

К.Р.Сарыкулов, С.Б.Абутаева*, А.Е.Жаксыбаева

заң ғылымдарының кандидаты, доцент, М.Әуезов атындағы Оңтүстік Қазақстан университеті,
Шымкент, Қазақстан

құқық магистрі, аға оқытушы, М.Әуезов атындағы Оңтүстік Қазақстан университеті,
Шымкент, Қазақстан

құқық магистрі, аға оқытушы, М.Әуезов атындағы Оңтүстік Қазақстан университеті,
Шымкент, Қазақстан

*Корреспондент авторы: asb_8008@mail.ru

ЖАСАНДЫ ИНТЕЛЛЕКТ АРҚЫЛЫ ЖАСАЛАТЫН ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫҢ АЗАМАТТАРДЫҢ КОНСТИТУЦИЯЛЫҚ ҚҰҚЫҚТАРЫН ҚОРҒАУ

Түйін

Мақалада жасанды интеллект құралдары арқылы жасалатын қылмыстық құқық бұзушылықтардан азаматтардың конституциялық құқықтарын қорғаудың қылмыстық-құқықтық және процестік тетіктерін бағалау, заңнаманы жетілдіру бағыттары ұсынылады. Зерттеуде формальды-заңдық, салыстырмалы-құқықтық, жүйелік және құқық қолдану практикасын талдау әдістері пайдаланылды. Қазақстан Республикасының Конституциясы, қылмыстық және ақпараттық заңнамасы, ұлттық сот практикасының ашық материалдары, Еуропалық Одақ пен Еуропа Кеңесінің актілері зерделенген. Зерттеудің ғылыми жаңалығы жасанды интеллектті дербес қылмыс субъектісі емес, қылмыс тәсілі, құралы және қоғамдық қауіптілікті күшейтетін фактор ретінде саралайтын құқықтық модельмен айқындалады. Нәтижесінде синтетикалық контентті қылмыстық мақсатта пайдалану белгісін есепке алу, цифрлық дәлелдемелердің түпнұсқалылығын тексеру хаттамасын енгізу, жәбірленушіні жедел қорғау және платформалардан дәлелдемелерді сақтау тәртібін қалыптастыру жөнінде ұсыныстар негізделген.

Кілттік сөздер: жасанды интеллект, конституциялық құқықтар, қылмыстық құқық бұзушылық, дипфейк, дербес деректер, цифрлық дәлелдеме, қылмыстық жауаптылық.

Кіріспе

Жасанды интеллекттің генеративтік модельдері мәтін, дауыс, кескін және бейне жасау құнын төмендетін, ақпарат өндірудің ауқымын түбегейлі өзгертті. Бұл мүмкіндіктер білім беру, медицина және мемлекеттік қызметтер үшін пайдалы болғанымен, қылмыстық ниетпен қолданылғанда адамның дауысын дәл қайталау, жалған бейнежазба құрастыру, фишингтік хабарламаларды жекелендіру, зиянды бағдарламалық кодты бейімдеу және құрбанды психологиялық манипуляциялау тәсілдерін күшейтеді. Сондықтан құқық үшін негізгі мәселе технологияны жалпы сипатта шектеу емес, адамның конституциялық игіліктеріне нақты қауіп туғызатын пайдалану сценарийлерін дәл анықтау болып табылады.

Қазақстан Республикасының 2026 жылғы Конституциясы адамның құқықтары мен бостандықтарын мемлекеттің ең жоғары құндылықтары ретінде бекітіп, цифрлық технологияларды пайдалана отырып, дербес деректерді заңсыз жинаудан, өндеуден, сақтаудан және пайдаланудан қорғауды жеке өмірге қол сұқпаушылық кепілдігінің ұрамына тікелей енгізді [1]. Осы конституциялық жаңарту қылмыстық-құқықтық қорғаудың объектісін кеңейтіп қана қоймай, құқық қолданушыдан цифрлық ортадағы зиянның жаңа нысандарын – тұлғаның цифрлық бейнесін иемденуді, биометриялық еліктеуді, жалған ақпараттық із қалыптастыруды және автоматтандырылған шешімдер арқылы кемсітуді – құқықтық тұрғыдан қайта пайымдауды талап етеді.

2025 жылы «Жасанды интеллект туралы» Қазақстан Республикасының Заңы адам құқықтарының басымдығын, әділдік пен теңдікті, ашықтықты, жариялылықты және жауапкершілікті салалық қағидаттар ретінде белгілейді. Заң синтетикалық нәтижелерді (жасанды интеллект жүйелері қызметінің синтетикалық нәтижелері) таңбалау міндетін

енгізіп, адамның сыртқы келбетін, дауысын, мінез-құлқын немесе болмаған оқиғаларды имитациялайтын материалдардың ерекше тәуекелін мойындайды [2]. Алайда таңбалау талабы қылмыстық қолсұғушылықтың алдын алудың бір ғана қабаты: қылмыскер таңбаны әдейі алып тастауы, шетелдік сервисті қолдануды немесе материалды жабық арнада таратуы мүмкін.

Зерттеу пәні – қолданыстағы қылмыстық-құқықтық құрамдар ЖИ көмегімен келтірілетін зиянды жеткілікті қамти ма және азаматтық бұзылған құқығын уақытылы қалпына келтіру үшін қосымша материалдық және процестік кепілдіктер қажеттігі. Авторлардың пікірінше технологияның өзін криминализациялау заңдылық пен технологиялық бейтараптық қағидаларына қайшы келеді. Негізгі құрамдар сақталуға тиіс, ал ЖИ қолдану қылмыстың тәсілі, дәлелдемелік ерекшелік және белгілі жағдайларда қоғамдық қауіптілікті арттыратын саралаушы мән-жай ретінде ескерілуі тиіс.

Зерттеу әдіснамасы

Зерттеудің нормативтік негізін Қазақстан Республикасының Конституциясы, Қылмыстық кодексі, Қылмыстық-процестік кодексі, «Дербес деректер және оларды қорғау туралы» және «Жасанды интеллект туралы» заңдары, Жоғары Соттың алаяқтық пен электрондық дәлелдемелерге қатысы бар нормативтік түсіндірмелері құрайды [1-6]. Практикалық материалдар ретінде сот актілерінің ашық банкіндегі ақпараттық технологиялар пайдаланылған алаяқтық, жеке өмірге қол сұғу және ақпараттық жүйелерге заңсыз қол жеткізу туралы істердің жарияланған сипаттамалары қарастырылды. Мұндай тәсіл сот актілерінде «жасанды интеллект қолданылды» деген дербес реквизиттің әдетте көрсетілмейтінін ескереді; сондықтан зерттеу нақты істі ЖИ-қылмыс деп қайта атауға емес, қолданыстағы саралау логикасын анықтауға бағытталды. Формальды-құқықтық әдіс қылмыс құрамдарының объективтік және субъективтік белгілерін, конституциялық құқықтарды шектеудің заңдылық өлшемдерін талдау үшін қолданылды. Жүйелік әдіс қылмыстық, ақпараттық және дербес деректер туралы нормалардың өзара байланысын ашуға мүмкіндік берді. Салыстырмалы-құқықтық әдіс Еуропалық Одақтың 2024/1689 Жасанды интеллект туралы актісіндегі тәуекелге негізделген модельді және Еуропа Кеңесінің ЖИ, адам құқықтары, демократия және құқық үстемдігі туралы негіздемелік конвенциясын Қазақстан жүйесімен салыстыруға пайдаланылды [7;8].

Зерттеу нәтижелері

Құқық қолдану практикасын талдауда үш өлшем алынды: біріншісі – қорғалатын конституциялық игілік; екіншісі – ЖИ нәтижесінің қылмыс механизміндегі функциясы;

Үшіншісі – цифрлық дәлелдеменің сенімділігі. Ғылыми нәтижелердің дұрыстығын арттыру үшін технологиялық ұғым мен құқықтық бағаның ара-жігі ажыратылды. Мысалы, «дипфейк» өздігінен қылмыс емес; ол алдау, қорқытып алушылық, жеке өмірге қол сұғу немесе беделге нұқсан келтіру әрекетінің құралы болғанда ғана тиісті құқықтық салдарға әкеледі.

Нәтижелер және оларды талқылау

ЖИ арқылы жасалатын қолсұғушылық бір мезгілде бірнеше конституциялық құқыққа әсер етуі мүмкін. Дауыс клоны арқылы ақша аударған жағдайда меншік құқығы бұзылады; адамның бейнесін әдепсіз контентке біріктіру жеке өмір, қадір-қасиет және абыройға нұқсан келтіреді; биометриялық деректерді рұқсатсыз пайдалану дербес деректердің қауіпсіздігіне қатер төндіреді; жалған саяси үндеу ақпарат алу мен еркін пікір қалыптастыру жағдайын бұрмалайды. Демек, бір технологиялық эпизодты тек мүліктік залалмен өлшеу жәбірленушіге келтірілген конституциялық зиянның толық сипатын ашпайды.

Конституциялық қорғаудың тиімділігі үш талапқа тәуелді. Біріншіден, мемлекеттің теріс міндеті – құқыққа заңсыз араласпау. Екіншіден, оң міндеті – жеке тұлғалардың және цифрлық платформалардың әрекетінен туындайтын қатерге қарсы жеткілікті құқықтық тетік құру. Үшіншіден, бұзылған құқықты қалпына келтіретін тиімді рәсім болуы керек. Қылмыстық жаза соңғы құрал болғандықтан, ол контентті жедел шектеу, дәлелдемені

сақтау, банк операциясын тоқтату, азаматтық-құқықтық залалды өтеу және деректер қауіпсіздігі шараларымен бірге қолданылғанда ғана нәтижелі болады.

«Жасанды интеллект туралы» заңдағы адамға бағдарлану және жауапкершілік қағидаттары қылмыстық заңды түсіндіруде бағдар бола алады, бірақ қылмыстылық пен жазаланушылық тек Қылмыстық кодекспен белгіленеді [2;3]. Осыдан заңдылықтың маңызды талабы туындайды: яғни шешім қабылдау тізбегінде әзірлеуші, жүйе иесі, пайдаланушы, платформа және деректер жеткізушісі болуы мүмкін, алайда қылмыстық жауаптылық нақты адамның кінәсі, әрекеті және салдармен себепті байланысы дәлелденгенде ғана туындайды.

Талқылау және нәтижелер

Зерттеу нәтижесінде ЖИ-дің қылмыс механизміндегі төрт функциясы ажыратылды: дайындықты автоматтандыру; алдаудың сенімділігін күшейту; шабуылды көп адамға масштабтау; цифрлық ізді бүркемелеу. Бұл функциялар жаңа қорғалатын объект жасамайды, бірақ қылмыскердің мүмкіндігін арттырып, жәбірленушінің жалғанды анықтау қабілетін төмендетеді. Сондықтан қылмыстық-құқықтық баға технология атауына емес, оның нақты әрекеттегі рөліне сүйенуге тиіс.

1-кесте – ЖИ қолданылатын қылмыстық сценарийлерді құқықтық бағалау

<i>ЖИ қолдану сценарийі</i>	<i>Негізгі конституциялық игілік</i>	<i>Ықтимал қылмыстық-құқықтық саралау</i>	<i>Дәлелдемелік түйін</i>
Дауыс немесе бейне клоны арқылы ақша талап ету	Меншік, қадір-қасиет, жеке өмір	Алаяқтық; қорқытып алушылық; қылмысқа дайындалу не оқталу	Түпнұсқа файл, метадерек, аккаунт және төлем ізі
Интимдік дипфейк жасау және тарату	Жеке өмір, қадір-қасиет, дербес деректер	Жеке өмірге қол сұғу; заңсыз дерек жинау/тарату; өзге құрамдар жиынтығы	Бет/дауыс үлгісінің көзі, генерация белгісі, тарату ниеті
Жекелендірілген фишинг және зиянды код	Ақпараттық қауіпсіздік, меншік	Ақпараттық жүйеге заңсыз қол жеткізу; зиянды бағдарлама; алаяқтық	Логтар, модельге берілген нұсқаулар, инфрақұрылым байланысы
Жалған қоғамдық немесе ресми хабарлама	Ақпарат алу, қоғамдық қауіпсіздік	Нақты зардап пен мақсатқа қарай жалған ақпарат, арандату не алаяқтық құрамдары	Қасақаналық, аудитория, таралу ауқымы және нақты салдар

Қолданыстағы Қылмыстық кодексте бөтеннің мүлкін алдау немесе сенімді теріс пайдалану арқылы иемдену, жеке өмір туралы мәліметтерді заңсыз жинау не тарату, ақпараттық жүйеге заңсыз қол жеткізу және зиянды бағдарламаларды жасау мен пайдаланғаны үшін жауаптылық көзделген [3]. Бұл құрамдар технологиялық тұрғыдан бейтарап, сондықтан генеративтік модельдің қолданылуы көп жағдайда саралауды жоққа шығармайды. Мысалы, туыстың дауысын имитациялап ақша аударуға қол жеткізу – алдаудың техникалық нысаны; қылмыстың аяқталуы мен залалы алаяқтықтың жалпы ережелерімен анықталады.

Сонымен бірге бейтараптық абсолютті жеткіліктілік дегенді білдірмейді. ЖИ бір шабуылды мыңдаған адамға бағыттауға, әлеуметтік желідегі деректерден әр жәбірленушіге сенімді мәтін құрауға және бірнеше тілде үздіксіз әрекет етуге мүмкіндік

береді. Мұндай масштаб, биометриялық ұқсату және кәмелетке толмаған адамның бейнесін пайдалану қоғамдық қауіптілікті айтарлықтай арттырады. Сондықтан Қылмыстық кодекстің Жалпы бөлігінде жаза тағайындағанда «жасанды интеллект құралдарын пайдалану» деген жалпылама ауырлататын бергі емес, нақты өлшенетін белгілер – көпшілікке автоматтандырылған ықпал, биометриялық сәйкестікті қасақана имитациялау, қорғансыз тұлғаға бағыттау, аса көп деректі өңдеу – ескерілуі орынды.

ЖИ-ге дербес қылмыстық жауаптылық жүктеу теориялық та, практикалық танегізсіз. Модельге құқықтық сана, кінә және жазаны сезіну қабілеті жоқ. Кінә пайдаланушының мақсатынан, алдын ала әрекеттерінен, таңдалған деректерден, жүйеге берілген нұсқаулардан, нәтижені тексеруінен және оны әрі қарай таратуынан анықталады. Өзірлеуші немесе сервис иесі тек зиянды мақсатты білгені және соған аналы түрде жағдай жасағаны не заңда бекітілген арнайы міндетті кінәлі түрде орындалмағаны дәлелденсе жауапты болуы мүмкін. Бұл ұстаным объективті айыптауға жол бермеуге қызмет етеді.

Қазақстанның ЖИ туралы заңы синтетикалық нәтижені таңбалауды, автоматтандырылған өңдеу туралы хабардар болуды және оған қарсылық білдіру мүмкіндігін бекітеді [2]. Бұл ережелер превентивтік маңызға ие: адал платформа материалдың шығу тегін көрсетеді, ал пайдаланушы автоматтандырылған шешімге адам қатысатын қайта қарауды талап ете алады. Қылмыстық контексте таңбаның болмауы автоматты түрде кінәні дәлелдемейді, бірақ өзге деректермен бірге материалдың жалған табиғатын жасыру ниетін көрсетуі мүмкін [4].

Бірінші олқылық – терминологиялық және есептік. Қылмыстық істердің статистикалық карточкаларында ЖИ қолданылғанын көрсететін бірыңғай белгі жоқ. Нәтижесінде құқық қорғау органдары мәселенің ауықымын, залал құрылымын және қай модельдер жиі пайдаланылатын сенімді бағалай алмайды. Қылмыстық кодекске әр технология үшін жаңа құрам енгізудің орнына, Сотқа дейінгі тергеп-тексерулердің бірыңғай тізілімінде «ЖИ көмегімен жасалған немесе күшейтілген әрекет» деген криминалистикалық белгі енгізу ұсынылады. Ол саралау нормасын алмастырмайды, тек дәлелденген технологиялық тәсілді тіркейді.

Екінші олқылық – синтетикалық материалды жедел тоқтату мен дәлелдемені сақтау арасындағы теңгерім. Контентті бірден өшіру жәбірленушінің құқығын қорғайды, бірақ файлдың бастапқы нұсқасы, жүктеу уақыты, IP-мәліметтері және аккаунт байланыстары жоғалуы мүмкін. Сондықтан уәкілетті орган мен платформаға арналған екі сатылы рәсім қажет: алдымен материалдың өзгермейтін көшірмесін, хэш-мәнін және негізгі метадеректерін сақтау; содан кейін қолжетімділікті шектеу. Рәсім сот бақылауын, шағымдану мүмкіндігін және сақтау мерзімін қамтуға тиіс.

Үшінші олқылық – тұлғаның цифрлық бейнесін кешенді қорғау. Дербес деректер туралы заң биометриялық мәліметтерді қорғайды [5], ал Қылмыстық кодекс жеке өмір туралы мәліметтерді заңсыз жинау мен таратуды жазалайды [3]. Бірақ көпшілікке бұрын жарияланған фотоны адамның келісімінсіз қылмыстық дипфейкке пайдалану жағдайында «жинаудың заңсыздығы», жеке өмір құпиясы және жаңа синтетикалық нәтижені құқықтық мәртебесі әр істің жағдайына тәуелді күрделі сұрақ туғызады. Мұнда бастапқы материалдың ашық болуы адамның бейнесін кез келген зиянды контексте пайдалануға келісім білдірмейтінін заңнамалық түсіндіру қажет.

Төртінші олқылық – жәбірленушінің жедел қалпына келтіру құқығы. Жалған бейне бірнеше сағат ішінде мыңдаған рет көшірілгенде, үкім шыққанға дейінгі ұзақ кезеңнің өзі орны толмас беделдік және психологиялық зиян келтіреді. Қылмыстық процесте прокурордың немесе тергеу судьясының негізделген актісі бойынша платформадан жүктеулердің цифрлық ізтаңба арқылы алдын алуды сұрататын арнайы жедел шара қарастырылуы тиіс. Бұл шара мазмұнды түпкілікті заңсыз деп танымайды және сөз бостандығына пропорционалды шектеу ретінде сот бақылауына жатады.

Қазақстан соттарының жарияланған тәжірибесінде ақпараттық технология қолданылған алаяқтық істері көбінесе классикалық құрамдармен сараланады: сот

алдаудың мазмұнын, мүлікті беру сәтін, қасақаналықты, залады және қатысушылардың ролін анықтайды. Жоғары соттың алаяқтық туралы нормативтік қаулысы алдау жәбірленушіні жаңылыстыруға бағытталған көрінеу жалған мәліметті хабарлау немесе шынайы мән-жайды жасыру түрінде болатынын түсіндіреді [6]. Дауыс клоны немесе генеративтік бейне осы анықтамадағы жалған мәліметті жеткізу тәсілі ретінде қарастырылуы мүмкін.

Сонымен бірге ашық сот актілерінде генеративтік ЖИ қолданылуы дербес іздеу белгісімен жүйеленбейді. Осы себепті жарияланған істің тек сыртқы сипаттамасына қарап, матеиалдың нақты қай модельмен жасалғанын немесе соттың оны арнайы саралау мән-жайы деп бағалағанын айту ғылыми тұрғыдан дұрыс емес. Бұл жағдай практика жоқ дегенді білдірмейді; ол сот статистикасы мен актілерді анонимдеу жүйесінде технологиялық тәсіл туралы құрылымдалған деректің жеткіліксіздігін көрсетеді.

Сот практикасын біріздендіру үшін Жоғары Соттың дәлелдемелер жөніндегі түсіндірмесінде синтетикалық аудио-бейне материалын бағалаудың ең төменгі өлшемдері бекітілуі қажет. Оларға файлдың шығу тегі, сақтау тізбегі, хэш бақылау, метадеректер, монтаж белгілері, куәгердің тікелей қабылдауы аккаунт иеленушісі және тәуелсіз сараптама нәтижесі жатады. Бір ғана «детектор» қорытындысы жеткілікті дәлел болмауы тиіс. Өйткені генераторлар мен анықтау құралдарының қателігі өзгеріп отырады. Сот дәлелдемелер жиынтығын бағалап, сараптаманың әдістемесін тексеруі керек.

Қылмыстық процестегі тараптардың теңдігі маңызды. Айыптау органы модель провайдерінен немесе платформадан техникалық мәлімет алған жағдайда, қорғаушы тарапқа оның мазмұнын, алу тәртібін және толықтығын тексеру мүмкіндігі берілуге тиіс. Коммерциялық құпия дәлелдемені жасырын ұстаудың абсолютті негізі бола алмайды; қажет болса, жабық сот отырысы немесе сарапшыға шектеулі қолжетімділік қолданылады.

Еуропалық Одақтың ЖИ туралы актісі қылмыстық кодекс емес, тәуекелге негізделген реттеу құралы. Ол адамның негізгі құқықтарына қауіп төндіретін қолдану түрлеріне қатаң талап қойып, синтетикалық контенттің белгілі санаттарына ашықтық міндетін көздейді [7]. Бұл модельдің Қазақстан үшін құндылығы – қылмыстық репрессияға дейінгі алдын алу қабатын құруында. Тәуекелі жоғары жүйелерге құжаттама, адам бақылауы, журнал жүргізу және сәйкестікті бағалау талаптары кейін қылмыстық іс туындағанда дәлелдеме көзін де қалыптастырады.

Еуропа Кеңесінің 2024 жылғы Негіздемелік конвенциясы ЖИ жүйесінің бүкіл өмірлік циклі барысында адам құқықтары, демократия және құқық үстемдігін қамтамасыз етуге бағытталған [8]. Оның тәуекелдің ықтималдылығы мен ауырлығын бірге бағалау тәсілі Қазақстанның конституциялық пропорционалдық қағидасына сай келеді. Қазақстан үшін маңызды элементтер – ықпалға ұшыраған адамға ақпарат беру, шағымдану, тиімді құқықтық қорғау және ЖИ тәуекелдерін кезендік бағалау.

Еurorol материалдары дипфейктердің басшы атынан төлем талап ету, дәлелдемені бұрмалау, бопсалау және келісімінсіз интимдік материалдар жасау үшін қолданылуы мүмкін екенін көрсетеді [9]. 2025 жылғы киберқылмыс бағалауында генеративтік модельдердің әлеуметтік инженерияны масштабтау қабілеті атап өтілді [10]. Бұл деректер шетелдік норманы механикалық көшіруді емес, қауіптің трансшекаралық табиғатын мойындауды талап етеді; қылмыскер, сервер, иодель иесі, жәбірленуші және төлем инфрақұрылымы әр юрисдикцияда орналасуы мүмкін.

Салыстыру Қазақстанға үш шешімді бейімдеуге мүмкіндік берді. Біріншісі – тәуекелге негізделген алдын алу мен қылмыстық жауаптылықты бөлу. Екіншісі – синтетикалық материалдың шығу тегін мехникалық белгілеуді құқықтық міндетпен ұштастыру. Үшіншісі – құқық бұзылғаннан кейін тиімді шағым, адам қатысатын қайта қарау және дәлелдемені сақтау тетігін кепілдендіру. ЕО тәжірибесіндегі нақты тыйымдар мен жоғары тәуекел санаттары ұлттық конституциялық құрылым, құқық қорғау өкілеттігі және деректерді қорғау режимімен үйлестіріле отырып қана енгізілуі тиіс.

Азаматтардың құқықтарын қорғауды төрт өзара байланысты деңгейден тұратын модель ретінде ұсынады. Бұл модельде қылмыстық заң соңғы, бірақ міндетті кепілдік болып қалады; өзге деңгейлер зиянды ерте анықтап, құқықты тез қалпына келтіруге қызмет етеді.

2-кесте – Конституциялық құқықтарды көпдеңгейлі қорғау моделі

Деңгей	Негізгі құрал	Ұсынылатын нәтиже
1. Алдын алу	Синтетикалық контентті таңбалау, тәуекелді бағалау, журнал жүргізу, қауіпсіз дизайн	Жасырын манипуляция мен дәлелдеме жоғалуын азайту
2. Жедел қорғау	Контентті уақытша шектеу, төлемді тоқтату, аккаунт пен файл деректерін сақтау	Зиянның таралуын тежеу және іздерді бекіту
3. Қылмыстық-құқықтық жауап	Негізгі құрам бойынша саралау, нақты ЖИ тәсілін және масштабты жаза кезінде есепке алу	Зандылықты сақтай отырып барабар жауаптылық
4. Қалпына келтіру	Залалды өтеу, теріске шығару, контентті жою, психологиялық және құқықтық көмек	Жәбірленушінің құқықтық жағдайын барынша қалпына келтіру

Материалдық құқық бойынша Қылмыстық кодекске «ЖИ пайдаланылған кез келген әрекет» деген әмбебап саралаушы белгі енгізу ұсынылмайды. Ол анықтық талабына сай келмейді және қарапайым мәтіндік түзеткіш қолданылған істі де орынсыз ауырлатуы ықтимал. Оның орнына Ерекше бөліктің тиісті құрамдарында қоғамдық қауіптілікті нақты арттыратын белгілер қарастырылуы мүмкін: адамның биометриялық ұқсастығын оның келісімінсіз қылмыстық мақсатта имитациялау; автоматтандырылған құралмен көп адамға бағытталған алдау; кәмелетке толмағанның синтетикалық интимдік бейнесін жасау немесе тарату; қорғаныс тетігін әдейі айналып өту.

Процестік құқық бойынша цифрлық дәлелдемені сақтау тізбегінің бірыңғай хаттамасы қажет. Алынған файлға бірден бақылау хәші есептеліп, құрылғының күйі, көшіру құралы, уақыт белдеуі, файл форматы және әрекетті орындағын тұлға тіркелуге тиіс. Бұл талап тек ЖИ істеріне емес, барлық цифрлық дәлелдемеге пайдалы. Синтетикалық материал бойынша қосымша түрде генерация немесе өңдеу ықтималдылығын анықтайтын кемінде екі тәуелсіз әдіс, бастапқы көзбен салыстыру және контекстік дәлелдер қолданылуы тиіс.

Институционалдық деңгейде прокуратура, ішкі істер органдары, цифрлық даму саласындағы уәкілетті орган және қаржы мониторингі органдары үшін бірлескен әрекет регламенті әзірлені керек. Оның өзегі – тәулік бойы дәлелдемені сақтау сұрауы, банктермен жылдам байланыс, шетелдік платформаларға стандартталған заңдық талап және жәбірленушіге бір терезе қағидатымен көмек көрсету. Уақыт факторы шешуші: синтетикалық алаяқтыққа алғашқы сағаттар төлемді қайтару мен аккаунттарды анықтау ықтималдылығына тікелей әсер етеді.

Азаматтардың өзін өзі қорғау міндеті мемлекеттің оң міндетін алмастырмайды. Дегенмен құқықтық сауаттылық бағдарламалары азаматқа шұғыл ақша сұраған дауысқа кері қоңырау шалу, отбасы ішінде тексеру сөзін пайдалану, бастапқы файлды өшірмеу, экран жазбасын және төлем деректерін сақтау сияқты әрекеттеді үйретуі қажет. Бұл ұсынымдар жәбірленушіні кінәлау емес, дәлелдемені сақтап, зиянды азайтудың практикалық құралы ретінде берілуі тиіс.

Ғылыми тұрғыдан ұсынылған модельдің артықшылығы – технология өзгергенде де қолданылуында. Ол нақты бағдарлама атауына емес, зиянның сипатына, адамның кінәсіне, жүйенің функциясына және құқықты қалпына келтіру қажеттігіне сүйенеді. Сонымен бірге модель инновацияға орын қалдырады: адал әзірлеуші қауіпсіздік стандартын орындағаны үшін қылмыстық тәуекелге ұшырамайды, ал технологияны қасақана қылмыс құралына айналдырған тұлға жалпы негізде жауап береді.

Қорытынды

Зерттеу жасанды интеллект арқылы жасалатын қылмыстық құқық бұзушылықтарды бөлек «виртуалды қылмыс әлемі» ретінде емес, конституциялық құқықтарға қол сұғудың технологиялық күшейтілген нысаны ретінде қарастыру қажет екенін көрсетті. ЖИ қылмыс субъектісі болмайды; оның құқықтық рөлі – тәсіл, құрал, дайындық инфрақұрылымы немесе зиян ауқымын арттыратын фактор. Қылмыстық жауаптылық нақты адамның кінәсі мен себепті байланысы негізінде белгіленуі тиіс.

Қазақстанның қолданыстағы қылмыстық құрамы алаяқтық, жеке өмірге қол сұғу, дербес деректерді заңсыз пайдалану және ақпараттық жүйелерге шабуылдың көп бөлігін қамтиды. Сондықтан жаппай жаңа құрамдар енгізу орнына, құқық қолдануды нақтылау және қоғамдық қауіптілікті шын мәнінде арттыратын өлшемдерді белгілеу орынды.

Біріншіден, қылмыстық статистикада ЖИ қолдану фактісін сипаттайтын, саралауға ықпал етпейтін технологиялық белгі енгізу қажет. Екіншіден, синтетикалық материал бойынша дәлелдемені сақтау, хэштеу, түпнұсқалықты кешенді тексеру және сараптама әдістемесін ашу тәртібі бекітілуі тиіс. Үшіншіден, платформадағы зиянды материалдың дәлелдік көшірмесін сақтап, кейін уақытша шектеуге мүмкіндік беретін сот бақылауындағы жедел рәсім қажет. Төртіншіден, адамның ашық жарияланған бейнесі мен дауысы қылмыстық синтетикалық контент жасауға үнсіз келісім болып саналмайтыны заң деңгейінде айқындалуы керек. Бесіншіден, Еуропалық Одақ пен Еуропа Кеңесінің тәжірибесіне сәйкес тәуекелді алдын ала бағалау, ашықтық, адам бақылауы және тиімді шағымданду кепілдіктері қылмыстық-құқықтық қорғаумен байланыстырылуы қажет.

Ұсынылған шаралар сөз бостандығы мен инновацияны негізсіз шектемеуі үшін заңдылық, қажеттілік және пропорционалдық өлшемдеріне бағынуға тиіс. Азаматтың конституциялық құқығын қорғаудың өлшемі тек кінәліні жазалау емес, жалған контенттің таралуын дер кезінде тоқтату, дәлелдемені жоғалтпау және жәбірленушінің құқықтық жағдайын нақты қалпына келтіру болып табылады.

Әдебиеттер

1. Қазақстан Республикасының Конституциясы: 2026 жылғы 15 наурыздағы республикалық референдумда қабылданған, 2026 жылғы 1 шілдеден қолданысқа енгізілген. Мына сілтемеде: <https://www.akorda.kz/kz/constitution-of-the-republic-of-kazakhstan-50912> (қаралған күні: 27.09.2026).
2. Жасанды интеллект туралы: Қазақстан Республикасының 2025 жылғы 17 қарашадағы № 230-VIII ҚРЗ Заңы. Мына сілтемеде: <https://adilet.zan.kz/kaz/docs/Z2500000230> (қаралған күні: 27.09.2026).
3. Қазақстан Республикасының Қылмыстық кодексі: 2014 жылғы 3 шілдедегі № 226-V ҚРЗ. Мына сілтемеде: <https://adilet.zan.kz/kaz/docs/K1400000226> (қаралған күні: 27.09.2026).
4. Қазақстан Республикасының Қылмыстық-процестік кодексі: 2014 жылғы 4 шілдедегі № 231-V ҚРЗ. Мына сілтемеде: <https://adilet.zan.kz/kaz/docs/K1400000231> (қаралған күні: 27.09.2026).
5. Дербес деректер және оларды қорғау туралы: Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы. Мына сілтемеде: <https://adilet.zan.kz/kaz/docs/Z1300000094> (қаралған күні: 27.09.2026).

6. Алаяқтық туралы істер бойынша сот практикасы туралы: Қазақстан Республикасы Жоғарғы Сотының 2017 жылғы 29 маусымдағы № 6 нормативтік қаулысы. Мына сілтемеде: <https://adilet.zan.kz/kaz/docs/P1700000006S> (қаралған күні: 27.09.2026).
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Official Journal of the European Union. 2024;L 2024/1689.
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Strasbourg: Council of Europe; 2024.
9. Europol. Facing reality? Law enforcement and the challenge of deepfakes. Luxembourg: Publications Office of the European Union; 2022.
10. Europol. Steal, deal and repeat: How cybercriminals trade and exploit your data. Internet Organised Crime Threat Assessment 2025. Luxembourg: Publications Office of the European Union; 2025.

1. References

1. Qazaqstan Respublikasynyn Konstitutsiyasy [Constitution of the Republic of Kazakhstan]: adopted at the republican referendum of 15 March 2026, effective from 1 July 2026. Available from: <https://www.akorda.kz/kz/constitution-of-the-republic-of-kazakhstan-50912> [cited 2026 Sep 27]. (In Kaz.).
2. Zhasandy intellekt turaly [On Artificial Intelligence]. Law of the Republic of Kazakhstan No. 230-VIII, 17 November 2025. Available from: <https://adilet.zan.kz/kaz/docs/Z25000000230> [cited 2026 Sep 27]. (In Kaz.).
3. Qazaqstan Respublikasynyn Qylmystyq kodeksi [Criminal Code of the Republic of Kazakhstan]. No. 226-V, 3 July 2014. Available from: <https://adilet.zan.kz/kaz/docs/K14000000226> [cited 2026 Sep 27]. (In Kaz.).
4. Qazaqstan Respublikasynyn Qylmystyq-protsestik kodeksi [Criminal Procedure Code of the Republic of Kazakhstan]. No. 231-V, 4 July 2014. Available from: <https://adilet.zan.kz/kaz/docs/K14000000231> [cited 2026 Sep 27]. (In Kaz.).
5. Derbes derekter zhane olardy qorgau turaly [On Personal Data and Their Protection]. Law of the Republic of Kazakhstan No. 94-V, 21 May 2013. Available from: <https://adilet.zan.kz/kaz/docs/Z13000000094> [cited 2026 Sep 27]. (In Kaz.).
6. Alayaqtyq turaly ister boiynsha sot praktikasy turaly [On judicial practice in fraud cases]. Regulatory Resolution of the Supreme Court of the Republic of Kazakhstan No. 6, 29 June 2017. Available from: <https://adilet.zan.kz/kaz/docs/P1700000006S> [cited 2026 Sep 27]. (In Kaz.).
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Official Journal of the European Union. 2024;L 2024/1689.
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Strasbourg: Council of Europe; 2024.
9. Europol. Facing reality? Law enforcement and the challenge of deepfakes. Luxembourg: Publications Office of the European Union; 2022.
10. Europol. Steal, deal and repeat: How cybercriminals trade and exploit your data. Internet Organised Crime Threat Assessment 2025. Luxembourg: Publications Office of the European Union; 2025.

К.Р.Сарыкулов, С.Б.Абутаева, А.Е.Жаксыбаева

кандидат юридических наук, доцент, kurman_sr@mail.ru,
Южно-Казахстанский университет имени М. Ауэзова, Шымкент, Казахстан
магистр права, старший преподаватель, asb_8008@mail.ru,
Южно-Казахстанский университет имени М. Ауэзова, Шымкент, Казахстан
магистр права, старший преподаватель, aigulzhaksy@mail.ru,
Южно-Казахстанский университет имени М. Ауэзова, Шымкент, Казахстан

ЗАЩИТА КОНСТИТУЦИОННЫХ ПРАВ ГРАЖДАН ОТ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация

В статье рассматриваются уголовно-правовые и процессуальные механизмы защиты конституционных прав граждан от уголовных правонарушений, совершаемых с применением искусственного интеллекта, и предложить направления совершенствования законодательства. Используются формально-правовой, сравнительно-правовой, системный методы и анализ правоприменительной практики. Изучены Конституция Республики Казахстан, уголовное и информационное законодательство, открытые материалы национальной судебной практики, акты Европейского Союза и Совета Европы. Научная новизна состоит в модели, рассматривающей искусственный интеллект не как самостоятельный субъект преступления, а как способ, орудие и фактор усиления общественной опасности. Обоснованы предложения по учету признака использования синтетического контента в преступных целях, внедрению протокола проверки подлинности цифровых доказательств, оперативной защите потерпевших и формированию порядка сохранения доказательств цифровыми платформами.

Ключевые слова: искусственный интеллект, конституционные права, дипфейк, цифровое доказательство, уголовная ответственность.

K.R.Sarykulov, S.B.Abutayeva, A.E.Zhaksybayeva

Candidate of Legal Sciences, Associate Professor, kurman_sr@mail.ru,
M. Auezov South Kazakhstan University, Shymkent, Kazakhstan
Master of Law, Senior Lecturer, asb_8008@mail.ru, M. Auezov South Kazakhstan University,
Shymkent, Kazakhstan
Master of Law, Senior Lecturer, aigulzhaksy@mail.ru, M. Auezov South Kazakhstan University,
Shymkent, Kazakhstan

PROTECTION OF CITIZENS' CONSTITUTIONAL RIGHTS FROM CRIMINAL OFFENCES COMMITTED USING ARTIFICIAL INTELLIGENCE

Abstract

The article assesses the criminal law and criminal procedure mechanisms for protecting citizens' constitutional rights against criminal offences committed using artificial intelligence and proposes directions for improving the legislation of the Republic of Kazakhstan. The study employs formal legal, comparative legal, and systemic methods, as well as an analysis of law enforcement practice. It examines the Constitution of the Republic of Kazakhstan, criminal and information legislation, publicly available materials from national judicial practice, and legal acts of the European Union and the Council of Europe. The scientific novelty of the study lies in developing a model in which artificial intelligence is regarded not as an independent subject of a criminal offence, but as a method and instrument of its commission and as a factor increasing the degree of social danger posed by the act. The article substantiates proposals to consider the use of synthetic content for criminal purposes when conducting the criminal-law assessment of an act, introduce a protocol for verifying the authenticity of digital evidence, ensure the prompt protection of victims, and establish a procedure requiring digital platforms to preserve information of evidentiary value.

Keywords: artificial intelligence, constitutional rights, deepfake, digital evidence, criminal liability.

