ƏQLİ MÜLKİYYƏT HÜQUQU

VİRTUAL MƏKANDA DEEPFAKE TƏTBİQLƏRİ: MÖVCUD TƏHLÜKƏLƏR VƏ HÜQUQİ TƏNZİMLƏMƏDƏKİ BOŞLUQLAR

Elnur Hümbətov*

Xülasə

Virtual məkanın formalaşması heç də hər zaman müsbət istiqamətdə təhlil olunmur. Rəqəmsal əsrdə yeni texnologiyaların təqdim etdiyi imkanlar vasitəsilə hüquq pozuntularının mahiyyətində də ciddi dəyişikliklər müşahidə edilir. Artıq fiziki müstəvidə deyil, virtual müstəvidə törədilən pozuntular müasir dünya əhalisi üçün ciddi narahatlıqlar yaradır. Belə pozuntular sırasında xüsusi çəkiyə malik olan deepfakelər dövrün aktual problemlərindəndir. Bu potensialı ciddiyə alan beynəlxalq təşkilatlar deepfakeləri gələcəyin ən böyük təhlükələrindən biri hesab edirlər. Məqalədə deepfake tətbiqləri ilə bağlı xarici dövlətlərin hüquqi tənzimləmələri müqayisəli təhlil olunmuş, deepfake məzmunların insan hüquq və azadlıqlarını pozduğu vəziyyətlər hüquq normaları əsasında tədqiq edilmiş, respublikamızda deepfake məzmunların sanksiyalaşdırılması ilə bağlı təklif və tövsiyələr irəli sürülmüşdür.

Açar sözlər: *deepfake, süni intellekt, virtual məkan, insan hüquqları, şəxsi toxunulmazlıq hüququ, internet.*

1.1. Giriş

Mütəxəssislərin hesablamalarına görə, 2026-cı ilə qədər onlayn məzmunun 90%-ə qədərinin sintetik şəkildə yaradılması gözlənilir. [24] Sintetik media süni intellekt (AI) istifadə edərək yaradılan və ya manipulyasiya edilən mediaya aiddir. Əksər hallarda, sintetik media oyun oynamaq, xidmətləri yaxşılaşdırmaq və ya həyat keyfiyyətini yaxşılaşdırmaq üçün yaradılsa da, [15, s.5] artıq bu gün sintetik medianın artması və təkmilləşdirilmiş texnologiya dezinformasiya imkanlarına, o cümlədən deepafake kimi mənfi xarakterizə olunan nəticələrə gətirib çıxarmışdır.

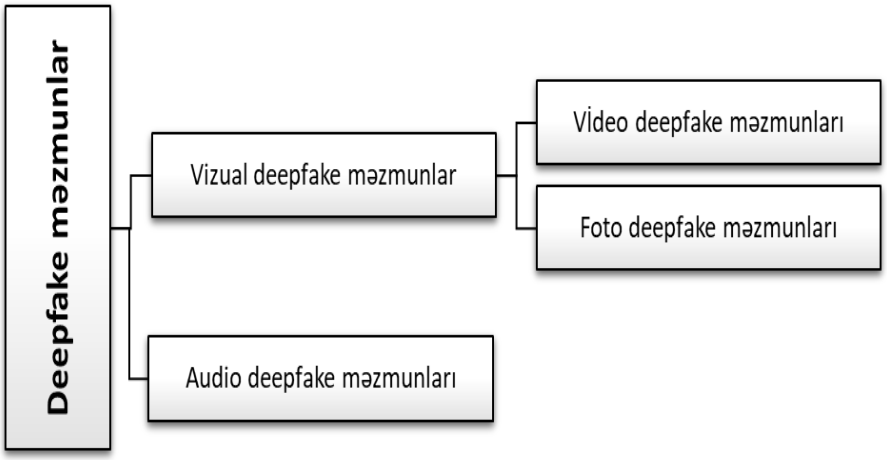
Şəxsin üzü və mimikasından istifadə edərək qeyri-real fotoşəkillər, videolar və audiolar hazırlamaq üçün qabaqcıl texnologiyalardan istifadə edən Deepfake tətbiqi hamımıza məlumdur. "Deepfake" termini "dərin öyrənmə - deep learning" və "saxta - fake" birləşməsindən yaranmışdır. Deepfake internetdə ilk dəfə 2017-ci ildə anonim bir Reddit istifadəçisi məşhur qadın məşhurları əks etdirən real pornoqrafik videolar yaratmaq üçün texnologiyanı tətbiq edərkən ortaya çıxdı. [22, s.299]

Deepfake ilə insanın etmədiyi və ya demədiyi şeylər sanki həmin şəxs bunları etmiş kimi görünür. Bu texnologiyanın inkişafı ilə saxta video və məzmun yaratmaq imkanı xeyli çoxalmışdır ki, Deepfake tətbiqinin fərdi məlumatların qorunması hüququnu pozması konkret faktdır.

* hüquq üzrə fəlsəfə doktoru, Bakı Dövlət Universiteti, İnsan hüquqları və informasiya hüququ UNESCO kafedrasının müəllimi

1.2. Deepfake məzmunların növləri

Deepfake məzmunlar aşağıdakı kimi qruplaşdırıla bilər:



Vizual deepfake məzmunlara foto deepfake məzmunları və video deepfake məzmunları daxildir. Hər vizual deepfake məzmunda yalnız bir insanın şəklini başqa bir insanın bədəninə yükləmək mümkün deyil, həm də dodaq sinxronizasiyası vasitəsilə bir insanın şəklinin dodaqlarının göründüyü deepfake məzmunlar da hazırlana bilər.

Foto deepfake məzmunu üz və bədən dəyişdirmə şəklində ola bilər və bir şəxsin üzünün və ya bədəninin şəklini digər şəxsin üzünün və ya bədəninin şəklinə əlavə etməklə həyata keçirilə bilər. Deepfake texnologiyası ilə təkcə insanların üzlərini başqa bədənlərə əlavə etmək mümkün deyil, dərin öyrənmə ilə süni intellekt bizə həmin insanın tamamilə yeni bir fotosunu verə bilər. Məsələn, qocalma filtrlərini ehitva edən proqramlar.

Video deepfake məzmunu təsvir edilən şəxsin yalnız üzünü deyil, səsini də təqlid edə bildiyi üçün daha realistdir və hədəfə alınmış auditoriyanı çaşdırmaq ehtimalı yüksəkdir.

Audio ilə deepfake məzmun səsin dəyişdirilməsi və ya mətndən nitqə çevrilmə şəklində həyata keçirilə bilər. Səs dəyişdirmək üçün hazırlanmış audio deepfake məzmununda insanın səsi dəyişdirilə və ya onun səsi təqlid edilə bilər. İnsanın səsini real şəkildə təqlid etməyin bir çox zərərləri ola bilər. Bunlara misal gətirək; Süni intellektə malik bir şirkətin baş direktorunun səsini təqlid edərək, şirkət rəhbərinin milyonlarla dollar itirməsinə səbəb olan saxtakarlıq edilmişdir. [20, s.142] Bununla bağlı bir neçə maraqlı fakta istinad etmək olar: Böyük Britaniyada yerləşən bir şirkətin baş direktorunun səsini kopyalayaraq, dələduzlar şirkətin Almaniyadakı tərəfdaş firmasına zəng etmiş və onlardan Bolqarıstandakı təchizatçılarının hesabına 243 min dollar köçürmələrini istəmişər. Bu ödənişin təcili olduğunu və müddətin gecikdiyini iddia edən dələduz məqsədinə nail olmuşdur. [8]

1.3. Maraqlı faktlar və hüquqi tənzimləmələr

Deepfake asanlıqla əldə edilə bilən, getdikcə daha ucuz olan və aşkarlanması olduqca çətin olan və özünü təkmilləşdirən texnologiya təklif edir. Bəzi deepfakelər zərərsiz və əyləncəli bədii ifadələr olsa da, internetdəki deepfakelərin doxsan faizindən çoxu qadınların pornoqrafik təsvirləridir. [18, p.2] Məşhur qadın simaları rəqəmsal olaraq pornoqrafik məzmuna əlavə edilib, dərin saxta porno videolar yaradır. Scarlett Johansson, Meghan Markle, Taylor Swift kimi qurbanların adını qeyd etmək olar. Lakin deepfake yalnız ayrı-ayrı fərdlərlə məhdudlaşmayıb, siyasi məqsədlərə qarşı da yönəlməyə başlamışdır. Deepfakesin yaratdığı ən böyük təhlükə onun etibarlı mənbələrdən gəldiyi görünən yalan məlumatları yaymaq qabiliyyətidir. Məsələn, bununla bağlı üç məşhur faktı qeyd etmək olar:

Facebook-un yaradıcısı Mark Zukerberq onun Facebookun necə sahibi olması ilə öyündüyünü göstərən deepfake videonun qurbanı olmuşdur. Video insanların Facebook kimi sosial media platformalarından xalqı aldatmaq üçün necə istifadə edə biləcəyini göstərmək üçün hazırlanmışdı.

ABŞ prezidenti Co Bayden 2020-ci ildə prezident seçkilərinə təsir etmək üçün onu şişirdilmiş koqnitiv tənəzzül vəziyyətlərində göstərən çoxsaylı deepfake videoların qurbanı oldu. [16] Prezidentlər Barak Obama və Donald Tramp da bəziləri dezinformasiya, bəziləri isə satira və əyləncə kimi yayılan deepfake videoların qurbanı olmuşlar. [13]

2022-ci ildə Ukrayna prezidenti Vladimir Zelenskinin qoşunlarından təslim olmağı xahiş etdiyi deepfake video yayımlandı. [14]

Qeyd olunan faktlar deepfake kimi proqramların nəinki fərdi məlumatların qorunması hüququnu pozduğunu, həmçinin ictimai və dövlət maraqları baxımdan necə təhlükəli olduğunu bir daha təsdiq edir. Bəs Deepfake qanunidirmi? – Problemə Avropa çərçivəsində yanaşsaq, iki hüquqi tənzimləmə faydalı ola bilər: Süni İntellekt Aktı [21] və Fərdi Məlumatların Qorunmasının Ümumi Qaydaları [17].

Birinci sənəddə təsbit olunan şəffaflıq öhdəlikləri insanlarla qarşılıqlı əlaqədə olan, emosiyaları aşkar etmək və ya biometrik məlumatlara əsaslanaraq (sosial) kateqoriyalarla əlaqəni müəyyən etmək üçün istifadə olunan və ya məzmun yaradan və ya manipulyasiya edən sistemlər (deepfakes) üçün tətbiq olunacaq. Əgər süni intellekt sistemi orijinal məzmuna nəzərəçarpacaq dərəcədə bənzəyən şəkil, audio və ya video məzmunu yaratmaq və ya manipulyasiya etmək üçün istifadə olunursa, məzmunun avtomatlaşdırılmış vasitələrlə yaradıldığını açıqlamaq öhdəliyi olmalıdır. Burada qanuni məqsədlər üçün (hüquq-mühafizə, ifadə azadlığı) istisna təşkil edir.

Bu qanun layihəsi perspektivli ilk addım kimi qiymətləndirilsə də, müəyyən problemlər hələ də qalmaqdadır. Zərərli məzmun yaradıcılarına, xüsusən də Avropa Birliyindən kənarda fəaliyyət göstərənlərə qarşı tətbiqetmə məsələsi olaraq qalır. Bundan əlavə, öz şəxsi imkanlarında (peşəkardan fərqli olaraq) zərərli

deepfake yaradanların bu cür şəffaflıq öhdəliklərinə tabe olub-olmayacağı hələ də aydın deyil.

Fərdi Məlumatların Qorunmasının Ümumi Qaydalarına gəldikdə isə, Qaydaların 5.1-ci maddəsinə əsasən, fərdi məlumatlar dəqiq olmalı və zəruri hallarda yenilənməlidir. Dəqiq olmayan fərdi məlumatların işlənilmə məqsədləri nəzərə alınmaqla, gecikmədən silinməsini və ya düzəldilməsini təmin etmək üçün bütün ağlabatan addımlar atılmalıdır. Deməli, deepfake-lə yaradılmış məzmun uyğunsuz, qeyri-dəqiq və ya saxtadırsa, onlar təxirə salınmadan silinməli və ya düzəldilməlidir. Üstəlik, hətta deepfake məzmunu doğru və ya dəqiq olsa da, məlumat subyekti deepfake-in qurbanı olduğu halda Qaydaların 17-ci maddəsində öz əksini tapmış sildirmək hüququndan istifadə edə bilər.

Bütün bunlara baxmayaraq, qəbul etməliyik ki, bu gün virtual məkanda baş verən istənilən pozuntuya qarşı hüquqi cavab tədbirləri texnologiyadan geri qalır. Ona görə də həm dövlətlər, həm də BigTechs deepfake problemlərinə qarşı tədbirlər görür. Virciniya, Nyu-York Corciya, Nyu-Cersi, Texas və Kaliforniya ABŞ-da deepfake tətbiqlərinin hüquqi problemlərinə qarşı tənzimləmələri olan ilk ştatlar qismində tanınırlar. Virciniya qanunvericiliyi konsensual olmayan deepfake pornoqrafiyasının yayılmasına görə cinayət cəzası tətbiq edir. [6] Birinci dərəcəli cinayət hesab edilən bu əməlin elementlərinə aşağıdakılar daxil edilir: pis niyyətlə yayan və ya satan hər hansı şəxs; istənilən vasitə ilə yaradılmış istənilən videoqrafik və ya hərəkətsiz görüntü; bu şəxs belə videoqrafik və ya hərəkətsiz təsviri yaymaq və ya satmaq üçün lisenziyasının və ya səlahiyyətinin olmadığını bildikdə və ya bilmək üçün əsas olduqda; belə əməl məcbur etmək, təqib etmək və ya qorxutmaq niyyəti ilə törədildikdə.

18 may 2021-ci il tarixində Nyu-York ştatının qəbul etdiyi qanuna əsasən, qurbanlara Deepfake məzmununun qeyri-qanuni yayılmasını izləmək və qarşısını almaq üçün səlahiyyətlər verən hüquqi dəyişikliklər etmişdir. Eyni zamanda, həmin dəyişikliyə əsasən, qeyri-qanuni hazırlanmış deepfake fotoları vasitəsilə insanları təqib və şantaj edənlər ağır cinayətlərə görə mühakimə olunacaqlar (S 6829A). [7]

Deepfake texnologiyasının geniş tətbiqi ilə Corciya ştatı da köhnə hüquqi qaydalara yenidən baxdı. Müvafiq olaraq, Deepfake vasitəsilə hazırlanmış şəkilləri yayan və qəsdən istifadə edən şəxslər 1 ildən 5 ilədək həbs və ya 100.000 dollardan çox olmayan cərimə ilə cəzalandırılırlar (SB 78). [4, s.713]

Texas qanunu dövlət vəzifəsinə namizədlərə zərər vurmaq və ya seçkilərə təsir etmək məqsədi daşıyan deepfake videoların yaradılmasını və yayılmasını qadağan edir. Belə ki, 2019-cu ildən etibarən Seçki Məcəlləsində edilmiş dəyişikliyə görə, namizədə xəsarət yetirmək və ya seçkinin nəticələrinə təsir etmək niyyəti ilə deepfake saxta videonun yaradılması və belə videonun seçkidən sonra 30 gün ərzində dərc edilməsinə və ya yayılmasına səbəb olma A kateqoriya pozuntu kimi qəbul edilir. Seçki Məcəlləsinin 255.004-cü bəndinə əsasən, deepfake videolar aldatmaq məqsədi ilə yaradılmış, real insanın reallıqda baş verməmiş hərəkəti həyata keçirməsini təsvir edən videolar kimi müəyyən edilir. [25]

Kaliforniya qanunvericiliyi isə problemə daha geniş aspektdən tənzimləmə nəzərdə tutmuşdur. Kaliforniyada seçkidən sonra 60 gün ərzində siyasi deepfake video və görüntülərin və razılaşdırılmamış deepfake pornoqrafiyanın istifadəsinə qarşı qanunlar qəbul edilmişdir. [26]

Analoji tənzimləməni aparan Nyu Cersi ştatında 2020-ci ildə seçkilərin təmin edilməsinə yönəlmiş qanun layihəsində təsbit olunmuşdur ki, seçkilər ərəfəsində namizədlərin nüfuzuna xələl gətirmək məqsədilə hazırlanan deepfake videoları cinayət məsuliyyətinə cəlb olunacaq. Lakin bu qanuna əsasən, yumoristik məqsədlər daşıyan videolar bu əhatə dairəsindən çıxarılır (AB 4985). [5]

ABŞ-la paralel dövrdə Çində də maraqlı hüquqi tənzimləmələr edilmişdir. 18 noyabr 2019-cu il tarixində Mədəniyyət və Turizm Nazirliyi, Dövlət Radio və Televiziya İdarəsi və Dövlət İnternet İnformasiya İdarəsi tərəfindən "Onlayn audio və video informasiya xidmətlərinin idarə edilməsi haqqında" Əsasnamə dərc edilmişdir ki, bu əsasnamənin tələbinə görə, onlayn xidmət təminatçıları istifadəçilərin telefon nömrələri, şəxsiyyət vəsiqələri və ya digər üsullarla real şəxsiyyətini yoxlamaq üçün Kibertəhlükəsizlik Qanununun müddəalarına əməl edəcəklər. Real şəxsiyyət məlumatlarını təqdim edilmədiyi təqdirdə, şəxslərə informasiya yayım xidmətləri göstərilməyəcək. Buna görə məzmun istehsalçıları platformalarda öz şəxsiyyətləri ilə qeydiyyatdan keçəcəkləri üçün sözügedən deepfake məzmunu kimin istehsal etdiyini müəyyən etmək çox asan olacaqdır. Bununla belə, bu kontekstdə dövlət qurumlarının nəzarəti altında onlayn platformalarda məzmun istehsal edən və ya paylaşan hər kəs müəyyən mənada dövlətin nəzarətində olacaqdır. Sözügedən Əsasnamənin 11-ci maddəsinə əsasən, onlayn audio (video) məlumatın provayderləri və istifadəçiləri, əslində mövcud olmayan audio və ya video məlumatı yaratmaq, dərc etmək və ya ötürmək üçün dərin öyrənmə və ya virtual reallıq kimi yeni texnologiyalar və ya proqramlardan istifadə etdikdə, görünən şəkildə açıqlamalıdırlar. Lakin həmin müddəanın ikinci bəndində saxta xəbər məlumatlarının yaradılması və yayılması bu qaydadan istisna kimi nəzərdə tutulur və bu məqsədlə deepfake yaradılması qadağandır. Buna əsaslanaraq, Çində deepfake və buna bənzər texnologiyalardan istifadə ilə bağlı baxışı saxta məlumatlara əsaslanan deepfake məzmunun yaradılmasının qeyri-qanuni hesab edildiyini söyləmək olar. Çünki bu məzmunda əslində mövcud olmayan yalan məlumatlar vardır. 12-ci maddəyə uyğun olaraq, onlayn xidmət təminatçıları istifadəçiləri tərəfindən dərc olunan məzmunu idarə edirlər. Onlar 11-ci maddənin birinci bəndinin tələblərinə cavab verməyən hər hansı məzmunla rastlaşdıqda, bu məlumatın ötürülməsini dərhal dayandırmalıdırlar. [12]

Bu gün artıq deepfake nəticələri məhkəmə proseslərində də görünməyə başlayıb desək, yanılmarıq. Məsələn, məşhur "deepfake cheerleader mom" işini misal göstərmək olar: 2021-ci ilin mart ayında Pensilvaniya ştatından olan Raffaela Spone adlı qadın həbs olundu və qızının şənlik edən rəqiblərini ələ salmaq üçün deepfakelər yaratdığına görə bir çox təqibdə ittiham olundu. Prokuror o zaman milli və beynəlxalq xəbərlər yayaraq, "deepfake cheerleader mom" kimi tanınan Spone-nun qurbanların sosial media hesablarını çılpaq, içki içən və siqa-

ret çəkən kimi göstərmək üçün dəyişdirdiyini, və onlara özlərini öldürmələrini söyləyən mətnlər və səsli mesajlar göndərdiyini söylədi. Hətta zərər çəkmiş yeniyetmələrdən biri ABC-nin "Günaydın Amerika" verilişində deepfake nəticəsində çəkdiyi zərər və sıxıntıları izah etmək üçün iştirak etdi. Spone deepafake yaratmağı inkar etdi və rəqəmsal sahə üzrə ixtisaslaşmış məhkəmə ekspertləri və digər ekspertlər onun video və fotoların deepfake deyil, orijinal olduğunu müəyyən etdilər. Bununla belə, onlar bildirdilər ki, video keyfiyyətinin aşağı olması və digər sübutların olmaması qəti nəticə çıxarmağı mümkünsüz edir. [11]

Baxmayaraq ki, cari iş üzrə deepfake faktını sübuta yetirmək mümkün olmamışdır, bu gün video və səs yazıları bir çox cinayət və mülki hərəkətlərin əvəzsiz elementini təşkil edir. Məhkəmə sistemi "görmək inanmaqdır" nəzəriyyəsi altında hisslərə güvənməklə nəyin real olduğunu müəyyən etmək üçün fitri insanın qabiliyyətinin effektivliyinə arxalanaraq fəaliyyət göstərir. Deepfake sübutlar bu prosesi alt-üst edir. Deepfake texnologiyası təkmilləşdikcə hakimlər dəlilin həqiqi olub-olmadığını, yəni sübutun müdafiəçinin iddia etdiyi kimi olub-olmadığını müəyyən etməkdə çətinlik çəkəcəklər. Ona görə də hal-hazırda məşhur dünya şirkətləri deepfakeləri müəyyən etmək və bloklamaq üçün texnologiya hazırlayır. Bəzi sosial media şirkətləri öz platformalarına icazə verməzdən əvvəl video və şəkillərin mənbəyini yoxlamaq üçün blokçeyn texnologiyasından istifadə edirlər. Beləliklə, etibarlı mənbələr yaradılır və saxtakarlığın qarşısı alınır. Bununla yanaşı, Facebook və Twitter hər ikisi zərərli deepfakeləri qadağan etmişdir. Bəs deepfakeləri aşkar edən texnologiyalar varmı? – 14 noyabr 2022-ci il tarixli yeni bir inkişafa görə, Türk mühəndis İlke Dəmir və onun həmkarı Umur Çiftçi tərəfindən Intel şirkəti daxilində yeni deepfake aşkarlama texnologiyası istehsal edilmişdir və bu, deepfake məzmunun aşkarlama nisbətini 96%-ə qaldırmışdır. [19]

Fakecatcher adlanan bu yeni texnologiya Intel aparat və proqram təminatından istifadə edən dünyanın ilk deepfake detektorudur və saxtakarlığı saniyələr ərzində aşkar edə bilir. Fakecatcheri digər deepfake aşkarlama proqramlarından fərqləndirən cəhət odur ki, bu texnologiya sözügedən məzmundakı piksellərdə qan axını ilə bağlı ipucular axtarır və qan axını ilə bədən rəngindəki rəng dəyişikliklərini izləyərək dərin öyrənmə yolu ilə məzmunun saxtalığını aşkar edir. Fakecatcher müxtəlif sahələrdə profilaktik olaraq istifadə edilə bilər Məsələn, Sosial media platformalarının istifadəçiləri video yükləmək istədikdə, bu video Fakecatcherdən ilk dəfə keçdikdən və onun dəqiqliyi müəyyən edildikdən sonra istifadəçi tərəfindən yüklənə bilər və ya qlobal xəbər təşkilatları manipulyasiyanın qarşısını almaq üçün saxtalaşdırılmış videoları çıxara bilər. [19]

Deepfake texnologiyası getdikcə daha real görüntülər yaradır. Ona görə də mütəxəssislər virtual məkan istifadəçilərinin informasiya savadlılığını artırmaq məqsədilə deepfake məzmunların aşkar olunması üçün aşağıdakı əlamətlərə diqqət yetirməyi tövsiyə edirlər:

- qeyri-təbii göz və dodaq hərəkətləri;
- qeyri-təbii üz ifadələri;

- qeyri-təbii bədən hərəkəti, daha dəqiq desək, yöndəmsiz görünən bədən duruşu;

- foto və videoların keyfiyyətinin aşağı olması və s. [23]

Deepfakes-ə qarşı qanunların olmaması insanların çoxunun yeni texnologiyadan, onun istifadəsi və təhlükələrindən xəbərsiz olması ilə nəticələnir. Bu səbəbdən, əksər deepfakes hallarında qurbanlar qanunla qorunmurlar. Bəs, belə vəziyyətlərin qarşısını almaq üçün hansı hüquqi tədbirlər görülməlidir? Yalnız siyasi və pornoqrafik məqsədli deepfakelərin sanksiyalaşdırılması yetərlidirmi? Sıravi şəxslərin təhqir olunması məqsədilə hər hansı saxta video və fotoların hazırlanması necə cəzalandırılmalıdır? - Bu kimi sualların cavablandırılması məqsədilə şəxsi toxunulmazlıq hüququna, şərəf və ləyaqətə qəsd edən əməllərlə mübarizə üzrə normalara diqqət yetirək.

Doktrinada əksər müəlliflər deepfakelərlə mübarizənin texniki əhəmiyyət daşıdığını vurğulayaraq, deepfakesləri məhdudlaşdıran yeni qanunvericiliyin yaradılmasına qarşı çıxış edirlər. Bu sahədə əsas arqumentlərdən biri ondan ibarətdir ki, bu texnologiyanın yaratdığı diffamasiya üçün hüquqi resurs artıq ictimai və yalan bəyanatlar vasitəsilə reputasiyaya xələl gətirən şəxsləri məsuliyyətə cəlb edən diffamasiya qanunları şəklində mövcuddur. [10] Lakin nəzərə almalıyıq ki, dünya dövlətlərinin heç də hamısında cinayət diffamasiyası hüquqi təsbitini tapmamışdır. Mülki diffamasiyanın qəbul edildiyi dövlətlərdə diffamasiya qanunları deepfakelərin qurbanları üçün hüquqi müraciət təmin edə bilsə də, pul kompensasiyası şərəf və ləyaqətə dəyən ziyanı aradan qaldıra bilməz və emosional rifahı adekvat şəkildə bərpa edə bilməz. Buna görə də həqiqət pərdəsi altında həyatları məhv etmək gücü ilə yeni deepfakelərin yaradılmasının və yayılmasının qarşısını almaq və texnologiyadan sui-istifadə edənlər üçün cinayət məsuliyyətinin tətbiqi üçün qanunvericilik bazası lazımdır.

Deepfakelərə qarşı sanksiyaların tətbiqi ilə bağlı daha yanlış bir yanaşma isə ondan ibarətdir ki, bəzi tədqiqatçıların fikrincə, deepfake texnologiyasından istifadə nəticəsində şəxsi toxunulmazlıq hüququnun pozulması mülki qanunvericilikdə kompensasiya sanksiyaları ilə, bu texnologiyadan seçkilərə təsir etmək və uşaq pornoqrafik deepfake məzmunu yaratmaq üçün istifadə edildiyi hallar isə cinayət qanunu sanksiyaları ilə həll edilməlidir. Çünki seçkilərə təsir etmək məqsədi ilə qanunsuzluq baş verdikdə, bu fərdi deyil, kollektiv nəticə yaradacaq və nəticədə dəymiş ziyanı ödəmək mümkün olmayacaqdır. Bu səbəbdən, demokratik hüquqi dövlətin təməl prinsipləri qorunmalı, xalqın iradəsi hər cür hücuma qarşı qorunmalıdır. Eyni zamanda, uşaqların pornoqrafik deepfake video və fotolarının kriminal sanksiyaya məruz qalması müəlliflər tərəfindən uşağın ən yüksək mənafeyi prinsipi ilə əlaqələndirilsə də, nəticə etibarilə ictimai maraqlara qəsd edildiyi iddia edilir: Uşaqların səsi və təsviri ilə hazırlanan deepfake məzmun ayrı-ayrı şəxslərə deyil, ictimai asayişə zərər vurduğu üçün bu əmələ görə cinayət məsuliyyəti tətbiq olunmalıdır. [3, s.87-88]

Evropol hesabatında bildirilir ki, qarşıdakı aylarda və illərdə çox güman ki, təhdid subyektləri müxtəlif cinayət əməllərini asanlaşdırmaq və ictimai rəyə

təsir etmək və ya təhrif etmək üçün dezinformasiya kampaniyaları aparmaq üçün deepfake texnologiyasından getdikcə daha çox istifadə edəcəklər. Ona görə də deepfake texnologiyasının yaratdığı təhlükələri effektiv şəkildə həll etmək üçün qanunvericilik və tənzimləmə hüquq-mühafizə orqanlarının ehtiyaclarını nəzərə almalıdır. Deepfakelə qarşılaşılan problemləri həll etmək üçün hüquq mühafizə orqanları bu kimi pozuntuların aşkarlanmasına dair təlim keçməlidir və normativ baza hüquq mühafizə orqanlarının hazırlıq səylərini dəstəkləməlidir [15, s.22].

1.4. Nəticə

Deepfake kiminsə demədiyi və ya etmədiyi bir şeyi söylədiyini və ya etmədiyini göstərən uydurma fotoşəkillər və videolar olmaqla, həqiqəti təhrif edərək, qanuni və saxta medianı ayırd etməyi çətinləşdirir, eləcə də insanların öz baxışlarına uyğun gələn məzmunu qəbul etmə ehtimalını artırır. Sürətlə inkişaf edən deepfake texnologiyası yalanları fakt kimi təqdim etmək üçün səsləri inandırıcı şəkildə təqlid etmək və videoları rəqəmsal şəkildə dəyişdirmək qabiliyyəti ilə - razılığa əsaslanmayan dərin saxta pornoqrafiya yaratmaq, siyasi dezinformasiyaları yaymaq və bizneslərı qəsb etmək üçün rəqəmsal cəmiyyətdə çox geniş istifadə olunur. Beynəlxalq Sülh üçün Karnegi Fondunun qeyd etdiyi kimi, deepfakes zorakılığı qızışdırmaq, seçkilərin nəticələrini dəyişdirmək və diplomatiyaya zərbə vurmaq potensialına malikdir. [9]

İlk dəfə ABŞ-da meydana çıxdığı üçün deepafeke texnologiyası ilə bağlı ilk hüquqi tənzimləmələr də bu dövlətdə aparılmışdır. Belə ki, Amerikanın Virciniya, Texas, Nyu-York, Corciya, Kaliforniya kimi ştatları müəyyən hallarda deepfake texnologiyasının siyasi istifadəsini qadağan etsə də, bəzi ştatlar yalnız pornoqrafik deepfake məzmunun istifadəsini məhdudlaşdırır. Deepfake texnologiyasının yaratdığı təhdidlərin fərqində olan bir dövlət olaraq Çin də ABŞ-la eyni vaxtda bu sahədə hüquqi tənzimləmələr etmişdir. Avropa Birliyi isə süni intellekt sistemlərinin tətbiqi çərçivəsində deepfake texnologiyasını qiymətləndirmiş və yalnız xidmət təminatçıları baxımından tənzimləmələr etmişdir. Belə ki, məzmun istehsalçısından şəffaflıq öhdəliyinə uyğun olaraq istehsal etdiyi deepfake məzmunu barədə açıqlama etməsi tələb olunur.

Bəs Azərbaycan qanunvericiliyində vəziyyət necədir? Əgər şəxs deepfakelə yaradılmış məzmunla kimisə şantaj, təhqir edirsə və ya belə məzmunu pornoqrafik məqsədlərlə istifadə edirsə və s. bu kimi hallarda hansı cəza və hansı norma əsasında tətbiq ediləcəkdir? - Respublikamızda deepfake texnologiyasının istifadəsi qanuni olaraq tənzimlənmir və bu texnologiyanın istifadəsi ilə yarana biləcək hüquq pozuntularına görə qüvvədə olan müxtəlif qanunvericilik normaları ilə qismən də olsa sanksiyalar tətbiq edilə bilər. Bununla belə, hesab edirik ki, deepfake texnologiyasından istifadə ehtiyatla tənzimlənməlidir, çünki bu texnologiyada olan potensial təhlükələr təkcə fərdi deyil, həm də ictimai nəticələrə səbəb ola bilər. Məqalədə istinad etdiyimiz müxtəlif siyasi faktlar (Ukraynada Zelenskinin müraciətinin deepfak-lə edilməsi, ABŞ-da president seçkiləri zamanı yaradılmış deepfake videolar və s.) bunu bir daha təsdiq edir.

Cinayət qanunvericiliyinin əlaqədar maddələrinin təhlilinə əsasən, belə bir nəticəyə gəlmək olar ki, əgər deepfake foto və videolar pornoqrafik məzmunludursa, Cinayət Məcəlləsinin 171-1 və 242-ci maddələri ilə sanksiya tətbiqi mümkündür. Lakin məzmun təhqir, böhtan və ya fərdi məlumatların açıqlanması ilə bağlıdırsa, cinayət məsuliyyətinin müəyyən olunmasında çətinliklər meydana çıxır. Belə ki, deepfake video və ya foto heç də hər bir halda təhqir və ya böhtan xarakterli olmur. Bu məzmunlar dezinformasiya məqsədilə də törədilə bilər. Belə olduğu halda, Cinayət Məcəlləsinin 148 və 149-cu maddələrinə əsasən əmələ tövsif vermək mümkün olmayacaqdır. Həmçinin 156-cı maddədəki cinayət tərkibi həqiqi məlumatların açıqlandığı halda meydana çıxır. Deepfake məzmunlar isə saxta olduğu üçün həmin normanın tətbiqi mümkün olmayacaqdır. Hesab edirik ki, kompüter məlumatlarına genişləndirilmiş təfsir verməklə, Cinayət Məcəlləsinin 273-2-ci maddəsində ikinci bəndin əlavə olunması ilə "informasiya texnologiyalarından istifadə etməklə saxta məzmuna malik video, foto və audioların hazırlanması və yayılması"na görə məsuliyyət müəyyən oluna bilər. Bu zaman cinayətin subyektinin maddənin birinci bəndindən fərqli olaraq, xüsusi subyekt kimi nəzərdə tutulmaması daha düzgündür. Bu yolla istənilən şəxs tərəfindən deepfake məzmunların yaradılması kriminallaşdırılmış olacaqdır.

İstinadlar:

1. Əliyev Ə.İ. İnsan hüquqları. Dərslik. Yenidən işlənmiş və əlavələr edilmiş ikinci nəşri. Bakı: Nurlar, 2019, 352 s.

2. Əliyev Ə.İ., Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S. İnformasiya hüququ. Dərslik. Bakı: Nurlar, 2019, 448 s.

3. Melike Alkaya Erdoğan. Deepfake teknolojisinin hukuka aykırı kullanımından doğan hukuki ve cezai sorumluluk / Yüksek lisans tezi / İstanbul, 2023, 94 s.

4. Fatih Arslan. Deepfake Technology: A Criminological Literature Review // The Sakarya Journal of Law (The SJL), - 2023. Vol. 11, № 1, - p. 701-720

5. 'Deepfakes' Emerging Issue in State Legislatures. https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/deepfakes-emerging-issue-in-state-legislatures

6. § 18.2-386.2. Unlawful dissemination or sale of images of another; penalty. https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/

7. 6829—A, Cal. No. 1113, 2021-2022 Regular Sessions, State of New York. https://custom.statenet.com/public/resources.cgi?id=ID:bill:NY2021000S6829&ciq=urn:user:PA6792530&client_md=1c73bcfa0f524a3afb44ed4419746c5a&mode=current_text

8. A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=77336c522416

9. Can the EU Prevent Deepfakes From Threatening Peace? https://carnegieeurope.eu/strategiceurope/79877

10. Caroline Quirk. The High Stakes of Deepfakes: The Growing Necessity of Federal Legislation to Regulate This Rapidly Evolving Technology. https://legaljournal.princeton.edu/the-high-stakes-of-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/

11. Cheerleader's mom accused of making "deepfake" videos of daughter's rivals. https://www.cbsnews.com/news/raffaela-spone-cheerleader-mom-deepfakes/

12. China issues regulation for online audio, video services. http://www.china.org.cn/china/2019-11/30/content_75463798.htm

13. Deepfake technology, beyond reality, cybersecurity and life (and death). https://www.telefonica.com/en/communication-room/blog/deepfake-technology-beyond-reality-cybersecurity-and-life-and-death/

14. Deepfakes in warfare: new concerns emerge from their use around the Russian invasion of Ukraine. https://theconversation.com/deepfakes-in-warfare-new-concerns-emerge-from-their-use-around-the-russian-invasion-of-ukraine-216393

15. Facing reality? Law enforcement and the challenge of deepfakes. An Observatory Report from the Europol Innovation Lab, 2022, 23 p.

16. False claims of 'deepfake' President Biden go viral. https://www.bbc.com/news/62338593

17. General Data Protection Regulation. https://gdpr-info.eu/art-4-gdpr/

18. Henry Ajder, Giorgio Patrini, Francesco Cavalli & Laurence Cullen. The state of deepfakes landscape, threats, and impact. Deeptrace, 2019, 20 p.

19. Intel's deepfake detector analyzes 'blood flow' in video pixels to return results in milliseconds with 96% accuracy. https://www.intel.com/content/www/us/en/newsroom/news/intel-introduces-real-time-deepfake-detector.html

20. Jan Kietzmann, Linda W. Lee, Ian P. McCarthy, Tim C. Kietzmann. Deepfakes: Trick or Treat? / Business Horizons, 2020, Vol 63, Issue 2, pp. 135-146

21. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

22. Rebecca A. Delfino. Deepfakes on Trial: A Call To Expand the Trial Judge's Gatekeeping Role To Protect Legal Proceedings from Technological Fakery / Hastings Law Journal? 2023, Vol 74, Issue 2, pp. 293-348

23. Sandeep Singh Mankoo. DeepFakes- The Digital Threat in the Real World // Gyan Management Journal, - 2023. No. 17/1, - pp. 71-77.

24. Schick, Nina. Deepfakes: The Coming Infocalypse: What You Urgently Need To Know. Hachette UK, 2020, 224 p.

25. Texas Election Code - ELEC § 255.004. True Source of Communication. https://codes.findlaw.com/tx/election-code/elec-sect-255-004/

26. Two New California Laws Tackle Deepfake Videos in Politics and Porn. https://www.dwt.com/blogs/media-law-monitor/2020/02/two-new-california-laws-tackle-deepfake-videos-in.

DEEPFAKE APPLICATIONS IN VIRTUAL SPACE: EXISTING THREATS AND REGULATORY GAPS

Elnur Humbatov[*]

Abstract

The formation of virtual space is not always analyzed in a positive way. In the digital age, serious changes are observed in the nature of legal violations through the opportunities provided by new technologies. Violations, which are no longer on the physical plane, but on the virtual plane, cause serious concerns for the modern world population. Deepfakes, which have a special

[*] Ph.D. in Law, Baku State University, Human Rights and Information Law UNESCO Chairs

weight among such violations, are one of the current problems of the time. International organizations that take this potential seriously consider deepfakes to be one of the greatest threats of the future. In the article, the legal regulations of foreign countries related to deepfake applications were comparatively analyzed, the situations in which deepfake contents violated human rights and freedoms were studied based on legal norms, and suggestions and recommendations were made regarding the sanctioning of deepfake contents in our republic.

Keywords: *deepfake, Artificial Intelligence, virtual space, human rights, right to privacy, internet.*

ПРИЛОЖЕНИЯ DEEPFAKE В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ: СУЩЕСТВУЮЩИЕ УГРОЗЫ И ЮРИДИЧЕСКИЕ ПРОБЛЕМЫ

Эльнур Гумбатов*

Резюме

Формирование виртуального пространства не всегда анализируется в положительном ключе. В эпоху цифровых технологий наблюдаются серьезные изменения в характере правонарушений благодаря возможностям, предоставляемым новыми технологиями. Нарушения, происходящие уже не в физическом, а в виртуальном плане, вызывают серьезные опасения у современного населения мира. Дипфейки, занимающие среди подобных нарушений особый вес, являются одной из актуальных проблем современности. Международные организации, которые серьезно относятся к этому потенциалу, считают дипфейки одной из величайших угроз будущего. В статье было сравнительно проанализировано правовое регулирование зарубежных стран, связанное с дипфейковыми приложениями, на основе правовых норм изучены ситуации, в которых дипфейковый контент нарушает права и свободы человека, а также сделаны предложения и рекомендации по санкционированию дипфейкового контента в нашей стране.

Ключевые слова: *дипфейк, искусственный интеллект, виртуальное пространство, права человека, право на неприкосновенность частной жизни, интернет.*

* доктор философии по праву, преподаватель кафедры ЮНЕСКО прав человека и информационного права Бакинского государственного университета.