Կիբեռանվտանգության կարգավորումներն ու դրանց ազդեցությունը բիզնես գործընթացների վրա

2025 թվականի դեկտեմբերի 4-ին Ազգային Ժողովը երկրորդ ընթերցմամբ ընդունեց «Կիբեռանվտանգության մասին»[1] և «Տեղեկատվական համակարգերի կարգավորման մասին»[2] ՀՀ նոր օրենքները, ինչպես նաև կիբեռանվտանգության կարգավորմանը միտված մի շարք այլ նորմատիվ իրավական ակտեր:

Այս նյութը նպատակ ունի ընդհանրական կերպով վեր հանել բիզնես գործընթացների վրա կիբեռանվտանգության իրավական կարգավորման դաշտի ստեղծման ազդեցությունը ու հակիրճ ներկայացնել սպասելիքները և անելիքները: Ուշադրություն կդարձնենք հիմնականում «Կիբեռանվտանգության մասին» ՀՀ օրենքի կարգավորումներին:

Ուժի մեջ մտնելը. «Տեղեկատվական համակարգերի կարգավորման մասին» ՀՀ օրենքն ուժի մեջ է 2025 թվականի դեկտեմբերի 26-ից, իսկ «Կիբեռանվտանգության մասին» (այսուհետ՝ Օրենք) ՀՀ օրենքը՝ 2026 թվականի հունվարի 4-ից :[3]

Օրենքը սահմանում է, որ տնտեսավարողների պարտականությունները սահմանող նորմերն են ուժի մեջ մտնելու այդ պարտականությունների մասով մանրամասն պահանջներ սահմանող ենթաօրենսդրական նորմատիվ իրավական ակտերի ուժի մեջ մտնելուց հետո: Բայց տեղին է ուշադրություն դարձնել «Նորմատիվ իրավական ակտերի մասին» ՀՀ օրենքի 27-րդ հոդվածի կանոնին, այն է՝ եթե նորմի կատարումը պայմանավորված է այլ նորմատիվ իրավական ակտի ընդունմամբ, տվյալ նորմը չի գործում այնքան, քանի դեռ ուժի մեջ չի մտնում այդ այլ նորմատիվ-իրավական ակտը:

Օրենքը գործողության ոլորտը. Եթե ուզում եք հասկանալ՝ արդյո՞ք Օրենքի պահանջները Ձեր բիզնեսի վրա տարածվում են կամ տարածվելու են, թե ոչ, պետք է քննարկել հետևյալը.

1 Օրենքը հասանելի է հետևյալ հղմամբ՝ https://www.arlis.am/hy/acts/218672/latest

2 Օրենքը հասանելի է հետևյալ հղմամբ՝ https://www.arlis.am/hy/acts/218686

3 Կիբեռնավտանգության կարգավորմանը միտված մնացած օրենքների ուժի մեջ մտնելու ժամկետները հիմնականում համընկնում են Օրենքը ուժի մեջ մտնելու ամսաթվի հետ:

Հարց 1. Արդյո՞ք Ձեր բիզնեսը կենսական նշանակության ոլորտում ծառայություն մատուցող է, թե ոչ:

Թեև կենսական նշանակության ոլորտի ցանկը հաստատված է Օրենքով (տե՛ս Ցանկ 1) , սակայն, այս պահին նույնականացման գործընթացը իրականացվել չի կարող, քանի որ Կառավարության կողմից դեռևս պետք է սահմանվեն ծառայության տեսակները /դասակարգիչները/՝ ըստ կենսական նշանակության ոլորտներում ծառայությունների տեսակների:

Եթե «Փոքր և միջին ձեռնարկատիրության պետական աջակցության մասին» օրենքով նախատեսված գերփոքր և փոքր ձեռնարկատիրության սուբյեկտների դասակարգման չափանիշները բավարարող իրավաբանական անձ և անհատ ձեռնարկատեր եք, Օրենքը Ձեզ վրա չի տարածվում, բացառությամբ, եթե շահագործում եք կրիտակական տեղեկատվական ենթակառուցվածք:

Հարց 2. Շահագործո՞ւմ եք արդյոք տեղեկատվական համակարգ:

Երբ Օրենքը գործածում է «տեղեկատվական համակարգ» եզրույթը, ապա հասկանում ենք, որ խոսքը գնում է կենսական նշանակության ոլորտներում շահագործվող՝

- էլեկտրոնային հաղորդակցության ցանցի,
- ցանկացած սարք կամ փոխկապակցված կամ հարակից (կապակցվող) սարքերի խմբի կամ
- տեխնիկական և ծրագրաապարատային միջոցների ամբողջության մասին:

Ընդ որում նշվում է, որ թվարկվածից մեկը կամ մի քանիսը միասին պետք է կատարեն թվային տվյալների ինքնաշխատ մշակում:

- կամ թվային տվյալների մասին, որոնք պահվում, մշակվում, ձեռք են բերվում կամ փոխանցվում են վերը թվարկված միջոցներով՝ դրանց օգտագործման, պաշտպանության և սպասարկման նպատակով:

Կարևոր է հիշել, որ միայն տեղեկատվական համակարգի շահագործումն ինքնին Օրենքի իմաստով չի հանգեցնում ծառայության մատուցողի որակման, սակայն կիբեռնավտանգության ոլորտի կարգավորող մարմնին (Օրենքում «Ինքնավար մարմին») իրավունք է տալիս դիտարկել տեղեկատվական համակարգը՝ որակելով այն համապատասխանող կենսական նշանակության ոլորտում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման չափանիշներին և ժամանակավորապես ճանաչելով որպես կենսական նշանակության ոլորտում կրիտիկական տեղեկատվական ենթակառուցվածք: **Այսինքն՝ տեղեկատվական համակարգ շահագործողը կարող է ժամանակավորապես ճանաչվել Օրենքի իմաստով ծառայություն մատուցող:**

Հարց 3. Շահագործո՞ւմ եք արդյոք կրիտակական տեղեկատվական ենթակառուցվածք:

Կրկին կարևոր է հասկանալ եզրույթի բովանդակությունը: Օրենքը **կրիտիկական տեղեկատվական ենթակառուցվածք** է ճանաչում կենսական նշանակության ոլորտներում շահագործվող՝

- ավտոմատացված կառավարման համակարգերը,
- տեղեկատվական համակարգերը,
- սարքավորումներ կամ դրանց մի մասը:

Ընդ որում՝ վերը թվարկվածի խափանումը կամ ոչնչացումը պետք է սպառնալիքներ ստեղծի ազգային անվտանգության, պաշտպանության, տնտեսության, սոցիալական բարեկեցության, բնակչության առողջության, շրջակա միջավայրի, հասարակական կարգի, միջազգային հարաբերությունների և կառավարման շարունակականության (governance continuity) համար, որպեսզի ենթակառուցվածքը որակվի որպես կրիտիկական:

Կարևոր է հիշել, որ միայն սահմանումն ինքնին չի ծառայելու ենթակառուցվածքը կրիտիկական որակելու պայմանները որոշելու հիմք:

Սահմանվել է, որ մշակվելու և Կառավարության կողմից հաստատվելու են կենսական նշանակության ոլորտում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքների **նույնականացման չափանիշները,** որոնց հիման վրա էլ ենթակառուցվածքները որակվելու կամ չեն որակվելու որպես կրիտիկական:

Հույժ կարևոր է ուշադրություն դարձնել, որ Օրենքը նախատեսել է, որ Կառավարությունը հաստատելու է նաև **կրիտիկական տեղեկատվական ենթակառուցվածքի ցանկ՝** կիբեռնանվտանգության պետական կառավարում և կարգավորում իրականացնելու նպատակով: Իսկ, ահա, Ազգային անվտանգության ծառայությունն իրավասություն է ունենալու Կառավարության կողմից սահմանված ցանկով հաստատված տեղեկատվական համակարգերի և կրիտիկական տեղեկատվական ենթակառուցվածքների նկատմամբ իրականացնելու Օրենքով լիազոր և Ինքնավար մարմնի վերապահված լիազորություններն ու գործառնությունները:

Ծառայություն մատուցող որակվելը Ձեր բիզնեսի համար հանգեցնելու է նոր պարտականությունների առաջացմանը: Պարտականություններն այժմ թվարկենք ընդհանրական կերպով.

- *ներքին ակտերի ընդունում,*
- *կազմակերպչական և տեխնիկական միջոցառումների ձեռնարկում կիբեռսպառնալիքները անընդհատ հայտնաբերելու և կառավարելու, կիբեռմիջադեպերը կանխելու, հայտնաբերելու, արգելելու և լուծելու, ինչպես նաև տեղեկատվական համակարգերի և կարևորագույն տեղեկատվական ենթակառուցվածքների անխափան գործունեությունն ապահովելու համար,*
- *ռիսկերի գնահատման իրականացում և դրանց կառավարում,*
- *կիբեռմիջադեպերի մասին Ինքնավար մարմնին ծանուցում և կիբեռմիջադեպին առնչվող Օրենքի պահանջների կատարում, այդ թվում Ինքնավար մարմնի ցուցումներին հետևելով և Ինքնավար մարմնին համակարգ մուտք գործելու հնարավորություն ընձեռելով,*
- *կիբեռանվտանգության մասնագետի նշանակում կամ գործառույթի*

պատվիրակում Օրենքի պահանջներին համապատասխանող կիբեռնավտանգության ծառայություններ մատուցող ընկերության,

► *կիբեռանվտանգության պարտադիր աուդիտ՝ եռամյա պարբերականությամբ,*

► *Ինքնավար մարմնին տեղեկատվական համակարգերին հասանելիության տրամադրում համապատասխանության գնահատում անցկացնելու համար:*

Պատասխանատվությունը սահմանված է հետևյալ արարքների համար (ներկայացված են ընդհանրական, տառացի չեն համընկնում Վարչական իրավախախտումների մասին օրենսգրքի 193,4 հոդվածին) և չափով.

► *Անվտանգության պահանջների խախտումները (կիբեռանվտանգության նվազագույն պահանջները չապահովելը, կիբեռանվտանգության ոլորտում միջազգային կամ ազգային ստանդարտներով սահմանված չափանիշները և պահանջները չպահպանելը կամ ոչ պատշաճ պահպանելը կամ համապատասխանությունը հավաստող փաստաթուղթ չունենալը)՝ 7,000,000 – 10,000,000 ՀՀ դրամ տուգանք,*

► *Ներքին ակտերի ընդունման և բիզնեսի ներքին գործընթացներին առաջադրվող պահանջների խախտումները (կիբեռանվտանգության ներքին կանոնակարգերի բացակայություն, ռիսկերի գնահատման (կամ գնահատման սանդղակի մշակման) չիրականացում, հնարավոր կիբեռմիջադեպի հետևանքների ծանրության/մասշտաբի չորոշում կամ կանխարգելիչ միջոցառումների ծրագրի չհաստատում, կիբեռանվտանգության մասնագետ չնշանակելը, կիբեռանվտանգության մասնագետի գործառույթների պատվիրակման պահանջները խախտելը)՝ 200,000 – 300,000 ՀՀ դրամ տուգանք,*

► *Կիբեռմիջադեպի մասին ծանուցման պահանջի կատարման խախտում և կիբեռմիջադեպին առնչվող այլ պարտականությունների խախտում՝ 500,000 – 700,000 ՀՀ դրամ տուգանք, բացառությամբ՝ տուժած անձանց ծանուցման պարտականության խախտման, որի տուգանքը սահմանված է՝ 200,000 – 300,000,*

► *Կիբեռանվտանգության աուդիտ չանցնելը՝ 200,000 – 300,000 ՀՀ դրամ տուգանք,*

► *Կիբեռնանվտանգության աուդիտի եզրակացության ներկայացման պահանջի խախտումը՝ 100,000 – 200,000 ՀՀ դրամ տուգանք,*

► *Ինքնավար մարմնի պահանջով փաստաթղթերի ու տեղեկությունների տրամադրման սահմանված ժամկետների խախտում 200,000 – 300,000 ՀՀ դրամ:*

Ցանկ 1

Կենսական նշանակության ոլորտներ

1. Էներգետիկայի ոլորտը.
2. արտադրության ոլորտը (քիմիական, սննդամթերքի, զենքի և զինամթերքի, բժշկական, Էլեկտրական, համակարգչային, Էլեկտրոնային և օպտիկական սարքերի արտադրության).
3. տրանսպորտային ոլորտը.
4. ջրի մատակարարման և կեղտաջրերի հեռացման ոլորտը.
5. կապի, այդ թվում՝ հեռահաղորդակցության ոլորտը.
6. փոստային կապի գործունեության ոլորտը.
7. ֆինանսական ծառայությունների ոլորտը.
8. առողջապահության ոլորտը.
9. տեղեկատվական տեխնոլոգիաների ոլորտը, այդ թվում՝ թվային ենթակառուցվածքները.
10. ռադիոակտիվ, ընդերքօգտագործման և վտանգավոր թափոնների կառավարման ոլորտը.
11. տիեզերական գործունեության ոլորտը.
12. տվյալների շտեմարանների կառավարման և շահագործման ոլորտը.
13. արտակարգ իրավիճակներում անվտանգության ապահովման ոլորտը.
14. պետական կառավարման ոլորտը, այդ թվում՝ պետական մարմինների կողմից շահագործվող թվային ենթակառուցվածքները:

Հեղինակների մասին

Նարինե Բեգլարյան

Ավագ գործընկեր, փաստաբան

Նարինե Բեգլարյանը ղեկավարում է ընկերության կորպորատիվ իրավունքի և կորպորատիվ վերակազմակերպումների (M&A) պրակտիկան, ինչպես նաև բանկային իրավունքի և կապիտալի շուկաների, անձնական տվյալների պաշտպանության ուղղությունները: Նա տրամադրում է խորհրդատություն և իրականացնում է ներկայացուցչություն: Ունի փաստաբանի արտոնագիր 2012 թվականից: Կոնցեռն Դիալոգի թիմին է միացել 2013 թվականին: Ավելի քան 15 տարվա փորձառություն ունեցող Նարինե Բեգլարյանի պրոֆեսիոնալիզմը գնահատված է նաև միջազգայնորեն նա ներառված է հեղինակավոր Chambers Global, Chambers Europe և IFLR1000 հիմնական վարկանիշավորման ցանկերում, ինչպես նաև Legal500-ի վարկանիշավորման առաջատար իրավաբանների ցանկում: Մինչ Կոնցեռն Դիալոգի թիմին միանալը շուրջ յոթ տարի աշխատել է բանկում և էլեկտրոնային հաղորդակցության ծառայություններ մատուցող ընկերությունում (in-house counsel):

Կոնցեռն Դիալոգի մասին

Կոնցեռն Դիալոգ փաստաբանական գրասենյակը 1998 թվականից սկսած վստահելի գործընկեր է բիզնեսների և անհատների համար իրավաբանության բոլոր ոլորտներում խորհրդատվությունից մինչև դատական պաշտպանություն: Ընկերությունը ճանաչված է կորպորատիվ իրավունքի, աշխատանքային իրավունքի, մրցակցության իրավունքի, հարկային իրավունքի, պայմանագրային իրավունքի, լիցենզիաների ու թույլտվությունների, ընտանեկան իրավունքի (ներառյալ երեխաների անդրսահմանային առևանգման /child abduction/) ոլորտների պրակտիկայով: Մասնավորապես, մենք մեծ փորձ ունենք SS, հեռահաղորդակցության և մեդիայի, հանքարդյունաբերության, Էներգետիկայի, կոմունալ ծառայությունների, բանկային և ֆինանսական, առողջապահության, անշարժ գույքի և ոչ առևտրային գործունեության ոլորտներում: Կոնցեռն Դիալոգի դատավարական փորձառությունը ՀՀ-ում առաջատարներից է, հատկապես բարդ քաղաքացիական, վարչական և արբիտրաժային գործերով: Փաստաբանական գրասենյակի անդամակցությունը TagLaw և Nextlaw ցանցերին և համագործակցությունն առանձին երկրներում գործով տեղական իրավաբանական կազմակերպությունների հետ թույլ է տալիս բարձրորակ ծառայություններ մատուցել հաճախորդներին փաստացիորեն ամբողջ աշխարհում: