Azərbaycan Respublikasının Qanunvericiliyinin BMT-nin Kibercinayətkarlıq Konvensiyasına Uyğunlaşdırılması: Mövcud Ziddiyyətlər

Gülnaz Rzayeva[1], Turan Məmmədzadə[2]
[1]Bakı Dövlət Universiteti, Bakı, Azərbaycan
[2]Milli Müdafiə Universiteti, Bakı, Azərbaycan
[1]*gulnazrzayeva@mail.ru*, [2]*turan932313@gmail.com*

***Xülasə*— Kibermәkanın tәqdim etdiyi geniş imkanlar, eyni zamanda, neqativ mәqsәdlәr üçün istifadә edilә bilәr. Ona görә dә kibercinayәtlәr vә onlara görә mәsuliyyәt müәyyәn olunması, elәcә dә hüquqi mәsәlәlәr dövrün aktual problemlәrindәndir. Kibercinayәtkarlıq qurbanlarının sayının artdığını, onlar üçün әdalәtin tәmin edilmәsinin zәruriliyini nәzәrә alaraq kibercinayәtlәrin effektiv şәkildә qarşısını almaq vә aşkar etmәk üçün 2024-cü ildә BMT tәrәfindәn Kibercinayәtkarlıq Konvensiyası qәbul edilmişdir. Azәrbaycan Respublikasında cinayәt qanunvericiliyinin BMT-nin kibercinayәtkarlıq konvensiyasına uyğunlaşdırılması istiqamәtindә mövcud vәziyyәt analiz edilmiş vә ziddiyyәtlәr müәyyәn olunmuşdur.**

***Açar sözlər*— kibercinayət; elektron verilənlər; cinayət qanunvericiliyi; Budapeşt Konvensiyası; Kibercinayətkarlıq Konvensiyası.**

I. Giriş

BMT tərəfindən 2024-cü ildə qəbul edilmiş Kibercinayətkarlıq Konvensiyası (rəsmi olaraq Kibercinayətkarlıq Konvensiyası: İKT sistemləri vasitəsilə törədilən cinayətlərlə mübarizə və ağır cinayətlərə dair sübutların elektron formada mübadiləsi üçün beynəlxalq əməkdaşlığın gücləndirilməsi adlandırılır) [1] qəbul edilmişdir. Konvensiyanın imzalanma mərasimi 2025-ci ildə Vyetnamın Hanoy şəhərində keçirildi. Azərbaycan Respublikası da Konvensiyanı ilk imzalayan dövlətlərdən biri olmuşdur ki, bundan sonra bu beynəlxalq-hüquqi sənəddə nəzərdə tutulan normaların milli hüquqa implementasiyası prosesi başlanmışdır. Azərbaycan Respublikasının Cinayət Məcəlləsində və Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində dəyişiklik edilməsi haqqında 3 mart 2026-cı il tarixli Qanun [2] həmin dəyişiklikləri nəzərdə tutur. Tədqiqatın növbəti bölmələrində BMT Konvensiyasında öz əksini tapan 11 kibercinayət əməli milli cinayət qanunvericiliyi ilə müqayisəli şəkildə təhlil olunacaq, təklif və tövsiyələr təqdim olunacaqdır.

II. BMT Konvensiyasının Qəbulundan Əvvəlki Hüquqi Tənzimləmələrə Ümumi Hüquqi Şərhi

Azərbaycan Respublikasının Cinayət Məcəlləsinin 30-cu fəsli “Kibercinayətlər” adlanır. Lakin belə adlandırma BMT Konvensiyasında əvvəl qəbul edilmiş və ölkəmiz tərəfindən ratifikasiya edilmiş Kibercinayətkarlıq haqqında 23 noyabr 2001-ci il Budapeşt Konvensiyasının müddəalarından irəli gəlmişdir. Maraqlı məqam ondan ibarətdir ki, kibərməkan çox geniş əhatə dairəsinə malikdir və burada yalnız kompüter informasiyası ilə bağlı cinayətlər törədilmir, eyni zamanda kibermühitdən istifadə edərək, digər qeyri-qanuni əməllər (dələduzluq, müəlliflik hüquqlarını pozma, təhqir, böhtan və s.) törədilir, yəni kibərməkanda mövcud əlaqələr və texniki vasitələr ənənəvi cinayətlərin törədilməsinin yeni vasitəsi kimi. çıxış edə bilir. Bəs belə olan halda “kibercinayət” anlayışının hədləri artmırmı? Cinayət Məcəlləsində yalnız kompüter informasiyası ilə bağlı cinayətlərin kibercinayətlər qismində tanınmasında qanunvericinin bu yanaşması nə dərəcədə əsaslıdır? – Kibercinayətkarlıq haqqında Konvensiyaya nəzər salsaq, burada kibercinayətlər fərqli qaydada qruplaşdırılır:

1. Kompüter verilənləri və sistemlərinin məxfiliyi, tamlığı və istifadə imkanlarına qarşı cinayətlər – qanunsuz daxil olma, qanunsuz ələ keçirmə, verilənlərə müdaxilə, sistemlərə müdaxilə, qurğulardan qanunsuz istifadə;

2. Kompüter vasitələrindən istifadə ilə bağlı cinayətlər – kompüter texnologiyalarından istifadə etməklə saxtalaşdırma, kompüter texnologiyalarından istifadə etməklə dələduzluq;

3. Məlumatların məzmunu ilə bağlı cinayətlər – uşaq pornoqrafiyası ilə bağlı cinayətlər;

4. Müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər – müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər.

Göründüyü kimi, Konvensiya kibercinayətləri kompüter cinayətlərinə və kompüter vasitəsilə törədilən cinayətlərə bölür. Əslində Konvensiyanın mövqeyi ilə razılaşmaq olar. Çünki yuxarıda sadalanan cinayətlərin hamısı kibərməkanda törədilir. Təbii ki, Azərbaycan Respublikasının cinayət qanunvericiliyində həmin əməllərin hamısı sanksiyalaşdırılmışdır. Sadəcə olaraq onlar kibercinayətlər fəslində deyil, müxtəlif fəsillərdə nəzərdə tutulmuşdur. Müasir dövrdə İKT-nin bütün insan həyatını əhatə etdiyini və onlardan kriminal məqsədlər üçün istifadənin geniş vüsət aldığına əsaslansaq, informasiya texnologiyaları cinayət əməllərinin törədilməsi üçün ən asan üsul kimi qiymətləndirilməlidir. Belə olan təqdirdə kibermühitdən istifadə etməklə törədilən bütün cinayətlərin kibercinayət kimi qəbul olunması bir qədər məntiqi sayılmır. Çünki cinayət əməllərinin obyekti və motivi (məqsədi) fərqli olur. Digər tərəfdən isə kibərməkanda törədilən bir çox əməllərin ənənəvi üsullarla da törədilməsi mümkündür [3]. Məsələn, Azərbaycan Respublikası Cinayət Məcəlləsinin 171-1-ci maddəsində [4] nəzərdə tutulan uşaq pornoqrafiyasının dövriyyəsi – uşaq pornoqrafiyasını yayma, reklam etmə, satma,

DOI: 10.25045/forensic.gov.2026.86

başqasına vermə, göndərmə, təklif etmə, əldə edilməsinə şərait yaratma, yaxud yaymaq və ya reklam etmək məqsədilə hazırlama, əldə etmə və ya saxlama ilə müşayiət olunur. Belə pornoqrafik məhsullar isə yalnız kibərməkanda deyil, müxtəlif nəşrlər, əşya və materiallar formasında da yayıla bilər [5]. Bütün bunlara istinad edərək, Azərbaycan Respublikasının qanunvericiliyinin yanaşmasını məqbul saymaq olar. Sadəcə olaraq İKT-nin inkişaf etdiyi mühitin xüsusiyyətlərini nəzərə alıb, bir çox ənənəvi cinayətlərin törədilməsi üsulları ilə bağlı dəyişikliklərin edilməsi məqsədə müvafiqdir. Digər bir məsələ isə ondan ibarətdir ki, terrorizm və s. bu kimi təhlükəli cinayətlər Konvensiyanın normalarından kənarda qalmışdır. X, Youtube və digər şəbəkələrdə müxtəlif terrorçuluğa açıq çağırışların yayılması kompüter vasitəsilə törədilən cinayətlərin siyahısının artırılmasını tələb edir. Ona görə də Budapeşt Konvensiyasının normalarındakı həm təcrübi, həm də hüquqi boşluqlar açıq-aydın görünür.

III. BMT Konvensiyasında Təsbit Olunmuş Kibercinayətlərin Milli Qanunvericiliklə Müqayisəli Təhlili

BMT Konvensiyasında ağır cinayət dedikdə, ən azı dörd il müddətinə azadlıqdan məhrum etmə və ya daha ciddi cəza ilə cəzalandırılan cinayət əməli nəzərdə tutulur. Deməli, burada kibercinayətlərin əksəriyyətinin ağır cinayət olması qəbul edilir. Həmin cinayətlərin Azərbaycan qanunvericiliyi ilə uyğunluğunu təhlil edək.

Qanunsuz daxil olma (maddə 7). Bu əməl İKT sisteminə bütövlükdə və ya onun hər hansı bir hissəsinə qəsdən qanunsuz girişi ehtiva edir. Konvensiya, həmçinin "cinayətin təhlükəsizlik tədbirlərini pozmaqla, elektron məlumatlar əldə etmək niyyəti ilə və ya digər vicdansız və ya cinayətkar niyyətlə və ya başqa bir İKT sisteminə qoşulmuş informasiya və kommunikasiya texnologiyaları sistemi ilə əlaqədar olaraq törədilməsinin" tərkib elementi kimi nəzərdə tutulmasını iştirakçı dövlətlərin səlahiyyətinə buraxır, yəni bu elementlərdən hər hansı birinin daxili qanunvericilikdə konkret əməli nəzərdə tutan dispozisiyada təsbiti yolveriləndir. Məsələn, AR CM-nin 271-ci maddəsində mühafizə tədbirlərini pozmaq və ya burada saxlanılan elektron verilənləri ələ keçirmək və yaxud da başqa şəxsi niyyət zəruri tərkib elementi kimi nəzərdə tutulmuşdur.

Qanunsuz ələ keçirmə (maddə 8). Bu cinayət İKT sisteminə, İKT sistemindən və ya belə sistemin daxilində elektron verilənlərin, o cümlədən bu cür elektron verilənlərin daşıyıcısı olan informasiya və kommunikasiya texnologiyaları sistemlərinin elektromaqnit şüalanmalarının texniki vasitələrdən istifadə etməklə qəsdən və qanunsuz ələ keçirilməsini nəzərdə tutur. Maddənin 2-ci bəndi cinayətin vicdansız və ya cinayətkar niyyətlə, yaxud başqa informasiya və kommunikasiya texnologiyaları sisteminə qoşulmuş informasiya və kommunikasiya texnologiyaları sistemi ilə əlaqədar olaraq törədilməsinin də tərkib elementi kimi qəbul edilməsini mümkün sayır. Lakin bizim cinayət qanunvericiliyinin 272-ci maddəsi belə elementləri nəzərdə tutmamışdır. Hesab edirik ki, verilənlərin qanunsuz ələ keçirilməsi əksər hallarda cinayətkar niyyətlə həyata keçirildiyi üçün bu cinayətin "qəsdən və qanunsuz" elementlərini ehtiva etməsi kifayətdir ki, məsuliyyət müəyyən olunsun. Maddənin məzmununun hədsiz genişləndirilməsinə gərək yoxdur.

Elektron verilənlərə müdaxilə (maddə 9). Konvensiya elektron verilənlərin qəsdən və qanunsuz zədələnməsini, silinməsini, korlanmasını, dəyişdirilməsini və ya bloklanmasını öz daxili qanunvericiliyinə əsasən cinayət kimi təsnif etmək üçün zəruri ola biləcək qanunvericilik və digər tədbirləri görülməsini dövlətlərdən tələb edir. Eyni zamanda, əhəmiyyətli zərər elementinin cinayət tərkibində nəzərdə tutulması səlahiyyəti dövlətlərin səlahiyyətinə buraxılır. AR CM-in 273-cü maddəsi bu elementi dispozisiyaya daxil edərək, elektron verilənlərə müdaxilə əməlini maddi tərkibli cinayət kimi tanımışdır. Fərqli cəhət ondadır ki, Konvensiyada *İKT sisteminə müdaxilə* ayrıca maddədə təsbit olunmuşdur (maddə 10). Milli qanunvericiliyimizdə isə hər iki əməl 273-cü maddədə ehtiva olunmuşdur. Mahiyyət etibarilə, eyni məzmuna malik olduğunu nəzərə alsaq, milli qanunvericiliyin yanaşmasını məqbul saya bilərik.

Cihazlardan sui-istifadə (maddə 11). Konvensiyaya görə, hər bir iştirakçı dövlət aşağıdakıların qəsdən və qanunsuz törədildiyi zaman öz daxili qanunvericiliyinə əsasən cinayət kimi kriminallaşdırılması üçün zəruri ola biləcək qanunvericilik və digər tədbirləri görməlidir: Konvensiyanın 7-10-cu maddələrinə uyğun olaraq müəyyən edilmiş cinayətlərin hər hansı birini törətmək məqsədi ilə hazırlanmış və ya uyğunlaşdırılmış proqram da daxil olmaqla cihaz və ya İKT sisteminin bütün və ya hər hansı bir hissəsinə daxil olmağın mümkün olduğu parol, giriş məlumatları, elektron imza və ya oxşar məlumatların əldə edilməsi, istehsalı, satışı, istifadə üçün satın alınması, idxalı, paylanması və ya başqa şəkildə təqdim edilməsi: qeyd olunan cihazların Konvensiyanın 7-10-cu maddələrinə uyğun olaraq müəyyən edilmiş cinayətlərdən hər hansı birini törətmək məqsədilə istifadə edilməsi niyyəti ilə saxlanması. AR CM-in 273-1-ci maddəsində də analoji əməl nəzərdə tutulmuşdur, lakin əhəmiyyətli zərərin də zəruriliyini əsas götürən milli qanunverici bu əməli maddi cinayət kimi qəbul etmişdir.

İKT sistemi ilə bağlı saxtalaşdırma (maddə 12). Bu əməl verilənlərin birbaşa oxunaqlı və anlaşılan olub-olmamasından asılı olmayaraq, qanuni məqsədlər üçün həqiqi hesab edilməsi və ya üzərində hərəkət edilməsi niyyəti ilə saxta verilənlərə səbəb olan elektron verilənlərin qəsdən və qanunsuz daxil edilməsini, dəyişdirilməsini, silinməsini və ya gizlədilməsini nəzərdə tutur. AR CM-in 273-2-ci maddəsi eyni əmələ görə sanksiya müəyyən etmişdir. Sual yaranır: Deepfake tətbiqlərdən qeyri-qanuni məqsədlər üçün istifadə bu maddə ilə əhatə olunurmu?

Əslində, deepfake tətbiqlər müxtəlif məqsədlər üçün edildiyi üçün ağır nəticələrə səbəb olan (məsələn, şəxsi həyata müdaxilə, siyasi məqsədlər və s.) saxta video, foto və səs yazıları cinayət əməli kimi qiymətləndirilməlidir. Lakin bu zaman 273-2-ci maddə ilə yanaşı, digər maddələrlə də tövsif yaranmalıdır. Çünki bu cür əməllərin qəsd obyektini məhz həmin maddələrin yönəldiyi ictimai münasibətlər təşkil edir.

İKT sistemi vasitəsilə oğurluq və ya dələduzluq (maddə 13). Konvensiyaya əsasən, hər bir iştirakçı dövlət özü və ya başqa bir şəxs üçün haqsız olaraq pul və ya digər əmlak əldə etmək kimi saxta və ya vicdansız niyyətlə başqa bir şəxsə əmlak itkisinin verilməsinin aşağıdakı yollarla törədilməsini öz daxili qanunvericiliyinə əsasən cinayət kimi təsnif etmək üçün zəruri ola biləcək qanunvericilik və digər tədbirləri görməlidir:

elektron verilənlərin daxil edilməsi, dəyişdirilməsi, silinməsi və ya bloklanması; İKT sisteminin fəaliyyətinə hər hansı müdaxilə; İKT sistemi vasitəsilə şəxsi hər hansı bir əməli etməyə məcbur edən hər hansı bir aldatma.

Respublikamızda oğurluq əməlini nəzərdə tutan 177-ci maddəyə İKT sistemindən istifadə etməklə törədilmə tövsifedici bənd kimi artırılsa da (AR CM, maddə 177.2.3-1), dələduzluq əməli üçün (AR CM, maddə 178) belə üsul nəzərdə tutulmamışdır. Ümumiyyətlə, İKT-dən istifadə etməklə törədilmənin ağırlaşdırıcı hal kimi nəzərdə tutulması dövrün tələbinə cavab verən bir müddəa kimi qiymətləndirilməməlidir. Çünki artıq istənilən əməli kibermәkandan istifadə etməklə törətmək mümkündür və hətta deyə bilərik ki, bu, daha asan törədilmə üsuludur. Ona görə də belə bir üsulun istifadəsi cinayətkarın daha çox ictimai təhlükəli olması ilə əlaqələndirilməməlidir.

Uşaqlara qarşı onlayn zorakılıqla bağlı cinayətlər. Konvensiyada bununla bağlı iki əməlin kriminallaşdırılması tələb olunur: onlayn uşaq cinsi istismarı və ya uşaq cinsi istismarı materialları ilə bağlı cinayətlər (maddə 14) və uşağa qarşı cinsi cinayət törətmək məqsədilə təhrik və ya himayə (grooming) (maddə 15). AR CM-də bu əməllər 150-153-cü maddələrdə nəzərdə tutulmuşdur. O ki qaldı Konvensiyada təsbit olunmuş *intim görüntülərin razılaşdırılmadan yayılması (maddə 16)* cinayətinə, artıq bu əməl şəxsi həyata müdaxilə olduğu üçün və eyni zamanda seksual məqsədlər olduğu üçün milli qanunvericilikdə bir neçə maddənin birgə tövsifi ilə cəzalandırılır.

Cinayət yolu ilə əldə edilmiş gəlirlərin yuyulması (maddə 17). Konvensiyaya müvafiq olaraq, hər bir iştirakçı dövlət öz daxili qanunvericiliyinin fundamental prinsiplərinə uyğun olaraq, qəsdən törədildikdə aşağıdakıları cinayət kimi təsnif etmək üçün zəruri ola biləcək qanunvericilik və digər tədbirləri görməlidir: əmlakın qanunsuz mənşəyini gizlətmək və ya ört-basdır etmək və ya əsas cinayətin törədilməsində iştirak edən hər hansı bir şəxsə həmin şəxsin hərəkətlərinin hüquqi nəticələrindən yayınmağa kömək etmək məqsədilə, həmin əmlakın cinayət yolu ilə əldə edildiyini bilərək, əmlakın çevrilməsi və ya başqasına verilməsi; əmlakın əsl təbiətinin, mənbəyinin, yerinin, sərəncamının, hərəkətinin və ya mülkiyyətinin və ya ona dair hüquqlarının gizlədilməsi və ya ört-basdır edilməsi, belə əmlakın cinayət yolu ilə əldə edilmiş gəlir olduğunu bilərək etmə; bu maddəyə uyğun olaraq müəyyən edilmiş hər hansı cinayətdə iştirak, onlarla əlaqə və ya sui-qəsd, törətməyə cəhdlər və onların törədilməsinə kömək etmək, təhrik etmək, asanlaşdırmaq və məsləhət vermək.

Qeyd etməliyik ki, milli qanunvericiliyimizdə cinayətlər qəsd obyektindən asılı olaraq, təsnifləşdirildiyinə görə cinayət yolu ilə əldə edilmiş gəlirlərin yuyulmasını kibercinayət kimi qiymətləndirmək düzgün deyil.

NƏTİCƏ

BMT Konvensiyası Budapeşt Konvensiyası ilə müqayisədə yeni olduğu üçün bir çox istiqamətlərdə dövrün tələbinə cavab verir. Ona görə də 25-26 oktyabr 2025-ci il tarixində Vyetnamın paytaxtı Hanoy şəhərində keçirilmiş imzalanma mərasimində Azərbaycan bu beynəlxalq-hüquqi sənədi imzalayan ilk dövlətlərdən biri olmuşdur və bunun ardınca 3 mart 2026-cı il tarixdə AR CM və AR CPM-ə edilən dəyişikliklər məhz həmin Konvensiyanın müddəaları nəzərə alınmaqla edilmişdir.

Xüsusilə, mövcud terminlər yeni və düzgün terminlərlə əvəz olunmuşdur. Məsələn, artıq kompüter məlumatı deyil, elektron verilən anlayışından istifadə olunur. Bu da cinayət qanunvericiliyimizin emal edilməmiş məlumat və ya verilənlərin kibercinayətlər kontekstində tanımadığının göstəricisidir. Eyni zamanda, İKT sistemi ifadəsinə üstünlük verilməsi də BMT Konvensiyasının normalarından irəli gəlir.

Qeyd etməliyik ki, dəyişikliklər edilməsinə baxmayaraq, bəzi çatışmazlıq və ziddiyyətlər də qalmaqdadır. Məsələn, AR CM-in 271-ci maddəsində tərkib elementi kimi niyyətin heç bir əhəmiyyəti olmamalıdır. Çünki "qanunsuz və qəsdən daxil olma" əməli formal tərkibli cinayət olduğundan, niyyətdən asılı olmayaraq məsuliyyət müəyyən olunmalıdır. Bundan başqa, hələ də "Kibercinayətlər" fəslində "ictimai əhəmiyyətli infrastruktur obyekti" ifadəsinə istinad olunur ki, bu, kritik informasiya infrastrukturu termini ilə əvəz olunmalıdır.

ƏDƏBİYYAT

[1] Ə.İ.Əliyev, G.A.Rzayeva, A.N.İbrahimova, B.A.Məhərrəmov, Ş.S.Məmmədrzalı, İnformasiya hüququ: dərslik, Bakı: Nurlar nəşriyyatı, - 2019, 448 s.

[2] "Azərbaycan Respublikasının Cinayət Məcəlləsində və Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində dəyişiklik edilməsi haqqında" 3 mart 2026-cı il tarixli 373-VIIQD nömrəli Azərbaycan Respublikasının Qanunu https://e-qanun.az/framework/61568

[3] Rzayeva, G.A. Protection of human rights violated by cybercrimes in global information society // Науковий вісник Дніпропетровського державного університету внутрішніх справ, - 2020. №2, - pp. 35-41. DOI: 10.31733/2078-3566-2020-2-35-41

[4] Azərbaycan Respublikası Cinayət Məcəlləsi https://e-qanun.az/framework/46947

[5] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.

Harmonisation of the Criminal Legislation of the Republic of Azerbaijan with the UN Convention on Cybercrime: Existing Contradictions

Gulnaz Rzayeva[1], Turan Mammadzada[2]

Baku State University, Baku, Azerbaijan

National Defence University, Baku, Azerbaijan

[1]gulnazrzayeva@mail.ru, [2]turan932313@gmail.com

Abstract - The vast opportunities offered by cyberspace can also be used for negative purposes. Therefore, cybercrime and the establishment of responsibility for it, as well as the legal issues involved, are among the current pressing problems of the day. In light of the increasing number of victims of cybercrime and the necessity of ensuring justice for them, the UN adopted the Convention on Cybercrime in 2024 to effectively prevent and detect cybercrimes. The current situation in the Republic of Azerbaijan regarding the alignment of criminal legislation with the UN Convention on Cybercrime has been analyzed, and discrepancies have been identified.

Keywords - cybercrime; electronic data; criminal legislation; Budapest Convention; Cybercrime Convention.