ПРАВО

Անձնական տվյալների պաշտպանության ամերիկյան մոդելի առանձնահատկությունները

Մինասյան Լ. Ս.

ՀՀ վարչապետի աշխատակազմի տեսչական մարմինների աշխատանքների համակարգման գրասենյակ: Շուկայի վերահսկողության և սննդամթերքի անվտանգության ոլորտների համակարգման և մեթոդաբանության վարչության խորհրդական (Երևան, Հայաստան)

lusineminasyansimon@gmail.com

Հանգուցաբառեր՝ անձնական տվյալներ, անձնական տվյալների պաշտպանության իրավունք, ամերիկան մոդել, անձնական տվյալների պաշտպանության առանձնահատկություններ

Особенности американской модели защиты персональных данных

Минасян Л. С.

Офис по координации инспекционных органов Аппарата премьер-министра РА Советник Департамента по координации и методологии сфер безопасности пищевых продуктов и надзора за рынком (Ереван, Армения)

lusineminasyansimon@gmail.com

Аннотация. Статья посвящена особенностям американской модели института защиты персональных данных. В ходе исследования были проанализированы важнейшие акты американского законодательства, которые обобщают право на защиту персональных данных. В то же время, в ходе исследования автор сделал важнейшие выводы и выявил те преимущества и недостатки, которыми американская модель защиты данных отличается от широко распространенной европейской модели.

Ключевые слова: личные данные, право на защиту персональных данных, американская модель, особенности защиты персональных данных

The characteristics of the american model of personal data protection

Minasyan L. S.

Inspection Bodies' Coordination Bureau of the Office of the Prime Minister of the Republic of Armenia Adviser of the Department of Coordination and Methodology of the Market Surveillance and Food Safety spheres (Yerevan, Armenia)

lusineminasyansimon@gmail.com

Abstract. The article is about the characteristics of the American model of personal data protection regulations. In the course of the study, the most important acts of American legislation about the right to personal data protection were meticulously analyzed.

At the same time, in this study, the author made a comprehensive legal conclusion about advantages and disadvantages of the American model of data protection and the unique approach that differs this model from more widespread European one.

Keywords: personal data, the right to personal data protection, the American model, characteristics of data protection

Այսօր, անձնական տվյալների պաշտպանության մասին իրավական ակտեր ընդունվել են աշխարհի ավելի քան 100 երկրներում, որոնցից 27-ը ԵՄ երկրներ են, իսկ 23-ը՝ Եվրոպայի Խորհրդի անդամ պետություններ: Այսպիսով ստացվում է, որ անձնական տվյալների պաշտպանության մասին օրենսդրություն ունեցող երկրների կեսը գտնվում են Եվրոպական մայրցամաքի վրա: Եվրոպայից դուրս կան մի քանի երկրներ, որոնք ևս զբաղվում են մադու հիմնական իրավունքների պաշտպանության հարցերով անձնական տվյալների մշակման շրջանակներում, որոնց մեծ մասը Տնտեսական համագործակցության և զարգացման կազմակերպության անդամ են հանդիսանում (Ավստրալիա, Կանադա, Ճապոնիա, Հարավային Կորեա, Նոր Զելանդիա, ԱՄՆ): Այս երկրներից շատերը կարողացել են հասնել ԵՄ անձնական տվյալների պաշտպանության մակարդակին: Մասնավորապես, Եվրոպայի կոմիտեն նշել է 12 պետություններ, որոնք ԵՄ անդամ չեն, բայց ունեն տվյալների պաշտպանության բավարար մակարդակ՝ Անդորրա, Արգենտինա, Կանադա, Շվեցարիա, Ֆարերյան կղզիներ, Հերնսի, Իզրաել, Մեն, Ջերսի, Նոր Զելանդիա, ԱՄՆ, Ուրուգվայ [**5**]: Մյուս երկրների դեպքում տվյալների անդրսահմանային փոխանցումների ժամանակ

անհրաժեշտ է տվյալների պաշտպանության համապատասխան մակարդակ ապահովել, որպես կանոն՝ համապատասխան համաձայնագիր կնքելու միջոցով:

Վերլուծելով օտարերկրյա և միջազգային պրակտիկան կարելի է պայմանականորեն ընդգծել անձնական տվյալների իրավական կարգավորման երկու հիմնական մոդել՝ եվրոպական և ամերիկյան: Այնուհանդերձ, հարկ է նշել, որ աշխարհում ավելի լայն տարածում է ստացել եվրոպական մոդելը, որը, ներկայիս դրությամբ, ներդրել են Եվրոպական մայրցամաքի աշխարհի 50 պետություններ, ինչպես նաև Կանադան, Արգենտինան, Ավստրալիան, Նոր Զելանդիան, Հարավային Կորեան, Բուրկինա Ֆասոն:

Ամերիկյան մոդելը ավելի քիչ տարածում է գտել և ներկայումս բացի ԱՄՆ-ից, անձնական տվյալների պաշտպանության նման կարգավորում առկա է Ճապոնիայում, Պարագվայում, Թայվանում և Թայլանդում [**2**, էջ 866–894]:

ԱՄՆ-ի անձնական տվյալների պաշտպանության մեխանիզմը այնքան է տարբերվում եվրոպական պետությունների մեծ մասում գործող մեխանիզմներից, որ կարելի է խոսել անձնական տվյալների իրավական կարգավորման բոլորովին նոր մոտեցման մասին: ԱՄՆ-ն վաղուց հայտնի է որպես պետություն, որտեղ մասնավոր կյանքի հարգանքի իրավունքը մեծ տարածում է ստացել: Պատահական չէ, որ «մասնավոր կյանք» և «մասնավոր կյանքի իրավունք» հասկացությունները շրջանառության մեջ են դրվել առաջին անգամ ամերիկյան իրավաբանների կողմից:

Սակայն, տվյալների պաշտպանության քաղաքականությունը ԱՄՆ-ում միշտ ձևավորվել է ազգային անվտանգության ավանդական մտահոգությունների լույսի ներքո, նույնիսկ երբ նման քաղաքականությունը և դրան ուղղված իրավական ակտերի ընդունումը ուղղակի բացասական ազդեցություն են ունեցել մասնավոր ոլորտում կազմակերպությունների շահույթի վրա[1] [**4**]:

Այսօր, անձնական տվյալների պաշտպանության գլխավոր երաշխիքը ԱՄՆ-ում, բացի Սահմանադրության 4-րդ փոփոխությունից հանդիսանում է 1974 թվականին ընդունված «Մասնավոր կյանքի պաշտպանության Ակտն է [**23**] (այսուհետ՝ Պաշտպանության ակտ): Այս փաստաթուղթն ինքնին հետազոտության համար բավականին հետաքրքիր նմուշ է, որն ամբողջովին բնութագրում է անձնական տեղեկատվության իրավակարգավորման յուրահատուկ ամերիկյան մոտեցումը:

Այսպիսով, վերլուծելով Պաշտպանության ակտը, կարելի է եզրակացնել, որ վերջինիս ազդեցության ոլորտը բավականին սահմանափակ է: Այն անձնական տվյալների պաշտպանության իրավունք, այդ թվում՝ դատական պաշտպանության իրավունք տրամադրում է միայն ԱՄՆ քաղաքացիներին և մշտական ռեզիդենտներին, իսկ պարտավորություններ սահմանում է միայն դաշնային պետական մարմինների համար, ինչպիսին են ԱՄՆ փոստային ծառայությունը, Կրթության դեպարտամենտը, Դաշնային հետաքննությունների բյուրոն և այլն: Արդյունքում, քաղաքացի չհանդիսացող անձանց իրավունքների պաշտպանությունն ու մասնավոր ոլորտի շահագրգիռ անձանց պարտավորությունները մնում են կարգավորումից դուրս:

Պաշտպանության ակտում ևս մեկ սահմանափակում է հանդիսանում «գրառումների /ֆայլերի համակարգ» հասկացության օգտագործումը, որը նշանակում էր գրառումների/ֆայլերի ցանկացած համակցություն, որտեղ անձի մասին տեղեկատվությունը կարելի է ստանալ իր անվան կամ անձնական նույնականացնող ցուցիչի միջոցով, ինչը բացառում է օրենքի կիրառումը այն տվյալների բազաների նկատմամբ, որոնք մուտքագրման այլ ձև ունեն, բայց ևս կարող են պարունակել անձնական տվյալներ:

Այնուհանդերձ, Պաշտպանության ակտի համաձայն՝ տվյալներ մշակողների, այսինքն դաշնային մարմինների հիմնական պարտականությունը անձնական տվյալների գաղտնիության պահպանումն է՝ երրորդ անձանց փոխանցելու արգելքը, բացառությամբ օրենքով նախատեսված 12 իրավիճակների, որոնք են՝

- Տվյալների տրամադրումը դրանց մշակումն իրականացնող պետական մարմնի ծառայողին՝ ծառայողական պարտականությունների իրականացման համար,
- Տվյալների տրամադրումը Տեղեկատվության ազատության ակտի [**21**] համաձայն,
- Տվյալների տրամադրումը «առօրեա օգտագործման» (routine use) համար
- Տվյալների տրամադրումը ԱՄՆ մարդահամարի բյուրոյին՝ մարդահամար իրականացնելու համար,
- Տվյալների տրամադրումը ըստ նախապես հասցեագրված դիմումի՝ վիճակագրական ուսումնասիրություններ կատարելու համար՝ պայմանով, որ կտրամադրվեն միայն ապանձնավորված տվյալներ,
- Տվյալների տրամադրումը ազգային արխիվների քարտուղարությանը՝ պատմական արժեք ունեցող գրառումների համար,

[1] Տեղեկատվական և կաբելային ընկերությունների ճնշման տակ, օրինակ, Կոնգրեսը 2017թ. փոփոխեց անձնական տվյալների իրավակարգավորումները

- Տվյալների տրամադրումը քաղաքացիական և քրեական արդարադատության իրականացման համար,
- Տվյալների տրամադրումը անձի կյանքի և առողջության պաշտպանության համար՝ պայմանով, որ դրա մասին կտեղեկացվի տվյալների սուբյեկտը,
- Տվյալների տրամադրումը Կոնգրեսին կամ դրա կոմիտեներին կամ ենթակոմիտեներին,
- Տվյալների տրամադրումը Գլխավոր աուդիտորին՝ [**16**] Գլխավոր հաշվիչ կոմիտեի գործառույթները իրականացնելու համար,
- Տվյալների տրամադրումը դատական որոշման համաձայն,
- Տվյալների տրամադրումը ի կատարումն օրենքի պահանջների:

Մի շարք հեղինակների կարծիքով նշված 12 բացառություններից ամենից մտահոգիչը դա «առօրեա օգտագործման համար» անձնական տվյալների մշակումն է, որը հաճախ բավականին լայն է մեկնաբանվում պետական մարմինների կողմից և հնարավոր չարաշահումների տեղիք է տալիս [**1**, էջ 49-50]:

Պաշտպանության ակտով նախատեսված է անձի իրավունքների պաշտպանության և՛ քաղաքացիական և՛ քրեական պատասխանատվություն: Մասնավորապես, քաղաքացիական պատասխանատվություն է նախատեսված անձնական տվյալների չլիազորված փոփոխության կամ անձնական տվյալները օգտագործելու մուտքի իրավունքի համար:

Իսկ քրեական պատասխանատվություն է նախատեսված դիտավորությամբ անձնական տվյալներ տարածելու, անձնական տվյալներով բազաների ստեղծման մասին չտեղեկացնելու, կեղծ հիմքերով անձնական տվյալների մասին հարցում անելու և այլնի համար:

Ընդհանուր առմամբ, վերլուծելով Պաշտպանության ակտը, ակնհայտ է, որ այն անձի իրավունքների պաշտպանության ոչ բավարար երաշխիքներ է նախատեսում, քանի որ կանոնակարգում է միայն պետական մարմինների կողմից անձնական տվյալների մշակման հիմնախնդիրները:

Սակայն, դա չի նշանակում, որ ԱՄՆ-ում բացակայում են այնպիսի նորմեր, որոնք կարգավորում են տնտեսության մասնավոր սեկտորում անձնական տվյալների պաշտպանության խնդիրները: Սա տվյալների մշակման ամերիկյան մոդելի ևս մեկ առանձնահատկությունն է: Բանն այն է, որ այստեղ ԱՄՆ-ն որդեգրել է այսպես կոչված անձնական տվյալների մշակման իրավական կարգավորումների ճյուղային մոտեցումը, իսկ որոշ հեղինակներ դա անվանում են ad hoc մոտեցում [**3**, էջ 128]: ԱՄՆ-ում անձնական տվյալների պաշտպանության առավել «կարգավորված» ոլորտներն են՝ ֆինանսական ոլորտը [**24**], բժշկական ծառայությունները [**22**], վարկավորման ծառայությունները [**19**], վիդեովարձույթի ծառայությունները [**26**], կաբելային հեռուստատեսությունը [**14**], մինչև 13 տարեկան երեխաների անձնական կյանքի պաշտպանությունը օնլայն տիրույթի ոլորտը [**15**], կրթական ծառայությունները [**20**], տրանսպորտային միջոցների գրանցման ոլորտը [**17**] և հեռախոսային վաճառքների ոլորտը [**25**]:

Ամերիկյան մոդելի մյուս առանձնահատուկը մասնավոր ոլորտում մարդու անձնական տվյալների պաշտպանության՝ հիմնականում ի օգուտ օգտատերերի և հաճախորդների իրականացնելու օրենսդրությունն ու պրակտիկան են: Պատահական չէ, որ «անձնական տվյալների սուբյեկտ» կամ «անձ» հասկացությունների փոխարեն ԱՄՆ օրենսդիրը գրեթե բոլոր իրավական ակտերում օգտագործում է «օգտատեր» (consumer) հասկացությունը: Որպես վառ օրինակ օրինակ կարող է ծառայել Ֆինանսական ոլորտում անձնական տիրույթի ակտը [**24**] կամ Էլեկտրոնային հաղորդակցությունների անձնական տիրույթի պաշտպանության ակտը [**18**], որտեղ որպես շահառու հանդիսանում է «օգտատերը»:

Ամերիկյան մոդելի հաջորդ առանձնահատկությունը դա անձնական տվյալների պաշտպանության վերահսկողություն իրականացնող մարմինների բազմազանությունն է: Պատահական չէ, որ Տնտեսական համագործակցության և զարգացման կազմակերպության հաշվետվություններից մեկի մեջ, ԱՄՆ-ն որպես անձնական տվյալների ոլորտում օրենսդրության կենսագործման պատասխանատու վերահսկող մարմին միանգամից նշել էր չորսը՝

- Արդարադատության դեպարտամենտ՝ արդարադատության իրականացման ոլորտում,
- Առողջապահության և սոցիալական պաշտպանության դեպարտամենտ՝ առողջապահության և սոցիալական պաշտպանության ոլորտում,
- Դաշնային բանկային գործակալություն՝ բանկային և ֆինանսական ոլորտում,
- Դաշնային առևտրական կոմիտե՝ առևտրի ոլորտում:

Ընդ որում, այս թվարկումը չի կարելի համարել սպառիչ ՝ քանի որ ամեն ոլորտի համար առանձնահատուկ իրավական կարգավորումներ կամ վերահսկող մարմիններ են նախատեսված: Ավելին, յուրաքանչյուր նահանգ իրավասու է ընդունելու տվյալների մշակման հավելյալ օրենքներ, ինչպես նաև ձևավորել ոլորտը վերահսկող առանձին մարմիններ [**13**, էջ 13-14]:

ԱՄՆ մասնավոր կյանքի և անձնական տվյալների պաշտպանության իրավական կարգավորման հարցում մեծ դերակատարում ունեն նաև Գերագույն Դատարանի որոշումները,

որոնք հիմնված են Սահմանադրության 4-րդ փոփոխության մեկնաբանությունների վրա: Նման որոշումները շատ են և պարբերաբար նոր մեկնաբանությունների տեղիք են տալիս: Օրինակ՝ մեկ գործով Գերագույն Դատարանը տրանսպորտային միջոցների սեփականատերերի տվյալները ճանաչեց առևտրային բնույթի և օրինական համարեց դաշնային կառավարության կողմից դրանց մշակումը [**12**, 141]: Մեկ այլ գործով սովորողների վարկանիշի ցուցադրումը և բարձրաձայն հրապարակումը Գերագույն Դատարանը չհամարեց Ընտանեկան, կրթական իրավունքների և մասնավոր կյանքի ակտի և Սահմանադրության 4-րդ փոփոխության դրույթների խախտում [**10,** 426]:

Այնուամենայնիվ, ԱՄՆ-ում շատ հարցեր թողնվում են «ինքնակարգավորման», այսինքն կարգավորվում են կորպորատիվ նորմերի մակարդակում և շուկայի նպատակահարմարությունից ելնելով [**3**, էջ 131], ինչն իր հերթին ազդում է տվյալների պաշտպանության որակի և երաշխիքների վրա: Սակայն, այսօր պետական և տեղական ինքնակառավարման մարմինները ընդունում են օրենքներ, որոնք պարտավորեցնում եմ պարտադիր ծանուցել օգտատերերին անձնական տեղեկատվություն պարունակող բազաների հակերային հարձակումների մասին [**6, 9**]:

Հարկ է նաև առանձնահատուկ նշել մասնավոր կյանքին վերաբերող օրենսդրական փոփոխությունները, որոնք կատարվեցին 2001 թվականի սեպտեմբերի 11-ի տխրահռչակ իրադարձություններից հետո: Արդյունքում ԱՄՆ կոնգրեսը ընդունեց «2001 թվականի Հայրենասիրական Ակտը», որով անհամեմատ ընդլայնվեցին հատուկ ծառայությունների, իրավապահ և իրավակիրառ մարմինների իրավասությունները [**28**]: Նշված ակտը հնարավորություն տվեց հատուկ ծառայություններին օգտագործել այնպիսի հատուկ տեխնիկական միջոցներ, որով հնարավոր կլիներ տվյալների մասսայական հավաքագրումը, ինչպես նաև այնպիսի գործողությունների իրականացումը, որի համար նախկինում դատարանի թույլտվությունն էր անհրաժեշտ, այն էլ էական իրավական հիմքերի առկայության դեպքում (անձը կասկածվում էր ծանր հանցագործություններ կատարելու մեջ, հիմնավոր կասկած կար ստանալու կատարված կամ կատարվելիք հանցագործության վերաբերյալ տեղեկատվություն և այլն): Այս փաստաթուղթն էր, որ դարձավ 2013 թվականին Էդվարդ Սնոուդենի սկանդալային բացահայտումների իրավական հիմքը, այն մասի, որ ԱՄՆ գաղտնի ծառայությունները ԱՄՆ ամենամեծ տեղեկատվական և տեխնոլոգիական ընկերությունների օգնությամբ վերահսկողություն էին իրականացնում այլ պետությունների առաջնորդների անձնական բջջային հեռախոսներով կարգավորվող գործողությունների նկատմամբ, ինչպես նաև կարող էին օպերատիվ հետախուզական տարբեր գործողություններ իրականացնել ԱՄՆ յուրաքանչյուր քաղաքացու նկատմամբ[2] [**8**]: Այս իրադարձություններից հետո այն ժամանակ նախագահ Օբաման հայտարարեց, որ ԱՄՆ կառավարությունը հատուկ պաշտպանության մեխանիզմներ կնախատեսի օտարերկրացիների համար [**11, 27**] և համապատասխան վարչական հրաման ստորագրեց Սպիտակ տունը լքելուց առաջ: Իրավիճակը փոխվեց Տրամպի նախագահության ժամանակ, ով հայտարարել էր, որ ահաբեկչական գործողությունների վերահսկումը պետք է գերակայի ցանկացած այլ նկատառումներ [**7**]:

Ամփոփելով, կարելի է եզրակացնել, որ Ամերիկյան մոդելի համար ՝ հիմնական բնութագրիչ հատկանիշներն են՝

- «անձնական տիրույթ» (privacy) հասկացության օգտագործումը և՛ մասնավոր և՛ հանրային ոլորտում, որով սահմանափակվում է պետության և պետական մարմինների միջամտությունը մարդու անձնական կյանքին,
- մարդու անձնական տվյալների պաշտպանության իրավունքի խնդիրների իրավական կարգավորման ճյուղային մոտեցումը, որտեղ օրենսդրական մակարդակում ամենից կարգավորված ոլորտը հանդիսանում է «հանրային ոլորտը»,
- և՛ մասնավոր և՛ հանրային ոլորտների համար անձնական տվյալների պաշտպանության միասնական սկզբունքներ ամրագրող մեկ միասնական իրավական ակտի բացակայություն,
- տնտեսության մասնավոր ոլորտում անձնական տվյալների պաշտպանության օրենսդրության կարգավորման շուկայական մեխանիզմների գերակայումը, ինչի արդյունքում մասնավոր ընկերությունների կողմից անձնական տվյալների մշակման խնդիրները դիտարկվում են «բարեխիղճ մրցակցության» և «օգտատերերի իրավունքների պաշտպանության» տեսանկյունից,
- անձնական տվյալների պաշտպանության ոլորտում վերահսկողություն իրականացնող մեկ միասնական պատասխանատու մարմնի բացակայություն:

Այս մոդելի թերություններն ակնհայտ են: Նման իրավակարգավորումների պայմաններում մասնավոր ոլորտում անձնական տվյալների

[2] Նույնիսկ տարիներ անց գերմանական օրենսդիրները քննության էին ենթարկում ԱՄՆ կողմից Գերմանիան վերահսկելու գործողությունները՝ որպես վկա կանչելով Անգելա Մերկելին, ով ցուցմունքի մեջ նշել էր «Ընկերների միջև լրտեսությունը անընդունել է»:

պաշտպանությունը իրականացվում է շուկայական հարաբորությունների կարգավորման մեխանիզմների կիրառմամբ, ինչը տվյալների սուբյեկտի իրավունքների պաշտպանության բավարար երաշխիքներ չի սահմանում: Նման պայմաններում օրինակ, տվյալների սուբյեկտը չի կարող պահանջել իր անձնական տվյալների օգտագործման վերաբերյալ տեղեկատվության տրամադրում, եթե նման պարտավորությունը բացակայում է մասնավոր կազմակերպությունների համար:

Ի հակադրումն այս թերությունների՝ ամերիկյան մոդելի առավելությունը այն է, որ ապահովում է տվյալների սուբյեկտի իրավունքների պաշտպանության պետության «հատուկ, հասցեական» մոտեցումը՝ արդյունքում հաշվի առնելով տնտեսության կամ պետական կառավարման յուրաքանչյուր ճյուղի առանձնահատկությունները:

Օգտագործված գրականության ցանկ

1. **Коровяковский, Д. Г.** Российский и зарубежный опыт в области защиты персональных данных / Д. Г. Коровяковский // Национальные интересы: приоритеты и безопасность. – 2009. – No 5.
2. **Параскевов, А. В.** Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом / А.В. Параскевов, А. В. Левченко, Ю. А. Кухоль // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГУ, 2015. – No 110. http://ej.kubagro.ru/2015/06/pdf/58.pdf (վերջին այցելություն՝ 08.06.2021)
3. **Burkert, H., Lerouge, J-F., Pichault, F., Poulin, D., Raab, C., Reidenberg, J., ... Poullet, Y.** (2002). Variations sur le droit de la société de l'information. (Cahiers du Centre de Recherches Informatique et Droit; Vol. 20). Bruxelles: Académia Bruylant
4. **Byers, A.** (2017), 'House votes to revoke broadband privacy rules', Politico, 28 March 2017, www.politico.com/story/2017/03/house-votes-to-revoke-broadband-privacy-rules-236607 (վերջին այցելություն՝ 08.06.2021)
5. Commission decisions on the adequacy of the protection of personal data in third countries. – (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en) (վերջին այցելություն՝ 08.06.2021)
6. **Davis Wright Tremaine LLP** (2016), 'Data Breach Notification Summary', https://www.dwt.com/files/Uploads/Documents/Publications/State%20Statutes/BreachNoticeSummaries.pdf ; (վերջին այցելություն՝ 08.06.2021)
7. Kaveh Waddell's interview with Susan Hennessey, managing editor of Lawfare, at Waddell, K. (2017), 'Why is Obama Expanding Surveillance Powers Right Before He Leaves Office', *The Atlantic*, 13 January 2017, www.theatlantic.com/technology/archive/2017/01/obama-expanding-nsa-powers/513041/. (վերջին այցելություն՝ 08.06.2021)
8. **Moulson, G.** (2017), 'Germany's Merkel testifies on alleged US eavesdropping', Associated Press, 16 February 2017, https://apnews.com/e384920d20d44f038d3f6a80a36b244f. (վերջին այցելություն՝ 08.06.2021)
9. National Conference of State Legislatures (2017), 'Security Breach Notification Laws', www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. (վերջին այցելություն՝ 08.06.2021)
10. Owasso Independent School District v. Falvo, 534 U.S. 426 (2001). – (https://supreme.justia.com/cases/federal /us/534/426/case.html) (վերջին այցելություն՝ 08.06.2021)
11. Presidential Policy Directive 28 at The White House (2014), 'Presidential Policy Directive – Signals Intelligence Activities', Office of the Press Secretary, 17 January 2017, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities; (վերջին այցելություն՝ 08.06.2021)
12. **Reno v. Condon**, 528 U.S. 141 (2000). – (https://supreme.justia.com/cases/federal/us/528/141/case.html) (վերջին այցելություն՝ 08.06.2021)
13. Report on the Cross-Boarder Enforcement of the Privacy Laws / OECD. – 2006
14. The Cable Communications Policy Act of 1984 (Pub. L. No. 98-549 (1984)). – (https://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1286.pdf) (վերջին այցելություն՝ 08.06.2021)
15. The Children's Online Privacy Protection Act of 1998 (COPPA) (Pub. L. No. 105-277 (1998)). – (https://epic.org/privacy/kids/#Act) (վերջին այցելություն՝ 08.06.2021)
16. The Comptroller General of the United States. – (http://www.gao.gov/cghome/index.html). (վերջին այցելություն՝ 08.06.2021)
17. The Driver's Privacy Protection Act of 1994 (Pub. L. No. 103-322 (1994)). – (https://www.gpo.gov/fdsys/pkg /USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap123-sec2721.pdf) (վերջին այցելություն՝ 08.06.2021)
18. The Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. § 2510 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf) (վերջին այցելություն՝ 08.06.2021)
19. The Fair Credit Reporting Act of 1970 (Pub. L. No. No. 91-508 (1970)). (https://uscode.house.gov/statutes/pl/91/508.pdf) (վերջին այցելություն՝ 08.06.2021)
20. The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment) (Pub. L. No. 93- 380 (1974)). –

(http://www.legisworks.org/GPO/STATUTE-88-Pg484.pdf) (վերջին այցելություն՝ 08.06.2021)
21. The Freedom of Information Act (FOIA) (5 U.S.C. § 552). – (https://www.gpo.gov/fdsys/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf) (վերջին այցելություն՝ 08.06.2021)
22. The Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104–191). – (https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf). (վերջին այցելություն՝ 08.06.2021)
23. The Privacy Act of 1974 (Pub. L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a). – (https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf (վերջին այցելություն՝ 08.06.2021)
24. The Right to Financial Privacy Act of 1978 (RFPA; codified at 12 U.S.C. ch. 35, § 3401 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg3641.pdf) (վերջին այցելություն՝ 08.06.2021)
25. The Telephone Consumer Protection Act of 1991 (Pub. L. No. 102-243 (1991)). – (https://www.gpo.gov/fdsys/pkg /USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partI-sec227.pdf) (վերջին այցելություն՝ 08.06.2021)
26. The Video Privacy Protection Act (Pub. L. No. 100-618 (1988)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg3195.pdf) (վերջին այցելություն՝ 08.06.2021)
27. The White House (2014), 'Remarks by the President on Review of Signals Intelligence', Office of the Press Secretary, 17 January 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence. (վերջին այցելություն՝ 08.06.2021)
28. Uniting and Strengthening America by Providing Appropri- ate Tools Required to Intercept and Obstruct Terrorism Act of 26, october 2001. URL: http://epic.org/pri- vacy/terrorism/hr3162.html
29. US Census Bureau. – (https://www.census.gov/) (վերջին այցելություն՝ 08.06.2021)

Сдана/Հանձնվել է՝ 08.06.2021
Рецензирована/Գրախոսվել է՝ 15.06.2021
Принята/Ընդունվել է՝ 20.06.2021