ХҒТАР 10.27.51; 10.77.51
ӘОЖ 347.121.1:343.4:004.8
JEL K14

https://doi.org/10.46914/2959-4197-2026-1-3-224-241

ЕРНИШЕВ К.А.,[1]
з.ғ.к., қауымдастырылған профессор.
e-mail: yernishev.k@mail.ru
ORCID ID: 0000-0003-3687-3009
САРЫКУЛОВ К.Р.,[2]
з.ғ.к., профессор.
e-mail: kurman_sr@mail.ru
ORCID ID: 0000-0002-8841-9871
РАХМЕТОВА Г.Р.,[2]
з.ғ.к., аға оқытушы.
e-mail: Rahmet-1976@mail.ru
ORCID ID: 0009-0007-3131-9494
УТАНОВ М.А.,*[2]
з.ғ.д., доцент, профессор.
*e-mail: mau_25@mail.ru
ORCID ID: 0009-0005-1119-3818
[1]М.Х. Дулати атындағы Тараз университеті,
Тараз қ., Қазақстан
[2]М.О. Әуезов атындағы
Оңтүстік Қазақстан университеті,
Шымкент қ., Қазақстан

ДИПФЕЙКТЕР АР-НАМЫСҚА, ҚАДІР-ҚАСИЕТКЕ, ЖЕКЕ ӨМІРГЕ ЖӘНЕ ҚОҒАМДЫҚ ҚАУІПСІЗДІККЕ ТӨНЕТІН ҚАТЕР РЕТІНДЕ: ҚҰҚЫҚТЫҚ ҚАРСЫ ІС-ҚИМЫЛ ТЕТІКТЕРІ

Аңдатпа

Мақала Қазақстан Республикасында дипфейктердің ар-намысқа, қадір-қасиетке, жеке өмірге, бейнеге құқыққа, іскерлік беделге және қоғамдық қауіпсіздікке төндіретін құқықтық тәуекелдерін зерттейді. Проблема жеке бір технологиялық ақау ретінде емес, синтетикалық аудио-, фото- және бейнемазмұн арқылы тұлғаға және жария тәртіпке зиян келтірудің жаңа тәсілі ретінде қарастырылады. Зерттеу материалдары ретінде Қазақстан Республикасының Конституциясы, Азаматтық кодекс, Қылмыстық кодекс, Әкімшілік құқық бұзушылық туралы кодекс, «Жасанды интеллект туралы» Заң, «Онлайн-платформалар және онлайн-жарнама туралы» Заң, халықаралық құжаттар және ЕО, АҚШ пен Ұлыбританияның салыстырмалы құқықтық тәсілдері алынды. Формалды-құқықтық, салыстырмалы-құқықтық, жүйелік және доктриналық әдістер, сондай-ақ құқықтық модельдеу қолданылды. Қолданыстағы қазақстандық құқық дипфейктер келтіретін зияннан қорғаудың жекелеген тетіктерін қамтитыны, бірақ бұл тетіктер фрагментарлы екені негізделеді: олар жала жабуға, жеке өмірді бұзуға, алаяқтыққа немесе жалған ақпарат таратуға жауап береді, бірақ тұлғаны синтетикалық имитацияны толық көлемде қамтымайды. Сонымен қатар дипфейкті анықтаудан жәбірленушінің құқықтарын қалпына келтіруге дейінгі кезеңдік алгоритм ұсынылып, анықтау нәтижелерін цифрлық дәлелдеме ретінде пайдаланудың шектері анықталды. Автор сараланған модель ұсынады: зиянды дипфейктің таралуын шұғыл тоқтатуға және оны жоюға арналған азаматтық-құқықтық тетік; қолданыстағы қылмыстық құрамдарды бірінші кезекте қолдану және келісімсіз интимдік дипфейк, кәмелетке толмаған адамның бейнесін сексуалдандырылған контексте пайдалану, алаяқтық, бопсалау мен қоғамдық қауіпсіздікке елеулі қатер төндіретін имитация үшін нысаналы қылмыстық-құқықтық өлшемдер әзірлеу; сондай-ақ таңбалау жөніндегі қолданыстағы талапты қайталамайтын арнайы платформалық міндеттер.

Тірек сөздер: дипфейк, ар-намыс және қадір-қасиет, жеке өмір, бейнеге құқық, қоғамдық қауіпсіздік, азаматтық-құқықтық қорғау, қылмыстық жауаптылық.

Кіріспе

Дипфейктің қаупі оның жасандылығында ғана емес. Генеративтік модельдер нақты адамның сөзін, дауысын, мимикасын не әрекетін сенімді әрі жедел имитациялайды. Жәбірленуші материалдың шынайы еместігін дәлелдегенше, ол көшіріліп, қайта жарияланып, бопсалау, алаяқтық, беделге нұқсан келтіру немесе қоғамдық қақтығысты арандату құралына айналуы мүмкін.

Қазақстандық құқықта бастапқы қорғау құралдары бар. Конституция қадір-қасиетке және жеке өмірге қол сұғылмаушылықты бекітеді [1]. Азаматтық кодекс ар-намысты, қадір-қасиетті, іскерлік беделді, жеке өмір құпиясын және өз бейнесіне құқықты қорғайды [2], ал моральдық зиянды өтеу оның Ерекше бөлімімен реттеледі [3]. Жоғарғы Сот интернетте мәлімет тарату мен теріске шығару тәсілдерін нақтылаған [4], моральдық зиян туралы нормативтік қаулы өтемді бағалау өлшемдерін белгілейді [5].

Қылмыстық кодекс жеке өмірді, дербес деректерді және хабарламалар құпиясын бұзу, алаяқтық, бопсалау, көрінеу жалған ақпарат тарату мен қоғамдық қауіпсіздікке қатер төндіретін әрекеттерді қамтиды [6]. ӘҚБтК жала жабу және ақпараттық құқық бұзушылықтар үшін жауаптылық көздейді [7]. «Жасанды интеллект туралы» Заң ашықтық пен пайдаланушыны хабардар ету талаптарын бекітеді [8], «Онлайн-платформалар және онлайн-жарнама туралы» Заң контент айналымының платформалық режимін белгілейді [9].

Соған қарамастан, бұл нормалар дипфейктің ерекшелігін толық қамтымайды. Синтетикалық материал сөздік мәлімдемесіз-ақ болмаған әрекетті «көрсете» алады; мүліктік шығынсыз беделге, қадір-қасиетке немесе жеке өмірге зиян келтіруі де мүмкін. Сондықтан құқық жекелеген салдарды танығанымен, зиян келтіру тәсілін – тұлғаны синтетикалық имитациялауды – дербес бағалауда қиналады.

Негізгі ғылыми мәселе дипфейктің азаматтық-құқықтық қорғау, қылмыстық құқық, ақпараттық реттеу және жасанды интеллект режимдерінің қиылысында орналасуынан туындайды. Практикалық мәселе дәлелдемелерді табу, жинау, бекіту және сақтау рәсімдерінің контенттің таралуын жедел тоқтатумен бірізді байланыспауынан көрінеді: жәбірленуші контенттің тараталғанын, тұлғаның танылуын, материалдың синтетикалық сипатын, келісімнің болмауын және зиянды дәлелдеуге тиіс; ал онлайн-деректер тез өзгеріп не жойылып кетеді. ӘҚБтК-нің 641-1-бабын қолдану үшін жасанды интеллект жүйесінің жауапты меншік иесін немесе иегерін айқындау қажет [7]. Қылмыстық процесте бастапқы файлды, аккаунтты, жүктеу уақытын, метадеректер мен желілік іздерді процестік нысанда сақтау шешуші. Цифрлық іздердің тұлғаны сәйкестендірудегі маңызы көрсетілген [10, 82 б.], ал провайдерлер мен платформалардағы тіркеу деректеріне қол жеткізудің қиындығы олардың жоғалу тәуекелін арттырады [11, 126 б.]. Қолданыстағы платформалық заң жедел сақтау рәсімін арнайы реттемейді [9].

Зерттеу объектісі – жеке мүліктік емес құқықтар мен қоғамдық қауіпсіздікке әсер ететін дипфейктерді жасау, тарату, жою және құқықтық бағалау кезінде туындайтын қоғамдық қатынастар. Зерттеу пәні – Қазақстан Республикасында зиянды дипфейктерге қарсы әрекет етудің азаматтық-құқықтық, қылмыстық-құқықтық және сабақтас ақпараттық-құқықтық тетіктері.

Мақаланың мақсаты – Қазақстанда дипфейктерге қарсы азаматтық-құқықтық, платформалық және нысаналы қылмыстық-құқықтық құралдардың қажеттілігі мен шегін анықтап, олардың өзара байланысқан моделін ұсыну. Мақсатқа жету үшін мынадай міндеттер шешіледі: дипфейктің құқықтық мәні бар белгілерін нақтылау; азаматтық, әкімшілік, қылмыстық және ақпараттық құқықтың қолданыстағы нормаларының шектерін анықтау; қазақстандық реттеуді ЕО, АҚШ және Ұлыбритания тәсілдерімен салыстыру; нысаналы қылмыстық-құқықтық құралдардың шегі мен нысанын айқындау; жәбірленушіні шұғыл қорғаудың азаматтық-құқықтық құралдарын ұсыну.

Зерттеу сұрағы былай тұжырымдалады: ар-намысты, қадір-қасиетті, жеке өмірді және қоғамдық қауіпсіздікті қорғаудың қолданыстағы жалпы тетіктері дипфейктерге қарсы әрекет ету үшін жеткілікті ме, әлде Қазақстанға арнайы азаматтық-құқықтық және қылмыстық-құқықтық конструкциялар қажет пе?

Мақаланың гипотезасы Қазақстанға барлық дипфейкті қамтитын әмбебап тыйым емес, құқықтық салдары мен қоғамдық қауіптілік деңгейіне қарай сараланған тетіктер қажет деген

тұжырымға негізделеді. Азаматтық-құқықтық тетік зиянды жедел тоқтатуға, бұзылған құқықты қалпына келтіруге және моральдық зиянды өтеуге бағытталуға тиіс. Қылмыстық-құқықтық деңгейде қолданыстағы құрамдар бірінші кезекте қолданылуға тиіс; сонымен бірге келісімсіз интимдік дипфейк, кәмелетке толмаған адамның бейнесін сексуалдандырылған контексте пайдалану, алаяқтық, бопсалау және қоғамдық қауіпсіздікке елеулі қатер төндіретін тұлғалық имитация үшін нысаналы арнайы құралдардың қажеттілігі негізді. Олардың дербес құрам немесе саралаушы белгі түрі мен санкциясы эмпирикалық және құқық қолдану материалдары негізінде айқындалуға тиіс.

Мақаланың ғылыми жаңалығы дипфейктерді реттеудің сараланған моделін ұсынудан тұрады: «дипфейк үшін бір бап» емес, үш өзара байланысты деңгей – тұлғаны азаматтық-құқықтық шұғыл қорғау, таңбалау және жою жөніндегі платформалық-әкімшілік міндеттер, жоғары қауіпті синтетикалық имитацияларға арналған нысаналы қылмыстық-құқықтық өлшемдер. Зерттеудің теориялық маңызы бейнеге құқық, ар-намыс пен қадір-қасиет, жеке өмір және синтетикалық цифрлық бірегейлік арасындағы байланысты нақтылауда көрінеді. Практикалық маңызы заң шығарушыға, соттарға, тергеу органдарына, онлайн-платформаларға және жәбірленушілерге арналған критерийлер ұсынумен айқындалады.

Зерттеу Қазақстанда дипфейктердің таралуы туралы автордың жеке статистикалық деректерін қамтымайды. Мұндай деректер пайдаланылған жоқ, өйткені тексерілетін ғылыми қорытынды үшін синтетикалық медиа қолдану белгісі бойынша арнайы жіктелген арыздардың, сот актілерінің, платформалық хабарламалардың және сараптамалық қорытындылардың ресми массивтері қажет. Мақаланың міндеті нормативтік-доктриналық сипатта: құбылыстың таралуын өлшеу емес, оған құқықтық жауап беру конструкциясын анықтау.

Шетелдік әдебиет дипфейктің жеке беделге ғана емес, аудио- және бейнедәлелдемелерге қоғамдық сенімге, демократиялық процестерге және қауіпсіздікке зиян келтіретінін көрсетеді [12, 1753–1764 бб.]. Келісімсіз интимдік синтетикалық контент шынайы жазба болмағанның өзінде интимдік құпиялылықты, қадір-қасиетті және адамның өз цифрлық бейнесін бақылауын бұзады [13, 1 б.; 14, 399 б., 404 б.]. Мұндай материалды реттеу сатира, өнер, білім беру және адал журналистиканы қамтымайтын кепілдіктермен ұштасуға тиіс [15, 892–897 б.].

Жәбірленушіге вирустық контентті өз бетімен іздеу және жою ауыртпалығын жүктеу жеткіліксіз [13, 1 б.], ал заңды тек «нақты фотосуретпен» шектеу синтетикалық интимдік және репутациялық зиянды қорғаудан тыс қалдырады [14, 399, 404 б.]. Осы талдаудан шығатыны: дипфейктің кең техникалық анықтамасы құқықтық мақсат үшін тұлғаның танылуы, келісім, адастыру, зиян және пайдалану контексті өлшемдерімен тарылтылуға тиіс.

Қазақстандық зерттеу технологиялық анықтау мен түпнұсқалықты бағалауды құқықтық қарсы іс-қимылдың бір бөлігі ретінде көрсетеді [16, 192 б., 194–195 б.]. Техникалық әдебиет анықтау модельдерінің нәтижелері белгісіз генераторларға, файлдың сығылуына және кейінгі өңделуіне тәуелді екенін көрсетеді [17, 1–4 бб.]. Сондықтан олардың жалпылау қабілеті мен орнықтылығы жеке тексерілуге тиіс [18, 9–13 бб.].

А.Б. Сманова, А.Ж. Муратова және Ш.Р. Жумагулова дипфейк-алаяқтық пен әлеуметтік инженерияны талдайды [16, 188–211 бб.]. А.Б. Сактаганова, И.С. Сактаганова және Б.У. Турегельдиев АҚШ, ЕО және Қазақстан модельдерін салыстырады [19, 260–261 бб.]. Алайда тұлғаны азаматтық-құқықтық қорғау, цифрлық дәлелдемелерді бекіту және нысаналы қылмыстық-құқықтық құралдар бір модельде жеткілікті біріктірілмеген.

Салыстырмалы материал ЕО-дағы ашықтықты [20], Еуропа Кеңесінің адам құқықтарына бағдарланған тәсілін [21], АҚШ-тағы интимдік цифрлық қолдан жасауға қатысты нысаналы тыйым мен жәбірленуші бастайтын жоюды [22], Ұлыбританиядағы келісімсіз интимдік синтетикалық бейнені жасауды криминализациялауды көрсетеді [23]. Осы зерттеудің ғылыми олқылығы – бұл тетіктерді Қазақстанның қолданыстағы құқығымен байланыстырып, азаматтық қорғау, платформалық міндеттер, дәлелдемелерді сақтау және жоғары қауіпті әрекеттерге қылмыстық реакцияны шамадан тыс тыйым салусыз бір жүйеге келтіру.

Материалдар мен әдістер

Зерттеудің материалдық базасы төрт блоктан құрылды: Қазақстанның конституциялық және азаматтық-құқықтық актілері; қылмыстық және әкімшілік-деликтік заңнама; жасанды интеллект, онлайн-платформалар және цифрлық қатынастар туралы актілер; ЕО, Еуропа Кеңесі, АҚШ және Ұлыбританияның салыстырмалы дереккөздері. Қазақстандық актілер тұлғаның қадір-қасиетін, жеке өмірін, бейнесін, дербес деректерін, мүліктік мүдделерін және қоғамдық қауіпсіздікті қорғау шектерін анықтау үшін пайдаланылды. Шетелдік материалдар ашықтық, нысаналы криминализация, жәбірленуші бастайтын жою және платформалық міндеттерді салыстыруға алынды.

Формалды-құқықтық әдіс азаматтық, қылмыстық, әкімшілік және цифрлық құқықтың қолданыстағы нормаларының шектерін анықтауға мүмкіндік берді. Жүйелік әдіс ар-намысты, қадір-қасиетті, бейнені, жеке өмірді, дербес деректерді және қоғамдық қауіпсіздікті қорғау арасындағы байланысты көрсету үшін қолданылды. Салыстырмалы-құқықтық әдіс қазақстандық модельді ЕО, АҚШ және Ұлыбритания тәсілдерімен салыстыру үшін пайдаланылды. Доктриналық талдау сөз бостандығы, интимдік құпиялылық, платформалық жауапкершілік және криминализацияға қатысты даулы тәсілдерді анықтауға мүмкіндік берді. Арнайы азаматтық-құқықтық және нысаналы қылмыстық-құқықтық құралдарды әзірлеу үшін құқықтық модельдеу әдісі қолданылды.

Зерттеу нормативтік-доктриналық және салыстырмалы-құқықтық сипатта. Бас прокуратураның дипфейк-жарнамаға қатысты хабарламасы [24] және дипфейк-технологиялар жаңа киберқатерлердің бірі ретінде аталған Үйлестіру кеңесінің материалы [25] Қазақстандағы ресми реакцияны көрсету үшін ғана пайдаланылды; олар сот немесе әкімшілік практикасының репрезентативті іріктемесін құрамайды. Нормативтік актілер мен ресми материалдар 2026 жылғы 1 қыркүйектегі жағдай бойынша, ғылыми әдебиет 2019–2026 жж. аралығында іріктелді. Қорытынды корпус 30 дереккөзден тұрады: 12 қазақстандық нормативтік-құқықтық дереккөз, 4 халықаралық немесе шетелдік акт пен ресми материал, Қазақстанның 4 ресми және ғылыми-практикалық материалы және 10 ғылыми еңбек. Іріктеу өлшемдері – дереккөздің ресми немесе рецензияланатын болуы, тақырыпқа тікелей қатыстылығы және құқықтық мәртебесінің тексерілуі.

ЕО, АҚШ және Ұлыбритания салыстыру үшін әртүрлі реттеушілік модельдерді көрсетуіне байланысты таңдалды: жалпы ашықтық міндеттері; қылмыстық тыйым мен жәбірленуші бастайтын жою рәсімінің ұштасуы; келісімсіз интимдік синтетикалық бейнені жасауды нысаналы криминализациялау. Кестелер статистикалық емес, авторлық талдамалық матрицалар болып табылады. 1-кесте «қорғалатын игілік – қолданыстағы құқықтық кіру нүктесі – олқылық», 2-кесте «анықтау тәсілі – анықталатын белгі – құқықтық маңызы мен шегі», 3-кесте «дипфейк санаты – ықтимал қылмыстық-құқықтық модель – міндетті шектеушілер», 4-кесте «юрисдикция – реттеу нысаны – ашықтық немесе жою – жауаптылық шегі» өлшемдері бойынша жасалды. Осы өлшемдер мен кестелерде көрсетілген баптарға жүгіну қорытындыларды қайта тексеруге мүмкіндік береді.

Зерттеудің әдіснамалық шектеулері – Қазақстан бойынша дипфейк істерінің авторлық эмпирикалық массивінің, арнайы жіктелген ресми статистиканың және анықтау жүйелерінің дәлдігін авторлық эксперимент арқылы тексерудің болмауы. Мақала дипфейкке қатысты істер мүлде жоқ деп мәлімдемейді; ашық ресми дереккөздерден дипфейк белгісі бойынша бөлінген сот, әкімшілік немесе платформалық статистикалық қатар анықталмағанын көрсетеді. Сондықтан қорытындылар нормативтік, доктриналық және салыстырмалы сипатқа ие, ал техникалық анықтау тәсілдері олардың құқықтық қолданылу шектері тұрғысынан бағаланады.

Нәтижелер және талқылау

Дипфейктің құқықтық мәні бар белгілері

Бұл мақалада сабақтас ұғымдар ажыратылады. «Синтетикалық нәтиже» – «Жасанды интеллект туралы» Заңның 1-бабының 4) тармақшасындағы кең құқықтық санат [8], ал «синтетикалық контент» – осындай нәтиженің аудио-, бейне- немесе кескін нысанын сипат-

тайтын, дербес құқық бұзушылық құрамын білдірмейтін жалпы атау. «Синтетикалық имитация» – тұлғаның, объектінің, орынның немесе оқиғаның белгілерін алгоритмдік жолмен еліктеу тәсілі; «дипфейк» – сол тәсілмен жасалған, шынайы көрінетін және адресатты адастыруға қабілетті контенттің тар түрі. Бұл түсінік ЕО-ның Жасанды интеллект туралы актісінің (AI Act) 3(60)-бабындағы анықтамамен үйлеседі [20]. «Жалған ақпарат» – «Онлайн-платформалар және онлайн-жарнама туралы» Заңның 1-бабының 3) тармақшасындағы санат [9], ал «дезинформация» – қасақана адастыруды білдіретін доктриналық ұғым. TAKE IT DOWN Act-тегі «цифрлық қолдан жасау» жасанды интеллектпен шектелмейтін келісімсіз интимдік бейнені қамтиды [22]. «Манипуляциялық контент» материалдың ықпал ету сипатын білдіреді, бірақ өздігінен құқық бұзушылық құрамын құрмайды.

Зерттеудің бірінші нәтижесі – дипфейктің құқықтық белгілерін бөліп көрсету. Алгоритмдік құралмен жасалған немесе өзгертілген кез келген аудио-, фото- не бейнемазмұн автоматты түрде құқыққа қайшы дипфейк болмайды. Өзгеше түсіндіру шығармашылық еркіндікке, сатираға, білім беруге, кинематографияға, журналистік реконструкцияға және жасанды интеллектіні адал пайдалануға негізсіз шектеу қояды.

Бірінші белгі – тұлғаның танылуы. Материал нақты адамды тікелей немесе жанама түрде тануға мүмкіндік беруі керек: беті, дауысы, денесі, аты, лауазымы, әлеуметтік контексті немесе белгілер жиынтығы арқылы. Танылу болмаса, нақты ар-намысқа, қадір-қасиетке, бейнеге немесе жеке өмірге қол сұғу болмайды.

Екінші белгі – синтетикалық имитация. Дипфейк жай ғана жалған мәлімдеме хабарламайды, ол тұлға сөйлегендей, әрекет жасағандай, қатысқандай, келіскендей немесе оқиғаға араласқандай көрініс жасайды. Осы ерекшелік дипфейкті кәдімгі жала жабудан, қорлаудан немесе мәтіндік дезинформациядан ажыратады.

Үшінші белгі – келісімнің болмауы немесе келісім шегінен шығу. Интимдік, репутациялық зиян келтіретін және коммерциялық тұрғыда пайдаланылатын дипфейктер үшін келісім айқын, нақты және бейнені пайдалану тәсілін қамтитын болуға тиіс. Фотосуретті әлеуметтік желіде жалпы орналастыру порнографиялық, қорлайтын немесе алаяқтық синтетикалық видео жасауға келісім дегенді білдіре алмайды.

Төртінші белгі – зиян немесе зиян тәуекелі. Азаматтық-құқықтық қорғау жеке мүліктік емес құқықтың бұзылу қаупі болған кезде-ақ іске қосылуы мүмкін, әсіресе контент онлайн таралса. Қылмыстық-құқықтық реакция анағұрлым жоғары шекті талап етеді: интимдік сипат, пайдакүнемдік мақсат, бопсалау, жаппай тарату, елеулі зиян келтіру, қоғамдық қауіпсіздікке араласу, кәмелетке толмаған адамды пайдалану немесе ұйымдасқан сипат.

Бесінші белгі – адастыратын сипат. Егер синтетикалық материал пародия, көркем шығарма немесе оқу реконструкциясы ретінде анық таңбаланса және жеке немесе жария зиян келтірмесе, құқықтық реакция ең төменгі деңгейде болуға тиіс. Керісінше, реалистік имитация кезінде таңбалаудың болмауы жауаптылық тәуекелін күшейтеді.

Осы бес белгіні біріктіре отырып, осы зерттеуде тұлғалық дипфейк деп нақты адамның бейнесін, дауысын, мінез-құлқын не өзге дараландыру белгілерін шынайы көрінетіндей имитациялайтын жасанды немесе өзгертілген аудио-, бейне- не кескін-контент түсініледі. Оның құқықтық қауіптілігі танылу, келісімнің болмауы не оның шегінен шығу, адастыру және жеке немесе жария зиян қаупі арқылы бағаланады. Объектіні, орынды не оқиғаны имитациялаған материал үшін танылу мен келісім емес, оның түпнұсқа ретінде қабылдану ықтималдығы және қорғалатын мүддеге зиян келтіру қаупі шешуші болады.

Қолданыстағы қазақстандық құқық: қорғау бар, бірақ ол салалар бойынша бөлшектенген

Қазақстандық құқықта дипфейктерге қолданылуы мүмкін бірнеше тетік бар. Бірақ олар әртүрлі логика бойынша жұмыс істейді және жәбірленушіні қорғаудың бірыңғай жүйесіне әрдайым біріге бермейді.

Қолданыстағы құқық таңбалау мәселесінде үнсіз емес. «Жасанды интеллект туралы» Заңның 1-бабының 4) тармақшасы синтетикалық нәтижені заңдық ұғым ретінде бекітеді. Заңның 21-бабының 2-тармағы оны машиналық оқылатын нысанда таңбалап, пайдаланушы қабылдайтын ескертумен сүйемелдеуді міндеттейді, ал 3-тармақ пайдаланушыларды хабардар ету міндетін жасанды интеллект жүйесінің меншік иелері мен иегерлеріне жүктейді. Заңның 24-бабы келтірілген зиянды азаматтық заңнамаға сәйкес өтеуді көздейді [8]. Осы міндеттерді

бұзудың жекелеген нысандары ӘҚБтК-нің 641–1-бабымен қамтылады; істерді жасанды интеллект саласындағы уәкілетті орган 692–3-бап бойынша қарайды [7]. 2026 ж. 1 қыркүйектегі қолданыстағы редакция бойынша 21-баптағы машиналық оқылатын таңба мен пайдаланушыға түсінікті ескерту талабы сақталған [8].

Сабақтас режимдер де қолданылады. «Онлайн-платформалар және онлайн-жарнама туралы» Заңның 11-бабы шағымға жиырма күн ішінде дәлелді жауап беруді, 15-бабы жалған ақпаратты жоюды талап ету және бас тартылған жағдайда сотқа жүгіну мүмкіндігін көздейді; 14-бап құқыққа қайшы контент айналымын тоқтатудың жалпы негіздерін белгілейді [9]. Азаматтық кодекстің 143–145-баптары ар-намысты, қадір-қасиетті, жеке өмірді және бейнеге құқықты қорғайды [2]. Кодекстің Ерекше бөліміндегі 951–952-баптар моральдық зиянды өтеуді реттейді [3]. «Дербес деректер және оларды қорғау туралы» Заң сәйкестендірілген немесе сәйкестендіруге болатын тұлға туралы мәліметтерді қорғаудың арнайы режимін белгілейді [26]. Қылмыстық кодекстің 147, 190, 194 және 274-баптары жеке өмірге қол сұғуды, алаяқтықты, бопсалауды және көрінеу жалған ақпаратты тиісті құрам белгілері болғанда қамтиды [6]. Демек анықталған олқылық қорғаудың мүлдем болмауында емес, дипфейкті саралаудың, шұғыл шектеудің, цифрлық дәлелдемелерді сақтаудың және осы режимдерді өзара байланыстырудың бірыңғай рәсімінің жоқтығында.

1-кестеде көрсетілгендей, бір дипфейк бір мезгілде ар-намыс пен қадір-қасиетке, бейнеге, жеке өмірге, дербес деректерге, мүліктік мүдделерге және қоғамдық қауіпсіздікке әсер етуі мүмкін. Мәселе қолданыстағы нормалардың синтетикалық имитация тәсілінің өзіне қарағанда көбіне түпкі зиянға жауап беруінде.

Кесте 1 – Дипфейктер және Қазақстан Республикасының қолданыстағы құқықтық тетіктері

Зиян түрі	Қолданыстағы құқықтық кіру нүктелері	Негізгі олқылық
Синтетикалық бейне немесе аудио арқылы беделге қасақана нұқсан келтіру	Ар-намысты, қадір-қасиетті және іскерлік беделді қорғау [2]. Жала жабу үшін әкімшілік жауаптылық [7]. Көрінеу жалған ақпаратқа қатысты қылмыстық норма [6].	Дипфейк сөздік мәлімдемесіз әрекетті еліктету мүмкін; теріске шығару стандарты синтетикалық бейнеге әрдайым сәйкес келмейді
Келісімсіз интимдік дипфейк	Жеке өмір мен бейнеге құқық [2]. Моральдық зиянды өтеу [3]. Жеке өмірге қол сұғу мен дербес деректерді заңсыз пайдалануға қатысты қылмыстық норма [6].	Келісімсіз интимдік синтетикалық бейненің заңсыздығы туралы арнайы презумпция жоқ
Алдау үшін дауыс немесе бейнені еліктету	Алаяқтық пен бопсалау [6]. Жасанды интеллект ашықтығы [8]. Онлайн-платформалар режимі [9]. Дербес деректерді қорғау [26].	Дипфейкті қолдану саралаушы белгі ме, әлде тек жасау тәсілі ме екені әрдайым анық емес
Дағдарыс жағдайындағы синтетикалық дезинформация	Көрінеу жалған ақпарат пен қоғамдық қауіпсіздікке қатысты қылмыстық нормалар [6]. Онлайн-платформалар режимі [9].	Қауіптіліктің жоғары шегі қажет, әйтпесе пікір білдіруді шамадан тыс шектеу тәуекелі туындайды
Платформаларда зиянды дипфейктің жаппай таралуы	Онлайн-платформалар туралы заң [9]. Жасанды интеллект ашықтығы талаптары [8]. Әкімшілік құрамдар [7].	Жылдам жою, дәлелдемелерді сақтау және қайта жүктеудің алдын алу рәсімдері қажет
Ескертпе: Авторлар [2, 3, 6–9, 26] дереккөздер негізінде құрастырған.		

Қолданыстағы нормалардан екі қорытынды шығады. Біріншіден, азаматтық қорғау ар-намыс, қадір-қасиет, бейне, жеке өмір және моральдық зиянды өтеу құралдары арқылы іске асуы мүмкін [2, 3], бірақ синтетикалық бет-әлпет пен дауысты пайдалану, жедел жою және цифрлық іздерді сақтау арнайы нақтыланбаған. Екіншіден, ҚК-нің 147, 190, 194 және 274-баптары нақты құрам белгілері болғанда қолданылады [6], алайда әрбір дипфейк қылмыс емес. Сондықтан төменде азаматтық қорғау кең әрі қалпына келтіруші, ал қылмыстық реакция нысаналы әрі жоғары қоғамдық қауіпті жағдайларға арналған модель ретінде ажыратылады.

Қазақстандағы құқық қорғау органдарының ресми материалдары

Қазақстан Республикасы Бас прокуратурасының 2026 ж. ресми хабарламасында «Право Онлайн І Консультации и Поддержка» атауымен тараған және 240 мыңнан астам қаралым жинаған бейнероликте прокуратура қызметкерінің бейнесі жасанды интеллект көмегімен имитацияланып, азаматтарды кейіннен ақша жымқыру мақсатында жаңылыстыруға бағытталғаны көрсетілді. Бас прокуратураның тапсырмасымен Ішкі істер министрлігі материалды жасаған және таратқан тұлғаларды анықтау үшін тексеру ұйымдастырған [24]. Бұл – сот актісі де, кінәлілік туралы түпкілікті қорытынды да емес; ол тек тексеруге бастамашылық жасалғанын растайтын құқық қорғау органының ресми хабарламасы.

Бас прокуратура жанындағы Үйлестіру кеңесінің 2026 ж. 17 сәуірдегі отырысы туралы материалда дипфейк-технологиялар 18 жаңа киберқатердің бірі ретінде аталды. Сол дереккөзде 2026 ж. киберқұқық бұзушылықтар саны 15,1%-ға, яғни 6 216-дан 5 275-ке дейін азайғаны, ҚК-нің 232-1-бабы бойынша 446 іс тіркелгені және Антифрод-орталықтың алаяқтық операцияларға байланысты 2,8 млрд теңгені бұғаттағаны хабарланды [25]. Бұл көрсеткіштер дипфейк фактілерінің саны емес; олар дипфейк қолданылуы ықтимал сабақтас киберқылмыстық ортаның жалпы сипаттамасын ғана береді.

2026 ж. 1 қыркүйектегі жағдай бойынша ашық ресми дереккөздерден дипфейк белгісі бойынша бөлек жүргізілетін сот, әкімшілік, құқық қорғау немесе платформалық шағым статистикасы анықталмады. Сондықтан жоғарыда келтірілген көрсеткіштер дипфейк фактілерінің саны ретінде түсіндірілмейді, ал мақала қалыптасқан біркелкі сот немесе әкімшілік практика бар деп мәлімдемейді. Арнайы жіктелген статистиканың болмауы құбылыстың ауқымын сандық бағалауды шектейді, бірақ ресми дипфейк жағдайын, сабақтас киберқылмыстық көрсеткіштерді және отандық мониторинг пен фактчекинг жобаларын функционалдық тұрғыдан жүйелеуге кедергі келтірмейді.

Дипфейктерді анықтау және цифрлық дәлелдемелерді бекіту

Дипфейктің синтетикалық сипатын анықтау құқықтық саралаудың бастапқы кезеңі, бірақ автоматтандырылған анықтау сервисі берген ықтималдық бағасы құқық бұзушылықты, контент авторын немесе тұлғаның кінәсін өздігінен дәлелдемейді. Қазақстандық зерттеу технологиялық анықтау мен түпнұсқалықты бағалауды құқықтық қарсы іс-қимылдың бір бөлігі ретінде көрсетеді [16, 192, 194–195 бб.]. Қолданылатын тәсілдер бейнеартефактілерді, кадрлар арасындағы сәйкессіздіктерді, бет қимылы мен микроэкспрессияларды, аудионың спектралдық және просодикалық белгілерін, файл метадеректерін, сондай-ақ дыбыс пен бейненің сәйкестігін талдауы мүмкін [17, 1–4 бб.]. Нәтиже оқыту деректеріне, белгісіз генераторларға, файлдың сығылуына және кейінгі өңделуіне тәуелді; сондықтан модельдің жалпылау қабілеті мен орнықтылығы тексерілуге тиіс [18, 9–13 бб.].

Дипфейкті автоматтандырылған анықтау жүйесінің қорытындысы бағдарлаушы техникалық нәтиже ретінде қарастырылуға тиіс. Оның дәлелдемелік маңызы бастапқы файл сақталған, хэш-мәні есептелген, алу уақыты мен тәсілі тіркелген, қолданылған құралдың атауы мен нұсқасы, модель, сенімділік көрсеткіші және шекті мәні көрсетілген жағдайда ғана бағаланады. Қылмыстық процесте мұндай деректер ҚПК-нің 111-бабына сәйкес заңды түрде алынуға және 125-бап бойынша өзге дәлелдемелермен жиынтықта бағалануға тиіс; арнайы білім қажет болғанда синтетикалық өзгерту белгілері 116-бапқа сәйкес сарапшы қорытындысы арқылы тексеріледі [27]. Азаматтық процесте электрондық материалдың түпнұсқалығы мен өзгертілуі туралы дау АПК-нің 92 және 100-баптары шегінде сараптама және жазбаша немесе электрондық дәлелдемелер арқылы шешіледі [28].

Қазақстандағы ашық жарияланған бастамалардың функциялары бірдей емес. 2025 жылғы материалда Мәдениет және ақпарат министрлігі фейк-контент пен дипфейктерді автоматты түрде анықтауға арналған цифрлық бастама әзірлеп жатқаны хабарланған. Оның практикалық алғышарты ретінде «Мерген» жасанды интеллект жүйесінің ақпараттық кеңістікке автоматты мониторинг жүргізіп, заңсыз интернет-ресурстарды, соның ішінде есірткі интернет-дүкендерін тікелей және жанама белгілер бойынша анықтайтыны көрсетілген; 5 000-шы осындай ресурс жабылған. Дипфейктерді анықтау функциясын қосу үшін үлкен тілдік модельдің (LLM) әлі оқытылып жатқаны хабарланған [29]. Сондықтан «Мергенді» қазірдің өзінде жұмыс істейтін немесе сот-сараптамалық тұрғыдан валидацияланған дипфейк-детектор деп сипаттауға болмайды. Оның нәтижесі ықтимал тәуекел нүктесін көрсететін бағдарлаушы сигнал ретінде

пайдаланылуы мүмкін, бірақ бастапқы файлды зерттеуді, алу-сақтау тізбегін және сарапшы қорытындысын алмастырмайды.

AI-Derek RasInfo мобильді ресурсына интеграцияланған, қазақ, орыс және ағылшын тілдерінде жұмыс істейтін фактчекинг пен медиасауаттылық құралы болып табылады. Ол жалған ақпаратты тексеру жөніндегі сұрақтарға жауап береді және журналистерге, ғалымдарға, оқытушыларға, студенттерге және өзге пайдаланушыларға бағытталған [30]. Ашық сипаттамада AI-Derek/RasInfo жүйесінің аудио- немесе бейнефайлдың синтетикалық өзгертілуін сот-сараптамалық деңгейде тікелей анықтайтыны не оның қателік көрсеткіштері жарияланғаны көрсетілмеген. Демек, оның нәтижесі бастапқы верификация мен кейінгі тексеру бағытын таңдауға қызмет етеді, бірақ сот үшін бастапқы файлды, метадеректерді, қолданылған әдістемені және сараптамалық қорытындыны ұсыну қажеттігін жоймайды.

Кесте 2 – Дипфейктерді анықтау тәсілдері және олардың құқықтық маңызы

Анықтау тәсілі	Не анықтайды	Құқықтық маңызы және шегі
Бейнеартефактілерді талдау	Монтаж шекараларын, жарық, текстура және кадрлар арасындағы сәйкессіздіктерді	Синтетикалық өзгерту туралы бастапқы болжам береді; жеке өзі түпкілікті дәлел емес
Бет қимылы мен микроэкспрессияларды талдау	Табиғи емес мимиканы, жыпылықтау мен қозғалыс сәйкессіздігін	Сараптамалық тексеруге бағыт береді; бейненің сапасына тәуелді
Аудио-спектралдық және просодикалық талдау	Дауыс синтезі, тембр, жиілік, ырғақ және үзіліс аномалияларын	Аудиоматериалды тексеруге негіз болады; салыстыру үлгілері қажет
Метадеректер, файл құрылымы және хэш-мән	Файлдың жасалу немесе өңделу тарихы мен бүтіндігін	Алу-сақтау тізбегін бекітеді; метадеректің болмауы дипфейкті автоматты түрде дәлелдемейді
Мультимодальдық талдау	Ерін қимылы, мимика, дауыс пен бейненің сәйкестігін	Кешенді бағалауды күшейтеді; нәтиже модель мен деректер жиынына тәуелді
Ескертпе: Авторлар [16–18] дереккөздер негізінде құрастырған.		

Көрсетілген тәсілдер ықтималдық бағасын береді және бастапқы файлды, алу-сақтау тізбегін, сараптамалық тексеруді және өзге дәлелдемелерді алмастырмайды.

Қазақстан жағдайындағы құқықтық іс-қимыл алгоритмі

Ұсынылатын алгоритм тоғыз өзара байланысты кезеңнен тұрады: 1) материалды анықтау және URL, жариялау уақыты мен аккаунт туралы деректерді тіркеу; 2) бастапқы файлды алу, хэш-мәнін есептеу және техникалық тексеру; 3) скриншоттарды, метадеректерді, таралу іздерін және көшірмелерді бекіту, контентті жасаушыны немесе таратушыны анықтауға қажетті платформалық деректерді сақтау; 4) платформаға дәлелді хабарлама жіберу; 5) жоғары тәуекелді контентке қолжетімділікті уақытша шектеу және оны жою туралы мәселені шешу; 6) қылмыс белгілері болғанда құқық қорғау органына хабарлау; 7) қажет болған жағдайда сот сараптамасын тағайындау; 8) әрекетті азаматтық, әкімшілік не қылмыстық-құқықтық тұрғыдан саралау; 9) контентті жою, теріске шығару, моральдық зиянды өтеу және қайта жүктеуді шектеу арқылы жәбірленушінің құқықтарын қалпына келтіру. Жедел шектеу дәлелдемелер сақталғаннан кейін немесе оларды қатар сақтай отырып жүргізілуге тиіс.

Азаматтық-құқықтық модель: шұғыл қорғау, жою, өтемақы

Зерттеудің екінші нәтижесі – арнайы азаматтық-құқықтық тетіктің қажеттігі туралы қорытынды. Оның міндеті әрбір жағдай үшін бөлек «дипфейк деликтін» жасау емес. Неғұрлым дәл конструкция – тұлғаның цифрлық бірегейлігін келісімсіз синтетикалық имитациядан арнайы қорғау.

Бірінші элемент – тұлғаның бейнесі мен оны сәйкестендіруге мүмкіндік беретін белгілерді кең мағынада түсіну. Азаматтық заңнама тек фотографиялық бейнені ғана емес, синтетикалық түрде жаңғыртылған бет-әлпетті, дауысты, денені, мимиканы, сөйлеу мәнерін, есімді, лауазымды немесе тұлғаны тануға мүмкіндік беретін өзге де белгілер жиынтығын қамтуға тиіс. Әйтпесе ең зиянды дипфейк дәл «шынайы емес» болғандықтан жауаптылықтан тыс қалады.

Екінші элемент – интимдік және анық қорлайтын синтетикалық контент үшін келісімнің болмауы презумпциясы. Егер жауапкер керісінше дәлелдеме ұсынбаса, жәбірленуші порнографиялық немесе қорлайтын дипфейк жасауға келісім бермегенін дәлелдеуге міндетті болмауға тиіс. Мұнда дәлелдеудің әдеттегі логикасы әділетсіз: зиян келтіруші жасау және тарату процесін бақылайды, ал жәбірленуші бұзушылық туралы жарияланғаннан кейін ғана біледі.

Үшінші элемент – шұғыл соттық немесе соттан тыс жою. Дипфейктер үшін уақыт зияннның бір бөлігі болып табылады. Егер ролик вирустық түрде таралып үлгерсе, бір жылдан кейінгі өтемақы беделді қалпына келтірмейді. Сондықтан уақытша шаралардың арнайы тәртібі қажет: одан әрі таратуға тыйым салу, бастапқы жарияланымды жою, көшірмелерге қолжетімділікті шектеу, платформаға техникалық деректер мен материал хэшін сақтауды ұйғару.

Төртінші элемент – таңбалауға, теріске шығаруға және аудиторияны хабардар етуге құқық. Кейбір жағдайларда жай ғана жою зиянды жоймайды: көрермендер материалды көріп қойған және оны шындық ретінде қабылдаған. Жәбірленушіге материал таралған сол цифрлық арнада контенттің синтетикалық сипаты туралы теріске шығару немесе хабарлама орналастыруды талап ету мүмкіндігі берілуге тиіс.

Бесінші элемент – цифрлық масштабты ескере отырып моральдық зиянды өтеу. Жоғарғы Соттың нормативтік қаулысы сотқа таратылған мәліметтердің сипатын, мазмұнын, таралу шектерін және өзге де мән-жайларды ескеруді жүктейді [5]. Дипфейк дауларында осы жалпы өлшемдер аудитория қамтылуын, таралу ұзақтығын, қайта жарияланымдарды, контенттің интимдік сипатын, жәбірленушінің жасын, оның лауазымдық немесе әлеуметтік мәртебесін пайдалануды, коммерциялық пайдалануды және хабарламадан кейін жауапкердің мінез-құлқын ескере отырып қолданылуға тиіс.

Алтыншы элемент – мұрагерлер мен жақын адамдарды қорғау. Қайтыс болған адамдардың дипфейктері алаяқтық, саяси манипуляция, естелікті қорлау, коммерциялық пайдалану немесе туыстарына қысым жасау үшін қолданылуы мүмкін. Азаматтық құқық дипфейк отбасының қадір-қасиетіне немесе қоғамдық мүддеге әсер етсе, мұндай контентті жоюды және қайтыс болған адамның естелігін қорғауды кім талап ете алатынын көздеуге тиіс.

Бұл модель қолданыстағы Азаматтық кодекске қайшы келмейді. Ол жеке мүліктік емес құқықтар, бейне және жеке өмір туралы нормаларды дамытады [2]. Моральдық зиянды өтеу тетігі Азаматтық кодекстің Ерекше бөлімінде бекітілген [3]. Бірақ арнайы цифрлық нақтылаусыз жәбірленуші дипфейкті басқа зиян түріне арналған конструкцияларға күштеп сыйғызуға мәжбүр болады.

Қылмыстық-құқықтық модель: жалпы тыйым емес, нысаналы арнайы құралдар

Үшінші нәтиже – барлық дипфейкті дербес қылмысқа айналдырмайтын нысаналы қылмыстық-құқықтық өлшемдерді негіздеу. Қолданыстағы ҚК нақты құрам белгілері бар жеке өмірге қол сұғу, алаяқтық, бопсалау және көрінеу жалған ақпарат жағдайларына бірінші кезекте қолданылуға тиіс. Сонымен бірге келісімсіз интимдік дипфейк, кәмелетке толмаған адамның бейнесін сексуалдандырылған контексте пайдалану, алаяқтық не бопсалау мақсатындағы имитация және қоғамдық қауіпсіздікке елеулі қатер төндіретін имитация үшін нысаналы арнайы құралдардың қажеттілігі негізді. Олардың нақты нысаны – дербес құрам, саралаушы белгі немесе қолданыстағы нормаларды арнайы түсіндіру – эмпирикалық және құқық қолдану материалдары негізінде айқындалуға тиіс.

3-кестеде қылмыстық-құқықтық шек қорғалатын объект, әрекет, қасақаналық, арнайы мақсат және нақты зиян не оның жоғары қаупі арқылы белгіленеді. ҚК-нің 147, 190, 194 және 274-баптары тиісті құрам белгілері болғанда бірінші кезекте қолданылуға тиіс. Нысаналы арнайы құралдардың қажеттілігі жоғары қауіпті жағдайлар үшін негізделеді, ал олардың дербес құрам немесе саралаушы белгі түріндегі нақты нысаны қолданыстағы нормалардың құқық қолданудағы жеткіліктілігі бағаланғаннан кейін айқындалуға тиіс [6].

Нысаналы арнайы қылмыстық-құқықтық құралдарды қарастыру төрт топқа қатысты негізді: келісімсіз интимдік дипфейк; кәмелетке толмаған адамның бейнесін сексуалдандырылған контексте пайдалану; алаяқтық немесе бопсалау үшін тұлғаны синтетикалық имитациялау; қоғамдық қауіпсіздікке нақты қатер төндіретін материал. Зорлық-зомбылықты немесе топаралық өшпенділікті арандататын материалдарға ҚК-дегі қолданыстағы нормалар қолданылуға тиіс, ал синтетикалық тәсіл саралау кезінде ескеріледі. Интимдік дипфейк үшін келісімнің болмауы

мен қасақаналық шешуші [22; 23]. Алаяқтықта дипфейкті пайдалану қолданыстағы құрам шегінде қылмыс жасау тәсілі ретінде бағаланып, құқық қолдану материалдары жеткілікті болғанда саралаушы белгі ретінде қарастырылуы мүмкін. Қоғамдық қауіпсіздік жағдайында нақты қауіп, арандату немесе дүрбелең тәуекелі дәлелденуге тиіс; сатира, өнер, білім беру және адал журналистика бұл шекке кірмейді.

Кесте 3 – Дипфейктерге қатысты қылмыстық-құқықтық реакцияның ұсынылатын өлшемдері

Дипфейк санаты	Ықтимал қылмыстық-құқықтық модель	Міндетті шектеушілер
Танылатын тұлғаның келісімсіз интимдік дипфейгі	ҚК-нің 147-бабын қолдану; оның жеткіліксіздігі дәлелденсе, арнайы құрам не саралаушы белгі	Тұлғаның танылуы, келісімнің болмауы, интимдік сипат, жасауға немесе таратуға қасақаналық
Кәмелетке толмаған адамның бейнесін сексуалдандырылған контексте пайдалану	Қолданыстағы қорғау нормаларын қолдану; олардың жеткіліксіздігі дәлелденсе, арнайы құрам не саралаушы белгі	Жәбірленушінің жасы, сексуалдандырылған сипат, тарату мақсатымен жасау, сақтау немесе тарату
Алаяқтық немесе бопсалау үшін дипфейк	ҚК-нің 190 немесе 194-бабын қолдану; дипфейкті ықтимал саралаушы белгі ретінде бағалау	Пайдакүнемдік мақсат, тұлғаны имитациялау арқылы алдау, мүліктік зиян келтіру немесе мүлікті беруді талап ету
Дағдарыс жағдайында мемлекеттік орган немесе лауазымды адам атынан жасалған дипфейк	ҚК-нің 274-бабын қолдану; қоғамдық қауіпсіздікке елеулі қатер үшін ықтимал саралаушы белгі	Дүрбелеңнің, қоғамдық тәртіптің бұзылуының, денсаулыққа немесе қауіпсіздікке зиянның нақты мүмкіндігі
Зорлық-зомбылықты немесе топаралық өшпенділікті арандататын дипфейк	ҚК-дегі қолданыстағы нормаларды қолдану; синтетикалық тәсілді саралау кезінде ескеру	Қасақаналық, қауіпті контекст, өшпенділік немесе зорлық-зомбылық қоздыруға бағытталу
Сатиралық, көркем, білім беру мақсатындағы, анық таңбаланған дипфейк	Арнайы «дипфейк жасау» құрамы қолданылмайды	Анық таңбалау, интимдік немесе алаяқтық сипаттың болмауы, қорғалатын игіліктерге нақты қатердің болмауы
Ескертпе: Авторлар Қазақстан ҚК-нің нормалары және АҚШ пен Ұлыбританияның нысаналы модельдері негізінде құрастырған [6, 22, 23].		

Қазақстан, ЕО, АҚШ және Ұлыбритания: реттеу тетіктерін салыстыру

Кесте 4 – Дипфейктерді реттеудің салыстырмалы құқықтық модельдері

Юрисдикция	Негізгі режим	Ашықтық немесе жою	Жауаптылық және шегі
Қазақстан	«Синтетикалық нәтиже» заңда бекітілген; арнайы «дипфейк» ұғымы жоқ [8]	21-бап - таңба және ескерту; платформалық шағымның жалпы тәртібі бар [8; 9]	ӘҚБтК 641-1; азаматтық және қылмыстық жалпы нормалар; бірыңғай шұғыл рәсім жоқ [2; 3; 6; 7]
Еуропалық Одақ	AI Act 3(60) – deep fake ұғымы [20]	50(2), 50(4) - таңбалау және ашу; мөлшерлі ерекшеліктер	Негізгі акцент - ашықтық; жою мен өтем өзге нормаларға тәуелді
АҚШ	Интимдік digital forgery [22]	Жарамды талап алынғаннан кейін 48 сағат ішінде контентті және оның бірдей көшірмелерін жою	Қасақана келісімсіз интимдік жариялау; барлық дипфейк қамтылмайды
Ұлыбритания	Purported intimate image [23]	Жалпы таңбалау емес, интимдік бейнені жасауға нысаналы тыйым	Арнайы қылмыстық жауаптылық және reasonable excuse кепілдігі
Ескертпе: Авторлар Қазақстан, ЕО, АҚШ және Ұлыбритания актілері негізінде құрастырған [7–9; 20; 22; 23].			

Салыстыру Қазақстан үшін шетелдік мерзімдер мен құрамдарды механикалық көшіру қажеттігін білдірмейді. Қазақстандағы қолданыстағы таңбалау [8] мамандандырылған хабарлау, уақытша шектеу, дәлелдемелерді сақтау және шағымдану кепілдіктерімен толықтырылуға тиіс. ЕО-ның ашықтық тәсілі [20], АҚШ-тың жәбірленуші бастайтын жоюы [22] және Ұлыбританияның нысаналы криминализациясы [23] осы тетіктердің жекелеген салыстырмалы үлгілері болып табылады.

Платформалық деңгей: таңбалау жәбірленушіні жоюсыз қорғамайды

Төртінші нәтиже – платформалық-әкімшілік деңгейдің қажеттігі туралы қорытынды. Азаматтық талап қою мен қылмыстық қудалау маңызды, бірақ олар жарияланғаннан кейінгі алғашқы сағаттар мәселесін шешпейді. Дипфейк негізгі зиянды таралу арқылы келтіреді. Сондықтан реттеу тек авторға ғана емес, тарату инфрақұрылымына да әсер етуге тиіс.

Қазақстанда таңбалауды енгізу авторлық ұсыныс емес: «Жасанды интеллект туралы» Заңның 21-бабы синтетикалық нәтижені машиналық оқылатын нысанда таңбалауды және пайдаланушыны хабардар етуді қазірдің өзінде міндеттейді [8], ал ӘҚБтК-нің 641-1-бабы тиісті бұзушылық үшін жауаптылық көздейді [7]. Қолданыстағы құқықтың элементтері – таңбалау мен хабардар ету. Осы мақаланың авторлық ұсынысы – мамандандырылған хабарлау рәсімін, жоғары тәуекелді материалға қолжетімділікті уақытша шектеуді, техникалық деректерді сақтауды, қайта жүктеуді болдырмауды және шешімге шағымдануды заңда нақтылау. Онлайн-платформалар туралы заңдағы жиырма күндік жауап беру мерзімі мен жалған ақпаратты жою рәсімі бұл мәселелерді арнайы реттемейді [9]. АҚШ-тағы 48 сағаттық мерзім Қазақстан үшін дайын норма емес, салыстырмалы бағдар ғана [22].

Сондықтан платформалық міндеттер төрт функцияны қамтуға тиіс.

Біріншісі – түсінікті хабарлау тетігі. Жәбірленуші дипфейк туралы жылдам хабарлап, бұзушылық негіздерін көрсетіп, танылу және келісімнің болмауы туралы ең төменгі дәлелдемелерді қоса алуы керек. Рәсім алғашқы кезеңде күрделі сараптаманы талап етпеуге тиіс.

Екіншісі – қолжетімділікті уақытша шектеу. Егер материал интимдік сипатта болса, алаяқтық үшін қолданылса, дағдарыс жағдайында мемлекеттік органның немесе лауазымды адамның атынан жасалғандай әсер қалдырса не қоғамдық зиянның айқын тәуекелін қамтыса, платформа түпкілікті тексеруге дейін қолжетімділікті жедел шектеуге міндетті болуға тиіс.

Үшіншісі – дәлелдемелерді сақтау. Бекітусіз жою жәбірленушіні азаматтық және қылмыстық қудалау мүмкіндігінен айырады. Платформа заң шегінде жарияланым, жүктеу уақыты, аккаунт, сілтемелер, материал хэші және қайталанған көшірмелер туралы техникалық мәліметтерді сақтауға тиіс.

Төртіншісі – қайта жүктеудің алдын алу. Ең зиянды контент айналар, жаңа аккаунттар, қиылған фрагменттер және өзгертілген файлдар арқылы қайта оралады. Сондықтан жою тетігі бірдей немесе елеулі түрде ұқсас көшірмелермен жұмыс істеуді қамтуға тиіс. Мұндай талап TAKE IT DOWN Act-інің 3-бөлімінде бірдей көшірмелерді жою міндеті түрінде бекітілген [22].

Бұл деңгей сот пен тергеуді алмастырмайды. Ол процестік кепілдіктерге кіріктірілуі тиіс: қате жоюға шағымдану мүмкіндігі, адал сатира мен журналистиканы қорғау, шамадан тыс мониторингті шектеу, дербес деректерді қорғау. Бірақ платформалық деңгейсіз азаматтық-құқықтық және қылмыстық-құқықтық қорғау кешігіп қалады.

Сөз бостандығы және шамадан тыс тыйым салу тәуекелі

Әрбір синтетикалық материал құқық бұзушылық емес. Пародия, сатира, өнер, білім беру, ғылыми зерттеу және адал журналистік реконструкция қоғамдық құндылыққа ие болуы мүмкін. Сондықтан құқықтық реакция танылатын тұлғаның құқықтарына қол сұғу немесе қоғамдық қауіпсіздікке нақты тәуекел болғанда ғана іске қосылуға тиіс.

Азаматтық қорғау үшін жеке мүліктік емес құқықты бұзу немесе оның нақты қаупі жеткілікті. Әкімшілік реакция таңбалау мен платформалық міндеттерді бұзуға бағытталады. Қылмыстық жауаптылық келісімсіз интимдік сипат, пайдакүнемдік мақсат, бопсалау, кәмелетке толмағанды пайдалану немесе қоғамдық қауіпсіздікке жоғары қатер сияқты белгілер болғанда ғана соңғы құрал ретінде қолданылуға тиіс.

Таңбалау материалды автоматты түрде заңды етпейді: ол адастыру тәуекелін азайтады, бірақ қадір-қасиетке, жеке өмірге немесе бейнеге қол сұғуды жоймайды. Арнайы рәсім қате

шектеуге шағымдануды, адал пайдалануды және санкциялардың мөлшерлестігін қамтамасыз етуге тиіс.

Қазақстанға арнайы тетіктер қажет пе?

Жүргізілген нормативтік және салыстырмалы талдау Қазақстанға қолданыстағы нормаларды алмастырмайтын нысаналы азаматтық-құқықтық, платформалық және жоғары қауіпті жағдайларға арналған қылмыстық-құқықтық құралдар қажет екенін көрсетеді. Бұл жалпы «дипфейк жасау» құрамын енгізуді білдірмейді: қолданыстағы құрамдар бірінші кезекте қолданылуға тиіс. Арнайы құралдың дербес құрам, саралаушы белгі немесе өзге нысан түріндегі нақты шегі қазақстандық сот материалдары, тергеу деректері және құқық бұзушылық статистикасы жүйелі талданғаннан кейін айқындалуға тиіс. Қазіргі дәлелдемелік база мұндай өлшемдерді негіздеуге жеткілікті, бірақ нақты санкцияны алдын ала белгілеуге жеткіліксіз.

Қазақстанда қылмыстық-құқықтық реакция қолданыстағы құрамдарды бірінші кезекте қолдануға негізделуге тиіс. Нысаналы арнайы құралдардың қажеттілігі келісімсіз интимдік дипфейкке, кәмелетке толмаған адамның бейнесін сексуалдандырылған контексте пайдалануға, алаяқтыққа немесе бопсалауға қызмет ететін имитацияға және қоғамдық қауіпсіздікке елеулі қатер төндіретін мемлекеттік орган не лауазымды адам атынан жасалған жалған хабарламаға қатысты негізді. Зорлық-зомбылықты немесе топаралық өшпенділікті арандату жағдайларында ҚК-дегі қолданыстағы құрамдар қолданылуға тиіс. Арнайы құралдың нақты нысаны мен санкциясы эмпирикалық және құқық қолдану материалдарына сүйеніп айқындалады; қалған жағдайларда азаматтық, әкімшілік және платформалық реакция жеткілікті.

Ұсынылатын модель үш деңгей түрінде баяндалуы мүмкін.

Бірінші деңгей – азаматтық-құқықтық. Ол синтетикалық цифрлық бірегейлікті қорғауды, интимдік және анық қорлайтын дипфейктер үшін келісімнің болмауы презумпциясын, шұғыл жоюды, қамтамасыз ету шараларын, моральдық зиянды өтеуді, теріске шығару және таңбалау құқығын, дәлелдемелерді сақтауды қамтиды.

Екінші деңгей – әкімшілік-платформалық. Ол заңда көзделген жағдайларда синтетикалық контентті міндетті таңбалауды, хабарлау және жою рәсімін, платформалардың айқын міндеттерді орындамағаны үшін жауаптылығын, техникалық деректерді сақтауды және қайта жүктеудің алдын алу тетіктерін қамтиды.

Үшінші деңгей – қылмыстық-құқықтық. Мұнда қолданыстағы қылмыс құрамдары бірінші кезекте қолданылады; жоғары қауіпті жағдайларға арналған нысаналы өлшемдер алдын ала әзірленуге тиіс. Ал дербес құрамды немесе саралаушы белгіні енгізу қолданыстағы нормалардың жеткіліксіздігі құқық қолдану материалдарымен дәлелденгенде ғана қарастырылуы мүмкін. Қылмыстық құқықты кез келген цифрлық қолдан жасауға дейін кеңейтпеу, керісінше қорғау объектісін, кінә нысанын, тәсілді, жәбірленушіні, салдарды және ерекшеліктерді дәл көрсету маңызды.

Үш деңгей мақсатымен, іске қосылу негізімен, құзыретті субъектісімен және құқықтық салдарымен ажыратылады. Азаматтық деңгейде құқығы бұзылған тұлға соттан контентті жоюды, таратуды тоқтатуды және талапты қамтамасыз етуді сұрай алады [2]. Моральдық зиянды өтеу талабы Азаматтық кодекстің Ерекше бөліміне негізделеді [3]. Әкімшілік деңгейде таңбалау және хабардар ету міндеті жасанды интеллект жүйесінің меншік иесіне немесе иегеріне жүктеледі [8], ал ӘҚБтК-нің 641–1-бабы бойынша істі 692–3-бапта көрсетілген уәкілетті орган қарайды [7]. Платформалық хабарламаны бастапқыда онлайн-платформа меншік иесі өңдейді [9]. Қылмыстық деңгейде сотқа дейінгі тергеп-тексеру органдары, прокурор және сот нақты қылмыс құрамының барлық белгілері болғанда әрекет етеді [6]. Бір оқиға бірнеше қорғау құралын туындатуы мүмкін, бірақ әр деңгей дербес заңдық негізге сүйенеді: таңбаның болмауы өздігінен қылмысқа айналмайды, ал азаматтық қалпына келтіру жария-құқықтық жауаптылықтың бар-жоғына автоматты түрде тәуелді емес.

Қорытынды

Зерттеу сұрағына берілген жауап: Қазақстанның азаматтық, әкімшілік, қылмыстық және ақпараттық-құқықтық тетіктері дипфейктерге ішінара қолданылады, бірақ тұлғаны синтетикалық имитациялауды, контенттің жедел таралуын және цифрлық іздердің жоғалу тәуекелін

бір рәсімде қамтымайды. Сондықтан барлық дипфейкке жалпы тыйым емес, келтірілген зиян мен қоғамдық қауіптілікке қарай сараланған құқықтық жауап қажет.

Зерттеу нәтижелері: 1) дипфейктің тұлғаның танылуы, синтетикалық имитация, келісімнің болмауы немесе оның шегінен шығу, зиян не зиян қаупі және адастыратын сипаттан тұратын құқықтық белгілері анықталды; 2) дипфейктің синтетикалық нәтиже және синтетикалық контент ұғымдарымен арақатынасы белгіленіп, синтетикалық имитация оны жасау тәсілі ретінде айқындалды; дипфейк жалған ақпараттан, дезинформациядан, цифрлық қолдан жасаудан және манипуляциялық контенттен ажыратылды; 3) Қазақстандағы қолданыстағы азаматтық, әкімшілік, қылмыстық және платформалық тетіктердің негізгі олқылықтары белгіленді; 4) бастапқы файлды, хэш-мәнді, метадеректерді, жариялау уақыты мен аккаунт деректерін жинау және сақтау проблемалары анықталды; 5) техникалық анықтау мен сот сараптамасының құқықтық маңызы, сондай-ақ «Мерген» мен AI-Derek/RasInfo нәтижелерінің бағдарлаушы сипаттағы дәлелдемелік шегі көрсетілді; 6) азаматтық, әкімшілік-платформалық және қылмыстық қорғаудың арақатынасы ұсынылды; 7) платформалық хабарлау, уақытша шектеу, дәлелдемелерді сақтау және қайта жүктеуді болдырмау жөніндегі ұсыныстар жасалды; 8) Қазақстан үшін анықтаудан жәбірленушінің құқықтарын қалпына келтіруге дейінгі кешенді модель қалыптастырылды.

Ұсынылған модельде азаматтық деңгей құқық бұзушылықты жедел тоқтатуға, контентті жоюға, теріске шығаруға және моральдық зиянды өтеуге бағытталады. Әкімшілік-платформалық деңгей қолданыстағы таңбалау талабын, хабарламаны қарауды, қолжетімділікті уақытша шектеуді және техникалық деректерді сақтауды қамтиды. Қылмыстық деңгейде қолданыстағы құрамдар бірінші кезекте қолданылып, келісімсіз интимдік дипфейк, кәмелетке толмаған адамның бейнесін сексуалдандырылған контексте пайдалану, алаяқтық, бопсалау және қоғамдық қауіпсіздікке елеулі қатер төндіретін имитация үшін нысаналы арнайы құралдар қарастырылуға тиіс; олардың нақты нысаны мен санкциясы эмпирикалық және құқық қолдану материалдары негізінде айқындалады. Бір оқиға бірнеше қорғау құралын туындатуы мүмкін, бірақ таңбаның болмауы өздігінен қылмыс болып табылмайды, ал азаматтық қорғау жария-құқықтық жауаптылықтың болуына тәуелді емес.

Қолданыстағы құқықтан айырмашылық әр ұсыныс бойынша мынадай: 1) «Жасанды интеллект туралы» Заң «синтетикалық нәтиже» ұғымын бекітеді [8], ал автор оны танылатын адамның бейнесін, дауысын, мінез-құлқын және өзге дараландыру белгілерін қамтитын тұлғалық дипфейк өлшемдерімен нақтылайды; 2) Азаматтық кодекс бейнені және жеке мүліктік емес игіліктерді қорғайды [2, 3], ал автор қорғау объектісін синтетикалық дауысқа және тұлғаны тануға мүмкіндік беретін өзге белгілерге кеңейтуді ұсынады; 3) онлайн-платформалар туралы заң шағымды қараудың және құқыққа қайшы контентке ден қоюдың жалпы тәртібін белгілейді [9], ал автор жоғары тәуекелді дипфейк үшін жедел хабарлау, уақытша шектеу, техникалық деректерді сақтау және қайта жүктеуді болдырмау рәсімін ұсынады; 4) ҚК-нің 147, 190, 194 және 274-баптары тиісті құрам белгілері болғанда қолданылады [6], ал автор жалпы «дипфейк жасау» құрамын емес, келісімсіз интимдік дипфейк, кәмелетке толмаған адамның бейнесін сексуалдандырылған контексте пайдалану, алаяқтық, бопсалау және қоғамдық қауіпсіздікке елеулі қатер төндіретін имитация үшін нысаналы қылмыстық-құқықтық өлшемдерді ұсынады.

Зерттеудің шектеулері – Қазақстан бойынша арнайы жіктелген статистиканың, репрезентативті сот практикасы массивінің және анықтау жүйелерін авторлық эксперимент арқылы бағалаудың болмауы. Бас прокуратура мен отандық жобалар туралы жария материалдар қауіптің ресми деңгейде танылғанын және практикалық жұмыс бағыттарын ғана көрсетеді, бірақ анықтау жүйелерінің сот-сараптамалық сенімділігін, нақты тұлғаның кінәсін немесе қалыптасқан сот практикасын дәлелдемейді [24, 25, 29, 30]. Кейінгі зерттеу сот және әкімшілік актілерді, сараптамалық қорытындыларды, платформалық шағымдарды және анықтау құралдарының нақты істердегі сенімділігін жүйелі жинауға бағытталуға тиіс.

ӘДЕБИЕТТЕР

1 Қазақстан Республикасының Конституциясы (2026 жылғы 15 наурыздағы республикалық референдумда қабылданған). URL: https://adilet.zan.kz/kaz/docs/K2600000000 (өтініш берілген күн: 01.09.2026)

2 Қазақстан Республикасының 1994 жылғы 27 желтоқсандағы № 268-XIII Азаматтық кодексі (Жалпы бөлім). URL: https://adilet.zan.kz/kaz/docs/K940001000_ (өтініш берілген күн: 01.09.2026)

3 Қазақстан Республикасының 1999 жылғы 1 шілдедегі № 409-I Азаматтық кодексі (Ерекше бөлім). URL: https://adilet.zan.kz/kaz/docs/K990000409_ (өтініш берілген күн: 01.09.2026)

4 Соттардың ар-намысты, қадір-қасиетті және іскерлік беделді қорғау жөніндегі заңнаманы қолдану туралы Қазақстан Республикасы Жоғарғы Сотының 2026 жылғы 20 мамырдағы № 3 нормативтік қаулысы. URL: https://adilet.zan.kz/kaz/docs/P260000003S (өтініш берілген күн: 01.09.2026)

5 Соттардың моральдық зиянды өтеу жөніндегі заңнаманы қолдануы туралы Қазақстан Республикасы Жоғарғы Сотының 2015 жылғы 27 қарашадағы № 7 нормативтік қаулысы. URL: https://adilet.zan.kz/kaz/docs/P150000007S (өтініш берілген күн: 01.09.2026)

6 Қазақстан Республикасының 2014 жылғы 3 шілдедегі № 226-V ҚРЗ Қылмыстық кодексі. URL: https://adilet.zan.kz/kaz/docs/K1400000226 (өтініш берілген күн: 01.09.2026)

7 Әкімшілік құқық бұзушылық туралы Қазақстан Республикасының 2014 жылғы 5 шілдедегі № 235-V ҚРЗ Кодексі. URL: https://adilet.zan.kz/kaz/docs/K1400000235 (өтініш берілген күн: 01.09.2026)

8 Жасанды интеллект туралы Қазақстан Республикасының 2025 жылғы 17 қарашадағы № 230-VIII ҚРЗ Заңы. URL: https://adilet.zan.kz/kaz/docs/Z2500000230 (өтініш берілген күн: 01.09.2026)

9 Онлайн-платформалар және онлайн-жарнама туралы Қазақстан Республикасының 2023 жылғы 10 шілдедегі № 18-VIII ҚРЗ Заңы. URL: https://adilet.zan.kz/kaz/docs/Z2300000018 (өтініш берілген күн: 01.09.2026)

10 Бисалиев М.С., Шакиров К.Н. Цифровые следы как фактор безопасности оборота персональных данных в сети Интернет // BULLETIN of L.N. Gumilyov Eurasian National University Law Series. – 2023. – Т. 142. – № 1. – С. 81–98. DOI: 10.32523/2616-6844-2023-142-1-81-98

11 Имангалиев Н.К., Темиржанова Л.А. Актуальные проблемы выявления и раскрытия уголовных правонарушений, совершаемых в сети Интернет // BULLETIN of L.N. Gumilyov Eurasian National University Law Series. – 2022. – Т. 138. – № 1. – С. 124–132. DOI: 10.32523/2616-6844-2022-138-1-124-132

12 Chesney R., Citron D.K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. 2019. Vol. 107. P. 1753–1819.

13 Kira B. When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act // Computer Law & Security Review. 2024. Vol. 54. Article 106024. DOI: 10.1016/j.clsr.2024.106024

14 Dunn S. Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI // McGill Law Journal. 2024. Vol. 69. No. 4. P. 395–416. DOI: 10.26443/law.v69i4.1626

15 Franks M.A., Waldman A.E. Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions // Maryland Law Review. 2019. Vol. 78. No. 4. P. 892–898.

16 Smanova A.B., Muratova A.Zh., Zhumagulova Sh.R. Deepfake Technologies and Social Engineering in Online Fraud Forms, Mechanisms, and Legal Challenges // BULLETIN of L.N. Gumilyov Eurasian National University Law Series. 2025. Vol. 152. No. 3. P. 188–211. DOI: 10.32523/2616-6844-2025-152-3-188-211.

17 Wang T., Liao X., Chow K.P., Lin X., Wang Y. Deepfake Detection: A Comprehensive Survey from the Reliability Perspective // ACM Computing Surveys. 2024. Vol. 57. No. 3. Article 58. P. 1–35. DOI: 10.1145/3699710

18 Guan H., Horan J., Zhang A. Guardians of Forensic Evidence: Evaluating Analytic Systems Against AI-Generated Deepfakes. Forensics@NIST 2024. 2025 // URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=959128 (accessed: 01.09.2026)

19 Saktaganova A.B., Saktaganova I.S., Turegeldiev B.U. Comparative analysis of legal approaches to countering deepfake fraud and social engineering: the experience of the USA, the EU, and the Republic of Kazakhstan // BULLETIN of L.N. Gumilyov Eurasian National University Law Series. 2026. Vol. 154. No. 1. P. 256–269. DOI: 10.32523/2616-6844-2026-154-1-256-269

20 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed: 01.09.2026)

21 Council of Europe. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. 2024. URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence (accessed: 01.09.2026)

22 Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), Public Law 119–12. 2025. URL: https://www.govinfo.gov/content/pkg/COMPS-18158/pdf/COMPS-18158.pdf (accessed: 01.09.2026)

23 Data (Use and Access) Act 2025, section 138; Sexual Offences Act 2003, sections 66E-66H. URL: https://www.legislation.gov.uk/ukpga/2025/18/section/138 (accessed: 20.08.2026)

24 Қазақстан Республикасы Бас прокуратурасы. Относительно дипфейк-рекламы с использованием образа сотрудника прокуратуры. 2026. URL: https://www.gov.kz/memleket/entities/prokuror/press/news/details/1214199?lang=ru (өтініш берілген күн: 20.08.2026)

25 Қазақстан Республикасы Бас прокуратурасы. В Генеральной прокуратуре состоялось заседание Координационного совета Республики Казахстан. 18.04.2026. URL: https://www.gov.kz/memleket/entities/prokuror/press/news/details/1203716?lang=ru (өтініш берілген күн: 20.08.2026)

26 Дербес деректер және оларды қорғау туралы Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы. URL: https://adilet.zan.kz/kaz/docs/Z1300000094 (өтініш берілген күн: 01.09.2026)

27 Қазақстан Республикасының 2014 жылғы 4 шілдедегі № 231-V Қылмыстық-процестік кодексі. URL: https://adilet.zan.kz/kaz/docs/K1400000231 (өтініш берілген күн: 01.09.2026)

28 Қазақстан Республикасының 2015 жылғы 31 қазандағы № 377-V Азаматтық процестік кодексі. URL: https://adilet.zan.kz/kaz/docs/K1500000377 (өтініш берілген күн: 01.09.2026)

29 Тусупбекова Л. ИИ: на пути к внедрению / Казахстанская правда. – 2025. – 20 сент. URL: https://kazpravda.kz/n/ii-na-puti-k-vnedreniyu/ (өтініш берілген күн: 05.09.2026)

30 Абай атындағы Қазақ ұлттық педагогикалық университеті. Первое казахстанское мобильное приложение для борьбы с фейками представили в Алматы. 12.12.2025. URL: https://www.kaznpu.kz/ru/44327/press/ (өтініш берілген күн: 05.09.2026)

REFERENCES

1 Qazaqstan Respublikasynyñ Konstitusiasy (2026 jylğy 15 nauryzdağy respublikalyq referendumda qabyldanğan). URL: https://adilet.zan.kz/kaz/docs/K2600000000 (ötınış berılgen kün: 01.09.2026) (In Kazakh)

2 Qazaqstan Respublikasynyñ 1994 jylğy 27 jeltoqsandağy No. 268-XIII Azamattyq kodeksı (Jalpy bölım). URL: https://adilet.zan.kz/kaz/docs/K940001000_ (ötınış berılgen kün: 01.09.2026) (In Kazakh)

3 Qazaqstan Respublikasynyñ 1999 jylğy 1 şıldedegı No. 409-I Azamattyq kodeksı (Erekşe bölım). URL: https://adilet.zan.kz/kaz/docs/K990000409_ (ötınış berılgen kün: 01.09.2026) (In Kazakh)

4 Sottardyñ ar-namysty, qadır-qasiettı jäne ıskerlık bedeldı qorğau jönındegı zañnamany qoldanu turaly Qazaqstan Respublikasy Joğarğy Sotynyñ 2026 jylğy 20 mamyrdağy No. 3 normativtık qaulysy. URL: https://adilet.zan.kz/kaz/docs/P260000003S (ötınış berılgen kün: 01.09.2026) (In Kazakh)

5 Sottardyñ moräldyq ziandy öteu jönındegı zañnamany qoldanuy turaly Qazaqstan Respublikasy Joğarğy Sotynyñ 2015 jylğy 27 qaraşadağy № 7 normativtık qaulysy. URL: https://adilet.zan.kz/kaz/docs/P150000007S (ötınış berılgen kün: 01.09.2026) (In Kazakh)

6 Qazaqstan Respublikasynyñ 2014 jylğy 3 şildedegı No. 226-V QRZ Qylmystyq kodeksi. URL: https://adilet.zan.kz/kaz/docs/K1400000226 (ötınış berılgen kün: 01.09.2026) (In Kazakh)

7 Äkımşılık qūqyq būzuşylyq turaly Qazaqstan Respublikasynyñ 2014 jylğy 5 şıldedegı No. 235-V QRZ Kodeksı. URL: https://adilet.zan.kz/kaz/docs/K1400000235 (ötınış berılgen kün: 01.09.2026) (In Kazakh)

8 Jasandy intelekt turaly Qazaqstan Respublikasynyñ 2025 jylğy 17 qaraşadağy No. 230-VIII QRZ Zañy. URL: https://adilet.zan.kz/kaz/docs/Z2500000230 (ötınış berılgen kün: 01.09.2026) (In Kazakh)

9 Onlain-platformalar jäne onlain-jarnama turaly Qazaqstan Respublikasynyñ 2023 jylğy 10 şıldedegı No.18-VIII QRZ Zañy. URL: https://adilet.zan.kz/kaz/docs/Z2300000018 (ötınış berılgen kün: 01.09.2026) (In Kazakh)

10 Bisaliev M.S., Shakirov K.N. (2023) Cifrovye sledy kak faktor bezopasnosti oborota personal'nyh dannyh v seti Internet // BULLETIN of L.N. Gumilyov Eurasian National University Law Series. Vol. 142. No. 1. P. 81–98. DOI: 10.32523/2616-6844-2023-142-1-81-98 (In Russian)

11 Imangaliev N.K., Temirzhanova L.A. (2022) Aktual'nye problemy vyjavlenija i raskrytija ugolovnyh pravonarushenij, sovershaemyh v seti Internet // BULLETIN of L.N. Gumilyov Eurasian National University Law Series. Vol. 138. No. 1. P. 124–132. DOI: 10.32523/2616-6844-2022-138-1-124-132 (In Russian)

12 Chesney R., Citron D.K. (2019) Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, vol. 107, pp. 1753–1819 (In English)

13 Kira B. (2024) When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act, Computer Law & Security Review, vol. 54, article 106024. DOI: 10.1016/j.clsr.2024.106024 (In English)

14 Dunn S. (2024) Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI, McGill Law Journal, vol. 69, no. 4, pp. 395–416. DOI: 10.26443/law.v69i4.1626 (In English)

15 Franks M.A., Waldman A.E. (2019) Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions, Maryland Law Review, vol. 78, no. 4, pp. 892–898 (In English)

16 Smanova A.B., Muratova A.Zh., Zhumagulova Sh.R. (2025) Deepfake Technologies and Social Engineering in Online Fraud Forms, Mechanisms, and Legal Challenges // BULLETIN of L.N. Gumilyov Eurasian National University Law Series. 2025. Vol. 152. No. 3. P. 188–211. DOI: 10.32523/2616-6844-2025-152-3-188-211 (In English)

17 Wang T., Liao X., Chow K.P., Lin X., Wang Y. (2024) Deepfake Detection: A Comprehensive Survey from the Reliability Perspective, ACM Computing Surveys, vol. 57, no. 3, article 58, pp. 1–35. DOI: 10.1145/3699710 (In English)

18 Guan H., Horan J., Zhang A. (2025) Guardians of Forensic Evidence: Evaluating Analytic Systems Against AI-Generated Deepfakes. Forensics@NIST 2024. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=959128 (accessed: 01.09.2026) (In English)

19 Saktaganova A.B., Saktaganova I.S., Turegeldiev B.U. (2026) Comparative analysis of legal approaches to countering deepfake fraud and social engineering: the experience of the USA, the EU, and the Republic of Kazakhstan // BULLETIN of L.N. Gumilyov Eurasian National University Law Series. 2026. Vol. 154. No. 1. P. 256–269. DOI: 10.32523/2616-6844-2026-154-1-256-269 (In English)

20 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed: 01.09.2026) (In English)

21 Council of Europe. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. 2024. URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence (accessed: 01.09.2026) (In English)

22 Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), Public Law 119-12. 2025. URL: https://www.govinfo.gov/content/pkg/COMPS-18158/pdf/COMPS-18158.pdf (accessed: 01.09.2026) (In English)

23 Data (Use and Access) Act 2025, section 138; Sexual Offences Act 2003, sections 66E-66H. URL: https://www.legislation.gov.uk/ukpga/2025/18/section/138 (accessed: 20.08.2026) (In English)

24 Qazaqstan Respublikasy Bas prokuraturasy. Otnositel'no dipfejk-reklamy s ispol'zovaniem obraza sotrudnika prokuratury. 2026. URL: https://www.gov.kz/memleket/entities/prokuror/press/news/details/1214199?lang=ru (ötınış berılgen kün: 20.08.2026) (In Russian)

25 Qazaqstan Respublikasy Bas prokuraturasy. V Generälnoi prokurature sostoialös zasedanie Koordinasionnogo soveta Respubliki Kazahstan. 18.04.2026. URL: https://www.gov.kz/memleket/entities/prokuror/press/news/details/1203716?lang=ru (ötınış berılgen kün: 20.08.2026) (In Russian)

26 Derbes derekter jäne olardy qorğau turaly Qazaqstan Respublikasynyñ 2013 jylğy 21 mamyrdağy No. 94-V Zañy. URL: https://adilet.zan.kz/kaz/docs/Z1300000094 (ötınış berılgen kün: 01.09.2026) (In Kazakh)

27 Qazaqstan Respublikasynyñ 2014 jylğy 4 şıldedegı No. 231-V Qylmystyq-prosestık kodeksı. URL: https://adilet.zan.kz/kaz/docs/K1400000231 (ötınış berılgen kün: 01.09.2026) (In Kazakh)

28 Qazaqstan Respublikasynyñ 2015 jylğy 31 qazandağy No. 377-V Azamattyq prosestık kodeksı. URL: https://adilet.zan.kz/kaz/docs/K1500000377 (ötınış berılgen kün: 01.09.2026) (In Kazakh)

29 Tusupbekova L. (2025) II: na puti k vnedreniju // Kazahstanskaja pravda. 20 sent. URL: https://kazpravda.kz/n/ii-na-puti-k-vnedreniyu/ (ötınış berılgen kün: 05.09.2026) (In Russian)

30 Abai atyndağy Qazaq ūlttyq pedagogikalyq universitetı. Pervoe kazahstanskoe mobilnoe prilojenie dlä börby s feikami predstavili v Almaty. 12.12.2025. URL: https://www.kaznpu.kz/ru/44327/press/ (ötınış berılgen kün: 05.09.2026) (In Russian)

ЕРНИШЕВ К.А.,[1]
к.ю.н., ассоциированный профессор.
e-mail: yernishev.k@mail.ru
ORCID ID: 0000-0003-3687-3009
САРЫКУЛОВ К.Р.,[2]
к.ю.н., профессор.
e-mail: kurman_sr@mail.ru
ORCID ID: 0000-0002-8841-9871
РАХМЕТОВА Г.Р.,[2]
к.ю.н., ст. преподаватель.
e-mail: Rahmet-1976@mail.ru
ORCID ID: 0009-0007-3131-9494
УТАНОВ М.А.,*[2]
д.ю.н., профессор.
*e-mail: mau_25@mail.ru
ORCID ID: 0009-0005-1119-3818
[1]Таразский университет им. М.Х. Дулати,
г. Тараз, Казахстан
[2]Южно-Казахстанский университет
им. М.О. Ауезова,
г. Шымкент, Казахстан

ДИПФЕЙКИ КАК УГРОЗА ЧЕСТИ, ДОСТОИНСТВУ, ЧАСТНОЙ ЖИЗНИ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ: ПРАВОВЫЕ МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ

Аннотация

Статья исследует правовые риски дипфейков для чести, достоинства, частной жизни, права на изображение, деловой репутации и общественной безопасности в Республике Казахстан. Проблема рассматривается не как частный технологический дефект, а как новый способ причинения вреда личности и публичному порядку через синтетическое аудио-, фото- и видеосодержание. Материалами исследования выступают Конституция Республики Казахстан, Гражданский кодекс, Уголовный кодекс, Кодекс об административных правонарушениях, Закон «Об искусственном интеллекте», Закон «Об онлайн-платформах и онлайн-рекламе», международные документы и сравнительные правовые подходы ЕС, США и Великобритании. Использованы формально-юридический, сравнительно-правовой, правовое моделирование, системный и доктринальный методы. Обосновано, действующее казахстанское право уже содержит отдельные механизмы защиты от вреда, причиняемого дипфейками, но эти механизмы фрагментарны: они реагируют на клевету, нарушение частной жизни, мошенничество или распространение ложной информации, но не охватывают в полной мере синтетическую имитацию личности. Предложен поэтапный алгоритм от выявления дипфейка до восстановления прав потерпевшего и определены пределы использования результатов детекции в качестве цифровых доказательств. Предлагается дифференцированная модель: гражданско-правовой механизм срочного пресечения распространения и удаления вредоносного дипфейка; приоритетное применение действующих составов преступлений и разработку целевых уголовно-правовых критериев для интимных дипфейков без согласия изображенного лица, использования образа несовершеннолетнего в сексуализированном контексте, мошенничества, вымогательства и имитаций, создающих существенную угрозу общественной безопасности; а также специальные платформенные обязанности, не дублирующие действующее требование о маркировке.

Ключевые слова: дипфейк, честь и достоинство, частная жизнь, право на изображение, общественная безопасность, гражданско-правовая защита, уголовная ответственность.

ERNISHEV K.A.,[1]
c.l.s., associate professor.
e-mail: yernishev.k@mail.ru
ORCID ID: 0000-0003-3687-3009
SARYKULOV K.R.,[2]
c.l.s., professor.
e-mail: kurman_sr@mail.ru
ORCID ID: 0000-0002-8841-9871
RAKHMETOVA G.R.[2]
c.l.s., senior lecturer.
e-mail: Rahmet-1976@mail.ru
ORCID ID: 0009-0007-3131-9494
UTANOV M.A.,*[2]
d.l.s., professor.
*e-mail: mau_25@mail.ru
ORCID ID: 0009-0005-1119-3818
[1]Dulaty University,
Taraz, Kazakhstan
[2]Auezov University,
Shymkent, Kazakhstan

DEEPFAKES AS A THREAT TO HONOR, DIGNITY, PRIVACY AND PUBLIC SAFETY: LEGAL MECHANISMS OF COUNTERACTION

Abstract

This article examines the legal risks that deepfakes pose to honour, dignity, privacy, the right to one's image, business reputation and public safety in the Republic of Kazakhstan. The problem is framed as a new means of harming individuals and public order through synthetic audio, photographic and video content, rather than an isolated technological defect. Sources comprise Kazakhstan's Constitution, Civil and Criminal Codes, Code of Administrative Offences, the Laws "On Artificial Intelligence" and "On Online Platforms and Online Advertising", international instruments, and EU, US and UK legal approaches. Formal legal, comparative, systemic and doctrinal methods and legal modelling are employed. Existing safeguards are fragmented: addressing defamation, privacy violations, fraud and dissemination of false information, they do not fully encompass synthetic impersonation. A sequential framework from detection to restoring victims' rights is proposed, with limits on using detection results as digital evidence. The author proposes a differentiated model: civil remedies for urgently halting dissemination and removing harmful deepfakes; priority application of existing offences and development of targeted criminal-law criteria for non-consensual intimate deepfakes, using minors' images in sexualised contexts, fraud, extortion and impersonation seriously threatening public safety; and specific platform obligations without duplicating existing labelling requirements.

Keywords: deepfake, honor and dignity, private life, image rights, public safety, civil-law protection, criminal liability.

Мақаланың редакцияға түскен күні: 06.07.2026