայքարող ՀՀ և այլ երկրների կառույցների տվյալների օպերատիվ փոխանակման մեխանիզմների կատարելագործումը, կիբեռահաբեկչության դեմ պայքարող մասնագիտացված ստորաբաժանումների արդի պայմաններին համընթաց տեխնիկական վերազինումը: Կարևոր է նաև կիբեռտարածության մեջ կատարվող տնտեսական և սեռական բնույթի հանցագործությունների դեմ պայքարը, ինչը շատ հաճախ կրում է կազմակերպված ցանցային բնույթ: Այդ առումով առանցքային նշանակություն ունի նաև նման բնույթի հանցագործությունների կանխման և բացահայտման ուղղությամբ իրականացվող*

*աշխատանքների, դրանց վերաբերյալ առկա օպերատիվ տվյալների փոխանակման ընթացակարգերի կատարելագործումը»*[1]*:*

Հայաստանի Հանրապետությունը 2001 թվականի նոյեմբերի 23-ին Բուդապեշտում ստորագրել և 2006 թվականի մարտի 21-ին վավերացրել է «Կիբերհանցագործությունների մասին» կոնվենցիան (այսուհետ՝ նաև Բուդապեշտի կոնվենցիա)[2], որը կիբերհանցավորության դեմ պայքարի նյութաիրավական և դատավարական հիմքերի ձևավորման տեսանկյունից հիմնարար նշանակություն ունեցող միջազգային իրավական փաստաթուղթ է[3]:

«Կիբերհանցագործությունների մասին» Բուդապեշտի կոնվենցիայի՝ Եվրոպայի խորհրդի նախարարների կոմիտեի մշակած բացատրական զեկույցի համաձայն՝ այս կոնվենցիայի նպատակներն են՝

1) կիբերհանցագործություններին առնչվող ներպետական քրեական օրենսդրության ներդաշնակեցումը.

2) կիբերհանցագործությունների կամ համակարգչային համակարգերի օգնությամբ կատարվող հանցանքների քննության կամ էլեկտրոնային տեսքով ապացույցների ձեռքբերման համար անհրաժեշտ դատավարական գործիքակազմի ապահովումը.

3) միջազգային համագործակցության արագ և արդյունավետ ռեժիմի ձևավորումը[4]:

Տեղեկատվական տեխնոլոգիաների հետ կիբերհանցագործությունների սերտ կապով պայմանավորված՝ դրանց զարգացման տեմպերը մշտապես արդիական խնդիր են դարձնում կիբերհանցագործություններին հակազդելու համար անհրաժեշտ օրենսդրական դաշտի ձևավորումը, և կիբերհանցավորության դեմ

---

[1] Հասանելի է հետևյալ հղմամբ՝ https://www.arlis.am/documentview.aspx?docid=121592

[2] Հասանելի է հետևյալ հղմամբ՝ https://www.arlis.am/DocumentView.aspx?DocID=48028

[3] Հայաստանի Հանրապետությունը 2003 թվականի հունվարի 28-ին Ստրասբուրգում ստորագրել է նաև «Համակարգչային համակարգերի միջոցով կատարվող ռասիստական և քսենոֆոբիական բնույթի արարքների քրեականացման մասին» լրացուցիչ արձանագրությունը:

[4] Հասանելի է հետևյալ հղմամբ՝ https://rm.coe.int/16800cce5b

պայքարի ոլորտին առնչվող օրենսդրության բարեփոխումը միտված է այս երևույթի դեմ պայքարի արդյունավետ գործիքակազմի ներդրմանը՝ հաշվի առնելով գործնականում արձանագրված խնդիրները և միջազգային չափանիշները:

Այսպես, բարեփոխումների շրջանակում նոր լուծումներ են պահանջում ներքոհիշյալ ուղղություններով գործնականում առկա հետևյալ խնդիրներով.

1) **Կիբերհանցագործություններին առնչվող նյութահիրավական և դատավարական հասկացութային ապարատի հստակեցումը.**

ՀՀ քրեական օրենսգիրքը և այլ իրավական ակտերը չեն պարունակում «կիբերհանցագործություն», «կիբերհարձակում» կամ «կիբերբռնություն» հասկացությունների սահմանումները: Վերաբերելի փաստաթղթերով, մասնավորապես՝ *Հայաստանի Հանրապետության ազգային անվտանգության ռազմավարության (ընդունվել է 2020 թվականին)* և *«Հայաստանի թվայնացման ռազմավարությանը, ռազմավարության միջոցառումների ծրագրին և արդյունքային ցուցանիշներին հավանություն տալու մասին» ՀՀ կառավարության 2021 թվականի փետրվարի 11-ի 183-Լ որոշման մեջ* հիշատակվում են «կիբերտիրույթ», «կիբերանվտանգություն», «կիբերհանցավորություն» և «կիբերհարձակում» եզրույթները, սակայն այդ եզրույթներն ուղղակիորեն սահմանված չեն ազգային օրենսդրության մեջ: *«Էլեկտրոնային հաղորդակցության մասին» ՀՀ օրենքը* պարունակում է վերաբերելի այլ սահմանումներ, ինչպիսիք են *«հաճախորդը և բաժանորդը», «ինտերնետային ծառայություն մատուցողը», «իրական ժամանակը» կամ «ծառայություն մատուցողը»*, որոնք ևս կարող են օգտագործվել՝ ի լրումն այն բնորոշումների, որոնք նախատեսված են միջազգային փաստաթղթերով, այդ թվում՝ «Կիբերհանցագործությունների մասին» Բուդապեշտի կոնվենցիայով և դրան կից Առաջին լրացուցիչ արձանագրությամբ, որոնք, ինչպես արդեն նշվել է, Հայաստանի Հանրապետությունը վավերացրել է:

Թեև խնդրո առարկա ոլորտի առնչությամբ օրենսդրության մեջ հասկացությունների սահմանումները պետք է հասցնել նվազագույնի, քանի որ կիբերհանցագործությունների նորանոր դրսևորումների զարգացման տեմպերը

բացառում են սպառիչ բնորոշումներ ունենալու հնարավորությունը և փոխարենը, մասնավորապես, պետք է առաջին պլան մղել այն արարքների քրեականացումը, որոնք կարող են դիտարկվել որպես կիբերհանցագործություն, այդուհանդերձ, գործնական անհրաժեշտությունն արդիական է դարձնում կիբերհանցագործությունների ընդհանուր շրջանակ ունենալու անհրաժեշտությունը՝ հիմքում ունենալով «Կիբերհանցագործությունների մասին» Բուդապեշտի կոնվենցիայով, ըստ էության, առաջ քաշված այն չափանիշը, համաձայն որի՝ իբրև այդպիսին դիտարկվում են այն հանցանքները, որոնցով թիրախավորվում են համակարգիչը, համակարգչային համակարգը կամ համակարգչային ցանցը, կամ այն հանցանքները, որոնք կատարվում են տեղեկատվական կամ հաղորդակցական տեխնոլոգիաների միջոցով:

Կիբերհանցագործությունների փաստացի բնորոշումը՝ այդպիսին համարվող ՀՀ քրեական օրենսգրքի հատուկ մասում արդեն իսկ նախատեսված հանցանքների առանձին ցանկ սահմանելով, կապահովի այս տեսակ հանցագործությունների քննությունը մասնագիտացած ստորաբաժանումների կողմից՝ բարձրացնելով համապատասխան դեպքերով նախաձեռնված քրեական վարույթներով բազմակողմանի, լրիվ և օբյեկտիվ քննություն իրականացնելու շանսերը:

Բացի այդ, նման հստակեցումը կիբերհանցագործությունների դեմ արդյունավետ պայքարի դատավարական հատուկ գործիքակազմի պատշաճ իրավակարգավորման հիմք կդառնա: Մասնավորապես, կիբերհանցագործությունների շրջանակի տարբերակման արդյունքում կբացառվի այն իրավիճակը, երբ էլեկտրոնային ապացույցների ձեռք բերման հիմնական դատավարական եղանակները կիրառելի չեն լինի կիբերհանցագործությունների որոշ տեսակների առնչությամբ նախաձեռնված քրեական վարույթի շրջանակում:

Կիբերհանցագործությունների որոշակի շրջանակի հստակեցումը հնարավորություն կտա լուծելու նաև վիճակագրական խնդիրները: Ոչ թե ընդհանրական, այլ կիբերհանցագործություններին վերաբերող վիճակագրության վարումը կարող է առանձնակի կարևորություն ունենալ քրեական

արդարադատության ոլորտի մարմինների կողմից կիբերհանցավորության դեմ առավել արդյունավետ պայքար մղելու համար հասցեական քաղաքականություն վարելու և անհրաժեշտ իրավակարգավորումներ մշակելու տեսանկյունից:

Բուդապեշտի կոնվենցիան, անդրադառնալով կոնվենցիոնալ կարգավորման առարկա տվյալների և դրանց ստացման դատավարական եղանակների մասին, տարանջատում է երեք խումբ տվյալներ, այն է՝ բաժանորդի տվյալներ (subscriber data), փոխանցվող տվյալներ (traffic data) և բովանդակային տվյալներ (content data): Ընդ որում, Կիբերհանցավորության մասին կոնվենցիայի 1-ին հոդվածի 4-րդ ենթակետի համաձայն՝ *««փոխանցվող տվյալներ» նշանակում է՝ ցանկացած համակարգչային տվյալ՝ կապված համակարգչային համակարգի միջոցով հաղորդակցության հետ, որն առաջացել է սփեղծված համակարգչային համակարգով, որը ձևավորված է որպես հաղորդակցության շղթայի մի մաս և ցույց է տալիս հաղորդակցությունների ծագումը, վերջնակետը, ուղին, ժամանակը, ամսաթիվը, չափը, տևողությունը կամ նշված ծառայության տեսակը»*:

Թեև Հայաստանի Հանրապետության քրեական դատավարության օրենսգիրքը (այսուհետ՝ նաև Օրենսգիրք) տեղեկատվության պահանջ քննչական գործողության (232-րդ հոդված) շրջանակում նախատեսվում է ֆիքսված կամ բջջային հեռախոսային ցանցի միջոցով հաղորդակցվողների հեռախոսահամարները, հեռախոսահամարի բաժանորդի անհատական տվյալները, հեռախոսային հաղորդակցությունն սկսելու պահին և դրա ընթացքում հաղորդակցվողների գտնվելու վայրը և նրանց տեղաշարժը պարզելու համար անհրաժեշտ տվյալները, համացանցին միանալու և համացանցից դուրս գալու վայրը, ժամանակը և տևողությունը, համացանցն օգտագործողի կամ բաժանորդի անհատականացման տվյալները, հեռախոսահամարը, որով նա միանում է ընդհանուր օգտագործման հեռախոսացանցին, համացանցային հասցեն, ներառյալ ինտերնետ պրոտոկոլի (IP) հասցեն, համացանցային հեռախոսազանգն ստացողի անհատականացման տվյալները ստանալու, կամ թվային, այդ թվում՝ հեռախոսային հաղորդակցության գաղտնի քննչական գործողության (249-րդ) շրջանակում՝ ֆիքսված կամ բջջային

հեռախոսային ցանցի դեպքում՝ հեռախոսային խոսակցության, տեքստային, պատկերային, ձայնային, տեսաձայնային և այլ հաղորդագրության բովանդակությունը, բաժանորդի մուտքային և ելքային զանգերը, հեռախոսային հաղորդակցությունն սկսելու և ավարտելու ժամանակը, հեռախոսազանգի վերահասցեագրման կամ փոխանցման դեպքում այն հեռախոսահամարը, որին փոխանցվել է հեռախոսազանգը, համացանցային հաղորդակցության, այդ թվում՝ համացանցային հեռախոսային հաղորդակցության և համացանցի միջոցով փոխանցվող էլեկտրոնային հաղորդումների դեպքում՝ հաղորդակցության բովանդակությունը, համացանցային հեռախոսազանգերի մուտքային և ելքային զանգերը վերահսկելու հնարավորություն, այդուհանդերձ, այս տվյալների որոշակի դասակարգման առկայությունը հնարավորություն կտա առավել հստակ կանոնակարգել դրանց ստացմանն ուղղված դատավարական գործիքները և դրանց կիրառման դատավարական երաշխիքները: Խոսքը, մասնավորապես, վերաբերում է նրան, որ այս տվյալներից յուրաքանչյուրի ստացումը ենթադրում է տարբեր աստիճանի միջամտություն անձի՝ նամակագրության, հեռախոսային խոսակցությունների և հաղորդակցության այլ ձևերի ազատության և գաղտնիության իրավունքին, հետևաբար՝ նշված իրավունքի համաչափ սահմանափակումը յուրաքանչյուր կոնկրետ դեպքում կարող է ենթադրել դատավարական տարբեր երաշխիքների և պայմանների առկայության անհրաժեշտություն (ավելի մասնրամասն, տե՛ս, ստորև՝ 2-րդ կետում):

**2) Դատական վերահսկողության երաշխիքների ընդլայնումը.**

ՀՀ Սահմանադրության 33-րդ հոդվածի համաձայն՝

*«1. Յուրաքանչյուր ոք ունի նամակագրության, հեռախոսային խոսակցությունների և հաղորդակցության այլ ձևերի ազատության և գաղտնիության իրավունք:*

*2. Հաղորդակցության ազատությունը և գաղտնիությունը կարող են սահմանափակվել միայն օրենքով՝ պետական անվտանգության, երկրի տնտեսական բարեկեցության, հանցագործությունների կանխման կամ բացահայտման,*

*հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով:*

*3. Հաղորդակցության գաղտնիությունը կարող է սահմանափակվել միայն դատարանի որոշմամբ, բացառությամբ երբ դա անհրաժեշտ է պետական անվտանգության պաշտպանության համար և պայմանավորված է հաղորդակցվողների՝ օրենքով սահմանված առանձնահատուկ կարգավիճակով»:*

ՀՀ Սահմանադրության 33-րդ հոդվածը, սահմանելով նամակագրության, հեռախոսային խոսակցությունների և հաղորդակցության այլ ձևերի ազատության և գաղտնիության իրավունքը, հստակեցնում է նաև այն իրավաչափ նպատակները, որոնց առկայության դեպքում այն կարող է սահմանափակվել: Բացի դրանից՝ երկրի հիմնական օրենքով նախատեսված է բացառապես դատարանի որոշմամբ այս իրավունքը սահմանափակելու պահանջ:

Այս հիմնարար իրավունքը նախատեսված է նաև Մարդու իրավունքների համընդհանուր հռչակագրում[5], «Մարդու իրավունքների և ազատությունների պաշտպանության մասին» եվրոպական կոնվենցիայում (այսուհետ՝ նաև Կոնվենցիա)[6], «Քաղաքացիական և քաղաքական իրավունքների պաշտպանության մասին» միջազգային դաշնագրում[7]:

Կոնվենցիայի 8-րդ հոդվածի համաձայն՝ *«Յուրաքանչյուր ոք ունի անձնական ու ընտանեկան կյանքի, բնակարանի և նամակագրության նկատմամբ հարգանքի իրավունք: Չի թույլատրվում պետական մարմինների միջամտությունն այդ իրավունքի իրականացմանը, բացառությամբ այն դեպքերի, երբ դա նախատեսված է օրենքով և անհրաժեշտ է ժողովրդավարական հասարակությունում՝ ի շահ պետական անվտանգության, հասարակական կարգի կամ երկրի տնտեսական*

[5] Մարդու իրավունքների համընդհանուր հռչակագիր, ընդունվել և հռչակվել է ՄԱԿ-ի գլխավոր ասամբլեայի 1948 թ. դեկտեմբերի 10-ի 217 Ա (III) բանաձևի համաձայն ուժի մեջ է մտել 10.12.1948:

[6] «Մարդու իրավունքների եւ հիմնարար ազատությունների պաշտպանության մասին» եվրոպական կոնվենցիա (ընդունվել է 04.11.1950 թ., ուժի մեջ է մտել 03.09.1953 թ., ՀՀ-ի համար կոնվենցիան ուժի մեջ է մտել 26.04.2002թ.:

[7] «Մարդու իրավունքների եւ հիմնարար ազատությունների պաշտպանության մասին» եվրոպական կոնվենցիա (ընդունվել է 04.11.1950 թ., ուժի մեջ է մտել 03.09.1953 թ., ՀՀ-ի համար կոնվենցիան ուժի մեջ է մտել 26.04.2002թ.:

*բարեկեցության, ինչպես նաև անկարգությունների կամ հանցագործությունների կանխման, առողջության կամ բարոյականության պաշտպանության կամ այլ անձանց իրավունքների և ազատությունների պաշտպանության նպատակով»:*

Կոնվենցիայի 8-րդ հոդվածով սահմանվում է անձնական և ընտանեկան կյանքի, բնակարանի և նամակագրության նկատմամբ հարգանքի իրավունքը: Կոնվենցիոնալ այս դրույթի առաջնային նպատակն է պաշտպանել անձնական և ընտանեկան կյանքը, բնակարանը և նամակագրությունը պետական մարմինների կամայական միջամտություններից (տե՛ս Մարդու իրավունքների եվրոպական դատարանի՝ Libert v. France գործով 2018 թվականի փետրվարի 22-ի վճիռը, գանգատ թիվ 588/13, կետեր 40-42)[8]:

Մարդու իրավունքների եվրոպական դատարանը (այսուհետ՝ նաև Եվրոպական դատարան) բազմիցս հաստատել է, որ անձի՝ անձնական կյանքի և նամակագրության նկատմամբ հարգանքի իրավունքին պետական մարմնի ցանկացած միջամտություն պետք է լինի օրենքի համաձայն: Այս արտահայտությունը պարտադրում է ոչ միայն պահպանել ներպետական օրենսդրությունը, այլև վերաբերում է օրենքի որակին՝ պահանջելով, որ այն համատեղելի լինի իրավունքի գերակայության սկզբունքի հետ: Ներպետական օրենսդրությունը պետք է լինի հստակ, կանխատեսելի և բավականաչափ մատչելի[9]: Օրինականության սկզբունքը պահանջում է նաև համապատասխան երաշխիքների առկայություն՝ ապահովելու համար, որ անհատի՝ Կոնվենցիայի 8-րդ հոդվածով սահմանված իրավունքները պահպանվեն: Պետական մարմինների կողմից գաղտնի վերահսկողության իրականացման համատեքստում ներպետական օրենսդրությամբ

[8] Տե՛ս «Ուղեցույց Մարդու իրավունքների և հիմնարար ազատությունների պաշտպանության մասին» Եվրոպական կոնվենցիայի 8-րդ հոդվածի վերաբերյալ, 2020թ. օգոստոսի 31-ի դրությամբ, հասանելի է՝
https://www.echr.coe.int/Documents/Guide_Art_8_HYE.pdf

[9] Տե՛ս Մարդու իրավունքների եվրոպական դատարանի՝ ***De Tommaso v. Italy [GC]*** գործով 2017 թվականի փետրվարի 23-ի վճիռը, գանգատ թիվ 43395/09, կետ 107, ***Brazzi v. Italy*** գործով 2018 թվականի սեպտեմբերի 27-ի վճիռը, գանգատ թիվ 57278/11, կետ 39, ***Giuliano Germano v. Italy*** գործով 2023 թվականի հունիսի 22-ի վճիռը, գանգատ թիվ 10794/12, կետ 91:

անհատի՝ 8-րդ հոդվածով նախատեսված իրավունքը պետք է ապահովվի պաշտպանությամբ կամայական միջամտությունից[10]:

Բուդապեշտի կոնվենցիայի բացատրական զեկույցի համաձայն՝ նշված միջազգային իրավական փաստաթուղթը, ամրագրելով պետությունների պարտավորությունը՝ նախատեսելու դրանով սահմանված դատավարական ընթացակարգերը կիբերհանցավորության դեմ արդյունավետ պայքարի շրջանակում, միաժամանակ ընդգծում է համապատասխան պայմանների և երաշխիքների առկայության անհրաժեշտությունը՝ դրանց շարքում ներառելով դատական կամ այլ անկախ վերահսկողության առկայությունը, այն անձանց շրջանակի հստակեցումը, ում նկատմամբ համապատասխան դատավարական մեխազնիմները կիրառելի են, անհրաժեշտությունը և համաչափությունը, հիմնավորվածությունը, նվազ միջամտություն ենթադրող միջոցի բացակայությունը և այլն: Ընդ որում, Կիբերհանցավորության մասին Բուդապեշտի կոնվենցիան, ինչպես արդեն նշվել է, տարանջատում է երեք տեսակ տվյալների ստացման դատավարական ընթացակարգեր, այն է՝ բաժանորդի տվյալներ (subscriber data), փոխանցվող տվյալներ (traffic data) և բովանդակային տվյալներ (content data): Բուդապեշտի կոնվենցիայի վերոնշյալ բացատարական զեկույցի համաձայն՝ թեև կոնկրետ տվյալների ստացման համար նախատեսված դատավարական ընթացակարգերի առնչությամբ որոշակի երաշխիքներ նախատեսելը (որոշակի հնացագործությունների շրջանակ, դատական վերահսկողություն և այլն) կոնկրետ պետության հայեցողության շրջանակում է, այդուհանդերձ, ընդգծելով բովանդակային տվյալների ստացման պարագայում հաղորդակցության գաղտնիության իրավունքին առավել լուրջ միջամտության փաստը, նույն զեկույցը հատուկ արձանագրում է նաև առանձին պետությունների ներպետական օրենսդրությամբ բովանդակային և փոխանցվող տվյալների ստացման համար

[10] Տե՛ս Մարդու իրավունքների եվրոպական դատարանի՝ ***Khan v. United Kingdom*** գործով 2000 թվականի մայիսի 12-ի վճիռ, գանգատ թիվ 35394/97, կետեր 26-28:

միատեսակ դատավարական երաշխիքների առկայությունը, այդ թվում՝ դատարանի որոշում ունենալու պահանջը:

Փոխանցվող տվյալների առնչությամբ միջազգային փորձի որոշակի վերլուծությունը ցույց է տալիս, որ խնդիրն առավելապես դիտարկվում է ստացվող տվյալների առնչությամբ գաղտնիության ողջամիտ ակնկալիքի առկայության չափանիշի հիման վրա:

Այսպես, ԱՄՆ Նյու Ջերսի նահանգի Գերագույն դատարանը 2008 թվականին ***State v. Reid*** գործով կայացված որոշման մեջ պարզաբանել է, որ՝ *«անհատներին ինտերնետ ծառայություններ մատուցողի կողմից տրամադրվող համապատասխան հասցեն անհրաժեշտ է համացանցին միանալու համար: Այնումենայնիվ, երբ օգտատերերը ճամփորդում են համացանցում իրենց անձնական բնակարաններից, վերջիններս հիմքեր ունեն ակնկալելու, որ իրենց գործողությունները գաղտնի են: Նրանցից շատերը տեղյակ չեն, որ թվային IP հասցեն կարող է ֆիքսվել իրենց այցելած կայքէջերի կողմից: Առավել փորձված օգտատերերը հասկանում են, որ առանձին վերցրած՝ այդ թվերի եզակի շարանը, շատ քիչ, եթե իհարկե ոչինչ չի բացահայտում արտաքին աշխարհի համար: Միայն ինտերնետ ծառայություն մատուցողը կարող է IP հասցեով վերծանել օգտատիրոջ անունը»:*

Այնուհետև Նյու Ջերսիի դատարանը վկայակոչել է գաղտնիության հայեցակարգի սկզբունքային վերափոխումը՝ պայմանավորված ժամանակից համացանցային գործողություններով, փաստելով որ՝ *«չնայած վերծանված IP հասցեները չեն բացահայտում համացանցային հաղորդակցության բովանդակությունը, բաժանորդի տվյալներն ինքնին կարող են անձի մասին շատ բան պատմել: IP հասցեների ամբողջական ցանցի միջոցով հնարավոր է հսկել համացանցի օգտագործումը: Նման տեղեկությունը կարող է բացահայտել ինչ-որ մեկի անձնական տեղեկություններն այնպես, ինչպես հեռախոսային վճարումների բացահայտումը: Չնայած համացանցային հաղորդակցության բովանդակությունը*

*կարող է առավել բացահայտող լինել, երկու տեսակ տեղեկություններն էլ կարող գաղտնիության շահ պարունակել»*[11]*:*

Եվրոպայի խորհրդի Խորհրդարանական վեհաժողովի՝ «Զանգվածային հսկողության մասին» բանաձևով Եվրոպայի խորհուրդը հորդորում է անդամ պետություններին *«երաշխավորել, որ իրենց ներպետական օրենսդրությունը թույլ է տալիս հավաքել և վերլուծել անձնական տվյալները (այդ թվում՝ այսպես կոչված՝ «մետատվյալներ«) անձի համաձայնությամբ կամ հանցավոր գործունեության մեջ ներգրավված լինելու ողջամիտ կասկածի հիման վրա դատարանի թույլտվությամբ»*[12]*:*

Միավորված ազգերի կազմակերպության «Մարդու իրավունքների խորհրդի բանաձևը թվային դարաշրջանում գաղտնիության իրավունքի մասին» բանաձևում ևս ընդգծվում է, որ՝ *«մինչ մետատվյալները կարող են օգուտներ տալ, մետատվյալների որոշ տեսակներ, երբ համախմբվում են, կարող են բացահայտել անձնական տեղեկություններ, որը կարող է լինել ոչ պակաս զգայուն, քան հաղորդակցության իրական բովանդակությունը, դրանցով կարելի է պատկերացում կազմել անհատի վարքագծի, սոցիալական հարաբերությունների, անձնական նախասիրությունների և ինքնության մասին»*[13]*:*

Այս խնդրի առնչությամբ տեղին է հիշատակել նաև Բենեդիկն ընդդեմ Սլովենիայի գործով Եվրոպական դատարանի արտահայտած դիրքորոշումը[14]: Այսպես, նշված գործով ոստիկանությունն առանց դատարանի որոշման ինտերնետ ծառայություն մատուցող ընկերությունից պահանջել էր տրամադրել դինամիկ IP հասցեի օգտատիրոջ վերաբերյալ տվյալներ: Անդրադառնալով խնդրո առարկա շահին՝ նշված գործով փաստվել է, որ բաժանորդի վերաբերյալ տվյալները՝

---

[11] Տե՛ս State v. Reid, 945 A.2d 26, 28 (N.J. 2008), կետ 399, հասանելի է՝ https://casetext.com/case/state-v-reid-190

[12] Տե՛ս PACE Resolution on Mass Surveillance 2045 (21 April 2015), 19.1-րդ կետ, հասանելի է՝ https://pace.coe.int/pdf/4a791d302366df9e7daf5e5f3631b48a3426aaad5b1325392649b32d58688def/res.%202045.pdf

[13] Տե՛ս UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (23 March 2017), հասանելի է՝ https://digitallibrary.un.org/record/1307661#record-files-collapse-header

[14] Տե՛ս Մարդու իրավունքների եվրոպական դատարանի՝ ***Bendik v. Slovenia*** գործով 2018 թվականի ապրիլի 24-ի վճիռը, գանգատ թիվ 62357/14:

համակցված դինամիկ IP հասցեների հետ, ըստ էության, անձնական տվյալներ են: Եվ քանի որ այն հանրորեն մատչելի չէր, հետևաբար չէր կարող համեմատվել այն տեղեկությունների հետ, որոնք առկա են հեռախոսահամարների գրանցամատյանում կամ մեքենաների հաշվառման համարների վերաբերյալ հանրային տվյալների շտեմարանում: Նույնականացնելու համար բաժանորդին, ում կոնկրետ պահին կցված է եղել դինամիկ IP հասցեն՝ ինտերնետ ծառայություն մատուցողը պետք է վերլուծեր կոնկրետ հաղորդակցության շղթայի առնչությամբ պահպանված տեղեկությունները: Պահպանված այդ տվյալները կարող էին մասնավոր կյանքի գաղտնիության առնչությամբ մտավախության տեղիք տալ: Բաժանորդի տվյալների վերաբերյալ տեղեկություններ ձեռք բերելու նպատակը կոնկրետ գործով IP հասցեի օգտատիրոջ նույնականացումն էր: Եվրոպական դատարանի գնահատմամբ՝ նման առցանց գործողությունների մասին տեղեկություններն առնչվում էին գաղտնիության խնդրին այնքանով, որքանով վերագրվում էին նույնականացված կամ նույնականացման ենթակա անձին: Հետևաբար, ոստիկանության կողմից հայցվող երկրորդային տեղեկատվությունը, այն է՝ բաժանորդի անունն ու հասցեն, պետք է դիտարկվեր որպես անքակտելիորեն կապված նրա համապատասխան առցանց գործունեության հետ՝ այդպիսով բացահայտելով անձնական տվյալներ: Եվրոպական դատարանի գնահատմամբ՝ հակառակը կնշանակեր բացառել այն տեղեկությունների պաշտպանության անհրաժեշտությունը, որոնք կարող են շատ բան բացահայտել անհատի առցանց գործունեության մասին, ներառյալ նրա հետաքրքրությունների, համոզմունքների և անձնական կյանքի զգայուն մանրամասները:

Անդրադառնալով այն խնդրին, թե արդյոք դիմումատուն կարող էր ունենալ գաղտնիության ողջամիտ ակնկալիք, Եվրոպական դատարանն արձանագրել է, որ առցանց տիրույթում գաղտնիության ակնկալիքը կարևոր գործոն է, որը պետք է հաշվի առնել: Եվ այդ առնչությամբ Դատարանը չի կարևորել այն հանգամանքը, որ դիմումատուն չի փակել իր IP հասցեն, որը թեև կարող էր տեսանելի լինել մյուս օգտատերերի համար, սակայն չէր կարող նույնացնել օգտատիրոջը առանց

ինտերնետ ծառայություններ մատուցող ընկերության կողմից տվյալների նույնականացման: Եվրոպական դատարանը նաև հավելել է, որ Սահմանադրությունն ամրագրում է նամակագրության և հաղորդակցության գաղտնիությունը և պահանջում, որ ցանկացած միջամտություն հիմնված լինի դատարանի որոշման վրա: Հետևաբար, Եվրոպական դատարանի գնահատմամբ դիմումատուի՝ իր առցանց գործունեության գաղտնիության ակնկալիքը չէր կարող ոչ ողջամիտ լինել, և հետևաբար Կոնվենցիայի 8-րդ հոդվածը կիրառելի էր դրա նկատմամբ:

Անդրադառնալով ներպետական օրենսդրության համապատասխանությանը Կոնվենցիայի 8-րդ հոդվածով սահմանված պահանջներին՝ Եվրոպական դատարանը, գտնելով, որ դիմումատուի գաղտնիության շահի պաշտպանության մակարդակի առումով ներպետական օրենսդրությունը հետևողական չէր, վկայակոչել է Սահմանադրական դատարանի մեկնաբանությանը, համաձայն որի՝ հաղորդակցվողի ինքնության և փոխանցվող տվյալների (traffic data) բացահայտումը պահանջում են դատարանի որոշում: Ինչ վերաբերում է Սահմանադրական դատարանի այն դիրքորոշմանը, որ դիմումատուն հրաժարվել էր գաղտնիության ողջամիտ ակնկալիքից, քանի որ որևէ կերպ չէր թաքցրել իր IP հասցեն, որով մուտք էր գործել համացանց, Եվրոպական դատարանն այն համատեղելի չէր համարել Կոնվենցիայի իմաստով մասնավոր կյանքի գաղտնիության իրավունքի հետ: Հետևաբար, Եվրոպական դատարանը գտել էր, որ կոնկրետ դեպքում անհրաժեշտ էր դատարանի որոշում: Ինչ վերաբերում էր ներպետական մարմինների կողմից Քրեական դատավարության օրենքի համապատասխան դրույթների վկայակոչմանը, Եվրապական դատարանը դա հիմնավոր չէր համարել, քանի որ այդպիսիք վերաբերում էին էլեկտրոնային հաղորդակցության միջոցների սեփականատիրոջ կամ օգտատիրոջ մասին տեղեկությունների հայցմանը և չէին պարունակում հատուկ դրույթներ բաժանորդի տվյալների և դինամիկ IP հասցեների միջև հարաբերակցությանը: Եվրոպական դատարանի գնահատմամբ՝ ներպետական օրենքը կամայական միջամտությունից որևէ երաշխիք չէր նախատեսում, գործի

քննության ժամանակ չի եղել որևէ կարգավորում, որը կհստակեցներ Քրեական դատավարության օրենքի համաձայն ձեռք բերված տվյալների պահպանման պայմանները և կնախատեսեր որևէ երաշխիք պետական պաշտոնյաների կողմից նման տվյալների հասանելիության և փոխանցման ընթացակարգում չարաշահումների դեմ: Ավելին, Եվրոպական դատարանը փաստել է, որ ոստիկանության կողմից այս լիազորությունների օգտագործման անկախ վերահսկողություն չի եղել, չնայած այն հանգամանքին, որ այդ լիազորությունները ստիպել են ինտերնետ ծառայություն մատուցողին վերականգնել պահպանված կապի տվյալները, և ոստիկանությանը հնարավորություն են տվել ստանալ որոշակի անձի առցանց գործունեության վերաբերյալ մեծ քանակությամբ տեղեկատվություն առանց նրա համաձայնության:

Եվրոպական դատարանը անձի՝ մասնավոր կյանքի գաղտնիության իրավունքին միջամտությունը «օրենքի համապատասխան» չի գնահատել այն հիմնավորվամբ, որ ընդհանուր առմամբ, օրենքը, որի վրա հիմնված էր վիճարկվող միջոցը և ներպետական դատարանների կողմից դրա կիրառման եղանակը, բավականաչափ հստակ չի եղել և բավարար երաշխիքներ չի տրամադրել կամայական միջամտությունից[15]:

ՀՀ քրեական դատավարության օրենսգրքի 209-րդ հոդվածի 3-րդ մասի համաձայն՝

*«Բացառապես դատախազի թույլտվությամբ են կատարվում՝*

*1) սույն օրենսգրքի 232-րդ հոդվածի 3-րդ մասով սահմանված տվյալներ պարունակող տեղեկատվության պահանջը.*

*(...)»:*

Նույն օրենսգրքի232-րդ հոդվածի համաձայն՝

«*1. Տեղեկատվության պահանջը քննիչի գրավոր դիմումն է վարույթի համար նշանակություն ունեցող հանգամանքների մասին տեղեկությունների փոխանցման*

[15] Տե՛ս Information Note on the Court's case-law 217, ապրիլ 2018, հասանելի է՝ https://www.echr.coe.int/Documents/CLIN_2018_04_217_ENG.pdf

*պետական կամ տեղական ինքնակառավարման մարմիններին, իրավաբանական անձին կամ ցանկացած այլ կազմակերպությանը:*

*(…)*

*3. Հսկող դատախազի կողմից հաստատված քննիչի որոշմամբ կարող են պահանջվել նաև՝*

*1) ֆիքսված կամ բջջային հեռախոսային ցանցի միջոցով հաղորդակցվողների հեռախոսահամարները, հեռախոսահամարի բաժանորդի անհատական տվյալները.*

*2) հեռախոսային հաղորդակցությունն սկսելու պահին և դրա ընթացքում հաղորդակցվողների գտնվելու վայրը և նրանց տեղաշարժը պարզելու համար անհրաժեշտ տվյալները.*

*3) համացանցին միանալու և համացանցից դուրս գալու վայրը, ժամանակը և տևողությունը, համացանցն օգտագործողի կամ բաժանորդի անհատականացման տվյալները, հեռախոսահամարը, որով նա միանում է ընդհանուր օգտագործման հեռախոսացանցին, համացանցային հասցեն, ներառյալ ինտերնետ պրոտոկոլի (IP) հասցեն, համացանցային հեռախոսազանգն ստացողի անհատականացման տվյալները:*

*4. Սույն հոդվածի 3-րդ մասի 2-րդ կետով նախատեսված տվյալները կարող են պահանջվել՝*

*1) այն ֆիզիկական անձի նկատմամբ, որի վերաբերյալ առկա են ենթադրյալ հանցանք կատարելու մասին վկայող փաստեր.*

*2) մեղադրյալի նկատմամբ.*

*3) տուժողի կամ վկայի նկատմամբ, եթե դա անհրաժեշտ է նրա ցուցմունքը ստուգելու համար»:*

Օրենսգքրի 241-րդ հոդվածի համաձայն՝

*«1. Գաղտնի քննչական գործողություններն են՝*

*(…)*

*4) թվային, այդ թվում՝ հեռախոսային հաղորդակցության վերահսկումը.*

*(…)»::*

Օրենսգրքի 249-րդ հոդվածի համաձայն՝

*«1. Թվային, այդ թվում՝ հեռախոսային հաղորդակցության վերահսկումը հատուկ կամ այլ տեխնիկական միջոցների օգտագործմամբ՝ սույն հոդվածի 2-րդ մասով նախատեսված տվյալների գաղտնի պարզումը, հավաքումը, ամրագրումն ու պահպանումն է դրանք փիրապետող ֆիզիկական կամ իրավաբանական անձանց կողմից:*

*2. Թվային, այդ թվում՝ հեռախոսային հաղորդակցության վերահսկման ենթակա են՝*

*1) ֆիքսված կամ բջջային հեռախոսային ցանցի դեպքում՝ հեռախոսային խոսակցության, տեքստային, պատկերային, ձայնային, տեսաձայնային և այլ հաղորդագրության բովանդակությունը, բաժանորդի մուտքային և ելքային զանգերը, հեռախոսային հաղորդակցությունն սկսելու և ավարտելու ժամանակը, հեռախոսազանգի վերահասցեագրման կամ փոխանցման դեպքում այն հեռախոսահամարը, որին փոխանցվել է հեռախոսազանգը.*

*2) համացանցային հաղորդակցության, այդ թվում՝ համացանցային հեռախոսային հաղորդակցության և համացանցի միջոցով փոխանցվող էլեկտրոնային հաղորդումների դեպքում՝ հաղորդակցության բովանդակությունը, համացանցային հեռախոսազանգերի մուտքային և ելքային զանգերը:*

*3. Պահպանված գաղտնի թվային տվյալները ենթակա են անհապաղ ոչնչացման, եթե դատարանի համապատասխան որոշման կայացումից հետո՝ 90 օրվա ընթացքում, հետաքննության մարմինը դրանք չի վերցրել:*

*4. Սույն հոդվածով նախատեսված գաղտնի քննչական գործողությունն անցկացնելիս հեռահաղորդակցության կազմակերպությունները պարտավոր են իրավասու մարմինների պահանջով տրամադրել տեխնիկական համակարգեր և ստեղծել գաղտնի քննչական գործողության կատարման համար անհրաժեշտ այլ պայմաններ»:*

Օրենսգրքի՝ գաղտնի քննչական գործողության կատարման հիմքը և պայմաններն ամրագրող 242-րդ հոդվածի համաձայն՝

*«(…)*

*2.Գաղտնի քննչական գործողությունը կատարվում է քննիչի հանձնարարությամբ՝ դատարանի որոշման հիման վրա:*

*3. Գաղտնի քննչական գործողությունները կարող են կատարվել ծանր կամ առանձնապես ծանր, ինչպես նաև կաշառք ստանալու կամ կաշառք տալու ենթադրյալ հանցանքների վերաբերյալ վարույթներով»:*

*Օրենսգրքի՝ գաղտնի քննչական գործողության իրավաչափության երաշխիքներն ամրագրող* 243-րդ հոդվածի համաձայն ՝

*«(…)*

*2. Սույն օրենսգրքի 241-րդ հոդվածի 1-ին մասի 1-4-րդ կետերով նախատեսված գաղտնի քննչական գործողությունները կարող են կատարվել՝*

*1) այն ֆիզիկական անձի նկատմամբ, որի վերաբերյալ առկա են ենթադրյալ հանցանք կատարելու մասին վկայող փաստեր.*

*2) մեղադրյալի նկատմամբ.*

*3) այն ֆիզիկական անձի նկատմամբ, որի վերաբերյալ առկա է հիմնավոր ենթադրություն այն մասին, որ մեղադրյալը պարբերաբար անմիջականորեն հաղորդակցվել է կամ ողջամտորեն կարող է հաղորդակցվել նրա հետ.*

*4) այն իրավաբանական անձի նկատմամբ, որի վերաբերյալ առկա է հիմնավոր ենթադրություն այն մասին, որ դրա գործունեությունն ամբողջությամբ կամ վերաբերելի մասով կառավարվում, վերահսկվում կամ որևէ կերպ փաստացի ուղղորդվում է սույն մասի 1-ին կամ 2-րդ կետով նշված անձի կողմից:*

*(…)*

*5. Անկախ կարգավիճակից՝ նույն անձի նկատմամբ սույն օրենսգրքի 241-րդ հոդվածի 1-ին մասի 1-5-րդ կետերով նախատեսված որևէ գաղտնի քննչական գործողության կատարման ընդհանուր ժամկետը նույն վարույթով չի կարող գերազանցել տասներկու ամիսը: Ընդ որում, յուրաքանչյուր անգամ դատարանի թույլտվությունը կարող է տրվել երեք ամիսը չգերազանցող ժամկետով»:*

Օրենսգրքի 232-րդ հոդվածի 3-րդ մասի 1-ին և 2-րդ կետերի բովանդակությունից բխում է, որ բաժանորդի տվյալները, ինչպես նաև առանձին փոխանցվող տվյալներ (traffic data), այն է՝ համացանցին միանալու և համացանցից դուրս գալու վայրը, ժամանակը և տևողությունը, համցանցային հասցեն, ներառյալ ինտերնետ պրոտոկոլի (IP) հասցեն, քրեական վարույթի ընթացքում կարող են ստացվել հսկող դատախազի կողմից հաստատված քննիչի որոշմամբ:

Փոխանցվող տվյալների առնչությամբ գաղտնիության ողջամիտ ակնկալիք ունենալու իրավաչափության վերաբերյալ միջազգային իրավական պրակտիկայում առկա վերոնշյալ մոտեցումներից բխում է, որ տեղեկատվության պահանջի շրջանակում նախատեսված՝ վերոնշյալ փոխանցվող տվյալներն առնչվում են հաղորդակցության գաղտնիության իրավունքի հետ: Սակայն քրեադատավարական նորմերի վերլուծությունից բխում է, որ անկախ փոխանցվող տվյալի բովանդակությունից՝ օրենսդիրը չի նախատեսում դատարանի որոշման առկայության պահանջ:

Մյուս կողմից՝ թվային, այդ թվում՝ հեռախոսային հաղորդակցության վերահսկում գաղտնի քննչական գործողության բովանդակության, դրա կատարման հիմքերի և իրավաչության երաշխիքների վերաբերյալ մեջբերված հոդվածների վերլուծությունը հանգեցնում է նրան, որ վերահսկման ենթակա են նաև փոխանցվող այնպիսի տվյալներ, ինչպիսիք են՝ բաժանորդի մուտքային և ելքային զանգերը, , սակայն միայն ծանր կամ առանձնապես ծանր ենթադրյալ հանցանքների վերաբերյալ վարույթներով:

Վերոշարադրյալի առնչությամբ խնդիրն էլ այն է, որ փոխանցվող տվյալները (traffic data) կիբերհանցավորության, և առհասարակ հանցավորության դեմ պայքարի համատեքստում առավել հաճախ պահանջվող գործի համար նշանակություն ունեցող տվյալներն են: Սակայն դրանց ստացումը գաղտնի քննչական գործողության շրջանակում էապես բարդացնում է խնդիրը, քանի որ ելնելով այդ գործողության իրավաչափության պայմաններից՝ նշված տվյալները չեն կարող ստացվել ոչ մեծ կամ միջին ծանրության հանցանքներով:

Բացի այդ, իրավաչափ կարող է լինել այն մեկնաբանությունը, որ նշված գաղտնի քննչական գործողության կատարման ժամկետային կարգավորումներից բխում է, որ թվային, այդ թվում՝ հեռախոսային հաղորդակցության վերահսկում գաղտնի քննչական գործողությամբ ստացվող տվյալները վերաբերելի են ապագային: Այսինքն՝ այս գործողության շրջանակում ստացվող, մասնավորապես՝ բաժանորդի մուտքային և ելքային հեռախոսազանգերն ապագայում՝ դատարանի որոշումը ստանալուց հետո, ստացվելիք տվյալներ են, և չեն կարող վերաբերել անցյալում համապատասխան կապի օպերատորների կողմից քրեական վարույթի շրջանակներից դուրս հավաքագրված տվյալներին: Նման մեկնաբանության պարագայում փաստորեն ստացվում է, որ քրեական վարույթի ընթացքում օբյեկտիվորեն գոյություն ունեցող ֆիքսված կամ բջջային հեռախոսկապով կամ համացանցային եղանակով հաղորդակվցող բաժանորդների մուտքային և ելքային (զանգերիվերաբերյալ տվյալների ստացման քրեադատավարական կարգ նախատեսված չէ, քանի որ նման տվյալների ստացումը չի բխում ինչպես ՀՀ քրեական դատավարության օրենսգքրի 232-րդ հոդվածով նախատեված՝ դատախազի կողմից քննիչի հաստատված որոշման հիման վրա տեղեկատվության պահանջի քննչական գործողության, այնպես էլ Օրենսգրքի 249-րդ հոդվածով նախատեսված՝ թվային, այդ թվում՝ հեռախոսային հաղորդակցության վերահսկում գաղտնի քննչական գործողության բովանդակությունից:

Քրեադատավարական վերոնշյալ կարգավորումների՝ հանրային և մասնավոր շահի հավասարակշռման տեսանկյունից հստակ կարգավորումներ ունենալու համար անհրաժեշտ է տարանջատել բաժանորդի վերաբերյալ, փոխանցվող և բովանդակային տվյայլների ստացման դատավարական մեխանիզմները՝ նախատեսելով ոչ միայն բովանդակային, այլ նաև փոխանցվող առանձին տվյալների ստացման նկատմամբ դատական վերահսկողության կառուցակարգեր: Բացի այդ, հաշվի առնելով կիբերհանցագործությունների վերաբերյալ գործերով ոչ միայն ապագայում, այլ նաև նախկինում ունեցած մուտքային և ելքային զանգերի ստացման կարևորությունըանկախ ծանրության աստիճանից, անհրաժեշտ է

նախատեսել դատական վերահսկողության առարկա տեղեկատվության պահանջի շրջանակում դրանց ստացման հնարավորություն:

**3) Թվային խուզարկության կիրառման գործիքակազմի ընդլայնումը. դատավարական երաշխիքների հստակեցումը.**

Քրեական դատավարության օրենսգրքի՝ թվային խուզարկություն քննչական գործողություոը նախատեսող՝ 236-րդ հոդվածը չի նախատեսում խուզարկությունը Հայաստանի Հանրապետության տարածքում գտնվող համակարգչային մեկ այլ համակարգի նկատմամբ նույնպես տարածելու հնարավորությունն այն դեպքում, երբ բավարար հիմքեր կան՝ կարծելու համար, որ տեղեկությունները կարող են պահեստավորված լինել համակարգչային այդ համակարգերում, և որ տվյալների նկատմամբ հնարավոր է օրինական հասանելիություն ձեռք բերել առաջին համակարգից:

Բուդապեշտի կոնվենցիայի մասին բացատրական զեկույցի համաձայն՝ նույն կոնվենցիայի 19-րդ հոդվածը, որը վերաբերում է խուզարկությանը և առգրավմանը, թույլ է տալիս քննչական մարմիններին ընդլյանել որոնողական գործողությունները կամ ունենալ հասանելիություն մեկ այլ համակարգչային համակարգի կամ դրա մի մասին, եթե հիմքեր կան ենթադրելու, որ պահանջվող տվյալները պահպանվում են այդ մեկ այլ համակարգչային համակարգում: Ընդ որում, այլ համակարգչային համակարգը կամ դրա մի մասը պետք է գտնի վարույթն իրականացնող մարմնի երկրի տարածքում: Չնայած Բուդապեշտի կոնվենցիան չի հստակեցնում, թե խուզարկության ընդլայնումն ինչ եղանակով պետք է թույլատրվի՝ թողնելով դա ներպետական օրենսդրի հայեցողությանը, այնուամենայնիվ, իբրև հնարավոր լուծումներ՝ հիշատակվում են հետևյալ մոդելները՝

1) կոնկրետ համակարգչային համակարգը խուզարկելու թույլտվություն տված դատական կամ այլ իրավասու մարմինը լիազորված է թույլատրել խուզարկության տարածումը նաև փոխկապակացված համակրգի նկատմամբ, եթե հիմքեր կան ենթադրելու (պահպանելով ներպետական օրենսդրությամբ սահմանված ապացուցողական շեմը և մարդու իրավունքների պաշտպանության երաշխիքները),

որ փոխկապակցված համակարգում կարող են հայտնաբերվել որոնվող տվյալները.

2) քննչական մարմինը լիազորված է թույլատրել խուզարկության տարածումը նաև փոխկապակցված համակարգի նկատմամբ, եթե հիմքեր կան ենթադրելու (պահպանելով ներպետական օրենսդրությամբ սահմանված ապացուցողական շեմը և մարդու իրավունքների պաշտպանության երաշխիքները), որ փոխկապակցված համակարգում կարող են հայտնաբերվել որոնվող տվյալները.

3) խուզարկությունը երկու համակարգերում իրականացվում է արագ և համակարգված եղանակով: Բոլոր դեպքերում որոնման ենթակա տվյալները պետք է օրինական եղանակով հասանելի լինեն սկզբնական համակարգչային համակարգից[16]:

ՀՀ քրեադատավարական գործող օրենքը նման գործիքակազմի կիրառման հնարավորություն չի նախատեսում, ուստի անհրաժեշտ է Բուդապեշտի կոնվենցիայի 19-րդ հոդվածի լիարժեք իրագործմանը վերաբերող օրենսդրական կարգավորումներ մշակել և դիտարկել խուզարկության շրջանակն ընդլայնելու և Հայաստանի Հանրապետության տարածքում գտնվող մեկ այլ համակարգչային համակարգի նկատմամբ տարածելու հնարավորությունը՝ իբրև դատավարական երաշխիք նախատեսելով թվային խուզարկության ընդլայնման հիմքերի և պայմանների նախատեսումը և այդպիսիք քննիչի կողմից համապատասխան միջնորդության մեջ հիմնավորելու պահանջի նախատեսումը:

Բացի այդ, ՀՀ քրեական դատավարության գործող օրենսգրքով հստակ օրենսդրական կարգավորում չունի այն հարցը, թե արդյոք ի սկզբանե դատարանի որոշմամբ իրականացված, օրինակ, բնակարանի խուզարկության արդյունքում հայտնաբերված էլեկտրոնային սարքերի կամ կրիչների թվային խուզարկությունը կարող է իրականացվել առանց խուզարկություն կատարելու մասին վարույթն իրականացնող մարմնի միջնորդությունը բավարարելու և միջնորդվող

[16] Տե՛ս «Կիբերհանցագործությունների մասին» Բուդապեշտի կոնվենցիայի՝ Եվրոպայի խորհրդի նախարարների կոմիտեի մշակած բացատրական զեկույց, հասանելի է հետևյալ հղմամբ՝ https://rm.coe.int/16800cce5b:

ապացուցողական գործողության կատարումը թույլատրելու մասին դատարանի որոշման: Հաշվի առնելով, որ չնայած թե՛ բնակարանի խուզարկությունը, թե՛ էլեկտրոնային սարքերի թվային խուզարկությունը դատարանի որոշմամբ կատարվող քննչական գործողություններ են, սակայն դրանք ինքնուրույն բովանդակություն ունեցող առանձին դատավարական գործիքներ են, և դատարանի որոշումը կոնկրետ խուզարկության յուրաքանչյուր կոնկրետ դեպքում կոչված է ուրվագծելու նաև խուզարկության սահմանները, որն իր հերթին անձի սահմանադրական իրավունքի համաչափ սահմանափակման դատավարական երաշխիք է: Ուստի անհրաժեշտ է թվային խուզարկություն կատարելու մասին վարույթն իրականացնող մարմնի միջնորդությունը բավարարելու և միջնորդվող ապացուցողական գործողության կատարումը թույլատրելու մասին դատարանի առանձին որոշում ստանալու պահանջ նախատեսել այն դեպքերում, երբ բնակարանի խուզարկության արդյունքում հայտնաբերվել են էլեկտրոնային սարքեր կամ կրիչներ, եթե դրանց ստացումը նախատեսված չէր տվյալ գործողության կատարումը թույլատրելու մասին որոշմամբ կամ ողջամտորեն չէր ակնկալվում:

**4) Հաղորդակցության ծառայություններ մատուցողների տեխնիկական կարողությունների ընդլայնում և լանորեն օգտագործում**

Կիբերհանցագործությունների դեմ պայքարի դատավարական գործիքակազմերի ընդլայնումը ենթադրում է նաև հաղորդակցության ծառայությունների մատուցողների տեխնիկական կարողությունների շարունակական բարելավում: Թեպետ ՀՀ քրեական դատավարության օրենսգրքով նախատեսվում է, որ գաղտնի քննչական գործողությունն անցկացնելիս հեռահաղորդակցության կազմակերպությունները պարտավոր են իրավասու մարմինների պահանջով տրամադրել տեխնիկական համակարգեր և ստեղծել գաղտնի քննչական գործողության կատարման համար անհրաժեշտ այլ պայմաններ (249-րդ հոդվածի 4-րդ մաս), այդուհանդերձ, նույնաբովանդակ նորմը բացակայում է համապատասխան տեղեկատվության պահանջի քննչական գործողության վերաբերյալ քրեադատավարական կարգավորումներում, չնայած որ շատ դեպքերում նշված

գործողության արդյունավետ կատարումը մեծապես կախված է հեռահաղորդակցության կազմակերպությունների կողմից համապատասխան տեխնիկական աջակցության տրամադրումից:

**5) Կրիպտոակտիվների իրավական կարգավորման հիմքերի ներմուծում.**

Կրիպտոաակտիվների վերաբերյալ տարբեր երկրների որդեգրած մոտեցումների ընդհանրացումը թույլ է տալիս նշել, որ դրանք հանգում են նման արժույթների գործածության արգելքի կամ թույլտվության: Ընդ որում, վերջին մոտեցումը որդեգրած երկրները իրենց քաղաքականությունը իրականացնում են տարբեր մեթոդներով: Մասնավորապես, դրանց մի մասը օրենսդրական կարգավորման են ենթարկել կրիպտոաակտիվների հետ կապված իրավահարաբերությունները, որը, ի թիվս այլնի, ներառում է կարգավորումներ կրիպտոակտիվի՝

1) արժույթ կամ այլ գույք հանդիսանալու վերաբերյալ.

2)վաճառք իրականացնողների լիցենզավորմանն վերաբերյալ.

3)հարկմանն վերաբերյալ:

Ի տարբերություն նշվածի՝ որոշ երկրներ կրիպտոակտիվների առնչությամբ չունեն որոշակի օրենսդրական կանոնակարգումներ: Այլ կերպ ասած՝ նրանք, ընդունելով նման արժույթների գոյության և շրջանառության փաստը, լռելյայն, արգելքի չսահմանմամբ թույլատրել են դա:

Հայաստանի Հանրապետությունում առկա իրավիճակը առավել մոտ է վերջին դեպքին, քանի որ մի շարք օրենսդրական ակտերում, օրինակ՝ «Ապօրինի ծագում ունեցող գույքի բռնագանձման մասին» ՀՀ օրենքում, ՀՀ կառավարության՝ 2020 թվականի հունվարի 30-ի՝ N 102-Ն որոշմամբ և այլն, այս կամ այն կերպ առկա է անդրադարձ կրիպտոարժույթներին:

Այուամենայնիվ, ներկայումս հստակ չէ կրիպոակտիվի բնույթի, շրջանառության, կոռուպցիայի կանխարգելման նպատակով դրանց պատկանելության ստուգման և մի շարք այլ հարցերի հետ կապված լուծումները: Եվ

դա այն դեպքում, երբ կրիպտոարժույթների հափշտակության դեպքերում Հայաստանում իրականացվում է քրեական հետապնդում:

Շարադրվածը վկայում է Հայաստանի Հանրապետության քրեական դատավարության օրենսգրքում և այլ օրենքներում փոփոխություններ և լրացումներ կատարելու անհրաժեշտության մասին:

**2. Կապը ռազմավարական փաստաթղթերի հետ.**

Նախագծի ընդունումը չի բխում ռազմավարական փաստաթղթերից:

**3. Առաջարկվող կարգավորման բնույթը**

«Հայաստանի Հանրապետության քրեական օրենսգրքում լրացում կատարելու մասին», «Հայաստանի Հանրապետության քրեական դատավարության օրենսգրքում լրացումներ և փոփոխություններ կատարելու մասին», «Հայաստանի հանրապետության քաղաքացիական օրենսգրքում լրացում կատարելու մասին», ««Անկանխիկ գործառնությունների մասին» Հայաստանի Հանրապետության օրենքում լրացում կատարելու մասին» և մյուս օրենքների նախագծերով կարգավորվել են հետևյալ հարցերը.

1) ՀՀ քրեական օրենսգրքում հստակեցվել է կիբերհանցագործությունների շրջանակը.

2) տարանջատվել են բաժանորդի, փոխանցվող և բովանդակային տվյալները, հստակ սահմանվել է դրանց շրջանակը.

3) սահմանվել է նախնական դատական վերահսկողության այնպիսի տվյալների վերաբերյալ տեղեկատվության պահանջի քննչական գործողության նկատմամբ, ինչպիսիք են՝ ֆիքսված կամ բջջային հեռախոսային ցանցի դեպքում՝ բաժանորդի մուտքային և ելքային զանգերը, համացանցային հաղորդակցության, այդ թվում՝ համացանցային հեռախոսային հաղորդակցության և համացանցի միջոցով փոխանցվող էլեկտրոնային հաղորդումների դեպքում՝ համացանցային հեռախոսազանգերի մուտքային և ելքային զանգերը, համացանցին միանալու և

համացանցից դուրս գալու վայրը, ժամանակը, տևողությունը, տեղաշարժը, համացանցային հասցեն, ներառյալ ինտերնետ պրտոկոլի (IP) հասցեն պարզելու համար անհրաժեշտ տվյալները,

4) նախատեսվել է դատարանի որոշմամբ կատարվող տեղեկատվության պահանջ քննչական գործողության միջոցով նաև մուտքային և ելքային զանգերը ստանալու հնարավորություն.

5) նախատեսվել է բացի խուզարկության որոշման մեջ նշվածից, թվային խուզարկությունը նաև Հայաստանի Հանրապետության տարածքում գտնվող համակարգչային մեկ այլ համակարգի նկատմամբ տարածելու հնարավորություն, երբ լուրջ հիմքեր կան ենթադրելու, որ վարույթի համար նշանակություն ունեցող տվյալներ կարող են պահեստավորված լինել համակարգչային այդ համակարգերում, որ այդ տվյալների նկատմամբ հասանելիություն հնարավոր է ձեռք բերել սկզնական համակարգչային համակարգից, և որ հապաղումը կարող է հանգեցնել ապացույցի վարույթի համար նշանակություն ունեցող տվյալների կորստի կամ ոչնչացման՝ սահմանելով նշված գործողության կատարման հիմքերն ու պայմանները համապատասխան միջնորդության մեջ հիմնավորելու պահանջ պահանջ.

6) նախատեսվել է բնակարանի խուզարկության արդյունքում ստացված էլեկտրոնային սարքերի և կրիչների համար թվային խուզարկություն իրականացնելու համար վարույթն իրականացնող մարմնի կողմից նոր միջնորդություն ներկայացնելու և միջնորդվող ապացուցողական գործողության կատարումը թույլատրելու մասին դատարանի առանձին որոշում ստանալու պահանջ, եթե դրանց ստացումը նախատեսված չէր տվյալ գործողության կատարումը թույլատրելու մասին որոշմամբ կամ ողջամտորեն չէր ակնկալվում.

7) նախատեսվել են կրիպտոակտիվի բնույթին և ձեռբերմանն առնչվող որոշ կարգավորումներ՝ ապահովելով այդ կապակցությամբ անհրաժեշտ հետագծելիություն, ինչպես նաև այլ օրենքներում «կրիպտոարժույթ» բառը փոխարինվել է ավելի ընդգրկուն «կրիպտոակտիվ» հասկացությամբ:

**4. <u>Նախագծի մշակման գործընթացում ներգրավված ինստիտուտները, անձինք և նրանց դիրքորոշումը.</u>**

Նախագծերը մշակվել են ՀՀ Ներքին գործերի նախարարության կողմից Զարգացման իրավունքի միջազգային կազմակերպության (IDLO) աջակցությամբ՝ ԱՄՆ Դեսպանատան Թմրամիջոցների դեմ պայքարի և իրավապահ համագործակցության գրասենյակի (INL) ֆինանսավորմամբ, ՀՀ կենտրոնական բանկի հետ համագործակցությամբ::

**5. <u>Ակնկալվող արդյունքը.</u>**

Առաջարկվող կարգավորմումը կոչված է ապահովելու կիբերհանցավորության դեմ պայքարի համատեքստում արդյունավետ օրենսդրական հիմքերի ձևավորումը՝ միջազգային իրավական պահանջներին համահունչ և գործնականում առկա խնդիրների հաշվառմամբ ձևավորելով անհրաժեշտ նյութական հիմքեր և դատավարական գործիկազմ:

***ՀՀ ներքին գործերի նախարարություն***