әл-Фараби атындағы Қазақ ұлттық университеті

ӘОЖ 343.18 (043) Қолжазба құқығында

ЖҰМАДИЛОВА НАЗЕРКЕ СЕРІКЖАНҚЫЗЫ

Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің қылмыстық-процестік мәселелері

8D04203 – «Құқықтану»

Философии докторы (PhD)
дәрежесін алу үшін дайындалған диссертация

Отандық ғылыми кеңесшілері:
1. Заң ғылымдарының кандидаты,
профессор міндетін атқарушы
Е.Т. Алимкулов (Алматы қ., Қазақстан);
2. Философия докторы (PhD), профессор
А.К. Жанибеков (Шымкент қ., Қазақстан).

Шетелдік ғылыми кеңесшісі:
Философия докторы (PhD), Judith Rich
Harris криминология профессоры
К.М. Бивер (Таллахасси қ., АҚШ)

Қазақстан Республикасы
Алматы, 2026

МАЗМҰНЫ

НОРМАТИВТІК СІЛТЕМЕЛЕР 3
АНЫҚТАМАЛАР 4
БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР 6
КІРІСПЕ 8
1 ҚЫЛМЫСТЫҚ ПРОЦЕСТЕ ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУДЫҢ ҚҰҚЫҚТЫҚ РЕЖИМІ МЕН ПРОЦЕСТІК КЕПІЛДІКТЕРІНІҢ ТЕОРИЯЛЫҚ НЕГІЗДЕРІ 26
1.1 Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтардың қылмыстық-құқықтық сипаттамасы, қылмыстық жауаптылықтың шектері және саралау өлшемдері 26
1.2 Дербес деректер саласындағы ұлттық құқықтық база және мемлекеттік саясат: киберқауіпсіздік пен мемлекеттік бақылау мәселелері 39
1.3 Қылмыстық процесте дербес деректерді қорғаудың процестік кепілдіктері 48
2 ДЕРБЕС ДЕРЕКТЕРДІ ЗАҢСЫЗ ЖИНАУМЕН, ӨҢДЕУМЕН ЖӘНЕ ТАРАТУМЕН БАЙЛАНЫСТЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫ СОТҚА ДЕЙІНГІ ТЕРГЕП-ТЕКСЕРУДІҢ ПРОЦЕСТІК МӘСЕЛЕЛЕРІ 58
2.1 Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық істер бойынша дәлелдеу пәні және сотқа дейінгі тергеп-тексеруді ұйымдастыру 58
2.2 Дербес деректерге қатысты дәлелдемелерді жинау және бекітудің процестік тәртібі 70
2.3 Құқықтарды шектеумен байланысты процестік құралдар: жасырын тергеу әрекеттері және цифрлық ортадағы дәлелдемелердің жол берілетіндігін бағалау 86
3 ТЕРГЕУ ТИІМДІЛІГІ МЕН ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУДЫ КҮШЕЙТУДІҢ ҚЫЛМЫСТЫҚ-ПРОЦЕСТІК КЕПІЛДІКТЕРІ 97
3.1 Қылмыстық процесте дербес деректермен жұмыс істеудің арнайы процестік режимі 97
3.2 Қылмыстық процесте дербес деректердің құпиялылығын сақтау: іс материалдарына қолжетімділік, жариялылық тәуекелдері және деректерді шектеу тетіктері 107
3.3 Қылмыстық-процестік заңнаманы және құқық қолдану тәжірибесін жетілдіру жөніндегі тұжырымдамалық ұсыныстар 118
ҚОРЫТЫНДЫ 125
ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ 145
ҚОСЫМША А, Б, В, Г, Д, Е

НОРМАТИВТІК СІЛТЕМЕЛЕР

Берілген диссертацияда келесі стандарттарға сәйкес сілтемелер қолданылды:

1. МЕМСТ 7.32-2001 (2006 жылғы өзгерістермен). Ғылыми-зерттеу жұмысы туралы есеп. Құрылымы мен ресімдеу ережелері;
2. МЕМСТ 7.1-2003. Библиографиялық жазба. Библиографиялық сипаттама. Жалпы талаптар және құрастыру ережелері.

АНЫҚТАМАЛАР

Диссертациялық зерттеу жұмысында төмендегі анықтамалар мен терминдер қолданылды:

Дербес деректер – дербес деректердің бір немесе бірнеше сәйкестендіргішімен толықтырылған, дербес деректер субъектісі туралы мәліметтер немесе мәліметтер жиынтығы.

Биометриялық деректер – дербес деректер субъектісінің физиологиялық және биологиялық ерекшеліктерін сипаттайтын, олардың негізінде осы субъектінің жеке басын анықтауға болатын дербес деректер.

Дербес деректерді жинау – дербес деректерді алуға бағытталған іс-әрекеттер.

Дербес деректерді өңдеу – дербес деректерді жинақтауға, сақтауға, өзгертуге, толықтыруға, пайдалануға, таратуға, иесіздендіруге, бұғаттауға және жоюға бағытталған іс-әрекеттер.

Дербес деректерді қорғау – дербес деректер және оларды қорғау туралы заңнамада белгіленген мақсаттарда жүзеге асырылатын құқықтық, ұйымдастырушылық және техникалық шаралар кешені.

Дербес деректерді қамтитын базаның және (немесе) цифрлық объектінің операторы (оператор) – дербес деректерді жинауды, өңдеуді және қорғауды жүзеге асыратын мемлекеттік орган, жеке және (немесе) заңды тұлға.

Дербес деректер субъектісі – дербес деректер өзіне қатысты болатын жеке тұлға.

Дерек ұстаушы – қылмыстық іс үшін маңызы бар дербес деректерді немесе өзге цифрлық ақпаратты заңды негізде иеленетін, сақтайтын немесе өңдейтін мемлекеттік орган, ұйым, оператор, провайдер немесе өзге тұлға.

Дербес деректердің құпиялылығы – дербес деректерге қол жеткізе алатын тұлғалардың оларды субъектінің келісімінсіз немесе өзге заңды негізсіз таратуға жол бермеу міндетін білдіретін құқықтық режим.

Дербес деректерді иесіздендіру – дербес деректердің нақты субъектке тиесілілігін анықтауға мүмкіндік бермейтіндей етіп оларды өзгерту жөніндегі әрекеттер.

Псевдонимдеу – дербес деректерді қосымша ақпаратты пайдаланбай нақты субъектпен тікелей байланыстыруға мүмкіндік бермейтін нысанда өңдеу тәсілі.

Қайта сәйкестендіру – иесіздендірілген немесе псевдонимделген деректерді қосымша мәліметтермен салыстыру арқылы нақты тұлғаны қайта анықтау процесі.

Цифрлық деректер – цифрлық нысанда берілген және оларды алу тәсіліне қарамастан автоматтандырылған және (немесе) талдамалық жинауға, сақтауға, өңдеуге, пайдалануға, беруге, таратуға немесе алып тастауға жарамды ақпарат.

Цифрлық жазба – мазмұнын, дереккөзін, құрылымын немесе мақсатын

анықтауға мүмкіндік беретін сәйкестендіру сипаттамалары бар цифрлық нысанда тіркелген ақпарат немесе осындай ақпарат туралы мәліметтер.

Цифрлық із – ақпараттық жүйелерді, құрылғыларды немесе желілерді пайдалану нәтижесінде автоматты түрде немесе пайдаланушы әрекеті арқылы қалыптасатын және белгілі бір оқиға, әрекет немесе тұлға туралы мәліметтерді қалпына келтіруге мүмкіндік беретін цифрлық ақпарат.

Метадеректер – деректердің мазмұнын, құрылымын, шығу тегін, уақытын, форматтарын, авторын немесе өзге сипаттамаларын сипаттайтын деректер.

Лог – ақпараттық жүйеде, бағдарламада немесе құрылғыда орын алған оқиғалар мен пайдаланушы әрекеттері туралы мәліметтер хронологиялық ретпен тіркелетін жазба немесе файл.

Аудит ізі – ақпараттық жүйеде жасалған операцияларды, пайдаланушы әрекеттерін, өзгерістерді және қолжетімділік фактілерін кейіннен тексеруге мүмкіндік беретін жүйелі цифрлық жазбалар жиынтығы.

Хэш – цифрлық деректерге хэштеу алгоритмін қолдану нәтижесінде алынатын тұрақты немесе белгіленген ұзындықтағы мән.

Хэштеу – цифрлық деректерді арнайы математикалық алгоритм арқылы хэш-мәнге түрлендіру процесі.

Дәлелдемелік тұтастық – электрондық ақпараттың алынған сәттен бастап зерттеу мен сотта пайдалану кезеңіне дейін рұқсатсыз өзгертілмегенін және оның бастапқы күйінің сақталғанын сипаттайтын қасиет.

Дәлелдемелік тізбек (chain of custody) – электрондық немесе материалдық дәлелдеменің алынуынан бастап сақталуына, берілуіне, зерттелуіне және сотта пайдаланылуына дейінгі барлық әрекеттер мен оған қол жеткізген тұлғаларды құжаттайтын жүйе.

Техникалық идентификатор – пайдаланушыны, құрылғыны, есептік жазбаны, байланыс сессиясын немесе ақпараттық жүйедегі өзге объектіні ажыратуға мүмкіндік беретін техникалық белгі, оның ішінде IP-мекенжай, IMEI, IMSI, MAC-мекенжай, аккаунт идентификаторы және өзге мәндер.

IP-мекенжай – желіге қосылған құрылғыны немесе желілік интерфейсті сәйкестендіруге арналған сандық мекенжай.

IMEI – ұялы байланыс құрылғысын сәйкестендіруге арналған халықаралық бірегей идентификатор.

Интернет-провайдер – пайдаланушыларға интернет желісіне қолжетімділік және онымен байланысты телекоммуникациялық қызметтер көрсететін ұйым.

Деректерді минимизациялау – нақты процестік мақсатқа қол жеткізу үшін қажетті және жеткілікті көлемдегі деректерді ғана жинау, алу және пайдалану қағидаты.

Мөлшерлестік – құқықтарды шектеу мен көзделген заңды мақсат арасында ақылға қонымды теңгерімнің болуын талап ететін қағида.

Цифрлық криминалистика – цифрлық құрылғылардан, жүйелерден және желілерден ақпаратты анықтау, алу, сақтау, зерттеу және түсіндіру әдістерінің жиынтығы.

БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР

ҚР ҚК	Қазақстан Республикасының Қылмыстық кодексі
ҚР ҚПК	Қазақстан Республикасының Қылмыстық-процестік кодексі
ҚР ӘҚБтК	Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы кодексі
GDPR	General Data Protection Regulation (ЕО деректерді қорғау регламенті)
ЭЦҚ	электрондық цифрлық қолтаңба
ЖСН	жеке сәйкестендіру нөмірі
АЖ	ақпараттық жүйе
СДТТ	сотқа дейінгі тергеп-тексеру
ЖТӘ	жасырын тергеу әрекеттері
ОЖ	операциялық жүйе
LED	Law Enforcement Directive (ЕО-ның 2016/680 Директивасы)
EDPB	European Data Protection Board (Еуропалық деректерді қорғау жөніндегі кеңес)
ENISA	European Union Agency for Cybersecurity (Еуропалық Одақтың киберқауіпсіздік агенттігі)
NIST	National Institute of Standards and Technology (АҚШ Ұлттық стандарттар және технологиялар институты)
ISO	International Organization for Standardization (Халықаралық стандарттау ұйымы)
IEC	International Electrotechnical Commission (Халықаралық электротехникалық комиссия)
ISO/IEC 27001	ақпараттық қауіпсіздік менеджменті жүйесіне қойылатын талаптарды белгілейтін халықаралық стандарт
ISO/IEC 27701	құпиялылық ақпаратын басқару жүйесіне қойылатын талаптар мен ұсынымдарды белгілейтін халықаралық стандарт
IP-address	Internet Protocol address (желідегі құрылғыны немесе интерфейсті сәйкестендіретін мекенжай)
URL	Uniform Resource Locator (интернет-ресурстың бірыңғай мекенжай көрсеткіші)
SIM-карта	Subscriber Identity Module (абонентті сәйкестендіру модулі)
IMEI	International Mobile Equipment Identity (мобильді құрылғының халықаралық сәйкестендіру нөмірі)
IMSI	International Mobile Subscriber Identity (мобильді абоненттің халықаралық сәйкестендіру нөмірі)
MAC-address	Media Access Control address (желілік құрылғы интерфейсінің аппараттық сәйкестендіргіші)
VPN	Virtual Private Network (виртуалды жеке желі)
MFA	Multi-Factor Authentication (көп факторлы аутентификация)
OTP	One-Time Password (бір реттік пароль)
API	Application Programming Interface (қолданбалы

	бағдарламалау интерфейсі)
OSINT	Open Source Intelligence (ашық дереккөздерден ақпарат жинау)
CRM	Customer Relationship Management (клиенттермен өзара қатынастарды басқару жүйесі)
ERP	Enterprise Resource Planning (ұйым ресурстарын жоспарлау жүйесі)
CCTV	Closed-Circuit Television (бейнебақылау жүйесі)
CDR	Call Detail Record (байланыс сеанстары туралы егжей-тегжейлі жазба)
ABAC	Attribute-Based Access Control (атрибуттарға негізделген қолжетімділікті басқару)
RBAC	Role-Based Access Control (рөлге негізделген қолжетімділікті басқару)
AI / ЖИ	Artificial Intelligence / жасанды интеллект
Big Data	үлкен көлемді деректерді сақтау, өңдеу және талдау технологияларының жиынтығы
PIMS	Privacy Information Management System (құпиялылық ақпаратын басқару жүйесі)
PII	Personally Identifiable Information (тұлғаны тікелей немесе жанама сәйкестендіруге мүмкіндік беретін ақпарат)

КІРІСПЕ

Зерттеу жұмысының жалпы сипаттамасы. Диссертациялық зерттеу Қазақстан Республикасында дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеру барысында туындайтын қылмыстық-процестік мәселелерді кешенді зерттеуге арналған. Зерттеудің тұжырымдамалық негізін дербес деректерді жинау, өңдеу және таратудың заңдылық шарттарын айқындайтын салалық және қылмыстық-құқықтық нормалар мен олардың сақталуын дәлелдеуге бағытталған қылмыстық-процестік құралдардың өзара байланысы құрайды.

Дербес деректерді зерттеу барысында олар тек ақпараттық және азаматтық-құқықтық қатынастардың объектісі ретінде емес, сонымен қатар жеке өмірге қол сұғылмаушылық пен құпиялылық құқықтары қорғайтын ақпараттық игілік ретінде де, қылмыстық іс бойынша маңызды мән-жайларды анықтауға жол ашатын дәлелдемелік ақпараттың ықтимал көзі ретінде де қаралады. Мұндай қосарлы табиғат деректерді алудың құқықтық негізін, қажеттілік пен мөлшерлестік қағидаттарын, процестік нысанды, техникалық тұтастықты, сондай-ақ қылмыстық іс материалдарында олардың кейінгі қорғалуын бір жүйеде қамтамасыз етуді қажет етеді.

Зерттеу шеңберінде дербес деректер мен олармен байланысты цифрлық мәліметтерді анықтау, шұғыл сақтау, алу, қарап-тексеру, криминалистикалық көшірмесін жасау, процестік нысанда бекіту, сақтау, тексеру және бағалау мәселелері жан-жақты зерделенді. Сонымен қатар дерек ұстаушылардан, меншік иелері мен операторлардан, байланыс операторларынан, интернет-провайдерлерден, цифрлық платформалардан және ақпараттық жүйелер әкімшілерінен мәліметтер алудың негіздері мен тәртібі, маман мен сарапшының қатысу ерекшеліктері, жасырын тергеу әрекеттерін қолдану шектері, сондай-ақ қылмыстық іс материалдарындағы дербес деректердің құпиялылығын қамтамасыз ететін кепілдіктер талдау нысанасына алынды.

Зерттеу нәтижесінде сотқа дейінгі тергеп-тексерудің кезеңдік моделі, цифрлық іздерді анықтау мен бекітудің процестік алгоритмі, дерек ұстаушылармен өзара іс-қимыл стандарты, маман мен сарапшының функцияларын ажырату өлшемдері, цифрлық ортадағы дәлелдемелердің жол берілетіндігі мен сенімділігін бағалау жүйесі, іс материалдарына сараланған қолжетімділік және дербес деректерді иесіздендіру тетігі негізделді. Сонымен қатар қылмыстық-процестік заңнама мен құқық қолдану практикасын қысқа, орта және ұзақ мерзімді перспективада жетілдіруге бағытталған тұжырымдамалық ұсыныстар әзірленді.

Зерттеу жұмысының өзектілігі. Қазіргі цифрландыру жағдайында дербес деректер мемлекеттік басқару, электрондық үкімет, қаржы, байланыс, денсаулық сақтау, білім беру, әлеуметтік желілер, интернет-платформалар және құқық қорғау қызметін қамтитын қоғамдық қатынастардың барлық саласында маңызды ақпараттық ресурсқа айналды. Осыған байланысты дербес деректерді заңсыз жинау, өңдеу және тарату адамның құқықтары мен

бостандықтарына ғана емес, ақпараттық қауіпсіздікке және қылмыстық сот ісін жүргізудің тиімділігіне де тікелей әсер етеді. Сондықтан дербес деректерді адамның жеке өмірі мен цифрлық қауіпсіздігін қамтамасыз ететін құқықтық категория ретінде ғана емес, қылмыстық процестегі дәлелдемелік қатынастардың ерекше объектісі ретінде де қарастыру қажеттілігі туындайды.

Қазақстан Республикасының Конституциясы адамның жеке өміріне қол сұғылмаушылығына, өзінің және отбасының құпиясына, ар-намысы мен қадір-қасиетін қорғауға кепілдік береді. Конституцияның 21-бабында цифрлық технологияларды қолдануды қоса алғанда, дербес деректерді заңсыз жинаудан, өңдеуден, сақтаудан және пайдаланудан қорғау құқығына заңмен кепілдік берілетіні бекітілген [1]. Сонымен қатар әркімнің заңмен тыйым салынбаған тәсілдермен ақпарат алу және тарату құқығы көзделген [1]. Бұл ережелер қылмыстық процесте, бір жағынан, қылмыстық құқық бұзушылықтарды ашуға қажетті ақпаратты алу, екінші жағынан, жеке өмір мен дербес деректерді қорғау арасындағы теңгерімді қамтамасыз етудің конституциялық негізін қалыптастырады.

Конституциялық кепілдіктер 2013 жылғы «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңында нақтыланып, оның 2026 жылғы конституциялық реформаға байланысты енгізілген толықтырулары деректерді қорғау режимін жаңа талаптарға сәйкестендіре түсті [2]. Аталған заң дербес деректерді жинау, өңдеу, сақтау, пайдалану, тарату және қорғау тәртібін, деректер субъектілерінің құқықтары мен деректер базаларының меншік иелері және операторларының міндеттерін айқындайды. Қылмыстық процесс үшін оның маңызы дербес деректерді дәлелдемелік мақсатта алудың және пайдаланудың құқықтық шектерін анықтаумен байланысты.

Сонымен бірге дербес деректерді қорғау туралы салалық заңнама мен қылмыстық-процестік заңнаманың арақатынасы толық жүйеленбеген. Дербес деректер іс үшін маңызы бар мән-жайларды анықтауға мүмкіндік берген жағдайда дәлелдеу процесіне енгізілуі мүмкін, алайда олардың дәлелдемелік күші мәліметтердің заңды түрде алынуына, процестік нысанда бекітілуіне, дереккөзінің айқын болуына, цифрлық тұтастығының сақталуына және сотта тексерілу мүмкіндігіне тікелей тәуелді. Осыған байланысты дербес деректерді қылмыстық процесте жай ақпараттық ресурс ретінде емес, дәлелдемелік және құқық қорғаушылық мәні қатар жүретін ерекше объект ретінде қарастыру қажет.

Мәселенің өзектілігі мемлекеттік цифрландыру саясатының бағыттарымен де айқындалады. Мемлекет басшысы Қасым-Жомарт Кемелұлы Тоқаев азаматтардың дербес деректерінің жария болып кету жағдайларының жиілегенін атап өтіп, оларды қорғау бойынша жүйелі жұмыс жүргізу қажеттігін көрсетті. Сонымен қатар құқық қорғау жүйесінде бірыңғай цифрлық экожүйе мен ортақ технологиялық стандарттарды қалыптастыру міндетін белгіледі [3]. Бұл талап қылмыстық процесте дербес деректермен жұмыс істеудің де бірыңғай құқықтық және технологиялық

стандарттарын әзірлеу қажеттігін көрсетеді.

Аталған бағыт Қазақстан Республикасының Цифрлық кодексінің қабылдануымен институционалдық сипат алды. Кодекс цифрлық кеңістіктегі қоғамдық қатынастарды кешенді реттеуге, ақпараттық жүйелердің өзара үйлесімділігі мен дербес деректердің қауіпсіз айналымын қамтамасыз етуге бағытталған [4]. Осы жағдайда дербес деректерді қорғау тек ақпараттық қауіпсіздік мәселесі емес, қылмыстық процестегі дәлелдемелердің заңдылығы, сот бақылауы, прокурорлық қадағалау және адам құқықтарының сақталуымен байланысты кешенді қылмыстық-процестік мәселе ретінде көрініс табады. Цифрлық технологияларды құқықтық реттеу сапасы заң шығару қызметінің тиімділігіне де байланысты. Қазақстандағы заң шығару процесін цифрландыру жөніндегі зерттеулер цифрлық технологияларды, ашық басқаруды және адам құқықтарын қорғау қағидаттарын өзара үйлестіру қажеттігін негіздейді [5, 7 б.].

Қазақстан Республикасының Қылмыстық-процестік кодексі дәлелдемелер ретінде заңды түрде алынған нақты деректерді таниды [6]. Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты істердің ерекшелігі – дәлелдемелік ақпараттың елеулі бөлігінің цифрлық ортада қалыптасуы. Оларға лог-файлдар, IP-мекенжайлар, құрылғы идентификаторлары, метадеректер, ақпараттық жүйелер мен деректер базасындағы жазбалар, банктік транзакциялар, әлеуметтік желілер мен мессенджерлердегі ақпарат, бейнебақылау материалдары және өзге де цифрлық іздер жатады. Мұндай мәліметтердің өзгертілуі, қашықтан жойылуы, шетелдік серверлерде сақталуы немесе қысқа мерзім ішінде қолжетімсіз болып қалуы оларды алу, бекіту, сақтау және верификациялаудың арнайы процестік талаптарын қалыптастыруды қажет етеді.

Дербес деректерді заңсыз жинау, өңдеу және таратуға қарсы қылмыстық-құқықтық нормалардың тиімділігі де дәлелдемелерді дұрыс жинау мен бекітуге тікелей байланысты. Осы саладағы зерттеулерде цифрландыру жағдайында қолданыстағы қылмыстық-құқықтық қорғаудың жеткіліктілігі мен заңнаманы жетілдіру қажеттілігі көрсетіледі [7, 1 б.]. Сондықтан қарастырылып отырған мәселе тек қылмыстық жауаптылықты белгілеумен шектелмей, дәлелдемелерді жинау, бекіту, тексеру, бағалау және қорғаудың қылмыстық-процестік тәртібін де қамтуы тиіс.

Аталған санаттағы істерде дерек ұстаушылардан ақпарат алу ерекше маңызға ие. Тергеу органдары байланыс операторларынан, интернет-провайдерлерден, банктерден, деректер базаларының меншік иелері мен операторларынан, цифрлық платформалардан және басқа ұйымдардан мәлімет алуға мәжбүр болады. Мұндай жағдайда ақпаратты сұратудың құқықтық негізі, алынатын деректердің көлемі мен қажеттілігі, олардың шығу көзі, өзгертілмегендігін растау және кейіннен сотта тексерілу мүмкіндігі нақты айқындалуы қажет. Сонымен қатар дерек ұстаушыларға ақпарат жіберу мен сұратудың өзі дербес деректердің қайталама жария етілуіне әкеп соқпауы тиіс.

Дербес деректерді алу адамның жеке өміріне, байланыс, банк және өзге де заңмен қорғалатын құпияларға араласумен ұштасуы мүмкін. Осыған байланысты жасырын тергеу әрекеттері мен басқа да құқықтарды шектеу құралдарын қолдану кезінде заңдылық, қажеттілік және мөлшерлестік талаптарының сақталуы ерекше маңызға ие. Қылмыстық қудалау мақсаты адамның негізгі құқықтарын негізсіз шектеуге әкелмеуі тиіс, ал алынатын деректер көлемі нақты дәлелдеу қажеттілігімен шектелуі қажет.

Қылмыстық іс материалдарында дербес деректердің құпиялылығын сақтау да өзекті мәселелердің бірі. Электрондық қылмыстық іс жүргізу, іс материалдарына қол жеткізу, құжаттардың көшірмелерін беру, сот актілерін жариялау және ақпараттық жүйелер арқылы құжат алмасу дербес деректердің қайталама таралу қаупін туындатады. Сондықтан жәбірленушілердің, куәлардың, кәмелетке толмағандардың және іске тікелей қатысы жоқ үшінші тұлғалардың мәліметтерін қорғау үшін иесіздендіру, бүркемелеу, редакциялау, қолжетімділікті шектеу және цифрлық ортадағы ақпаратты қорғалған режимде сақтау сияқты процестік тетіктерді жетілдіру қажет.

Жасанды интеллект пен Big Data технологияларын құқық қорғау қызметінде пайдалану зерттеу өзектілігінің тағы бір бағытын құрайды. Биометриялық сәйкестендіру, бейнеаналитика, автоматтандырылған іздеу және үлкен деректер массивтерін салыстыру технологиялары тергеп-тексерудің тиімділігін арттырғанымен, жеке өмірге қол сұғылмаушылық, деректерді қорғау, алгоритмдік ашықтық және автоматтандырылған шешімдердің құқықтық салдарына қатысты жаңа тәуекелдер туғызады. «Жасанды интеллект туралы» Қазақстан Республикасының Заңын талдауға арналған зерттеулерде ЖИ-ді қауіпсіз және адам мүддесіне сай пайдалану үшін оның құқықтық, этикалық және әлеуметтік салдарын кешенді бағалау қажеттігі атап өтіледі [8, 43 б.]. Бұл қылмыстық процесте ЖИ көмегімен алынған мәліметтердің дәлелдемелік мәртебесі мен жол берілетіндігін анықтау қажеттігін күшейтеді.

Мәселенің трансшекаралық сипаты да ерекше назар аударуды талап етеді. Цифрлық дәлелдемелер шетелдік серверлерде, бұлттық сервистерде немесе халықаралық платформаларда сақталуы мүмкін. Дәстүрлі халықаралық құқықтық көмек рәсімдерінің ұзақтығы ақпараттың жойылуына, өзгертілуіне немесе сақтау мерзімінің өтіп кетуіне әкеп соғуы ықтимал. Сондықтан трансшекаралық деректерді жедел сақтау, алу, процестік тұрғыдан заңдастыру және ұлттық қылмыстық процеске енгізу тетіктерін жетілдіру қажеттілігі туындайды.

Дербес деректерді қорғаудың халықаралық стандарттары бұл бағыттың маңызын одан әрі арттырады. Деректерді өңдеудің заңдылығы, мақсаттылығы, деректер көлемін шектеу, қауіпсіздік, ашықтық және тұлғаның өз деректерін бақылау құқығы Еуропалық Одақтың GDPR регламентінде [9], Еуропа Кеңесінің №108 конвенциясында және оны жаңғыртқан халықаралық актілерде бекітілген [10; 11]. Бұл стандарттар қылмыстық процесте дербес деректерді жинау мен пайдалануды қылмыстық

қудалау мүддесімен ғана емес, адамның негізгі құқықтарын қорғау талаптарымен де үйлестіру қажеттігін көрсетеді.

Осылайша, диссертациялық зерттеудің өзектілігі Қазақстан Республикасының қылмыстық-процестік заңнамасындағы дәлелдемелердің заңдылығы мен жол берілетіндігі талаптарын дербес деректердің цифрлық табиғатымен, дерек ұстаушылардан ақпарат алу ерекшеліктерімен, жасырын тергеу әрекеттерімен, жасанды интеллект технологияларымен және трансшекаралық деректер алмасумен өзара байланыстыра отырып, сотқа дейінгі тергеп-тексеру кезеңінде дербес деректермен жұмыс істеудің ғылыми негізделген процестік моделін қалыптастыру қажеттілігімен айқындалады. Мұндай модель деректерді табу, алу, процестік нысанда бекіту, олардың цифрлық тұтастығы мен дереккөзін растау, сотта тексерілуін қамтамасыз ету, қолжетімділікті шектеу және дербес деректердің қайталама жария етілуіне жол бермеу тетіктерін қамтуы тиіс. Бұл бағыттағы ғылыми шешімдер қылмыстық процесте дербес деректерді қорғау мен тиімді дәлелдеудің теңгерімін қамтамасыз етуге мүмкіндік береді.

Тақырыптың зерттелу деңгейі. Дербес деректерді қорғау және дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің қылмыстық-процестік мәселелері қазіргі құқық ғылымында кешенді сипатқа ие ғылыми бағыт ретінде қалыптасып келеді. Бұл тақырыптың ерекшелігі оның бір ғана құқық саласының шеңберімен шектелмейтіндігінде: дербес деректерді қорғау мәселесі конституциялық құқықпен, ақпараттық құқықпен, қылмыстық құқықпен, қылмыстық-процестік құқықпен, криминалистикамен, прокурорлық қадағалаумен, киберқауіпсіздікпен және халықаралық құқықпен тікелей ұштасады. Осы тұрғыдан алғанда, зерттеліп отырған мәселенің ғылыми негіздері белгілі бір деңгейде қалыптасқанымен, дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды тергеп-тексеру барысында туындайтын дәлелдемелік, процестік және кепілдік сипаттағы мәселелер әлі де толық әрі жүйелі түрде шешімін тапты деп айту қиын.

Халықаралық құқықтық доктринада дербес деректерді қорғау мәселесі ең алдымен жеке өмірге қол сұғылмаушылық, ақпараттық өзін-өзі айқындау, адамның цифрлық ортадағы автономиясы, деректер субъектісінің құқықтары және деректерді өңдеудің заңдылығы қағидаттары тұрғысынан зерттелді. Бұл бағытта Сэмюэль Д. Уоррен мен Л. Брандейстің жеке өмірге қол сұғылмаушылық құқығы туралы классикалық тұжырымдары, А. Вестиннің ақпараттық құпиялылық пен тұлғаның өзі туралы ақпаратты бақылау құқығы жөніндегі ілімі, Д. Соловтың жеке өмірге қол сұғылмаушылықты көпқырлы құқықтық категория ретінде түсіндіретін еңбектері, сондай-ақ К. Кунер, Л. Байгрейв, П. Шварц, Г. Гринлиф, О. Лински, А. Кавукян және басқа да авторлардың дербес деректерді қорғау стандарттары жөніндегі зерттеулері ерекше маңызға ие. Бұл еңбектерде дербес деректерді қорғау адамның негізгі құқықтарының құрамдас бөлігі ретінде қарастырылып, деректерді өңдеудің заңдылығы, мақсатқа сәйкестік, пропорционалдық, ашықтық, есеп берушілік,

қауіпке негізделген тәсіл, деректерді жобалау кезеңінен бастап қорғау және қорғау қағидаттары ғылыми тұрғыдан негізделді.

Қазіргі халықаралық зерттеулерде GDPR, Еуропа Кеңесінің №108 және 108+ конвенциялары, трансшекаралық деректер алмасу, жасанды интеллект, Big Data, цифрлық іздер мен алгоритмдік шешім қабылдау мәселелеріне ерекше назар аударылады. М.С. Бисалиев дербес деректерді халықаралық-құқықтық қорғаудың теориялық негіздерін, GDPR мен 108+ конвенциясын, трансшекаралық деректерді беру, жасанды интеллект, тәуекелге негізделген тәсіл және тәуелсіз уәкілетті орган құру мәселелерін кешенді талдаған [12]. Аталған еңбек Қазақстандағы дербес деректерді қорғау режимін халықаралық стандарттармен үйлестіру үшін маңызды болғанымен, сотқа дейінгі тергеп-тексеру кезінде дербес деректерді алу, бекіту және дәлелдеу процесіне енгізу мәселелерін арнайы зерттемейді.

Ақпараттық құқық саласында М.В. Бундин дербес деректердің құқықтық сипатын, олардың шектеулі қолжетімді ақпарат жүйесіндегі орнын, белгілерін, түрлерін және құпиялылық режимін зерттеген [13]. Оның тұжырымдары дербес деректерді құпия ақпараттың ерекше түрі ретінде сипаттау үшін маңызды. Алайда дербес деректерді қылмыстық іс бойынша дәлелдеме ретінде алу, бекіту, сақтау және олардың құпиялылығын сотқа дейінгі өндірісте қамтамасыз ету мәселелері зерттеудің негізгі пәніне кірмеген.

Дербес деректерге қарсы қылмыстық қол сұғушылықтар қылмыстық құқық ғылымында да зерттелген. С.И. Гутник дербес деректерді заңсыз жинау, тарату және пайдалану әрекеттерінің қылмыстық-құқықтық сипаттамасын, жауаптылық негіздері мен саралау мәселелерін қарастырған [14]. Е.В. Хохлова дербес деректерге қатысты заңсыз әрекеттер үшін қылмыстық жауаптылықтың әлеуметтік-құқықтық негіздерін, шетелдік модельдерді, дербес деректердің қылмыстық-құқықтық белгілерін және оларды қорғауды жетілдіру бағыттарын зерттеген [15]. Бұл еңбектер қылмыстық-құқықтық саралау үшін маңызды болғанымен, дәлелдемелерді жинау, тексеру және бағалау, процестік мәжбүрлеу мен құқықтарды шектеудің шектері сияқты қылмыстық-процестік мәселелерді толық қамтымайды.

Қазақстандық құқық ғылымында дербес деректерді қорғаудың ұлттық жүйесі, мемлекеттік бақылау және прокурорлық қадағалау мәселелері бойынша бірқатар зерттеулер жүргізілген. А.М. Амиров Қазақстан Республикасында дербес деректер саласындағы прокурорлық қадағалаудың теориялық негіздерін, әдістемесін және прокурордың құқықтық құралдарын зерттеген [16]. Автор дербес деректерді қорғау, жеке және отбасылық құпияны сақтау, қылмыстық процеске қатысушылар туралы ақпараттың жария етілуіне жол бермеу мәселелерін прокурорлық қадағалаудың маңызды бағыттары ретінде қарастырған. Дегенмен, сотқа дейінгі тергеп-тексеру кезінде дерек ұстаушылардан ақпарат алу, цифрлық дәлелдемелердің жол берілетіндігі, жасырын тергеу әрекеттерін жүргізу және тергеу судьясының бақылауы арнайы кешенді зерттелмеген.

С.Б. Ахметованың еңбегінде Қазақстан Республикасында дербес деректерді мемлекеттік-құқықтық қорғаудың теориялық негіздері, дербес деректердің ұғымы мен түрлері, ұлттық және шетелдік реттеу модельдері, арнайы қағидаттар және мемлекеттік реттеуді жетілдіру мәселелері талданған [17]. Бұл зерттеу дербес деректерді қорғаудың институционалдық және әкімшілік-құқықтық негіздерін ашқанымен, оларды қылмыстық процесте дәлелдемелік мақсатта пайдалану тәртібін арнайы қарастырмайды. Осы диссертацияда С.Б. Ахметова негіздеген мақсатпен шектеу мен деректерді барынша азайту қағидаттары тергеу органы алатын мәліметтердің көлемін айқындайтын қылмыстық-процестік өлшемдер ретінде дамытылады.

Зерттеу тақырыбымен сабақтас еңбектердің қатарына Д.А. Дигайдың ақпаратқа қол жеткізуді құқықтық реттеу мәселелеріне арналған зерттеуін де жатқызуға болады [18]. Автор халықаралық стандарттарды, Қазақстандағы ақпаратқа қол жеткізу тәжірибесін және цифрландыру жағдайындағы ашықтық мәселелерін талдайды. Бұл тұжырымдар жариялылық пен құпиялылық, ақпаратқа қол жеткізу мен дербес деректерді қорғау арасындағы теңгерімді анықтау үшін маңызды, алайда дербес деректерді заңсыз жинау, өңдеу және таратуға байланысты қылмыстық құқық бұзушылықтарды тергеп-тексерудің ерекшеліктерін тікелей қамтымайды.

Қылмыстық-процестік ғылымда сотқа дейінгі тергеп-тексеру, дәлелдемелерді жинау, тексеру және бағалау, процестік кепілдіктер мен қылмыстық процеске қатысушылардың құқықтарын қорғау мәселелері Е.Т. Алимкулов, А.К. Жанибеков, Л.Ш. Берсугурова, Г.Н. Мухамадиева, А.Б. Шарипова, Б.Х. Төлеубекова, С.Д. Оспанов, Т.А. Ханов және басқа отандық ғалымдардың еңбектерінде зерттелген. Алайда дербес деректер қылмыстық процестің арнайы объектісі ретінде, ал оларды алу, сақтау, қорғау, жария етпеу және цифрлық дәлелдемелермен байланыстыру мәселелері дербес кешенді институт деңгейінде жеткілікті қалыптаспаған.

Осылайша, зерттеліп отырған мәселеге арналған ғылыми еңбектерді бірнеше негізгі бағытқа біріктіруге болады: дербес деректерді халықаралық-құқықтық қорғау; ақпараттық-құқықтық режим және құпиялылық; дербес деректерге қарсы қылмыстық қол сұғушылықтар және қылмыстық жауаптылық; ұлттық мемлекеттік-құқықтық реттеу мен прокурорлық қадағалау; сондай-ақ қылмыстық процесс пен дәлелдемелер теориясы. Аталған бағыттардың әрқайсысында елеулі ғылыми база қалыптасқанымен, олардың нәтижелері дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің бірыңғай қылмыстық-процестік моделін қалыптастырмайды.

Осыған байланысты ұсынылып отырған диссертациялық зерттеудің ғылыми орны дербес деректерді қорғаудың жалпы құқықтық режимін сипаттаумен шектелмей, оларды заңсыз жинаумен, өңдеумен және таратумен байланысты істерді сотқа дейінгі тергеп-тексеру барысында туындайтын арнайы қылмыстық-процестік мәселелерді кешенді зерттеуімен айқындалады. Зерттеуде дәлелдеу пәні, дерек ұстаушылардан ақпарат алу,

цифрлық дәлелдемелерді алу, бекіту және верификациялау, олардың жол берілетіндігі, жасырын тергеу әрекеттерін қолдану шектері, дербес деректердің құпиялылығын қамтамасыз ету және процестік кепілдіктер жүйесі қарастырылады.

Сондықтан зерттеу тақырыбының ғылыми әзірлену деңгейін қалыптасу үстіндегі және әрі қарай тереңдетуді қажет ететін бағыт ретінде бағалауға болады. Қазақстан Республикасының қылмыстық-процестік құқығы шеңберінде дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды тергеп-тексеру кезінде дербес деректермен жұмыс істеудің процестік стандарттары, цифрлық дәлелдемелердің жол берілетіндігі, дерек ұстаушылармен өзара іс-қимыл, құқықтарды шектеудің заңдылық өлшемдері және қылмыстық іс материалдарындағы құпиялылықты сақтау тетіктері кешенді түрде арнайы зерттелмеген. Аталған ғылыми олқылық диссертациялық зерттеудің дербес ғылыми бағытын және оның жаңалығын айқындайды.

Зерттеу жұмысының объектісі. Зерттеу жұмысының объектісін дербес деректерді қорғау және оларды заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеру барысында туындайтын қылмыстық-процестік қоғамдық қатынастар, сондай-ақ дербес деректерді қылмыстық іс бойынша дәлелдеу процесіне енгізуге, пайдалануға және қорғауға байланысты қатынастар құрайды.

Зерттеу жұмысының пәні. Зерттеу жұмысының пәнін дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеруді реттейтін қылмыстық-құқықтық және қылмыстық-процестік нормалар, дербес деректер мен цифрлық мәліметтерді анықтау, шұғыл сақтау, алу, процестік бекіту, тексеру, бағалау және қорғау заңдылықтары, дерек ұстаушылармен өзара іс-қимыл жасау, маман мен сарапшыны қатыстыру, құқықтарды шектейтін процестік құралдарды қолдану, сондай-ақ қылмыстық іс материалдарындағы дербес деректердің құпиялылығын қамтамасыз ету практикасы құрайды.

Зерттеу жұмысының мақсаты мен міндеттері. Зерттеудің мақсаты – дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің тиімділігі мен жеке тұлғаның дербес деректерін қорғау арасындағы теңгерімді қамтамасыз ететін ғылыми негізделген қылмыстық-процестік модель әзірлеу, сондай-ақ цифрлық мәліметтерді анықтау, алу, бекіту, тексеру, бағалау және қорғау тәртібін жетілдіру жөніндегі тұжырымдамалық ұсыныстар қалыптастыру.

Осы мақсатқа қол жеткізу үшін мына міндеттер қойылды:

- дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтардың қылмыстық-құқықтық сипаттамасын, олардың белгілерінің дәлелдеу пәнін қалыптастырудағы маңызын және дербес деректердің дәлелдеу процесіндегі орнын айқындау;
- дербес деректер саласындағы ұлттық құқықтық база мен

мемлекеттік реттеу бағыттарын жүйелеу, сондай-ақ ҚР «Дербес деректер және оларды қорғау туралы» Заңындағы жалпыға қолжетімді және қолжетімділігі шектеулі дербес деректерді қылмыстық процесте алу, пайдалану, сақтау және қорғаудың сараланған процестік өлшемдерін негіздеу;

– дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтар бойынша қылмыстық жауаптылық шектері мен саралау өлшемдерінің сотқа дейінгі тергеп-тексеру барысындағы дәлелдеу пәніне ықпалын талдау;

– заңда көзделген жағдайларда прокурордың санкциясымен дерек ұстаушылардан мәлімет сұрату кезінде жәбірленушінің, куәнің немесе өзге де тұлғалардың дербес деректерінің қайталама жариялануын болдырмауға бағытталған, сыртқы сұратуда қылмыстық-құқықтық саралау туралы артық мәліметтерді жария етпеуді көздейтін құпияландырылған процестік тетікті негіздеу;

– дербес деректерді заңсыз жинауға, өңдеуге және таратуға қатысты істерде цифрлық ортадағы дәлелдемелердің, оның ішінде лог-файлдардың, метадеректердің, IP-мекенжайлардың, жүйелік журналдардың, құрылғы идентификаторларының және деректер базасының транзакциялық жазбаларының жол берілетіндігін бағалаудың бірыңғай өлшемдер жүйесін қалыптастыру;

– қылмыстық іс материалдарына қолжетімділік, процестік құжаттардың көшірмелерін беру және сот актілерін жариялау кезінде дербес деректерді иесіздендірудің міндетті тетігін қалыптастыру, оның кезеңдерін, қолданылу шектерін және түпнұсқа материалдарды шектеулі қолжетімділік режимінде сақтау тәртібін негіздеу;

– шетелдік юрисдикцияда сақталған трансшекаралық цифрлық мәліметтер ағымына байланысты қылмыстық істерді тергеп-тексеру кезінде халықаралық ынтымақтастықтың қолданыстағы рәсімдерін талдау және цифрлық ортадағы дәлелдемелердің жойылып кету қаупін ескере отырып, оларды жеделдетудің арнайы процестік тетіктерін ұсыну.

Зерттеу жұмысының әдіснамалық негізі. Диссертациялық зерттеуде дербес деректерді қорғау және дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеру барысында туындайтын қылмыстық-процестік мәселелерді кешенді түрде зерделеу үшін жалпығылыми және арнайы-ғылыми әдістердің өзара үйлескен жүйесі қолданылды.

Диалектикалық, жүйелік және құрылымдық әдістер материалдық-құқықтық белгілердің дәлелдеу пәнімен, цифрлық іздермен, процестік әрекеттермен және дербес деректерді қорғау кепілдіктерімен өзара байланысын анықтауға пайдаланылды. Талдау, синтез, индукция және дедукция әдістері қылмыстық жауаптылық пен саралау мәселелерін, тергеп-тексеру кезеңдеріндегі типтік тәуекелдерді және құқық қолдану практикасының нәтижелерін жүйелеуге мүмкіндік берді.

Формальды-заңи әдіс ұлттық қылмыстық, қылмыстық-процестік және

дербес деректер туралы заңнаманы талдауға; логикалық, жүйелік және мақсатқа сай түсіндіру әдістері тиісті нормалардың мазмұны мен қолданылу шектерін айқындауға; салыстырмалы-құқықтық әдіс халықаралық стандарттар мен шетелдік тәжірибені ұлттық реттеумен салыстыруға қолданылды. Құқықтық модельдеу әдісі сотқа дейінгі тергеп-тексерудің кезеңдік моделін, дерек ұстаушылармен өзара іс-қимыл стандартын, маман мен сарапшының қатысу үлгісін және цифрлық ортадағы дәлелдемелерді бағалау жүйесін әзірлеуге мүмкіндік берді.

Құқық қолдану практикасын зерделеу барысында статистикалық талдау, сауалнама, сарапшылық бағалау, контент-талдау және кейстік талдау әдістері пайдаланылды. Осы әдістер кешені зерттеу мақсатына қол жеткізуге және ұсынылған ғылыми тұжырымдар мен практикалық ұсынымдардың негізділігін қамтамасыз етуге мүмкіндік берді.

Зерттеу жұмысының нормативтік және эмпирикалық базасы. Зерттеудің нормативтік базасын Қазақстан Республикасының Конституциясы, Қазақстан Республикасының Қылмыстық-процестік кодексі, Қазақстан Республикасының Қылмыстық кодексі, Қазақстан Республикасының Цифрлық кодексі, «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңы, «Ақпараттандыру туралы» Қазақстан Республикасының Заңы, «Жедел-іздестіру қызметі туралы» Қазақстан Республикасының Заңы, жасырын тергеу әрекеттерін жүргізу және санкциялау мәселелерін реттейтін нормативтік құқықтық актілер, сондай-ақ дербес деректерді қорғау, ақпараттық қауіпсіздік, киберқауіпсіздік және цифрлық ортадағы дәлелдемелерге қатысты халықаралық құжаттар құрайды.

Зерттеудің эмпирикалық базасына Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің деректері бойынша 2021–2025 жылдары ҚР ҚК-нің 147-бабының 3–5-бөліктерімен тіркелген 302 қылмыстық құқық бұзушылық туралы мәліметтер енгізілді. Оның ішінде 2021 жылы – 35, 2022 жылы – 39, 2023 жылы – 66, 2024 жылы – 64, 2025 жылы – 98 құқық бұзушылық тіркелген. Жалпы массивтің 154-і (51,0%) – 147-баптың 5-бөлігіне, 77-сі (25,5%) – 4-бөлігіне, 71-і (23,5%) – 3-бөлігіне тиесілі. 2021–2025 жылдар аралығында тіркелген құқық бұзушылықтар саны 35-тен 98-ге дейін, яғни 2,8 есеге артқан.

Сонымен қатар эмпирикалық зерттеуде Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің №10 «Сот актілері шығарылған адамдардың саны туралы» және №11 «Қылмыстық құқық бұзушылық жасаған сотталғандардың құрамы туралы» 2021–2025 жылдардағы статистикалық есептерінің деректері құрады. Зерттелген кезеңде ҚР ҚК-нің 147-бабы бойынша 53 адам сотталған, оның 41-і (77,4%) – 147-баптың 5-бөлігі бойынша. 147-баптың 2-бөлігі бойынша 31 іс тоқтатылып, 34 адам ақталған, 3 адам сотталған, ал 5-бөлігі бойынша 1 іс тоқтатылып, 2 адам ақталған және 41 адам сотталған. Сотталғандардың орташа жасы 34,2 жасты құрады, олардың 62,3%-ының білімі – орта білім, 66,0%-ы – жұмыс істемейтін және оқымайтын адамдар.

Аталған статистикалық көрсеткіштер ҚК-нің 147-бабы бойынша сот практикасының құрылымын және оның жекелеген бөліктері бойынша істі тоқтату, ақтау және соттау көрсеткіштерінің арақатынасын анықтауға мүмкіндік берді.

Статистикалық талдау кезінде тіркелген қылмыстық құқық бұзушылықтар, сотталған тұлғалар, ақталған тұлғалар және тоқтатылған қылмыстық істер дербес есептік бірліктер ретінде қарастырылды. Олардың көрсеткіштері бір жиынтыққа механикалық түрде біріктірілмей, қылмыстық қудалау мен сот практикасының әртүрлі кезеңдерін сипаттайтын көрсеткіштер ретінде талданды.

Эмпирикалық зерттеу шеңберінде дербес деректерге қатысты дәлелдемелерді жинау, бекіту және пайдалану мәселелері бойынша 5 нысаналы топты қамтыған 850 респонденттің (Алматы қаласы бойынша) сауалнама нәтижелері пайдаланылды: тергеу практикасы өкілдері – 150, прокурорлар мен тергеу судьялары – 100, қорғау тарапы өкілдері – 150, дерек ұстаушы ұйымдардың өкілдері – 200, деректер субъектілері – 250 адам. Сауалнама нәтижелері бойынша респонденттердің 67,4–78,6%-ы дербес деректермен жұмыс істеудің бірыңғай процестік стандарттарын қолдайтынын көрсеткен; 71,0%-ы цифрлық ортадағы дәлелдемелерді бекіту тәртібін нақтылау қажеттігін атап өткен; деректер субъектілерінің 70,8%-ы деректердің қайта таралу қаупін көрсетсе, 62,0%-ы құқық қорғау органдарына мүлдем жүгінбеген.

Жинақталған эмпирикалық материалдар дербес деректерді алу, бекіту және пайдалану кезінде туындайтын негізгі процестік тәуекелдерді айқындауға мүмкіндік берді. Олардың қатарына дереккөзінің тиісінше көрсетілмеуі, цифрлық ақпараттың тұтастығы мен түпнұсқалығын растайтын белгілердің жеткіліксіз бекітілуі, сұратудың құқықтық негізінің дұрыс айқындалмауы, дерек ұстаушыдан алынған мәліметтердің процестік нысанға толық енгізілмеуі, жасырын тергеу әрекеттері барысында артық көлемдегі дербес деректердің алынуы және іс материалдарына қолжетімділік кезінде олардың қайталама таралу тәуекелі жатады.

Зерттеу жұмысының ғылыми жаңалығы. Диссертациялық зерттеудің ғылыми жаңалығы ұсынылған жұмыстың Қазақстан Республикасында дербес деректерді қорғау және оларды заңсыз жинауға, өңдеуге және таратуға байланысты қылмыстық құқық бұзушылықтарды тергеп-тексерудің қылмыстық-процестік мәселелерін дербес деректердің дәлелдеу процесіндегі қозғалысымен және процестік кепілдіктер жүйесімен сабақтастыра отырып, кешенді түрде қарастыратын зерттеу болуымен айқындалады.

Зерттеудің ғылыми жаңалығы, ең алдымен, зерттеу міндеттерін орындау нәтижесінде алынған мына қорытындылармен негізделеді:

Бірінші кезекте, қылмыстық процестегі дербес деректердің авторлық ұғымы ұсынылып, олар бір мезгілде дәлелдемелік ақпарат көзі және жеке өмірге қол сұғылмаушылық құқығымен қорғалатын ерекше ақпараттық объект ретінде негізделді. Осы тұжырымға сәйкес жалпыға қолжетімді және

қолжетімділігі шектеулі дербес деректердің әрқайсысы үшін өзіндік процестік өлшемдер жүйесі ұсынылды.

Осы негізде іс жүргізудегі тікелей көрінісі ретінде прокурор санкциясымен дерек ұстаушылардан мәлімет сұрату кезінде тергеп-тексеру жүргізіліп жатқан істің нақты бабын сыртқы сұратуда көрсетпеудің құпияландырылған процестік тетігі ұсынылады. Бұл тетік бойынша істің саралау бабы, сұратудың қажеттілігі мен мөлшерлестігі прокурорға жолданатын ішкі негіздемеде толық сақталады, ал заңды тұлғаға жіберілетін сұратуда тек оны орындау үшін қажетті реквизиттер мен деректер көлемі ғана көрсетіледі, осылайша жеке өмірге қол сұғылмаушылық пен құпиялылықты қорғаудың қосымша кепілі қамтамасыз етіледі.

Дәлелдеу процесінің цифрлық сипатын ескере отырып, ҚР ҚПК жүйесіне «цифрлық ортадағы дәлелдемелер» ұғымын енгізу қажеттігі жан-жақты негізделді және оның тек электрондық құжатпен шектелмейтін, цифрлық ортада қалыптасатын лог-файлдар, метадеректер, транзакциялық жазбалар мен аудиттік іздерді де толық қамтитын авторлық анықтамасы ұсынылды. Бұл анықтамамен тікелей байланысты түрде цифрлық ортадағы дәлелдемелердің жол берілетіндігін бағалаудың бірыңғай жүйесі қалыптастырылды. Аталған жүйе ақпараттың алыну заңдылығын, дереккөзінің айқындығын, техникалық және цифрлық тұтастығын, өзгермегендігін хэш-мән немесе электрондық қолтаңба арқылы растауды, сондай-ақ дәлелдеу пәніне қатыстылығы мен жеткіліктілігін бағалаудың нақты өлшемдерін белгілей отырып, дәлелдемелердің жарамсыз деп танылу тәуекелін елеулі түрде төмендетеді.

Зерттеу нәтижесінде сот төрелігінің жариялылығы мен жеке өмірге қол сұғылмаушылық арасындағы тепе-теңдікті қамтамасыз ететін маңызды іс жүргізу кепілдігі – қылмыстық іс материалдары мен сот актілерінде дербес деректерді иесіздендірудің міндетті тетігі негізделді. Бұл тетік дербес деректерді анықтау, оларды техникалық тұрғыдан жабу немесе өшіру, редакцияланған нұсқаны қалыптастыру және толық түпнұсқаны шектеулі қолжетімділік режимінде сақтау кезеңдерінен тұратын айқын рәсімді ұсынады.

Қылмыстық істердің трансшекаралық сипаты күшейген жағдайда, дәстүрлі халықаралық құқықтық көмек рәсімдерінің жеткіліксіздігі ескеріліп, ынтымақтастықты жеделдетудің арнайы процестік тетіктері әзірленді. Бұл орайда, шетелдік серверлер мен бұлтты сервистердегі цифрлық ортадағы дәлелдемелердің жойылып кетуіне жол бермеу үшін деректерді шұғыл сақтап қою сұратылуы, халықаралық сұраулардың стандартталған электрондық нысаны, тәулік бойы жұмыс істейтін ұлттық байланыс және алдын ала сақталған деректерді кейіннен заңдастыру рәсімдері кешенді негіздемесімен ұсынылды.

Аталған жаңалықтардың жиынтығы дербес деректерді заңсыз жинауға, өңдеуге және таратуға байланысты істерде сотқа дейінгі тергеп-тексеру тиімділігі мен адам құқықтарын қорғау арасындағы тепе-теңдікті қамтамасыз ететін арнайы қылмыстық-процестік кепілдіктер жүйесін қалыптастырды.

Бұл жүйе дербес деректердің санаттық режимін нақтылауды, ақпарат алуды стандарттауды, цифрлық ортадағы дәлелдемелерді процестік нысанда бекітуді, жасырын тергеу әрекеттерінің заңдылығын бағалауды және іс материалдарындағы құпиялылықты сақтауды өзара байланыстағы біртұтас механизмге біріктіреді.

Осылайша, зерттеу нәтижелері дербес деректерді заңсыз жинауға, өңдеуге және таратуға қатысты істер бойынша сотқа дейінгі тергеп-тексерудің тиімділігін арттыруға және дербес деректерді қорғаудың процестік кепілдіктерін күшейтуге бағытталған жаңа теориялық қағидалар мен тәжірибелік ұсынымдарды қалыптастыруға негіз болды, бұл өз кезегінде диссертациялық жұмыстың қорғауға шығарылатын тұжырымдарын құрайды.

Қорғауға шығарылатын тұжырымдар:

1. Қылмыстық процесте пайдаланылатын дербес деректердің қылмыстық-процестік ұғымын нақтылау қажет.

Дербес деректер – белгілі бір жеке тұлғаны тікелей немесе жанама айқындайтын не айқындауға мүмкіндік беретін, қылмыстық іс бойынша дәлелденуге жататын мән-жайларды анықтау үшін маңызы бар немесе қылмыстық-процестік әрекеттер барысында пайдаланылатын, алынуының заңдылығына қарамастан арнайы құқықтық қорғауға жататын мәліметтер.

Мұндай деректер қылмыстық процесте қосарлы құқықтық сипатқа ие: бір жағынан, олар қылмыстық іс үшін маңызы бар дәлелдемелік ақпарат көзі ретінде танылады; екінші жағынан, жеке өмірге қол сұғылмаушылық, құпиялылық және дербес деректерді қорғау құқығымен тікелей байланысты ерекше қорғалатын ақпараттық объект болып табылады.

2. ҚР «Дербес деректер және оларды қорғау туралы» Заңындағы жалпыға қолжетімді және қолжетімділігі шектеулі дербес деректердің санаттарын нақтылау, сондай-ақ оларға қылмыстық процесте қолданылатын сараланған алу, пайдалану, сақтау және қорғау режимін бекіту қажет.

ҚР «Дербес деректер және оларды қорғау туралы» Заңында дербес деректер қолжетімділік деңгейі бойынша жалпыға бірдей қолжетімді дербес деректер және қолжетімділігі шектеулі дербес деректер болып бөлінеді. Алайда аталған санаттардың қылмыстық процесс шеңберіндегі нақты мазмұны, оларға жататын мәліметтердің түрлері, оларды алу, бекіту, сақтау және дәлелдеме ретінде пайдалану тәртібі арнайы процестік өлшемдер арқылы айқындалмаған. Мұндай құқықтық нақтылықтың болмауы тергеу және сот тәжірибесінде дербес деректерді әркелкі бағалауға, дәлелдемелердің жол берілетіндігі жөнінде даулардың туындауына және жеке өмірге қол сұғылмаушылық құқығының негізсіз шектелу қаупіне әкеледі.

Осыған байланысты қылмыстық процесте дербес деректердің қолжетімділік деңгейлері бойынша санаттарын тек формалды ақпараттық-құқықтық белгілері негізінде ғана емес, оларды дәлелдеу процесінде алу, пайдалану, сақтау және қорғау тәртібі мен құқықтық режимін ескере отырып нақтылау қажеттілігі негізделеді.

Жалпыға бірдей қолжетімді дербес деректер деп заңды негізде ашық мемлекеттік реестрлерде, ресми интернет-ресурстарда, бұқаралық ақпарат

құралдарында, ашық дереккөздерде немесе дербес деректер субъектісінің ерікті түрде жария етуі нәтижесінде көпшілікке қолжетімді болған, бірақ дәлелдеу процесіне енгізілген кезде дереккөзінің заңдылығы, шынайылығы, өзектілігі, өзгертілмегендігі және дәлелдеу пәнімен байланыстылығы міндетті түрде тексерілуі тиіс жеке тұлғаға қатысты мәліметтерді түсіну ұсынылады.

Қолжетімділігі шектеулі дербес деректер деп субъектінің келісімінсіз немесе заңда көзделген арнайы процестік негізсіз алуға, өңдеуге, пайдалануға және таратуға болмайтын, жеке өмірдің қорғалатын саласына қатысты, жария етілуі немесе заңсыз пайдаланылуы тұлғаның құқықтары мен заңды мүдделеріне зиян келтіруі мүмкін мәліметтерді түсіну ұсынылады. Бұл санатқа ЖСН, жеке басты куәландыратын құжат деректері, тұрғылықты жері немесе мекенжайы, телефон нөмірі, банк деректері, геолокациялық мәліметтер, байланыс құпиясына қатысты деректер, медициналық деректер, биометриялық деректер, кәмелетке толмағандарға қатысты мәліметтер, аккаунттар мен цифрлық сәйкестендіру деректері, сондай-ақ жария етілуі тұлғаның жеке өміріне, ар-намысына, қадір-қасиетіне, мүліктік немесе өзге де заңды мүдделеріне елеулі зиян келтіруі мүмкін өзге де мәліметтер жатқызылуы тиіс.

Аталған санаттарды нақтылау дербес деректерді дәлелдеу процесіне енгізу кезінде алынатын мәліметтердің көлемін шектеуге, оларды алудың заңды негізін дұрыс таңдауға, құқықтарды шектеудің қажеттілігі мен мөлшерлестігін бағалауға, сондай-ақ қылмыстық іс материалдарындағы дербес деректердің құпиялылығын қамтамасыз етуге мүмкіндік береді. Осылайша, дербес деректердің қолжетімділік режимін нақтылау дәлелдемелердің жол берілетіндігін қамтамасыз етудің және адамның жеке өміріне қол сұғылмаушылық құқығын қорғаудың маңызды қылмыстық-процестік кепілдігі ретінде қарастырылуы тиіс.

3. Дерек ұстаушыларға прокурордың санкциясымен жолданатын сұратуларда қылмыстық құқық бұзушылықтың нақты бабын көрсетпеуге негізделген құпияландырылған процестік тетікті қалыптастыру қажет.

ҚР ҚПК 122-бабының нормативтік мазмұны дәлелдемелерді жинауды сотқа дейінгі тергеп-тексеру мен сот талқылауы барысында жүзеге асырылатын процестік әрекеттер жүйесімен байланыстырады. Аталған бап қылмыстық процесті жүргізуші уәкілетті органға жеке және заңды тұлғалардан, лауазымды адамдардан, мекемелер мен ұйымдардан іс мән-жайына қатысы бар құжаттар мен өзге де заттай объектілерді талап ету құқығын береді. Сонымен бірге, ҚР ҚПК сотқа дейінгі тергеп-тексеру органына прокурор санкциясы бойынша өз іс жүргізуіндегі қылмыстық іс материалдары аясында заңды тұлғалардан, лауазымды иелерден, кәсіпорын, мекеме және ұйым басшыларынан банк құпиясы, микрокредиттер, коллекторлық қызмет және коммерциялық құпия туралы мәліметтерді сұрата отырып алуға жол береді.

Алайда дерек ұстаушыларға жолданатын мұндай сұратуларда сотқа дейінгі тергеп-тексерудің ҚР ҚК-нің нақты қай бабы бойынша жүргізіліп

жатқанын көрсету тәжірибесі бірқатар тәуекелдерді туындатады. Әсіресе жеке өмірге қол сұғылмаушылық, жыныстық еркіндік пен жыныстық қол сұғылмаушылық, кәмелетке толмағандарға қатысты қылмыстық құқық бұзушылықтар, медициналық құпия, банктік деректер, интимдік сипаттағы мәліметтер немесе дербес деректерді заңсыз жинау, өңдеу немесе тарату бойынша істерде қылмыстық құқық бұзушылықтың нақты бабын көрсету жәбірленушінің мәртебесін, оқиғаның сипатын және жеке өміріне қатысты арнайы қорғауды қажет ететін ақпаратты дерек ұстаушы ұйымның қызметкерлеріне жанама түрде ашып береді.

Мұндай жағдайда сұрату тек дәлелдеме жинау құралы ғана емес, сонымен бірге дербес деректердің қайталама жария болуына себеп болатын тәуекел көзіне айналады. Тәжірибеде сұрату мәтінімен тек ұйым басшысы ғана емес, кеңсе қызметкері, заң бөлімі, ақпараттық жүйе әкімшісі, комплаенс маманы, бухгалтерия, қауіпсіздік қызметі немесе техникалық персонал танысуы мүмкін. Бұл адамдар қылмыстық процеске қатысушылар болып табылмайды және әрдайым ҚР ҚПК-нің 201-бабында көзделген сотқа дейінгі тергеп-тексеру деректерін жария етпеу туралы арнайы процестік ескерту мен қолхат тәртібімен қамтылмайды. Ал ҚПК-нің 201-бабы сотқа дейінгі тергеп-тексеру деректерінің жария етілмеуі керек екенін және олар тек прокурор рұқсат еткен көлемде ғана жария етілуі мүмкін екенін бекітеді.

Осыған байланысты сотқа дейінгі тергеп-тексеру органының прокурор санкциясымен дерек ұстаушылардан мәліметтер сұратуы кезінде қылмыстық құқық бұзушылықтың нақты саралау бабын сыртқы сұратуда көрсетпеу тетігін енгізу ұсынылады. Бұл тетік сұратудың заңдылығын әлсіретпейді, себебі қылмыстық істің нақты бабы, сұратылатын мәліметтердің дәлелдеу пәнімен байланысы, олардың қажеттілігі мен мөлшерлестігі прокурорға ұсынылатын толық уәжделген материалдарда және қылмыстық іс құжаттарында сақталады. Ал дерек ұстаушыға жолданатын сұратуда тек мәлімет беруге жеткілікті процестік реквизиттер ғана көрсетіледі.

4. ҚР ҚПК жүйесіне цифрлық ортадағы дәлелдемелердің қылмыстық-процестік ұғымын енгізу және олардың жол берілетіндігін бағалаудың бірыңғай жүйесін қалыптастыру қажет.

Дербес деректерді заңсыз жинау, өңдеу және таратумен байланысты қылмыстық істерде дәлелдемелік ақпараттың едәуір бөлігі цифрлық ортада қалыптасады. Оларға лог-файлдар, жүйелік журналдар, метадеректер, IP-мекенжайлар, құрылғы идентификаторлары, деректер базасының транзакциялық жазбалары, электрондық хат-хабарлар, мессенджер жазбалары, әлеуметтік желі материалдары, бұлттық сервистердегі мәліметтер және өзге де цифрлық іздер жатады. Алайда қылмыстық-процестік заңнамада цифрлық ортадағы дәлелдемелер дербес дәлелдемелік категория ретінде толық ашылмағандықтан, оларды алу, бекіту, сақтау, сараптамалық зерттеу және сотта бағалау бойынша біркелкі тәсіл қалыптаспаған.

Осыған байланысты ҚР ҚПК жүйесіне «цифрлық ортадағы дәлелдемелер» ұғымын енгізу және олардың жол берілетіндігін бағалаудың бірыңғай қылмыстық-процестік жүйесін қалыптастыру қажет деп негізделеді.

Авторлық анықтама бойынша, цифрлық ортадағы дәлелдемелер – қылмыстық іс бойынша маңызы бар мән-жайларды анықтауға мүмкіндік беретін, электрондық құрылғыларда, ақпараттық жүйелерде, деректер базаларында, цифрлық платформаларда, байланыс желілерінде немесе бұлттық сервистерде жасалған, сақталған, өңделген, берілген, қабылданған не қалпына келтірілген, заңда көзделген тәртіппен алынған және процестік нысанда бекітілген цифрлық нысандағы нақты деректер.

Цифрлық ортадағы дәлелдемелердің жол берілетіндігін бағалау кезінде олардың алыну заңдылығы, дереккөзінің айқындығы, цифрлық ортадағы ақпараттың тұтастығы, өзгертілмегендігі, метадеректерінің сақталуы, хэш-мәні немесе өзге техникалық сәйкестендіру белгілері арқылы расталуы, сақтау тізбегінің қамтамасыз етілуі, дәлелдеу пәнімен байланыстылығы және сотта тексерілу мүмкіндігі негізгі өлшемдер ретінде танылуы тиіс.

Аталған өлшемдер цифрлық ортадағы дәлелдемелерді тек электрондық құжат ретінде ғана емес, цифрлық ортада пайда болатын барлық дәлелдемелік ақпарат ретінде бағалауға мүмкіндік береді. Мұндай ақпаратқа лог-файлдар, метадеректер, жүйелік жазбалар, транзакциялық деректер, бұлттық сервистердегі мәліметтер және өзге де цифрлық іздер жатады. Сондықтан цифрлық ортадағы дәлелдемелердің қылмыстық-процестік ұғымын бекіту дербес деректерді заңсыз жинау, өңдеу және таратумен байланысты істерде алынған мәліметтердің заңдылығын, тұтастығын және сотта пайдалануға жарамдылығын қамтамасыз етудің маңызды кепілдігі болып табылады.

5. Жарияланатын сот актілері мен іске қатысы жоқ тұлғаларға берілетін қылмыстық іс материалдарының көшірмелерінде дербес деректерді иесіздендірудің міндетті тетігін қалыптастыру қажет.

Қылмыстық процесте дербес деректерді қорғау оларды тергеу барысында заңды түрде алумен ғана шектелмеуі тиіс. Іс материалдарына тіркелгеннен кейін жәбірленушілердің, куәлардың, кәмелетке толмағандардың, сарапшылардың, мамандардың, жәбірленушінің туыстарының, сондай-ақ іске тікелей қатысы жоқ үшінші тұлғалардың дербес деректері қылмыстық іс материалдарында, сот актілерінде және электрондық сот жүйелерінде сақталады. Мұндай деректердің кейіннен жариялануы немесе үшінші тұлғаларға қолжетімді болуы дербес деректердің қайталама таралуына, жәбірленушілер мен куәлардың қауіпсіздігіне қатер төндіруге және тұлғаның ар-намысы мен жеке өміріне зиян келтіруге әкелуі мүмкін.

Осыған байланысты қылмыстық іс материалдары мен сот актілерінде дербес деректерді иесіздендірудің міндетті қылмыстық-процестік тетігін қалыптастыру қажет деп негізделеді. Иесіздендіру қылмыстық процесте қосымша техникалық әрекет ретінде емес, сот төрелігінің жариялылығы мен жеке өмірге қол сұғылмаушылық арасындағы тепе-теңдікті қамтамасыз ететін дербес процестік кепілдік ретінде танылуы тиіс. Қылмыстық істің толық түпнұсқасы өзгеріссіз сақталып, оған қолжетімділік процестік мәртебе мен қажеттілікке қарай шектеледі.

6. Шетелдік юрисдикцияда сақталған трансшекаралық цифрлық

мәліметтер ағымына қатысты тергеуде халықаралық ынтымақтастықты жеделдетудің арнайы процестік тетіктерін қалыптастыру қажет.

Дербес деректерді заңсыз жинау, өңдеу және таратумен байланысты қылмыстық істердің едәуір бөлігі трансшекаралық сипатқа ие. Деректер шетелдік серверлерде, бұлттық сервистерде, халықаралық цифрлық платформаларда, әлеуметтік желілерде, мессенджерлерде немесе шетелдік байланыс операторларының инфрақұрылымында сақталуы мүмкін. Мұндай жағдайларда дәстүрлі халықаралық құқықтық көмек рәсімдерінің ұзақтығы цифрлық ортадағы дәлелдемелердің жойылуына, лог-файлдардың сақталу мерзімінің өтіп кетуіне, аккаунттардың бұғатталуына немесе қылмыстық іздердің жоғалуына әкеледі. ҚР ҚПК-де құқықтық көмек бір мемлекеттің құзыретті органдарының екінші мемлекеттің құзыретті органдарына сұрау салуы арқылы жүзеге асырылатын механизм ретінде қарастырылғанымен, цифрлық дәлелдемелердің жедел сақталуын қамтамасыз ету үшін бұл рәсімдерді қосымша процестік құралдармен толықтыру қажет.

Осыған байланысты трансшекаралық дербес деректер ағымына қатысты қылмыстық істерді тергеу кезінде халықаралық ынтымақтастықты жеделдетудің арнайы қылмыстық-процестік тетіктерін қалыптастыру қажет деп негізделеді.

Бұл бағытта Қазақстан Республикасының Будапешт конвенциясына қосылу мәселесін жеделдету, цифрлық ортадағы дәлелдемелерді трансшекаралық алу бойынша Будапешт конвенциясының Екінші қосымша хаттамасында көзделген тетіктерді ұлттық қылмыстық-процестік заңнамамен үйлестіру, сондай-ақ БҰҰ-ның Киберқылмысқа қарсы конвенциясына қосылу немесе оны ратификациялау кезінде адам құқықтарын, дербес деректерді қорғау, соттық бақылау, прокурорлық қадағалау, қажеттілік және мөлшерлестік қағидаттарын сақтау кепілдіктерін нақтылау қажет деп негізделеді.

Сонымен қатар трансшекаралық дербес деректерді беру кезінде Еуропа Кеңесінің 108+ Конвенциясында көзделген деректерді қорғау, қауіпсіздік, мақсаттылық, мөлшерлестік және тәуелсіз бақылау қағидаттарын ескеру қажет.

Диссертациялық зерттеудің теориялық маңыздылығы. Диссертациялық зерттеудің теориялық маңыздылығы дербес деректерді қылмыстық-процес ғылымындағы дербес зерттеу объектісі ретінде негіздеуде. Жұмыс дербес деректердің құқықтық сипаты туралы ақпараттық-құқықтық және халықаралық-құқықтық тұжырымдарды қылмыстық-процестік дәлелдеу теориясымен байланыстырады. Бұл қылмыстық процесс бойынша дәлелдемелердің жол берілетіндігі, процестік нысан, жеке өмірге қол сұғылмаушылық, құпиялылық, цифрлық ортадағы дәлелдемелер және құқықтарды шектеу институттарының өзара байланысын жаңа қырынан түсіндіруге мүмкіндік береді.

Диссертациялық зерттеудің тәжірибелік маңыздылығы. Зерттеу нәтижелері тергеушілер, прокурорлар, тергеу судьялары, адвокаттар және дерек ұстаушы ұйымдар үшін әдістемелік ұсынымдар әзірлеуде, сондай-ақ

цифрлық ортадағы дәлелдемелерді алу, бекіту, сақтау және бағалау жөніндегі ведомстволық нұсқаулықтарды жетілдіруде қолданылуы мүмкін. Ұсынылған алгоритмдер дербес деректерді заңсыз жинауға, өңдеуге және таратуға қатысты істер бойынша алғашқы әрекеттерді жоспарлауға, цифрлық ортадағы ақпаратты жоғалтпай бекітуге, дерек ұстаушыларға дұрыс сұрау жолдауға, ЖТӘ қолдану туралы өтінішхаттарды негіздеуге және алынған мәліметтердің жол берілетіндігін бағалауға көмектеседі.

Тәжірибелік ұсынымдар қылмыстық процесте дербес деректердің құпиялылығын сақтауға да бағытталған. Іс материалдарындағы деректерді санаттау, қорғау режимін белгілеу, көшірме беруді шектеу, жария сот талқылауы кезінде деректерді иесіздендіру және электрондық тасымалдағыштардың қозғалысын есепке алу тәрізді тетіктер дербес деректердің қайталама таралу тәуекелін төмендетеді. Бұл ұсыныстар құқық қорғау органдарының әдістемелік құжаттарын, прокурорлық қадағалау өлшемдерін және сот бақылау тәжірибесін жетілдіруде пайдаланылуы мүмкін.

Зерттеу жұмысының ғылыми-теориялық мәні. Жұмыс дербес деректерді қылмыстық процесте қорғаудың ғылыми категорияларын нақтылап, процестік кепілдіктердің мазмұнын дербес деректермен жұмыс істеу контексінде қайта пайымдауға мүмкіндік береді. Сонымен қатар, цифрлық ортадағы дәлелдемелердің жол берілетіндігін бағалау және іс материалдарындағы деректердің құпиялылығын сақтау жөніндегі доктриналық тәсілді толықтырады.

Зерттеу нәтижелерінің сыннан өтуі. Зерттеу нәтижелері бойынша жалпы 11, оның ішінде Scopus халықаралық деректер базасында индекстелетін ғылыми журналдарда 2, Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым және жоғары білім саласындағы сапаны қамтамасыз ету комитеті ұсынған ғылыми басылымдарда 3, халықаралық конференция материалдарында 2 мақала жарияланды. Сонымен қатар Комитет ұсынған ғылыми басылымдарға 1 ғылыми мақала жариялануға қабылданған және қазіргі уақытта басылымда. Диссертациялық зерттеу нәтижелері бойынша 2 ғылыми еңбекке авторлық құқық объектілеріне құқықтарды мемлекеттік тіркеу туралы куәлік алынды.

Зерттеу жұмысының құрылымы. Зерттеу жұмысының құрылымы оның мақсаты мен міндеттеріне, сондай-ақ зерттелетін мәселелерді баяндаудың логикалық бірізділігіне сәйкес айқындалды. Диссертация нормативтік сілтемелерден, анықтамалардан, белгілер мен қысқартулардан, кіріспеден, тоғыз бөлімді қамтитын үш тараудан, қорытындыдан, пайдаланылған әдебиеттер тізімінен және қосымшалардан тұрады.

1 ҚЫЛМЫСТЫҚ ПРОЦЕСТЕ ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУДЫҢ ҚҰҚЫҚТЫҚ РЕЖИМІ МЕН ПРОЦЕСТІК КЕПІЛДІКТЕРІНІҢ ТЕОРИЯЛЫҚ НЕГІЗДЕРІ

1.1 Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтардың қылмыстық-құқықтық сипаттамасы, қылмыстық жауаптылықтың шектері және саралау өлшемдері

Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің қылмыстық-процестік мәселелерін зерттеу, ең алдымен, қылмыстық жауаптылықтың қандай жағдайларда туындайтынын және қылмыстық құқық бұзушылық құрамының қандай белгілері дәлелдеуге жататынын айқындаудан басталуы тиіс. Қылмыстық-процестік қызмет материалдық-құқықтық негіздерден оқшау қарастырыла алмайды: қылмыстық заң қорғалатын объектіні, тыйым салынған әрекетті, оның салдарын, субъектісі мен кінә нысанын белгілесе, қылмыстық-процестік заң осы белгілерді қандай нақты деректермен және қандай тәртіппен анықтауға болатынын реттейді. Сондықтан қылмыстық-құқықтық сипаттама тек теориялық мақсатта емес, кейінгі дәлелдеу пәнін, цифрлық іздерді және тиісті процестік құралдарды анықтайтын бастапқы бағдар ретінде қарастырылуы маңызды [6; 19].

Дербес деректерге қатысты қылмыстық-құқықтық тыйымдарды дұрыс түсіндіру үшін Қылмыстық кодекстің нормаларын дербес деректер туралы салалық заңнамамен өзара байланыста қолдану қажет. ҚР ҚК-нің 147-бабы бланкеттік сипатқа ие: қылмыстық заң жауаптылықтың негізгі белгілерін белгілегенімен, «дербес деректер», «жинау», «өңдеу», «тарату», «келісім», «қорғау шаралары» және деректер субъектілері мен операторларының міндеттері «Дербес деректер және оларды қорғау туралы» Заңда және өзге де салалық нормативтік құқықтық актілерде ашылады [2; 19]. Демек, әрекеттің заңсыздығы тек Қылмыстық кодекстің диспозициясын формалды оқумен анықталмайды, ол деректерге қатысты нақты операцияның құқықтық негізін, мақсатын, көлемін, өкілеттігін, мерзімін, қауіпсіздік талаптарын және үшінші тұлғаларға беру шарттарын тексеруді талап етеді.

С.Б. Ахметова дербес деректерді қорғау режимін заңдылық, әділдік пен ашықтық, мақсатпен шектеу, деректерді барынша азайту, дәлдік, сақтау мерзімін шектеу, тұтастық пен құпиялылық және есеп берушілік қағидаттарының өзара байланысы арқылы түсіндіреді. Деректерді барынша азайту қағидатының мазмұнын аша отырып, автор: «Деректерді барынша азайту қағидаты жиналатын ақпарат көлемін қатаң қажеттілік өлшемімен шектейді. Дербес деректер оларды өңдеудің нақты мақсаттарына барабар және сол мақсаттарға тікелей қатысты болуы тиіс (артық ештеңе болмауы керек)», – деп атап өтеді [17, 85 б.]. Бұл қағидаттар дербес деректерді заңсыз

жинау, өңдеу және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеру шеңберінде екі өлшемде қылмыстық-процестік мәнге ие болады. Біріншіден, олар «заңсыздық» белгісін дәлелдеу пәні деңгейінде нақтылайды: мақсатпен шектеу мен деректерді барынша азайту қағидаттарынан ауытқу – күдіктінің жинау, өңдеу немесе тарату әрекетінің құқыққа қайшылығын дәлелдеуге тиіс мән-жайлар қатарына кіреді. Екіншіден, дәл осы қағидаттар – атап айтқанда, деректерді барынша азайту және сақтау мерзімін шектеу – тергеу, анықтау және жедел-іздестіру органдарының өздерінің дерек ұстаушылардан ақпарат алу, оны бекіту және іс материалдарына қосу өкілеттігінің процестік шегін белгілейді: дәлелдеу пәнімен шектелмеген «артық дербес дерек» алу мен сақтау сотқа дейінгі тергеп-тексерудің заңдылығына қатысты дербес проблема ретінде қарастырылады. Осылайша, деректерді қорғау қағидаттары бұл жұмыста материалдық құқық бұзушылықтың құрамын ашудың да, сотқа дейінгі сатыда дәлелдемелерді жинау мен бекітудің процестік шегін айқындаудың да ортақ әдіснамалық негізі болып табылады.

М.С. Бисалиев дербес деректерді қорғаудың халықаралық-құқықтық режимін цифрлық іздер, трансшекаралық ақпарат алмасу және құқықтық реттеудің технологиялық тетіктерімен байланыстыра зерттейді [12]. Цифрлық іздердің дербес деректерді қорғаудағы маңызын аша отырып, автор: «Дербес деректермен жасалатын кез келген операция цифрлық із қалдырады – бұл жүйелік журналда осы деректермен кімнің, қашан және қандай әрекеттер жасағаны туралы автоматты түрде тіркелетін жазба. Тиісті түрде қолданылған жағдайда цифрлық іздер (лог-файлдар) белгіленген талаптардың сақталуын, есептілікті және аудит жүргізу мүмкіндігін қамтамасыз етудің пәрменді тетігіне айналады», – деп көрсетеді [12, 131 б.]. Аталған тұжырым дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеру үшін ерекше маңызға ие. Цифрлық іздер дербес деректермен жасалған операцияның өзін ғана емес, оның уақытын, орындалу ретін, пайдаланылған есептік жазбаны, қолжетімділік субъектісін және белгілі бір жағдайларда деректердің кейінгі қозғалысын қалпына келтіруге мүмкіндік береді. Осыған байланысты ақпараттық жүйедегі авторизация жазбалары, лог-журналдар, метадеректер, жүктеу тарихы, құрылғы идентификаторлары, желілік байланыстар мен транзакциялық жазбалар ҚК-нің 147-бабында көзделген әрекеттің объективтік белгілерін және оны белгілі бір тұлғамен байланыстыратын мән-жайларды анықтауда елеулі дәлелдемелік ақпарат көзі бола алады. Сонымен бірге цифрлық іздің болуы оны автоматты түрде қылмыстық-процестік дәлелдемеге айналдырмайды. Мұндай мәліметтердің дәлелдемелік мәні оларды заңда белгіленген тәртіппен алу, дереккөзін айқындау, процестік нысанда бекіту, тұтастығын сақтау және кейіннен тексеру мүмкіндігі қамтамасыз етілген жағдайда ғана қалыптасады. Осы тұрғыдан М.С. Бисалиевтің цифрлық іздерді есептілік пен аудит құралы ретінде қарастыратын ұстанымы осы зерттеуде қылмыстық-процестік бағытта дамытылады: цифрлық іздер дербес деректермен жасалған

әрекеттерді реконструкциялауға мүмкіндік беретін бастапқы цифрлық мәлімет ретінде қарастырылып, олардың қылмыстық іс бойынша пайдаланылуы тиісті процестік нысанмен қамтамасыз етілуі тиіс. Бұл мәселе цифрлық мәліметтердің сақталу ерекшеліктерімен де күрделене түседі. Лог-журналдар мен өзге де жүйелік жазбалардың бір бөлігі шектеулі мерзім сақталуы, автоматты түрде қайта жазылуы немесе кейін өзгертілуі мүмкін. Сондықтан сотқа дейінгі тергеп-тексерудің бастапқы кезеңінде ықтимал цифрлық іздерді уақтылы анықтау, оларды шұғыл сақтау, тиісті дерек ұстаушыны белгілеу және процестік тәртіппен бекіту кейінгі дәлелдеудің қажетті шарты ретінде қарастырылуы тиіс.

ҚР ҚК-нің 147-бабы жеке өмірге қолсұғылмаушылықты және дербес деректер мен оларды қорғау туралы заңнаманы сақтауды қылмыстық-құқықтық қорғау объектісіне айналдырады [19]. Аталған баптың негізгі тікелей объектісі – адамның жеке өміріне қолсұғылмаушылық, жеке және отбасы құпиясының сақталуы, сондай-ақ өзінің дербес деректерін бақылау және оларды заңсыз ақпараттық әрекеттерден қорғау жөніндегі конституциялық құқықтары мен заңды мүдделері. Бұл жерде қылмыстық-құқықтық қорғау тек ақпараттың құпия сипатына ғана емес, адамның ақпараттық автономиясына, қадір-қасиетіне, қауіпсіздігіне және өзінің жеке басына қатысты мәліметтердің қозғалысын бақылау мүмкіндігіне бағытталады [1; 24, Б. 35-36].

Дербес деректерге қарсы қолсұғушылықтың нысанасы – белгілі бір жеке тұлғаны тікелей немесе жанама айқындайтын не айқындауға мүмкіндік беретін, электрондық, қағаз немесе өзге материалдық жеткізгіште тіркелген мәліметтер. Олардың қылмыстық-құқықтық маңызы ақпараттың тасымалдағышымен емес, тұлғаны сәйкестендіру мүмкіндігімен, деректердің қорғалатын салаға қатыстылығымен және заңсыз әрекет нәтижесінде тұлғаның құқықтарына келтірілген немесе келтірілуі мүмкін зиянмен анықталады [2; 17, 55 б.]. Сондықтан қағаздағы медициналық карта, бұлттық сервистегі лог-файл, банктің транзакциялық жазбасы, мессенджердегі хабарлама немесе биометриялық шаблон бірдей жағдайда дербес деректердің қылмыстық-құқықтық нысанасы бола алады.

ҚР ҚК-нің 147-бабы дербес деректермен байланысты заңсыз әрекеттерге жауаптылықты белгілеу кезінде қорғалатын мәліметтерді мазмұны бойынша екі негізгі топқа ажыратады. Бұл ажырату баптың 2-бөлігінде (жинау және өңдеу) және 4-бөлігінде (тарату) бірдей логикамен қайталанады. Бірінші топқа жеке немесе отбасылық құпияны құрайтын жеке өмір туралы мәліметтер жатады. Мұндай ақпараттың ерекше қорғалуы оның адамның автономиясымен, интимдік, медициналық, отбасылық, әлеуметтік және өзге де сезімтал салаларымен байланысына негізделеді. Екінші топты өзге дербес деректер құрайды – жеке басты сәйкестендіруге мүмкіндік беретін, бірақ жеке өмірдің сезімтал саласына тікелей қатысы жоқ ақпарат (мысалы, ЖСН, мекенжай, байланыс деректері, банктік реквизиттер, геолокация, аккаунт және құрылғы идентификаторлары, кәсіби және білім туралы мәліметтер). Саралау кезінде деректің қай топқа жататынын анықтау

шешуші мәнге ие, өйткені заң оларға әртүрлі құрам түрін белгілейді: бірінші топ бойынша құрам формальды – келісімсіз жинаудың немесе таратудың өзі-ақ жеткілікті, ал екінші топ бойынша құрам материалдық – әрекет заңсыз болғанымен, тұлғаның құқығы мен заңды мүддесіне елеулі зиян келтірілгені дәлелденбейінше, қылмыс құрамы жоқ деп танылады [19, 1].

Қылмыстық-құқықтық қорғаудың дербес объектісі ретінде тек деректердің өзі емес, олармен жұмыс істеудің заңда белгіленген тәртібі де көрінеді. ҚР ҚК-нің 147-бабының 1-бөлігі дербес деректерді қорғау жөніндегі міндет жүктелген тұлғаның қорғау шараларын сақтамауына жауаптылық белгілейді. Демек, бұл құрамда қоғамдық қатынастардың екі элементі қорғалады: біріншісі – нақты тұлғаның дербес деректері, екіншісі – деректердің құпиялылығы, тұтастығы және заңды қолжетімділігі қамтамасыз етілетін ұйымдастырушылық-техникалық режим. Бұл ерекшелік қылмыстық құқық бұзушылық субъектісін, оның міндеттерінің қайнар көзін және сол міндеттерді орындау мүмкіндігін жеке дәлелдеуді талап етеді.

Қылмыстық жауаптылықтың шегін дұрыс белгілеу үшін «жинау», «өңдеу» және «тарату» әрекеттерін біртекті ұғымдар ретінде қарастыруға болмайды. Олар дербес деректердің өмірлік циклiндегі әртүрлі операцияларды білдіреді және әрқайсысы дербес дәлелдеу міндетін қалыптастырады. Салалық заңнама дербес деректерді жинауды оларды алуға бағытталған әрекеттер ретінде, өңдеуді жинақтау, сақтау, өзгерту, толықтыру, пайдалану, иесіздендіру, бұғаттау және жоюды қамтитын операциялар жиынтығы ретінде түсіндіреді [2]. Тарату дербес деректерді тұлғалардың белгісіз тобына беру немесе өзге тәсілмен қолжетімді ету арқылы сипатталады.

Заңсыз жинау деп мәліметтерді субъектінің келісімінсіз немесе заңда көзделген өзге құқықтық негізсіз алу ғана емес, деректерге заңды түрде берілген қолжетімділіктің мақсаты мен өкілеттік шегінен тыс пайдалану да түсінілуі тиіс. С.Б. Ахметова құқық қолдану тәжірибесінде дербес деректермен жұмыс істейтін меншік иелері мен операторлар өз қызметінің құқықтық негізін және қойылған мақсаттарға жету үшін қажетті деректер көлемін алдын ала айқындау қа жетекенін атап көрсетеді: «Құқық қолдану тәжірибесінде меншік иелері мен операторлар дербес деректермен байланысты өз қызметін талдап, мақсаттары мен міндеттерін іске асыру үшін деректерді өңдеудің құқықтық негіздері мен қажетті көлемін айқындауға және осы талдау негізінде талап етілетін дербес деректердің тізбесін бекітіп, түзетіп отыруы тиіс» [17, 89 б.]. Осы тұрғыдан қызметкердің ақпараттық жүйеге жалпы қолжетімділік құқығының болуы оның жүйедегі барлық дербес деректермен кез келген мақсатта жұмыс істеуіне автоматты түрде құқықтық негіз бермейді. Мысалы, қызметкердің жүйеге заңды түрде кіруге құқығы болғанымен, өзінің қызметтік міндеттеріне қатысы жоқ тұлғаның мәліметтерін қарауы, жүктеуі немесе көшіріп алуы нақты мән-жайларға байланысты заңсыз жинау немесе өңдеу белгісі ретінде бағалануы мүмкін. Сондықтан әрекеттің заңсыздығын анықтау кезінде келісімнің бар-жоғымен қатар деректерді алудың мақсаты, қажетті көлемі, тұлғаның функционалдық

рөлі мен өкілеттік шегі де тексерілуі тиіс [2; 17, 89 б.].

Заңсыз өңдеу дербес деректерді бастапқы заңды мақсаттан тыс пайдалануды, тиісті құқықтық негізсіз өзге ақпараттық жүйеге біріктіруді, өзгерту мен сақтауды, сондай-ақ профилинг немесе автоматтандырылған талдау сияқты операцияларды оларды жүргізуге заңды негіз болмаған не мұндай әрекеттер бастапқы өңдеу мақсатымен үйлеспеген жағдайларда қамтуы мүмкін. С.Б. Ахметова мақсатпен шектеу қағидатының мазмұнын аша отырып: «Мақсатпен шектеу қағидаты дербес деректерді нақты тұжырымдалған, айқын және заңды мақсаттарсыз жинауға тыйым салады, сондай-ақ оларды бастапқы мақсаттармен үйлеспейтін мақсаттарда кейіннен пайдалануға жол бермейді», – деп көрсетеді [17, 84 б.]. Автор сонымен қатар деректерді барынша азайту қағидаты жиналатын ақпарат көлемін қатаң қажеттілік өлшемімен шектейтінін, ал сақтау мерзімін шектеу қағидаты дербес деректердің өңдеу мақсатына қажетті уақыттан артық сақталмауын талап ететінін атап өтеді [17, 85 б.]. Осы тұрғыдан белгілі бір қызмет көрсету немесе өзге заңды мақсат үшін алынған дербес деректерді кейін субъектінің келісімінсіз не өзге заңды негізсіз маркетингтік мақсатта, тұлғаны бақылау үшін, оған қысым көрсетуге немесе қылмыстық мақсатта пайдалану бастапқы өңдеудің құқықтық негізімен автоматты түрде ақталмайды. Біздің ойымызша, мұндай кейінгі операцияның заңдылығы оның бастапқы мақсатпен үйлесімділігіне, дербес құқықтық негізінің болуына, пайдаланылатын деректер көлемінің қажеттілігіне және сақтау мерзімінің сақталуына қарай жеке бағалануы тиіс.

Салалық заңнамадағы «өңдеу» ұғымы таратуды да кең мағынада қамтуы мүмкін. Алайда ҚР ҚК-нің 147-бабының 2-бөлігі өзге дербес деректерді заңсыз жинау және (немесе) өңдеуді «таратуды қоспағанда» бөлек белгілейді, ал тарату 4 және 5-бөліктерде дербес қылмыстық-құқықтық әрекет ретінде көрсетілген [19]. Осыған байланысты қылмыстық құқықта өңдеу ұғымы баптың ішкі жүйесіне сай тар мағынада қолданылуы тиіс: таратуға дейінгі немесе одан бөлек операциялар 2–3-бөліктермен, ал үшінші тұлғаларға беру немесе көпшілікке қолжетімді ету 4–5-бөліктермен бағаланады.

Заңсыз тарату нақты адресатқа беру, бірнеше тұлғаға жіберу, ортақ деректер базасына рұқсат беру, интернет-ресурста жариялау, мессенджер тобына орналастыру, бұқаралық ақпарат құралдары немесе телекоммуникация желілері арқылы тарату сияқты әртүрлі нысандарда жүзеге асуы мүмкін. Тарату әрекеті мәліметтің үшінші тұлғаға нақты қолжетімді болған сәтінен аяқталған деп бағалануға негіз бар. Егер кінәлі жариялауға бағытталған әрекеттер жасағанымен, техникалық себептермен мәлімет адресатқа жетпесе, қылмысқа оқталу туралы мәселе қылмыстық заңның жалпы ережелері бойынша шешілуі тиіс.

Осы үш әрекетті ажыратудың практикалық маңызы зор. Бір оқиғада деректерді алдымен заңсыз жинау, кейін өңдеу, соңында тарату орын алуы мүмкін. Мұндай жағдайларда құқықтық бағалау әр әрекеттің дербес объектіге, салдарға және қылмыстық-құқықтық мағынаға ие болуына қарай

жүргізіледі. Егер кейінгі тарату алдыңғы жинау немесе өңдеудің табиғи жалғасы бола тұра заңның басқа бөлігімен қорғалатын дербес қоғамдық қатынасқа қол сұқса, қылмыстық құқық бұзушылықтар жиынтығы немесе бап бөліктерінің бәсекелестігі туралы мәселе туындайды.

ҚР ҚК-нің 147-бабының қолданыстағы редакциясы бес бөліктен тұрады және дербес деректермен байланысты заңсыз әрекеттерді қоғамдық қауіптілік сипаты мен тәсіліне қарай саралайды [19]. Оның 1-бөлігі дербес деректерді қорғау шараларын сақтамауға, 2-бөлігі жеке немесе отбасы құпиясын құрайтын жеке өмір туралы мәліметтерді келісімсіз заңсыз жинауға немесе өзге дербес деректерді заңсыз жинау және (немесе) өңдеуге, 3-бөлігі осы әрекеттердің сараланған түрлеріне, 4-бөлігі жеке немесе отбасы құпиясын құрайтын мәліметтерді келісімсіз таратуға немесе өзге дербес деректерді заңсыз таратуға, 5-бөлігі таратудың сараланған нысандарына жауаптылық белгілейді. Мұндай құрылым заң шығарушының қорғау шараларын бұзуды, жинау мен өңдеуді және таратуды бір-бірінен дербес қоғамдық қауіпті әрекеттер ретінде қарастырғанын көрсетеді.

Баптың 1-бөлігінде қылмыстық құқық бұзушылықтың арнайы субъектісі көзделеді: ол дербес деректерді қорғау шараларын қабылдау міндеті заңмен, қызметтік өкілеттікпен, еңбек шартымен, ішкі актімен немесе ақпараттық жүйедегі рөлімен жүктелген тұлға. Объективтік жағы тиісті шараларды сақтамау және соның нәтижесінде елеулі зиян келтіру арқылы сипатталады. Сондықтан қызметкердің формалды лауазымы жеткіліксіз, оның нақты міндеті, қауіпсіздік шараларын орындау мүмкіндігі, бұзылған талап, салдар және себептік байланыс анықталуы тиіс. Техникалық ақаудың өзі кінәні автоматты түрде дәлелдемейді.

2-бөлік екі құқықтық нысанды біріктіреді: біріншісі – адамның жеке немесе отбасы құпиясын құрайтын жеке өмірі туралы мәліметтерді оның келісімінсіз заңсыз жинау, екіншісі – өзге дербес деректерді заңсыз жинау және (немесе) өңдеу. Диспозицияның синтаксистік құрылымы елеулі зиян белгісін қолдану мәселесінде әркелкі түсіндіруге мүмкіндік беруі ықтимал. Құқықтық айқындық қағидаты тұрғысынан елеулі зиянның әр баламаға қатыстылығын заң мәтінінде не нормативтік түсіндірмеде нақтылау қажет. Қолданыстағы редакцияны қолдану кезінде тергеу органы залалдың болуын, мазмұнын және әрекетпен себептік байланысын барлық жағдайда мұқият тексеруі тиіс. Бұл – қылмыстық заңды кеңейтіп түсіндіруге жол бермеудің кепілдігі болып табылады.

3-бөлік 2-бөліктегі әрекеттердің қызметтік жағдайды пайдалану, ақпаратты жасырын алуға арналған арнайы техникалық құралдарды қолдану, ақпараттық жүйеге заңсыз қол жеткізу немесе телекоммуникация желісі арқылы берілетін ақпаратты заңсыз ұстап қалу, пайда немесе артықшылық алу мақсаты, сондай-ақ адамның қызметтік, кәсіби немесе қоғамдық міндеттерін орындауына кедергі келтіру не сол үшін кек алу мақсатымен жасалған түрлерін қамтиды [19]. Бұл белгілер әрекеттің тәсілі мен мотивін саралаушы мән-жайға айналдырады және әрқайсысы дербес дәлелденуі тиіс.

4-бөлік тарату әрекеттерін дербес құрам ретінде бекітеді. Тарату

кезінде деректер бұрын алынған болуы мүмкін, бірақ жауаптылық үшін кінәлінің мәліметті үшінші тұлғаларға заңсыз жеткізуі немесе қолжетімді етуі шешуші мәнге ие. 5-бөлік таратудың көпшілік алдында сөз сөйлеу, бұқаралық ақпарат құралдары, телекоммуникация желілері, ақпараттандыру объектілері немесе онлайн-платформалар арқылы жасалған түрлерін, сондай-ақ қызметтік, кәсіби немесе қоғамдық міндеттерді орындауға кедергі келтіру не кек алу мотивін саралайды [19]. Цифрлық ортадағы жария тарату қысқа уақыт ішінде шектеусіз аудиторияға жетіп, қайта көшірілуі мүмкін болғандықтан, оның қоғамдық қауіптілігі жоғары.

ҚР ҚК-нің 147-бабының жүйесі материалдық құқық пен дәлелдеу арасындағы тікелей байланысты көрсетеді. Баптың әр бөлігі бойынша деректердің санаты, әрекеттің нысаны, заңсыздықтың негізі, салдар, субъект, кінә және саралаушы тәсіл әртүрлі. Сондықтан тергеп-тексеру барысында «дербес деректер туралы заң бұзылды» деген жалпы тұжырым жеткіліксіз, нақты құрамның барлық міндетті белгілері анықталуы тиіс.

1-кесте – ҚР ҚК-нің 147-бабы бойынша қылмыстық-құқықтық бағалау матрицасы

Бап бөлігі	Негізгі әрекет	Қорғалатын мәлімет/міндет	Міндетті немесе негізгі белгілер	Дәлелдеудің негізгі бағыты
1	Қорғау шараларын сақтамау	Дербес деректерді қорғау міндеті	Арнайы субъект, нақты міндетті бұзу, елеулі зиян, себептік байланыс, кінә	Міндеттің қайнар көзі, қауіпсіздік стандарты, бұзушылық, оқиға журналы, зиян және себептік байланыс
2	Заңсыз жинау және (немесе) өңдеу	Жеке/отбасы құпиясын құрайтын мәліметтер немесе өзге дербес деректер	Келісімнің не өзге құқықтық негіздің болмауы, заңсыз операция, залалдың бар-жоғы мен мазмұны	Дерек санаты, келісім, мақсат, өкілеттік, нақты операция, залал, себептік байланыс
3	2-бөліктегі әрекеттердің сараланған түрлері	2-бөліктегі деректер	Қызметтік жағдай, арнайы техникалық құрал, заңсыз қолжетімділік/ұстап қалу, пайда мақсаты, кедергі келтіру/кек алу	Қолжетімділік рөлі, қолданылған құрал, лог-журнал, желілік іздер, мотив және мақсат
4	Заңсыз тарату	Жеке/отбасы құпиясы немесе өзге дербес деректер	Келісімсіз не өзге құқықтық негізсіз үшінші тұлғаға беру/қолжетімді ету, залалдың бар-жоғы мен мазмұны	Адресат, тарату арнасы, көлемі, уақыты, келісім, салдар және қайта таралу
5	4-бөліктегі таратудың сараланған түрлері	4-бөліктегі деректер	Жария сөз, шығарма, БАҚ, телекоммуникация желісі, ақпараттандыру объектісі, онлайн-платформа, кедергі/кек алу мотиві	Жарияланымның қолжетімділігі, аудиториясы, URL/аккаунт, уақыт белгісі, көшірмелер, мотив

Объективтік жақты белгілеу кезінде әрекеттің фактісін ғана емес, оның тәсілін, уақытын, орнын, қолданылған ақпараттық жүйені, деректер көлемін, құқықтық негіздің жоқтығын және пайда болған салдарды анықтау қажет. Цифрлық ортада бір операцияның техникалық көрінісі бірнеше заңдық әрекетті қамтуы мүмкін. Мысалы, деректер базасына кіру – қолжетімділік,

мәліметтерді қарау – танысу, файлды жүктеу – жинау, оны басқа базаға біріктіру – өңдеу, мессенджер арқылы жіберу – тарату. Тергеу хаттамасында және сараптамалық зерттеуде осы операциялар нақты ажыратылмаса, құқықтық саралау жалпылама сипатта қалады.

Елеулі зиян қылмыстық жауаптылық шегін айқындайтын маңызды белгі болып табылады және оны тек мүліктік залалмен шектеуге болмайды. С.И. Гутник дербес деректерді олардың иесінің бақылауынсыз жинау, тарату және пайдалану адамның жеке өміріне қолсұғылмаушылық құқығына ғана емес, оның өзге де құқықтары мен заңды мүдделеріне, соның ішінде өмірі мен меншігіне қауіп төндіруі мүмкін екенін көрсетеді [14]. Е.В. Хохлова дербес деректерге қатысты заңсыз әрекеттердің қоғамдық қауіптілігін жеке өмірге қолсұғылмаушылыққа, меншікке, ар-намысқа, қадір-қасиетке, іскерлік беделге және тұлғаның өзге де құқықтық игіліктеріне зиян келтіру мүмкіндігімен байланыстырып, мұндай әрекеттердің салдары материалдық залалмен қатар моральдық зияннан да көрінуі мүмкін екенін негіздейді [15]. Осыған байланысты дербес деректерді заңсыз жинау, өңдеу немесе тарату нәтижесінде жеке өмірдің жария болуы, мүліктік шығынның туындауы, тұлғаның беделі мен қадір-қасиетіне нұқсан келуі, оның қауіпсіздігіне қатер төнуі және өзге де елеулі мүліктік немесе мүліктік емес салдар елеулі зиянды бағалау кезінде ескерілуі мүмкін. Алайда зиянның елеулілігі абстрактілі болжамға немесе деректердің таралу фактісінің өзіне ғана емес, нақты іс материалдарымен расталған салдардың сипатына, ауырлығына және жәбірленушінің құқықтары мен заңды мүдделеріне тигізген нақты әсеріне қарай анықталуы тиіс.

Себептік байланыс та дербес дәлелдеу нысанасы болып табылады. Ақпараттың заңсыз таралуы немесе зиянның туындауы зерттеліп отырған әрекетпен ғана емес, одан бұрын болған оқиғамен, басқа тұлғаның әрекетімен, ақпараттық жүйедегі техникалық ақаумен немесе деректер субъектісінің өзінің әрекеттерімен байланысты болуы мүмкін. Сондықтан тергеу барысында деректердің бастапқы көзін, оқиғалардың уақыттық ретін, әрбір қолжетімділік пен көшіру фактісін, тарату арнасын және мәліметтердің кейінгі пайдаланылуын қалпына келтіру қажет. М.С. Бисалиев цифрлық іздердің осы тұрғыдағы маңызын атап өтіп: «Дербес деректермен жасалатын кез келген операция цифрлық із қалдырады, яғни жүйелік журналда осы деректермен кімнің, қашан және қандай әрекеттер жасағаны туралы автоматты жазба қалыптасады», – деп көрсетеді [12, 131-б.]. Автордың пайымдауынша, дербес деректер қауіпсіздігі бұзылған жағдайда цифрлық іздер бұзушылықтың себептерін жедел анықтауға және жауапты тұлғаларды айқындауға мүмкіндік береді. Осыған байланысты лог-журналдарды, авторизация жазбаларын, уақыт белгілерін және өзге де цифрлық іздерді уақтылы сақтау мен алу себептік байланысты белгілеудің маңызды қылмыстық-процестік алғышарты болып табылады.

Қылмыстық құқық бұзушылықтың аяқталу сәтін дұрыс анықтау да саралау үшін маңызды. Заңсыз жинау деректер нақты алынған немесе кінәлінің бақылауына өткен кезде, өңдеу тыйым салынған операция жүзеге

асқанда, тарату мәлімет үшінші тұлғаға нақты қолжетімді болған кезде аяқталған деп бағалануы мүмкін. Ал деректерді алу немесе таратуға бағытталған, бірақ кінәліге байланысты емес себептермен соңына жеткізілмеген әрекеттерге қылмысқа оқталу туралы жалпы ережелер қолданылуы мүмкін.

ҚР ҚК-нің 147-бабы бойынша субъект құрамның нақты бөлігіне қарай жалпы немесе арнайы болуы мүмкін. 1-бөлікте дербес деректерді қорғау шараларын қабылдау міндеті жүктелген арнайы субъект талап етіледі. Бұл тұлғаның мәртебесі ұйымның ішкі құжаттарымен, лауазымдық нұсқаулығымен, ақпараттық жүйедегі рөлімен, қолжетімділік матрицасымен және қауіпсіздік саясаты арқылы дәлелденеді. 2 және 4-бөліктерде жалпы субъект болуы мүмкін, ал 3 және 5-бөліктердегі қызметтік жағдайды пайдалану белгісі субъектінің арнайы мүмкіндігін саралаушы мән-жайға айналдырады.

Субъективтік жақты анықтауда кінәлінің деректердің сипаты, оларды алудың немесе таратудың заңсыздығы және өзінің әрекетінің салдары туралы психикалық қатынасы зерттеледі. Арнайы мақсат немесе мотив 3 және 5-бөліктерде тікелей саралаушы белгі ретінде көрінеді. Пайда немесе артықшылық алу, тұлғаның қызметтік, кәсіби немесе қоғамдық міндеттерін орындауына кедергі келтіру, не сол міндеттерді орындағаны үшін кек алу ниеті электрондық хат-хабарлар, төлемдер, келіссөздер, іздеу тарихы, жарияланым контексті және өзге дәлелдемелер арқылы анықталуы мүмкін [19].

Қорғау шараларын сақтамау құрамында кінә нысанын формалды түрде тек лауазымға немесе техникалық оқиғаға сүйеніп белгілеуге болмайды. Тергеу тұлғаның міндет туралы хабардар болғанын, қауіптің алдын алу мүмкіндігін, нақты бұзушылықты, салдардың болжамдылығын және оған психикалық қатынасын анықтауы керек. Мұндай тәсіл объективті айып тағуға және ақпараттық жүйедегі кез келген ақауды қылмыстық құқық бұзушылық ретінде бағалауға жол бермейді.

Дербес деректер саласындағы заңнама талаптарының кез келген бұзылуы қылмыстық құқық бұзушылық құрамын автоматты түрде қалыптастырмайды. Қылмыстық жауаптылық тек қылмыстық заңда көзделген құрамның барлық міндетті белгілері анықталған жағдайда туындайды. ҚР ӘҚБтК-нің 79-бабы дербес деректерді заңсыз жинау және (немесе) өңдеу, қорғау шараларын сақтамау және осы саладағы өзге де бұзушылықтар үшін, егер әрекетте қылмыстық жазаланатын іс-әрекет белгілері болмаса, әкімшілік жауаптылық көздейді [20]. Демек, әкімшілік және қылмыстық жауаптылықтың шекарасы қылмыстық заңдағы міндетті белгілердің жиынтығы арқылы анықталады.

Ажыратудың негізгі өлшемдеріне деректер санаты, әрекеттің нақты нысаны, елеулі зиян, арнайы техникалық құралды немесе заңсыз қолжетімділікті пайдалану, қызметтік жағдай, пайда немесе артықшылық алу мақсаты, жария немесе желілік тарату, жәбірленушінің қызметтік, кәсіби немесе қоғамдық міндеттерімен байланыс, кінәнің мазмұны және

әрекеттердің жүйелілігі жатады. Бір ғана деректер көлемі, жәбірленушілер саны немесе ақпараттың цифрлық нысаны қылмыстық жауаптылықты автоматты түрде туындатпайды. Осыған байланысты әкімшілік және қылмыстық жауаптылықты ажырату әрекеттің сыртқы нысанына ғана емес, нақты қылмыстық құрам үшін заңда көзделген міндетті және саралаушы белгілердің бар-жоғына, олардың мазмұнына және дәлелдену дәрежесіне негізделуі тиіс.

Қылмыстық-құқықтық ықпал ету шараларын үнемді пайдалану қағидаты құқық бұзушылықтың әрбір фактісін автоматты түрде қылмыстық жолмен қудалауды талап етпейді. Тұлғаның жеке өміріне және дербес деректерін қорғау құқығына қоғамдық қауіп төндіретін қолсұғушылық анықталып, қылмыстық құрамның барлық белгілері толық дәлелденген жағдайда ғана қылмыстық жауаптылық орын алуы тиіс. Дәлелдеу жеткіліксіз немесе даулы болған сәттерде қылмыстық заң нормасын ұқсастығы бойынша кеңейтіп түсіндіруге болмайды: саралау заңдылық қағидатына және айыпталушының кінәсіздік презумпциясына сәйкес жүргізілуі тиіс.

2-кесте – Қылмыстық және әкімшілік жауаптылықты ажыратудың негізгі өлшемдері

№	Өлшем	Әкімшілік-құқықтық бағалауға тән белгі	Қылмыстық-құқықтық бағалауға тән белгі
1	Құрам белгілері	ҚР ҚК-нің 147-бабында көзделген барлық міндетті белгілер жоқ	ҚР ҚК-нің 147-бабының нақты бөлігіндегі барлық міндетті белгілер бар
2	Салдар	Елеулі зиян дәлелденбеген және ол құрам үшін міндетті	Елеулі зиян құрамның міндетті белгісі ретінде нақты дәлелденген
3	Тәсіл	Қарапайым тәртіп бұзушылық, саралаушы тәсіл жоқ	Заңсыз қолжетімділік, ұстап қалу, арнайы техникалық құрал, жария/желілік тарату және т.б.
4	Субъект	Жалпы немесе әкімшілік міндет жүктелген тұлға	Қылмыстық құрам талап ететін жалпы/арнайы субъект және оның өкілеттігі дәлелденген
5	Мақсат/мотив	Арнайы қылмыстық мақсат дәлелденбеген	Пайда/артықшылық, кедергі келтіру немесе кек алу сияқты арнайы белгі бар
6	Қоғамдық қауіптілік	Бұзушылықтың салдары мен тәсілі қылмыстық деңгейге жетпейді	Жеке өмір мен деректерді қорғау құқығына елеулі және нақты қоғамдық қауіпті қолсұғу бар

Дербес деректерді заңсыз жинау, өңдеу және тарату көбіне өзге қылмыстық құқық бұзушылықтармен ұштасады. Деректер ақпараттық жүйеге заңсыз қол жеткізу, телекоммуникациялық хабарды ұстап қалу немесе құрылғыға жасырын бағдарлама орнату арқылы алынуы мүмкін; кейін алаяқтық, қорқытып алушылық, жалған құжат жасау, банктік операция жүргізу немесе қызметтік өкілеттікті теріс пайдалану үшін қолданылуы ықтимал. Мұндай жағдайларда дербес деректер қылмыстық қолсұғушылықтың нысанасы ғана емес, өзге қылмыстың құралы немесе қылмыстық нәтижеге жетудің тәсілі ретінде көрінеді [7, 5 б.].

Сабақтас құрамдарды ажыратудың негізгі сұрағы – ҚР ҚК-нің 147-бабы өзге құрамның барлық белгілерін толық қамти ма, әлде дербес объектіге, әрекетке және салдарға қолсұғу орын алды ма. Егер ақпараттық жүйеге заңсыз кіру деректерді жинаудың тәсілі болып қана қоймай, ақпараттандыру объектісінің қауіпсіздігіне дербес зиян келтірсе, қылмыстық құқық бұзушылықтар жиынтығы туралы мәселе қойылады. Сол сияқты заңсыз алынған деректерді пайдаланып мүлікті иемдену, қорқытып алу немесе жалған құжат рәсімдеу дербес меншікке немесе басқару тәртібіне қарсы құрамды туындатуы мүмкін.

Құрамдар бәсекелестігі кезінде арнайы норма жалпы норманы ығыстыратыны, ал дербес объектілер мен салдарлар болған жағдайда жиынтық қолданылатыны ескерілуі тиіс. Бұл бағалау үшін тергеу әрекеттердің уақыттық ретін, әр әрекеттің мақсаттарын, деректердің қозғалысын және әрбір құқықтық игілікке келтірілген зиянды анықтауы тиіс. Сондықтан саралау бір ғана файлдың немесе жарияланымның мазмұнына емес, оқиғаның толық цифрлық және құқықтық реконструкциясына негізделуі қажет.

Қылмыстық жауаптылықтың шектері мен саралау өлшемдерінің практикалық маңызын 2021–2025 жылдардағы ресми сот статистикасы көрсетеді. Зерттелген кезеңде ҚР ҚК-нің 147-бабы бойынша 53 адам сотталған, оның 41-і немесе 77,4%-ы 5-бөлік бойынша сотталған [21; 22]. 2-бөлік бойынша 31 іс тоқтатылып, 34 адам ақталған және 3 адам сотталған; 5-бөлік бойынша 1 іс тоқтатылып, 2 адам ақталған және 41 адам сотталған. Бұл көрсеткіштер әртүрлі есептік бірліктерді – істер мен адамдарды – сипаттайтындықтан, олар бір жиынтыққа механикалық түрде біріктірілмейді.

2 және 5-бөліктер бойынша сот нәтижелерінің елеулі айырмашылығы қылмыстық-құқықтық саралау мен дәлелдеудің күрделілігі туралы ғылыми мәселе қоюға мүмкіндік береді, бірақ себептік қорытынды жасауға жеткіліксіз. 2-бөлік бойынша заңсыздықтың негізін, келісімнің шегін, өңдеудің мақсатын, елеулі зиянды және себептік байланысты дәлелдеу қажеттілігі істің нәтижесіне ықпал етуі мүмкін деген болжам туындайды. Ал 5-бөліктегі жария немесе желілік тарату фактісі көбіне жарияланым, URL, аккаунт, уақыт белгісі, жүктеу және көру деректері түріндегі тұрақты цифрлық іздермен расталуы ықтимал.

Сотталғандардың әлеуметтік-демографиялық құрылымы да қылмыстық құқық бұзушылықтардың әлеуметтік профилін сипаттайды: орташа жас – 34,2 жас, 62,3%-ының білімі орта, 66,0%-ы жұмыс істемейтін және оқымайтын адамдар [22]. Дегенмен бұл сипаттамалар кінәні немесе криминогендік себептерді тікелей түсіндірмейді; олар тек профилактикалық және криминологиялық талдауға арналған қосымша эмпирикалық көрсеткіштер ретінде пайдаланылуы тиіс.

Қылмыстық құқық бұзушылықты дұрыс саралау мен оны дәлелдеудің арасында тікелей байланыс бар. ҚР ҚПК-нің 113-бабы қылмыстық құқық бұзушылық оқиғасын, оны жасаған адамды, кінә нысанын, себептері мен мақсаттарын, жауаптылық дәрежесі мен сипатына әсер ететін мән-жайларды,

келтірілген зиянның сипаты мен мөлшерін және өзге де заңдық маңызы бар жағдайларды анықтауды талап етеді [6]. Дербес деректерге қатысты істерде бұл жалпы дәлелдеу пәні арнайы мазмұнмен толығады. Заңсыз жинау бойынша деректердің нақты қайдан, кімнің қолжетімділігі арқылы, қандай техникалық тәсілмен, қандай құқықтық негізсіз және қандай көлемде алынғаны дәлелденуі тиіс. Заңсыз өңдеу бойынша бастапқы мақсат, кейінгі операция, өңдеу мерзімі, пайдаланылған алгоритм немесе жүйе, өкілеттік шегі және деректердің қайда берілгені анықталады. Заңсыз тарату бойынша адресат, тарату арнасы, уақыт, аудитория, қолжетімділік дәрежесі, мәліметтің өзгермегендігі және кейінгі қайта таралуы тексеріледі.

Материалдық белгі мен оны растайтын цифрлық із арасында бірмәнді автоматты байланыс жоқ. IP-мекенжай тұлғаның әрекетін өздігінен дәлелдемейді, аккаунт жазбасы оның нақты пайдаланушысын автоматты түрде анықтамайды, файлдың құрылғыда болуы оны сол тұлға жасағанын білдірмейді. Сондықтан цифрлық іздер атрибуция, тұтастық, контекст және басқа дәлелдемелермен сәйкестік тұрғысынан тексерілуі керек. Бұл жерде маманның тергеу әрекетіне техникалық жәрдемі мен сарапшының арнайы зерттеуі маңызды, бірақ олардың функциялары кейінгі бөлімдерде дербес қарастырылады. Осы санаттағы істер бойынша дәлелдеу пәнін «қылмыстық-құқықтық белгі → дәлелденетін мән-жай → ықтимал цифрлық із немесе құжат → дерек ұстаушы → процестік әрекет → құқықтарды қорғау кепілдігі» формуласы бойынша құру ұсынылады. Бұл формула қылмыстық құқықтағы әрбір белгіні нақты тергеу міндетіне айналдырады және дәлелдеу қажеттілігіне қатысы жоқ артық дербес деректерді алуға жол бермейді.

3-кесте – Қылмыстық-құқықтық белгі мен дәлелдеу міндетінің байланысы

№	Қылмыстық-құқықтық белгі	Дәлелдеуге жататын мән-жай	Ықтимал дереккөз/цифрлық із	Негізгі процестік бағыт
1	Деректердің санаты	Тұлғаны сәйкестендіру мүмкіндігі; жеке/отбасы құпиясына қатыстылығы	Деректер базасының құрылымы, құжат, профиль, медициналық/банктік жазба	Құжаттарды алу, қарап-тексеру, маман түсіндірмесі
2	Құқықтық негіздің болмауы	Келісімнің, заңдық өкілеттіктің немесе өзге негіздің жоқтығы/шегінен шығу	Келісім нысаны, шарт, ішкі регламент, қолжетімділік матрицасы	Сұрату, құжаттарды алу, жауап алу, құқықтық аудит
3	Нақты операция	Жинау, өңдеу немесе тарату фактісі мен уақыты	Лог-журнал, жүктеу тарихы, метадеректер, транзакциялық жазба	Қарап-тексеру, криминалистикалық көшірме, сараптама
4	Саралаушы тәсіл	Қызметтік жағдай, арнайы құрал, заңсыз қолжетімділік, жария желі	Рөлдік қолжетімділік, бағдарламалық құрал, желілік журнал, URL	Тінту/алу, ЖТӘ, провайдерден мәлімет алу, маман қатыстыру

№	Қылмыстық-құқықтық белгі	Дәлелдеуге жататын мән-жай	Ықтимал дереккөз/цифрлық із	Негізгі процестік бағыт
5	Елеулі зиян және себептік байланыс	Зиянның нақты сипаты, мөлшері және әрекетпен байланысы	Қаржылық құжат, медициналық мәлімет, жарияланым аудиториясы, жәбірленуші жауабы	Жауап алу, сараптама, құжаттық және цифрлық дәлелдемелерді салыстыру
6	Кінә, мақсат және мотив	Заңсыздықты ұғыну, ниет, пайда/кек алу мақсаты	Хат-хабар, төлем, іздеу тарихы, келіссөз, әрекеттер реттілігі	Жауап алу, цифрлық материалдарды зерттеу, дәлелдемелер жиынтығын бағалау

Дербес деректерді заңсыз жинау, өңдеу және таратуға байланысты әрекеттерді бірізді бағалау үшін мынадай кезеңдік алгоритм ұсынылады:

1) зерттелетін мәліметтің белгілі бір тұлғаны тікелей немесе жанама айқындайтынын және оның дербес дерек болып табылатынын анықтау;

2) деректердің жеке немесе отбасы құпиясына жататынын не өзге дербес деректер санатына кіретінін белгілеу;

3) деректерді жинау, өңдеу немесе тарату үшін келісімнің, заңдық өкілеттіктің немесе өзге құқықтық негіздің болған-болмағанын тексеру;

4) жасалған нақты операцияны, оның уақытын, көлемін, тәсілін және пайдаланылған ақпараттық жүйені анықтау;

5) әрекет субъектісін, оның қолжетімділік өкілеттігін және арнайы міндеттерін белгілеу;

6) елеулі зиянды, оның мазмұнын және әрекетпен себептік байланысын анықтау;

7) қызметтік жағдай, арнайы техникалық құрал, заңсыз қолжетімділік, пайда мақсаты, жария немесе желілік тарату және өзге саралаушы белгілерді тексеру;

8) әкімшілік құқық бұзушылықпен және сабақтас қылмыстық құрамдармен арақатынасын шешу;

9) әрбір материалдық белгіге сәйкес дәлелдеу мән-жайын, цифрлық ізді, дерек ұстаушыны және процестік әрекетті айқындау.

Ұсынылған алгоритм құқық қолданушыны қылмыстық заңдағы бір ғана терминге немесе деректердің көлеміне сүйенетін формалды бағалаудан сақтайды. Оның ерекшелігі – қылмыстық-құқықтық саралауды бір мезгілде дербес деректерді қорғау қағидаттарымен, цифрлық іздердің табиғатымен және қылмыстық-процестік дәлелдеу талаптарымен байланыстыруында.

Жүргізілген талдау дербес деректерді заңсыз жинау, өңдеу және таратуға байланысты қылмыстық жауаптылықтың шектері бір ғана Қылмыстық кодекстің мәтінімен анықталмайтынын көрсетті. ҚР ҚК-нің 147-бабындағы «заңсыздық» белгісі дербес деректер туралы салалық заңнамада бекітілген келісім, мақсатпен шектеу, деректерді барынша азайту, өкілеттік, сақтау мерзімі, қауіпсіздік және тарату шарттары арқылы ашылады. Сондықтан бап бланкеттік нормалар мен қылмыстық-құқықтық белгілердің өзара байланысында қолданылуы тиіс.

Қылмыстық-құқықтық қорғаудың негізгі объектісі – адамның жеке өміріне қолсұғылмаушылығы, дербес деректерін бақылауы және оларды заңсыз ақпараттық әрекеттерден қорғау құқығы. Қылмыстық қолсұғушылықтың нысанасы ақпараттың қағаз немесе цифрлық нысанымен емес, тұлғаны айқындау қабілетімен және қорғалатын құқықтық салаға қатыстылығымен анықталады. Жинау, өңдеу және тарату қылмыстық құқықта мазмұны мен аяқталу сәті бойынша ажыратылатын дербес әрекеттер болып табылады.

ҚР ҚК-нің 147-бабы бойынша саралау деректердің санатын, құқықтық режимін, нақты операцияны, заңсыздық негізін, елеулі зиянды, себептік байланысты, субъектіні, кінә нысанын, мақсат-мотивті және саралаушы тәсілді жеке-жеке тексеруді талап етеді. Әкімшілік және қылмыстық жауаптылықтың шекарасы деректер көлемімен немесе оқиға фактісімен емес, қылмыстық құрамның барлық міндетті белгілерінің дәлелденуімен анықталады.

Қылмыстық-құқықтық саралаудың әрбір белгісі сотқа дейінгі тергеп-тексеру барысында нақты дәлелдеу міндетіне айналуы тиіс. Бұл міндет тиісті мән-жайларды анықтауды, оларды растайтын цифрлық мәліметтер мен өзге дереккөздерді белгілеуді, қажетті ақпаратты иеленуші субъектіні анықтауды және заңда көзделген процестік құралдарды дұрыс таңдауды қамтиды. Осындай өзара байланыс қылмыстық-құқықтық бағалаудың негізділігін қамтамасыз етіп қана қоймай, дәлелдемелерді жинаудың мақсаттылығы мен жеке өмірге араласудың қажеттілік және мөлшерлестік талаптарына сәйкестігін де қамтамасыз етеді.

1.2 Дербес деректер саласындағы ұлттық құқықтық база және мемлекеттік саясат: киберқауіпсіздік пен мемлекеттік бақылау мәселелері

Дербес деректерді қорғаудың ұлттық құқықтық базасы қазіргі кезеңде ақпараттық қоғамның, цифрлық мемлекеттің және қылмыстық сот ісін жүргізудің өзара тоғысында қалыптасып отыр. Сондықтан дербес деректер саласындағы құқықтық режимді тек салалық ақпараттық заңнама аясында ғана емес, конституциялық құқық, әкімшілік құқық, қылмыстық құқық, қылмыстық-процестік құқық, киберқауіпсіздік және халықаралық стандарттармен байланыста талдау қажет.

Қазақстан Республикасында дербес деректерді қорғаудың бастапқы құқықтық негізі конституциялық кепілдіктерден туындайды. 2026 жылғы 15 наурыздағы республикалық референдум нәтижесінде қабылданып, 2026 жылғы 1 шілдеден бастап күшіне енген қолданыстағы Конституция адамның жеке өміріне қол сұғылмаушылық, өзінің және отбасының құпиясын сақтау, ар-намысы мен қадір-қасиетін қорғау құқықтарын бекітеді, сондай-ақ цифрлық технологияларды қолдануды қоса алғанда, дербес деректерді заңсыз жинаудан, өңдеуден, сақтаудан және пайдаланудан қорғау құқығына заңмен кепілдік беретінін тікелей көрсетеді

[1]. Сонымен қатар ақпаратты заңмен тыйым салынбаған тәсілмен алу және тарату құқығы да конституциялық деңгейде танылған. Осы екі кепілдік дербес деректер саласындағы ұлттық құқықтық саясаттың өзегін құрайды: бір жағынан, ақпаратқа қол жеткізу және цифрлық қызметтерді дамыту қажет болса, екінші жағынан, жеке тұлғаның деректері заңсыз жиналмауы, өңделмеуі және таратылмауы тиіс. Дербес деректерді қорғау институтының дәл осы конституциялық реформа аясында айрықша бекітілуі – оның салалық реттеуден конституциялық кепілдік деңгейіне көтерілу үрдісін көрсетеді және диссертациялық зерттеудің құқықтық негізін нығайтады.

Арнайы құқықтық реттеу жүйесінде орталық орынды «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңы алады [2]. Бұл заң дербес деректер саласындағы қоғамдық қатынастарды реттейді, дербес деректерді жинау, өңдеу және қорғау қызметінің мақсаттарын, қағидаттарын, құқықтық негіздерін, меншік иесі мен оператордың міндеттерін, дербес деректер субъектісінің құқықтарын және мемлекеттік бақылау тетіктерін белгілейді. Қылмыстық процесс үшін аталған заңның маңызы дербес деректерді дәлелдемелік мақсатта алудың құқықтық шегін айқындауында. Тергеу органы қылмыстық іс үшін маңызы бар мәліметтерді жинаған кезде бұл деректердің жеке тұлғаға қатысты құқықтық режимін ескеруі тиіс.

Аталған заңда дербес деректерді жинау мен өңдеу белгілі бір мақсатқа сәйкес, заңды негізде және қажетті көлемде жүргізілуі тиіс екені көзделеді [2]. Бұл қағидаттар қылмыстық-процестік қызметпен тікелей байланысты. Қылмыстық істі тергеп-тексеру барысында тергеуші немесе анықтаушы дербес деректерді дәлелдеу пәнімен байланысы болғанда ғана алуы керек. Қылмыстық іс үшін қажет емес мәліметтерді жинау, деректер көлемін шектемеу немесе оларды іске артық тіркеу дербес деректерді қорғау қағидаттарына ғана емес, дәлелдемелердің жол берілетіндігіне де күмән тудыруы мүмкін.

Дербес деректерді қорғау туралы заңнаманың қылмыстық процесс үшін маңызды тағы бір элементі – дербес деректерді жалпыға бірдей қолжетімді және қолжетімділігі шектеулі деректерге бөлу. Бұл жіктеу тергеу органдары үшін формалды ақпараттық белгі ғана емес, дәлелдемелік айналымдағы құқықтық режимді анықтайтын өлшем болуы тиіс. Ашық дереккөзден алынған мәліметтің өзі қылмыстық іс бойынша автоматты түрде жол берілетін дәлелдемеге айналмайды – оның дереккөзі, алыну уақыты, өзгертілмегендігі және дәлелдеу пәнімен байланысы тексерілуі тиіс. Ал қолжетімділігі шектеулі деректерді алу кезінде заңды негіз, санкция, қажеттілік, мөлшерлестік және деректер көлемін шектеу талаптары сақталуы қажет.

Дербес деректерді жинау және өңдеу қағидалары Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 21 қазандағы № 395/НҚ бұйрығымен бекітілген [25]. Бұл қағидалар меншік иесі мен оператордың дербес деректерді жинау және өңдеу кезінде қажет әрі жеткілікті көлем қағидатын сақтауы тиіс

екенін нақтылайды. Қылмыстық процесс үшін мұның маңызы зор: дерек ұстаушыдан сұратылатын ақпарат нақты іс бойынша дәлелдеу пәнімен шектелуі тиіс. Құқық қорғау органының сұратуы неғұрлым нақты болса, алынған деректердің жол берілетіндігі мен құпиялылықтың сақталуы соғұрлым сенімді болады. Меншік иесінің, оператордың және үшінші тұлғаның дербес деректерді қорғау жөніндегі шараларды жүзеге асыру қағидалары да бұл талаптарды нақтылайды: дербес деректердің сақталуын, оларға рұқсатсыз қол жеткізуді болдырмауды, өңдеу процесіндегі қауіпсіздік шараларын және жауапты субъектілердің міндеттерін айқындайды [26]. Қылмыстық процесс контексінде бұл талаптар дерек ұстаушылардың құқық қорғау органдарына ұсынатын электрондық материалдарының түпнұсқалығы, тұтастығы, қауіпсіз арна арқылы берілуі және кейінгі тексерілуі үшін маңызды.

Дербес деректер саласындағы ұлттық құқықтық база ақпараттандыру туралы заңнамамен де тығыз байланысты. «Ақпараттандыру туралы» Қазақстан Республикасының Заңы ақпараттық жүйелерді, электрондық ақпараттық ресурстарды, ақпараттық-коммуникациялық инфрақұрылымды және ақпараттық қауіпсіздікті қамтамасыз етуге байланысты қатынастарды реттейді [27]. Қылмыстық процесте дербес деректер көбіне мемлекеттік ақпараттық жүйелерде, ведомстволық деректер базаларында, электрондық үкімет инфрақұрылымында, байланыс операторларының жүйелерінде немесе жеке цифрлық платформаларда сақталады, сондықтан деректерді алу мен қорғау тәртібі ақпараттандыру объектілерінің құқықтық режимімен тікелей ұштасады.

Ақпаратқа қол жеткізу туралы заңнама да дербес деректерді қорғау режимімен тығыз байланысты. «Ақпаратқа қол жеткізу туралы» Заң азаматтардың ақпаратқа қол жеткізу құқығын жүзеге асырудың жалпы тәртібін белгілей отырып, заңмен қорғалатын құпияны және дербес деректерді қорғау қажеттігін де ескереді [28]. Қылмыстық процесте бұл тепе-теңдік ерекше көрінеді: сот актілерінің жариялылығы, мемлекеттік органдар қызметінің ашықтығы, электрондық сот жүйелері және қылмыстық іс материалдарына қолжетімділік бір жағынан жариялылық қағидатын іске асырса, екінші жағынан жәбірленушілердің, куәлардың және үшінші тұлғалардың дербес деректерінің қайталама таралу қаупін туындатады.

Д.А. Дигай ақпаратқа қол жеткізу құқығы мен оны шектеудің арақатынасын зерттей отырып: «Ақпаратқа қол жеткізу құқығы мемлекеттік құпияны, дербес деректерді және заңмен қорғалатын өзге де мәліметтерді қорғау қажеттілігімен теңгерілуі тиіс», – деп көрсетеді [18, 66 б.]. Автордың пікірінше, ақпаратқа қол жеткізуді қамтамасыз ету кезінде өзге тұлғалардың құқықтары мен заңды мүдделерін қорғау талаптары сақталуы тиіс, өйткені мұндай тәсіл үшінші тұлғаларға зиян келтірудің алдын алып, ақпараттық қатынастардағы мүдделер теңгерімін қамтамасыз етеді [18, 45 б.]. Бұл ұстаным қылмыстық процесте ерекше мәнге ие. Сот төрелігінің жариялылығы, қылмыстық іс материалдарына процеске қатысушылардың

қолжетімділігі, сот актілерін жариялау және цифрлық сот сервистерін пайдалану ақпараттық ашықтықты қамтамасыз еткенімен, жәбірленушілердің, куәлардың және іске қатысы бар өзге тұлғалардың дербес деректерінің қайталама таралу тәуекелін де туындатады. Сондықтан қылмыстық іс жүргізудегі жариялылық пен ақпаратқа қолжетімділік абсолютті сипатта қарастырылмай, жеке өмірге қолсұғылмаушылықты, дербес деректердің құпиялылығын және үшінші тұлғалардың құқықтары мен заңды мүдделерін қорғау талаптарымен үйлестірілуі тиіс.

Электрондық құжат және электрондық цифрлық қолтаңба туралы 2003 жылғы заң дербес деректердің электрондық нысандағы айналымын түсіндіруде маңызды рөл атқарған болатын, алайда бұл заң 2026 жылғы Цифрлық кодекстің қабылдануымен 2026 жылғы 12 шілдеден бастап өз күшін жойды, сондықтан оның нормалары қазір Цифрлық кодекс шеңберінде қаралады [29; 4]. Электрондық құжат, электрондық цифрлық қолтаңба, куәландырушы орталық және электрондық өзара іс-қимыл тетіктері қылмыстық процестегі цифрлық ортадағы дәлелдемелерді түсіндірумен тығыз байланысты. Дербес деректерді заңсыз таратумен, жинаумен және өідеумен байланысты істерде ЭЦҚ-ны заңсыз пайдалану, бір реттік парольдерді үшінші тұлғаларға беру, аккаунтқа заңсыз кіру немесе электрондық қызметтер арқылы жалған операция жасау сияқты фактілер жиі кездеседі; мұндай жағдайларда электрондық құжаттың түпнұсқалығы мен ЭЦҚ қолдану іздері дәлелдемелік маңызға ие болады.

2026 жылғы Цифрлық кодекстің қабылдануы Қазақстанда цифрлық қатынастарды жүйелі кодификациялаудың жаңа кезеңін көрсетеді [4]. Кодекс цифрлық кеңістіктегі қоғамдық қатынастарды кешенді реттеуге, цифрлық инфрақұрылымның өзара үйлесімділігін қамтамасыз етуге, деректерді басқару мен цифрлық қызметтердің құқықтық негізін орнықтыруға бағытталған. Қылмыстық процесс үшін Цифрлық кодекстің маңызы дербес деректерді, цифрлық жазбаларды, ақпараттық жүйелерді және электрондық өзара іс-қимыл тетіктерін біртұтас құқықтық ортада қарастыруға мүмкіндік беруінде. Бұл нормалардың толық қолданысқа енуі тергеу органдарының электрондық ақпаратпен жұмыс істеу стандарттарын қайта қарау қажеттігін туындатады. Цифрлық кодекстің қабылдануы дербес деректерді қорғау мен киберқауіпсіздікті оқшау салалар ретінде емес, біртұтас цифрлық экожүйенің құрамдас бөліктері ретінде қарастыруға мүмкіндік береді. Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық істер көбіне ақпараттық жүйелердің қорғалмауы, әлсіз аутентификация, ішкі қолжетімділік тәртібінің бұзылуы, қызметкерлердің құқықтарын шектемеу, лог-журналдардың болмауы немесе деректердің артық жиналуы сияқты факторлармен байланысты, сондықтан дербес деректерді қорғау мемлекеттік саясатында құқықтық, ұйымдастырушылық және техникалық шаралар өзара үйлесуі тиіс.

Мемлекеттік саясаттың маңызды бағыты ретінде киберқауіпсіздік тұжырымдамасы ерекше орын алады. Қазақстан Республикасының Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны»)

цифрлық инфрақұрылымды қорғауға, ақпараттық қауіпсіздікті күшейтуге, мемлекеттік және жеке сектордағы ақпараттық жүйелердің орнықтылығын арттыруға бағытталған [30]. Дербес деректердің қауіпсіздігі осы тұжырымдаманың табиғи құрамдас бөлігі, өйткені азаматтар туралы мәліметтердің заңсыз таралуы ақпараттық қауіпсіздік инциденті ғана емес, жеке өмірге қол сұғылмаушылыққа тікелей қауіп болып табылады. Кибершабуыл, фишинг, зиянды бағдарлама, бот арқылы деректер жинау, SIM-swap, аккаунтты иелену, деректер базасын заңсыз көшіру немесе қызметкердің ішкі жүйеден ақпарат таратуы сияқты әрекеттер бір мезгілде киберқауіпсіздік инциденті, дербес деректердің бұзылуы және қылмыстық құқық бұзушылықтың белгісі болуы мүмкін. Мұндай істерде тергеу органдары тек қылмыстық-құқықтық саралау мәселесін ғана емес, ақпараттық қауіпсіздік стандарттарын, оператордың міндеттерін және деректер субъектісінің құқықтарын да ескеруі тиіс. «Қазақстан Республикасының ұлттық қауіпсіздігі туралы» Заң ақпараттық қауіпсіздікті ұлттық қауіпсіздік элементтерінің бірі ретінде қарастырады [31]: ақпараттық жүйелердегі дербес деректердің жаппай таралуы азаматтардың құқықтарына ғана емес, мемлекеттік басқару тұрақтылығына, қаржы жүйесіне, денсаулық сақтау, білім беру және құқық қорғау салаларына да әсер етуі мүмкін. Осы тұрғыдан дербес деректерді қорғау жеке құқықты қорғаумен шектелмей, қоғамдық және мемлекеттік қауіпсіздіктің де құрамдас бөлігіне айналады.

Байланыс туралы заңнама дербес деректердің қылмыстық процестегі айналымы үшін тағы бір маңызды құқықтық қабат құрайды. «Байланыс туралы» Қазақстан Республикасының Заңы байланыс қызметтерін көрсетуге, байланыс операторларының міндеттеріне және байланыс желілерін пайдалану тәртібіне қатысты қатынастарды реттейді [32]. Қылмыстық істерде телефон нөмірі, SIM-карта, IMEI, абоненттік деректер, байланыс сеанстары, IP-мекенжайлар және трафик туралы мәліметтер жиі дәлелдемелік мәнге ие болады, алайда мұндай деректер байланыс құпиясымен байланысты болғандықтан, оларды алу арнайы процестік негізді және құқықтарды шектеудің мөлшерлестік өлшемін талап етеді.

Денсаулық сақтау саласындағы дербес деректер де күшейтілген құқықтық қорғауды қажет етеді. Халық денсаулығы және денсаулық сақтау жүйесі туралы кодекс медициналық ақпарат пен пациентке қатысты мәліметтердің ерекше құпиялылық сипатын бекітеді [33]. Цифрлық денсаулық сақтау субъектілерінің дербес медициналық деректерді жинау, өңдеу, сақтау, қорғау және беру қағидалары бұл деректердің электрондық медициналық жазбаларда, ақпараттық жүйелерде және цифрлық денсаулық сақтау инфрақұрылымында айналымға түсетінін көрсетеді [34]. Қылмыстық процесте медициналық деректерді алу кезінде жәбірленушінің, күдіктінің немесе куәнің жеке өміріне араласу тәуекелі жоғары болғандықтан, мұндай деректерді сұрату ерекше негізділікті талап етеді. Мемлекеттік құпиялар туралы заңнама, банк құпиясы, коммерциялық құпия және қызметтік ақпарат режимдері де дербес деректерді қорғау жүйесімен қиылысады [35].

Қылмыстық іс материалдарында кейде тұлғаның дербес деректері басқа қорғалатын құпия түрлерімен бірге кездеседі: банк шоттары туралы мәліметтер бір мезгілде банк құпиясы және дербес дерек болып табылады, медициналық диагноз – медициналық құпия және дербес дерек, байланыс сеанстары – байланыс құпиясы және дербес дерек ретінде бағалануы мүмкін. Сондықтан тергеу органы алынатын мәліметтің бір ғана құқықтық режимін емес, бірнеше құқықтық режимнің қабаттасуын ескеруі тиіс.

Дербес деректер саласындағы мемлекеттік бақылау институты Қазақстанда салыстырмалы түрде жаңа бағыт болып табылады. А.М. Амиров Қазақстандағы дербес деректерді қорғау және осы саладағы прокурорлық қадағалау институттарының қалыптасу кезеңін арнайы талдай отырып: «Қазақстан Республикасында дербес деректерді қорғау және дербес деректерді қорғау саласындағы прокурорлық қадағалау институттарын салыстырмалы түрде жас институттар деп атауға болады. Дербес деректерді қорғау саласындағы прокурорлық қадағалау дербес бағыт ретінде 2013 жылы қалыптасты», – деп көрсетеді [16, Б. 42–43]. Автордың талдауынша, 2020 жылға дейін прокуратура дербес деректерді қорғау саласында бақылау-қадағалау өкілеттіктерін жүзеге асыратын негізгі мемлекеттік орган болып келсе, 2020 жылдан бастап дербес деректерді қорғау жөніндегі уәкілетті органның қалыптасуы бұл саладағы мемлекеттік бақылаудың институционалдық құрылымын өзгертті [16, 43 б.].

Қазіргі құқықтық модельде дербес деректер субъектісі өзінің құқықтары бұзылған жағдайда уәкілетті органға жүгінуге құқылы, ал уәкілетті орган дербес деректер және оларды қорғау туралы заңнаманың сақталуына мемлекеттік бақылауды жүзеге асырады [2]. Бұл ретте мемлекеттік бақылаудың тиімділігі тек уәкілетті органға өкілеттіктер берумен шектелмей, оның институционалдық дербестігіне, кәсіби мамандануына және құқық қолдану құралдарының жеткіліктілігіне де байланысты. С.Б. Ахметова Еуропа мен Қазақстандағы дербес деректерді қорғау органдарының өкілеттіктерін салыстырмалы талдай отырып, Қазақстандағы уәкілетті органның көпсалалы министрлік құрылымындағы жағдайы оның дербес әрі ықпалды қызметіне кедергі келтіруі мүмкін екенін көрсетеді. Автор уәкілетті органды дербес мемлекеттік орган ретінде қалыптастыруды, оның өкілеттіктерін нақтылауды, консультациялық және түсіндіру функцияларын кеңейтуді, сондай-ақ дербес деректерді қорғау саласында арнайы біліктілігі бар мамандармен қамтамасыз етуді ұсынады [17, 55 б.].

Аталған ғылыми ұстанымдар қылмыстық процесс үшін де маңызды. Дербес деректерді заңсыз жинау, өңдеу немесе тарату белгілері анықталған жағдайда уәкілетті органның бақылау материалдары қылмыстық қудалау органдары үшін құқық бұзушылық туралы бастапқы ақпараттың және іс үшін маңызы бар мәліметтердің дереккөзі болуы мүмкін. Сонымен қатар прокуратураның жоғары қадағалау функциясы мен уәкілетті органның мемлекеттік бақылау өкілеттіктері бірін-бірі алмастырмайды. Сондықтан дербес деректерге қатысты қылмыстық құқық бұзушылықтарды анықтау

және тергеп-тексеру кезінде уәкілетті орган, прокуратура және сотқа дейінгі тергеп-тексеру органы арасындағы өзара іс-қимылдың құқықтық шектері мен ақпарат алмасу тәртібін нақты айқындау қажет.

Прокурорлық қадағалау дербес деректерді қорғаудың ұлттық жүйесінде ерекше орын алады. «Прокуратура туралы» Қазақстан Республикасының Конституциялық заңына сәйкес прокуратура мемлекет атынан заңдылықтың сақталуына жоғары қадағалауды жүзеге асырады, адамның бұзылған құқықтары мен бостандықтарын қорғау мен қалпына келтіруді, заңдылық бұзушылықтарды анықтау мен жоюды және құқық қорғау органдарының қызметін үйлестіруді қамтамасыз етеді [36].

Дербес деректер саласында прокурорлық қадағалау тек тиісті заңнаманың бұзылуын анықтаумен шектелмей, қылмыстық процесте тұлғаның жеке өмірі мен дербес деректерінің қорғалуын қамтамасыз етуге де бағытталуы тиіс. А.М. Амиров прокурорлық қадағалаудың арнайы қағидаттары қатарында «жәбірленушілер мен қылмыстық процеске басқа да қатысушылардың дербес деректерін қорғауды», сондай-ақ «сотқа дейінгі өндірістер мен жабық сот талқылауларынан дербес деректердің жария етілуіне жол бермеуді» көрсетеді [16, 49 б.]. Автор прокурорлық қадағалаудың дербес деректер саласындағы құқықтық құралдарына заңдылықтың сақталуын тексеруді, заңдылықтың жай-күйін талдауды, сотқа дейінгі тергеп-тексеруді бастамашылық етуді, заңсыз жедел-іздестіру іс-шаралары мен жасырын тергеу әрекеттерін тоқтатуды, сотқа дейінгі тергеп-тексеру және жабық сот талқылауы деректерінің құпиялылығын қамтамасыз етуді, сондай-ақ ведомствоаралық өзара іс-қимылды жатқызады [16, Б. 63–64].

Бұл тұжырымдар осы зерттеудің қылмыстық-процестік бағыты үшін маңызды. Сотқа дейінгі тергеп-тексерудің заңдылығын қадағалау кезінде прокурор дербес деректерді алу мен пайдаланудың құқықтық негізіне, сұратылатын мәліметтердің дәлелдеу пәнімен байланысына, олардың көлемінің қажеттілігі мен мөлшерлестігіне, сондай-ақ алынған ақпараттың құпиялылығының сақталуына назар аударуы тиіс. Осы тұрғыдан прокурорлық қадағалау қылмыстық қудалаудың тиімділігі мен қылмыстық процеске қатысушылардың жеке өміріне қолсұғылмаушылық құқығы арасындағы теңгерімді қамтамасыз ететін процестік кепілдіктердің бірі ретінде қарастырылады.

Қылмыстық-процестік кодекс дербес деректерді қорғаудың тікелей арнайы тарауын қамтымаса да, оның көптеген нормалары бұл институтпен тығыз байланысты [6]. Дәлелдемелерді жинау мен бекіту, тергеу әрекеттерін жүргізу, жасырын тергеу әрекеттерін санкциялау, тінту мен алу, ақпаратты сұрату, сотқа дейінгі тергеп-тексеру деректерін жария етпеу, процеске қатысушылардың қауіпсіздігін қамтамасыз ету және сот талқылауының жариялылығы қылмыстық процестегі дербес деректер режимін қалыптастырады. Демек, дербес деректерді қорғау ҚПК-де бір ғана нормамен емес, өзара байланысты процестік кепілдіктер жиынтығымен қамтамасыз етіледі. Егер дербес деректер заңсыз алынса, рұқсатсыз қол

жеткізілсе, процестік нысанда бекітілмесе немесе олардың шығу көзі мен тұтастығы дәлелденбесе, олар дәлелдемелік мәнін жоғалтуы мүмкін – бұл әсіресе электрондық деректерге қатысты маңызды, себебі олар оңай өзгертіледі, көшіріледі немесе жойылады. Іс материалдарына қатысушылардың қолжетімділігі, көшірме беру, сот актілерін жариялау және ведомстволық ақпараттық жүйелер арқылы құжат алмасу кезінде дербес деректердің қайталама жария етілу қаупі туындайтынын ескерсек, ҚПК нормаларын дербес деректерді иесіздендіру, редакциялау және қолжетімділікті саралау тетіктерімен толықтыру қажеттігі байқалады.

Халықаралық стандарттар ұлттық құқықтық базаны бағалаудың маңызды өлшемі болып табылады. GDPR дербес деректерді өңдеудің заңдылық, әділдік, ашықтық, мақсатты шектеу, деректерді минимизациялау, дәлдік, сақтау мерзімін шектеу, тұтастық және құпиялылық қағидаттарын бекітеді [9]. Бұл қағидаттар қылмыстық процесте тікелей қолданылатын нормалар болмаса да, дербес деректерді дәлелдемелік айналымға енгізудің әдіснамалық өлшемдері ретінде маңызды; әсіресе деректер көлемін шектеу, мақсаттылық және қауіпсіздік қағидаттары тергеу органдарының сұратуларын негіздеу кезінде ескерілуі тиіс. Еуропа Кеңесінің жеке тұлғаларды дербес деректерді автоматтандырылған өңдеуге қатысты қорғау туралы Конвенциясы және оның жаңартылған 108+ моделі дербес деректерді қорғаудың халықаралық-құқықтық стандарттарын қалыптастырды [10; 11]. Бұл стандарттар деректерді өңдеу заңдылығы, арнайы санаттағы деректерді қорғау, трансшекаралық беру, қауіпсіздік шаралары және тәуелсіз бақылау органының рөлін мойындайды. Қазақстан үшін бұл стандарттар ұлттық заңнаманы халықаралық деректер айналымы мен цифрлық тергеу талаптарына бейімдеуде маңызды бағдар бола алады.

М.С. Бисалиев дербес деректерді қорғаудың халықаралық-құқықтық тетіктерін талдай отырып, ұлттық құқықтық режимдерді халықаралық стандарттармен үйлестіруді дербес деректерді қорғаудың тиімділігін арттырудың негізгі бағыттарының бірі ретінде қарастырады. Автор трансшекаралық деректер айналымына қатысты құқықтық режимдердің үйлесімділігін қамтамасыз етуде GDPR мен жаңартылған 108+ Конвенциясының қағидаттарын ескерудің маңызын атап көрсетеді [12, 84 б.; 134 б.]. Қазақстандағы трансшекаралық деректер беру мәселесін арнайы қарастыра отырып, ол: «Перспективада трансшекаралық деректер берудің өлшемдері мен тәртібін әзірлеу орынды, оның ішінде екіжақты келісімдер жасау немесе 108+ Конвенциясына қосылу тетіктерін пайдалану мүмкін», – деп көрсетеді [12, 144-б,]. Бисалиевтің бұл ұстанымы қылмыстық процесс үшін де ерекше маңызға ие. Дербес деректерді заңсыз жинау, өңдеу немесе таратуға байланысты қылмыстық істер бойынша іс үшін маңызы бар цифрлық мәліметтер шетелдік онлайн-платформаларда, бұлттық сервистерде немесе Қазақстан Республикасының юрисдикциясынан тыс орналасқан ақпараттық инфрақұрылымда сақталуы мүмкін. Мұндай жағдайда дәлелдемелік ақпаратты алу тек ұлттық қылмыстық-процестік рәсімдермен шектелмей, трансшекаралық деректерді беру талаптарын,

халықаралық құқықтық көмек тетіктерін және тиісті шетелдік юрисдикцияның деректерді қорғау режимін ескеруді қажет етеді. Сондықтан халықаралық стандарттармен құқықтық үйлесімділік дербес деректерді қорғау құралы ғана емес, трансшекаралық цифрлық мәліметтерді заңды түрде алу мен кейін қылмыстық процесте пайдалану мүмкіндігін қамтамасыз ететін маңызды алғышарт ретінде қарастырылуы тиіс.

Кристофер Кунер трансшекаралық деректер ағындарын құқықтық реттеуді бір ғана ұлттық құқықтық тәртіп шеңберінде түсіндіру жеткіліксіз екенін көрсетеді. Автор трансшекаралық деректер ағындарын реттеу кезінде әртүрлі ұлттық және халықаралық құқықтық режимдердің қатар әрекет ететінін атап өтіп, мұндай реттеуді «құқықтық плюрализм нысаны» ретінде қарастырады [37, Б. 157–188.]. Оның пікірінше, трансшекаралық деректер қозғалысын тиімді реттеу ұлттық құқықтық режимдердің оқшауланuына емес, олардың халықаралық құқықтық өзара үйлесімділігіне, юрисдикциялық ұстамдылыққа және деректерді қорғау стандарттарының өзара сәйкестігіне негізделуі тиіс [37, Б. 160–165].

Ли Байгрейв дербес деректерді қорғау құқығының мақсаттарын тек жеке өмірге қолсұғылмаушылықпен шектемейді. Автор дербес деректерді қорғаудың құқықтық режимі адамның автономиясын, тұтастығын және қадір-қасиетін қорғауға да бағытталатынын атап көрсетеді [38, Б. 119–120]. Осы тұрғыдан деректерді қорғау құқығы тұлғаның өзі туралы ақпаратты өңдеу процестеріне ықпал ету мүмкіндігін сақтауға және цифрлық ортадағы жеке автономиясын қамтамасыз етуге қызмет етеді [38, Б. 145–167].

Грэм Гринлиф дербес деректерді қорғау заңнамасының 1970-жылдардан бастап жаһандық ауқымда кеңейгенін және 2014 жылға қарай мұндай арнайы заңдар жүзден астам мемлекетте қабылданғанын көрсетеді [39, Б. 2–22]. Сонымен қатар автор ұлттық деректерді қорғау режимдерінің қалыптасуына халықаралық және өңірлік стандарттардың, соның ішінде Еуропалық Одақ, ЭЫДҰ және АТЭС тетіктерінің елеулі ықпал еткенін атап өтеді [39, Б. 23–50-. Оның салыстырмалы талдауы дербес деректерді қорғаудың біртіндеп ұлттық құқық шеңберінен шығып, халықаралық құқықтық үйлесімділік пен трансшекаралық деректер айналымының маңызды элементіне айналғанын көрсетеді [39, Б. 528–551].

Аталған еңбектерді жиынтықта қарастыру Қазақстандағы дербес деректерді қорғаудың ұлттық құқықтық базасын тек ішкі әкімшілік-құқықтық реттеу жүйесі ретінде емес, трансшекаралық деректер қозғалысы, халықаралық құқықтық стандарттар және әртүрлі юрисдикциялар арасындағы өзара іс-қимыл жағдайында дамитын кешенді құқықтық режим ретінде бағалау қажеттігін көрсетеді.

Мемлекеттік саясат тұрғысынан дербес деректерді қорғау үш бағытта дамуы тиіс. Бірінші бағыт – нормативтік-құқықтық жүйені жетілдіру, яғни дербес деректер, ақпараттандыру, Цифрлық кодекс, қылмыстық процесс және киберқауіпсіздік нормаларын өзара үйлестіру. Екінші бағыт – институционалдық бақылауды күшейту: уәкілетті органның, прокуратураның, тергеу судьясының, ақпараттық қауіпсіздік

субъектілерінің және дерек ұстаушылардың өкілеттіктері нақты үйлесуі керек. Үшінші бағыт – техникалық және ұйымдастырушылық қауіпсіздік: қауіпсіз арналар, көп факторлы аутентификация, лог-журналдар, хэш-мәндер, қолжетімділікті тіркеу, деректерді иесіздендіру және ішкі бақылау рәсімдері.

Қылмыстық процесс үшін ұлттық құқықтық базаның басты проблемасы – дербес деректердің ақпараттық-құқықтық режимі мен қылмыстық-процестік дәлелдеу тетіктерінің толық үйлеспеуінде. «Дербес деректер және оларды қорғау туралы» Заң деректерді қорғаудың жалпы талаптарын белгілейді, ҚПК дәлелдемелерді жинау мен бағалау тәртібін реттейді, ақпараттандыру және киберқауіпсіздік заңнамасы техникалық инфрақұрылым қауіпсіздігін көздейді. Алайда дербес деректерді дәлелдемелік айналымға енгізудің арнайы қылмыстық-процестік стандарты әлі толық қалыптаспаған. Осы олқылық тергеу тәжірибесінде сұратулардың мазмұны, деректер көлемі, техникалық формат, тұтастықты растау және құпиялылықты сақтау бойынша әркелкілікке әкеледі. Осыған байланысты ұлттық құқықтық база қылмыстық процестегі дербес деректермен жұмыс істеудің арнайы режимін қалыптастыруға бағытталуы тиіс – мұндай режим деректердің санатын анықтауды, алыну негізін таңдауды, сұратылатын ақпарат көлемін шектеуді, дерек ұстаушыдан алынған мәліметтерді процестік нысанда бекітуді, электрондық тұтастықты растауды, қолжетімділікті саралауды және іс материалдарындағы деректерді иесіздендіруді қамтуы қажет, әрі бір мезгілде тергеудің тиімділігін және адамның жеке өмірін қорғауды қамтамасыз етуі тиіс.

Қылмыстық процестегі басты міндет – дербес деректерді заңды түрде алу, дәлелдемелік айналымға дұрыс енгізу және оларды қайталама жария етуден қорғау арасындағы тепе-теңдікті қамтамасыз ету болып қала береді. Аталған тепе-теңдікті сақтау дербес деректерге қатысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің заңдылығын, дәлелдемелердің жарамдылығын және қылмыстық процеске қатысушылардың конституциялық құқықтары мен заңды мүдделерінің қорғалуын қамтамасыз етудің маңызды шарты болып табылады.

1.3 Қылмыстық процесте дербес деректерді қорғаудың процестік кепілдіктері

Қылмыстық процесте дербес деректерді қорғаудың процестік кепілдіктері – қылмыстық құқық бұзушылықтарды тиімді ашу мен тергеп-тексеру міндетін, дәлелдемелердің заңдылығы мен жол берілетіндігін, сондай-ақ жеке тұлғаның жеке өміріне қол сұғылмаушылық және дербес деректерінің құпиялылығы құқықтарын қатар қамтамасыз ететін құқықтық құралдар, рәсімдер және бақылау тетіктерінің жүйесі. Мұндай кепілдіктерді тек дербес деректер туралы салалық заңнаманың техникалық талаптары ретінде қарастыру жеткіліксіз. Олар қылмыстық процестің жалпы қағидаттарымен, дәлелдемелер институтымен, құқықтарды шектеудің заңды

тәртібімен, сот бақылауымен, прокурорлық қадағалаумен және қылмыстық іс материалдарындағы құпия ақпаратты сақтау режимімен тікелей байланысты.

Дербес деректерді қорғау кепілдіктерінің қылмыстық-процестік мәні ең алдымен қылмыстық процесс табиғатынан туындайды. Қылмыстық сот ісін жүргізу жария-құқықтық сипатқа ие болғанымен, ол адамның құқықтары мен бостандықтарын негізсіз шектеуге жол бермеуі тиіс. ҚР ҚПК қылмыстық процестің міндеттерін қылмыстық құқық бұзушылықтарды тез және толық ашу, оларды жасаған адамдарды әшкерелеу және жауаптылыққа тарту, сондай-ақ адамды заңсыз айыптау мен соттаудан, құқықтары мен бостандықтарын негізсіз шектеуден қорғау ретінде белгілейді [6]. Сондықтан дербес деректерді алу мен пайдалану тергеу мүдделеріне ғана емес, адамның құқықтарын қорғау міндетіне де бағынуы қажет.

Конституциялық деңгейде бұл кепілдіктер жеке өмірге қол сұғылмаушылық, өзінің және отбасының құпиясын сақтау, ар-намыс пен қадір-қасиетті қорғау, сондай-ақ заңда белгіленген шекте ақпарат алу құқығымен байланысты [1]. Дербес деректерге қол жеткізу көп жағдайда жеке өмір саласына араласуды білдіреді. Сондықтан қылмыстық процесте дербес деректерді қорғау жеке құқықтарды формалды танумен ғана шектелмей, нақты процестік тетіктер арқылы іске асырылуы тиіс. Мұндай тетіктер болмаған жағдайда тергеу барысында заңды алынған деректердің өзі кейін негізсіз таралуы, артық көлемде пайдаланылуы немесе сотта жол берілмейтін дәлелдеме ретінде танылуы мүмкін.

ҚР «Дербес деректер және оларды қорғау туралы» Заңы дербес деректерді жинау, өңдеу және қорғау кезінде заңдылық, мақсатқа сәйкестік, деректер көлемінің жеткіліктілігі және қауіпсіздік талаптарын белгілейді [2]. Бұл талаптар қылмыстық процеске де бейімделіп қолданылуы тиіс. Себебі тергеуші, анықтаушы немесе прокурор қылмыстық істі тергеп-тексеру барысында дербес деректерді жинап қана қоймайды; оларды процестік құжаттарға енгізеді, электрондық тасымалдағыштарға тіркейді, сараптамаға жолдайды, сотқа ұсынады, тараптардың танысуына береді және сот актілерінде көрсетуі мүмкін. Демек, дербес деректердің қылмыстық процестегі қозғалысы оларды қорғаудың үздіксіз режимін талап етеді.

Процестік кепілдіктердің бірінші тобы дербес деректерді алудың заңды негізіне қатысты. Дербес деректер қылмыстық іс бойынша маңызы бар мән-жайларды анықтау үшін қажет болған жағдайда ғана алынады. Бұл ретте алынатын деректердің түрі, көлемі, уақыттық шегі, дереккөзі және дәлелдеу пәнімен байланысы алдын ала айқындалуы тиіс. Егер деректер ашық дереккөздерден алынған болса, олардың дереккөзі, жариялану уақыты, шынайылығы және өзгертілмегендігі тексеріледі. Ал қолжетімділігі шектеулі дербес деректерді алу кезінде арнайы процестік негіз, прокурор санкциясы немесе тергеу судьясының рұқсаты қажет болуы мүмкін [6].

Дербес деректерді алудың заңды негізі құқықтарды шектеу шегін де анықтайды. Мысалы, байланыс құпиясына, банктік мәліметтерге, медициналық ақпаратқа, геолокациялық деректерге немесе электрондық хат-хабарға қол жеткізу адамның жеке өмір саласына елеулі араласуды білдіреді.

Мұндай жағдайда деректерді алу қажеттілік және мөлшерлестік талаптарына сай болуы тиіс. Қажеттілік нақты тергеу мақсатына жету үшін осы деректерсіз істің мән-жайын анықтау мүмкін еместігін білдіреді. Мөлшерлестік сұратылатын деректер көлемінің істің мән-жайына сәйкес келуін және жеке өмірге араласудың шектен тыс болмауын талап етеді [6].

Процестік кепілдіктердің екінші тобы деректерді жинау мен бекіту тәртібіне қатысты. ҚР ҚПК дәлелдемелердің заңды түрде алынуын талап етеді, ал заңсыз тәсілмен алынған нақты деректерді дәлелдеме ретінде пайдалануға жол бермейді [6]. Осы тұрғыдан дербес деректердің дәлелдемелік мәні олардың мазмұнымен ғана емес, алыну және бекітілу рәсімімен де айқындалады. Тергеу әрекетінің хаттамасында немесе сұрату нәтижесінде алынған материалда деректің қайдан алынғаны, кім бергені, қандай процестік негізбен алынғаны, қандай форматта ұсынылғаны және қандай қосымша файлдар тіркелгені нақты көрсетілуі қажет.

Электрондық нысандағы дербес деректер бойынша бұл талаптар одан әрі күшейеді. Лог-файлдар, IP-мекенжайлар, метадеректер, транзакциялық жазбалар, мессенджер хабарламалары, бұлттық сервистегі мәліметтер немесе бейнебақылау жазбалары өзгертілуі, жойылуы немесе толық емес күйде ұсынылуы мүмкін. Сондықтан оларды процестік нысанда бекіту кезінде файлдың атауы, көлемі, форматы, алынған уақыты, дерек ұстаушының атауы, техникалық сипаттамалары, хэш-мәні немесе өзге сәйкестендіру белгілері көрсетілуі тиіс. Бұл талап дәлелдеменің тұтастығын, өзгертілмегендігін және сотта тексерілу мүмкіндігін қамтамасыз етеді.

Процестік кепілдіктердің үшінші тобы деректерді сақтау және қолжетімділікті шектеу режиміне қатысты. Дербес деректер қылмыстық іс материалдарына енгізілгеннен кейін олардың қорғау режимі тоқтамайды. Керісінше, іс материалдарына тіркелген деректер жаңа тәуекелдерге ұшырайды: тараптардың танысуы, көшірме алу, электрондық іс жүргізу, ведомстволық жүйелер арқылы жіберу, сараптамаға жолдау, сот талқылауының жариялылығы және сот актілерін жариялау кезінде деректердің қайталама таралу қаупі артады. Сондықтан дербес деректерді қылмыстық іс материалдарында сақтау жеке қорғалған ақпараттық режим ретінде қарастырылуы тиіс.

Қылмыстық процесте құпиялылықты қамтамасыз етудің дәстүрлі тетіктерінің бірі – сотқа дейінгі тергеп-тексеру деректерін жария етпеу. ҚР ҚПК сотқа дейінгі тергеп-тексеру деректерін жария етуге прокурор рұқсат еткен көлемде ғана жол беретін қағиданы бекітеді [6]. Алайда бұл жалпы ереже дербес деректерді қорғаудың барлық мәселесін толық шешпейді. Себебі дербес деректер тек тергеу деректері ретінде ғана емес, жеке тұлғаның құпия ақпараты ретінде де қорғалуы тиіс. Сондықтан сотқа дейінгі тергеп-тексеру деректерін жария етпеу режимі дербес деректердің мазмұнына қарай қолжетімділікті саралау, артық деректерді шектеу және көшірмелерді редакциялау тетіктерімен толықтырылуы қажет.

И.В. Смолькова қылмыстық сот ісін жүргізуде дербес деректерді қорғаудың нақты процестік тәсілдері ретінде қылмыс туралы хабарды

тексеру барысында алынған мәліметтерді жария етпеуді, алдын ала тергеу деректерінің құпиялылығын сақтауды, қылмыстық процеске қатысушының жеке басы туралы мәліметтерді жасырын ұстап, бүркеншік ат қолдануды, сондай-ақ істі жабық сот отырысында қарауды бөліп көрсетеді [41, Б. 139–141]. Автордың пікірінше, бүркеншік ат қолдану іс жүргізу әрекетіне қатысушының дербес деректерін жасыру тәсілі болып табылады, ал жабық сот отырысы қылмыстық процеске қатысушылардың дербес деректерінің құпиялылығын сақтауға мүмкіндік береді [41, Б. 140–141]. Аталған тәсілдер Қазақстанның қылмыстық процесі үшін де салыстырмалы-құқықтық тұрғыдан маңызды. Қылмыстық іс материалдарында жәбірленушілердің, куәлардың және өзге де қатысушылардың тұрғылықты жері, байланыс деректері, отбасы жағдайы, медициналық мәліметтері, геолокациялық ақпараты және өзге де дербес деректері болуы мүмкін. Мұндай мәліметтердің негізсіз жария етілуі адамның жеке өміріне араласумен ғана шектелмей, оған қысым көрсету, қорқыту, құдалау немесе алынған деректерді кейіннен заңсыз пайдалану тәуекелін арттырады. Сондықтан дербес деректерді қорғау қылмыстық іс жүргізудің барлық кезеңдерінде оларға қолжетімділікті шектеу және қайталама жария етілуіне жол бермеу жөніндегі процестік кепілдіктермен қамтамасыз етілуі тиіс.

Процестік кепілдіктердің төртінші тобы қылмыстық процестегі қатысушылардың құқықтарымен байланысты. Қорғау тарапы істің барлық материалдарымен танысуға және дәлелдемелерді даулау құқығына ие. Бұл құқықты шектеу әділ сот талқылауы қағидатына қайшы келуі мүмкін [6]. Алайда іс материалдарында жәбірленушілердің, куәлардың, кәмелетке толмағандардың немесе үшінші тұлғалардың артық дербес деректері болған жағдайда, толық және бақылаусыз қолжетімділік олардың құқықтарына зиян келтіруі ықтимал. Демек, қылмыстық процесте қорғау құқығы мен дербес деректерді қорғау құқығы арасында теңгерім қажет.

Мұндай теңгерім қолжетімділікті саралау арқылы қамтамасыз етілуі мүмкін. Қорғау тарапы дәлелдеменің мазмұнын, дереккөзін және жол берілетіндігін тексеруге мүмкіндік алуы тиіс, бірақ дәлелдеу пәніне қатысы жоқ жеке мәліметтер көшірмеде бүркемеленуі немесе иесіздендірілуі мүмкін. Мысалы, жәбірленушінің нақты тұрғылықты мекенжайы немесе кәмелетке толмаған куәнің байланыс деректері қорғау құқығын іске асыру үшін қажет болмаған жағдайда, оларды бөлек қорғалған қосымшада сақтау немесе көшірмеде жабу орынды. Бұл тәсіл тараптардың процессуалдық құқықтарын шектемей, дербес деректердің қайталама таралуын азайтады.

И.В. Смолькова қылмыстық сот ісін жүргізу барысында құпия ақпаратты, соның ішінде дербес деректерді қорғауға бағытталған бірнеше процестік тәсілді бөліп көрсетеді: қылмыс туралы хабарды тексеру кезінде алынған мәліметтерді жария етпеу, алдын ала тергеу деректерін жария етуге жол бермеу, қылмыстық процеске қатысушының жеке басы туралы мәліметтерді жасырын сақтап, бүркеншік ат қолдану, сондай-ақ істі жабық сот отырысында қарау [41, Б. 139–141]. Автор бүркеншік ат қолдануды «қылмыстық процеске қатысушылардың дербес деректерін жасыру тәсілі»

ретінде сипаттайды [41, 140 б.]. Сонымен қатар жабық сот отырысы қылмыстық процеске қатысушылардың дербес деректерін құпия сақтауға мүмкіндік беретін кепілдіктердің бірі ретінде қарастырылады [41, 141 б.].

Бұл тәсілдер Қазақстанның қылмыстық процесі үшін де салыстырмалы-құқықтық тұрғыдан маңызды сипатқа ие. Қылмыстық іс материалдарында жәбірленушілердің, куәлардың және өзге де қатысушылардың мекенжайы, телефон нөмірі, электрондық поштасы, отбасы жағдайы, медициналық мәліметтері, орналасқан жері туралы ақпарат және өзге де дербес деректері болуы мүмкін. Мұндай мәліметтердің негізсіз жария етілуі адамның жеке өміріне араласумен ғана шектелмей, оған қысым көрсету, қорқыту, қудалау немесе деректерді кейіннен заңсыз пайдалану тәуекелін күшейтеді. Сондықтан қылмыстық процесте дербес деректерді қорғау дәлелдемелерді заңды түрде жинаумен қатар, іс жүргізудің барлық кезеңінде оларға қолжетімділікті шектеу және қайталама жария етілуіне жол бермеу жөніндегі процестік кепілдіктерді де қамтуы тиіс.

Процестік кепілдіктердің бесінші тобы сот бақылауы мен прокурорлық қадағалауға қатысты. Дербес деректерді алу кейбір жағдайларда адамның конституциялық құқықтарын шектеумен байланысты болғандықтан, мұндай әрекеттер тәуелсіз бақылау мен қадағалауды қажет етеді. Тергеу судьясының санкциясы құқықтарды шектеудің заңдылығы мен негізділігін алдын ала бағалауға мүмкіндік береді. Ал прокурорлық қадағалау сотқа дейінгі тергеп-тексеру барысында деректерді алудың, пайдаланудың және сақтаудың заңдылығын тексеруге бағытталады [36].

А.М. Амиров дербес деректерді қорғау саласындағы прокурорлық қадағалаудың дербес маңызын негіздей отырып, оның негізгі қағидаттарына дербес деректер туралы заңнаманы бұзу фактілеріне уақтылы ден қоюды, алынған дербес деректердің сақталуы мен жария етілмеуін, жәбірленушілер мен қылмыстық процеске өзге де қатысушылардың дербес деректерін қорғауды, сондай-ақ сотқа дейінгі өндіріс пен жабық сот талқылауларынан мұндай мәліметтердің жария болуына жол бермеуді жатқызады. Автор прокурорлық қадағалаудың негізгі бағытын дербес деректер саласындағы заңдылықты қамтамасыз етуге, бұзылған құқықтар мен бостандықтарды қорғау және қалпына келтіруге бағытталған шаралар кешенімен байланыстырады [16, 49 б.]. Сонымен қатар А.М. Амиров дербес деректерді қорғау саласындағы прокурордың құқықтық құралдары ретінде заңдылықтың сақталуын тексеруді, заңдылықтың жай-күйін талдауды, дербес деректерді өңдеуге қатысты актілерді бағалауды, сотқа дейінгі тергеп-тексеруді бастамашылық етуді, заңсыз жедел-іздестіру іс-шаралары мен жасырын тергеу әрекеттерін тоқтатуды және сотқа дейінгі тергеп-тексеру деректерінің құпиялылығын қамтамасыз етуді көрсетеді [16, Б. 63–64]. Бұл тұжырымдар қылмыстық процесс үшін ерекше маңызды. Дербес деректерді заңсыз жинау, өңдеу және таратуға байланысты істерде прокурорлық қадағалау қылмыстық қудалаудың жалпы заңдылығын тексерумен ғана шектелмеуі тиіс. Сотқа дейінгі тергеп-тексеру барысында дербес деректерді алудың құқықтық негізі, алынған ақпарат көлемінің дәлелдеу қажеттілігіне сәйкестігі, құқықтарды

шектеудің қажеттілігі мен мөлшерлестігі, сондай-ақ алынған мәліметтердің құпиялылығы мен оларды рұқсатсыз жария етуден қорғау шаралары да бағалануы тиіс. Осы тұрғыдан прокурорлық қадағалау қылмыстық құдалаудың тиімділігі мен дербес деректер субъектілерінің құқықтарын қорғау арасындағы теңгерімді қамтамасыз ететін процестік кепілдіктердің бірі ретінде қарастырылады.

Дербес деректерді қорғау кепілдіктері жасырын тергеу әрекеттерін қолдану кезінде ерекше маңызға ие болады. ЖТӘ қылмыстық құқық бұзушылықтың жасырын сипатын ашу үшін қажет болуы мүмкін, бірақ олар жеке өмір, байланыс құпиясы, электрондық коммуникация және цифрлық іздер саласына терең араласуды көздейді [6]. Сондықтан ЖТӘ қолдану кезінде өтінішхатта нақты объект, мерзім, идентификатор, деректер түрі, күтілетін дәлелдемелік нәтиже және баламалы ашық тәсілдермен деректерді алу мүмкін еместігі негізделуі тиіс. Бұл талаптар сақталмаса, ЖТӘ нәтижесінде алынған деректердің жол берілетіндігіне күмән туындайды.

ЖТӘ арқылы алынатын дербес деректер бойынша минимизация қағидаты ерекше орын алады. Тергеу органы барлық коммуникацияны, барлық аккаунт тарихын немесе барлық геолокациялық мәліметтерді емес, дәлелдеу пәніне байланысты нақты деректерді ғана алуға ұмтылуы тиіс [9]. Уақыт аралығын, құрылғыны, аккаунтты, телефон нөмірін, IP-мекенжайды немесе тұлғалар шеңберін нақтылау құқықтарды шектеудің мөлшерлестік сипатын қамтамасыз етеді. Мұндай тәсіл Еуропа Кеңесінің деректерді қорғау стандарттарындағы мақсаттылық және деректер көлемін шектеу қағидаттарымен де үйлеседі [10; 11].

Процестік кепілдіктердің алтыншы тобы дербес деректерді иесіздендіру және редакциялау тетіктеріне қатысты. Иесіздендіру қылмыстық процесте қосымша техникалық әрекет ретінде емес, сот төрелігінің жариялылығы мен жеке өмірге қол сұғылмаушылық арасындағы тепе-теңдікті қамтамасыз ететін дербес процестік кепілдік ретінде танылуы тиіс. Бұл әсіресе сот актілерін жариялау, іс материалдарының көшірмелерін беру, ғылыми немесе талдамалық мақсатта материалдарды пайдалану, сондай-ақ электрондық сот жүйелерінде ақпарат орналастыру кезінде маңызды.

Иесіздендірудің негізгі мақсаты – дәлелдемелік маңызы жоқ, бірақ тұлғаны сәйкестендіруге мүмкіндік беретін ақпаратты ашық айналымнан алып тастау немесе бүркемелеу. Мұндай деректерге ЖСН, нақты мекенжай, телефон нөмірі, банк шоты, медициналық мәлімет, кәмелетке толмаған адамның деректері, геолокация, аккаунт идентификаторы немесе үшінші тұлғалардың жеке мәліметтері жатуы мүмкін. Бұл ретте түпнұсқа материалдар қылмыстық іс құрамында қорғалған режимде сақталады, ал танысуға немесе жариялауға арналған нұсқада артық деректер шектеледі.

Дербес деректерді қорғау кепілдіктерінің маңызды элементі – деректерді сақтау тізбегін қамтамасыз ету. Электрондық дәлелдемелер мен дербес деректердің тұтастығын сақтау үшін оларды алған сәттен бастап сотқа ұсынылғанға дейінгі барлық қозғалысы тіркелуі тиіс. Қай орган, қай күні,

қандай арнамен, қандай форматта дерек алды, файл кімге берілді, қандай тасымалдағышта сақталды, көшірме жасалды ма, хэш-мән өзгерді ме – осы мәліметтер дәлелдеменің сенімділігін бағалау үшін қажет. Егер сақтау тізбегі бұзылса, деректердің өзгермегендігін дәлелдеу күрделенеді.Бұл кепілдік цифрлық криминалистикамен тығыз байланысты. Электрондық деректерді алған кезде маманның қатысуы, техникалық сипаттама жасау, файлдардың құрылымын көрсету, метадеректерді сақтау, хэш-мәнді есептеу және деректерді тек оқуға арналған форматта бекіту қажет болуы мүмкін. Мұндай техникалық шаралар қылмыстық-процестік кепілдіктің мазмұнын толықтырады, өйткені электрондық ақпараттың тұтастығы тек құқықтық рәсіммен емес, техникалық дұрыстықпен де қамтамасыз етіледі.

Дербес деректерді қорғау кепілдіктері дерек ұстаушылармен өзара іс-қимыл кезінде де іске асырылуы тиіс. Банктер, байланыс операторлары, интернет-провайдерлер, медициналық ұйымдар, мемлекеттік ақпараттық жүйелер, цифрлық платформалар және бұлттық сервистер қылмыстық іс үшін маңызы бар деректерді сақтауы мүмкін. Тергеу органы мұндай субъектілерге сұрату жолдағанда сұратудың құқықтық негізін, мақсаттарын, деректер көлемін, уақыт шегін және ұсынылатын форматты нақты көрсетуі тиіс. Бұл дерек ұстаушының артық деректер бермеуіне және берілген материалдың кейін сотта тексерілуіне мүмкіндік береді. Осы тұрғыдан дерек ұстаушыларға жолданатын сұратуларда деректерді минимизациялау қағидаты сақталуы қажет. Қылмыстық іс бойынша қажет бір транзакцияны анықтау үшін барлық есепшот тарихын сұрату, бір IP-мекенжай бойынша нақты уақыт аралығын тексеру орнына абоненттің барлық интернет белсенділігін талап ету немесе бір аккаунттағы нақты хабарламаны дәлелдеу үшін барлық жеке хат-хабарды алу мөлшерлестік талабына қайшы келуі мүмкін. Сұрату неғұрлым нақты болса, алынған деректердің дәлелдемелік құндылығы да, құқықтарды қорғау деңгейі де соғұрлым жоғары болады.

Дерек ұстаушыларға жолданатын сұратуларда қылмыстық құқық бұзушылықтың нақты бабын көрсету мәселесі де процестік кепілдіктер жүйесінде ерекше орын алады. Кейбір істерде нақты саралау бабын сыртқы сұратуда көрсету жәбірленушінің мәртебесін, оқиғаның сипатын немесе сезімтал жеке ақпаратты ұйым қызметкерлеріне жанама түрде ашып беруі мүмкін. Сондықтан қылмыстық істің нақты саралау бабы, сұратылатын мәліметтердің дәлелдеу пәнімен байланысы және қажеттілігі прокурорға ұсынылатын ішкі негіздемеде толық көрсетіліп, ал дерек ұстаушыға жолданатын сыртқы сұратуда оны орындауға жеткілікті процестік реквизиттер мен сұратылатын деректер көлемі ғана қамтылғаны жөн. Бұл тәсіл сұратудың заңдылығын әлсіретпей, дербес деректердің қайталама жария болу тәуекелін азайтады.

Дербес деректерді қорғау кепілдіктері сот талқылауы сатысында да сақталуы тиіс. Сот талқылауының жариялылығы – әділ соттың маңызды қағидаты. Алайда жариялылық абсолютті емес және жеке өмірге, мемлекеттік құпияға, кәмелетке толмағандардың құқықтарына немесе жәбірленушілердің қауіпсіздігіне қауіп төнген жағдайда шектелуі мүмкін [6].

Сондықтан дербес деректерді қамтитын істерде сот сот отырысының ашық немесе жабық өтуін, сот актісінде қандай мәліметтердің көрсетілуін және жария нұсқада қандай деректердің иесіздендірілуін жеке бағалауы қажет.

Сот актілерін жариялау кезінде дербес деректерді қорғау мәселесі ерекше күрделі. Бір жағынан, сот актілерінің ашықтығы сот төрелігіне қоғамдық бақылауды қамтамасыз етеді. Екінші жағынан, сот актісінде жәбірленушінің, куәнің, кәмелетке толмағанның, медициналық немесе интимдік мәліметтердің, банктік деректердің немесе нақты мекенжайдың жариялануы тұлғаның құқықтарына қосымша зиян келтіруі мүмкін. Осы себепті сот актілерінің жария нұсқаларында тұлғаны тікелей сәйкестендіретін мәліметтерді алып тастау немесе бүркемелеу дербес деректерді қорғаудың міндетті кепілдігі ретінде қарастырылуы тиіс.

Халықаралық стандарттар дербес деректерді қорғау кепілдіктерінің қылмыстық процесс үшін де өзекті екенін көрсетеді. GDPR деректерді өңдеудің заңдылық, әділдік, ашықтық, мақсатты шектеу, деректер көлемін азайту, дәлдік, сақтау мерзімін шектеу, тұтастық және құпиялылық қағидаттарын белгілейді [9]. Еуропа Кеңесінің 108 және 108+ Конвенциялары дербес деректерді өңдеу кезінде қауіпсіздік, құқықтық негіз, мақсаттылық және тәуелсіз бақылау қағидаттарын күшейтеді [10; 11]. Бұл стандарттар ұлттық қылмыстық процесте тікелей қолданылатын норма ретінде емес, деректермен жұмыс істеудің құқықтық бағдарлары ретінде бағалануы мүмкін.

Еуропалық адам құқықтары сотының практикасы дербес деректерді қорғауды жеке өмірге қолсұғылмаушылық құқығының құрамдас бөлігі ретінде кеңінен түсіндіреді. S. and Marper v. the United Kingdom ісінде Сот дербес деректерді қорғаудың Конвенцияның 8-бабымен кепілдік берілген жеке және отбасылық өмірді құрметтеу құқығын жүзеге асыру үшін іргелі маңызы бар екенін атап өтіп, сақталатын деректер олардың жиналу мақсатына қатысты, шамадан тыс емес және қажетті мерзімнен артық сақталмайтын болуы тиіс екенін көрсетті [42, §§ 103, 107]. Сонымен қатар күдік келтірілген, бірақ сотталмаған тұлғалардың саусақ іздерін, жасушалық үлгілері мен ДНҚ-профильдерін жаппай және сараланбаған түрде сақтау жеке және қоғамдық мүдделер арасындағы әділ теңгерімді бұзатын мөлшерлес емес араласу деп танылды [42, §§ 119, 125]. Big Brother Watch and Others v. the United Kingdom ісінде Еуропалық адам құқықтары сотының практикасы электрондық коммуникацияларды жаппай ұстап қалу режиміне қатысты «толық циклді кепілдіктер» талабын қалыптастырды. Сот мұндай араласудың әрбір кезеңінде қолданылатын шаралардың қажеттілігі мен мөлшерлестігі бағалануға, бастапқы кезеңде тәуелсіз рұқсат берілуге, ал кейіннен тәуелсіз бақылау мен тексеру қамтамасыз етілуі тиіс екенін атап көрсетті [43, §§ 348–356, әсіресе § 350]. Аталған құқықтық ұстанымдар қылмыстық процесте дербес деректерді алу мен сақтауды тек формалды заңдық негіздің болуымен шектеуге болмайтынын көрсетеді. Деректердің көлемі, сақтау мерзімі, оларды алу мақсаты, тұлғаның құқықтарына араласу дәрежесі және тәуелсіз бақылау тетіктерінің болуы да бағалануы тиіс. Осы

тұрғыдан Еуропалық адам құқықтары сотының практикасы дербес деректермен жұмыс істеуде мақсаттылық, қажеттілік, мөлшерлестік және тиімді бақылау талаптарының өзара байланысын айқындайды.

Қылмыстық процесте дербес деректерді қорғаудың процестік кепілдіктерін жүйелеу үшін оларды бірнеше деңгейге бөлуге болады. Бірінші деңгей – нормативтік кепілдіктер: Конституция, ҚПК, дербес деректер туралы заңнама, ақпараттандыру, прокуратура, адвокаттық қызмет, жедел-іздестіру қызметі және мемлекеттік құпиялар туралы актілер. Екінші деңгей – институционалдық кепілдіктер: тергеу судьясы, прокурор, сот, қорғаушы, уәкілетті орган және дерек ұстаушының жауаптылығы. Үшінші деңгей – рәсімдік кепілдіктер: санкциялау, сұратуды негіздеу, хаттамалау, деректер көлемін шектеу, сақтау тізбегі, сараптамалық тексеру және дәлелдемелерді бағалау. Төртінші деңгей – техникалық кепілдіктер: хэш-мән, метадеректерді сақтау, қауіпсіз арна, қолжетімділікті тіркеу, резервтік сақтау және ақпараттық жүйелердегі аудит журналдары. Осы деңгейлер өзара байланыста болғанда ғана дербес деректерді қорғау тиімді болады. Мысалы, тек заңда деректерді қорғау міндетін бекіту жеткіліксіз, егер сұратулар нақты құрылмаса немесе электрондық материалдардың тұтастығы расталмаса, дәлелдемелік база әлсірейді. Сол сияқты техникалық қорғау шаралары жеткілікті болғанымен, тараптардың құқықтары, прокурорлық қадағалау немесе сот бақылауы қамтамасыз етілмесе, адамның құқықтары негізсіз шектелуі мүмкін. Сондықтан дербес деректерді қорғаудың процестік кепілдіктері құқықтық және техникалық элементтердің тұтас жүйесі ретінде қарастырылуы тиіс.

Қорғаушының рөлі де дербес деректерді қорғау кепілдіктерінің маңызды бөлігі болып табылады. Адвокат дәлелдемелердің жол берілетіндігін, деректердің заңды алынуын, алынған мәліметтердің дәлелдеу пәнімен байланысын және артық деректердің іске тіркелуін тексеруге құқылы. Сонымен қатар қорғаушы өз қорғауындағы адамның дербес деректері негізсіз жария етілмеуін талап ете алады [6]. Бұл қылмыстық процестегі жарыспалылық қағидатының деректерді қорғау саласындағы көрінісі болып табылады.

Жәбірленуші мен куәлар үшін дербес деректерді қорғау кепілдіктері қауіпсіздікпен тығыз байланысты. Кейбір істерде олардың мекенжайы, телефон нөмірі, жұмыс орны, отбасы құрамы, денсаулық жағдайы немесе цифрлық аккаунттары туралы мәліметтер жария етілсе, оларға қысым көрсету, қорқыту немесе қайта виктимизациялау қаупі туындайды. Сондықтан қылмыстық процесте куә мен жәбірленушінің деректерін қорғау тек құпиялылық мәселесі емес, олардың қауіпсіздігі мен процеске қатысу мүмкіндігін қамтамасыз ететін кепілдік ретінде қарастырылуы тиіс.

Кәмелетке толмағандарға қатысты дербес деректерді қорғау күшейтілген сипатқа ие болуы тиіс. Кәмелетке толмаған жәбірленуші немесе куә туралы ақпараттың жариялануы оның психологиялық жағдайына, әлеуметтік ортасына және болашақ құқықтық мәртебесіне зиян келтіруі мүмкін. Сондықтан мұндай істерде аты-жөнін, оқу орнын, мекенжайын,

отбасы туралы мәліметтерді, медициналық деректерді және іс мән-жайынан туындайтын жанама сәйкестендіру белгілерін шектеу қажет. Бұл талап сот актілерін жариялау кезінде де сақталуы тиіс.

Дербес деректерді қорғаудың процестік кепілдіктері заңсыз алынған немесе артық алынған деректердің салдарын да қамтуы тиіс. Егер деректер заңсыз алынса, олар дәлелдеме ретінде жол берілмейтін деп танылуы мүмкін. Егер деректер артық көлемде алынса, оларды бөліп сақтау, іске толық тіркемеу, көшірмеде редакциялау немесе жою тәртібі белгіленуі қажет. Қылмыстық процесте мұндай тетіктің болмауы дербес деректерді қорғау режимін әлсіретеді және сотқа дейінгі тергеп-тексерудің заңдылығына күмән туғызады.

Бұл жерде «арнайы процестік режим» идеясы маңызды. Дербес деректерді қорғаудың арнайы процестік режимі деп қылмыстық іс материалдарында дербес деректерді анықтау, санаттау, қолжетімділігін шектеу, техникалық тұтастығын бекіту, көшірмелерді редакциялау, түпнұсқаны қорғалған режимде сақтау және жария нұсқаларды иесіздендіру бойынша бірізді рәсімдер жиынтығын түсіну ұсынылады. Мұндай режим жалпы құпиялылық талабын нақты процестік әрекеттер жүйесіне айналдырады.

Біздің тұжырымдауымызша, қылмыстық процесте дербес деректерді қорғаудың процестік кепілдіктері төрт негізгі мақсатқа қызмет етуі тиіс:

1. деректерді заңды және мөлшерлі алуды қамтамасыз ету;
2. алынған деректердің дәлелдемелік жарамдылығын сақтау;
3. қылмыстық іс материалдарында деректердің негізсіз таралуына жол бермеу;
4. тараптардың құқықтары мен тергеу тиімділігі арасындағы құқықтық тепе-теңдікті сақтау.

Осы мақсаттар бірлікте іске асқанда ғана дербес деректерді қорғау қылмыстық процестің шынайы кепілдігіне айналады.

Дербес деректерді қорғаудың процестік кепілдіктері қылмыстық процестегі қосалқы элемент емес, дәлелдемелерді заңды түрде алу, бекіту, тексеру және пайдалану тәртібін қамтамасыз ететін маңызды кепілдіктердің бірі болып табылады. Дербес деректер заңда көзделген негіздер мен рәсімдер сақталмай алынған, олардың дереккөзі анықталмаған, цифрлық тұтастығы мен шығу тегі тиісті түрде расталмаған жағдайларда мұндай мәліметтердің жол берілетіндігі мен анықтығы ҚПК талаптары тұрғысынан арнайы бағалауды қажет етеді. Ал дәлелдеу қажеттілігімен байланысы жоқ деректерді шамадан тыс көлемде жинау, оларды негізсіз сақтау немесе іс материалдарында құпиялылық режимін қамтамасыз етпеу дәлелдеменің мазмұнынан бөлек, адамның жеке өміріне қолсұғылмаушылық құқығы мен қылмыстық-процестік қызметтің заңдылығына қатысты дербес мәселе туындатады. Сондықтан дербес деректерді қорғаудың процестік кепілдіктері дәлелдеу қызметінің заңдылығын, қылмыстық процеске қатысушылардың құқықтарын қорғауды және мемлекеттік араласудың қажеттілігі мен мөлшерлестігін қамтамасыз ететін өзара байланысты

тетіктер жүйесі ретінде қарастырылуы тиіс.

2 ДЕРБЕС ДЕРЕКТЕРДІ ЗАҢСЫЗ ЖИНАУМЕН, ӨҢДЕУМЕН ЖӘНЕ ТАРАТУМЕН БАЙЛАНЫСТЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫ СОТҚА ДЕЙІНГІ ТЕРГЕП-ТЕКСЕРУДІҢ ПРОЦЕСТІК МӘСЕЛЕЛЕРІ

2.1 Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық істер бойынша дәлелдеу пәні және сотқа дейінгі тергеп-тексеруді ұйымдастыру

Дербес деректерге қатысты құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің мазмұны бірінші тарауда анықталған қылмыстық-құқықтық белгілерді нақты іс бойынша тексерілетін мән-жайларға айналдыру арқылы ашылады. Қылмыстық заң әрекеттің жазаланатын шегін белгілейді, ал қылмыстық-процестік заң сол шектің сақталғанын қандай деректермен және қандай рәсіммен анықтауға болатынын айқындайды. Осы сабақтастықтың бұзылуы біріншіден – дербес деректердің таралу фактісін құрамның өзге белгілерін тексерместен қылмыс деп бағалау, екіншіден – цифрлық ақпараттың техникалық күрделілігін сылтау етіп, заңмен қорғалатын мүддеге жасалған қолсұғушылықтың процестік тексерілуін қамтамасыз етпеу сияқты екі түрлі қателікке әкелуі мүмкін [2; 6; 19].

ҚР ҚПК-нің 113-бабында белгіленген дәлелдеу пәні осы істер үшін де бастапқы нормативтік негіз болып табылады. Оқиға, әрекетті жасаған адам, кінә, зиянның сипаты мен мөлшері және жауаптылыққа әсер ететін мән-жайлар цифрлық орта ерекшелігімен нақтыланады. Алайда дәлелдеу пәнін тергеуші алдын ала таңдаған айыптау нұсқасының шегіне дейін тарылтуға болмайды. ҚПК-нің 24, 25, 112 және 125-баптарын өзара байланысты қолдану айыптайтын және ақтайтын мәліметтерді тексеруді, әрбір дәлелдеменің қатыстылығын, жол берілетіндігін, анықтығын, ал жиынтықтың жеткіліктілігін бөлек бағалауды талап етеді. Жоғарғы Соттың дәлелдемелерді бағалау жөніндегі нормативтік қаулысы бұл бағалаудың уәжді болуына бағдар береді [6; 44].

О.С. Керр цифрлық дәлелдемелерді жинаудың дәстүрлі заттай дәлелдемелерді іздеу мен алудан елеулі ерекшеленетінін атап көрсетеді. Автор компьютерлік тергеуде құрылғыны немесе ақпарат жеткізгішті физикалық түрде алу мен ондағы цифрлық мәліметтерді кейіннен криминалистикалық зерттеу іс жүзінде бір-бірінен ажыратылатын кезеңдер екенін көрсетіп, дәстүрлі қылмыстық-процестік ережелердің мұндай ерекшеліктерді әрдайым толық ескере бермейтінін негіздейді [45, Б. 285–289]. Бұл тұжырым Қазақстан жағдайында цифрлық мәліметтерді алу кезінде процестік өкілеттіктің негізі мен көлемін тек бастапқы алу сәтінде ғана емес, оларды кейіннен іздеу, зерттеу және іс бойынша пайдалану кезеңдерінде де

нақты айқындау қажеттігін көрсетеді.

Б. Кэрриер мен Ю. Спаффорд физикалық және цифрлық оқиға орнын өзара байланыстыратын тергеу моделін ұсынып, компьютерлік жүйені дербес «цифрлық оқиға орны» ретінде қарастырады [46, Б. 5–11]. Авторлардың моделінде цифрлық зерттеудің мақсаты жүйеде болған электрондық оқиғаларды анықтау және алынған нәтижелерді физикалық оқиға орнын реконструкциялау үшін пайдалану болып табылады. Сонымен бірге цифрлық әрекетті белгілі бір тұлғамен байланыстыру үшін физикалық дәлелдемелер мен нақты жағдайдың контексті де ескерілуі тиіс [46, Б. 8–10]. Осы ғылыми ұстанымдардан цифрлық іздің табылуы мен оны нақты қылмыстық әрекетке және белгілі бір тұлғаға жатқызу бірдей ұғымдар емес деген қорытынды туындайды. Цифрлық мәліметтер олардың шығу тегі, уақыттық және оқиғалық контексті, нақты пайдаланушымен байланысы, тұтастығы және басқа дәлелдемелермен сәйкестігі тұрғысынан дербес тексерілуі тиіс.

Дәлелдеу пәнінің бірінші блогын ақпараттың дербес дерекке жататыны құрайды. Тергеу мәліметтің нақты немесе айқындалатын тұлғамен байланысын, оны сәйкестендірудің тікелей не жанама тәсілін, жеке немесе отбасы құпиясына қатыстылығын анықтауы керек. Дерек атауы ғана жеткіліксіз: бір жүйеде техникалық белгі болып көрінетін идентификатор басқа кестемен біріктірілгенде адамның медициналық қызмет алуын немесе орналасуын ашуы мүмкін. Сондықтан алынған массивтің құрылымы, өрістердің мағынасы және сәйкестендіру кілттері түсіндіріледі. Мұндай талдау деректердің бәрін тергеушіге толық ашуды міндетті етпей, тұлғамен байланысты көрсету үшін жеткілікті іріктелген жазбалар мен жүйе сипаттамасы пайдаланылуы мүмкін [2; 4].

Екінші блок әрекеттің заңсыздық негізін анықтауға бағытталады. Бұл ретте субъектінің келісімінің болмауы, берілген келісімнің мазмұны мен шегінен шығу және дербес деректерді келісімсіз жинауға немесе өңдеуге заңда көзделген өзге құқықтық негіздің болмауы бірдей құқықтық жағдайлар ретінде қарастырылмауы тиіс. «Дербес деректер және оларды қорғау туралы» Заңның 7-бабына сәйкес дербес деректерді жинау мен өңдеу, жалпы ереже бойынша, субъектінің немесе оның заңды өкілінің келісімімен жүзеге асырылады, ал 9-бапта мұндай келісім талап етілмейтін арнайы жағдайлар көзделген [2]. Сондықтан тергеу органы келісімнің формалды бар-жоғын анықтаумен шектелмей, оның алыну тәсілін, мазмұнын, қолданылу мерзімін, қамтитын деректер мен операциялар көлемін, үшінші тұлғаларға беру мүмкіндігін және оны кері қайтарып алу жағдайларын тексеруі тиіс. Заңның 8-бабы келісімнің жазбаша, мемлекеттік немесе мемлекеттік емес сервис арқылы не оны алғанын растауға мүмкіндік беретін өзге тәсілмен берілуі мүмкін екенін, сондай-ақ келісімде жиналатын деректердің тізбесі мен оларды үшінші тұлғаларға беру туралы мәліметтер көрсетілуі қажет екенін белгілейді [2]. Осыған байланысты тұлғаның ақпараттық жүйеге жалпы қолжетімділік құқығы оның кез келген субъектінің дербес деректерін кез келген мақсатта қарауға, жүктеуге немесе пайдалануға автоматты түрде құқық бермейді. Деректерді пайдаланудың заңдылығы нақты қызметтік

өкілеттікпен, өңдеу мақсатымен және қажетті әрі жеткілікті деректер көлемімен салыстырылып бағалануы тиіс [25]. Ал келісімді растайтын жеке файлдың табылмауы келісімнің мүлде болмағанын өздігінен дәлелдемейді, өйткені заң келісім берудің бірнеше нысанын көздейді. Мұндай жағдайда келісімнің бар-жоғын анықтау үшін мемлекеттік немесе мемлекеттік емес сервистегі жазбалар, ақпараттық жүйенің тіркеу мәліметтері, шарттар, өтініштер, архивтік құжаттар және деректерді өңдеуге құқық беретін өзге де заңдық негіздер жиынтық түрде тексерілуітиіс [2; 25].

Үшінші блок нақты операцияны және оның аяқталу сәтін анықтауға бағытталады. Жинау кезінде деректің қай көзден алынғаны, өңдеу кезінде қандай өзгерту, салыстыру, біріктіру немесе пайдалану әрекеті орындалғаны, тарату кезінде кімге және қандай арнамен қолжетімді болғаны ажыратылады. Бір файлдың табылуы осы операциялардың барлығын қатар дәлелдемейді. Мысалы, автоматты синхрондау файлды құрылғыға пайдаланушының тікелей пәрменінсіз жеткізуі мүмкін, ал сәтсіз жіберу туралы жазба хабарламаның адресатқа жеткенін растамайды. Құрам материалдық сипатта болған жағдайда оның аяқталуын тиісті салдардың туындауымен байланыстыру қажет; операцияның техникалық аяқталуы қылмыстың заңдық аяқталуымен барлық жағдайда сәйкес келмейді [6; 19].

Төртінші блок әрекетті белгілі бір адамға телуге, яғни атрибуцияға арналған. Аккаунт иесі, абонент, құрылғыны иеленуші, жүйелік әкімші және нақты пайдаланушы әртүрлі тұлғалар болуы ықтимал. Ортақ пароль, қызметтік аккаунт, қашықтан басқару, зиянды бағдарлама немесе ұрланған сеанс туралы нұсқалар тексеріледі. Жеке тұлғаның қатысуын негіздеу үшін аутентификация журналы, құрылғыдағы жергілікті із, жұмыс кестесі, байланыс деректері, куә айғақтары және операцияның контексті салыстырылады. Бұл жерде деректердің көптігі сапалы байланыстың орнын алмастырмайды: бір серверден алынған бірнеше есеп бір бастапқы жазбаның туындысы болуы мүмкін.

Бесінші блок кінәға, мақсат пен мотивке, ал арнайы субъект көзделген жағдайда оның міндетіне қатысты. ҚК-нің 147-бабының 1-бөлігі бойынша тұлғаға қандай қорғау шарасы жүктелгені, оны орындауға нақты мүмкіндігі болғаны және бұзушылықтың салдармен байланысы зерттеледі. Қызметтік жағдайды пайдалану белгісі лауазым атауымен шектелмейді: лауазым берген мүмкіндіктің нақты операцияны жасауға қалай пайдаланылғаны көрсетіледі. Заңсыздықты ұғыну, пайдакүнемдік мақсат немесе кек алу ниеті хат-хабармен, төлеммен, ескертулерге реакциямен және әрекеттердің жүйелілігімен салыстырылады. Құрылғыда шифрлау бағдарламасының болуы немесе адамның құпиялылық құралын қолдануы кінәнің дербес дәлелі ретінде қарастырылмайды [19].

Алтыншы блок зиянды және себептік байланысты қамтиды. Елеулі зиян ҚК-нің қолданылатын бөлігінде міндетті белгі болған жағдайда нақты анықталуы тиіс. Барлық бөліктерге бірдей, диспозициядан тыс міндетті салдар енгізу де, салдар талап етілетін құрамда оны болжаммен алмастыру да дұрыс емес. Қаржылық шығын, жеке өмір туралы мәліметтің жария болуы,

қауіпсіздік қатері, психологиялық зардап және өзге салдарлар тиісті дәлелдемелермен нақтыланады. Бір тұлғаның дерегі бірнеше көзден тараған жағдайда осы істегі әрекеттің қандай салдарға себеп болғаны жеке тексеріледі. Жәбірленушінің бағасы ескеріледі, бірақ зиянның құқықтық елеулілігі туралы түпкілікті шешім сарапшыға жүктелмейді [6; 19].

Осы алты блоктың байланысын дәлелдеу міндеттерінің картасы арқылы ұйымдастыру ұсынылады. Картада әрбір тексерілетін белгіге қатысты бастапқы және балама нұсқа, күтілетін із, оның ұстаушысы, жойылу тәуекелі, алу негізі, тексеру тәсілі және шешілмеген қайшылық белгіленеді. Мұндай карта ҚПК-де көзделген процестік құжатты алмастырмайтын жұмыс құралы болып табылады. Оның ғылыми маңызы – дерек жинауды техникалық мүмкіндікпен емес, құрамның нақты белгісімен шектеуінде; практикалық маңызы – әрбір тергеу әрекетінен кейін дәлелдеу жоспарын жаңартуға мүмкіндік беруінде.

Осы зерттеуде цифрлық із деп адамның әрекеті, бағдарламалық құралдың жұмысы немесе ақпараттық жүйелердің өзара әрекеттесуі нәтижесінде цифрлық ортада пайда болған, өзгерген, берілген не сақталған және қылмыстық іс үшін маңызы бар оқиғаның мән-жайларын анықтауға мүмкіндік беретін ақпараттық өзгерісті түсіну ұсынылады. Бұл ұғым осы жұмыста криминалистикалық жұмыс анықтамасы ретінде пайдаланылады. Цифрлық іздің анықталуы оның автоматты түрде қылмыстық-процестік дәлелдеме мәртебесіне ие болғанын білдірмейді: ондағы мәліметтер заңда көзделген тәртіппен алынуға, процестік нысанда бекітілуге, тексерілуге және бағалануы тиіс. С. Гарфинкель цифрлық криминалистиканың одан әрі дамуы деректерді ұсыну мен криминалистикалық өңдеудің стандартталған және модульдік тәсілдерін қалыптастыруды қажет ететінін көрсетеді [47, S64 б.]. Автор стандартталған абстракциялар мен деректер форматтарының болмауы әртүрлі криминалистикалық құралдар мен зерттеу нәтижелерінің өзара үйлесімділігін төмендететінін атап өтіп, бірыңғай форматтарды пайдалану деректерді әртүрлі құралдар арасында алмасуға, алынған нәтижелерді салыстыруға және өзара тексеруге мүмкіндік беретінін негіздейді [47, Б. S68–S69]. Қазақстанның қылмыстық процесі үшін бұл ұстанымның маңызы әртүрлі техникалық құралдармен алынған цифрлық мәліметтерді олардың шығу тегін, құрылымын және өңдеу кезеңдерін түсінуге әрі кейіннен тексеруге мүмкіндік беретін бірізді нысанда бекіту қажеттілігімен айқындалады.

Цифрлық іздерді қалыптасу көзіне қарай пайдаланушы жасаған мазмұнға, жүйе автоматты тіркеген оқиғаларға және өңдеуден алынған туынды нәтижелерге бөлу орынды. Бірінші топқа хат-хабар, фото, құжат және жарияланым; екіншісіне кіру, өзгерту, экспорттау және беру журналдары; үшіншісіне сараптамалық есеп, уақыттық кесте және іздеу нәтижесі жатады. Сақталу орны бойынша құрылғыдағы, ұйым жүйесіндегі, провайдердегі және бұлттағы іздер ажыратылады. Тұрақтылық белгісі бойынша жедел жад, белсенді сеанс және уақытша журнал сияқты тез жоғалатын іздер ұзақ сақталатын архивтерден ерекшеленеді. Жіктеудің

мақсаты – әр объектіні алу кезегін және тексерудің шегін анықтау.

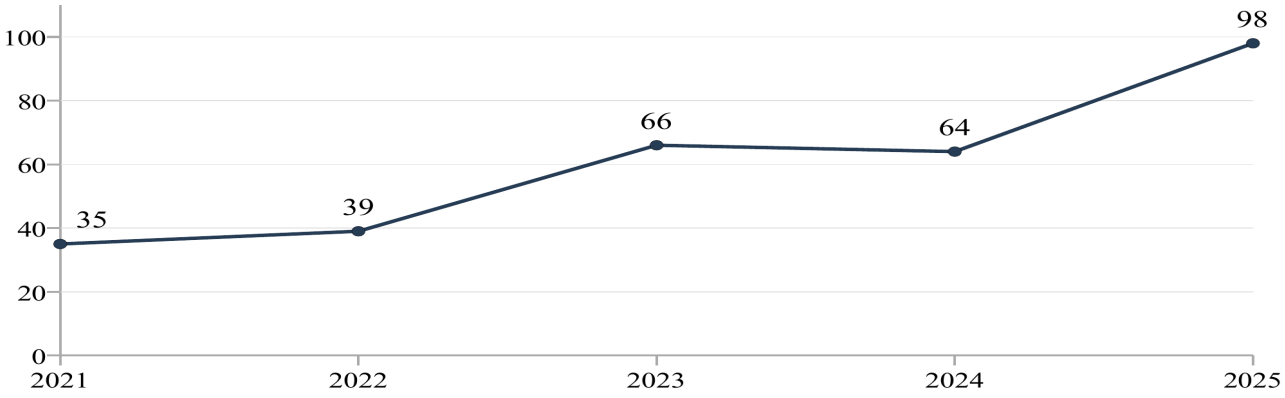
Д. Куик пен К.-К.Р. Чу цифрлық криминалистикалық зерттеуге ұсынылатын деректер көлемінің тұрақты өсуі оларды алу, өңдеу және талдау мүмкіндіктеріне елеулі жүктеме түсіретінін, соның салдарынан цифрлық материалдарды зерттеу мерзімдерінің ұзаруы мен жиналған деректердің қордалануы мүмкін екенін көрсетеді [48, 273–275 б.]. Авторлар бұл мәселені шешудің ықтимал бағыттары ретінде деректерді қысқарту, цифрлық триаж, деректерді интеллектуалдық талдау және өңдеу қуатын арттыру сияқты тәсілдерді қарастырады. Қылмыстық-процестік тұрғыдан деректер көлемінің ұлғаюына жауап барлық қолжетімді ақпаратты саралаусыз жинау болмауы тиіс. Цифрлық мәліметтерді уақыт, ақпараттық жүйе, пайдаланушы, құрылғы немесе нақты операция бойынша мақсатты түрде іріктеу тергеудің жұмыс көлемін азайтуға және іске қатысы жоқ тұлғалардың дербес деректерін негізсіз жинауды шектеуге мүмкіндік береді. Сонымен бірге мұндай іріктеу іс үшін маңызы болуы мүмкін, оның ішінде күдіктіні ақтайтын немесе жауаптылығын жеңілдететін контекстің жоғалуына әкелмеуі тиіс. Сондықтан қолданылған сүзгі өлшемдері, іріктеуге енгізілген және одан тыс қалған деректер санаттары, сондай-ақ қажет болған жағдайда іздеу шегін кеңейту мүмкіндігі процестік және техникалық тұрғыдан құжатталуы қажет. Осылайша, деректерді азайту қағидаты дәлелдеудің толықтығына қарсы қойылмай, нақты іс бойынша қажетті және қатысты цифрлық мәліметтерді айқындаудың негізделген шегі ретінде қолданылуы тиіс.

К. Руан, Дж. Карти, Т. Кечади және М. Кросби бұлттық криминалистиканы тек техникалық мәселе ретінде емес, техникалық, ұйымдастырушылық және құқықтық өлшемдердің өзара байланысы ретінде қарастырады [49, Б. 35–46]. Авторлар бұлттық ортада деректердің әртүрлі юрисдикцияларда орналасуы, бұлттық қызмет провайдері мен тұтынушы арасындағы міндеттердің бөлінуі, көп пайдаланушылық орта және провайдерлер арасындағы өзара тәуелділік тергеуді күрделендіретінін көрсетеді. Сонымен қатар цифрлық мәліметтерді жинау мүмкіндігі бұлттық қызметтің нақты моделіне және провайдердің тергеушіге не тұтынушыға беретін қолжетімділік деңгейіне тәуелді екенін атап өтеді [49]. Руан және бірлескен авторлардың еңбегінде бұлттық криминалистиканың үш өлшемді сипаты тікелей негізделген. NISTIR 8006 бұлттық ортадағы криминалистикалық қиындықтарды жүйелей отырып, лог-журналдардың қолжетімділігі мен сапасы, уақыт белгілерін синхрондау, цифрлық мәліметтердің физикалық және логикалық орналасуын анықтау, сондай-ақ құпия және дербес деректермен жұмыс істеу мәселелерін жеке проблемалық бағыттар ретінде бөледі [50, Б. 12–14]. Құжатта дәлелдеме дер кезінде анықталмаса, оның қайта жазылуы немесе жоғалуы мүмкін екені, ал бұлттық инфрақұрылымда деректердің нақты физикалық орналасуын анықтау күрделі болуы ықтимал екені арнайы көрсетілген. NIST SP 800-201 бұл проблемаларды «криминалистикалық дайындық» (forensic readiness) тұрғысынан дамытады. Құжатта бұлттық жүйе архитектурасы цифрлық дәлелдемелерді кейіннен тиімді анықтау, алу, сақтау және зерттеу

мүмкіндігін алдын ала ескеру қажет екені көрсетіліп, Cloud Computing Forensic Reference Architecture жүйенің функционалдық мүмкіндіктеріне криминалистикалық талаптарды кіріктіруге арналған әдіснамалық модель ретінде ұсынылады [51, Б. 5–7, 20 б.]. Аталған ұстанымдарды Қазақстанның сотқа дейінгі тергеп-тексеру тәжірибесіне бейімдеу дерек ұстаушы ұғымын тек ақпарат физикалық орналасқан субъектпен шектемеуді талап етеді. Бұлттық инфрақұрылым жағдайында ұйым серверді немесе сақтау құрылғысын тікелей иеленбеуі мүмкін, алайда шарттық немесе техникалық өкілеттіктеріне байланысты қажетті журналдарды, аккаунт деректерін немесе өзге цифрлық мәліметтерді алу, экспорттау не оларды сақтауға бастамашылық ету мүмкіндігіне ие болуы ықтимал. Сондықтан тергеу барысында «деректер нақты қайда орналасқан?» және «оларды кім заңды әрі техникалық тұрғыдан бере алады?» деген сұрақтар дербес анықталуы тиіс.

Тергеуді ұйымдастырудың эмпирикалық негізін 2021–2025 жылдары тіркелген 302 құқық бұзушылық туралы массив және сот актілері шығарылған адамдар жөніндегі статистика құрайды. Бірінші массив кіріспеде ҚК-нің 147-бабының 3–5-бөліктеріне қатысты сипатталған. Сот статистикасы осы баптың 1–5-бөліктерін қамтиды және өзге есеп бірлігін пайдаланады. Сондықтан жылдық қатарларды қатар көрсету олардың бір істер жиынтығы екенін білдірмейді. Тіркелген оқиға бойынша сот шешімі басқа жылы шығарылуы, бір іске бірнеше адам қатысуы немесе бір тұлғаға бірнеше эпизод тағылуы мүмкін [21; 22].

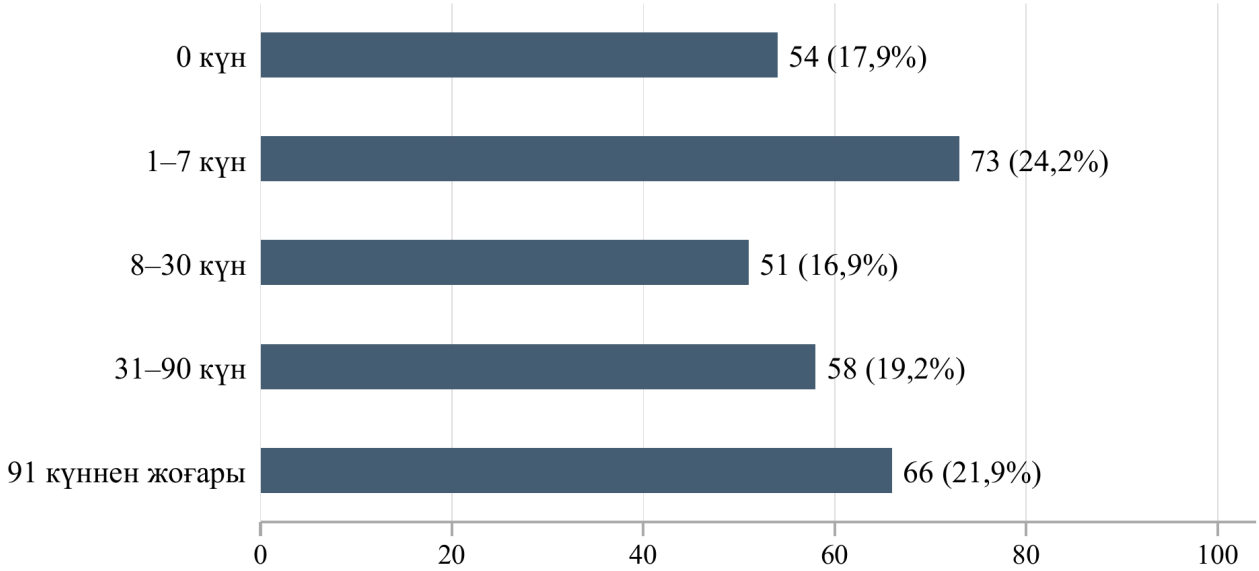
Тіркелген құқық бұзушылықтар саны 2021 жылғы 35-тен 2025 жылғы 98-ге дейін өскен. Бұл өзгеріс тергеу жүктемесінің ұлғаюын сипаттайды, бірақ қылмыстылықтың нақты таралуы дәл осы мөлшерде артқанын жеке өзі дәлелдемейді: тіркеу практикасы, азаматтардың жүгінуі және анықтау мүмкіндігі де көрсеткішке ықпал етеді. Сол сияқты 53 сотталған тұлғаны 302 тіркелген оқиғаға бөліп, алынған нәтижені ашылу немесе соттау коэффициенті деп көрсету әдіснамалық тұрғыдан негізсіз. Нақты процестік кедергілерді анықтау үшін тіркеуден түпкілікті шешімге дейін байланыстырылған істер деректері қажет.



1-сурет – ҚК-нің 147-бабының 3–5-бөліктері бойынша тіркелген құқық бұзушылықтардың динамикасы

Көрсетілген деректер массивінде оқиға болған күн мен оны тіркеу күні

арасындағы уақыт аралығы цифрлық іздердің сақталуына ықпал етуі мүмкін тәуекел факторларын бағалауға мүмкіндік береді. Көрсетілген мерзім құқық қорғау органының әрекет ету уақытын емес, құқық бұзушылық оқиғасының орын алған сәті мен оның ресми тіркелуі арасындағы уақыт алшақтығын сипаттайды. Сондықтан аталған уақыт аралығын түсіндіру кезінде жәбірленушінің құқық бұзушылық туралы кеш хабарлауы, құқық бұзушылық фактісінің кейінірек анықталуы және тіркеуге дейінгі өзге мән-жайлар ескерілуі тиіс. Осы факторлар ажыратылмаған жағдайда әртүрлі себептерден туындаған уақыт аралығы бір көрсеткішке біріктіріліп, тергеу органының әрекетіне қатысты негізсіз қорытынды жасау қаупі туындайды.

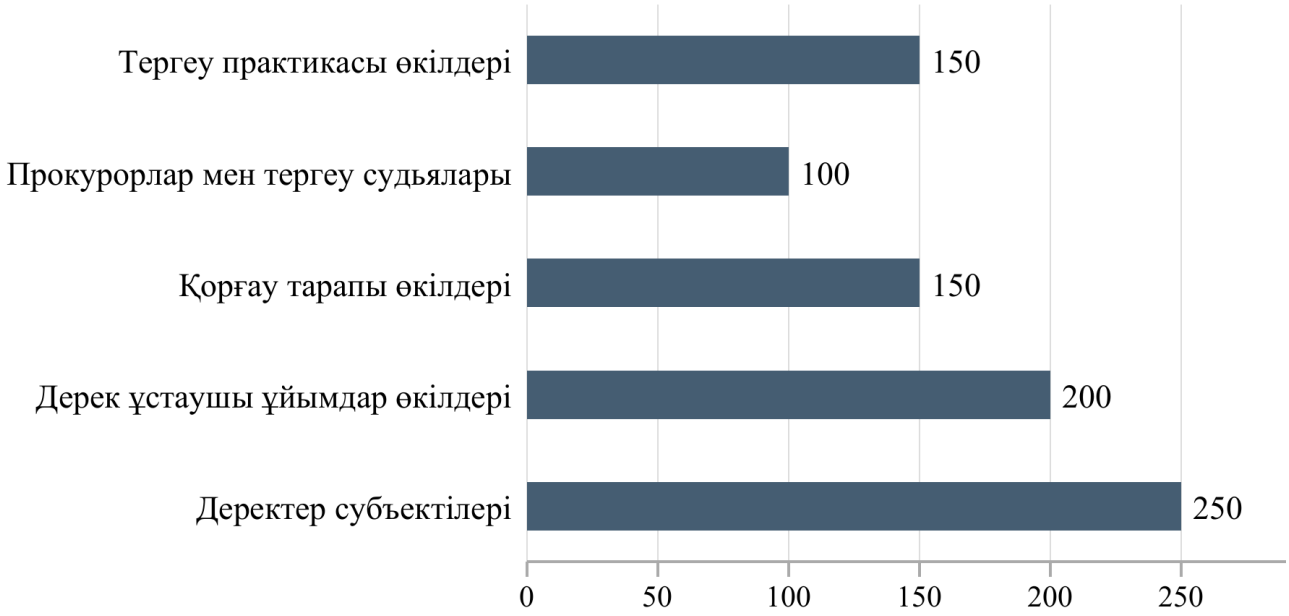


2-сурет – Оқиға мен тіркеу арасындағы уақыт аралығының құрылымы

Оқиғадан кейін 91 күннен астам уақыт өткен соң тіркелген 66 жазбаның болуы цифрлық іздердің сақталуына қатысты тәуекелдің бар екенін көрсететін индикатор ретінде бағаланады. Бұл көрсеткіш аталған барлық жағдайларда бастапқы лог-журналдар немесе өзге цифрлық мәліметтер жойылғанын білдірмейді. Оның мәні – тергеп-тексеру басталған сәтте жекелеген ақпараттық жүйелердегі қысқа мерзім сақталатын жазбалардың қолжетімді болмау ықтималдығына назар аудартуда. Осыған байланысты арыз немесе хабар тіркелген бастапқы кезеңде ықтимал дерек ұстаушыларды, олардағы деректерді сақтау мерзімдерін, резервтік көшірмелердің бар-жоғын және архивтік сақтау мүмкіндігін мүмкіндігінше ерте анықтау ұсынылады. Цифрлық мәліметтердің жоғалу тәуекелі әрбір нақты ақпараттық жүйенің техникалық конфигурациясы, сақтау саясаты және оператор ұсынған мәліметтер негізінде жеке бағалануы тиіс, барлық провайдерлерге бірыңғай шартты сақтау мерзімін қолдану ғылыми және практикалық тұрғыдан негізсіз.

Алматы қаласында жүргізілген 850 респондентті қамтыған сауалнама бес нысаналы топтан тұрды: тергеу практикасының өкілдері – 150 адам, прокурорлар мен тергеу судьялары – 100, қорғау тарапы – 150, дерек ұстаушы ұйымдардың өкілдері – 200 және деректер субъектілері – 250 адам.

Мұндай құрылым зерттелетін проблеманы әртүрлі процестік және институционалдық позициялар тұрғысынан бағалауға мүмкіндік берді. Сауалнама нәтижесінде респонденттердің 71,0%-ы цифрлық ортадағы дәлелдемелерді бекіту тәртібін нақтылау қажеттігін көрсетті. Деректер субъектілері тобында 70,8% дербес деректердің қайта таралу қаупіне алаңдаушылық білдірсе, 62,0% құқық қорғау органдарына жүгінбегенін көрсеткен. Бұл нәтижелер цифрлық мәліметтермен жұмыс істеуді стандарттауға сұраныс бар екенін және дербес деректердің құпиялылығына қатысты алаңдаушылықтың елеулі екенін көрсетеді. Сонымен бірге аталған көрсеткіштер тергеу органдары тарапынан нақты заң бұзушылықтардың жиілігін өлшемейді және мұндай қорытынды жасауға тікелей негіз бола алмайды.



3-сурет – Сауалнамаға қатысқан бес нысаналы топтың құрамы

Сауалнама нәтижелерін қолданудың шегі оның аумақтық және іріктеу сипатынан туындайды. Бес топтың жауаптарын біртекті кәсіби пікір ретінде біріктіруге, топтық пайыздың бөлімін 850 адам деп автоматты қабылдауға немесе бастапқы жауаптарсыз жаңа қиылыстық кестелер жасауға болмайды. Осы тарауда сауалнама ұйымдық ұсыныстардың қажеттігін түсіндіретін қосымша материал ретінде пайдаланылады, ал нақты құқықтық қорытынды норманы талдауға және дәлелденген процестік жағдайға сүйенеді. Сауалнамадағы алаңдаушылық пен статистикадағы тіркеу аралығы арасындағы себептік байланысты анықтау дербес эмпирикалық тексеруді талап етеді.

Қылмыстық процестің заңда белгіленген сатыларын криминалистикалық ұйымдастыру кезеңдерінен ажырату қажет. Сотқа дейінгі тергеп-тексеру шеңберіндегі бастапқы, негізгі және қорытынды жұмыстар ҚПК-де көзделген дербес жаңа сатылар емес. Осы зерттеуде бес ұйымдастыру кезеңі ұсынылады: хабарды қабылдау және тиісті процестік бағытты таңдау; жоғалуы ықтимал іздерді сақтау; деректерді жүйелі жинау

және нұсқаларды тексеру; зерттеу мен құқықтық бағалауды толықтыру; іс материалдарын аяқтау және прокурорлық тексеруге дайындау. Кезеңдер бірін-бірі қатаң кезекпен алмастырмайды: жаңа із табылғанда алғашқы әрекеттерге қайта оралу қажеттігі туындайды.

Бірінші кезеңде арыздың мазмұны, ықтимал құрам, қудалау тәртібі, тергеулік және шұғыл әрекеттің негізі айқындалады. ҚПК-нің 32-бабы ҚК-нің 147-бабының 1 және 2-бөліктеріне қатысты жекеше айыптау тәртібін көздейтіндіктен, барлық өтінішті бірдей жариялы қудалау моделімен жүргізу дұрыс емес; заңдағы ерекшеліктер мен прокурордың өкілеттігі жеке тексеріледі. ҚПК-нің 179–181, 187 және 191-баптары, сондай-ақ арыздарды қабылдау мен тіркеу қағидалары бастапқы шешімнің құқықтық негізін құрайды [6; 52]. Тергеулік жөніндегі мәселені шешу іздерді сақтаудың заңды шұғыл шараларын кейінге қалдыруға негіз болмауы тиіс.

Екінші кезеңдегі басты проблема – дәлелдеменің жоғалу жылдамдығы мен процестік шешім қабылдау уақытының сәйкес келмеуі. NIJ-дің алғашқы әрекеттер жөніндегі нұсқаулығы құрылғының күйін сақтауға және табылған объектілерді дұрыс құжаттауға мән береді, ал RFC 3227 өзгергіштігі жоғары деректерді жинау кезегін ескеруді ұсынады [53; 54]. Ұлттық рәсімге бейімделген шешім құрылғының қосылған-қосылмағанын, шифрланғанын, желіге қосылуын және қашықтан жойылу қаупін маманмен бірге бағалаудан басталады. Құрылғыны барлық жағдайда дереу өшіру немесе желіден ажырату жөніндегі әмбебап нұсқау дұрыс емес: бір жағдайда ол деректі сақтаса, басқа жағдайда жедел жадтағы мәліметті жоғалтады.

Алғашқы 24–72 сағатқа арналған вариативтік алгоритмді заңда белгіленген процестік мерзім ретінде емес, сотқа дейінгі тергеп-тексерудің бастапқы кезеңіндегі жұмысты ұйымдастыруға арналған әдістемелік бағдар ретінде пайдалану ұсынылады. Алғашқы кезеңде хабардың мазмұны, жарияланымның немесе цифрлық объектінің сол сәттегі қолжетімді күйі тіркеліп, ықтимал дерек ұстаушылар айқындалады және қысқа мерзімде өзгеруі немесе жойылуы мүмкін цифрлық мәліметтерді заңды түрде сақтап қалу мүмкіндігі бағаланады. Бұдан кейін нақты істің мән-жайларына қарай қажетті процестік негіздер айқындалып, тиісті санкцияны алу, мәліметтерді сұрату, қарап-тексеру, ал заңда көзделген негіздер болған жағдайда тінту немесе алу жүргізу мәселесі шешіледі. Алынған цифрлық материалдар бойынша олардың толықтығы, уақыт белгілері, дереккөзі, тұтастығы және бастапқы нұсқалармен сәйкестігі тексерілуі тиіс. Цифрлық мәліметтердің жоғалу немесе өзгеру қаупі нақты анықталған жағдайда қажетті әрекеттер шартты сағаттық кезеңдердің аяқталуын күтпей жүргізіледі. Бұл ретте ұсынылып отырған ұйымдастырушылық алгоритм ҚПК-де көзделген санкциялау, хабарлау және өзге де міндетті процестік мерзімдер мен рәсімдерді алмастырмайды.

Үшінші кезеңде тергеу әртүрлі дереккөздерден алынған мәліметтерді біртұтас оқиғалық және уақыттық тізбекке келтіруге бағытталады. Бұл кезеңде дерек ұстаушыларға бірін-бірі қайталайтын немесе шамадан тыс кең сұратулар жіберу, әртүрлі ақпараттық жүйелердегі уақыт форматтарының

сәйкес келмеуі, ұйымның ішкі есептік құжатын бастапқы жүйелік журналмен теңестіру, сондай-ақ негізгі нұсқамен үйлеспейтін немесе тұлғаны ақтауы мүмкін мәліметтерді елемеу тәуекелдері туындайды. NIST SP 800-86 цифрлық криминалистикалық жұмысты деректерді жинау, зерттеу, талдау және нәтижелерді есеп түрінде рәсімдеу кезеңдерінің өзара сабақтастығы ретінде қарастырады [55, 3.1–3.4 бөлімдер]. ISO/IEC 27043 цифрлық оқиғаларды тергеп-тексеруді оқиғаға дейінгі дайындықтан бастап деректерді алу, зерттеу, талдау және тергеуден кейінгі рәсімдерге дейін қамтитын жүйелі процесс ретінде белгілейді [56]. Аталған құжаттар Қазақстан Республикасының қылмыстық процесі үшін міндетті процестік құқықтың қайнар көзі болып табылмайды. Олардың әдістемелік құндылығы цифрлық мәліметтермен жасалған әрбір әрекеттің алдыңғы және кейінгі кезеңдермен байланысын сақтауға, орындалған операцияларды құжаттауға және алынған нәтижелерді кейіннен қайта тексеруге мүмкіндік беретін жүйелі тәсіл ұсынуында. Осы тұрғыдан халықаралық техникалық стандарттар ұлттық қылмыстық-процестік нормаларды алмастырмайды, бірақ цифрлық мәліметтерді жинау, зерттеу және талдау рәсімдерін ұйымдастырудың қосымша әдістемелік бағдары ретінде пайдаланылуы мүмкін.

4-кесте – Сотқа дейінгі тергеп-тексеруді ұйымдастырудың бес кезеңдік авторлық моделі

№	Ұйымдастыру кезеңі	Негізгі проблема	Процестік және техникалық әрекет	Кезең нәтижесінің өлшемі
1	Бастапқы бағалау	Деректердің таралуын құрам белгілерімен шатастыру	Арызды тіркеу; қудалау тәртібін, тергеулікті және саралау нұсқаларын анықтау	Қандай мән-жайлар тексерілетіні және органның құзыреті айқындалған
2	Өзгергіш іздерді сақтау	Логтың жойылуы; құрылғы күйінің өзгеруі; санкцияны күту	Сақтау қажеттігін бағалау; заңды негізбен бастапқы күйді бекіту; маманды қатыстыру	Із сақталған немесе алынбау себебі, тәуекелі мен келесі әрекет тіркелген
3	Негізгі жинау және тексеру	Толық емес экспорт; дерек ұстаушының формалды жауабы	Нысаналы сұрату; тиісті тергеу әрекеті; логтар мен бастапқы файлдарды салыстыру	Деректің шығу тегі және айыптайтын әрі ақтайтын нұсқалар тексерілген
4	Арнайы зерттеу	Аккаунтты тұлғамен теңестіру; құрал қатесін елемеу	Маман көмегі немесе сараптама; әдіс шегін және балама түсіндірмелерді бағалау	Техникалық тұжырымның негізі, шегі және заңдық сұрақпен байланысы ашылған
5	Аяқтау және бақылау	Тексерілмеген қарсылық; қорғауға маңызды деректің жабық қалуы	Іс материалдарымен танысу; өтінішхаттарды шешу; уәжді қорытынды және прокурорлық тексеру	Негізгі тұжырымдар дәлелдемелермен байланыстырылған; құқықтар қамтамасыз етілген

Төртінші кезеңде тергеуші техникалық қорытынды мен заңдық қорытындының арақатынасын тексереді. Сарапшы белгілі бір уақытта файл экспортталғанын анықтауы мүмкін, бірақ экспорттың заңсыздығы

келісіммен, міндетпен және ҚК диспозициясымен салыстырылады. Қорғану тарапы ұсынған балама нұсқа зерттеу объектісін толықтыруды немесе қосымша сұрақ қоюды қажет етсе, оған уәжді жауап беріледі. Бесінші кезеңде әрбір маңызды тұжырымның нақты дәлелдемелік тірегі, бастапқы материалға қолжетімділік, өтінішхаттарды шешу және құпия деректермен жұмыс істеу тәртібі тексеріледі. ҚПК-нің 302-бабы осы аяқтау шеңберіндегі прокурор шешімдеріне қатысты; компьютерлер мен серверлерден ақпаратты жасырын түсіріп алу мәселесі ҚПК-нің 245-бабымен байланысты қарастырылады [6].

Аяқтау тәртібін сипаттағанда ҚПК редакциясының уақыт бойынша қолданылуын ескеру қажет. 302-бапқа қатысты өтпелі ережелер сотқа дейінгі тергеп-тексерудің аяқталғаны туралы есеп пен прокурор жасайтын айыптау актісінің моделін істер санатына қарай кезең-кезеңімен енгізеді. Сондықтан 2026 жылғы редакцияда көрінетін ережені барлық істерге дереу қолданылатын бірыңғай рәсім деп түсіндіру дұрыс емес. Тергеу органы нақты іс үшін қолданыстағы нұсқаны, қылмыстың санатын және енгізілу мерзімін тексеруі тиіс. 2021–2025 жылдар практикасы кейін қабылданған нормамен кері бағаланбайды; техникалық ұсыныстар да сол кезеңдегі заңдылықты автоматты түрде теріске шығармайды [6].

Тергеуді ұйымдастыру киберқауіпсіздік оқиғасына ден қою шараларымен үйлестірілуі тиіс. Ұйым қауіпсіздік инцидентін тоқтату немесе оның салдарын шектеу мақсатында аккаунтты бұғаттауы, парольді өзгертуі, жүйені қайта конфигурациялауы немесе серверді қалпына келтіруі мүмкін. Алайда мұндай әрекеттер іс үшін маңызы болуы ықтимал цифрлық іздердің күйіне әсер етуі мүмкін. NIST SP 800-61 Rev. 3 киберқауіпсіздік инциденттеріне ден қоюды ұйымның жалпы киберқауіпсіздік тәуекелдерін басқару қызметімен ықпалдастыру қажеттігін көрсетеді [57]. Ал NIST Cybersecurity Framework 2.0 киберқауіпсіздік тәуекелдерін басқаруды алты өзара байланысты функция арқылы жүйелейді: басқару, айқындау, қорғау, анықтау, ден қою және қалпына келтіру [58]. Осы тәсілді қылмыстық-процестік тұрғыдан бейімдеу кезінде қауіпсіздікті қалпына келтіруге бағытталған әрбір техникалық әрекеттің уақыты, оны орындаған тұлға, қолданылған құрал және цифрлық мәліметтерге ықтимал әсері бөлек тіркелуі тиіс. Киберқауіпсіздік маманының есебі іс үшін маңызды ақпарат көзі болуы мүмкін, алайда ол заңда көзделген процестік хаттаманы, маманның қатысуын немесе сарапшы қорытындысын өздігінен алмастырмайды.

Желілік атрибуцияны ұйымдастыру кезінде IP-мекенжаймен қатар уақыт белгісі мен бастапқы порт нөмірінің маңызы ескерілуі қажет. RFC 6302 интернетке бағытталған серверлерге кіріс қосылымдар бойынша IP-мекенжаймен бірге бастапқы порт нөмірін және UTC бойынша секунд дәлдігіне дейінгі уақыт белгісін тіркеуді ұсынады [59]. Бұл талап әсіресе бір сыртқы IP-мекенжай бірнеше пайдаланушы арасында ортақ пайдаланылатын жағдайларда маңызды. Breyer v. Bundesrepublik Deutschland ісінде Еуропалық Одақ Соты динамикалық IP-мекенжай сайт операторының қолында болған қосымша құқықтық құралдар арқылы нақты тұлғаны сәйкестендіруге

мүмкіндік беретін жағдайда дербес дерек ретінде қарастырылуы мүмкін екенін көрсетті [60]. Аталған құқықтық ұстаным Қазақстан Республикасының тергеу органдарына тікелей қылмыстық-процестік өкілеттіктер бермегенімен, IP-мекенжайға қатысты мәліметтерді алу кезінде жеке өмірге қол сұғылмаушылық құқығы мен дербес деректерді қорғау кепілдіктерін сақтаудың маңыздылығын айқындайды. Сонымен қатар IP-мекенжайдың белгілі бір абонентпен байланысының анықталуы қылмыстық құқық бұзушылыққа қатысты нақты әрекеттердің сол тұлға тарапынан жасалғанын өздігінен растамайтындықтан, мұндай мәліметтер өзге де дәлелдемелермен жиынтықта бағалануы тиіс.

Уақыттық реконструкция кезінде файлдық жүйе метадеректерінің дәлелдемелік мүмкіндіктері мен шектеулері ескерілуі тиіс. Ф. Бухгольц пен Ю. Спаффорд файлдық жүйе метадеректері «кім, не, қайда, қашан, қалай және не үшін» деген тергеу сұрақтарының барлығына бірдей жауап бере алмайтынын, ал қолданыстағы жүйелердегі уақыт белгілері нақты оқиғаның толық контекстін әрдайым көрсетпейтінін атап өтеді [61, 298–309-б.]. RFC 3339 күн мен уақытты UTC-мен арақатынасы нақты көрсетілген бірізді форматта белгілеуге мүмкіндік береді және UTC қолданудың үйлесімділік үшін артықшылығын атап көрсетеді [62, 4.1, 4.2, 5.6-бөлімдер]. Осыған байланысты бастапқы уақыт белгісі өзгеріссіз сақталуға, ал салыстырмалы талдау үшін UTC-ге немесе өзге бірыңғай уақыт шкаласына түрлендірілген мән бөлек көрсетілуі тиіс. Сағат ауытқуы, уақыт белдеуі және қолданылған түрлендіру тәсілі міндетті түрде түсіндірілуі қажет. Тергеушіге ыңғайлы етіп құрылған уақыт шкаласы бастапқы деректің өзін алмастырмауы тиіс.

Дербес деректерге қатысты қылмыстық істер бойынша дәлелдеу пәні деректердің санатын, әрекеттің заңсыздық негізін, нақты операцияны, әрекетті белгілі бір тұлғамен байланыстыруды, кінә мен арнайы міндеттің болуын, сондай-ақ нақты құрам талап еткен жағдайда зиян мен себептік байланысты анықтауды қамтиды. Бұл элементтердің әрқайсысы айыптайтын ғана емес, ақтайтын және баламалы нұсқалар тұрғысынан да тексерілуі қажет. Цифрлық іздер осы міндеттерді шешуге мүмкіндік беретін бастапқы ақпараттық негіз болып табылады, ал олардың қылмыстық-процестік дәлелдемелік маңызы заңда белгіленген тәртіппен алынғаннан, бекітілгеннен, тексерілгеннен және бағаланғаннан кейін ғана қалыптасады.

Ұсынылған бес кезеңдік модельдің ерекшелігі әрбір ұйымдастыру кезеңін нақты процестік проблемамен және келесі кезеңге өту шарттарымен байланыстыруында. Бастапқы кезеңде қылмыстық қудалау тәртібі мен тергеулік мәселелері, цифрлық іздерді сақтау кезеңінде олардың өзгергіштігі мен тиісті санкциялау рәсімдері, негізгі тергеу барысында алынған мәліметтердің толықтығы мен баламалы нұсқаларды тексеру, зерттеу кезеңінде арнайы білімді пайдаланудың шектері, ал аяқтау кезеңінде тараптардың процестік құқықтары мен прокурорлық бағалау шешуші мәнге ие болады. Алғашқы 24–72 сағатқа арналған алгоритм осы модель шеңберіндегі икемді ұйымдастырушылық бағдар ретінде ұсынылады.

Эмпирикалық материалдар цифрлық мәліметтерді уақтылы сақтау мен

оларды бірізді процестік тәртіппен бекітудің практикалық маңызын көрсетеді. Сонымен бірге 302 тіркелген қылмыстық құқық бұзушылық, сот статистикасындағы тұлғалар туралы мәліметтер және 850 респонденттің сауалнама нәтижелері мазмұны мен есептік бірлігі әртүрлі деректер жиынтықтары ретінде бөлек талдануы тиіс. Осындай әдіснамалық шектеулер сақталған жағдайда статистикалық және сауалнамалық деректер заңдық қорытындының орнына жүрмей, тергеп-тексеру рәсімдерін жетілдіру қажеттігін негіздейтін эмпирикалық материал ретінде пайдаланылуы мүмкін.

2.2 Дербес деректерге қатысты дәлелдемелерді жинау және бекітудің процестік тәртібі

Дербес деректерге қатысты дәлелдемелерді жинаудың негізгі проблемасы ақпаратқа техникалық қолжетімділік пен оны қылмыстық іс бойынша пайдалануға құқықтық өкілеттіктің сәйкес келе бермеуінен туындайды. Тергеуші файлды қарай алуы мүмкін, бірақ оны қарауға негіз болмауы ықтимал; керісінше, заңды сұратуға алынған жауап бастапқы жазбаны тексеруге жеткіліксіз болуы мүмкін. Сондықтан осы бөлімде жинау және бекіту құқықтық негізді таңдау, ақпаратты алу, процестік көзді қалыптастыру және кейінгі тексеру мүмкіндігін сақтау байланысында қарастырылады. Бірінші тараудағы деректердің қосарлы құқықтық сипаты осы жерде нақты талапқа айналады: ақпарат дәлелдеу үшін алынады және сол мезеттен бастап қайта таралудан қорғалуы тиіс [2; 6].

ҚПК-нің 111-бабы нақты деректер белгіленетін процестік көздерді айқындайды. Цифрлық ортада қалыптасқан мәлімет заттай дәлелдеменің құрамында, процестік әрекет хаттамасында, өзге құжатта, маманның не сарапшының қорытындысында көрініс табуы мүмкін. Ақпараттың цифрлық нысаны оның дәлелдемелер жүйесіндегі орнын жалғыз өзі шешпейді. Құрылғы құқық бұзушылықтың құралы не із сақтаушысы ретінде маңызды болса, оны заттай дәлелдеме ретінде тану мәселесі қаралады; ұйым жасаған жүйелік есеп мазмұнына және алыну тәсіліне қарай құжат ретінде бағалануы мүмкін. Бір деректі бірнеше нысанда көрсету жаңа тәуелсіз дәлелдемелерді автоматты түрде көбейтпейді [6].

NIJ-дің цифрлық дәлелдемелерді зерттеу жөніндегі нұсқаулығы цифрлық зерттеу процесін объектіні бағалау, дәлелдемені алу, зерттеу, сондай-ақ орындалған әрекеттер мен алынған нәтижелерді құжаттау және есеп түрінде рәсімдеу кезеңдерінің өзара сабақтастығы ретінде қарастырады. Нұсқаулық цифрлық дәлелдемелерді алу, зерттеу, сақтау және беру барысында жасалған әрекеттердің құжатталуын, сақталуын және кейіннен тексеруге қолжетімді болуын талап ететін жалпы криминалистикалық қағидаттарға ерекше мән береді [63]. ISO/IEC 27037:2012 ықтимал цифрлық дәлелдемелермен жұмыс істеу барысында оларды анықтау (identification), жинау (collection), көшіру арқылы алу (acquisition) және сақтау (preservation) әрекеттерін бір-бірінен ажыратады [64]. Аталған жіктеу Қазақстан Республикасының ҚПК-де көзделген процестік әрекеттер жүйесін

өзгертпейді және дербес процестік өкілеттік қалыптастырмайды; оның әдістемелік маңызы нақты процестік әрекеттің шеңберінде қандай техникалық операцияның орындалғанын, оның реттілігі мен мақсатын түсіндіруге мүмкіндік беруінде. Осыған байланысты Қазақстан жағдайында цифрлық мәліметтермен жасалатын әрбір техникалық операция ҚПК-де көзделген тиісті процестік нысан шеңберінде жүзеге асырылып, оның құқықтық негізі, орындалу тәсілі, қатысушылар, қолданылған техникалық құралдар және алынған нәтиже тиісті түрде бекітілуі тиіс.

Құрылғыны қарап-тексеру мен мәліметті ұйымнан сұратудың арақатынасы объектінің орналасуына ғана тәуелді емес. Тергеушіге нақты белгілі құжатты заңды тәртіппен ұсыну мүмкіндігі бар болса, сұрату тиімді болуы мүмкін. Мәліметтің жасырылғаны, жойылуы немесе ерікті берілмеуі туралы жеткілікті негіз болғанда тиісті мәжбүрлі әрекеттің шарттары тексеріледі. Жай сұрату хатымен тінтуге тән белгісіз кеңістікті шексіз зерттеу өкілеттігін қалыптастыруға болмайды. Ал дерек ұстаушының ерікті жауабы заңмен қорғалатын құпияға қатысты арнайы тәртіпті айналып өтудің құралы ретінде қабылданбауы тиіс [6].

Алудың алдында мобильді құрылғының бастапқы күйі мүмкіндігінше толық белгіленуі қажет: оның атауы, моделі, сериялық немесе өзге идентификаторы, сыртқы күйі, қосулы не өшірулі болуы, уақыт көрсеткіші және желілік байланысының жай-күйі тіркеледі. Құрылғы белсенді күйде болған жағдайда экранда ашық тұрған ақпарат, іске қосылған қосымшалар, қуат көзіне қосылуы, желілік қосылымдары және деректерді қорғау немесе шифрлау ерекшеліктері кейінгі алу тәсілін таңдауға ықпал етуі мүмкін. NIST SP 800-101 Rev. 1 мобильді құрылғылармен жұмыс істеуді дәлелдемені сақтау, құрылғы мен оқиға орнын құжаттау, деректерді алу, зерттеу мен талдау және нәтижелерді есеп түрінде рәсімдеу кезеңдерінің сабақтастығы ретінде қарастырады [65, Б. 27–29, 40–42; 48 б., 55 б.]. Нұсқаулықта құрылғының күйі деректерді алу тәсіліне тікелей әсер етуі мүмкін екені көрсетіледі. Мәселен, құрылғы белсенді күйде болған кезде ішкі жадты алынбалы тасымалдағыштан бұрын алу орынды болуы мүмкін, ал құрылғы өшірулі болса әрекеттердің реттілігі өзгеше болуы ықтимал; сонымен қатар алу барысында жасалған кейбір әрекеттер құрылғыдағы уақыт көрсеткіштеріне немесе өзге деректерге өзгеріс енгізуі мүмкін [65, Б. 41–42]. Осыдан мобильді құрылғылардың барлығына бірдей техникалық тәсілді механикалық түрде қолдануға болмайтыны туындайды. Нақты алу әдісін таңдау құрылғының күйіне, техникалық сипаттамаларына, шифрлау ерекшеліктеріне және қолжетімді криминалистикалық құралдарға байланысты негізделуі тиіс. Маман қолданылған тәсілді, оны таңдаудың себептерін, жүргізілген операцияларды, олардың құрылғыдағы мәліметтерге ықтимал әсерін және таңдалған әдіспен алынбай қалуы мүмкін деректер санаттарын хаттамада немесе оған қоса берілетін техникалық материалдарда көрсетуі қажет.

SWGDE компьютерлік деректерді алу жөніндегі ұсынымдарында бастапқы деректерге ықпал етуді барынша азайту және орындалған

техникалық әрекеттерді толық құжаттау қағидатына ерекше мән береді [66]. Бұл талап қылмыстық-процестік тұрғыдан тергеу әрекетінің барысы мен нәтижесін кейіннен қалпына келтіруге мүмкіндік беретін жеткілікті сипаттамамен қамтамасыз етілуі тиіс. Осыған байланысты қолданылған бағдарламалық құрал мен оның нұсқасы, деректерді алу тәсілі, зерттелген бөлімдер мен көлем, сәтсіз аяқталған әрекеттер, оқылмаған секторлар, құрал тіркеген қателер және өзге де техникалық шектеулер хаттамада немесе оған қоса берілетін техникалық материалдарда көрсетілуі керек. Егер техникалық есеп деректердің белгілі бір бөлігі алынбағанын, оқылмағанын немесе алу барысында шектеулер болғанын көрсетсе, «ақпарат толық көшірілді» деген жалпылама тұжырымды қолдану дұрыс емес. Мұндай жағдайда нақты қандай мәліметтердің алынғаны, қандай бөлігінің қолжетімсіз қалғаны және бұл шектеудің зерттеу нәтижелеріне ықтимал әсері ашық көрсетілуі керек. Техникалық шектеулерді жасырудан гөрі олардың дәлелдемелік мәнге ықпалын түсіндіру цифрлық мәліметтердің кейіннен тексерілуі мен бағалануын қамтамасыз етеді.

Жұмыс істеп тұрған ақпараттық жүйеден немесе құрылғыдан цифрлық мәліметтерді алу бастапқы ортаға белгілі бір өзгерістер енгізуі мүмкін. SWGDE цифрлық дәлелдемелерді жинау жөніндегі ұсынымдарында жұмыс істеп тұрған жүйеден деректерді алу кезінде жүйенің күйіне ықпал ету қаупін ескеріп, қажетті ақпаратты сақтап қалуға мүмкіндік беретін және бастапқы деректерге әсерді барынша азайтатын тәсілді таңдауға мән береді [67, 5 б.]. Сонымен қатар жүргізілген әрекеттердің реттілігі, қолданылған құралдар және олардың нәтижелері құжатталуы керек [67, 6 б.]. Қылмыстық-процестік тұрғыдан бастапқы ортадағы кез келген өзгерісті өздігінен жол берілмейтін араласу ретінде бағалауға болмайды. Мұндай жағдайда өзгерістің қажеттілігі, көлемі, оның қандай техникалық әрекет нәтижесінде туындағаны және цифрлық мәліметтердің мазмұнына ықтимал әсері анықталуы тиіс. Мысалы, жедел жадтағы жоғалып кетуі мүмкін ақпаратты сақтау мақсатында орындалған техникалық операция жүйеде жаңа жазбалардың пайда болуына немесе жекелеген уақыт белгілерінің өзгеруіне әкелуі ықтимал. Сондықтан зерттеу барысында мұндай өзгерістер құқық бұзушылық оқиғасы кезінде қалыптасқан бастапқы цифрлық іздерден ажыратылып, маманның немесе зерттеушінің кейінгі әрекеттері оқиғаның бастапқы реконструкциясына қате енгізілмеуі керек. Бастапқы күйді өзгеріссіз сақтау техникалық тұрғыдан мүмкін болмаған жағдайда оның себептері, орындалған әрекеттер және туындаған өзгерістер хаттамада немесе оған қоса берілетін техникалық материалдарда нақты көрсетілуі қажет.

Жәбірленуші ұсынған хат-хабар немесе скриншот та бастапқы ақпарат көзі ретінде қаралады. Оны ұсынған адамның мәліметті қайдан алғаны, қандай әрекет жасағаны және бастапқы құрылғы не аккаунттың сақталғаны анықталады. Хабарлама мазмұнын көрсетуге келісім басқа қатысушының барлық хат-хабарын толық зерттеуге автоматты құқық бермейді. Құрылғыны ерікті ұсыну, жекелеген файлды беру және кең көлемді іздеуге келісімнің шектері ажыратылады. Тергеуші ұсынылған материалды заңды рәсіммен

бекітіп, оның тұтастығын және контекстін тексереді; жәбірленушінің дереккөзіне сенім тексеру қажеттігін жоймайды [6].

Дерек ұстаушы ұғымы осы зерттеуде қылмыстық іс үшін маңызы болуы ықтимал мәліметті заңды негізде иеленетін, сақтайтын не оны ұсынуға өкілетті ұйымды немесе тұлғаны белгілеу үшін қолданылады. Бұл ұғым дербес деректердің меншік иесі, оператор, үшінші тұлға, байланыс операторы немесе бұлттық қызмет көрсетуші сияқты заңда белгіленген мәртебелерді бір құқықтық санатқа біріктірмейді. Ол дәлелдемелік ақпараттың нақты қай субъектінің бақылауында екенін және оны кімнің заңды әрі техникалық тұрғыдан ұсына алатынын айқындауға арналған жұмыс ұғымы болып табылады. ISO/IEC 27050-1:2019 электрондық түрде сақталатын ақпаратпен жұмыс істеуді оны анықтау, сақтау, жинау, өңдеу, шолу, талдау және ұсыну сияқты өзара байланысты кезеңдер арқылы қарастырады [69]. Стандарттың әдістемелік маңызы ұйымнан алынған жай ақпараттық жауап пен электрондық түрде сақталған мәліметтердің шығу тегін, сақталу жағдайын, алыну тәсілін және кейінгі өңдеу тарихын түсіндіруге мүмкіндік беретін толық ақпараттық пакет арасындағы айырмашылықты айқындауға көмектесуінде. Осыған байланысты сұрату жіберілетін субъект тек белгілі бір мәліметтің бар-жоғын хабарлаумен шектелмей, мүмкін болған жағдайда оның қандай ақпараттық жүйеде қалыптасқанын, қандай мерзім мен көлемде сақталатынын, қандай техникалық тәсілмен алынғанын немесе экспортталғанын және ұсынылған файлдар мен жазбалардың қандай бастапқы дереккөзге негізделетінін түсіндіре алуы тиіс.

ҚПК-нің 122-бабы бойынша мәлімет талап ету құқығы салалық құпия режимдерінен бөлек қолданылмайды. Банк құпиясы, микроқаржы және коллекторлық қызмет жөніндегі мәліметтер мен заңда арнайы аталған өзге санаттарға қатысты прокурор санкциясының талаптары нақты тексеріледі. Бұл норманы кез келген дербес дерек немесе кез келген коммерциялық ақпарат прокурор санкциясымен сұратылады деп жалпылауға болмайды. Байланыс құпиясына қол сұғатын жасырын әрекетке тиісті соттық санкция тәртібі қолданылады. Демек, деректердің «құпия» деп аталуы жеткіліксіз: нақты құқықтық режим, операцияның мазмұны және қолданылатын ҚПК нормасы сәйкестендіріледі [6].

Кіріспеде ұсынылған құпияландырылған сұрату тетігін екі деңгейлі құжат ретінде дамыту орынды. Ішкі негіздемеде қылмыстық-құқықтық саралау, дәлелденетін мән-жай, сұрату қажеттілігі, деректер көлемі және санкциялау негізі толық көрсетіледі. Сыртқы орындау құжатында адресатқа тапсырманы заңды әрі дәл орындауға жеткілікті реквизиттер, объектілер, уақыт аралығы, формат және беру арнасы сақталады. Құпиялылық үшін артық фабуланы шектеу ұсынылады, бірақ заң талап ететін реквизитті алып тастауға немесе адресаттың өкілеттікті тексеру мүмкіндігін жоюға болмайды. Қажетті реквизиттерді өзгерту заңнамалық не ведомстволық реттеуді талап ететін бөлігінде бұл модель жетілдіру ұсынысы ретінде қарастырылады.

Осы екі деңгейлі құжатты сақтауға бағытталған жедел өтініш пен

кейінгі мәлімет алудың екі кезеңімен шатастырмау қажет. Біріншісі ақпаратты кімге және қандай көлемде ашу мәселесін шешеді. Екіншісі деректі жоғалтпай ұстап тұру және оған қол жеткізу мәселелерін ажыратады. Сақтау туралы өтініш жаңа жаппай жинауды бастауды немесе деректерді бірден тергеушіге беруді білдірмеуі тиіс. Қазақстанда барлық дерек ұстаушыға міндетті болатын әмбебап жедел сақтау өкілеттігі бар деп тұжырымдауға болмайды: міндеттеу негізі әр жағдайда тексеріледі, ал арнайы тетік жетіспеген бөлігі үшін заңнаманы толықтыру ұсынылады.

Сыртқы сұратудың техникалық анықтығы деректер көлемін азайтудың да құралы болып табылады. «Тұлға туралы барлық ақпаратты беріңіз» деген талаптың орнына нақты аккаунт не объект идентификаторы, тексерілетін операция, басталу және аяқталу уақыты, уақыт белдеуі, қажетті өрістер мен формат көрсетіледі. Аккаунт атауы өзгеруі мүмкін болғандықтан, тұрақты ішкі идентификатордың бар-жоғы сұралады. Провайдерде дерек болмаса, оның ешқашан тіркелмегені, сақтау мерзімі біткені, сұрату параметрі сәйкес келмегені немесе техникалық себеппен алынбағаны ажыратылады. Осындай теріс жауап та іздеудің шегін түсіндіретін материал ретінде бекітіледі.

Ұсынылатын ең аз дәлелдемелік пакет деректің өзін, оны сипаттайтын метадеректерді және оны алу рәсімінің сипаттамасын қамтиды. Пакеттің құрамына бастапқы жүйенің атауы, экспорт параметрлері, орындаушының мәртебесі, алынған уақыт, файл тізілімі, тұтастық көрсеткіштері және берудің есебі енгізіледі. Бұл талаптар ҚПК-дегі құжаттарға жаңа формалды жарамсыздық негізін қоспайды. Олардың мақсаты – кейін деректің қайдан шыққанын және неге толық деп есептелгенін тексеруге жағдай жасау. Арнайы құқықтық талапты бұзу мен ұсынылатын техникалық өрістің болмауы 2.3-бөлімде бөлек бағаланады.

5-кесте – Дерек ұстаушыдан алынатын ең аз дәлелдемелік пакеттің ұсынылатын құрамы

№	Блок	Бекітілетін мәлімет	Тексеру мақсаты
1	Құқықтық негіз	Сұратушы орган, іс реквизиті, алу негізі, қажет санкция, тапсырма шегі	Дерек алудың құзыреті мен заңды көлемін тексеру
2	Бастапқы жүйе	Дерек ұстаушы, қызмет түрі, жүйе және аккаунт идентификаторы	Мәліметтің қайда және кімнің бақылауында қалыптасқанын анықтау
3	Іріктеу параметрі	Уақыт аралығы, уақыт белдеуі, объектілер, сүзгі, сұралған өрістер	Сұрату мен жауап ауқымын салыстыру
4	Деректің өзі	Бастапқы форматтағы файлдар не экспорт, файлдар тізімі	Мазмұнды тәуелсіз тексеруге мүмкіндік сақтау
5	Метадерек	Жасалу/өзгеру уақыты, оқиға коды, сеанс, операция нәтижесі, өрістер түсіндірмесі	Контекстті және уақыттық байланысты қалпына келтіру
6	Алу тәсілі	Экспорт құралы мен нұсқасы, орындаушы, алынған уақыт, қателер, қамтылмаған деректер	Толықтық пен техникалық шектеулерді бағалау

№	Блок	Бекітілетін мәлімет	Тексеру мақсаты
7	Тұтастық және беру	Хэш алгоритмі мен мәні қолданылса; тасымалдағыш, арна, беру-қабылдау есебі	Көшірмелерді сәйкестендіру және қозғалысын бақылау

Ескерту: Авторлық модель. Құрамы нақты дерекке бейімделеді; ұсынылатын техникалық өрістің болмауы өздігінен автоматты жол берілмейтіндік негізін қалыптастырмайды [6; 64; 69].

Ұйымнан алынған жиынтық анықтама немесе есеп көбіне ақпараттық жүйеде қалыптасқан бастапқы жазбаларды іріктеу, сүзу және өңдеу нәтижесінде жасалады. Сондықтан мұндай құжаттағы қорытындыны бастапқы жүйелік жазбамен автоматты түрде теңестіруге болмайды. Мәселен, анықтамада «қызметкер деректі қараған» деп көрсетілсе, бұл қорытындының қандай журнал өрістеріне, оқиға кодтарына немесе өзге техникалық белгілерге негізделгені, есепті қалыптастыру кезінде қандай сүзгі қолданылғаны және тіркелген техникалық оқиғаның баламалы түсіндірмесі бар-жоғы анықталуы қажет. NIST SP 800-92 журналдарды басқаруды журналдық деректердің қалыптасуы, сақталуы, қорғалуы, талдануы және кейін жойылуы өзара байланысты процесс ретінде қарастырады [70, 2.2–2.3 бөлімдер]. Құжатта ұйымның журнал жүргізу саясаты қандай оқиғалардың тіркелетінін, журналдардың қандай мерзім сақталатынын, оларға кімнің қол жеткізетінін және оларды басқару тәртібін алдын ала айқындауы қажет екені көрсетіледі [70, 4.2-бөлім]. Сонымен қатар журналдарды сақтау мен жою тәртібі арнайы қарастырылып, олардың кейінгі тергеу және талдау үшін қолжетімділігін қамтамасыз ету қажеттігі атап өтіледі [70, 5.1.2 бөлім]. Журналдық жазбаларды дұрыс түсіндіру үшін олардың құрылымын, мазмұнын, жүйелік контекстін және талдау ерекшеліктерін ескеру қажет [70, 5.2.1–5.2.3 бөлімдер]. Осыдан дерек ұстаушыдан нақты журнал жазбаларын сұратумен қатар, зерттелетін оқиғаға қатысты көлемде журнал жүргізу саясаты, сақтау мерзімі, оқиға кезінде қолданылған баптаулар, есепті қалыптастыру тәсілі және пайдаланылған сүзгілер туралы мәліметтерді де алу қажеттігі туындайды. Мұндай қосымша ақпарат жиынтық есептің бастапқы цифрлық жазбалармен арақатынасын тексеруге, ұйым жасаған қорытындының негізділігін бағалауға және техникалық оқиғаның баламалы түсіндірмелерін жоққа шығаруға немесе растауға мүмкіндік береді. Бұл құжаттар мен мәліметтер дәлелдеу қажеттілігіне сәйкес және зерттелетін оқиғаға қатысты шекте ғана сұратылуы тиіс.

Лог-журнал деп ақпараттық жүйеде немесе бағдарламалық қосымшада болған оқиғалар туралы жүйелі түрде қалыптасатын жазбалар жиынтығын түсінуге болады. Алайда кез келген лог-журнал пайдаланушының нақты әрекетін толық әрі бірмәнді түрде бейнелей бермейді. Мәселен, аутентификацияның сәтті аяқталуы тұлғаның белгілі бір деректі нақты қарағанын автоматты түрде білдірмейді, сол сияқты жүйелік сұраудың орындалуы оның нәтижесі пайдаланушыға толық жеткізілгенін немесе пайдаланылғанын өздігінен дәлелдемейді. Сондықтан журналдық жазбалар олардың техникалық және оқиғалық контекстімен бірге бағалануы тиіс. RFC 5424 syslog хабарламасының құрылымын жүйелей отырып, хабарламаның

уақыт белгісін, хост атауын, қолданбаның атауын, процесс идентификаторын, хабарлама идентификаторын және құрылымдалған деректер өрістерін айқындайды [71, Б. 8–17]. Қылмыстық-процестік тұрғыдан жүйелік жазбаны бағалау кезінде оқиға кодының мағынасы, пайдаланушы немесе сеанс идентификаторы, операция жасалған объект, әрекеттің нәтижесі және уақыт белгісі нақты түсіндірілуі тиіс. Қысқартылған кодтар немесе техникалық идентификаторлар пайдаланылған жағдайда олардың мағынасы зерттелетін оқиға кезінде жүйеде қолданылған бағдарламалық нұсқа мен конфигурацияға сәйкес анықталуы қажет.

Логтарды іріктеу кезінде бір ғана қолданба журналына тәуелді болмау ұсынылады. Қажетті жағдайда аутентификация, деректер базасының аудиті, файл экспорты, желілік қосылу және қауіпсіздік жүйесі жазбалары салыстырылады. 2024 жылғы оқиғаларды журналдау жөніндегі бірлескен ұсыным орталықтандырылған жинауды, сапалы журналдарды және оларды рұқсатсыз өзгертуге қарсы қорғауды байланыстырады [72]. Алайда орталық жүйеге көшірілген лог бастапқы логпен толық бірдей деп болжанбайды: қалыптандыру, сүзгілеу, уақытты түрлендіру және қайталанатын жазбаларды жою орын алуы мүмкін. Сондықтан бастапқы және өңделген нұсқаның арақатынасы көрсетіледі.

Метадеректер файлдың немесе цифрлық жазбаның пайда болу, өзгеру және пайдаланылу контекстін түсіндіруге мүмкіндік беретін қосымша ақпараттық қабат болып табылады. Олардың құрамына уақыт белгілері, қолжетімділік туралы мәліметтер, файл өлшемі, пайдаланушы мен рұқсаттар туралы ақпарат және файлдың жүйедегі орналасуына қатысты өзге де техникалық деректер кіруі мүмкін [61, Б. 300–301]. Алайда метадеректердің жекелеген өрістері нақты оқиғаны немесе тұлғаның әрекетін өздігінен бірмәнді дәлелдемейді. Бухгольц пен Спаффорд әртүрлі файлдық жүйелерде уақыт белгілерінің атауы мен мағынасы ерекшеленетінін, олардың жаңартылу тәртібі жүйеге тәуелді екенін және кейбір уақыт белгілерінің пайдаланушы немесе бағдарлама әрекеттері нәтижесінде өзгертілуі мүмкін екенін көрсетеді [61, Б. 305–306]. Осыған байланысты автор атауы, геолокациялық өріс, файлдың жасалу немесе өзгеру уақыты сияқты метадеректер нақты авторды, файлдың пайда болған орнын немесе белгілі бір әрекетті жеке өздері дәлелдемейді. Мұндай мәліметтер файлдың мазмұнымен, басқа цифрлық іздермен, жүйелік журналдармен және іс бойынша өзге дәлелдемелермен салыстырылып бағалануы тиіс. Метадеректерді түсіндіру кезінде олардың қандай жүйеде және қандай техникалық жағдайда қалыптасқаны, қандай әрекеттер нәтижесінде өзгеруі мүмкін екені және нақты өрістің техникалық мағынасы анықталуы қажет [61, Б. 299–300, 305–306].

Бұлттық қызмет көрсетушіден алынған цифрлық мәліметтердің сенімділігін бағалау бірнеше деңгейдегі тәуелділікті ескеруді талап етеді. Дж. Дайкстра мен А. Шерман бұлттық ортадағы криминалистикалық зерттеу кезінде дәлелдеменің сенімділігі оны алу жүзеге асырылған инфрақұрылым қабатына байланысты екенін көрсетеді. Авторлар IaaS бұлттық ортасын алты

деңгейге бөліп, әр деңгейде қонақ операциялық жүйеге, гипервизорға, хост операциялық жүйесіне, аппараттық құралдарға және желіге қатысты әртүрлі сенім көлемі қалыптасатынын негіздейді [73, Б. S92–S93]. Провайдер деректерді өзі іздеп, жинап және құқық қорғау органына берген жағдайда тергеуші деректердің өзімен қатар провайдер қызметкерінің әрекеттеріне, қолданылған аппараттық және бағдарламалық құралдарға және бұлттық инфрақұрылымға да тәуелді болады [73, Б. S93–S94]. SWGDE бұлттық қызмет көрсетушілерден цифрлық дәлелдемелерді алу жөніндегі ұсынымында платформалар мен провайдерлер санының көптігіне байланысты барлық жағдайға бірдей қолданылатын бірыңғай нақты техникалық рәсім белгілеу мүмкін еместігін атап көрсетеді [74, 2 б.]. Құжат бұлттық деректерді провайдерден тікелей алу, заңды дерек ұстаушының экспорттық құралдарын пайдалану, клиенттік қосымша немесе API арқылы алу сияқты әртүрлі тәсілдерді ажыратады [74, Б. 4–6]. Бұл ретте провайдердің жергілікті экспорт құралы арқылы алынған деректердің провайдер құқықтық сұрату бойынша тікелей ұсынған мәліметтермен салыстырғанда толық болмауы мүмкін екені арнайы ескертіледі [74, 5 б.]. Ал деректер алынғаннан кейін олардың толықтығын, тұтастығын, хэш-мәндерін және алу барысының құжатталуын тексеру ұсынылады [74, 8 б.]. Осыған байланысты бұлттық деректерді бағалау кезінде ұйымның мәліметті қандай интерфейс немесе экспорттау тетігі арқылы алғаны, сұратудың және экспорттың нақты ауқымы, аккаунт пен қызмет түрі, қолданылған уақыт жүйесі, алынған және алынбай қалған деректер санаттары анықталуы тиіс. Провайдердің ресми мәртебесі немесе деректерді өзі ұсынғаны экспортталған пакеттің толықтығы мен техникалық дұрыстығын автоматты түрде дәлелдемейді. Сондықтан провайдерден алынған мәліметтердің шығу тегі, толықтығы, тұтастығы және оларды қалыптастыру тәсілі дербес тексерілуі тиіс.

Бұлттық есептеулердегі қауіпсіздік пен құпиялылық мәселелерін талдайтын NIST SP 800-144 ақпараттық қызметтерді сыртқы бұлттық провайдерге беру ұйымның қауіпсіздік пен дербес деректерді қорғауға қатысты жауапкершілігін жоймайтынын көрсетеді. Құжатта бұлттық қызметтерді пайдаланушы ұйым таңдалған бұлттық ортаның және аутсорсингке берілген қызметтердің қауіпсіздігі мен құпиялылығы үшін түпкілікті жауапты болып қалатыны атап өтіледі [75, 6 б., 15 б.]. Сонымен қатар бұлттық ортаға көшу ақпарат пен жүйелік компоненттерге тікелей бақылаудың бір бөлігін провайдерге берумен байланысты болғандықтан, ұйымның мониторинг, инциденттерге ден қою және деректерді қорғау жөніндегі міндеттерді орындауы провайдердің ынтымақтастығына тәуелді болуы мүмкін [75, 21 б.]. Қылмыстық-процестік тұрғыдан бұл ұстаным екі бағытта маңызды. Біріншіден, дерек ұстаушының «ақпарат бұлттық ортада орналасқан» деген жауабы оның сол мәліметке қандай техникалық немесе шарттық қолжетімділігі бар екенін, оны алу, экспорттау немесе сақтау мүмкіндігін нақтылау қажеттігін жоймайды. Екіншіден, тергеу барысында алынған құпия немесе дербес деректерді кез келген сыртқы бұлттық сервиске жүктеу бейтарап техникалық әрекет ретінде қарастырылмауы тиіс. Мұндай

жағдайда өңделетін деректердің сипаты, қызмет көрсетушіге берілетін қолжетімділік көлемі, мәліметтердің көшірілу немесе қайта пайдаланылу мүмкіндігі, сондай-ақ деректер орналасатын юрисдикция алдын ала бағалануы қажет. NIST SP 800-144 трансшекаралық деректер ағындарында деректер жиналған және кейін орналастырылған юрисдикциялардағы құқықтық режимдердің айырмашылығы қосымша қауіпсіздік пен құпиялылық тәуекелдерін туындатуы мүмкін екенін көрсетеді [75, 27 б.].

Цифрлық материалдың тұтастығы оны анықтау, алу, сақтау, зерттеу және кейінгі пайдалану кезеңдері арасындағы өзгерістерді бақылауды білдіреді. NIST IR 8387 цифрлық дәлелдемелерді сақтау дәстүрлі заттай объектілерді сақтаудан ерекшеленетінін атап көрсетеді: цифрлық дәлелдеме физикалық тасымалдағышта орналасқанымен, дәлелдемелік мән көбіне тасымалдағыштың өзіне емес, оның цифрлық мазмұны мен онымен байланысты ақпаратқа тиесілі [76, 1 б.]. Құжат цифрлық файлдардың тұтастығын қамтамасыз ету үшін олардың бастапқы дереккөзін және қалай алынғанын құжаттауды, сондай-ақ хэш-мәндер немесе цифрлық қолтаңбалар арқылы кейінгі өзгерістерді бақылауды ұсынады [76, 7 б., 8 б.]. Осы айырмашылық қылмыстық-процестік тұрғыдан маңызды. Құрылғының немесе тасымалдағыштың сыртқы орамасының бүтін болуы ондағы цифрлық мазмұнның оған дейін өзгермегенін өздігінен дәлелдемейді. Сол сияқты заңды зерттеу мақсатында құрылғыны ашу немесе оның цифрлық көшірмесін жасау, егер орындалған әрекеттер тиісті түрде құжатталып, алынған материалдың тұтастығы тексерілсе, цифрлық дәлелдеменің тұтастығы бұзылды дегенді автоматты түрде білдірмейді. Сондықтан физикалық объектінің қозғалысын тіркейтін сақтау есебі мен цифрлық мазмұнның шығу тегін, көшірілуін және өзгеріссіздігін бақылауға мүмкіндік беретін техникалық есеп өзара толықтырушы тетіктер ретінде қарастырылуы тиіс.

Хэштеу кіріс деректерін криптографиялық хэш-функция арқылы өңдеп, белгіленген ұзындықтағы хэш-мәнді қалыптастыруды білдіреді. FIPS 180-4 қауіпсіз хэш алгоритмдерінің хабарламадан қысқартылған цифрлық көрініс қалыптастыратынын және бастапқы хабарламадағы кез келген өзгеріс өте жоғары ықтималдықпен өзге хэш-мәннің пайда болуына әкелетінін көрсетеді [77, 3 б.]. SHA-256 алгоритмі бойынша есептеу нәтижесінде 256 биттік хэш-мән қалыптасады [77, 21 б.]. Хэштеу шифрлау немесе иесіздендіру тәсілі болып табылмайды: ол деректердің құпиялылығын қамтамасыз етпейді және цифрлық материалды тиісті сақтау тәртібін алмастырмайды. Оның қылмыстық-процестік маңызы белгілі бір уақыт сәттерінде есептелген хэш-мәндерді салыстыру арқылы цифрлық объектінің салыстырылатын нұсқалары арасында өзгеріс болған-болмағанын тексеруге мүмкіндік беруінде. Осы зерттеуде бастапқы алынған көшірме мен кейін пайдаланылған немесе берілген көшірменің хэш-мәндерін SHA-256 сияқты жарамды алгоритм арқылы есептеп, қолданылған алгоритмнің атауын, есептеу уақытын және тиісті объектіні тіркеу ұсынылады. Хэш-мәндердің сәйкес келуі салыстырылған екі цифрлық объектінің хэш есептелген тиісті сәттердегі мазмұнының бірдей екенін растауға мүмкіндік береді. Алайда

мұндай сәйкестік деректің хэш алғаш есептелгенге дейін өзгермегенін, оның авторын немесе нақты пайдаланушысын, мазмұнының шынайылығын не деректі алудың қылмыстық-процестік заңдылығын өздігінен дәлелдемейді. Сондықтан хэш-мән цифрлық тұтастықты тексеру құралы ретінде пайдаланылғанымен, дәлелдеменің қатыстылығы, анықтығы және жол берілетіндігі өзге мән-жайлармен бірге дербес бағалануы тиіс.

Бір логикалық мазмұн әртүрлі экспорт форматында берілгенде оның хэші өзгеруі мүмкін. Мысалы, файлды басқа кодтауға ауыстыру, жол аяқталуын өзгерту немесе контейнерге қайта орау байттық құрамға әсер етеді. Сондықтан «хэш сәйкес келмейді» деген белгі бірден қасақана бұрмалау деп бағаланбайды. Бастапқы объект, өзгерту операциясы және туынды объекттің жеке хэші көрсетіледі, өзгерту қажет болмаса, түпнұсқа көшірме сақталады. Бірнеше файлдан тұратын пакет үшін манифестте әр файлдың атауы, өлшемі және хэші берілгені жөн. Тізілімнің өзі де кейін өзгертілмегенін тексеруге мүмкіндік беретін тәсілмен бекітіледі.

Уақытты сенімді бекіту цифрлық материалдың хэш-мәнін есептеуден бөлек қарастырылуы тиіс. RFC 3161 уақыт белгісі қызметін белгілі бір деректің нақты уақыт сәтіне дейін болғанын растауға мүмкіндік беретін тетік ретінде сипаттайды [78, Б. 1–2]. Уақыт белгісін қалыптастыру кезінде деректің өзі емес, оның криптографиялық хэш-мәні пайдаланылады, ал уақыт белгісін беретін сенімді тарап тиісті уақыт мәнінің дұрыстығын қамтамасыз етуі тиіс [78, Б. 2- 4]. Сондықтан уақыт белгісінің болуы цифрлық объектінің белгілі бір уақыттан кешіктірмей болғанын растауға көмектескенімен, оның авторын, мазмұнының шынайылығын немесе деректі алудың қылмыстық-процестік заңдылығын өздігінен дәлелдемейді. Электрондық цифрлық қолтаңба электрондық құжаттың түпнұсқалығын, белгілі бір қол қоюшыға тиесілілігін және қол қойылғаннан кейін мазмұнының өзгермегендігін тексеруге мүмкіндік береді [4]. Алайда ЭЦҚ-ның болуы қол қоюшының құжатта сипатталған бастапқы оқиғаны өзі тікелей қабылдағанын немесе құжаттағы әрбір фактілік тұжырымның шынайылығын автоматты түрде растамайды. Сондықтан ЭЦҚ-ның қылмыстық процестегі маңызы оның техникалық жарамдылығымен ғана емес, құжаттың шығу тегімен, жасалу жағдайларымен және іс бойынша өзге дәлелдемелермен өзара байланысы арқылы бағалануы тиіс [4; 6].

Сақтау тізбегі деп объектінің табылған сәтінен бастап оны алу, көшіру, беру, зерттеу, сақтау және түпкілікті шешім қабылдау кезіндегі қозғалысы мен оған жасалған әрекеттердің құжатталған сабақтастығын түсіну ұсынылады. Бұл термин ҚПК-де жаңа дербес дәлелдеме көзі ретінде емес, қолданыстағы хаттамалар, қосымшалар, қабылдау-беру жазбалары және сақтау есебін біріктіретін әдістемелік ұғым ретінде қолданылады. Әр жазбада объект идентификаторы, әрекет уақыты, орындаушы, құқықтық не ұйымдастыру негізі, беруші мен алушы, орама күйі және қажет болғанда хэш көрсетіледі. Тізбектің мақсаты – объектіге кімнің қол жеткізгенін және қандай өзгеріс болуы мүмкін екенін тексеру.

Ұйымдастырушылық және техникалық ақпараттық қауіпсіздік

шаралары цифрлық мәліметтердің сақталуы мен кейіннен тексерілу мүмкіндігіне де ықпал етеді. ISO/IEC 27001:2022 ақпараттық қауіпсіздікті басқару жүйесін құру, енгізу, қолдау және үздіксіз жетілдіру талаптарын белгілеп, ақпараттың құпиялылығы, тұтастығы мен қолжетімділігін тәуекелдерді басқару негізінде қамтамасыз етуге бағытталады [79, 4–10 бөлімдер]. Стандарттың А қосымшасында қолжетімділікті басқару, резервтік көшіру, журналдау, мониторинг және уақытты синхрондау сияқты бақылау шаралары көзделген [79, A.5.15–A.5.18, A.8.13, A.8.15–A.8.17]. ISO/IEC 27002:2022 аталған бақылау шараларын іске асыру жөніндегі практикалық ұсынымдарды нақтылайды және қолжетімділікті басқару, криптографиялық құралдарды пайдалану, резервтік көшіру, журналдарды қалыптастыру мен қорғау, мониторинг және ақпараттық қауіпсіздік инциденттеріне ден қою мәселелерін қамтиды [80]. ISO-ның ресми сипаттамасы да бұл стандарттың қолжетімділікті бақылау, криптография және инциденттерге ден қою сияқты ақпараттық қауіпсіздік шараларына арналғанын көрсетеді. Алайда ұйымның ISO/IEC 27001 немесе ISO/IEC 27002 талаптары мен ұсынымдарына сәйкестігі нақты цифрлық файлдың қылмыстық процестегі жол берілетіндігін немесе анықтығын автоматты түрде айқындамайды. Бұл стандарттардың әдістемелік маңызы тергеу органында немесе өзге дерек ұстаушыда цифрлық материалдарды сақтау ортасына рөлдер бойынша қолжетімділікті шектеу, көшірмелердің қозғалысын тіркеу, резервтік көшіруді ұйымдастыру, журналдарды қорғау және әкімшілік әрекеттерді бақылау тәртібін негіздеуге көмектесуінде. Мұндай бақылау сыртқы кибершабуылдардың алдын алумен ғана шектелмей, қызметкерлердің деректерді рұқсатсыз қарауы, көшіруі, өзгертуі немесе таратуы сияқты ішкі қауіптерді де қамтуы тиіс.

NIST SP 800-53 Rev. 5 ақпараттық жүйелердегі қауіпсіздік пен құпиялылықты қамтамасыз етуге арналған бақылау шараларын жүйелейді. Қолжетімділікті басқару бөлігінде стандарт мақұлданған қолжетімділік өкілеттіктерін іске асыруды және пайдаланушыға тек оның міндеттерін орындау үшін қажетті ең төмен көлемдегі құқықтарды беруді көздейді [81, Б. 23–28, 38б., 40 б.]. NIST SP 800-122 тұлғаны сәйкестендіруге мүмкіндік беретін ақпаратты қорғау деңгейін деректердің сипатына ғана емес, оларды пайдалану контекстіне, көлеміне, қолжетімділік жағдайына және құпиялылық бұзылған жағдайда тұлғаға немесе ұйымға келуі ықтимал зиянға қарай анықтауды ұсынады [82, 16 б., 20 б.]. Авторлар бірдей дербес деректердің әртүрлі пайдалану контекстінде әртүрлі құпиялылық деңгейін талап етуі мүмкін екенін арнайы көрсетеді [82, 19 б.]. Аталған тәсілдерді қылмыстық процеске бейімдеу іс материалдарына қолжетімділікті тек «толық ашық» немесе «толық жабық» деген екі режиммен шектеудің жеткіліксіз екенін көрсетеді. Тергеуші, маман, сарапшы, прокурор, қорғаушы және өзге де процеске қатысушылардың функциялары мен процестік өкілеттіктері әртүрлі болғандықтан, дербес деректерге қолжетімділік те нақты міндет пен заңда көзделген құқық көлеміне сәйкес сарапануы тиіс. Осыған байланысты жұмыс көшірмелерінде іске қатысы жоқ немесе нақты міндетті орындауға қажет емес дербес деректерді шектеу, бүркемелеу немесе

бөлек сақтау мүмкіндігі қарастырылуы мүмкін. Сонымен бірге мұндай шаралар қорғау тарапының іс материалдарымен танысу, дәлелдемелерді тексеру және өз позициясын негіздеу жөніндегі процестік құқықтарын негізсіз шектемеуі тиіс [6]. Сондықтан құпиялылықты қорғау шарасының заңдылығы оның деректерді қорғауға қаншалықты тиімді екенімен ғана емес, қылмыстық процеске қатысушылардың құқықтарына, әсіресе қорғану құқығына ықпалымен бірге бағалануы керек.

Арнайы білім қолдану осы санаттағы істерде техникалық амалдардың күрделілігімен ғана емес, алынған ақпараттың мағынасын дұрыс түсіндіру қажеттігімен негізделеді. ҚПК-нің 79 және 80-баптары сарапшы мен маманның мәртебесін, ал сот-сараптама қызметі туралы заң сараптамалық зерттеудің ұйымдастырылуы мен тәуелсіздігіне қатысты талаптарды белгілейді [6; 83]. Маман тергеу әрекетіне жәрдем көрсете алады және заңда белгіленген жағдайларда зерттеу жүргізіп, қорытынды береді. Сондықтан «маман тек құрылғыны қосады, сарапшы ғана кез келген талдау жасайды» деген қатаң бөлу қолданыстағы реттеудің мазмұнын дәл жеткізбейді.

Конституциялық Соттың 2023 жылғы 20 шілдедегі № 24-НҚ қаулысы ҚПК-нің 80-бабының екінші бөлігін маманның іске мүдделі болмауы, арнаулы білімі мен құзыреті, сондай-ақ тиісті бөлімшенің функционалдық мақсаты тұрғысынан түсіндіреді [84]. Бұл құқық қорғау органының кез келген қызметкерін зерттеу жүргізуге маман ретінде тағайындауға жеткілікті негіз емес. Дерек ұстаушы ұйымның жүйелік әкімшісі ақпаратты түсіндіріп, экспортқа қатысуы мүмкін, бірақ оның ұйымдағы оқиға үшін жауаптылығы немесе іске мүдделілігі тексерілуі тиіс. Ол беретін түсініктемелердің процестік мәртебесі мен тәуелсіз арнайы зерттеудің мәртебесі ажыратылады.

Маманның бастапқы кезеңдегі міндеттеріне жүйені қауіпсіз қарау тәсілін таңдау, өзгергіш деректерді анықтау, техникалық көшірме алу, журналдар құрылымын түсіндіру және қолданылған құралдың жұмысын тіркеуге көмектесу жатады. Сараптама арнаулы ғылыми зерттеу арқылы шешілетін сұрақтар болғанда тағайындалады. Мұндай сұрақтар файлдардың өзгертілуін, операциялар кезегін, деректердің қалпына келтірілуін немесе бірнеше құрылғыдағы іздердің байланысын қамтуы мүмкін. Таңдау лауазым атауына емес, міндеттің мазмұнына, зерттеу әдісіне және заңдық талапқа сүйенеді. ҚПК бойынша сараптама міндетті болған жағдайларда оны маманның түсіндірмесімен алмастыруға болмайды.

6-кесте – Маман мен сарапшының міндеттерін процестік сұрақ бойынша ажырату

№	Мәселе	Маманның ықтимал көмегі	Сараптамалық зерттеу қажет болатын жағдай
1	Ізді сақтау	Құрылғы күйін бағалау, алу тәсілін таңдау, операцияны түсіндіру	Арнайы зерттеу арқылы шешілетін дербес диагностикалық сұрақ пайда болса
2	Логты түсіндіру	Өрістер мен уақыт жүйесін түсіндіру; жинау және бекітуге қатысу	Операциялар тізбегін, өзгеріс белгілерін немесе күрделі байланысты зерттеу қажет болса

№	Мәселе	Маманның ықтимал көмегі	Сараптамалық зерттеу қажет болатын жағдай
3	Тұтастық	Көшірме жасауға көмектесу, хэш есептеу және салыстыру	Бұрмалау, қалпына келтіру немесе өзгерістің сипаты туралы даулы мәселе туындаса
4	Авторлық және атрибуция	Құрылғы, аккаунт, сеанс байланысын техникалық түсіндіру	Арнайы әдіспен сәйкестендіру қажет болса; кінә туралы құқықтық бағаны сарапшы бермейді
5	Нәтиженің нысаны	ҚПК рұқсат ететін көмек, түсіндірме, зерттеу және қорытынды	Қаулыда қойылған арнайы ғылыми сұрақтар бойынша сарапшы қорытындысы

Ескерту: ҚПК-нің 80, 117 және сараптамаға қатысты нормалары [6], Сот-сараптама қызметі туралы заң [83] және Конституциялық Соттың № 24-НҚ қаулысы [84] негізінде автор құрастырған. Маманның заңда көзделген зерттеу және қорытынды беру өкілеттігі сақталады.

Сарапшыға қойылатын сұрақтар құқықтық саралауды алдын ала шешпеуі тиіс. «Күдікті дербес деректерді заңсыз таратты ма?» деген сұрақтың орнына сарапшының арнайы білімінің шегінде анықталуға жататын мән-жайларға, атап айтқанда, ұсынылған жазбада тіркелген операциялардың сипатына, жіберілген файлдардың немесе деректер жиынтығының мазмұнына, ақпаратты жіберу әрекетінің аяқталу белгілеріне, уақыт көрсеткіштерінің өзара сәйкестігіне, файлдардың өзгертілу ықтималдығына және ұсынылған материалдар негізінде қорытынды жасау мүмкіндігінің шектеріне қатысты сұрақтар қойылуы тиіс. Сұрақтарды осылай құру құқықтық бағалауды тергеуші мен соттың құзыретінде сақтайды және сараптаманың тексерілетін мазмұнын нақтылайды [6; 83].

Әдістің жарамдылығы мен нәтиженің түсіндірілуін ажырату қажет. ISO/IEC 27041 әдістің қойылған мақсатқа сай екенін негіздеуге, ISO/IEC 27042 талдау мен түсіндірудің сабақтастығына, жарамдылығына және қайталанатындығына бағытталған [85; 86]. NIST IR 8354 цифрлық зерттеу техникасының ғылыми негіздерін бағалайды [87]. Осы материалдардан шығатын процестік талап – сараптамалық қорытындыда құрал атауын ғана емес, әдістің не үшін таңдалғанын, қандай деректерге қолданылғанын және нәтижені қандай шекте түсіндіруге болатынын көрсету. Құралдың сертификаты нақты іске қолданудың дұрыстығын жеке тексеруді жоймайды.

Дж. Бранти цифрлық криминалистикалық құралдар мен әдістерді валидациялауды олардың нақты зертханалық қолданылуын, ғылыми қағидаларға негізделген бақыланатын сынақтарды және кәсіби рецензиялауды біріктіретін жүйелі процесс ретінде қарастырады [88, 1 б.]. Автордың пікірінше, құралдың немесе әдістің белгілі бір нәтиже шығара алуы оның барлық ықтимал қолдану жағдайларында ғылыми тұрғыдан сенімді екенін автоматты түрде білдірмейді. Сондықтан валидация жоспарланған сынақтар мен тексерілетін өлшемдерге негізделуі тиіс [88]. Н. Хьюз пен Ү. Қарабийик цифрлық криминалистикада сенімді нәтижеге қол жеткізуді өлшеу ғылымының қағидаларымен байланыстырады. Авторлар валидацияны процестің дәлдігі мен сенімділігін ғылыми тұрғыдан дәлелдеудің қабылданған тәсілі ретінде сипаттап, құралдарды тестілеу

олардың шектеулерін түсінуге көмектескенімен, бұл барлық ықтимал құрылғы жағдайларын, конфигурацияларды және функционалдық ерекшеліктерді толық қамтитын валидацияны алмастырмайтынын көрсетеді [89, 1 б., 3 б.]. Осы екі ғылыми бағыттан туындайтын ортақ қорытынды – құралдың техникалық тұрғыдан нәтиже қалыптастыру қабілеті мен оның нақты дәлелдеу сұрағына дұрыс әрі сенімді жауап беру қабілеті бір ұғым емес. Мысалы, бағдарламалық құрал белгілі бір файл форматын дұрыс ашуы мүмкін, бірақ нақты қосымша нұсқасындағы уақыт өрісін немесе өзге метадеректі қате түсіндіруі ықтимал. Сондықтан нақты іс бойынша қорытынды үшін шешуші функциялар алдын ала тексеріліп, анықталған шектеулер мен ықтимал қателік жағдайлары құжатталуға, ал нәтижені қайталап тексеруге мүмкіндік беретін бастапқы және аралық материалдар сақталуы тиіс.

Г. Хорсман ұсынған FRED (Framework for Reliable Experimental Design) моделі цифрлық деректерді зерттеудің сенімділігін қамтамасыз ету мақсатында зерттеу мәселесін айқындау, тәжірибені жоспарлау, жүргізу және алынған нәтижелерді талдау кезеңдерінің өзара байланысына негізделген [90, Б. 294–306]. Ғалым цифрлық іздерді түсіндіру ғылыми негізделген және нәтижелерін қайта тексеруге мүмкіндік беретін тәжірибелік зерттеуге сүйенуі қажеттігін атап көрсетеді [90, Б. 294–296]. Аталған тәсіл цифрлық деректердің техникалық мағынасына қатысты күмән туындаған жағдайларда ерекше маңызға ие. Мәселен, белгілі бір қолданбадағы белгі хабарламаның оқылғанын растайтынын анықтау үшін арнайы бақыланатын ортада тәжірибелік зерттеу жүргізілуі мүмкін. Мұндай жағдайда пайдаланылған құрылғының сипаттамалары, операциялық жүйе мен қолданбаның нұсқалары, зерттеудің бастапқы шарттары, орындалған әрекеттер және алынған нәтижелер толық тіркелуі тиіс. Алайда тәжірибелік жағдайда анықталған заңдылықтар нақты қылмыстық іс бойынша зерттелетін құрылғыда дәл сондай әрекеттердің орын алғанын өздігінен дәлелдемейді. Сондықтан тәжірибе жүргізілген жағдайлар мен қылмыстық істің нақты мән-жайлары арасындағы сәйкестіктер мен айырмашылықтарды ескеру зерттеу нәтижелерінің ғылыми негізділігін және оларды дәлелдеу процесінде пайдалану шектерін дұрыс бағалауға мүмкіндік береді.

Н. Сунде мен И. Дрор цифрлық криминалистикалық зерттеулер нәтижелерінің сенімділігіне қолданылатын техникалық құралдар мен әдістермен қатар, зерттеушінің когнитивтік ерекшеліктері және оған ұсынылатын контекстік ақпараттың да әсер ететінін атап көрсетеді [91, Б. 103–106]. Ғалымдардың пікірінше, алдын ала қалыптасқан болжамдар, күтілетін нәтижелер және зерттеу міндетіне тікелей қатысы жоқ айыптаушы сипаттағы мәліметтер зерттеу барысына және алынған нәтижелерді түсіндіруге ықпал етуі мүмкін [91, Б. 104–106]. Осыған байланысты тергеушінің сарапшыға немесе маманға зерттеу жүргізу үшін қажетті ақпаратпен қатар, алдын ала қалыптасқан айыптау нұсқасын және іске қатысты өзге де мәліметтерді шамадан тыс ұсынуы зерттеу нәтижелерінің объективтілігіне әсер ету қаупін арттырады. Сондықтан сарапшыға немесе

маманға зерттеу міндеттерін орындау үшін қажетті материалдар ұсынылып, зерттеу нәтижелеріне ықпал етуі мүмкін, бірақ қойылған сұрақтарға тікелей қатысы жоқ ақпараттың көлемі шектелуі тиіс. Мұндай шектеу қылмыстық іс үшін маңызды мәліметтерді жасыруды емес, зерттеудің объективтілігін қамтамасыз ету мақсатында ақпараттың маңыздылығын ажыратуды көздейді. Сонымен қатар зерттеу барысында тікелей анықталған фактілер, олардың техникалық түсіндірмелері және құқықтық бағалау нәтижелері өзара ажыратылуы қажет. Цифрлық іздердің мағынасына қатысты баламалы түсіндірулер немесе анықталмаған мән-жайлар болған жағдайда олар сарапшының қорытындысында нақты көрсетілуі тиіс. Бұл тәсіл арнайы білімді қолдану нәтижелерінің ғылыми негізділігін арттыруға, сараптамалық тұжырымдардың шегін айқындауға және цифрлық дәлелдемелерді қылмыстық процесте жан-жақты әрі объективті бағалауға мүмкіндік береді.

С. Гарфинкель, П. Фаррелл, В. Русев және Г. Динолт цифрлық криминалистикада стандартталған зерттеу деректер жиынтықтарын пайдаланудың ғылыми маңызын негіздейді. Авторлардың пікірінше, репрезентативті эталондық корпустар зерттелетін әдіс немесе құрал үшін бастапқы «дұрыс нәтиже» өлшемін қалыптастыруға, жаңа құралдар мен әдістердің тиімділігін объективті көрсеткіштер арқылы бағалауға және әртүрлі зерттеулердің нәтижелерін салыстыруға мүмкіндік береді [92, Б. S2–S3]. Сонымен қатар стандартталған деректер жиынтықтары зерттеу нәтижелерінің қайталанушылығын қамтамасыз етуге және оларды оқыту мен құралдарды сынау мақсатында пайдалануға жағдай жасайды [92, Б. S3–S5]. Авторлар нақты адамдарға тиесілі деректерді оқу және зерттеу мақсатында пайдалану құпиялылық пен этикалық шектеулер туғызатынын атап өтіп, арнайы құрастырылған тестілік деректерді дербес санат ретінде бөліп көрсетеді [92, Б. S4–S5]. Осы тәсілді Қазақстан жағдайына бейімдеу цифрлық криминалистика мамандарын даярлау мен техникалық құралдарды валидациялау кезінде нақты жәбірленушілердің немесе қылмыстық іс қатысушыларының құпия материалдарын негізсіз пайдалануды шектеуге мүмкіндік береді. Осы мақсатта құқықтық негізі айқын, иесіздендірілген не арнайы жасалған сынақ массивтері қолданылуы мүмкін. Сонымен бірге мұндай сынақ массивтерінің мақсаты нақты құқық қолдану практикасын сипаттау емес, зерттеу әдістері мен құралдарының жұмыс қабілетін тексеру болып табылады. Сондықтан тестілік деректер бойынша алынған нәтижелер эмпирикалық қылмыстық статистикамен немесе осы диссертация шеңберінде жүргізілген 850 респонденттің сауалнама нәтижелерімен араластырылмауы тиіс. Құралды немесе әдісті валидациялау мен нақты құқық қолдану деректерін эмпирикалық талдау зерттеу мақсаты, объектісі және нәтижелерді интерпретациялау тәсілі бойынша дербес бағыттар ретінде сақталуы қажет.

Э. Кейси цифрлық криминалистика мен жалпы сот ғылымының жеткіліксіз ықпалдасуын осы саланың негізгі проблемаларының бірі ретінде қарастырады. Автор цифрлық іздердің көлемі мен күрделілігінің өсуі жағдайында цифрлық криминалистикалық зерттеулер сапасының төмендеуі, қателер мен елеусіз қалған мән-жайлардың қылмыстық сот төрелігі үшін

теріс салдар туғызуы мүмкін екенін атап көрсетеді [93, Б. 649–652]. Осыған байланысты ол цифрлық криминалистиканы жалпы сот ғылымының ғылыми қағидаттарымен неғұрлым тығыз байланыстыру және криминалистикалық білімді жүйелі басқару қажеттігін негіздейді [93, Б. 649–664]. Бұл ұстаным цифрлық зерттеудің сапасын тек жаңа бағдарламалық құралдар мен техникалық мүмкіндіктердің көбеюімен байланыстыру жеткіліксіз екенін көрсетеді. Зерттеу нәтижелерінің сенімділігі зерттеу объектісінің дұрыс айқындалуына, баламалы түсіндірулердің жан-жақты тексерілуіне, қолданылған әдістердің мүмкіндіктері мен шектеулерінің ескерілуіне, сондай-ақ алынған қорытындылардың мазмұнын түсінуге және олардың негізділігін кейіннен тексеруге мүмкіндік беретіндей баяндалуына байланысты. Осы тұрғыдан осы зерттеуде маман немесе сарапшыны тартудың қажеттілігін «құрылғының техникалық күрделілігімен» ғана анықтамау ұсынылады. Негізгі өлшем – арнайы білім қолданылмаған жағдайда қандай дәлелдеу тәуекелі шешілмей қалатынын және оны маманның қатысуы, сараптама немесе өзге тиісті процестік нысан арқылы қалай жоюға болатынын анықтау.

Техникалық толық көшірме жасау қажеттігі сол көшірмедегі барлық ақпаратты шектеусіз қарау қажеттігін білдірмейді. SWGDE-нің нысаналы жинау жөніндегі ұсынымдары нақты мақсатқа сәйкес деректер ауқымын анықтау мәселесін қарастырады [94]. Компьютерлік зерттеу жөніндегі ұсынымдары зерттеудің көлемі мен міндетінің айқын болуына мән береді [95]. Ұсынылатын модельде толықтықты сақтау үшін алынған бақылау көшірмесі мен күнделікті талдауға берілетін жұмыс жиынтығы ажыратылады. Іріктеу шарттары, шектелген санаттар және қосымша зерттеу қажеттігі туындағанда ауқымды кеңейту негізі құжатталады.

Басқа адамдардың медициналық деректері, интимдік материалдар немесе қорғаушымен хат-хабар кездейсоқ қамтылғанда арнайы сүзу тәртібі қажет. Мұндай материалды бірден жою дәлелдемелік контекстті жоғалтуы мүмкін, ал барлық қатысушыға тарату қайталама зиян келтіреді. Сондықтан заңды шешім қабылданғанға дейін бастапқы көшірме қорғалған күйде сақталып, қатысы жоқ мазмұн жұмыс көшірмесінде шектеледі. Сүзудің негізі мен нәтижесін тексеруге мүмкіндік сақталады. Қорғану үшін маңызды материалды «дербес дерек» деген жалпы себеппен жасыруға болмайды: қолжетімділік дауы процестік тәртіппен шешілуі тиіс [6].

Деректерді жою цифрлық материалдармен жұмыс істеудің соңғы техникалық кезеңдерінің бірі ретінде қарастырылуы мүмкін, алайда оны жүргізу тек тиісті құқықтық негіз болған жағдайда ғана жол беріледі. NIST SP 800-88 Rev. 2 ақпарат жеткізгіштегі нысаналы деректерге кейіннен қол жеткізуді іс жүзінде мүмкін емес етуге бағытталған санитарлық тазарту тәсілдерін жүйелейді және оларды clear, purge және destroy әдістеріне бөледі [96, 8б., 11 б.]. Құжат санитарлық тазарту тәсілін ақпараттың сезімталдығы, тасымалдағыштың кейінгі пайдаланылуы және құпиялылық тәуекелдері ескеріле отырып таңдауды көздейді [96, 18б., 22 б.]. Алайда NIST ұсынымдары цифрлық материалды жоюға дербес құқықтық рұқсат бермейді.

Қылмыстық процесте техникалық жою тәсілін таңдауға дейін істің процестік мәртебесі, материалды сақтау жөніндегі міндет, шағымдану немесе қайта тексеру мүмкіндігі, сондай-ақ заттай және өзге дәлелдемелердің тағдыры туралы тиісті шешім айқындалуы тиіс. Тек осы құқықтық алғышарттар сақталғаннан кейін жою тәсілі таңдалып, жойылған объект, жоюдың негізі, қолданылған әдіс, орындалған уақыт, жауапты тұлға және нәтиже құжатталуы қажет. NIST SP 800-88 Rev. 2 де санитарлық тазарту бағдарламасында орындалған әрекеттерге қатысты қажетті жазбалар мен құжаттаманы жүргізудің маңызын атап көрсетеді [96, Б. 18–19]. Сондықтан киберқауіпсіздік немесе ақпараттық құпиялылық мақсатындағы «тазарту» талабы қылмыстық іс үшін маңызы бар цифрлық мәліметтерді олардың процестік тағдыры шешілмей тұрып мерзімінен бұрын жоюға негіз болмауы керек. Техникалық қауіпсіздік талабы мен дәлелдемелерді сақтау міндеті бір-бірімен үйлестіріліп қолданылуы қажет.

Дербес деректерге қатысты дәлелдемелерді жинау және бекіту құқықтық негізді таңдаудан басталып, деректің шығу тегін, алыну шегін және кейінгі қозғалысын тексеруге мүмкіндік беретін рәсіммен аяқталуы тиіс. Ұсынылған ең аз дәлелдемелік пакет бастапқы мәліметті, оның метадеректерін, экспорт сипаттамасын және беру есебін біріктіреді. Екі деңгейлі сұрату моделі ішкі құқықтық негіздеменің толықтығын сақтай отырып, сыртқы орындау құжатында артық ақпараттың ашылуын азайтуға бағытталған.

Хэш, уақыт белгісі, электрондық цифрлық қолтаңба және сақтау тізбегі өзара байланысты, бірақ бірін-бірі алмастырмайтын құралдар болып табылады. Хэш мәні цифрлық деректердің әртүрлі уақыттағы жай-күйінің сәйкестігін тексеруге, уақыт белгісі белгілі бір әрекеттің немесе оқиғаның уақытын анықтауға, электрондық цифрлық қолтаңба электрондық құжаттың тұтастығын және оған қол қойған тұлғаны сәйкестендіруге, ал сақтау тізбегі зерттеу объектісінің алынуынан бастап кейінгі қозғалысы мен сақталу тәртібін анықтауға мүмкіндік береді. Аталған құралдардың ешқайсысы цифрлық деректерді алудың заңдылығын, нақты әрекетті жасаған тұлғаны және ақпарат мазмұнының шынайылығын жеке өзі толық дәлелдей алмайды.

Маман мен сарапшыны қатыстыру қажеттілігі шешілетін міндеттердің сипатына, қолданылатын зерттеу әдістеріне, олардың тәуелсіздігіне және заңнамада белгіленген өкілеттіктеріне сәйкес айқындалуы тиіс. Зерттеу нәтижелерінің сапасы қолданылған техникалық құралдардың атауымен емес, таңдалған әдістердің ғылыми негізділігімен, олардың мүмкіндіктері мен шектеулерінің ескерілуімен, сондай-ақ алынған қорытындылардың негізділігін кейіннен тексеру мүмкіндігімен бағаланады. Аталған талаптардың сақталуы адамның құқықтары мен бостандықтарын шектеуге байланысты қылмыстық-процестік әрекеттерді жүргізу барысында да маңызды болып табылады. Бұл талаптардың бұзылуы алынған дәлелдемелердің жол берілетіндігіне, анықтығына және жеткіліктілігіне әсер етуі мүмкін.

2.3 Құқықтарды шектеумен байланысты процестік құралдар: жасырын тергеу әрекеттері және цифрлық ортадағы дәлелдемелердің жол берілетіндігін бағалау

Дербес деректерді заңсыз жинауды, өңдеуді және таратуды тергеп-тексеру барысында адамның жеке өміріне заңды түрде араласу қажеттілігі туындауы мүмкін. Осы қайшылық зерттеудің негізгі процестік проблемасын ашады: деректерге жасалған қолсұғушылықты анықтайтын орган сол деректерді қайта жинайды, жүйелейді және іске қатысушыларға ұсынады. Сондықтан тергеу мақсатына сілтеме жасау кез келген көлемдегі араласуды ақтамайды. Қолданылатын құрал заңда көзделуі, нақты дәлелдеу міндетімен байланысуы және алынған мәліметтің кейінгі пайдаланылуы тексеруге келетіндей ұйымдастырылуы тиіс [1; 2; 6].

Жасырын тергеу әрекеттерін жедел-іздестіру қызметімен теңестіруге болмайды. Олардың әдістері ұқсас болғанымен, құқықтық негізі, жүргізілу жағдайы және нәтижені іске енгізу рәсімі өзара ажыратылады. Жедел-іздестіру қызметі туралы заң тиісті қызметтің дербес міндеттерін айқындайды, ал нақты қылмыстық іс шеңберіндегі ЖТӘ ҚПК-нің 30-тарауына бағынады [97; 6]. Жоғарғы Соттың ЖТӘ-ні санкциялау жөніндегі нормативтік қаулысы тергеу судьясының бақылауына, бастамашылық құжаттарының заңдылығына және әрекеттің процестік сипатына қатысты түсіндірмелер береді [98]. Ұйымдастыру қағидалары тапсырманы уәкілетті бөлімшеге беру мен орындаудың тәртібін нақтылайды, бірақ ҚПК-де жоқ өкілеттікті туындатпайды [99].

ҚПК-нің 231-бабындағы түрлерді дерек алудың техникалық тәсілімен дәл байланыстыру қажет. Байланыс желілеріндегі ақпаратты жасырын бақылау, абоненттер арасындағы қосылулар туралы мәліметті жасырын алу және компьютерлерден, серверлерден ақпаратты жасырын алу әртүрлі әрекеттер ретінде қарастырылады. Компьютерлерден, серверлерден және ақпаратты жинауға, өңдеуге, жинақтауға әрі сақтауға арналған басқа құрылғылардан ақпаратты жасырын алу 245-баппен реттеледі. Демек, құрылғыға қашықтан қосылудың техникалық мүмкіндігі өздігінен осындай әрекетті жүргізуге негіз болмайды; қолданылатын процестік түр мен оның шарттары алдымен анықталады [6].

ҚПК-нің 232-бабының үшінші бөлігі бойынша 231-баптың 1)–6) тармақтарындағы ЖТӘ тергеу судьясының санкциясымен жүргізіледі. Осы баптың төртінші бөлігіндегі қылмыстың жазалану шегі мен қылмыстық топқа қатысты шарттарды нақты саралаумен салыстыру қажет: заңда бір жылдан астам мерзімге бас бостандығынан айыру жазасы көзделген қылмыстар немесе қылмыстық топ жасаған қылмыстар туралы талап бекітілген. Сондықтан ЖТӘ-ні тек «ауыр қылмыстарға» қатысты құрал деп сипаттау қолданыстағы мәтінді дәл бермейді. Сонымен қатар дербес деректерге қатысты кез келген арыз бойынша барлық ЖТӘ түріне жол беріледі деген қорытынды да жасалмайды. Қылмыстық теріс қылықтар мен өзге қылмыстар үшін 232-баптың бесінші бөлігіндегі шектеулер және

заңдағы арнайы жағдайлар ескеріледі [6].

Заңда белгіленген процестік негіздердің болуы тергеу әрекетін жүргізудің қажеттілігі мен мөлшерлестігін өздігінен айқындамайды. Ұсынылатын негіздеу құрылымы тергеушіден қандай фактіні анықтау керектігін, оның іс үшін маңызын, неге қолда бар ашық құралдар жеткіліксіз екенін, кімнің немесе қандай құрылғының нысана болатынын және қандай уақыт аралығы қажет екенін көрсетуін талап етеді. Мұнда «ақпарат алу қажет» деген жалпы тұжырымның орнына, мысалы, белгілі кезеңдегі заңсыз экспортты ұйымдастырған тұлғалардың өзара байланысын тексеру міндеті жазылады. Бұл мысал нақты істің дерегі ретінде емес, өтінішхаттың дәлелдеу міндетіне бағдарлануын көрсететін әдістемелік жағдай ретінде ұсынылады.

Азаматтық және саяси құқықтар туралы халықаралық пактінің 17-бабы жеке өмірге заңсыз немесе ерікті араласудан қорғауды көздейді [100]. БҰҰ Адам құқықтары жөніндегі комитетінің № 16 жалпы түсіндірмесі заңда көзделген араласудың өзі Пактінің мақсаттарына сай болуы қажеттігін ашады [101]. Осы өлшемдер ұлттық санкциялау рәсімін мазмұнмен толықтыруға мүмкіндік береді: заңда рұқсат етілген құралдың нақты қолданылуы да негізделуі тиіс. Қазақстан үшін міндетті халықаралық шарт нормалары мен шетелдік соттардың салыстырмалы-құқықтық бағдар ретінде пайдаланылатын шешімдерінің мәртебесі бөлек сақталады.

Roman Zakharov ісінде Еуропалық адам құқықтары соты жасырын бақылауға қатысты заңның айқындығын, бақылауға жататын тұлғалар мен құқық бұзушылықтар санаттарын, бақылау мерзімін, алынған деректерді зерттеу, пайдалану, сақтау, беру және жою тәртібін, сондай-ақ алдын ала, ағымдағы және кейінгі бақылау кепілдіктерін біртұтас жүйе ретінде қарастырды [102, § 229–234, 257–267]. Бірінші тарауда талданған Big Brother Watch ісі де ақпаратты іріктеу, зерттеу, сақтау және беру кезеңдеріндегі кепілдіктердің өзара байланысын көрсетеді [43, § 348–356]. Бұл шешімдер Қазақстан үшін дайын процестік рәсім белгілемейді; олардың салыстырмалы-құқықтық маңызы санкцияны тек бастапқы рұқсат ретінде емес, деректермен кейінгі жұмыс істеудің де бақыланатын шегі ретінде түсіндіруінде.

Деректердің тікелей ақпараттық мазмұнды қамтымауы адамның құқықтары мен бостандықтарына араласу дәрежесін өздігінен төмендетпейді. Benedik ісінде динамикалық IP-мекенжайды нақты абонентпен сәйкестендіру жеке өмірге қол сұғылмаушылық құқығына қатысты мәселе туындататыны, сондай-ақ мұндай мәліметтерді алу үшін нақты құқықтық негіз бен жеткілікті кепілдіктердің болуы қажеттігі атап көрсетілген [103, § 100–119]. Қосылу уақыты, байланыс орнатылған абоненттер, орналасқан жері және желіге кіру жиілігі туралы мәліметтерді өзара байланыстыра талдау адамның жүріс-тұрысы мен байланыстары туралы маңызды ақпаратты анықтауға мүмкіндік береді. Осыған байланысты тек метадеректердің сұратылуы адамның құқықтарына араласу дәрежесін төмен деп бағалауға жеткілікті негіз бола алмайды. Мұндай жағдайда сұратылатын мәліметтердің сипаты, көлемі, оларды біріктіріп талдау мүмкіндігі және осының нәтижесінде жеке өмірге қол сұғылмаушылық құқығына ықтимал әсері ескерілуі тиіс.

Құрылғыдағы деректерге қол жеткізу мәселесіне қатысты Trabajo Rueda ісінде полицияның компьютерді заңды түрде иеленуі оның мазмұнын соттың алдын ала рұқсатынсыз зерттеуге өздігінен жеткілікті негіз болып табылмайтыны көрсетілген. Сот аталған іс бойынша сот рұқсатынсыз әрекет етуді негіздейтін шұғыл қажеттіліктің болмағанын атап өткен [104, § 30–38]. Saber ісінде смартфонның толық цифрлық көшірмесінен адвокатпен жүргізілген хат-хабарларды бөліп алу барысында кәсіби құпияны қорғауға бағытталған нақты әрі алдын ала айқындалған процестік кепілдіктердің болуы қажеттігі қарастырылған [105, § 48–57]. Аталған сот тәжірибесін талдау негізінде Қазақстан Республикасының қылмыстық процесі үшін маңызды қорытынды жасауға болады. Атап айтқанда, ақпарат тасымалдағышты заңды түрде алу ондағы барлық деректерді шектеусіз зерттеуге құқық бермейді. Осыған байланысты кәсіби құпияны құрайтын мәліметтерге, қылмыстық іске қатысы жоқ хат-хабарларға және үшінші тұлғалардың дербес деректеріне қол жеткізудің нақты шектерін айқындау, сондай-ақ оларды іріктеу мен қорғаудың тиісті процестік кепілдіктерін қамтамасыз ету қажет.

Еуропалық одақ Сотының Н.К. (Prokuratuur) ісі трафик пен орналасу деректеріне қол жеткізудің ауырлығын, сұратудың нақты мақсатпен байланысын және, заңда көзделген шұғыл жағдайларды қоспағанда, соттың немесе тәуелсіз әкімшілік органның алдын ала бақылауын талап ететін тәсілді қалыптастырды [106, § 35, 50–59]. Ал La Quadrature du Net бойынша 2024 жылғы C-470/21 шешімі IP-мекенжайды азаматтық сәйкестендіру деректерімен байланыстыруға қатысты, мұндай байланыстыру адамның жеке өмірі туралы дәл қорытынды жасауға мүмкіндік бермейтіндей деректерді бөлек сақтау және қорғау кепілдіктері қамтамасыз етілген жағдайда сараланған тәсіл қолданылуы мүмкін екенін көрсетті [107, § 72–94]. Екі шешімді қатар талдау метадеректерге бірыңғай абсолютті тыйым не бірыңғай жеңілдетілген рұқсат ұсынудың орнына, нақты сұратудың ақпараттық әлеуеті мен құқыққа араласу дәрежесін бағалау қажеттігін көрсетеді. Бұл ЕО-құқықтық өлшемдер Қазақстандағы прокурордың немесе тергеу судьясының құзыретін тікелей өзгерту ретінде түсіндірілмейді.

7-кесте – Жасырын тергеу әрекетін негіздеу және оның шегін бақылау матрицасы

№	Бақылау сұрағы	Негіздемеде көрсетілетін мазмұн	Қорғалатын мүдде
1	Қандай факт анықталады?	Құрам белгісі, дәлелдеу міндеті, бар мәліметтер және тексерілетін нұсқа	Негізсіз немесе барлау сипатындағы шексіз жинауды шектеу
2	Неге осы құрал қажет?	Өзге тәсілдердің жеткіліксіздігі; күтілетін нәтиженің маңызы	Қажеттілік пен мөлшерлестік
3	Кім немесе не нысана болады?	Тұлға, құрылғы, аккаунт, нөмір; олардың оқиғамен байланысы	Үшінші тұлғаларды негізсіз қамтымау
4	Қандай дерек және мерзім?	Қатысты санаттар, басталу/аяқталу, қайта бағалау шарты	Мақсат, көлем және уақыт шегі
5	Қандай рұқсат қажет?	ҚПК-дегі әрекет түрі, құзыретті орган, санкция; ерекше тәртіптің нақты негізі	Заңдылық және соттық бақылау

№	Бақылау сұрағы	Негіздемеде көрсетілетін мазмұн	Қорғалатын мүдде
6	Нәтиже қалай тексеріледі?	Беру тізілімі, зерттеу хаттамасы, іріктеу өлшемі, танысу және шағымдану рәсімі	Қорғану құқығы, тұтастық және құпиялық

Ескерту: ҚПК-нің 231–241-баптары [6] және Жоғарғы Соттың түсіндірмелері [98] негізінде ұсынылған авторлық тексеру матрицасы.

ҚПК-нің 235-бабындағы кейінге қалдыруға болмайтын тәртіп жалпы санкциялау рәсімін айналып өтудің құралы емес. Ол тергеу судьясын жиырма төрт сағат ішінде хабардар етуді және кейіннен санкция алуды көздейді. Егер судья кейінге қалдыруға болмайтынына келіспесе, әрекетті тоқтату және алынған нәтижелерді дәлелдемелер ретінде пайдалануға жол берілмейтіні туралы қаулы шығарады. Сондықтан жеделдік туралы уәжде нақты қауіп, уақыт жоғалтудың салдары және оны растайтын мәліметтер көрсетілуі тиіс. Деректердің жалпы өзгергіштігі әрбір іс бойынша ерекше тәртіпті автоматты түрде негіздемейді [6, 235-бап].

Санкцияланатын ЖТӘ-нің отыз тәуліктен аспайтын мерзімі мен оны ұзартудың рәсімі ҚПК-нің 236-бабында белгіленген. Осы мерзімді барлық жағдайда толық пайдаланылатын стандарт ретінде қабылдауға болмайды: қажеттілік жойылған кезде әрекет тоқтатылуы тиіс. Нысана аккаунтты, телефон нөмірін немесе техникалық идентификаторды ауыстыру қосымша құқықтық бағалауды талап етеді. Өзгерген идентификатордың сол тұлғаға тиесілігі тексерілмей, бастапқы санкцияның шегін кеңейтуге болмайды. Техникалық тапсырма заңдық қаулыдағы шекті нақты көрсетуі, ал орындалу есебі сол шектің сақталуын тексеруге мүмкіндік беруі қажет [6; 98].

Киберқауіпсіздік өлшемі мұнда деректерді қорғаумен қатар, қолданылатын құралдың өзі туындататын тәуекелдерді де қамтиды. Шифрлауды жалпы әлсірету, бақылаусыз қосымша көшірмелер қалыптастыру немесе материалды қорғалмаған арнамен беру тергеудің өзінен жаңа қолсұғушылық тәуекелін туындатуы мүмкін. Podchasov ісінде Еуропалық адам құқықтары соты шифрланған коммуникацияларға қол жеткізуді қамтамасыз ету үшін барлық пайдаланушыларға әсер ететін техникалық осалдық қалыптастыру қаупін бағалап, мұндай жалпы әлсіретудің мөлшерлестігіне күмән келтірді [108, § 76–80]. Бұл салыстырмалы талдау нақты объектіге бағытталған, заңды және бақыланатын алу тәсілдерін басым қолдану қажеттігін негіздейді. Тергеу тиімділігі бүкіл ақпараттық жүйенің қорғанысын әлсірету есебінен қамтамасыз етілмеуі тиіс.

ЖТӘ нәтижесінің уәкілетті бөлімшеден берілуі оны автоматты түрде дәлелденген факт етпейді. ҚПК-нің 237-бабы материалдарды ұсынуды, 238-бабы зерттеу мен хаттамалауды, 239-бабы бағалау мен дәлелдеуде пайдалануды реттейді. Нәтижені зерттеуге қажетті жағдайда маман тартылып, маңызы бар нақты деректер хаттамаға қоса беріледі. Демек, ілеспе хат, тасымалдағыш, зерттеу хаттамасы және техникалық қосымшалар өзара сәйкестікте қарастырылуы тиіс. Материалдың қай әрекеттен, қай уақыт аралығында және қандай нысанадан алынғаны анықталмай қалса, оның шығу

тегі мен заңдылық шегін тексеру қиындайды [6].

Ұсынылатын беру тәртібі материалдың сәйкестендіргішін, файлдар тізімін, жазу аралығын, үзілген тұстарды, көшірме қалыптастырылған уақытты, пайдаланылған форматты және тұтастықты тексеру деректерін қамтиды. Қызметтік құпияны қорғау қажеттігі дәлелдеменің мазмұны мен пайда болу жағдайын тексеруге жеткілікті ақпаратты негізсіз жасыруға әкелмеуі тиіс. Қорғалатын әдіс туралы толық техникалық мәліметті ашу мен дәлелдемені тексерудің барлық мүмкіндігін шектеудің арасында процестік заң рұқсат ететін шешімдер ізделеді: қорғалған танысу, тиісті бөлікті көрсету, түсіндірме алу және сараптамалық тексеру.

ҚПК-нің 239-бабы құпия тіркелген сөздері немесе әрекеттері дәлелдеуде пайдаланылатын адамнан бұл туралы міндетті түрде жауап алуды көздейді. Осы талап жазбаны адамның түсіндірмесімен, әңгіме контекстімен және ықтимал балама мағынамен салыстыруға мүмкіндік береді. Үзіндіні ғана тыңдау, дыбыстың кімге тиесілігін болжаммен шешу немесе техникалық үзілісті түсіндірместен алып тастау нәтижені біржақты бағалау қаупін күшейтеді. Тергеуші толық жазба мен пайдаланылатын үзіндінің арақатынасын, іріктеу өлшемін және аударма жасалған болса оның негізін көрсетеді [6].

ҚПК-нің 240-бабында қылмыстық іске тіркелмеген материалдармен танысу, заңда көзделген жағдайларда мүдделі тұлғаларды хабардар ету және шағымдану мүмкіндіктері қарастырылған, ал 241-бапта жасырын тергеу әрекеттеріне қатысты ақпарат пен жеке өмірге байланысты мәліметтердің құпиялылығын қамтамасыз етуге бағытталған талаптар белгіленген. Осыған байланысты материалдардың қылмыстық іске қатысы жоқ деп бастапқы бағалануы олардың күдіктіні ақтайтын немесе оның жауаптылығын жеңілдететін мән-жайларды анықтау үшін ықтимал маңызын тексерместен жоюға негіз болмауы тиіс. Мұндай материалдарды сақтау және жою мәселелері заңда белгіленген процестік тәртіпті, мүдделі тұлғаларды хабардар ету талаптарын және тиісті өтінішхаттар мен шағымдарды қарау мүмкіндігін ескере отырып шешілуі қажет. Бұл ретте ақпараттың құпиялылығын қамтамасыз ету процестік бақылауды шектеуге емес, оны жүзеге асыру барысында адамның құқықтары мен заңды мүдделеріне қосымша зиян келтірудің алдын алуға бағытталуы тиіс [6].

Yüksel Yalçınkaya ісінде цифрлық мәліметтердің айыптау үшін шешуші маңызы, бастапқы деректерге қорғау тарапының қол жеткізу мүмкіндігі, олардың тұтастығы мен сенімділігін тексеру, сондай-ақ ұлттық соттардың осы мәселелер жөніндегі қарсылықтарға жеткілікті жауап беруі әділ сот талқылауы тұрғысынан бағаланды [109, § 326–330, 333–341]. Сот цифрлық деректердің көлемі мен техникалық күрделілігі олардың негізінде жасалған айыптаушы тұжырымдарды қорғау тарапының тиімді тексеру мүмкіндігін жоққа шығармауы тиіс екенін көрсетті. Бастапқы деректерге қолжетімділік шектелген жағдайда мұндай шектеу жеткілікті процестік кепілдіктермен өтеліп, қорғау тарапына деректердің шығу тегіне, тұтастығына, сенімділігіне және олардан жасалған қорытындыларға тиімді түрде қарсылық білдіруге

нақты мүмкіндік берілуі қажет [109, § 326–330, 333–341]. Бұл ұстаным шифрланған қосымшаны пайдалану фактісінен қылмыстық кінә туралы автоматты қорытынды шығаруға болмайтыны жөніндегі осы зерттеудің атрибуция қағидатымен үйлеседі. БҰҰ Адам құқықтары жөніндегі комитетінің № 32 жалпы түсіндірмесі тараптардың теңдігі қағидатын әр тарапқа қарсы тарап ұсынған дәлелдерге дау айтуға тең мүмкіндік берілуімен байланыстырады [110]. Сонымен қатар қорғануға жеткілікті уақыт пен мүмкіндік құқығы айыпталушыға қарсы сотта пайдаланылатын құжаттар мен өзге де дәлелдемелерге қол жеткізуді қамтиды [110]. Сондықтан цифрлық ортадағы дәлелдемелердің техникалық күрделілігі қорғану құқығын әлсіретуге емес, керісінше, оларды тиімді тексеруге мүмкіндік беретін процестік кепілдіктерді нақтылауға негіз болуы тиіс.

Дәлелдемені бағалаудың бірінші деңгейі оның қандай фактіні растауға немесе теріске шығаруға қатысты екенін анықтайды. Екінші деңгейде деректі кім, қандай өкілеттікпен, қандай тәсілмен алғаны және заң талаптарының сақталғаны тексеріледі. Үшінші деңгейде оның мазмұнының шынайылығы, тұтастығы мен дұрыс түсіндірілгені бағаланады. Соңында барлық дәлелдемелер жиынтығының тиісті тұжырым жасауға жеткіліктілігі анықталады. Бұл рет логикалық талдау моделі ретінде ұсынылады; ол ҚПК-нің 112 және 125-баптарындағы өлшемдерді алмастырмайды [6; 44].

Хэштің болмауы, уақыт белдеуінің көрсетілмеуі немесе экспорт сипаттамасының жеткіліксіздігі бірдей құқықтық салдарға әкелмейді. Хэштің жоқтығы байттық сәйкестікті тексеруді қиындатуы мүмкін, бірақ заңда кез келген цифрлық объектіге хэш есептеудің әмбебап міндеті белгіленбесе, бұл кемшілік өздігінен автоматты түрде жол берілмейтіндік туғызбайды. Оның деректің анықтығына, шығу тегін тексеруге және тараптардың құқықтарына әсері бағаланады. Ал міндетті санкцияның болмауы сияқты заңдық ақауды кейін есептелген хэшпен түзету мүмкін емес. Техникалық дұрыстық заңдық өкілеттіктің орнына жүрмейді [6; 76].

Сақтау тізбегіндегі үзіліс те мазмұнды талдауды қажет етеді. Тасымалдағыштың кімде болғаны көрсетілмеген кезеңде өзгерту мүмкіндігі болған-болмағаны, тәуелсіз бақылау жазбаларының сақталғаны, хэштердің сәйкестігі және бастапқы дерекпен салыстыру мүмкіндігі тексеріледі. Егер объектінің шығу тегін анықтау мүмкін болмаса немесе бұзушылық ҚПК-нің 112-бабында көзделген салдарға әкелсе, жол берілмейтіндік мәселесі шешіледі. Егер түсіндіруге болатын құжаттау кемшілігі ғана болса, оның анықтық пен дәлелдемелік салмаққа әсері жеке негізделеді. Тергеушінің субъективті сенімі жетіспейтін тіркеу деректерінің орнын толтырмайды.

8-кесте – Цифрлық дәлелдемеге қатысты ақауларды саралап бағалау

№	Ақау немесе қарсылық	Бастапқы бағалау мәселесі	Қажетті тексеру	Ықтимал процестік салдар
1	Міндетті санкция жоқ	Алу заңдылығы	Әрекет түрі, ерекше тәртіп негізі, санкциялау құжаттары	ҚПК талаптарына қарай жол берілмейтіндік; хэш ақауды түзетпейді

№	Ақау немесе қарсылық	Бастапқы бағалау мәселесі	Қажетті тексеру	Ықтимал процестік салдар
2	Дереккөз белгісіз	Шығу тегі және тексерілу мүмкіндігі	Бастапқы файл, ұсынушы, алу жағдайы	Шығу тегі анықталмайтын дерекке ҚПК-нің 112-бабы тұрғысынан баға
3	Хэш көрсетілмеген	Тұтастықты тексерудің жеткіліктілігі	Басқа бақылау деректері, бастапқы нұсқа, нақты өзгеріс белгілері	Автоматты алып тастау емес; нақты әсеріне қарай шешім
4	Уақыттар сәйкес емес	Анықтық және түсіндіру	Уақыт белдеуі, сағат ауытқуы, экспорт пен көшірме уақыты	Түсіндіруді толықтыру немесе тұжырымның дәлелдемелік салмағын қайта бағалау
5	Сақтау тізбегінде үзіліс	Өзгеру мүмкіндігі, шығу тегі	Қолжетімділік журналы, хэш, беру есебі, тәуелсіз көшірме	Бұзушылық сипаты мен ҚПК-дегі өлшемдерге сай негізделген шешім
6	Қорғануға маңызды бөлік ашылмаған	Тараптардың құқықтары	Құпиялылық негізі, танысу тәсілі, іріктеу мен толық контекст	Құқықты қамтамасыз ету; бұзушылықтың дәлелдеуге ықпалын бағалау
7	Құрал әдісі түсіндірілмеген	Зерттеу нәтижесінің анықтылығы	Нұсқа, әдіс жарамдылығы, қателер мен балама түсіндірмелер	Түсіндірме, қосымша не қайталама зерттеу мәселесін шешу

Ескерту: ҚПК-нің 112, 125, 235 және 239-баптары [6], Жоғарғы Соттың дәлелдемелер жөніндегі түсіндірмесі [44] негізіндегі авторлық жүйелеу. Соңғы құқықтық салдар нақты істің мән-жайлары бойынша анықталады.

Зерттеу шеңберінде ұсынылатын процестік тексеру тәсілі қорғау тарапының әрбір қарсылығын қарау барысында төрт негізгі мән-жайды анықтауды көздейді: дауланатын процестік әрекетті немесе зерттеу объектісін айқындау, қолданылуға жататын құқықтық нормаларды белгілеу, орын алған бұзушылықтың сипаты мен оның құқықтық салдарын анықтау, сондай-ақ қабылданған процестік шешімнің негізділігін қамтамасыз ету. Дәлелдеменің заңды жолмен алынғаны туралы тұжырым оны алу және бекіту барысында заң талаптарының сақталғанын растайтын нақты мән-жайларды тексерумен негізделуі тиіс. Сонымен қатар қорғаушының арнайы техникалық білімінің болмауы оның дәлелдемелерге қатысты сұрақтарын қараудан бас тартуға негіз бола алмайды. Егер мұндай сұрақтар дәлелдемелердің анықтығын, жол берілетіндігін немесе оларды тексеру мүмкіндігін анықтауға бағытталса, тиісті түсініктемелер беру не арнайы білімді пайдалану қажеттілігі қарастырылуы тиіс [6].

Жоғалған логты кейін жасалған қызметтік анықтамамен толықтыру бастапқы жазбаның бар болғанын және оның нақты мазмұнын автоматты түрде дәлелдемейді. Сол сияқты заңсыз алынған файлдан жасалған жаңа көшірме дербес заңды көз ретінде көрсетілмеуі тиіс. Егер ақпарат кейін басқа, тәуелсіз және заңды көзден алынса, оның шығу тегі мен алыну негізі бөлек тексеріледі; бұрынғы бұзушылық жаңа рәсім туралы мәліметтің ішіне жасырылмайды. Заңдық салдар нақты іс бойынша қолданылатын ұлттық нормаларға сүйеніп анықталады, шетелдік құқықтағы дәлелдемені алып тастау доктриналары механикалық түрде көшірілмейді [6; 44].

Сарапшы қорытындысы мен бастапқы цифрлық деректердің арақатынасы да тексерілуі қажет. Сарапшы белгілі файлдың құрылымын, өзгерістерін немесе техникалық байланысын анықтай алады, бірақ оның қорытындысы бастапқы объектінің заңсыз алынуын заңдастырмайды. Сонымен қатар бастапқы объектіге қатысты әрбір техникалық сұрақ сараптаманың барлық қорытындысын жоққа шығармайды: мәселе қай тұжырымға әсер ететіні нақтыланады. Қорытындыда құралдың шектеуі, нәтиженің ықтимал түсіндірмелері және шешілмеген сұрақтар көрсетілсе, сот оны өзге дәлелдемелермен саналы түрде салыстыра алады [6; 86; 87].

Сот статистикасы бойынша ақталған адамдар санын цифрлық дәлелдемелердің жол берілмейтіндігімен тікелей байланыстыруға болмайды. Ұсынылған жинақталған есептерде ақтау себептерінің осы өлшем бойынша жіктемесі жоқ. Мұндай байланысты дәлелдеу үшін сот актілерін арнайы мазмұндық талдау және әрбір ақауды бірізді кодтау қажет болар еді. Осы тарауда ол зерттеу жүргізілді деп мәлімделмейді. Қолда бар көрсеткіштер процестік сапа мәселесін қоюға мүмкіндік береді, ал нақты себеп-салдар қорытындысының орнына жүрмейді [21; 22].

Бұлттық сервистегі деректің орналасуы, оны бақылайтын ұйымның тіркелген жері және қызметті пайдаланушының орналасуы сәйкес келмеуі мүмкін. Сондықтан трансшекаралық элемент сервердің шетелде болуымен ғана анықталмайды. Тергеу органы қандай ұйым мәліметті ұсына алатынын, оған қай мемлекеттің құқығы қолданылатынын, қандай халықаралық шарт немесе ұлттық рәсім сұратуды орындауға мүмкіндік беретінін және алынған материалды Қазақстанда қалай бекіту керектігін анықтайды. Дербес деректердің трансшекаралық берілу режимі қылмыстық істер бойынша құқықтық көмек тәртібімен бірге қаралады [2; 6; 37].

Будапешт конвенциясы компьютерлік деректерді жедел сақтап қалуды, ұсынуды талап етуді, сақталған деректерді іздеу мен алуды және халықаралық ынтымақтастықты өзара байланысты құралдар ретінде қарастырады [111]. Оның түсіндірме баяндамасы сақтап қалу мен жария ету арасындағы айырманы ашады [112]. Сақтап қалу деректі жоюдан қорғауға бағытталған, ал оны тергеу органына беру дербес құқықтық негізді талап етеді. Осы айырма 2.1 бөлімдегі уақытқа сезімтал іздер проблемасын шешуге көмектеседі: құқықтық көмек жауабын күту кезінде ақпаратты сақтап қалу мәселесі мүмкіндігінше ерте қойылады.

Қазақстанның халықаралық шартқа қатысу мәртебесі әрбір ұсыныстың қолданылу шегін анықтайды. Еуропа Кеңесінің 2026 жылғы 15 қыркүйекте тексерілген ресми тізімінде Қазақстан Будапешт конвенциясының тараптары қатарында емес, қол қойған және қосылуға шақырылған бақылаушы мемлекеттер санатында көрсетілген [113]. Сондықтан Конвенцияның тетіктері Қазақстан үшін толық іске қосылған шарттық өкілеттік ретінде ұсынылмайды. Оның ережелері салыстырмалы үлгі ретінде талданады, ал нақты сұрату Қазақстанға және сұрау салынатын мемлекетке қолданылатын құқықтық негізбен жіберіледі.

Конвенцияның 32-бабындағы ашық деректерге немесе заңды әрі ерікті

келісім арқылы қол жеткізу ережесі шетелдік серверді шексіз зерттеуге рұқсат бермейді. Келісім берушінің деректерді ашуға заңды өкілеттігі, келісімнің көлемі және ақпаратқа қол жеткізу сипаты тексерілуі тиіс. Қазақстанға қатысты шарттық мәртебе жөніндегі алдыңғы шектеу бұл бапты қолдану мәселесінде де сақталады. Техникалық қолжетімділік, пайдаланушының паролі немесе сервистің веб-интерфейсі халықаралық юрисдикция мәселесін өздігінен шешпейді [111; 112].

Будапешт конвенциясының Екінші қосымша хаттамасы домендік атауды тіркеу туралы ақпаратты тікелей сұрату, абоненттік ақпаратты қызмет көрсетушіден алу, төтенше жағдайда сақталған компьютерлік деректерді жедел ашу және өзге де күшейтілген халықаралық ынтымақтастық құралдарын көздейді [114]. Оның түсіндірме баяндамасы мұндай сұратулардың нақты қылмыстық іс немесе іс жүргізу шеңберімен байланысын, құзыретті органды, сұратылатын деректер санатын және орындау шарттарын нақтылайды [115]. Хаттаманың 14-бабы дербес деректерді қорғаудың арнайы кепілдіктерін белгілейді [114]. Осы модельден шығатын әдіснамалық нәтиже – дерек санаттарын ажырату, құзыретті органды айқындау, мақсатты шектеу және берілген ақпараттың кейінгі пайдаланылуы мен қорғалуын бақылау. Аталған үлгі Қазақстан үшін оның Конвенция мен Хаттамаға қатысу мәртебесі ескеріліп, салыстырмалы-құқықтық бағдар ретінде қарастырылады.

ЕО-ның 2023/1543 регламенті электрондық дәлелдемені ұсыну және сақтап қалу жөніндегі еуропалық ордерлерді енгізеді; оның қолданылуы 2026 жылғы 18 тамыздан басталады. Құжатта ұсынудың жалпы тәртібіне байланысты он күндік және төтенше жағдайдағы сегіз сағаттық мерзімдер қарастырылған [116]. 2023/1544 директивасы тиісті мекемелер мен заңды өкілдерді белгілеу арқылы сұратудың нақты адресатын қамтамасыз етуге бағытталған [117]. Бұл мерзімдерді Қазақстандағы сұратуға тікелей көшіруге болмайды. Салыстыру үшін маңыздысы – жеделдікпен қатар орындалатын адресат, дерек санаты, бақылау және бас тарту негіздерінің бір жүйеде реттелуі.

Қылмыстық қудалау мақсатындағы өңдеуді жалпы коммерциялық өңдеу режимімен теңестіру де қате болады. ЕО құқығында құзыретті органдардың қылмыстық-құқықтық мақсаттар үшін деректерді өңдеуі арнайы 2016/680 директивасымен реттеледі [118]. Сондықтан бірінші тарауда пайдаланылған GDPR қағидаттары салыстырмалы тұрғыдан пайдалы болғанымен, оларды қылмыстық тергеуге ешбір айырмашылықсыз қолданылатын жалғыз акт деп көрсетуге болмайды [9]. Қазақстан үшін бұл айырма тергеу органының өзіндегі деректерді өңдеудің мақсаты, қолжетімділігі және сақталуы жөніндегі арнайы кепілдіктерді негіздеуге көмектеседі.

БҰҰ Бас Ассамблеясының 2024 жылғы 24 желтоқсандағы 79/243 қарарымен қабылданған Киберқылмысқа қарсы конвенция электрондық нысандағы дәлелдемелермен алмасуды жаһандық деңгейде реттеуге бағытталған [119]. Алайда халықаралық құжаттың қабылдануы, оған қол

қою, ратификациялау және нақты мемлекет үшін күшіне енуі – әртүрлі заңдық фактілер. Сондықтан тергеуші жалпы халықаралық үрдіске сүйеніп өкілеттік тұжырымдамай, сұрату жіберілетін күні қолданылатын шарттық негізді анықтауы тиіс. Осы талап халықаралық ынтымақтастықтың тиімділігі мен алынған дәлелдеменің кейінгі тексерілуін бірдей қамтамасыз етеді.

M.N. (EncroChat) ісінде басқа мемлекетте бұрын жиналған дәлелдемені беру мен оны бастапқы жинаудың құқықтық шарттары ажыратылып, соттық бақылау және тараптың мәліметке тиімді түсініктеме беру мүмкіндігі қарастырылды [120]. Бұл шешімнен ұлттық зерттеу үшін туындайтын қорытынды – шетелден ресми арнамен келу деректің барлық сапалық мәселесін шешпейді. Қазақстанда алынған материалдың қандай әрекетпен қалыптасқаны, бастапқы дерекпен байланысы, аудармасы, тұтастығы және қорғау тарапының тексеру мүмкіндігі ұлттық процестік талаптармен бағаланады.

Осыған байланысты зерттеу шеңберінде трансшекаралық сұратуларды дайындау кезінде қылмыстық істің құқықтық негізін, құзыретті органды, сұратылатын деректердің санаты мен сәйкестендіру белгілерін, уақыт аралығын, деректерді сақтау қажеттілігін, оларды берудің құқықтық және техникалық шарттарын, сондай-ақ құпиялылық талаптарын нақты көрсету ұсынылады. Алынған жауаптың толықтығы мен ұсынылған мәліметтердің сәйкестігі тексеріліп, қажет болған жағдайда қосымша ақпарат сұратылуы тиіс. Бұл тәсіл халықаралық шарттарда белгіленген тәртіпті алмастырмай, трансшекаралық сұратулардың негізділігін және алынатын цифрлық дәлелдемелердің толықтығын қамтамасыз етуге бағытталған.

Трансшекаралық жағдайда сақтау тізбегі беруші ұйымнан немесе шетелдік органнан басталып, қазақстандық істегі зерттеуге дейін жалғасады. Аралық аудару, форматты өзгерту немесе архивті ашу бастапқы файлдың орнына жаңа объект қалыптастырса, олардың байланысы тіркеледі. Түпнұсқа тілдегі ақпарат сақталып, аударма бөлек туынды құжат ретінде беріледі. Құқықтық көмек рәсімінің талаптары мен техникалық есеп бірін-бірі толықтырады: біріншісі алудың өкілетті негізін, екіншісі қандай ақпарат алынғанын және оның қалай өзгергенін түсіндіруге мүмкіндік береді [6; 76].

Жасырын тергеу әрекеттерінің заңдылығы нақты әрекет түрінің ҚПК-дегі негізіне, қылмыстың сарапануына, санкциялау тәртібіне, нысана мен мерзімнің шегіне және кейінгі бақылауға тәуелді. Құқықтарды шектеу туралы шешім айқын дәлелдеу міндетімен негізделуі тиіс. Мөлшерлестік тек бастапқы рұқсат кезінде емес, деректерді іріктеу, зерттеу, беру және сақтау барысында да қамтамасыз етіледі.

Жол берілетіндік пен анықтық өзара байланысты, бірақ дербес бағаланады. Техникалық кемшіліктің салдары оның нақты әсерімен анықталады; міндетті құқықтық рәсімнің бұзылуы техникалық құралмен заңдастырылмайды. Хэш, метадеректер және сақтау тізбегі тексерудің маңызды құралдары болғанымен, санкцияны, тараптардың құқықтарын немесе дәлелдемелерді жиынтықта бағалауды алмастырмайды. Ұсынылған бағалау матрицасы әр ақауды тиісті құқықтық мәселемен байланыстырып,

шешімді уәждеуге арналған.

Трансшекаралық ынтымақтастықта деректі сақтап қалу мен оны берудің құқықтық негіздері ажыратылып, халықаралық шарттың нақты қолданылу мәртебесі тексерілуі қажет. Шетелдік және халықаралық үлгілер Қазақстан үшін салыстырмалы бағдар береді, ұлттық өкілеттіктерді өздігінен кеңейтпейді. Екінші тарауда негізделген кезеңдік модель, ең аз дәлелдемелік пакет және құқықтарды шектеуді бағалау өлшемдері үшінші тарауда арнайы қорғау режимі мен заңнаманы жетілдіру ұсыныстарын әзірлеудің процестік негізін құрайды.

3 ТЕРГЕУ ТИІМДІЛІГІ МЕН ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУДЫ КҮШЕЙТУДІҢ ҚЫЛМЫСТЫҚ-ПРОЦЕСТІК КЕПІЛДІКТЕРІ

3.1 Қылмыстық процесте дербес деректермен жұмыс істеудің арнайы процестік режимі

Дербес деректерге қатысты қылмыстық құқық бұзушылықтарды тергеп-тексерудің тиімділігі мәліметті уақтылы алумен қатар, оны пайдаланудың құқықтық шектерін сақтауға тәуелді. Бірінші тарауда анықталған қылмыстық-құқықтық белгілер алынатын ақпараттың дәлелдеу пәнімен байланысын айқындайды. Екінші тарауда ұсынылған кезеңдік модель, дерек ұстаушылармен өзара іс-қимыл және цифрлық мәліметтерді бекіту тәртібі осы байланысты тексеруге мүмкіндік береді. Алайда заңды түрде алынған ақпарат кейіннен негізсіз көшірілсе, бөгде адамдарға ашылса немесе бастапқы мақсатынан тыс пайдаланылса, тергеудің өзі дербес деректерге жаңа қауіп туғызады. Сондықтан қорғау міндеті деректер алынған сәтпен аяқталмайды, ол қылмыстық іс бойынша ақпаратпен орындалатын кейінгі әрекеттерді де қамтуы тиіс.

Осы зерттеуде арнайы процестік режим деп қылмыстық іс үшін алынатын дербес деректердің мақсатын, көлемін, пайдаланушыларын, олармен жасалатын әрекеттерді және сақталу негіздерін айқындайтын, құқықтарды шектеу туралы шешімді тексеру мен оған шағым жасау мүмкіндігін қамтамасыз ететін өзара байланысты қылмыстық-процестік талаптар жүйесі түсініледі. Бұл анықтамада режимнің арнайы сипаты мәліметтің цифрлық нысанымен ғана шектелмейді. Қағаз медициналық құжат, бейнежазбадағы тұлға бейнесі және ақпараттық жүйедегі лог жеке адаммен байланыстырылған жағдайда бірдей құқықтық қорғауды қажет етеді. Техникалық тәсіл объектінің ерекшелігіне қарай өзгереді, ал заңдылық пен тексерілу талабы сақталады [1; 2; 6].

С. Уоррен мен Л. Брандейстің жеке өмірді қорғауға арналған классикалық еңбегі тұлғаның жеке саласына негізсіз араласу мен жеке сипаттағы мәліметтерді жария етуді дербес құқықтық қорғауды қажет ететін

мәселе ретінде қарастыруға негіз қалады [121, Б. 195–198]. Авторлар адамның өз ойлары, сезімдері мен жеке өміріне қатысты мәліметтердің қандай көлемде өзгелерге жеткізілетінін өзі айқындау мүддесін құқықтық қорғаумен байланыстырады [121, 198 б.]. Қазіргі қылмыстық процесс үшін бұл ұстанымның маңызы тұлға туралы мәліметті тек тергеуге қолайлы ақпараттық ресурс ретінде емес, дербес құқықтық мүдделермен байланысты объект ретінде қарастыру қажеттігінде. Сонымен бірге Уоррен мен Брандейстің жария етуге негізделген классикалық құпиялылық тұжырымдамасы қазіргі цифрлық өңдеуден туындайтын барлық тәуекелдерді толық қамтымайды. Деректер көпшілікке жария етілмеген күннің өзінде оларды мақсатсыз біріктіру, қате тұлғамен байланыстыру, бастапқы мақсаттан тыс қайта пайдалану немесе қажеттілік жойылғаннан кейін негізсіз сақтау адамның құқықтары мен заңды мүдделеріне әсер етуі мүмкін. Сондықтан қылмыстық процестегі дербес деректерді қорғау жария етуді шектеумен ғана емес, оларды жинау, байланыстыру, пайдалану және сақтау кезеңдеріндегі процестік кепілдіктермен де қамтамасыз етілуі тиіс.

Х. Ниссенбаумның контекстік тұтастық тұжырымдамасы құпиялылықты ақпараттың мүлдем таралмауымен емес, оның нақты әлеуметтік және институционалдық контекске сәйкес қозғалуымен байланыстырады. Автор ақпарат ағынының сәйкестігін оған қатысатын субъектілер, берілетін ақпараттың сипаты және оны бір тұлғадан екіншісіне берудің шарттары арқылы бағалауды ұсынады [122, 157 б.]. Контекстік ақпараттық нормалардың негізгі элементтері ретінде жіберуші, ақпарат субъектісі мен алушы, ақпараттың түрі және оны беруді шектейтін немесе рұқсат ететін қағидаттар қарастырылады [122, 146 б.]. Бұл тәсілді қылмыстық процеске бейімдеу бір мақсат үшін заңды түрде жиналған дербес деректерді өзге мақсатта пайдалану бастапқы құқықтық негіздің автоматты жалғасы болып табылмайтынын көрсетеді. Мысалы, медициналық көмек көрсету үшін жиналған деректі қылмыстық іс бойынша тергеу органына беру дербес құқықтық және процестік негізді талап етеді. Мұндай беру заңды болған күннің өзінде, сол мәліметті кейін баспасөз хабарламасына, ведомстволық таныстырылымға немесе өзге жария материалға енгізу бөлек бағаланатын әрекет болып қалады. Демек, деректермен жұмыс істеудің бір кезеңіндегі заңдылық оларды кейінгі барлық мақсатта пайдалануға автоматты түрде рұқсат бермейді. Осыған байланысты арнайы процестік режим деректердің бастапқы алыну мақсатын, кейінгі пайдалану мақсатын және бір контекстен екіншісіне ауысудың құқықтық негізін құжаттауды қамтамасыз етуі тиіс.

Д. Солове құпиялылыққа төнетін қауіптерді ақпаратты жинау, ақпаратты өңдеу, ақпаратты тарату және адамның жеке саласына тікелей араласу сияқты төрт негізгі топқа жүйелейді [123, Б. 490–491]. Ақпаратты өңдеу санатына автор деректерді біріктіруді, тұлғамен сәйкестендіруді, ақпараттық қауіпсіздіктің жеткіліксіздігін, деректерді бастапқы мақсаттан тыс қайта пайдалануды және тұлғаның өзі туралы ақпаратты өңдеу процесінен шеттетілуін жатқызады [123, Б. 490–491, Б. 506–522]. Ақпаратты таратуға байланысты қауіптер құпиялылықты бұзу, жария ету,

қолжетімділіктің кеңеюі және ақпаратты бұрмалау сияқты әртүрлі нысандарды қамтиды [123, Б. 522–552]. Осы жіктеуден зерттеу үшін маңызды әдіснамалық қорытынды туындайды: дербес деректерді қорғауды тек оларды «жарияламау» міндетімен шектеу жеткіліксіз. Құқыққа қауіп деректерді тарату сәтінде ғана емес, оларды шамадан тыс жинау, әртүрлі дереккөздерден біріктіру, қате тұлғамен сәйкестендіру немесе бастапқы мақсаттан тыс пайдалану кезеңінде де туындауы мүмкін. Сондықтан қылмыстық процестегі қорғау тетіктері деректермен жасалатын нақты әрекетке сәйкес саралануы тиіс. Артық жинау алынатын мәліметтің көлемін дәлелдеу пәні мен нақты процестік міндетке сәйкестендіру арқылы, қате сәйкестендіру дереккөз бен атрибуцияны тексеру арқылы, ал рұқсатсыз беру алушыны, беру мақсатын және оның құқықтық негізін тіркеу арқылы шектелуі қажет.

Б.Я. Копс дербес деректерді қорғауды тұлғаның өз мәліметтерін бақылау мүмкіндігімен және заңнамада белгіленген формалды талаптардың орындалуымен ғана байланыстырудың шектеулерін атап көрсетеді [124, Б. 250–254, Б. 259–261]. Ғалымның пікірінше, деректер субъектісіне өз мәліметтерін бақылау құқығын беру күрделі ақпараттық жүйелер жағдайында олардың тиімді қорғалуын толық қамтамасыз ете алмайды. Бұл тұжырым қылмыстық сот ісін жүргізу барысында ерекше маңызға ие, өйткені күдікті, жәбірленуші және өзге де қатысушылар дербес деректерінің сақталу тәртібін, ақпараттық жүйелердің техникалық құрылымын және оларға қол жеткізу шарттарын өз бетінше айқындай алмайды. Сонымен қатар қылмыстық процесте дербес деректерді жинау мен өңдеу көптеген жағдайларда тұлғаның келісіміне емес, заңда белгіленген процестік өкілеттіктерге негізделеді. Сондықтан дербес деректерді қорғаудың тиімділігі тек келісімнің болуымен немесе заңнама талаптарының формалды орындалуымен бағаланбауы тиіс.

М. Хильдебрандт құқықтық реттеу мен технологиялық жүйелердің өзара байланысын қарастыра отырып, ақпараттық технологиялардың құрылымы адамның құқықтары мен бостандықтарын іс жүзінде жүзеге асыру мүмкіндіктеріне тікелей ықпал ететінін көрсетеді [125, Б. 159–185]. Осыған байланысты ғалым құқықтық кепілдіктерді ақпараттық жүйелерді жобалау және әзірлеу кезеңінен бастап ескеруді көздейтін Legal Protection by Design тәсілін негіздейді [125, Б. 214–226].

Аталған ғылыми ұстанымдарды салыстырмалы талдау қылмыстық процесте дербес деректерді қорғаудың арнайы құқықтық режимі заңнамалық талаптар мен процестік кепілдіктерді белгілеумен ғана шектелмеуі тиіс деген қорытынды жасауға мүмкіндік береді. Олардың нақты орындалуын қамтамасыз ететін техникалық және ұйымдастырушылық тетіктерді де қалыптастыру қажет. Атап айтқанда, ақпаратқа қол жеткізуді процестік өкілеттіктерге сәйкес шектеу, рұқсаттарды нақты қылмыстық іспен байланыстыру, деректермен жүргізілген әрекеттерді тіркеу, артық көшірмелердің жасалуын болдырмау және тиісті өкілеттіктер тоқтатылғаннан кейін ақпаратқа қолжетімділікті шектеу дербес деректерді

қорғаудың құқықтық кепілдіктерін тәжірибеде іске асыруға бағытталуы тиіс.

Қазақстандағы бастапқы нормативтік негіз Конституциядағы жеке өмір мен дербес деректерді қорғау кепілдіктерінен, ҚПК-нің құқықтарды қорғау, жеке өмірге қол сұқпаушылық және құпиялықты сақтау нормаларынан құралады [1; 6]. «Дербес деректер және оларды қорғау туралы» заңның 9-бабы құқық қорғау органдары мен соттардың қызметі кезінде келісімсіз жинау мен өңдеуге жол береді [2]. Алайда бұл ережені кез келген мәліметті кез келген тәсілмен алуға арналған жалпы өкілеттік ретінде түсіндіруге болмайды. Қылмыстық іс жүргізудегі нақты әрекеттің негізі, оны жүзеге асыратын субъект және санкциялау тәртібі ҚПК бойынша айқындалады. Келісімнің талап етілмеуі процестік нысанның талап етілмеуін білдірмейді.

Бұл ретте дербес деректерді қорғау туралы салалық заңнаманың қолданылу аясы мен ерекшеліктерін ескеру қажет. Аталған Заңның 3-бабында мемлекеттік құпияларға жатқызылған дербес деректерге, сондай-ақ заңда белгіленген жағдайларда барлау, қарсы барлау және жедел-іздестіру қызметіне қатысты ерекшеліктер қарастырылған [2]. Осыған байланысты салалық заңнамада көзделген талаптарды тергеу және жедел-іздестіру қызметі барысында туындайтын барлық құқықтық қатынастарға бірдей қолдануға болмайды. Қылмыстық процесте дербес деректерді қорғаудың ұсынылатын құқықтық режимі ҚПК-де белгіленген процестік кепілдіктерге негізделіп, заңмен қорғалатын құпия мәліметтерге қатысты арнайы құқықтық режимдердің талаптарымен үйлестірілуі тиіс. Сонымен қатар жедел-іздестіру қызметі нәтижесінде алынған мәліметтерді қылмыстық іс бойынша дәлелдеу процесінде пайдалану кезінде олардың заңдылығын, анықтығын және жол берілетіндігін тексеру, сондай-ақ тиісті дербес деректердің қорғалуын қамтамасыз ету мәселелері ҚПК талаптарына сәйкес шешілуі қажет [6; 97].

Халықаралық деңгейде ЭЫДҰ-ның құпиялылық жөніндегі қағидаттары дербес деректерді жинау мен пайдалануды мақсатпен байланыстырып, кейінгі өңдеудің бастапқы мақсатпен үйлесімді болуын және деректерді өңдеуші субъектінің есептілігін талап етеді. Атап айтқанда, Purpose Specification Principle деректерді жинау мақсатын алдын ала айқындауды және кейінгі пайдалануды осы мақсатпен немесе онымен үйлесімді жаңа мақсатпен шектеуді көздейді [126], ал Use Limitation Principle деректерді бастапқы мақсаттан тыс ашуға немесе пайдалануға тек тиісті құқықтық негіз болғанда ғана жол береді [126]. Accountability Principle деректерді бақылаушы субъектінің осы қағидаттардың сақталуына жауапты болуын бекітеді [126]. Еуропа Кеңесінің полиция секторында дербес деректерді пайдалану жөніндегі практикалық нұсқаулығы аталған қағидаттарды қылмыстың алдын алу, тергеп-тексеру және қудалау жағдайында нақтылайды. Нұсқаулық деректерді өңдеудің заңды, қажетті және мөлшерлес болуын, оның алдын ала айқындалған мақсатпен байланысын және жиналған деректердің істің нақты міндеті үшін қажетті көлемнен аспауын талап етеді [127, Б. 3–4]. Сонымен қатар кейінгі пайдалану дербес жаңа өңдеу әрекеті ретінде қарастырылып, оның құқықтық негізі, мақсаты, қажеттілігі мен мөлшерлестігі қайта бағалануы тиіс [127, Б. 4–5]. Деректерді сақтау

қажеттілігі де өңдеудің бүкіл өмірлік циклі бойында мерзімді түрде қайта қаралуы керек [127, Б. 11–12]. Еуропа Кеңесінің R (87) 15 ұсынымы полиция секторындағы дербес деректерді өңдеудің негізгі кепілдіктерін ертерек жүйелеп, сыртқы тәуелсіз бақылауды, деректерді жинау мен сақтаудың мақсатқа сәйкестігін, ақпарат сапасын, пайдалануды шектеуді және сақтау мерзімін қайта қарауды көздеді [128]. Осы құжатта полиция секторынан тыс тәуелсіз қадағалау органы болуы қажеттігі арнайы көрсетілген [128]. Аталған халықаралық актілер Қазақстан үшін жаңа тергеу өкілеттіктерін автоматты түрде туындатпайды. Олардың салыстырмалы-құқықтық маңызы жалпы деректерді қорғау қағидаттарын нақты басқару міндеттеріне айналдыруында. Қылмыстық іс шеңберінде қандай деректердің жиналғаны, олардың қандай мақсат үшін пайдаланылатыны және сақталатыны, кімге және қандай құқықтық негізбен берілгені, сондай-ақ олардың әрі қарай сақталу қажеттілігі қашан және қандай өлшемдер бойынша қайта қаралатыны тексерілуі тиіс. Осы тұрғыдан арнайы процестік режим деректердің қозғалысын ғана емес, әрбір кейінгі пайдалану әрекетінің мақсаты мен құқықтық негізін құжаттауды қамтамасыз етуі қажет.

Арнайы режимнің объектілерін тек «ашық» және «қолжетімділігі шектеулі» деректерге бөлу жеткіліксіз. Бірінші тарауда қарастырылған салалық жіктеу деректің жалпы қолжетімділік мәртебесін сипаттайды. Қылмыстық іс ішінде қосымша екі өлшем қажет: мәліметтің дәлелдеу үшін маңызы және оны пайдаланудан тұлғаға келетін қауіп. Интернетте бұрын жарияланған мекенжай қудалау қаупі туындаған куә үшін жоғары тәуекелді болуы мүмкін. Керісінше, құпия ақпараттағы бір техникалық белгі айыптауды тексеру үшін шешуші мәнге ие болса, оны қорғау тарабына ашу мәселесі нақты процестік кепілдіктермен шешілуі тиіс.

Осыған байланысты зерттеу шеңберінде қылмыстық іс материалдарына енгізілетін мәліметтерді төрт функционалдық топқа бөлу ұсынылады: дәлелдеу үшін қажетті деректер; олардың шығу тегі мен тұтастығын тексеруге мүмкіндік беретін мәліметтер; қылмыстық іске қатыстылығы әлі анықталмаған ақпарат; қылмыстық процеске қатысушылардың қауіпсіздігін немесе заңмен қорғалатын құпияны қамтамасыз етуді талап ететін деректер. Аталған топтар заңнамада белгіленген дербес деректер санаттарын алмастырмайды және бір-бірімен өзара байланысты болуы мүмкін. Мәселен, адамның орналасқан жері туралы мәліметтер бір мезгілде дәлелдемелік маңызға ие болып, оның қауіпсіздігіне қатысты тәуекелдер туындатуы мүмкін. Сондықтан мұндай мәліметтерге қатысты процестік шешімдер олардың дәлелдемелік маңызы мен қорғау қажеттілігін ескере отырып қабылдануы тиіс.

9-кесте – Деректердің процестік қызметі мен қорғау қажеттілігін саралау

№	Деректер тобы	Негізгі сұрақ	Ұсынылатын кепілдік
1	Дәлелдеу үшін қажетті дерек	Қандай мән-жайды анықтайды?	Қатыстылықты негіздеу; қажетті контексті сақтау

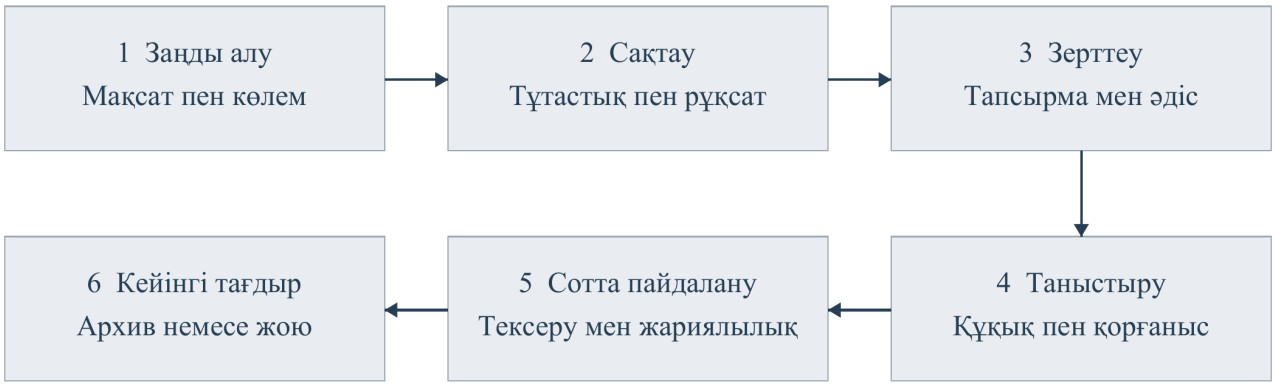
№	Деректер тобы	Негізгі сұрақ	Ұсынылатын кепілдік
2	Шығу тегі мен тұтастық деректері	Нәтижені қайта тексеруге бола ма?	Метадерек, тізімдеме, хэш және алу жағдайын тіркеу
3	Ілеспе, қатыстылығы анықталмаған мәлімет	Оны зерттеу мен сақтауға негіз бар ма?	Іріктеуді негіздеу; қолжетімділікті шектеу; мәртебені қайта қарау
4	Қауіпсіздікке немесе ерекше құпияға қатысты дерек	Ашу кімнің қандай құқығына қауіп төндіреді?	Заңды арнайы режим; қорғалған танысу; уәжді шешім

Ескерту: Авторлық жүйелеу. Топтар өзара қабаттасуы мүмкін; заңдағы дербес деректер санаттарын алмастырмайды. Негіз: [2; 6; 127].

Деректердің ерекше сезімталдығы олардың дәлелдемелік қажеттілігін жоққа шығармайды, бірақ оларды алу мен пайдаланудың негізділігіне қойылатын талапты күшейтеді. Z v. Finland ісінде медициналық мәліметтердің құпиялылығы мен қылмыстық құқық бұзушылықтарды тергеп-тексеру және сот төрелігінің қажеттіліктері арасындағы арақатынас қарастырылды [129, Б. 22–23]. Avilkina and Others v. Russia ісінде медициналық ақпаратты мемлекеттік органға беру кезінде нақты қоғамдық қажеттіліктің болуы, араласудың негізділігі және балама тәсілдердің мүмкіндігі бағалануы тиіс екені көрсетілді [130, Б. 13–15]. Осы ұстанымдар негізінде ұлттық практикада толық медициналық құжаттаманы алу қажеттілігі мен нақты кезеңге немесе мән-жайға қатысты жекелеген мәліметтерді алудың жеткіліктілігін бөлек бағалау ұсынылады. Егер толық құжатты алу қажет болса, оның көлемі мен қажеттілігі процестік шешімде нақты негізделуі тиіс.

Биометриялық және генетикалық деректерді қорғау мәселесіне қатысты Еуропалық Одақ Сотының C-205/21 ісі бойынша шешімінде айыпталушылардың мұндай мәліметтерін жүйелі түрде жинау қатаң қажеттілік талабына сәйкес жүзеге асырылуы тиіс екені көрсетілген [131, Б. 24–25]. Сот адамның айыпталушы мәртебесіне ие болуы биометриялық және генетикалық деректерді жинаудың қажеттілігін өздігінен негіздемейтінін атап өткен. Сонымен қатар Еуропалық деректерді қорғау кеңесінің (EDPB) құқық қорғау қызметінде бет-әлпетті тану технологияларын қолдану жөніндегі нұсқаулығында биометриялық деректерді өңдеудің нақты мақсатын айқындау, қажеттілік пен мөлшерлестік қағидаттарын сақтау және тиісті құқықтық кепілдіктерді қамтамасыз ету талаптары қарастырылған [132]. Аталған халықаралық тәжірибені талдау Қазақстан Республикасының тергеу практикасында биометриялық деректерді жаппай жинау мен салыстырудың орнына оларды пайдаланудың нақты процестік мақсатын, зерттелетін деректердің көлемін және қате сәйкестендіру нәтижелерін тексеру тәртібін негіздеу қажеттігін көрсетеді. Бұл ретте шетелдік құқықтық актілерде белгіленген талаптар Қазақстан Республикасында тікелей қолданылатын құқықтық нормалар ретінде емес, ұлттық қылмыстық-процестік заңнаманы жетілдіруге бағытталған салыстырмалы-құқықтық негіз ретінде қарастырылуы тиіс.

Режимнің үздіксіздігі деректі алу, сақтау, зерттеу, тараптарға ұсыну, сотта пайдалану және іс аяқталғаннан кейінгі тағдырын шешу кезеңдерінің өзара байланысын білдіреді. Әр ауысу кезінде бұрынғы құқықтық негіздің жаңа әрекетке жеткіліктілігі тексеріледі. Мәселен, сарапшыға берілген тасымалдағыштың зерттеу көшірмесін оқу мақсатындағы базаға енгізу бастапқы тапсырмадан туындамайды. Сол сияқты тергеу үшін заңды алынған бейнежазбаны ведомстволық таныстырылымда көрсету бөлек бағалауды қажет етеді. Нысаналы пайдаланудың шегі файлдың қай органда тұрғанына емес, орындалатын әрекеттің мақсатына байланысты анықталады.



4-сурет – Дербес деректерді процестік қорғаудың толық циклі

NIST Privacy Framework құпиялылық тәуекелін ұйым қызметінің бүкіл циклімен байланыстыруға мүмкіндік береді [133, 12 б.]. NIST IR 8062 қауіпсіздік инцидентінсіз де тұлғаға теріс салдар туғызатын өңдеу жағдайларын қарастырады [134]. Осы айырмашылық қылмыстық процесс үшін маңызды: ақпараттық жүйеге сырттан шабуыл жасалмай-ақ, уәкілетті қызметкер деректі қызметтік міндетіне қатысы жоқ мақсатпен іздеуі мүмкін. Демек, жүйенің бұзылмауы дербес деректер режимінің сақталғанын толық дәлелдемейді. Заңдылықты бағалау нақты пайдаланушының құзыреті мен нақты іздеудің мақсатын қамтуы тиіс.

Әр қылмыстық іс бойынша деректерді өңдеу туралы қысқа есептік жазба жүргізу ұсынылады. Онда дереккөз, алу негізі, мақсат, мәлімет санаты, сақтау орны, негізгі пайдаланушылар және қайта қарау оқиғасы көрсетіледі. Бұл есеп дербес деректердің мазмұнын қайталап жинайтын жаңа тізілімге айналмауы керек. Оның міндеті бұрыннан бар процестік құжаттар мен техникалық журналдардың арасындағы байланысты қамтамасыз ету. Электрондық іс жүйесінде есептік жазба қаулыға, хаттамаға және тасымалдағыштың тізімдемесіне сілтеме жасай алады. Мұндай ұйымдастыру қолданыстағы қылмыстық сот ісін электрондық форматта жүргізу нұсқаулығымен үйлестірілуі тиіс [135].

А. Кавукян, С. Тейлор және М. Абрамс Privacy by Design қағидатын ұйымның есептілігімен байланыстырып, дербес деректерді қорғау тетіктерін ақпараттық жүйелер мен ұйымдық процестерге олардың бастапқы жобалану кезеңінен енгізудің маңызын көрсетеді [136, Б. 408–409]. EDPB-ның жобалау кезіндегі және әдепкі деректерді қорғау жөніндегі нұсқаулығында әдепкі

параметрлер нақты мақсатқа қажетті деректер көлемімен шектелуге, ал қызметкерлердің қолжетімділігі олардың рөлі мен нақты қажеттілігіне қарай сараланууы тиіс екені көрсетілген [137, Б. 11–13]. Осы ұстанымдарды қылмыстық іс жүргізудің электрондық жүйесіне бейімдеу жаңа пайдаланушыға барлық істерге қолжетімділікті автоматты түрде бермеуді, сондай-ақ іс материалдарымен танысу құқығы мен оларды жүйеден сыртқа шығару құқығын бөлек реттеуді талап етеді. Сонымен қатар ақпаратқа қол жеткізуді бастапқы шектеу ҚПК-де көзделген қылмыстық процеске қатысушылардың құқықтарын жүзеге асыруға кедергі келтірмеуі тиіс. Тиісті процестік құқық туындаған жағдайда ақпараттық жүйе оны уақтылы және толық көлемде іске асыру мүмкіндігін қамтамасыз етуі қажет.

Ақпараттық жүйелердегі деректерге қол жеткізуді қызметкердің лауазымдық мәртебесіне қарай ғана шектеу дербес деректерді қорғаудың жеткілікті кепілі болып табылмайды. NIST SP 800-162 стандартында атрибуттарға негізделген қолжетімділікті басқару субъектінің, ақпараттық объектінің, сұратылатын әрекеттің және оны жүзеге асыру жағдайларының ерекшеліктерін кешенді бағалауға негізделетіні көрсетілген [138, 7 б.]. Аталған тәсілді қылмыстық сот ісін жүргізуге бейімдеу барысында қызметкердің лауазымдық өкілеттіктерімен қатар, оның нақты қылмыстық іске қатысуы, берілген тапсырманың орындалу мерзімі және сұратылатын әрекеттің сипаты ескерілуі тиіс. Сонымен қатар NIST SP 800-207 стандартында ақпараттық ресурстарға қол жеткізу құқығын әрбір сұрату кезінде тиісті субъектінің сипаттамаларын, қауіпсіздік талаптарын және өзге де мән-жайларды қайта бағалау қажеттігі қарастырылған [139, 18 б.]. Осыған байланысты Қазақстан Республикасының қылмыстық процесінде ақпараттық жүйелерге қол жеткізу құқықтарын қызметкердің нақты процестік өкілеттіктерімен байланыстыру және олардың сақталуын тұрақты бақылау маңызды. Атап айтқанда, қызметкер қылмыстық істі тергеп-тексеруден шеттетілген, басқа іске ауыстырылған немесе берілген тапсырманың мерзімі аяқталған жағдайда оның бұрынғы қылмыстық іс материалдарына қол жеткізу құқығы тиісті құқықтық негіз болмаған кезде тоқтатылуы тиіс.

NIST SP 800-63B-4 жүйеге кіретін тұлғаны аутентификациялау, аутентификация сенімділігінің деңгейлерін және аутентификаторларды басқару талаптарын айқындайды [140, Б. 1–9]. Құжатта жоғалған немесе бақылаудан шыққан аутентификаторларды қалпына келтіру мен қайта байланыстыру рәсімдері де арнайы регламенттелген [140, Б. 47–51]. Бұл ұсынымдар қылмыстық іс жүргізудің электрондық жүйесінде ортақ тіркелгілерді пайдалануды болдырмау, тәуекел деңгейіне сәйкес аутентификация тетігін таңдау және жоғалған қолжетімділік құралдарын қалпына келтіру рәсімдерін бақылау қажеттігін негіздеуге мүмкіндік береді. Алайда электрондық тіркелгінің техникалық сәйкестендірілуі тұлғаның заңды процестік мәртебесіне теңестірілмеуі қажет. Жүйеге сәтті кіру пайдаланушының тек техникалық тұрғыдан расталғанын білдіреді, ал нақты іс материалына қол жеткізу құқығы ҚПК-де көзделген өкілеттіктер мен нақты іске қатысу негіздерінен туындайды.

Тергеуші деректердің қылмыстық іс үшін маңыздылығын анықтауға және тиісті процестік шешімдер қабылдауға, жүйе әкімшісі ақпаратты қорғаудың техникалық талаптарын орындауға, маман цифрлық деректерді көшіру мен тіркеуге, ал сарапшы өз құзыреті шегінде арнайы зерттеу жүргізуге жауапты болады. Прокурор мен сот бақылау және қадағалау функцияларын ҚПК-де белгіленген өкілеттіктері шегінде жүзеге асырады [6; 83; 84]. Дербес деректерді қорғауға жауапты қызметкер аталған субъектілердің процестік өкілеттіктерін алмастырмайды және дәлелдемелерді қылмыстық іске енгізу туралы шешім қабылдамайды. Оның міндеттері дербес деректерді қорғау талаптарының сақталуын бақылауды, ықтимал тәуекелдерді анықтауды және анықталған бұзушылықтарды жою жөніндегі ұйымдастырушылық шараларды үйлестіруді қамтуы мүмкін.

Бұл ретте салалық заңның 25-бабындағы жауапты тұлғаны тағайындау талабы мен оның соттар қызметінде деректерді өңдеуге қатысты ерекшелігі ескерілуі қажет [2]. Сондықтан барлық сотқа дәл сол модельдегі лауазымды міндетті түрде енгізу қолданыстағы заңның талабы ретінде ұсынылмайды. Сот жүйесінде ұйымдастырушылық қорғау сот тәуелсіздігін сақтайтын тәртіппен қамтамасыз етіледі. Ақпараттық қауіпсіздік тексерісі соттың дәлелдемеге берген бағасын әкімшілік тәртіппен қайта қарауға айналмауы тиіс.

10-кесте – Деректердің қозғалысы кезіндегі шешімдер мен жауапкершілік

№	Әрекет	Құжатталатын шешім	Орындалуын тексеру
1	Алу және қабылдау	Құқықтық негіз, мақсат, көлем, дереккөз	Тергеуші; ҚПК-дегі өкілеттік шегінде прокурор мен сот
2	Зерттеу көшірмесін жасау	Түпнұсқамен байланыс; әдіс; тұтастық	Тергеуші және қатыстырылған маман
3	Сарапшыға беру	Зерттеу міндеті, объектілер, шектеулер	Тергеуші; сарапшының өз құзыреті
4	Тараптармен таныстыру	Көлем, тәсіл, уақыт; шектеудің негізі	Процесті жүргізетін орган; өтінішхат пен шағым рәсімі
5	Жария көшірмені шығару	Жабылған бөліктер және тексеру нәтижесі	Құзыретті органның уәкілетті орындаушысы
6	Іс аяқталғаннан кейін	Сақтау, архивке беру, артық көшірмені жою	Тиісті орган; заңды сақтау тәртібі және есеп

Ескерту: Авторлық модель. Кесте жаңа процестік өкілеттіктер белгілемейді. Негіз: [6; 76; 83; 135].

Сақтау режимінде дербес деректердің «қажеттілік мерзімі» мен қылмыстық іс материалдарының заңды сақталу мерзімін ажырату керек. Іске дәлелдеме ретінде енгізілген құжатты субъектінің жалпы өтініші бойынша дереу жою сотта тексеруді, шағымдануды және істі қайта қарауды қиындатуы мүмкін. Ал жұмыс үстелінде қалған артық көшірмені негізгі іспен бірдей мерзімге сақтау да әрдайым негізделмейді. Сондықтан негізгі іс материалы, зерттеу көшірмесі, уақытша экспорт және резервтік көшірме үшін бөлек есеп пен жою шарттары қажет [2; 6; 76; 96].

M.M. v. the United Kingdom ісі соттылыққа қатысты мәліметтердің сақталуы мен жариялануына қойылатын кепілдіктерді талдауға мүмкіндік береді [141, Б. 45–47]. Gaughran v. the United Kingdom ісінде биометриялық ақпаратты мерзімсіз сақтау, құқық бұзушылықтың ауырлығын және сақтаудың жалғасқан қажеттілігін ескермеу, сондай-ақ нақты қайта қарау мүмкіндігінің болмауы бағаланды [142, Б. 27–28]. Catt v. the United Kingdom ісі заңды қоғамдық белсенділік туралы полиция мәліметтерін бастапқыда жинау мен оларды кейін сақтаудың қажеттілігін бөлек бағалау қажеттігін көрсетеді [143, Б. 25–27]. Бұл тәжірибеден барлық деректерді бірыңғай мерзім өткен соң міндетті түрде жою туралы әмбебап ереже туындамайды. Негізгі талап – деректерді сақтаудың мақсаты мен мерзімінің негізді болуы және оларды одан әрі сақтаудың қажеттілігін мерзімді әрі тиімді қайта қарау мүмкіндігінің қамтамасыз етілуі.

Еуропалық Одақ Сотының C-118/22 ісі бойынша шешімінде сотталған тұлғалардың биометриялық және генетикалық деректерін өмір бойы жалпы тәртіппен, жеке мән-жайларды ескермей сақтау мәселесі қарастырылған [144, 14–16 б.]. Сот мұндай деректерді сақтау қажеттілігін бағалау кезінде қылмыстық құқық бұзушылықтың сипаты мен ауырлығын, тұлғаның жеке жағдайын және деректерді одан әрі сақтаудың негізділігін ескеру қажеттігін атап көрсеткен. Аталған сот тәжірибесін салыстырмалы-құқықтық талдау нәтижесінде Қазақстан Республикасының қылмыстық процесінде іс жүргізу аяқталғаннан кейін дербес деректерді одан әрі сақтау қажеттілігі мен олардың құқықтық мәртебесін қайта қарау ұсынылады. Бұл ретте қылмыстық істің негізгі материалдары заңнамада белгіленген тәртіппен сақталуы, қажеттілігі жойылған қосымша көшірмелер жойылуы, деректерді өзге қылмыстық істер бойынша пайдалану тиісті құқықтық негіздерге сәйкес жүзеге асырылуы, ал архивтік материалдарға қол жеткізу заңда көзделген талаптармен шектелуі тиіс. Аталған шаралар «Ұлттық архив қоры және архивтер туралы» Қазақстан Республикасының Заңымен және құжаттарды сақтаудың қолданыстағы тәртібімен үйлестірілуі қажет [145]. Осыған байланысты дербес деректерді сақтаудың бірыңғай мерзімін белгілеудің орнына олардың құқықтық мәртебесін, дәлелдемелік маңызын және одан әрі сақтау қажеттілігін ескеретін тәсілді қолдану ұсынылады.

Surikov v. Ukraine ісінде денсаулыққа қатысты бұрын жиналған мәліметтерді кейін еңбек қатынастарында, атап айтқанда қызметтік жоғарылату мәселесін шешу кезінде пайдалану бастапқы жинау мақсатынан тыс өңдеудің салдарын көрсетеді [146, Б. 19–21]. Сот сезімтал денсаулық деректерін ұзақ уақыт сақтау, оларды өзге мақсатта пайдалану және мұндай өңдеуді шектейтін жеткілікті кепілдіктердің болмауын жеке өмірге араласудың пропорционалдылығы тұрғысынан бағалады. Осы тәсіл қылмыстық іс жүргізу барысында алынған деректерді кейін кадрлық, оқу, талдамалық немесе статистикалық мақсаттарға пайдалану кезінде де ескерілуі тиіс. Қылмыстық процестің нақты мақсаты үшін алынған дерек ведомстволық кез келген өзге мақсатына автоматты түрде пайдалануға жарамды болып саналмайды. Жаңа мақсат үшін деректерді пайдаланудың

дербес құқықтық негізі, қажетті көлемі және тұлғаны сәйкестендіруді қажет етпейтін балама тәсілдің болуы бағалануы тиіс. Ғылыми және статистикалық талдау кезінде нақты тұлғаны сәйкестендіруге мүмкіндік бермейтін жиынтық немесе иесіздендірілген көрсеткіштерді пайдалану осы талапты іске асыру тәсілдерінің бірі болып табылады.

ISO/IEC 27701:2025 дербес деректерді басқару саласында ұйым ішіндегі рөлдер мен жауапкершілікті белгілеуге, құпиялылық тәуекелдерін жүйелі бағалауға және оларды басқару рәсімдерін ұйымдастыруға арналған құрылымдық бағдар ұсынады [147, 7 б.]. Стандартқа сәйкестік туралы сертификаттың болуы нақты тергеу әрекетінің қылмыстық-процестік заңнама талаптарына сай жүргізілгенін өздігінен дәлелдемейді. Дегенмен өңдеу мақсаттарын құжаттау, жауапты тұлғаларды айқындау, тәуекелдерді бағалау және қолданылатын рәсімдерді жүйелі түрде қайта қарау заң талаптарын күнделікті қызметте іске асыруға ықпал етеді. Сондықтан арнайы режимнің тиімділігі техникалық және ұйымдастырушылық сәйкестікті процестік заңдылықпен теңестірмей, осы екі талаптың дербес әрі өзара байланысты түрде орындалуын тексеруге негізделуі тиіс.

Қылмыстық процестегі дербес деректердің арнайы режимі ақпаратты алуға берілген өкілеттікті кейінгі барлық өңдеу әрекеттеріне таратпайтын, әр әрекетті мақсатымен және құқықтық негізімен байланыстыратын талаптар жүйесі ретінде негізделді. Оның мазмұны деректердің іске қатыстылығын, қажетті көлемін, пайдаланушының өкілеттігін, сақталу негізін және құқықтарды қорғау тәсілін бірізді тексеруден құралады. Жалпы салалық жіктеу процестік маңыз бен тұлғаға төнетін қауіп өлшемдерімен толықтырылуы тиіс.

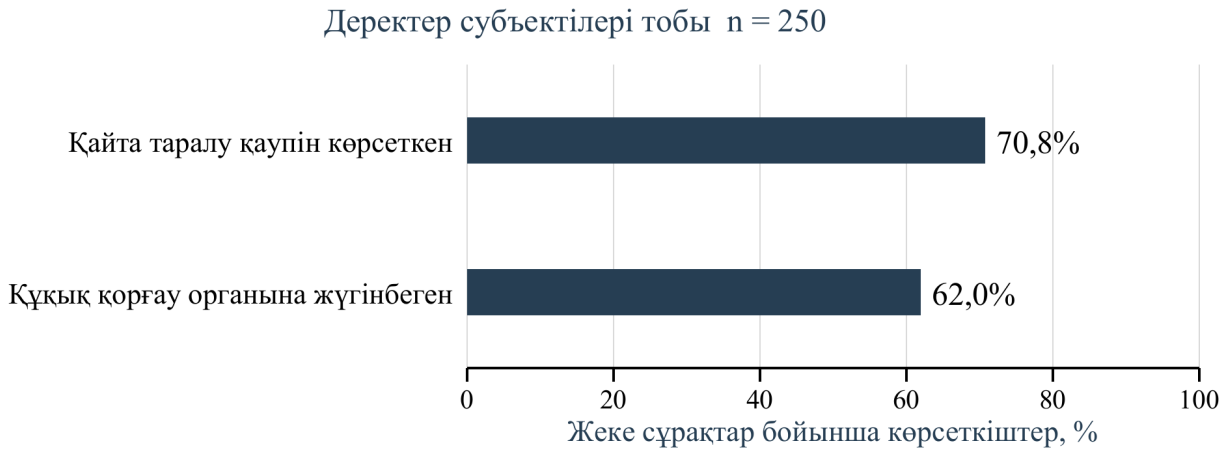
Ұсынылған режимнің ерекшелігі – заңдылықты ақпараттық жүйенің қорғалуымен ғана өлшемеу. Техникалық рұқсаты бар тұлғаның мақсаттан тыс пайдалануы, дәлелдеменің артық көшірмелерінің сақталуы және жаңа міндетке негізсіз берілуі жеке бағалауды талап етеді. Осыған байланысты қысқа есептік жазба, нақты іске байланыстырылған қолжетімділік және деректердің мәртебесін оқиғалар бойынша қайта қарау тәртібі ұсынылды. Режимді іске асыруда іс материалдарының тұтастығы, қорғау құқығы және заңды архивтік сақтау қамтамасыз етілуі тиіс. Деректерді азайту дәлелдемелік контексті жоюға, ал құпиялылық тараптарды ақпараттан толық айыруға негіз бола алмайды.

3.2 Қылмыстық процесте дербес деректердің құпиялылығын сақтау: іс материалдарына қолжетімділік, жариялылық тәуекелдері және деректерді шектеу тетіктері

Қылмыстық іс материалдарындағы дербес деректерді қорғаудағы негізгі қайшылық ақпаратты толық жабу мен толық ашу нұсқаларының арасындағы таңдаумен шектелмейді. Бір материалды тергеушіге, қорғаушыға, сарапшыға және көпшілікке ұсынудың құқықтық мақсаттары әртүрлі. Қорғаушы айыптаудың негізін тексеруге, сарапшы тапсырмадағы

сұрақтарды шешуге, ал қоғам сот төрелігінің жүзеге асырылуын бақылауға мүдделі. Сондықтан қолжетімділік көлемі алушының мәртебесі мен заңды міндетіне сәйкес белгіленуі керек. Іс материалымен танысу, оның көшірмесін алу, басқа тұлғаға беру және интернетте жариялау бірдей құқықтық әрекеттер ретінде қарастырылмауы тиіс.

Құпиялылықты қамтамасыз етудің негізгі мақсаты қылмыстық іс үшін маңызы бар мән-жайларды анықтауға кедергі келтіру емес, дербес деректердің құқықтық негізсіз таралуының алдын алу болып табылады. Осыған байланысты тергеп-тексеру барысында қажетті ақпаратты алу мен пайдаланудың заңдылығын қамтамасыз етумен қатар, жәбірленушінің дербес деректерінің қайта таралуы салдарынан қосымша зиян келтіруге жол бермеу маңызды. Диссертациялық зерттеу шеңберінде жүргізілген сауалнама нәтижелері бойынша деректер субъектілерінің 70,8%-ы дербес деректердің қайта таралу қаупін атап көрсетсе, 62,0%-ы құқық қорғау органдарына мүлдем жүгінбеген. Аталған көрсеткіштер әртүрлі мән-жайларды сипаттайтындықтан, олардың арасында тікелей себеп-салдарлық байланыс бар деп тұжырым жасауға болмайды. Дегенмен бұл нәтижелер дербес деректерді қорғаудың қылмыстық-процестік кепілдіктерін жетілдіру қажеттілігін негіздеуде ескерілуі тиіс.



5-сурет – Деректер субъектілерінің қайта таралу қаупі және құқық қорғау органдарына жүгінуі

ҚПК-нің 295-бабы жәбірленушіні және өзге де тиісті қатысушыларды материалдармен таныстыруды, ал 296-бабы күдікті мен оның қорғаушысын істің барлық материалдарымен таныстыру тәртібін реттейді [6]. Соңғы бапта құжаттарды көшіруге қатысты мемлекеттік құпиялар мен заңмен қорғалатын өзге де құпияларға байланысты ерекшеліктер көзделген. Демек, қолжетімділікті талдау кезінде танысу құқығы мен көшірмені еркін алып шығу мүмкіндігі ажыратылуы керек. Құпияны қорғау үшін белгіленген көшірме сақтау тәртібін бүкіл материалмен таныстырудан бас тарту ретінде түсіндіру қорғау құқығын негізсіз тарылтады.

ҚПК-нің 47-бабы қылмыстық сот ісін жүргізу кезінде алынатын құпия мәліметтерді қорғауды талап етеді [6]. Осы норма құпия ақпаратты заңда

көзделген тәртіппен алуға да мүмкіндік береді және оны қорғау міндетін жүктейді. Алайда «дербес деректер бар» деген жалпылама уәж әр құжатқа бірдей қолданыла алмайды. Қандай мәліметтің қандай заңмен қорғалатыны, оның құжаттағы орны және қандай әрекеттің шектелетіні анықталуы тиіс. Егер құжаттың бір бөлігіндегі байланыс дерегі дәлелдеу үшін қажет болмаса, оның жария көшірмесін шектеу жеткілікті болуы мүмкін; ал құжаттағы сәйкестендіру белгісі қорғау үшін маңызды болса, оны тексерудің қолжетімді тәсілі қамтамасыз етіледі.

«Адвокаттық қызмет және білікті заң көмегі туралы» заңдағы кәсіби құпия кепілдіктері адвокатқа берілетін материалды қорғаудың қосымша негізін құрайды [148]. Бірақ адвокаттың құпияны сақтау міндеті тергеу органының қауіпсіз беру арнасын қамтамасыз ету міндетін жоймайды. Сол сияқты қорғаушыны мәліметті жарияламау туралы ескерту оның заңда көзделген өтінішхат, шағым немесе сарапшылық көмек арқылы қорғауды жүзеге асыруына кедергі болмауы керек. ҚПК-нің 201-бабының үшінші бөлігіндегі ерекшеліктер осы мәселені шешкенде тікелей ескеріледі [6].

ЕО-ның 2012/13/EU директивасының 7-бабы іс материалдарына қолжетімділікті әділ сот талқылауын қамтамасыз ету және қорғауды тиімді дайындау мүмкіндігімен байланыстырады, сондай-ақ жекелеген материалдарға қолжетімділікті шектеуге тек тиісті кепілдіктер болған жағдайда жол береді [149, 6 б.]. 2013/48/EU директивасының 4-бабы күдікті немесе айыпталушы мен оның адвокаты арасындағы кездесулердің, хат-хабардың, телефон сөйлесулерінің және өзге де байланыстардың құпиялылығын қорғауды көздейді [150, 9 б.]. Бұл актілер Қазақстан Республикасында тікелей қолданылатын қылмыстық-процестік тәртіпті алмастырмайды. Олардың салыстырмалы-құқықтық маңызы іс материалдарына қолжетімділікті формалды таныстыру рәсімі ретінде емес, қорғауды нақты және тиімді дайындауға жеткілікті мүмкіндік ретінде бағалаудан көрінеді. Цифрлық дәлелдемелерге қатысты мұндай мүмкіндік файлға қол жеткізуді ғана емес, оның мазмұнын түсінуді, техникалық сипаттамаларын тексеруді және қажет болған жағдайда маманның көмегін пайдалануды да қамтуы тиіс.

Практикалық проблема үлкен деректер массивін тек экраннан көрсетумен шектегенде туындайды. Бірнеше минуттық танысу күрделі логтағы оқиғаларды салыстыруға немесе метадеректегі уақыт айырмасын анықтауға жеткіліксіз болуы мүмкін. Сондықтан ұсынылатын тәртіпте танысу тәсілі материалдың сипатына сай таңдалады: қорғалған жұмыс орны, уақытша рұқсат, заңды шектерде жұмыс көшірмесі немесе маманмен бірге зерттеу. Қорғаудың нақты сұрауы бойынша бастапқы файл мен ұсынылған үзіндінің байланысын тексеруге мүмкіндік беріледі. Мұндай шешім қабылданғанда ҚПК-нің уақыт, құпия және көшірме сақтау жөніндегі талаптары сақталады [6; 76; 109].

Қолжетімділік журналы қылмыстық іс материалдарының кімге және қашан берілгенін тіркеуге бағытталған және қорғаушының кәсіби қызметін бақылау құралы ретінде пайдаланылмауы тиіс. Адвокаттың іздеу сұраулары, жұмыс

жазбалары немесе қорғалушымен жүргізген талқылаулары туралы мәліметтердің айыптау тарабына қолжетімді болуы адвокаттық құпияның сақталуына қауіп төндіруі мүмкін. Осыған байланысты зерттеу шеңберінде ақпараттық қауіпсіздікті қамтамасыз етуге арналған техникалық тіркеу деректерін қорғаушының кәсіби қызметінің мазмұнына қатысты ақпараттан ажырату ұсынылады. Қолжетімділік журналында материалдарды беру фактісі, қол жеткізу рұқсатының мерзімі және ақпараттық қауіпсіздікке қатысты оқиғалар тіркелуі тиіс, ал қорғаушының құқықтық ұстанымы мен кәсіби қызметіне қатысты құпия мәліметтерге негізсіз қол жеткізуге жол берілмеуі қажет [6; 148].

11-кесте – Іс материалдарына қолжетімділіктің мақсаты мен шектері

№	Алушы	Құқықтық мақсат	Қорғау тәсілі және шек
1	Күдікті және қорғаушы	Айыптауды және дәлелдемені тексеру	ҚПК-ге сай толық танысу; құпия көшірмелердің арнайы тәртібі
2	Жәбірленуші және өкілі	Құқықтарын қорғау, іс материалымен танысу	ҚПК-нің 295-бабындағы тәртіп; өзге тұлғалар туралы артық жариялауды шектеу
3	Сарапшы және маман	Берілген процестік міндетті орындау	Тапсырмаға сай объектілер; жеткіліксіз болса қосымша материал сұрату
4	Жүйе әкімшісі	Техникалық қызмет және қорғаныс	Қажетті техникалық өкілеттік; мазмұнды мақсатсыз қарауға тыйым
5	Медиа және көпшілік	Қоғамдық бақылау және ақпарат алу	Заңды жария мәтін; құпия мен жеке өмірді қорғау; мәртебені дәл көрсету

Ескерту: Авторлық салыстыру. Азаматтық талапкерлер мен жауапкерлердің қолжетімділігі ҚПК-нің 295-бабындағы талапқа қатысты көлеммен анықталады. Негіз: [6; 148; 166].

Қолжетімділікті шектеу туралы шешімнің мазмұны кемінде шектелетін материалды, қорғалатын мүддені, қолданылатын норманы, тәуекелдің нақты сипатын және балама тәсілдің неліктен жеткіліксіз екенін көрсетуі тиіс. Мұндай шешімді стандартты «тергеу мүддесі» деген тіркеспен негіздеу оның мөлшерлестігін тексеруге мүмкіндік бермейді. Ұсынылатын тәртіп бойынша құжаттың бар екені мен шектеудің қолданылғаны тарапқа заңда рұқсат етілетін көлемде белгілі болады. Мәліметтің өзін ашпай-ақ, шешімге қарсылық білдіруге қажетті сипаттама беру жолы қарастырылады. Ерекше құпия немесе қауіпсіздік режиміндегі алып тастаулар тек тиісті заң негізінде қолданылады.

Rowe and Davis v. the United Kingdom ісі айыптау тарапының материалды қорғаудан жасыруы кезінде тәуелсіз сот бақылауы мен жеткілікті процестік кепілдіктердің маңызын көрсетеді [151, 22 б.]. Jasper v. the United Kingdom ісінде құпия материалды соттың өзі қарап, оны жария ету қажеттілігін сот талқылауы барысында тұрақты бағалап отырған рәсім өзге құқықтық нәтижеге алып келді [152, 23 б.]. Осы екі шешімді бірге қарастыру құпия ақпараттың болуы өздігінен әділ сот талқылауының бұзылғанын да, қолжетімділікті шектеудің заңдылығын да автоматты түрде білдірмейтінін көрсетеді. Бағалау кезінде шектеу туралы шешімді кім қабылдағаны, соттың қандай материалды тексергені, қорғау тарапының ұстаным білдіру мүмкіндігі

және оның құқықтарына келтірілген шектеудің қандай процестік кепілдіктермен өтелгені ескерілуі тиіс. Қазақстандық модельде бұл мәселелер ҚПК-де көзделген сот бақылауы мен шағымдану тәртібі шеңберінде шешілуі қажет.

ҚПК-нің 105–106-баптары мен Қазақстан Республикасы Жоғарғы Сотының тиісті нормативтік қаулысы процестік шешімдерге, әрекеттерге және әрекетсіздікке шағым жасаудың құқықтық негіздерін белгілейді [6; 153]. Осыған байланысты зерттеу шеңберінде жаңа шағымдану тәртібін енгізу емес, қылмыстық іс материалдарына қолжетімділікті шектеу туралы шешімдердің негізділігін қамтамасыз ету және оларды тексеруге қажетті мәліметтерді қолданыстағы шағымдану тетіктері арқылы қарау мүмкіндігін жетілдіру ұсынылады. Бұл ретте тергеу судьясының өкілеттіктері ҚПК-де белгіленген құзырет шегінде жүзеге асырылуы тиіс және техникалық регламенттер арқылы кеңейтілуіне жол берілмейді.

Деректер субъектісінің өзі туралы ақпаратты білу құқығы мен қылмыстық іс қатысушысының барлық тиісті материалмен танысу құқығы да ажыратылуы керек. Біріншісі деректерді өңдеуге, екіншісі процестік мәртебеге байланысты туындайды. EDPB-ның қолжетімділік жөніндегі нұсқаулығы деректер субъектісіне берілетін ақпараттың түсініктілігі мен өзге адамдардың құқықтарын ескеруді талдайды [154, 45 б.]. Оның жалпы логикасы пайдалы болғанымен, GDPR тәртібін тергеудегі барлық сұрауға тікелей көшіруге болмайды. Қылмыстық қудалау мақсатындағы ЕО өңдеуі үшін 2016/680 директивасының бөлек қолданылу саласы бар [118]. Қазақстанда тиісті құқық пен ерекшелік ұлттық заңдар бойынша анықталады.

EDPB-ның құқықтарды шектеу жөніндегі нұсқаулығы деректер субъектісі құқықтарын шектеудің заңда айқындалуын, оның мақсатының жеткілікті түрде нақтылануын, сондай-ақ әрбір шектеудің қажеттілік пен пропорционалдық талаптарына сәйкестігін бағалауды талап етеді [155, 11 б.]. Сонымен қатар шектеуді қолдануға негіз болған мән-жайлар жойылғаннан кейін оны одан әрі сақтауға негіз қалмайтыны көрсетіледі. Осы тәсілге сүйене отырып, деректер субъектісіне ақпарат беруді кейінге қалдыруға негіз болған мән-жайлар жойылған кезде бұрын қабылданған шешімді қайта қарау ұсынылады. Бұл қағида жасырын тергеу әрекеттері туралы хабарлаудың арнайы қылмыстық-процестік тәртібін алмастырмайды. ҚПК-нің 240-бабында көзделген хабарлау тәртібі өз қолданылу аясында сақталуы тиіс, ал жалпы ұйымдастырушылық ереже арқылы онда белгіленген мерзімдер мен ерекшеліктер өзгертілмеуі қажет [6].

ҚПК-нің 96–97-баптары мен «Қылмыстық процеске қатысушы адамдарды мемлекеттік қорғау туралы» заң нақты қауіп туындағанда қорғау шараларын қолданудың негіздерін белгілейді [6; 156]. ҚПК-нің 97-бабы қорғалатын адамның сауалнамалық деректерін негізгі материалдан бөлек сақтау мен бүркеншік ат пайдалануды көздейді. Сондықтан мұндай шараларды толығымен жаңа институт ретінде ұсыну негізсіз. Жетілдіру міндеті осы құқықтық механизмді электрондық көшірмелерге, іздеу индексіне, қосымша файлдарға және жүйелік метадеректерге дәйекті

қолданумен байланысты. Негізгі хаттамада бүркеншік ат болып, файл атауында немесе техникалық қасиетінде шынайы аты қалса, шара іс жүзінде әлсірейді.

Куәнің қауіпсіздігі мен оның айғақтарын қорғау тарапының тексеру мүмкіндігі өзара байланыста бағалануы тиіс. Doorson v. the Netherlands ісінде жасырын куәнің қауіпсіздігін қамтамасыз ету кезінде қорғауға келтірілетін шектеулердің тиісті процестік кепілдіктермен өтелуі, оның ішінде қорғаушының куәға сұрақ қою мүмкіндігі мен айғақтың сенімділігін даулауы қажеттігі көрсетілген [157, 24 б.]. Van Mechelen and Others v. the Netherlands ісінде де жасырын куәлардың айғақтарын пайдалану кезінде қорғау мүмкіндіктері, соттық бақылау және айғақтарды басқа дәлелдемелермен растау талаптары ерекше мәнге ие екені атап өтілген [158, 20 б.]. Осы тәжірибе куәға бүркеншік ат берудің өзі жеткілікті кепілдік болып табылмайтынын көрсетеді. Қазақстандық қылмыстық процесте қауіпсіздік шаралары куәға сұрақ қою, айғақтың қайнар көзі мен сенімділігін бағалау және оның өзге дәлелдемелермен байланысын тексеру мүмкіндігімен үйлесуі тиіс. Қауіпсіздікті қамтамасыз етудің техникалық тәсілдері ҚПК-де көзделген дәлелдеу тәртібі мен қорғау құқықтарын сақтай отырып таңдалуы қажет.

БҰҰ-ның қылмыс құрбандары туралы декларациясы жәбірленушінің қадір-қасиетін құрметтеу, көмек алу және сот төрелігіне қолжетімділік мәселелерін байланыстырады [159]. UNODC-ның куәларды қорғау жөніндегі нұсқаулығы нақты қауіпке сай шараны таңдау мен оны ұйымдастыру қажеттілігін көрсетеді [160]. Осы материалдардан туындайтын ұсыныс – қайта таралу қаупі бар жәбірленушіге тек қолхат бергізумен шектелмей, оның байланыс деректерін пайдалану тәртібін, қауіпсіз хабарласу арнасын және жария құжаттағы сәйкестендіру белгілерін алдын ала анықтау. Қорғау шарасы тұлғаның процестік құқықтарын түсінікті түрде іске асыруына көмектесуі керек.

Балаларға қатысты деректердің таратылуы олардың кейінгі өміріне ұзақ ықпал етуі мүмкін. Бала құқықтары туралы конвенциядағы жеке өмірді қорғау және баланың үздік мүдделерін ескеру талаптары осы саладағы бастапқы бағдар болып табылады [161]. БҰҰ Комитетінің № 25 жалпы түсіндірмесі цифрлық ортадағы қауіптерді балалардың құқықтарымен бірге қарастырады [162]. Қылмыстық іс құжатында баланың аты-жөнін алып тастау жеткіліксіз болуы ықтимал: мектеп, сынып, туыстық байланыс, шағын елді мекен және ерекше оқиға бірге оның кім екенін ашуы мүмкін. Сондықтан жария көшірме тікелей және жанама сәйкестендіру белгілері бойынша тексерілуі ұсынылады.

Volodina v. Russia (No. 2) ісінде жалған профильдер жасау, интимдік фотосуреттерді келісімсіз жариялау, онлайн қудалау және цифрлық ортадағы өзге де араласуларға тиімді құқықтық әрі тергеулік жауап беру қажеттілігі көрсетілген [163, 17 б.]. Buturugă v. Romania ісінде электрондық хат-хабарға заңсыз қол жеткізу, оны көшіру және киберқудалауға байланысты шағымдарды мәні бойынша зерттеу міндеті атап өтілген [164, 22 б.]. Бұл тәжірибенің осы зерттеу үшін маңызы дербес деректерді қорғауды тек

ақпаратты таратпау міндетімен шектеуге болмайтынында. Егер жеке ақпарат қорқыту, жалған профиль жасау, қудалау немесе өзге құқық бұзушылық құралына айналса, уәкілетті орган цифрлық іздерді уақтылы сақтау, олардың шығу тегін анықтау және тиісті әрекеттерді тергеп-тексеру міндеттерін де орындауы тиіс. Құпиялылықты қамтамасыз ету нақты құқық бұзушылықты тергеп-тексеруден бас тартуға негіз болмауы қажет.

K.U. v. Finland ісі де осы теңгерімнің екінші жағын ашады: интернеттегі анонимділікті қорғау кәмелетке толмаған жәбірленушінің құқықтарын қорғауға қажетті заңды сәйкестендіру мүмкіндігін толық жоймауы керек [165, 14 б.]. Қазақстандық модельде осы міндет дерек ұстаушыдан мәлімет алудың заңды негізі, қажетті көлемі және беру тәртібі арқылы шешіледі. Жәбірленушіні қорғау үшін алынған ақпараттың өзі кейіннен тараптарға немесе көпшілікке артық таратылмауы тиіс. Тергеу мен қорғау осылайша бір процестің өзара байланысты міндеттері болып қалады.

ҚПК-нің 29-бабы қылмыстық істерді ашық қарауды негізгі қағида ретінде бекітіп, жабық отырыстың заңды негіздерін көздейді [6]. Жоғарғы Соттың жариялылық қағидатын сақтау туралы нормативтік қаулысы осы талаптың сот практикасындағы мәнін нақтылайды [166]. Дербес деректердің болуы барлық істі жабық қарауға жеткілікті дербес негіз ретінде түсіндірілмеуі керек. Сот қорғалатын құпияны, интимдік өмір туралы мәліметті немесе қауіпсіздік мүддесін нақты бағалайды. Егер құқықты қорғау үшін тек белгілі дәлелдемені жабық зерттеу жеткілікті болса, шектеудің көлемі де осы қажеттілікпен байланыстырылады.

Ашық сот отырысы, үкімді жариялау және сот актісін интернетке орналастырудың таралу ауқымы бірдей емес. ҚПК-нің 29-бабында жабық отырыста қаралған іс бойынша үкімнің кіріспе және қарар бөліктерін көпшілік алдында жариялау ерекшелігі бар [6]. Ал интернеттегі жариялау материалды іздеу жүйелері арқылы ұзақ уақыт табуға, басқа дереккөздермен біріктіруге және жаппай көшіруге мүмкіндік береді. Осыған байланысты ашықтықтың мақсаты соттың уәжін қоғамға түсіндіру арқылы орындалуы, ал іске қатысы жоқ жеке мәліметтердің жаппай таралуы шектелуі тиіс. Мұндай тәсіл сот актісінің заңды мазмұнын өзгертуге жол бермейді.

L.L. v. France ісіндегі сот шешімінде медициналық мәліметті қайталау мәселесі жария құжатқа қандай дерек енгізілетінін бағалауға негіз береді [167, 13 б.]. Vicent Del Campo v. Spain ісі іс жүргізуге қатыспаған тұлғаны сот шешімінде атаудың жеке өмірге ықпалын көрсетеді [168, 10 б.]. Бұл материалдар Қазақстан сотына шетелдік рәсімді көшіру үшін емес, қажеттілік өлшемін нақтылау үшін пайдаланылады. Егер соттың құқықтық қорытындысын түсіндіруге диагноздың толық сипаттамасы немесе үшінші тұлғаның мекенжайы қажет болмаса, жария мәтінде оларды көрсетудің негізі бөлек дәлелденуі керек.

Медиаға ақпарат беру ҚПК-нің 201-бабындағы сотқа дейінгі тергеп-тексеру деректерін жария ету тәртібімен және «Масс-медиа туралы» заңмен үйлестіріледі [6; 169]. Еуропа Кеңесінің Rec(2003)13 ұсынымы қылмыстық процесс туралы ақпарат таратуды кінәсіздік презумпциясымен және жеке

өмірді қорғаумен байланыстырады [170]. ЕО-ның 2016/343 директивасы да жария мәлімдемеде кінәлі деп көрсету проблемасын қарастырады [171]. Осы материалдардан ұлттық практика үшін қорытынды: хабарламада тұлғаның процестік мәртебесі дәл көрсетіліп, болжамды айыптау заңды күшіне енген кінәлілік қорытындысы ретінде берілмеуі тиіс.

Bédat v. Switzerland ісінде тергеу құпиясын құрайтын материалдарды жариялаған журналистке қолданылған шектеу жарияланған ақпараттың мазмұны, оның қоғамдық пікірталасқа қосқан үлесі, айыпталушының жеке өмірі мен кінәсіздік презумпциясына ықпалы тұрғысынан бағаланған [172, Б. 20–24]. Axel Springer AG v. Germany ісінде ақпараттың қоғамдық мүддеге қосқан үлесі, тұлғаның танымалдық дәрежесі, жарияланымның тақырыбы, ақпараттың алыну тәсілі мен дұрыстығы және жарияланымның ықтимал салдары құқықтар арасындағы теңгерімді айқындайтын өлшемдер ретінде қарастырылған [173, Б. 12–15]. Осы екі істі қатар талдау қылмыстық іс туралы ақпаратқа толық тыйым салу да, оның кез келген көлемде жариялануын қоғамдық қызығушылықпен негіздеу де жеткіліксіз екенін көрсетеді. Ақпараттың қоғамдық маңызы мен нақты дербес мәліметті жариялау қажеттілігі әрқайсысы жеке бағалануы тиісғ қоғамдық қызығушылықтың болуы іс материалдарындағы барлық мәліметті ашуға өздігінен негіз болмайды.

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland ісі бойынша Еуропалық адам құқықтары сотының шешімінде бұрын заңды түрде қолжетімді болған дербес деректерді кең көлемде жинау, жүйелеу және жаппай тарату жеке өмірге қол сұғылмаушылық құқығы тұрғысынан дербес бағалауды қажет ететіні көрсетілген [174, 50 б.]. Сот дербес деректердің бастапқыда жалпыға қолжетімді болуы оларды кейіннен шектеусіз жинақтау мен таратуды өздігінен негіздемейтінін атап өткен. Аталған құқықтық ұстаным қылмыстық сот ісін жүргізу барысында да маңызды, өйткені жекелеген құжаттардың заңды түрде қолжетімді болуы олардағы мәліметтерді белгілі бір тұлға бойынша біріктіріп, жүйеленген ақпараттық база қалыптастыруға автоматты түрде құқық бермейді. Мұндай әрекеттер дербес деректердің құпиялылығына қатысты қосымша тәуекелдер туындатуы мүмкін. Осыған байланысты қылмыстық іс материалдарын жариялау кезінде жекелеген құжаттардың мазмұнымен қатар, олардағы деректерді іздеу, жүйелеу, біріктіру, қайта пайдалану және өзге ақпарат көздерімен байланыстыру мүмкіндіктері де ескерілуі тиіс. Бұл ретте қылмыстық сот ісін жүргізудің жариялылық қағидаты адамның жеке өмірі туралы мәліметтерді барынша толық ашумен емес, қоғамның ақпарат алу құқығы мен дербес деректерді қорғау кепілдіктерінің арасындағы тепе-теңдікті сақтаумен қамтамасыз етілуі қажет.

Иесіздендіру, псевдонимдеу және құжаттың жекелеген бөліктерін жасыру дербес деректерді қорғаудың өзара байланысты, бірақ қолданылу ерекшеліктері бойынша ажыратылатын тәсілдері болып табылады. Иесіздендіру тұлғаны сәйкестендіру мүмкіндігін болдырмауға, псевдонимдеу тұлғаны анықтауға мүмкіндік беретін белгілерді шартты

сәйкестендіргіштермен алмастыруға және бастапқы мәліметтермен қайта байланыстыруға қажетті ақпаратты бөлек сақтауға, ал құжаттың жекелеген бөліктерін жасыру белгілі бір тұлғаға ұсынылатын ақпарат көлемін шектеуге бағытталған. Бұл ретте қылмыстық іс материалдарындағы бастапқы цифрлық дәлелдемелердің тұтастығы сақталуы тиіс, сондықтан олардың жұмыс немесе жария етуге арналған көшірмелеріндегі сәйкестендіру белгілерін өзгерту бастапқы деректердің мазмұнын өзгертумен теңестірілмеуі қажет [2; 76; 175].

П. Ом анонимдендіруді дербес деректерді қорғаудың жеткілікті әрі түпкілікті тәсілі ретінде қабылдаудың шектеулерін және қосымша ақпарат болған жағдайда тұлғаны қайта сәйкестендірудің құқықтық салдарын талдайды [176, Б. 1716–1723]. А. Нараянан мен В. Шматиков сирек әрі жоғары өлшемді деректер жиынтығындағы жазбаларды сыртқы ақпаратпен салыстыру арқылы нақты тұлғаны қайта сәйкестендіру мүмкіндігін көрсетеді [177, Б. 1–3]. Бұл зерттеулердегі эмпирикалық көрсеткіштер қазақстандық қылмыстық істердің статистикалық деректері ретінде қолданылмайды. Олардың осы диссертация үшін әдіснамалық маңызы – тікелей идентификаторларды алып тастау тұлғаны қайта сәйкестендіру тәуекелін әрдайым жоймайтынын көрсетуінде. Мұндай тәуекел қолжетімді қосымша ақпараттың көлеміне, жарияланатын деректердің ерекшелігі мен сиректігіне, сондай-ақ оларды өзге деректер жиынтықтарымен байланыстыру мүмкіндігіне тәуелді.

Л. Суини ұсынған k-анонимдік моделі кестелік деректердегі жанама сәйкестендіргіштердің комбинациясы бойынша тұлғаны даралау мүмкіндігін шектеуге бағытталған [178, 1 б., 7 б.]. Бұл тәсіл құрылымдалған статистикалық деректерді жариялау кезінде пайдалы болғанымен, шағын көлемдегі қылмыстық іс мәтінінің қауіпсіздігін автоматты түрде қамтамасыз етпейді: ерекше оқиға, сирек сипаттама немесе бірегей туыстық байланыс тұлғаны тікелей идентификаторларсыз да қайта тануға мүмкіндік беруі мүмкін. С. Гарфинкельдің NIST IR 8053 шолуында сәйкестендіруден арылтудың әртүрлі дерек нысандарына қолданылатын тәсілдерінің шектері және сыртқы ақпаратпен байланыстыру нәтижесінде қайта сәйкестендіру тәуекелінің сақталатыны көрсетілген [179, 1 б., 5 б.]. NIST SP 800-188 бұл міндетті жариялау алдындағы басқарушылық шешіммен, деректерді бөлісу моделін таңдаумен және қайта сәйкестендіру тәуекелін алдын ала бағалаумен байланыстырады [180, Б. 19–20, Б. 25, Б. 31–32].

ENISA-ның псевдонимдеу мәселелеріне арналған есебінде тиісті әдістерді таңдау кезінде деректерді өңдеудің ерекшеліктерін, қажетті қорғау деңгейін және ықтимал қауіпсіздік қатерлерін ескеру қажеттігі атап көрсетілген [181, 5 б.]. Осыған байланысты адамның аты-жөнін қарапайым криптографиялық хэш-мәнмен алмастыру дербес деректердің құпиялылығын толық қамтамасыз етпейді, өйткені бастапқы мәліметтердің ықтимал нұсқалары шектеулі болған жағдайда оларды салыстыру арқылы тұлғаны қайта сәйкестендіру мүмкіндігі сақталады. Сондықтан псевдонимделген деректерді нақты тұлғамен байланыстыруға мүмкіндік беретін қосымша ақпарат бөлек сақталып, оған қол жеткізу шектелуі тиіс. Бұл ретте

псевдонимдеу мақсатында қолданылатын хэштеу мен цифрлық файлдардың тұтастығын тексеруге арналған хэш-мәннің қызметін ажырату қажет. Файлдың хэш-мәні оның мазмұнындағы өзгерістерді анықтауға мүмкіндік бергенімен, дербес деректердің құпиялылығын өздігінен қамтамасыз етпейді.

12-кесте – Деректерді шектеу тәсілдерінің қызметі мен қолданылу шегі

№	Тәсіл	Қолданылатын міндет	Маңызды шектеу
1	Псевдонимдеу	Жұмыс мәтініндегі тікелей сәйкестікті шектеу	Қайта байланыстыру кілті бөлек қорғалады; толық анонимдік емес
2	Жария көшірмеде бөлікті жабу	Көпшілікке қажет емес мәліметті алып тастау	Жасырын мәтін, метадерек және жанама белгілер тексеріледі
3	Жиынтықтау	Сыртқы статистикалық мәлімет дайындау	Шағын топ пен сирек белгілер арқылы тану қаупі бағаланады
4	Қорғалған ортада танысу	Құпия дәлелдемені заңды тексеру	Қорғау құқығын іс жүзінде іске асыруға жағдай қажет
5	Шифрлау	Сақтау мен тасымалдауда құпиялылық	Кілтке қолжетімділік пен оны қалпына келтіру тәртібі керек
6	Хэш арқылы тексеру	Файлдың тұтастығын бақылау	Мазмұнды жасырмайды; заңсыз алуды заңдастырмайды

Ескерту: Авторлық жүйелеу. Түпнұсқа дәлелдемеге өзгеріс енгізу ұсынылмайды. Негіз: [76; 77; 175; 181; 180].

Ұсынылатын жариялау рәсімі мазмұнды саралау, жария көшірмені дайындау және оны қайта тексеру сатыларынан тұрады. Мазмұнды саралауда тікелей идентификаторлар, жанама белгілер және қорғалатын құпия анықталады. Көшірме дайындалғанда жабылған мәтін іздеу қабатында, түсініктемеде, өзгерістер тарихында немесе файл қасиетінде сақталмағаны тексеріледі. Қайта тексеру кезінде құжат басқа ашық ақпаратпен бірге оқылады. Бұл рәсім техникалық тазалаудың сапасын ғана емес, сот уәжінің түсініктілігі мен дәлелдемелік байланыстардың сақталуын да бағалайды. Бастапқы материал мен жария көшірме бөлек нұсқалар ретінде есепке алынады.

С. Дворктің дифференциалдық құпиялылық тәсілі жиынтық статистикадан жеке адамның қатысуы туралы артық қорытынды шығаруды шектеуге бағытталған [182, 5 б.]. Оны қылмыстық іс бойынша бастапқы дәлелдемеге шу қосу немесе нақты логтағы мәндерді өзгерту үшін қолдану ұсынылмайды. Мұндай өзгеріс дәлелдеменің мағынасын бұрмалайды. Тәсілдің ықтимал орны – заңды түрде дайындалатын сыртқы статистикалық жарияланым.

Іс материалынан дерек тараған жағдайда ақпараттық қауіпсіздік инциденті мен қылмыстық-процестік салдар қатар бағаланады. Алғашқы әрекет таралудың көзін оқшаулау, қолжетімділікті тексеру және журналдарды сақтау болуы мүмкін. Сонымен қатар жарияланған материалдың іс дәлелдемелерімен байланысы, қатысушыға төнген қауіп және материалға заңсыз өзгеріс енгізілген-енгізілмегені анықталады. Жария болу

фактісі әрбір дәлелдемені автоматты түрде жол берілмейтін етпейді. Мұндай қорытынды ҚПК-нің 112 және 125-баптарындағы өлшемдер бойынша нақты бұзушылықтың сипатына қарай жасалады [6; 44].

«Дербес деректер және оларды қорғау туралы» заңның 25-бабында қолданылатын қатынастар үшін қауіпсіздік бұзылғаны анықталған кезден бастап уәкілетті органды бір жұмыс күні ішінде хабардар ету міндеті көзделген [2]. Бұл мерзім деректер субъектісіне хабарлаудың барлық жағдайына немесе ҚПК-дегі ЖТӘ туралы хабарлауға бірдей мерзім ретінде көшірілмеуі тиіс. Арнайы режимге қатысты ерекшеліктер заңның қолданылу аясымен бірге тексеріледі. EDPB-ның бұзушылықтар туралы хабарлау мысалдары оқиғаның сипатын, ықтимал салдарын және қабылданған шараларды байланыстыруға әдіснамалық бағдар береді [183, 7 б.]. Бұл ретте шетелдік құқықта көзделген хабарлау мерзімдерін Қазақстан Республикасының ұлттық заңнамасында белгіленген мерзімдердің орнына қолдану ұсынылмайды.

Ішкі инцидентті қарау қорғалатын адамдардың жаңа тізімін бейберекет таратуға әкелмеуі керек. Хабарлама алушыға оның міндетін орындау үшін қажетті мазмұн ғана беріледі. Жәбірленушіге қауіпсіз арнамен түсіндірілетін ақпаратта қандай деректің ашылғаны, ықтимал қауіп және құқықты қорғау жолы қамтылуы мүмкін. Оқиғаны тексеруге қатысқан тұлғалардың әрекеттері тіркеледі. Қажеттілік туындағанда қауіпсіздік шаралары қайта қаралып, заңда көзделген жауаптылық мәселесі тиісті рәсім бойынша шешіледі. Осылайша, инцидентке жауап беру техникалық қалпына келтірумен қатар тұлғаның құқықтық жағдайын қалпына келтіруге бағытталады.

Қылмыстық процесте дербес деректердің құпиялылығын қамтамасыз ету іс материалдарымен танысу, олардың көшірмелерін алу, процестік мақсаттарда пайдалану және көпшілікке жариялау әрекеттерінің құқықтық ерекшеліктерін ажыратуды талап етеді. Бұл ретте қорғау тарапының дәлелдемелерді жан-жақты зерделеу және тексеру мүмкіндігі қамтамасыз етілуі тиіс, ал қылмыстық іс материалдарына қол жеткізуді шектеу нақты құқықтық негіздер мен дербес деректердің құпиялылығына төнетін қауіптерді ескере отырып, уәжді процестік шешім арқылы жүзеге асырылуы қажет. Сонымен қатар дербес деректер субъектісінің өз мәліметтеріне қол жеткізу құқығы мен қылмыстық процеске қатысушылардың іс материалдарымен танысу құқығы құқықтық табиғаты мен жүзеге асырылу тәртібі бойынша ажыратылуы тиіс. Осыған байланысты ақпараттық қауіпсіздікті қамтамасыз ету және кәсіби құпияны қорғау шаралары қылмыстық процеске қатысушылардың ҚПК-де көзделген құқықтары мен заңды мүдделерін негізсіз шектемеуі қажет.

Цифрлық ортада ақпараттың жария болуы оның ұзақ уақыт сақталуымен, іздеу жүйелері арқылы қолжетімділігімен, индекстелуімен және өзге мәліметтермен біріктірілу мүмкіндігімен ерекшеленеді. Осыған байланысты қылмыстық іс материалдарын жариялауға дайындау барысында тұлғаны тікелей сәйкестендіруге мүмкіндік беретін мәліметтерді алып

тастаумен ғана шектелмей, жанама сәйкестендіру белгілерін, жеке тұлғаға қатысты ерекше мән-жайларды, файлдардың техникалық сипаттамалары мен метадеректерін, сондай-ақ тұлғаны қайта сәйкестендіру тәуекелдерін ескеру қажет. Дербес деректерді иесіздендірудің жеткіліктілігі жарияланатын ақпараттың сипатына және оны өзге ақпарат көздерімен байланыстыру мүмкіндігіне қарай бағалануы тиіс. Бұл ретте қылмыстық іс бойынша бастапқы дәлелдемелер, зерттеу мақсатында пайдаланылатын жұмыс көшірмелері және жариялауға арналған материалдар өзара ажыратылып, олардың арасындағы сәйкестік тиісті техникалық және ұйымдастырушылық құралдар арқылы тіркелуі қажет.

Дербес деректердің таралуы анықталған жағдайда құқықтық және ұйымдастырушылық шаралар оқиғаның одан әрі таралуын тоқтатуға, цифрлық іздерді сақтауға, ықтимал зардаптарды бағалауға, деректер субъектілерінің қауіпсіздігін қамтамасыз етуге, сондай-ақ орын алған жағдайдың дәлелдемелердің тұтастығы мен жол берілетіндігіне ықпалын жеке тексеруге бағытталуы тиіс. Бұл ретте оқиғаның сипаты, оның ықтимал құқықтық салдары және қабылданған шаралардың тиімділігі өзара байланыста бағалануы қажет. Осыған байланысты құпиялылықты қамтамасыз етудің тиімділігі ақпаратқа қол жеткізуді барынша шектеумен емес, қылмыстық процеске қатысушылардың заңда көзделген құқықтарын және дәлелдемелерді тексеру мүмкіндігін сақтай отырып, дербес деректердің заңсыз таралу қаупін төмендету деңгейімен айқындалуы тиіс.

3.3 Қылмыстық-процестік заңнаманы және құқық қолдану тәжірибесін жетілдіру жөніндегі тұжырымдамалық ұсыныстар

Қылмыстық-процестік заңнаманы жетілдірудің негізгі бағыты тергеп-тексеру үшін қажетті цифрлық деректерді уақтылы алуды, олардың дәлелдемелік маңызын жан-жақты тексеруді және дербес деректерді қорғаудың тиісті кепілдіктерін қамтамасыз етуді көздейді. Диссертациялық зерттеудің екінші тарауында цифрлық деректерді алу, бекіту және дәлелдеме ретінде пайдалану мәселелері қарастырылса, үшінші тараудың алдыңғы бөлімдерінде алынған мәліметтерді одан әрі пайдалану барысында адамның құқықтары мен заңды мүдделерін қорғау қажеттілігі негізделді. Осыған байланысты қылмыстық-процестік заңнаманы жетілдіру жөніндегі ұсыныстар дербес деректерге қол жеткізудің құқықтық негіздерін нақтылаумен қатар, оларды алудың мақсатын, көлемін, сақтау тәртібін және пайдаланылуын бақылаудың процестік кепілдіктерін айқындауға бағытталуы тиіс.

Қылмыстық-процестік заңнаманы жетілдіру қажеттілігі тек цифрлық технологиялардың дамуымен ғана емес, оларды қолдану барысында туындайтын нақты құқықтық және практикалық мәселелермен де байланысты. Атап айтқанда, деректерді ұстаушыдан жауап алу мерзімінің ұзақтығы цифрлық іздердің жойылуына, алынған файлдардың шығу тегі туралы мәліметтердің толық тіркелмеуі олардың дәлелдемелік маңызын

тексерудің қиындауына, көлемді ақпараттық массивтерді алу іске қатысы жоқ тұлғалардың дербес деректерінің негізсіз ашылуына, ал құпиялылық талаптарының жалпылама қолданылуы қорғау тарапының процестік құқықтарының шектелуіне әкелуі мүмкін. Осыған байланысты заңнаманы жетілдіру жөніндегі әрбір ұсыныс анықталған құқықтық проблеманы, қолданыстағы заңнама талаптарын, оны шешудің процестік тәртібін, бақылау тетіктерін және ықтимал құқықтық салдарын өзара байланыстыра отырып негізделуі тиіс. Осы зерттеу шеңберінде ұсынылатын заңнамалық өзгерістер қолданыстағы құқықтық нормалардан ажыратылып, оларды жетілдіруге бағытталған ғылыми ұсыныстар ретінде қарастырылады.

ҚПК-нің 1–2-баптары қылмыстық сот ісін жүргізу тәртібінің қайнар көздері мен нормалардың басымдығын айқындайды [6]. Құқықтарды шектеудің негіздері, қатысушылардың өкілеттіктері және материалға қолжетімділіктің ерекше тәртібі заң деңгейінде бекітілуі тиіс. Ведомстволық нұсқаулық мұндай шектеулерді өз бетінше туындата алмайды. «Құқықтық актілер туралы» заң талаптарына сәйкес заңнамалық өзгерістің мазмұны, нысаны және құқықтық иерархиясы үйлестіріледі [184]. ҚПК-ге өзгерістер енгізу туралы заң жобасының рәсімделуінде Кодекстің өзіндегі арнайы талаптар да сақталуы қажет.

Құқықтық реттеу үш деңгейде ұсынылады. ҚПК дербес деректермен жұмыс істеудің негізгі кепілдіктерін және құқықты шектеу рәсімін белгілейді. Уәкілетті органдардың нормативтік актілері осы талаптарды орындаудың техникалық және ұйымдастырушылық тәртібін нақтылайды. Әдістемелік ұсынымдар нақты жағдайға сай әрекетті таңдауға көмектеседі. Осы деңгейлердің айырмашылығы практикалық мәнге ие: логты экспорттау нысанын нұсқаулықпен біріздендіруге болады, ал қорғаушыға материал бермеудің жаңа негізін нұсқаулықпен белгілеуге болмайды. Техникалық стандарттың орындалмауының процестік салдары да ҚПК талаптарымен бағаланады.

БҰҰ Жоғарғы комиссарының цифрлық дәуірдегі жеке өмір туралы 2018 жылғы баяндамасы мәліметті өңдеу ауқымы ұлғайғанда құқықтық кепілдіктердің нақтылығын қамтамасыз ету мәселесін көтереді [185]. 2022 жылғы баяндамада цифрлық бақылау мен қорғалған коммуникацияға қатысты қауіптер қарастырылады [186]. Осы материалдардан диссертация үшін туындайтын қорытынды – реформаның мақсатын тек қолжетімділікті кеңейту немесе деректер қорын біріктіру арқылы анықтауға болмайды. Әр жаңа функцияның тұлғаға ықпалы және оны шектеудің құқықтық тетігі бірге негізделуі керек. Бұл өлшем ұлттық конституциялық кепілдіктерден туындайтын міндеттерді нақтылауға қызмет етеді [1].

EDPS әзірлеген қажеттілікті бағалау құралы мақсатқа жетудің араласуы азырақ баламаларын салыстыруға бағытталған [187]. Мөлшерлестік жөніндегі нұсқаулығы ұсынылатын шараның тиімділігін, құқыққа араласу ауырлығын және кепілдіктерін бірге бағалауға мүмкіндік береді [188]. Қазақстандық заң жобасына қолданылатын авторлық өлшем бойынша жаңа өкілеттіктің мақсатқа жарамдылығы түсіндіріліп, қолданыстағы құралдың

неліктен жеткіліксіз екені көрсетіледі. Сонымен қатар жаңа рәсімнің қорғау тарабына, дерек ұстаушыға және үшінші тұлғаларға түсіретін ауыртпалығы қарастырылады. Технологиялық ыңғайлылық өздігінен жеткілікті құқықтық негіз болып саналмайды.

Бірінші ұсыныс ҚПК-нің 47-бабында көзделген талаптармен өзара байланысты қылмыстық сот ісін жүргізу барысында дербес деректерді өңдеу және қорғау кепілдіктерін жеке норма ретінде бекітуді көздейді. Бұл ретте қолданыстағы құпиялылық талаптарын қайталаумен шектелмей, дербес деректерді жинау мен өңдеудің мақсатын, көлемін, оларды сақтау және одан әрі пайдалану тәртібін нақты айқындау ұсынылады. Осыған байланысты ҚПК-ні «Қылмыстық сот ісін жүргізуде дербес деректерді өңдеу және қорғау кепілдіктері» деп аталатын жаңа баппен толықтыру ұсынылады. Жаңа баптың нөмірі заңнамалық өзгерістерді енгізу барысында заң техникасының талаптарына сәйкес айқындалуы тиіс.

ҚПК-ні толықтыру үшін ұсынылатын «Қылмыстық сот ісін жүргізуде дербес деректерді өңдеу және қорғау кепілдіктері» атты жаңа баптың мазмұны бес негізгі ережені қамтиды.

Біріншіден, қылмыстық процесті жүргізетін орган дербес деректерді ҚПК-де көзделген міндеттерді орындау үшін қажетті және жеткілікті көлемде, нақты процестік мақсаттарға сәйкес жинауы және пайдалануы тиіс. Дербес деректерді бастапқы алу негізі оларды өзге мақсаттарда пайдалануға немесе үшінші тұлғаларға беруге өздігінен құқық бермейді. Мұндай әрекеттер заңда көзделген дербес құқықтық негіздер бойынша жүзеге асырылуы қажет. Бұл талап деректер субъектісінің келісімі талап етілмейтін жағдайларда да дербес деректерді мақсатқа сай пайдалану қағидатын сақтауға бағытталған [2; 6].

Екіншіден, қылмыстық іс үшін маңызы бар мән-жайларды анықтауға, цифрлық деректердің шығу тегі мен тұтастығын тексеруге қажетті ақпараттың сақталуы қамтамасыз етілуі тиіс. Іске қатыстылығы анықталмаған қосымша мәліметтерге қол жеткізу олардың дәлелдемелік маңызын анықтау үшін қажетті көлеммен шектелуі қажет. Бұл ретте мұндай шектеулер қорғау тарапы үшін маңызы болуы мүмкін мәліметтердің жойылуына немесе негізсіз жасырылуына әкелмеуі тиіс.

Үшіншіден, дербес деректерді беру барысында оларды алушы тұлға, берудің құқықтық негізі мен мақсаты, ұсынылған ақпараттың көлемі және берілген күні тіркелуі тиіс. Қылмыстық іс материалдарындағы бастапқы цифрлық деректер, зерттеу үшін дайындалған көшірмелер және жариялауға арналған материалдар өзара ажыратылуы қажет. Дербес деректердің құпиялылығын қамтамасыз ету мақсатында бастапқы дәлелдемелердің мазмұнын өзгертуге жол берілмеуі тиіс. Сонымен қатар техникалық тіркеу мәліметтері мен процестік құжаттардың өзара сәйкестігі қамтамасыз етілуі қажет [6; 76].

Төртіншіден, қылмыстық іс материалдарына қол жеткізуді шектеу заңда көзделген негіздер бойынша қабылданған уәжді процестік шешім арқылы жүзеге асырылуы тиіс. Мұндай шешімде шектеу қолданылатын

материалдар, оның көлемі, құқықтық негіздері, қайта қарау шарттары және шағымдану тәртібі көрсетілуі қажет. Егер дербес деректерді қорғау мақсатына қылмыстық процеске қатысушылардың құқықтарын азырақ шектейтін тәсілдер арқылы қол жеткізу мүмкін болса, материалдарға толық қолжетімділікті шектеуге жол берілмеуі тиіс [6; 153].

Бесіншіден, қылмыстық іс бойынша іс жүргізу аяқталғаннан кейін дербес деректерді одан әрі сақтау және пайдалану қажеттілігі қайта қаралуы тиіс. Негізгі іс материалдары заңнамада белгіленген тәртіппен сақталып, қосымша жұмыс көшірмелерін жою, сақтауды жалғастыру немесе басқа қылмыстық іске беру туралы шешімдер тиісті түрде тіркелуі қажет. Бұл ретте процестік шешімдерге шағымдану, қылмыстық істі қайта қарау және архивтік сақтау талаптары ескерілуі тиіс [6; 145].

Ұсынылған ережелер қылмыстық сот ісін жүргізуде дербес деректерді жинау, пайдалану, сақтау және қорғаудың өзара байланысты процестік кепілдіктерін қалыптастыруға бағытталған. Оларды ҚПК-де жеке норма ретінде бекіту цифрлық дәлелдемелермен жұмыс істеудің құқықтық тәртібін нақтылауға, дербес деректердің негізсіз таралуының алдын алуға және қылмыстық процеске қатысушылардың құқықтары мен заңды мүдделерін қорғауды күшейтуге мүмкіндік береді.

Екінші ұсыныс – деректі уақытша сақтап қалу мен оны тергеу органына беруді заңнамалық тұрғыдан анық ажырату. Қазіргі дәлелдеме жинау өкілеттіктерін түсіндіру арқылы жаңа мәжбүрлеу шарасын енгізуге болмайды. Сондықтан дерек ұстаушыға нақты сақталған мәліметті жоймау міндетін жүктейтін арнайы рәсім қажет деп танылса, оның негіздері, мерзімі, бақылауы және шағымдану тәртібі ҚПК-де тікелей бекітілуі тиіс. Екінші тараудағы екі сатылы модель осы ұсыныстың практикалық негізін құрайды [6; 111; 112].

Ұсынылатын норма мазмұны бойынша сақтап қалу талабы тек бұрыннан бар және нақты сәйкестендірілген деректерге бағытталады; болашақ коммуникацияны жинауды немесе жаңа бақылау жүргізуді қамтымайды. Талапта қылмыстық іс, дерек ұстаушы, есептік жазба не өзге идентификатор, уақыт аралығы, жойылу қаупі және сақтау көлемі көрсетіледі. Сақтап қалу деректердің мазмұнын ашуға құқық бермейді; оларды алу тиісті тергеу әрекеті немесе сұрату тәртібімен жүзеге асырылады. Сақтау қажеттілігі жойылғанда міндет тоқтатылып, бұл туралы дерек ұстаушыға хабарланады.

Зерттеу шеңберінде деректерді бастапқы сақтау мерзімін отыз тәулік деп белгілеу және қажет болған жағдайда соттың уәжді шешімі негізінде бір рет отыз тәулікке ұзарту ұсынылады. Аталған мерзімдер қолданыстағы заңнамада белгіленген талаптар ретінде емес, қылмыстық-процестік заңнаманы жетілдіруге бағытталған ғылыми ұсыныс ретінде қарастырылады. Оларды заңнамалық тұрғыдан бекіту кезінде ақпараттық жүйелер операторларының деректерді сақтау мерзімдерін, халықаралық құқықтық көмек көрсету рәсімдерінің ұзақтығын және адамның құқықтары мен бостандықтарын шектеу дәрежесін ескеру қажет. Бұл ретте заңмен

қорғалатын құпия мәліметтерге қол жеткізудің қолданыстағы процестік кепілдіктері сақталуы тиіс. Шұғыл жағдайларда деректерді сақтаудың ерекше тәртібін енгізу қажеттілігі туындаған жағдайда оның құқықтық негіздері мен қолданылу шарттары ҚПК-де жеке айқындалуы қажет. Жасырын тергеу әрекеттеріне қатысты қолданыстағы нормаларды өзге процестік әрекеттерге ұқсастық бойынша қолдануға жол берілмеуі тиіс.

С-548/21 ісінде ЕО Соты мобильдік телефон деректеріне қолжетімділіктің қарқындылығын нақты жағдайлармен, құқықтық негізбен және тәуелсіз алдын ала бақылаумен байланысты қарастырды [189]. Бұл шешімнен телефондағы кез келген деректі алуға жалпы тыйым немесе жалпы рұқсат шықпайды. Қазақстандық сұрату мен сақтап қалу рәсіміне арналған қорытынды: құрылғы түрі немесе деректің «техникалық» деп аталуы шектеудің нақты көлемін бағалауды алмастырмайды. Операцияның қандай ақпаратты ашатыны және басқа адамдарға әсері құқықтық негіздемеде көрсетілуі тиіс.

Үшінші ұсыныс – ҚПК-нің 199-бабындағы хаттама талаптарын цифрлық объектілердің ерекшелігімен толықтыру. Қолданыстағы бап әрекеттің уақыты, қатысушылары, барысы және нәтижелерін тіркеуді көздейді [6]. Ұсынылатын толықтыру осы талаптарды алмастырмайды. Оның редакциялық мазмұны: «Цифрлық мәлімет алынған немесе көшірілген жағдайда хаттамада не оның ажырамас қосымшасында дереккөз, объектінің сәйкестендіру белгілері, алу тәсілі, пайдаланылған құралдың атауы мен нұсқасы, уақыт белдеуі, файлдар тізімі және тұтастықты тексеру тәсілі көрсетіледі. Қолданылған техникалық шектеулер, іріктеу шарттары және мәліметке енгізілген қажетті өзгерістер түсіндіріледі».

Хэш есептеу мүмкін болғанда алгоритм мен мән көрсетіледі; мүмкін болмаған жағдайда себеп пен балама бақылау тәсілі тіркеледі. Бұл ерекшелік тірі жүйедегі динамикалық дерек пен кейін қалыптасатын экспорттың табиғатын ескереді. Хэштің жоқтығын барлық жағдайда автоматты жарамсыздыққа айналдыру ұсынылмайды. Процестік салдар ҚПК-нің 112 және 125-баптарына сәйкес нақты ақаудың шығу тегін, тұтастығын және тексерілуін бағалауға әсерімен анықталады [6; 44; 77]. Осындай редакция техникалық талапты шынайы орындауға мүмкіндік беріп, формалды жазбамен шектелу қаупін азайтады.

Төртінші ұсыныс ҚПК-нің 295–296-баптарын қылмыстық іс материалдарындағы цифрлық деректермен танысу тәртібін нақтылайтын ережелермен толықтыруға бағытталған. Атап айтқанда, цифрлық материалдармен танысу олардың мазмұнын толық зерделеуге және ҚПК-де белгіленген тәртіппен тексеруге мүмкіндік беретін нысанда жүзеге асырылуы тиіс. Бұл ретте заңмен қорғалатын құпияны сақтау қажеттілігі қылмыстық процеске қатысушылардың іс материалдарымен танысу құқықтарын негізсіз шектеуге әкелмеуі қажет. Цифрлық материалдардың көшірмелерін алуға заңды шектеулер белгіленген жағдайда оларды арнайы қорғалған ақпараттық ортада зерделеу және қажет болған жағдайда заңда көзделген тәртіппен маманның көмегін пайдалану мүмкіндігі қамтамасыз етілуі тиіс. Ұсынылған

толықтырулар құпия мәліметтерді қамтитын материалдарды сақтау мен пайдаланудың қолданыстағы талаптарын ескере отырып, қорғау тарапының цифрлық дәлелдемелерді тиімді тексеру мүмкіндігін қамтамасыз етуге бағытталған [6].

Қолжетімділіктің жаңа рәсімі қорғануға жеткілікті уақыт, қажетті техникалық құрал және түсінікті тізімдеме болғанда ғана тиімді болады. Материалдың көлемі, файл саны немесе форматы туралы ақпарат тарапқа танысуды жоспарлауға көмектеседі. Ашылмайтын форматтағы файлды беру құқықтың орындалғанын формалды көрсетуге жеткіліксіз. Егер материал өзгертілген жұмыс көшірмесі түрінде ұсынылса, тарапқа оның қандай операция арқылы дайындалғаны түсіндіріледі. Дербес деректі қорғау мақсатындағы шектеу дәлелдеменің контекстін бұрмалаған жағдайда, толық нұсқаны заңды қорғалған тәртіппен тексеру мәселесі шешіледі.

Бесінші ұсыныс ҚПК-нің 201-бабын іске асыратын рәсімдерде жариялау мен заңды процестік беруді нақты ажыратуға бағытталады. Кодексте процестік құжаттар арқылы және тиісті міндеттеме берген қорғаушы, сарапшы не маманға мәлімет беруге қатысты ерекшеліктер бар [6]. Сондықтан бұл құқықтарды қайтадан «жаңа рұқсат» ретінде енгізу қажет емес. Нақтылау ақпарат берудің көлемін, қауіпсіз арнасын және алушының міндетін тіркеуге қатысты болуы тиіс. Мұндай есептің болмауы заңда рұқсат етілген қорғау әрекетін өздігінен тыйым салынған жариялау деп тануға негіз болмауы керек.

Алтыншы ұсыныс сот актілерінің көпшілікке жариялауға арналған көшірмелерін дайындаудың бірыңғай тәртібін нормативтік деңгейде бекітуді көздейді. Бұл тәртіп ҚПК-де белгіленген жариялылық қағидаты мен дербес деректердің құпиялылығын қамтамасыз ету талаптарының өзара үйлесімділігіне негізделуі тиіс [6]. Атап айтқанда, сот актілерін жариялауға дайындау барысында тұлғаны тікелей және жанама сәйкестендіруге мүмкіндік беретін мәліметтерді анықтау, жарияланатын көшірменің түпнұсқамен сәйкестігін қамтамасыз ету, қате жарияланған деректерді түзету және тиісті өтініштерді қарау рәсімдерін нақтылау ұсынылады. Бұл ретте дербес деректерді қорғау мақсатында сот актісінің түпнұсқасын, оның құқықтық негіздемесін немесе қарар бөлігін өзгертуге жол берілмеуі тиіс. Сонымен қатар қылмыстық процеске қатысушыларға сот актілерін заңда белгіленген тәртіппен ұсыну және олардың көпшілікке арналған көшірмелерін жариялау рәсімдері өзара ажыратылуы қажет.

13-кесте – ҚПК-ні нақтылау жөніндегі ұсыныстардың мазмұны

№	Реттеу бағыты	Ұсынылатын өзгеріс	Сақталатын кепілдік
1	47-баппен байланысты арнайы норма	Мақсат, көлем, беру есебі, сақтау мәртебесі	Қолданыстағы құпия режимдері мен қорғау құқығы
2	Сақтап қалудың жеке рәсімі	Бұрыннан бар нақты деректі уақытша жоймау	Сақтау мазмұнға қолжетімділік бермейді; бақылау және шағым
3	199-баптағы цифрлық тіркеу	Дереккөз, құрал, уақыт белдеуі, тізімдеме, тұтастық	Техникалық мүмкіндіктің шегі түсіндіріледі; жеке бағалау

№	Реттеу бағыты	Ұсынылатын өзгеріс	Сақталатын кепілдік
4	295–296-баптардағы танысу	Түсінікті формат, жеткілікті уақыт, қорғалған тексеру	Танысу құқығы мен құпия көшірме тәртібі сақталады
5	201-бапты іске асыру	Заңды процестік беру мен жариялауды ажырату	Қорғаушының заңды әрекетіне жаңа тыйым енгізілмейді
6	29 және 47-баптарды үйлестіру	Жария көшірме және қате жариялауды түзету	Сот актісінің түпнұсқасы мен құқықтық уәжі өзгермейді

Ескерту: Авторлық заңнамалық ұсыныстар. Қолданыстағы норма ретінде қолдануға арналмаған. Нормативтік негіз: [6; 184].

Заң нормасы электрондық жүйеде орындалатын нақты әрекетке айналмаса, оның тиімділігі шектеулі болады. Сондықтан жаңа режимді енгізу алдында дерек ағындарының картасын жасау ұсынылады: материал қайдан түседі, қайда сақталады, қандай көшірмелер пайда болады және кімге беріледі. ISO/IEC 29134:2023 жеке өмірге ықпалды бағалау процесіне арналған бағдар береді [190]. Қылмыстық процесс үшін мұндай бағалау нақты іс бойынша судьяның шешімін алмастырмайды; ол ақпараттық жүйе немесе жалпы рәсім енгізілгенге дейінгі ұйымдастырушылық тәуекелдерді анықтайды. Қорғау мен жәбірленуші өкілдерінің қатысуы құқықтарға әсерді жан-жақты бағалауға мүмкіндік береді.

NIST SP 800-53A бақылау шараларының бар екенін ғана емес, олардың орындалуын тексеруді қарастырады [191]. Осы тәсілге сәйкес пилоттық жүйеде рұқсаттың уақтылы тоқтатылуы, журналдың толықтығы, жария көшірменің қауіпсіздігі және резервтік қалпына келтіру тексеріледі. Бірақ тексеру хаттамасында шынайы қылмыстық іс материалын қажетсіз таратуға жол берілмейді. Функционалдық сынақтар үшін құпия дерегі жоқ арнайы оқу объектілерін пайдалануға болады; нақты істер бойынша тексеру заңды өкілеттікпен және қажетті көлемде жүргізіледі. Ақпараттық қауіпсіздік аудиті сот төрелігінің мазмұнына араласуға негіз болмайды.

Деректерді ұстаушылармен өзара іс-қимыл барысында екінші тарауда ұсынылған екі деңгейлі сұрату моделін қолдану көзделеді. Бұл модель қылмыстық іс материалдарында сұратудың толық құқықтық негіздемесін сақтауды және деректерді ұстаушы ұйымға сұратуды орындау үшін қажетті мәліметтерді ғана ұсынуды қамтиды. Мұндай тәсіл тергеу болжамдары мен іске қатысы жоқ тұлғалардың дербес деректерінің негізсіз жария етілуін болдырмауға бағытталған. ЭЫДҰ-ның 2022 жылғы жеке сектордағы деректерге мемлекеттік органдардың қол жеткізуі жөніндегі декларациясында құқықтық негіздердің айқындығы, тиісті рұқсат беру рәсімдері, деректерді өңдеу және бақылау кепілдіктерінің өзара байланысы көрсетілген [192]. Аталған халықаралық құжат салыстырмалы-құқықтық бағдар ретінде қарастырылып, Қазақстан Республикасында деректерді сұратудың заңдылығы ұлттық заңнама мен қолданылатын халықаралық шарттардың талаптарына сәйкес айқындалуы тиіс.

Трансшекаралық бағытта негізгі ұсыныс – сақтап қалу, беру және кейінгі пайдалану шарттарын бір сұратудың ішінде айқын ажырату.

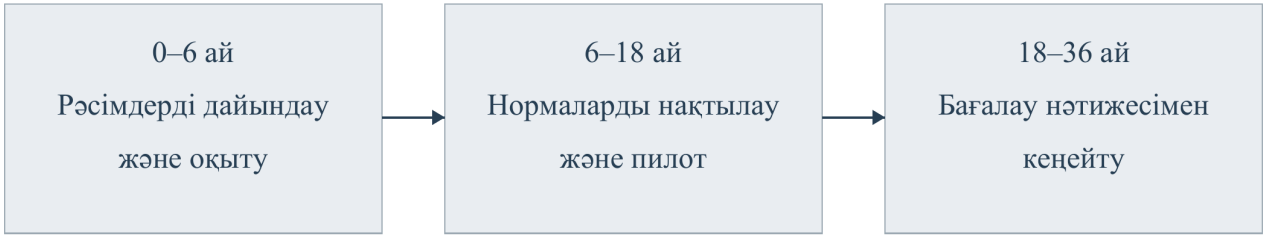
Қазақстанның нақты халықаралық шартқа қатысу мәртебесі әр құрал үшін тексеріледі. Екінші тарауда қаралған Будапешт конвенциясы мен ЕО-ның электрондық дәлелдемелер актілері ұлттық органға өздігінен шетелдік провайдерге міндетті талап қою өкілеттігін бермейді. Құқықтық көмек арқылы алынған ақпараттың мақсаты, қайта берілуі және сақталуы жөніндегі шарттар іс материалындағы есепке енгізілуі керек. Осындай тәртіп трансшекаралық қатынаста да деректің қозғалысын тексерілетін етеді.

Үлкен массивтегі жеке деректерді іздеу, құжаттарды жіктеу және жария көшірмедегі сәйкестендіру белгілерін табу автоматтандырылуы мүмкін. Қазақстанның «Жасанды интеллект туралы» заңы осы жүйелерді пайдалану кезіндегі жалпы құқықтық ортаны қалыптастырады [193]. Алайда мұндай жүйенің болуы ҚПК-де көзделмеген тергеу өкілеттігін туғызбайды. Бағдарлама берген сәйкестік адамның кінәсін дәлелдейтін дербес қорытынды ретінде қабылданбауы керек. Нәтиженің негізі, пайдаланылған деректер және ықтимал қате түсіндірулер тиісті процестік нысанда тексеріледі [6; 87].

NIST AI RMF тәуекелдерді анықтау, бағалау және басқару міндеттерін жүйелейді [194]. CEPEJ-дің жасанды интеллект жөніндегі этикалық хартиясы сот төрелігінде құқықтарды сақтау, кемсітпеу, сапа және пайдаланушы бақылауына назар аударады [195]. Осы құжаттарға сүйенген авторлық ұсыныс бойынша автоматтандыруға арналған жүйе алдымен көмекші міндетте қолданылуы тиіс: ықтимал жеке деректі белгілеу, техникалық қайталануды табу, тізімдеме жасау. Маңызды материалды тараптан жасыру, деректі жою немесе тұлғаға процестік салдар жүктеу туралы шешімді құзыретті адам қабылдап, уәжін көрсетуі керек.

ЕО Сотының C-817/19 шешімінде жолаушылар туралы деректерді автоматтандырылған талдау мен адам арқылы тексерудің шектері қарастырылған [196]. Бұл салыстырмалы материал алгоритмнің түсіндірілетіндігі мен қате сәйкестікті тексеруге көңіл бөлуге негіз береді. Қазақстандағы тергеу жүйесі үшін ұсынылатын талаптар: бағдарламаның нұсқасын тіркеу, маңызды нәтижені бастапқы дерекпен салыстыру, өзгерген модельдің ықпалын бағалау және адамның түзету әрекетін есепке алу. Жүйенің жалпы дәлдік көрсеткіші нақты іс бойынша нәтижені тексерудің орнына қолданылмайды. Дәл сол сияқты құжаттарды автоматты иесіздендіру адам тексеруінсіз жариялауға жеткілікті кепілдік ретінде қабылданбайды.

CEPEJ-дің цифрлық сот төрелігіне көшу жөніндегі нұсқаулығы технологиялық өзгерісті жұмыс процесімен, пайдаланушылармен және ұйымдастырушылық дайындықпен байланыстырады [197]. Осы негізде реформаны бірден барлық органға бірдей енгізудің орнына шектеулі пилот арқылы тексеру ұсынылады. Пилоттың заңды шегі айқын болуы тиіс: ол техникалық тәртіп пен ұйымдастыруды сынай алады, бірақ заң күшіне енбей жаңа мәжбүрлеу шарасын қолдануға құқық бермейді. Қолданыстағы қатысушы құқықтары пилоттың зерттеу мақсаты үшін шектелмеуі тиіс.



6-сурет – Ұсыныстарды кезеңдермен енгізу моделі

Қысқа мерзімді кезеңде қолданыстағы өкілеттіктер шегінде деректер ағынының есебі, цифрлық хаттаманың техникалық қосымшасы, қауіпсіз беру тәртібі және жария көшірмені тексеру әдістемесі дайындалады. Орта мерзімді кезең ҚПК-ге ұсынылған өзгерістерді құқықтық сараптауды, мүдделі тараптармен талқылауды және заңнамалық рәсім аяқталғаннан кейін пилоттауды қамтиды. Ұзақ мерзімді кезеңде пилот нәтижесі бойынша жүйелерді кеңейту, тәуелсіз бағалау және халықаралық өзара іс-қимыл тетіктерін жетілдіру жүргізіледі. Кезеңдердің ұсынылатын уақыт аралықтары жоспарлау параметрлері болып табылады; олардың орындалғаны туралы эмпирикалық тұжырым жасалмайды.

14-кесте – Ұсыныстарды енгізудің кезеңдері мен нәтижелері

№	Ұсынылатын кезең	Негізгі жұмыс	Тексерілетін нәтиже
1	Қысқа мерзім 0–6 ай	Дерек ағындарын есептеу; үлгілер; оқыту; қауіпсіз беру	Қолданыстағы заң шегіндегі бірыңғай рәсімдер
2	Орта мерзім 6–18 ай	Заң жобасы; құқықтық сараптама; заңды негізі бар пилот	Құқықтарға ықпалы тексерілген нормативтік және техникалық шешім
3	Ұзақ мерзім 18–36 ай	Бағалау нәтижесі бойынша кеңейту; сыртқы тексеру; халықаралық үйлестіру	Өлшенетін нәтижесі бар және қайта қаралатын тұрақты режим

Ескерту: Уақыт аралықтары – авторлық жоспарлау параметрлері. Қысқа мерзімді жұмыс қолданыстағы өкілеттіктермен шектеледі; жаңа мәжбүрлеу шарасы заң күшіне енгеннен кейін ғана қолданылады.

OECD-ның реттеушілік ықпалды бағалау жөніндегі қағидаттары мәселені анықтау, баламаларды салыстыру және кейінгі бағалауды байланыстырады [198]. Осы әдіс бойынша нормативтік өзгерістен бөлек баламалар да қаралады: қолданыстағы норманы түсіндіру, мамандарды оқыту, сұрату нысанын жақсарту немесе жүйелік рұқсатты реттеу. Егер проблема өкілеттіктің жетіспеуінен емес, қолданыстағы талаптың орындалмауынан туындаса, жаңа шектеу енгізу артық болуы мүмкін. Сондықтан әр ұсыныстың нормативтік қажеттілігі мен ұйымдастырушылық жеткіліктілігі жеке тексеріледі.

Тергеу тиімділігін тек сотқа жіберілген істердің немесе сотталған адамдардың санымен өлшеу деректерді қорғаудың сапасын көрсетпейді. Екінші тарауда қарастырылған 302 тіркелген құқық бұзушылық пен сот шешімі қабылданған тұлғалар жөніндегі қатарлар бірдей когортаны құрамайды. Осы себепті оларды бір-біріне бөліп, реформаның табыстылық көрсеткішін есептеу негізсіз. БҰҰ-ның қылмыстық әділет статистикасы

жөніндегі нұсқаулығы есеп бірліктері мен дерек жүйесінің құрылымын анықтаудың маңызын көрсетеді [199]. Жаңа мониторингте құқық бұзушылық, қылмыстық іс, сұрату, дерек объектісі және тұлға жеке есеп бірліктері ретінде ажыратылуы керек.

15-кесте – Тергеу тиімділігі мен деректерді қорғауды бірге бағалау көрсеткіштері

№	Өлшем	Есептеу немесе тіркеу тәртібі	Түсіндіру шегі
1	Деректі сақтап қалу уақыты	Заңды талаптың тіркелуі мен орындалуы арасындағы уақыт	Оқиға мен тіркеу күндерінің айырмасымен шатастырылмайды
2	Беру есебінің толықтығы	Негізі, мақсаты, алушысы толық операциялар / тексерілген тиісті операциялар	Қолданылатын міндет пен іріктеме алдын ала анықталады
3	Қайта тексерілу мүмкіндігі	Тәуелсіз тексеруге жеткілікті құжаттары бар объектілердің үлесі	Хэштің бар болуымен ғана өлшенбейді
4	Қолжетімділік даулары	Өтініштер, шешімдер, өзгертілген шектеулер және себептер	Шағым санының өсуі құқықты пайдалану артуынан да болуы мүмкін
5	Қайта таралу оқиғалары	Расталған оқиғалар, зардап шеккен дерек түрлері және әсері	Анықтау сапасы өзгергенде кезеңдер тікелей салыстырылмайды
6	Жария көшірме сапасы	Тексерілген мәтіндердегі тікелей және жанама ашылу ақаулары	Автоматты белгілердің санымен ғана бағаланбайды
7	Пайдаланушыға түсетін ауыртпалық	Техникалық кідіріс, қайта сұрату және танысу жағдайы	Заңды қорғауға қажетті уақыт тиімсіздік деп есептелмейді

Ескерту: Болашақ мониторингке арналған авторлық индикаторлар. Бұл кестеде өлшенген нәтижелер немесе жаңа эмпирикалық сандар берілмейді. Әдіснамалық негіз: [199; 198].

Бағалау үшін көрсеткіштің алымы мен бөлімі, бақылау кезеңі және дереккөзі алдын ала белгіленеді. Мысалы, «құқықтық негізі толық тіркелген беру операцияларының үлесі» осы талап қолданылатын тексерілген операциялар санына қатысты есептеледі. «Деректі сақтап қалу уақыты» оқиға болған күннен емес, заңды талап тіркелген сәттен бастап өлшенеді. Ал қорғаушының материалмен танысуына кеткен уақыт жүйенің техникалық кідірісінен бөлек тіркелуі тиіс. Осы ажыратулар тергеудің баяулығын құқықты іске асыруға қажетті уақытпен шатастырмауға көмектеседі.

The Magenta Book бағалау нұсқаулығы пилоттық араласудың нәтижесін бағалау кезінде бастапқы көрсеткіштерді және мүмкін болған жағдайда салыстыру тобын алдын ала айқындаудың маңызын көрсетеді [200, 23 б.]. Сонымен қатар байқалған өзгерісті интервенцияның өз әсеріне жатқызу үшін кеңірек контексті және өзге ықпалдарды – жалпы үрдістерді, қатар жүргізілген өзге шараларды, кездейсоқ факторлар мен іріктеу ерекшеліктерін – ескеру қажеттігі атап өтіледі [200, 53 б.]. Осыған сүйене отырып, пилот нәтижесін оны енгізуге дейінгі кезеңмен және салыстыруға келетін бөлімшелермен бағалау ұсынылады. Бағалау кезінде істердің күрделілігі, цифрлық материалдардың көлемі, шетелдік дереккөздердің болуы және мамандармен қамтамасыз етілу деңгейі ескерілуі тиіс. Егер салыстыру тобы құрылмаса немесе өзге ықпалдарды сенімді түрде ажырату мүмкін болмаса,

алынған нәтижелер себеп-салдарлық әсердің дәлелі ретінде емес, сипаттамалық бақылау ретінде ұсынылуы қажет. Реформаның тиімділігіне қатысты пайыздық өсім алдын ала белгіленбей, нақты эмпирикалық деректер негізінде ғана айқындалуы тиіс.

Кіріспеде көрсетілген 850 респонденттің сауалнамасы реформаның қажеттілігі туралы пікірлерді сипаттайды, бірақ ұсынылатын нормалардың тиімділігін тәжірибеде тексерген эксперимент болып табылмайды. Бірыңғай стандарттарды қолдау мен олардың іс жүзінде орындалуы әртүрлі зерттеу сұрақтары. Сондықтан сауалнамадағы 71,0% бекіту тәртібін нақтылау қажеттілігін негіздеуде пайдаланылғанымен, бұл көрсеткішті болашақ қателердің азаю үлесі ретінде көрсетуге болмайды. Реформаның нәтижесін бағалау үшін сұратулар, цифрлық объектілер, қолжетімділік шешімдері және инциденттер бойынша жаңа заңды мониторинг қажет. Осы мониторингтің өзі деректерді азайту қағидасына бағынады.

Қылмыстық-процестік заңнаманы жетілдіру дербес деректердің арнайы кепілдіктерін бекіту, сақтап қалу мен алуды ажырату, цифрлық объектіні хаттамада тіркеуді нақтылау және материалмен тиімді танысу рәсімін қамтамасыз ету бағыттарында ұсынылды. Редакциялық үлгілер қолданыстағы құқықтарды қайталамай, олардың цифрлық ортада орындалуына қажетті шарттарды нақтылауға арналған. Жаңа мәжбүрлеу өкілеттігі заңмен енгізілуі, ал техникалық регламент оның шектерін кеңейтпеуі тиіс.

Институционалдық енгізудің негізгі шарттары – жауапкершілікті бөлу, құқықтарға ықпалды алдын ала бағалау, пилоттың заңды шегін сақтау және автоматтандырылған нәтижені адам арқылы тексеру. Дерек ұстаушылармен және шетелдік органдармен өзара іс-қимылда әрбір беру операциясының құқықтық негізі, мақсаты және кейінгі пайдалану шарттары есепке алынуы тиіс. Қолжетімділік журналы мен техникалық аудит қорғау құпиясын немесе сот тәуелсіздігін шектеуге пайдаланылмайды.

Реформаның нәтижесі тергеу жылдамдығы, дәлелдеменің тексерілуі және деректер субъектілерінің құқықтарын қорғау көрсеткіштерінің жиынтығымен бағалануы керек. Ұсынылған кезеңдер мен индикаторлар іске асыруға арналған модель болып табылады. Олардың тиімділігі кейінгі эмпирикалық бағалауда анықталады; бастапқы статистика мен сауалнама нәтижелері мұндай бағалаудың орнына жүрмейді.

Жүргізілген талдау нәтижесінде дербес деректерді қорғаудың қылмыстық-процестік кепілдіктері деректі алудан бастап оның кейінгі тағдырын шешуге дейінгі бірізді міндеттер жүйесі ретінде негізделді. Арнайы режимнің мәні мақсатпен шектелген өңдеу, деректің процестік қызметіне сәйкес қолжетімділік және әрбір операцияның құқықтық негізін тексеру арқылы ашылады. Осылайша, дербес деректерді қорғау талаптары қылмыстық іс жүргізудің жекелеген кезеңдеріне қосымша элемент ретінде емес, дәлелдемелермен жұмыс істеудің бүкіл процесіне кіріктірілген кепілдіктер жүйесі ретінде қарастырылады.

Диссертацияның негізгі тұжырымы бойынша тергеу тиімділігі мен

дербес деректерді қорғау бірін-бірі толықтыратын процестік міндеттер болып табылады. Құқықтық негізі айқын, көлемі қажетті, техникалық тұтастығы сақталған және тараптар тексере алатын ақпарат дәлелдеуге де, адамның құқықтарын қорғауға да қызмет етеді. Осы байланыс сақталған жағдайда ғана цифрландыру қылмыстық процестің сапасын арттыратын құралға айналады. Ұсынылған нормалар, қолжетімділік рәсімдері және бағалау өлшемдері осы тұжырымды заңнама мен құқық қолдану тәжірибесіне енгізудің өзара байланысты жолдарын құрайды.

ҚОРЫТЫНДЫ

Диссертациялық зерттеу барысында дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің қылмыстық-процестік мәселелері кешенді түрде қарастырылып, олардың теориялық-құқықтық негіздері, құқықтық реттелу ерекшеліктері және құқық қолдану практикасында туындайтын проблемалары зерделенді. Қазақстан Республикасының қылмыстық және қылмыстық-процестік заңнамасына, дербес деректерді қорғау саласындағы нормативтік құқықтық актілерге, халықаралық стандарттарға, шетелдік тәжірибеге, ресми статистикалық мәліметтерге және эмпирикалық зерттеу материалдарына жүргізілген талдау нәтижесінде аталған санаттағы қылмыстық құқық бұзушылықтарды тергеп-тексерудің тиімділігін арттыруға бағытталған ғылыми тұжырымдар қалыптастырылды.

Зерттеу нәтижелері цифрлық технологиялардың дамуы дербес деректерді заңсыз жинау, өңдеу және тарату әрекеттерінің жасалу тәсілдерін ғана емес, оларды анықтау мен дәлелдеудің мазмұнын да елеулі түрде өзгерткенін көрсетті. Қазіргі жағдайда қылмыстық құқық бұзушылықтың мән-жайларын анықтау электрондық құрылғыларда, ақпараттық жүйелерде, деректер базаларында және цифрлық платформаларда қалыптасатын мәліметтерді алумен тығыз байланысты. Мұндай ақпараттың ерекшелігі оның өзгертілуі, көшірілуі, жойылуы немесе бірнеше юрисдикцияда қатар сақталуы мүмкін екенінен көрінеді. Сонымен бірге тергеп-тексеру барысында алынатын деректердің едәуір бөлігі адамның жеке өміріне қатысты мәліметтерді қамтиды. Осы жағдай қылмыстық іс бойынша дәлелдемелерді жинау қажеттілігі мен дербес деректер субъектілерінің құқықтарын қорғау арасындағы теңгерімді қамтамасыз етуді дербес ғылыми мәселе ретінде қарастыруды талап етеді.

Диссертациялық зерттеудің мақсатына сәйкес дербес деректердің қылмыстық процестегі құқықтық табиғаты анықталып, оларды пайдаланудың сараланған режимі негізделді, дерек ұстаушылардан мәліметтер алудың процестік тәртібін жетілдіру жолдары ұсынылды, цифрлық ортадағы дәлелдемелердің ұғымы мен оларды бағалау өлшемдері тұжырымдалды, дербес деректерді иесіздендірудің құқықтық тетігі әзірленді және трансшекаралық цифрлық ақпаратты алудың халықаралық-құқықтық мүмкіндіктері қарастырылды. Аталған нәтижелер зерттеудің жеті міндетін орындау барысында алынған және қорғауға ұсынылған алты ғылыми тұжырымның мазмұнын құрайды.

1. Дербес деректердің қылмыстық процестегі қосарлы құқықтық табиғаты негізделіп, олардың авторлық қылмыстық-процестік анықтамасы тұжырымдалды.

Дербес деректердің құқықтық табиғатын зерттеу олардың құқықтық мәртебесі тек ақпараттық қатынастар шеңберінде айқындалмайтынын көрсетті. Қылмыстық іс жүргізу барысында дербес деректер құқықтық қорғау

объектісі болумен қатар, қылмыстық құқық бұзушылықтың жасалу тәсілін, оқиғаның мән-жайларын, оған қатысы бар адамдарды, құқыққа қайшы әрекеттердің салдарын және дәлелденуге жататын өзге де фактілерді анықтауға мүмкіндік беретін ақпарат көзі ретінде пайдаланылады. Осы ерекшелік олардың қылмыстық процестегі дербес құқықтық сипаттамасын қалыптастыру қажеттігін негіздейді.

Қолданыстағы құқықтық реттеуде дербес деректерді қорғаудың жалпы талаптары белгіленгенімен, қылмыстық іс жүргізу барысында мұндай мәліметтердің дәлелдемелік маңызы мен оларды қорғау қажеттілігінің өзара байланысын арнайы ғылыми тұрғыдан айқындау маңызды. Өйткені тергеу органы үшін белгілі бір ақпараттың қылмыстық іс бойынша маңызы болуы оны шектеусіз жинауға, пайдалануға немесе таратуға құқықтық негіз бола алмайды. Кез келген мәліметті алу оның қылмыстық іс үшін қажеттілігімен, заңда белгіленген процестік тәртіппен және адамның құқықтарын қорғау талаптарымен байланыстырылуы тиіс.

Осыған байланысты зерттеуде дербес деректердің қосарлы құқықтық табиғаты туралы ғылыми тұжырым қалыптастырылды. Біріншіден, олар қылмыстық іс бойынша дәлелденуге жататын мән-жайларды анықтауға мүмкіндік беретін ақпараттық мазмұнға ие. Екіншіден, олар адамның жеке өміріне қол сұғылмаушылық, жеке және отбасылық құпияны сақтау, өзі туралы мәліметтердің заңсыз пайдаланылуынан қорғалу құқықтарымен байланысты ерекше құқықтық қорғау объектісі болып табылады. Бұл екі сипат бір-бірінен оқшау қарастырылмайды, керісінше дербес деректерді қылмыстық процесте пайдаланудың құқықтық шектерін бірлесе айқындайды.

Жүргізілген талдау негізінде келесі авторлық анықтама ұсынылды: «Дербес деректер – белгілі бір жеке тұлғаны тікелей немесе жанама айқындайтын не айқындауға мүмкіндік беретін, қылмыстық іс бойынша дәлелденуге жататын мән-жайларды анықтау үшін маңызы бар немесе қылмыстық-процестік әрекеттер барысында пайдаланылатын, алынуының заңдылығына қарамастан арнайы құқықтық қорғауға жататын мәліметтер».

Ұсынылған анықтаманың ғылыми ерекшелігі дербес деректердің ақпараттық мазмұнын олардың қылмыстық-процестік айналымдағы құқықтық режимімен байланыстыруында. Анықтамада тұлғаны тікелей немесе жанама сәйкестендіру мүмкіндігі дербес деректердің негізгі белгісі ретінде қарастырылса, оларды қылмыстық іс жүргізу мақсатында алу, өңдеу, пайдалану және қорғау осы мәліметтердің процестік ерекшелігін сипаттайды. Мұндай тәсіл дербес деректердің жалпы құқықтық ұғымын алмастыруды емес, олардың қылмыстық процесте пайдаланылуына тән белгілерді ғылыми тұрғыдан нақтылауды көздейді.

Дербес деректердің дәлелдемелік маңызы олардың нақты қылмыстық іс бойынша қандай мән-жайларды анықтауға мүмкіндік беретінімен айқындалады. Мәселен, ақпараттық жүйеге қол жеткізу уақыты, пайдаланушының әрекеттері, деректерді көшіру фактісі немесе мәліметтердің үшінші тұлғаларға берілуі туралы ақпарат қылмыстық құқық бұзушылықтың объективтік белгілерін анықтауға ықпал етуі мүмкін. Алайда осы

мәліметтердің құрамында іске қатысы жоқ адамдардың дербес деректері де болуы ықтимал. Сондықтан дәлелдемелік ақпаратты жинау кезінде оның қажетті көлемін анықтау және артық мәліметтердің алынуын шектеу маңызды процестік талап ретінде қарастырылуы тиіс.

Осы ғылыми тұжырымның негізінде дербес деректерді қылмыстық процесте пайдаланудың заңдылық, қажеттілік, мөлшерлестік және құпиялылық талаптарына сүйенетін құқықтық тәсілі ұсынылды. Аталған талаптар қылмыстық іс бойынша дәлелдемелерді жинаудың тиімділігіне кедергі келтірмей, адамның жеке өміріне негізсіз араласуды болдырмауға бағытталған. Сонымен қатар олар дербес деректерді алу мен пайдалану жөніндегі процестік шешімдердің негізділігін тексеруге мүмкіндік береді.

Демек, зерттеудің бірінші ғылыми нәтижесі дербес деректердің қылмыстық-процестік мәртебесін олардың қосарлы құқықтық табиғаты арқылы айқындап, авторлық анықтамасын қалыптастырумен сипатталады. Бұл тұжырым дербес деректерді дәлелдемелік мақсатта пайдаланудың құқықтық шектерін нақтылауға және оларды қорғаудың арнайы процестік кепілдіктерін ғылыми тұрғыдан негіздеуге мүмкіндік береді.

2. Жалпыға бірдей қолжетімді және қолжетімділігі шектеулі дербес деректерді қылмыстық процесте пайдаланудың сараланған құқықтық режимі ғылыми тұрғыдан негізделді.

Дербес деректерді қылмыстық іс жүргізу барысында алу мен пайдаланудың ерекшеліктерін талдау олардың қолжетімділік деңгейі тиісті процестік тәртіпті айқындауда маңызды рөл атқаратынын көрсетті. Дегенмен мәліметтердің жалпыға бірдей қолжетімді немесе қолжетімділігі шектеулі санатқа жатқызылуы олардың дәлелдемелік маңызын өздігінен анықтамайды. Бұл мәселе ақпараттың алыну көзімен, мазмұнымен, пайдаланылу мақсатымен және қылмыстық іс бойынша қажеттілігімен өзара байланыста бағалануға тиіс.

Зерттеу барысында жалпыға бірдей қолжетімді дербес деректердің ашық ақпараттық ресурстарда орналастырылуы оларды кез келген мақсатта және шектеусіз көлемде пайдалануға құқық бермейтіні негізделді. Атап айтқанда, әлеуметтік желілерде, ашық деректер базаларында немесе интернет-ресурстарда жарияланған мәліметтердің қылмыстық іс үшін маңызы болуы мүмкін. Алайда олардың ашық жариялануы қылмыстық процесті жүргізетін органды мәліметтерді жинаудың заңды мақсатын айқындау, ақпараттың дәлелденуге жататын мән-жайларға қатыстылығын тексеру және адамның конституциялық құқықтарын сақтау міндетінен босатпайды.

Қолжетімділігі шектеулі дербес деректерге қатысты құқықтық талаптар ақпараттың мазмұнына және заңмен белгіленген қорғау режиміне қарай нақтылануға тиіс. Мұндай мәліметтерді алу кезінде тиісті құқықтық негіздің болуы, қажетті процестік шешімнің қабылдануы, заңда көзделген жағдайларда санкция алу, сұратылатын ақпараттың көлемін шектеу және оған қол жеткізетін тұлғалар шеңберін айқындау ерекше маңызға ие. Аталған

талаптардың сақталуы қылмыстық іс бойынша дәлелдемелерді жинаудың заңдылығын қамтамасыз етудің құрамдас бөлігі болып табылады.

Жүргізілген зерттеу нәтижесінде дербес деректерді пайдаланудың сараланған қылмыстық-процестік өлшемдер жүйесі ұсынылды. Оның мазмұны мәліметтердің құқықтық мәртебесін айқындауды, алыну көзінің заңдылығын анықтауды, қылмыстық іс бойынша дәлелдемелік маңызын негіздеуді, ақпарат көлемінің тергеп-тексеру мақсатына сәйкестігін бағалауды, заңда белгіленген рұқсат беру тәртібін сақтауды және алынған деректерді одан әрі пайдалану мен қорғаудың құқықтық шектерін белгілеуді қамтиды.

Бұл тәсілдің ғылыми жаңалығы дербес деректердің қолжетімділік деңгейі мен оларды қылмыстық процесте пайдаланудың заңдылығын өзара байланысты, бірақ дербес құқықтық өлшемдер ретінде ажыратуында. Мәліметтің жалпыға бірдей қолжетімді болуы оны кез келген тергеу әрекеті барысында шектеусіз пайдалануға құқықтық негіз болып табылмайды. Сол сияқты ақпараттың қолжетімділігі шектеулі болуы оны қылмыстық іс жүргізу мақсатында алуға абсолютті тыйым салуды білдірмейді. Негізгі мәселе тиісті құқықтық негіздің, процестік тәртіптің және адамның құқықтарын қорғау кепілдіктерінің сақталуымен айқындалады.

Дербес деректерді цифрлық өңдеу жағдайында мұндай саралаудың маңызы арта түседі. Бірнеше ашық дереккөзден алынған мәліметтерді біріктіру арқылы адамның жеке өміріне қатысты бастапқы ақпаратта тікелей көрсетілмеген мән-жайларды анықтау мүмкіндігі туындайды. Осыған байланысты ақпараттың құқықтық режимін бағалау кезінде оның жеке дереккөздегі қолжетімділігімен шектелмей, мәліметтерді біріктіру және өңдеу нәтижесінде қалыптасатын ақпараттың мазмұнын, оны пайдаланудың мақсатын және дербес деректер субъектісінің құқықтарына ықтимал әсерін де ескеру қажет.

Ұсынылған ғылыми тәсіл дербес деректерді алу мен пайдаланудың қажеттілігі және мөлшерлестігі талаптарын қылмыстық-процестік деңгейде нақтылауға бағытталған. Қылмыстық іс бойынша қажетті ақпараттың көлемін алдын ала айқындау тергеу әрекеттерінің мақсаттылығын арттыруға, іске қатысы жоқ адамдар туралы мәліметтердің негізсіз жиналуын шектеуге және алынған ақпараттың сақталуы мен пайдаланылуының құқықтық режимін дұрыс белгілеуге мүмкіндік береді.

Зерттеу барысында анықталған құқықтық және практикалық мәселелерді шешу мақсатында Қазақстан Республикасы Қылмыстық-процестік кодексінің 122-бабын мынадай мазмұндағы жаңа бөлікпен толықтыру ұсынылады:

«Қылмыстық іс бойынша дербес деректерді жинау олардың дәлелденуге жататын мән-жайларға қатыстылығы, алынуының қажеттілігі, сұратылатын мәліметтер көлемінің мөлшерлестігі және қолжетімділік деңгейі ескеріле отырып жүзеге асырылады.

Жалпыға бірдей қолжетімді дербес деректерді жинау кезінде олардың алыну көзінің заңдылығы, қылмыстық іс бойынша маңыздылығы және пайдаланудың құқықтық негізі анықталуы тиіс.

Қолжетімділігі шектеулі дербес деректерді жинау осы Кодексте және Қазақстан Республикасының өзге де заңдарында белгіленген құқықтық негіздер мен арнайы процестік кепілдіктер сақталған жағдайда жүзеге асырылады.

Қылмыстық іс бойынша дәлелденуге жататын мән-жайларды анықтау үшін қажетті көлемнен артық дербес деректерді негізсіз жинауға жол берілмейді».

Ұсынылған нормативтік толықтыру дербес деректерді жинаудың жалпы құқықтық талаптарын қылмыстық-процестік қатынастардың ерекшеліктеріне сәйкес нақтылауға бағытталған. Оның ғылыми жаңалығы жалпыға бірдей қолжетімді және қолжетімділігі шектеулі дербес деректердің қолданыстағы құқықтық жіктелуін қайталауда емес, осы жіктеуді дәлелдемелерді жинаудың заңдылығын бағалауға арналған сараланған процестік өлшемдер жүйесімен байланыстыруында. Атап айтқанда, дербес деректердің қолжетімділік деңгейі, дәлелдемелік маңызы, оларды алудың қажеттілігі мен мөлшерлестігі өзара байланысты құқықтық талаптар ретінде қарастырылып, қылмыстық іс жүргізу барысында адамның жеке өміріне негізсіз араласуды шектеудің қосымша кепілдіктері ұсынылады.

Осылайша, зерттеудің екінші ғылыми нәтижесі дербес деректерді қылмыстық процесте пайдаланудың сараланған құқықтық режимін ғылыми тұрғыдан негіздеумен және оны Қазақстан Республикасы Қылмыстық-процестік кодексінің 122-бабында нормативтік бекіту жөніндегі нақты ұсыныс әзірлеумен сипатталады. Аталған ұсыныс дәлелдемелік ақпаратты жинаудың тиімділігін қамтамасыз ету мен адамның жеке өміріне қол сұғылмаушылық құқығын қорғау арасындағы құқықтық теңгерімді нығайтуға бағытталған.

3. Дербес деректерді қамтитын мәліметтерді дерек ұстаушылардан талап етіп алу барысында қылмыстық іс бойынша ақпараттың құпиялылығын қамтамасыз етуге бағытталған құпияландырылған сұратудың арнайы қылмыстық-процестік тетігі әзірленді.

Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеру барысында қылмыстық іс үшін маңызы бар мәліметтерді мемлекеттік органдардан, ақпараттық жүйелердің меншік иелері мен операторларынан, байланыс қызметтерін көрсетушілерден, қаржы ұйымдарынан және өзге де дерек ұстаушылардан талап етіп алу қажеттілігі туындайды. Мұндай мәліметтер қылмыстық құқық бұзушылықтың жасалу тәсілін, дербес деректерге қол жеткізудің мән-жайларын, ақпаратты өңдеу мен тарату әрекеттерінің сипатын, сондай-ақ қылмыстық іс бойынша дәлелденуге жататын өзге де мән-жайларды анықтау үшін маңызды ақпарат көзі болып табылады.

Зерттеу барысында дерек ұстаушылардан мәліметтер талап етіп алудың қолданыстағы құқықтық тәртібі дәлелдемелерді жинау міндеттерін орындауға бағытталғанымен, сұратулардың мазмұны арқылы қылмыстық іс бойынша артық ақпараттың жария етілу тәуекелін арнайы бағалау қажеттігі анықталды. Атап айтқанда, дерек ұстаушыларға жолданатын сұратуларда қылмыстық құқық бұзушылықтың нақты құқықтық сарапануын, тергеп-тексерудің жекелеген мән-жайларын және қылмыстық іске қатысушылар туралы мәліметтерді көрсету белгілі бір тұлғаның қандай құқық бұзушылық бойынша тексеріліп жатқанын немесе қандай құқыққа қайшы әрекеттен зардап шеккенін жанама түрде анықтауға мүмкіндік беруі мүмкін.

Бұл мәселе дербес деректерді заңсыз жинау, өңдеу және таратуға байланысты қылмыстық істер бойынша ерекше маңызға ие. Өйткені мұндай құқық бұзушылықтарды тергеп-тексеру кезінде жәбірленушілер мен өзге де тұлғалардың жеке өміріне қатысты мәліметтер қылмыстық іс бойынша дәлелдемелік ақпарат ретінде пайдаланылуы мүмкін. Алайда осы ақпаратты алу мақсатында жолданатын сұратудың өзі дербес деректердің қосымша жария етілуіне себеп болмауға тиіс. Демек, дербес деректерді қорғаудың қылмыстық-процестік кепілдіктері ақпарат алынғаннан кейінгі сақтау және пайдалану кезеңдеріне ғана емес, оны талап етіп алу рәсіміне де қолданылуы қажет.

Жүргізілген талдау нәтижесінде дерек ұстаушыға жолданатын сыртқы сұратудың мазмұны мен оны жолдаудың заңдылығын негіздейтін ішкі процестік материалдардың мазмұнын функционалдық тұрғыдан ажырату қажеттігі негізделді. Мұндай ажырату сұратуды орындау үшін дерек ұстаушыға қажетті ақпарат көлемін шектеуге, сонымен бірге қылмыстық процесті жүргізетін органның тиісті шешімін толық негіздеу және оның заңдылығын тексеру мүмкіндігін сақтауға бағытталған.

Осыған байланысты зерттеуде құпияландырылған сұратудың авторлық қылмыстық-процестік тетігі ұсынылды. Оның мәні дерек ұстаушыға жолданатын сұратуда қылмыстық іс бойынша ақпараттың тек сұратуды заңды түрде орындау үшін қажетті бөлігін көрсетумен, ал қылмыстық құқық бұзушылықтың толық құқықтық сарапануын, мәліметтерді талап етіп алудың нақты және құқықтық негіздерін, олардың дәлелдемелік маңызын тиісті ішкі процестік материалдарда сақтаумен сипатталады.

Аталған тетіктің ерекшелігі қылмыстық іс бойынша мәліметтерді дерек ұстаушыдан жасыруды дербес мақсат ретінде қарастырмай, ақпараттың жария етілу көлемін оның құқықтық қажеттілігімен байланыстыруында. Осы тұрғыдан алғанда, сұратудың құпияландырылуы оның құқықтық негізін көрсетпеуді немесе дерек ұстаушыны сұратудың заңдылығын тексеру мүмкіндігінен айыруды білдірмейді. Керісінше, сыртқы сұратуда оны жолдаған уәкілетті орган, сұратудың құқықтық негізі, талап етілетін мәліметтердің нақты көлемі, олар қамтитын уақыт кезеңі және заңда көзделген өзге де міндетті реквизиттер сақталуға тиіс.

Зерттеу барысында дерек ұстаушыларға жолданатын сұратуларда қылмыстық құқық бұзушылықтың құқықтық сарапануы туралы мәліметтерді

көрсету көлеміне ерекше назар аударылды. Қылмыстық құқық бұзушылықтың нақты құқықтық сарапануы сотқа дейінгі тергеп-тексерудің заңдылығын және процестік әрекеттердің негізділігін бағалау үшін маңызды болғанымен, оны дерек ұстаушыға толық көлемде хабарлау барлық жағдайда бірдей қажетті болмауы мүмкін. Осыған байланысты, егер заңда өзгеше көзделмесе және сұратудың заңдылығын тексеруге кедергі келтірмесе, сыртқы сұратуда қылмыстық құқық бұзушылықтың нақты бабы мен бөлігінің орнына Қазақстан Республикасы Қылмыстық кодексінің тиісті тарауын көрсету мүмкіндігін нормативтік тұрғыдан бекіту ұсынылды. Мұндай тәсіл дерек ұстаушыны тергеп-тексерудің жалпы қылмыстық-құқықтық бағыты туралы хабардар ете отырып, нақты құқықтық саралауға қатысты мәліметтердің артық жария етілуін шектеуге бағытталған. Бұл ретте қылмыстық құқық бұзушылықтың толық сарапануы ішкі процестік материалдарда сақталып, прокурорлық қадағалау мен сот бақылауының толықтығы қамтамасыз етілуге тиіс.

Ұсынылған тәсіл прокурорлық қадағалау мен сот бақылауының мазмұнын өзгертуді көздемейді. Заңда прокурордың санкциясы немесе өзге де процестік рұқсат талап етілетін жағдайларда тиісті уәкілетті тұлғаға қылмыстық құқық бұзушылықтың құқықтық сарапануы, мәліметтерді алудың қажеттілігі, олардың дәлелдемелік маңызы және сұратудың құқықтық негіздемесі толық көлемде ұсынылуға тиіс. Бұл талап сұратудың құпиялылығын қамтамасыз ету мен процестік шешімдердің заңдылығын бақылау арасындағы теңгерімді сақтауға мүмкіндік береді.

Құпияландырылған сұрату тетігінің ғылыми жаңалығы дербес деректерді талап етіп алу рәсіміндегі ақпарат алмасуды сыртқы және ішкі процестік деңгейлерге ажыратып, әр деңгейде көрсетілуге тиіс мәліметтердің қажетті әрі жеткілікті көлемін айқындауында. Мұндай тәсіл тергеп-тексеру құпиясын сақтауды, дербес деректер субъектілерінің құқықтарын қорғауды және дәлелдемелерді жинаудың заңдылығын қамтамасыз етуді өзара байланысты қылмыстық-процестік талаптар ретінде қарастыруға негізделеді.

Осы ғылыми тұжырымды нормативтік тұрғыдан іске асыру мақсатында Қазақстан Республикасы Қылмыстық-процестік кодексінің 122-бабын мынадай мазмұндағы жаңа бөлікпен толықтыру ұсынылады:

«Сотқа дейінгі тергеп-тексеру барысында дербес деректерді қамтитын мәліметтерді талап етіп алу туралы сұратуда, егер Қазақстан Республикасының заңдарында өзгеше көзделмесе, қылмыстық құқық бұзушылықтың нақты құқықтық сарапануының орнына Қазақстан Республикасы Қылмыстық кодексінің тиісті тарауы көрсетілуі мүмкін.

Бұл жағдайда сұратуда оны жолдаған орган, мәліметтерді талап етіп алудың процестік құқықтық негізі, сұратылатын деректердің нақты көлемі, олар қамтитын уақыт кезеңі және сұратудың заңдылығын тексеру үшін қажетті өзге де мәліметтер көрсетіледі.

Қылмыстық құқық бұзушылықтың нақты құқықтық сарапануы, мәліметтерді талап етіп алудың құқықтық және нақты негіздері, олардың

қылмыстық іс бойынша маңызы тиісті ішкі процестік материалдарда толық көрсетіледі.

Қылмыстық құқық бұзушылықтың нақты құқықтық сараланууы туралы мәліметтерді Қазақстан Республикасы Қылмыстық кодексінің тиісті тарауымен алмастыру дерек ұстаушының сұратудың заңдылығын тексеру және оған заңда белгіленген тәртіппен шағым жасау құқықтарын, сондай-ақ прокурорлық қадағалау мен сот бақылауын жүзеге асыру мүмкіндігін шектемеуі тиіс.

Осы Кодексте көзделген жағдайларда прокурордың санкциясын немесе өзге де процестік рұқсатты алу міндеттілігі сақталады».

Ұсынылған нормативтік толықтыру дербес деректерді талап етіп алу кезінде ақпараттың құпиялылығын қамтамасыз етудің арнайы қылмыстық-процестік кепілдігін қалыптастыруға бағытталған. Оның мазмұны қылмыстық іс бойынша ақпаратты сұрату рәсімінің заңдылығын сақтай отырып, дерек ұстаушыға тергеп-тексерудің мән-жайлары туралы артық мәліметтердің берілуін шектеуге негізделеді. Бұл ретте қылмыстық құқық бұзушылықтың нақты құқықтық саралануының орнына Қазақстан Республикасы Қылмыстық кодексінің тиісті тарауын көрсету мүмкіндігі жалпыға бірдей міндетті талап ретінде емес, тиісті құқықтық рәсімнің ерекшеліктеріне және сұратудың заңдылығын тексеру қажеттілігіне байланысты қолданылатын арнайы құқықтық мүмкіндік ретінде қарастырылады. Аталған тетікті қолдану дерек ұстаушының сұратудың заңдылығын тексеру және оған заңда белгіленген тәртіппен шағым жасау құқықтарын, сондай-ақ прокурорлық қадағалау мен сот бақылауының толықтығын шектемеуге тиіс. Сонымен қатар ұсынылған тәсіл қылмыстық сот ісін жүргізудің жариялылығы мен ашықтығын шектеуді көздемейді, керісінше сотқа дейінгі тергеп-тексеру деректерінің құпиялылығын қамтамасыз ету мен процестік әрекеттердің заңдылығын бақылау арасындағы құқықтық теңгерімді сақтауға бағытталған.

Осылайша, зерттеудің үшінші ғылыми нәтижесі дерек ұстаушылардан мәліметтер талап етіп алу барысында сыртқы сұрату мен ішкі процестік негіздеменің мазмұнын ажыратуға негізделген құпияландырылған сұратудың арнайы қылмыстық-процестік тетігін әзірлеумен және оны Қазақстан Республикасы Қылмыстық-процестік кодексінің 122-бабында нормативтік бекіту жөніндегі нақты ұсынысты қалыптастырумен сипатталады. Ұсынылған тетік дәлелдемелерді жинаудың заңдылығын, прокурорлық қадағалау мен сот бақылауының толықтығын сақтай отырып, дербес деректер субъектілерінің құқықтарын қорғауды және сотқа дейінгі тергеп-тексеру барысында ақпараттың негізсіз жария етілуінің алдын алуды қамтамасыз етуге бағытталған.

4. «Цифрлық ортадағы дәлелдемелер» ұғымының авторлық анықтамасы қалыптастырылып, олардың жол берілетіндігін бағалаудың бірыңғай қылмыстық-процестік өлшемдері ұсынылды.

Дербес деректерді заңсыз жинау, өңдеу және тарату әрекеттерін сотқа дейінгі тергеп-тексеру барысында цифрлық ақпараттың дәлелдемелік

маңызы ерекше орын алады. Қылмыстық құқық бұзушылықтың жасалу тәсілі, деректерге қол жеткізу жағдайлары, ақпараттың өзгертілуі немесе үшінші тұлғаларға берілуі көбінесе электрондық құрылғыларда, ақпараттық жүйелерде және цифрлық платформаларда қалыптасатын мәліметтер арқылы анықталады. Осыған байланысты цифрлық ақпаратты қылмыстық іс бойынша дәлелдеме ретінде пайдаланудың құқықтық шарттарын нақтылау қажеттілігі туындайды.

Зерттеу барысында цифрлық ортадағы дәлелдемелерді тек электрондық құжаттармен немесе материалдық ақпарат жеткізгіштерімен шектеу олардың ерекшеліктерін толық ашпайтыны анықталды. Қылмыстық іс үшін маңызы бар мәліметтер лог-файлдарда, метадеректерде, ақпараттық жүйелердің журналдарында, IP-мекенжайлар туралы жазбаларда, құрылғы идентификаторларында, деректер базасындағы операциялар тарихында және цифрлық әрекеттердің өзге де іздерінде қамтылуы мүмкін. Мұндай мәліметтердің дәлелдемелік маңызы олардың нақты материалдық жеткізгішіне ғана емес, пайда болу жағдайына, мазмұнына және процестік тәртіппен алынуына байланысты айқындалады.

Осыған байланысты келесі авторлық анықтама тұжырымдалды: «Цифрлық ортадағы дәлелдемелер – қылмыстық іс бойынша маңызы бар мән-жайларды анықтауға мүмкіндік беретін, электрондық құрылғыларда, ақпараттық жүйелерде, деректер базаларында, цифрлық платформаларда, байланыс желілерінде немесе бұлттық сервистерде жасалған, сақталған, өңделген, берілген, қабылданған не қалпына келтірілген, заңда көзделген тәртіппен алынған және процестік нысанда бекітілген цифрлық нысандағы нақты деректер».

Ұсынылған анықтаманың ғылыми жаңалығы цифрлық дәлелдемелерді олардың техникалық нысанына ғана сүйенбей, ақпараттың қалыптасу ортасын, қылмыстық іс бойынша маңыздылығын, алыну заңдылығын және процестік бекітілуін өзара байланысты белгілер ретінде қарастыруында. Мұндай тәсіл цифрлық ақпараттың технологиялық ерекшеліктерін қылмыстық-процестік дәлелдеудің жалпы құқықтық талаптарымен үйлестіруге мүмкіндік береді.

Цифрлық ақпараттың дәлелдемелік маңызын анықтау кезінде оның алыну заңдылығы негізгі талаптардың бірі болып табылады. Ақпараттың қылмыстық іс бойынша маңызды болуы оны заңда көзделмеген тәсілдермен алуға негіз бола алмайды. Сондықтан цифрлық мәліметтерді жинау кезінде тиісті процестік әрекеттің құқықтық негізі, оны жүргізген тұлғаның өкілеттігі, қажет болған жағдайда санкцияның болуы және ақпаратты алу тәртібінің сақталуы тексерілуі тиіс.

Сонымен қатар цифрлық ақпараттың тұтастығын қамтамасыз ету мәселесі ерекше маңызға ие. Цифрлық мәліметтердің өзгертілуі немесе олардың бастапқы мазмұнын тексеру мүмкіндігінің жоғалуы дәлелдемелерді бағалауды қиындатады. Осыған байланысты ақпаратты алу сәтінен бастап оны сақтау, көшіру, зерттеу және сотқа ұсыну кезеңдеріне дейін жүргізілген әрекеттерді құжаттау қажеттігі негізделді.

Зерттеу нәтижесінде цифрлық дәлелдемелердің жол берілетіндігін бағалау үшін мәліметтердің заңды түрде алынуын, тиісті процестік нысанда бекітілуін және заңда белгіленген талаптардың сақталуын қамтитын құқықтық өлшемдер, сондай-ақ ақпарат көзінің анықталуын, деректердің тұтастығын, метадеректердің сақталуын, олармен жүргізілген әрекеттердің тіркелуін және ақпаратты сотта тексеру мүмкіндігін қамтитын техникалық-процестік өлшемдер жүйесі ұсынылды. Аталған өлшемдер өзара байланыста қолданылғанымен, техникалық тұтастықтың расталуы дәлелдеменің жол берілетіндігін автоматты түрде білдірмейді.

Ақпараттың тұтастығын тексеру мақсатында криптографиялық хеш-мәндерді, электрондық цифрлық қолтаңбаны, техникалық тіркеу жазбаларын және басқа да тексеру құралдарын қолданудың маңызы анықталды. Алайда мұндай техникалық құралдардың болуы мәліметтердің заңды түрде алынғанын немесе олардың мазмұнының шынайылығын өздігінен толық растамайды. Сондықтан техникалық тексеру нәтижелері процестік әрекеттердің заңдылығымен және қылмыстық іс бойынша өзге дәлелдемелермен өзара байланыста бағалануы тиіс.

Осы орайда цифрлық дәлелдемелердің жол берілетіндігін олардың қатыстылығынан, анықтығынан және жеткіліктілігінен ажырату қажеттігі негізделді. Ақпараттың техникалық тұрғыдан өзгермегендігі оның нақты қылмыстық құқық бұзушылыққа қатыстылығын автоматты түрде дәлелдемейді. Сол сияқты мәліметтің іске қатыстылығы оны алудың заңда белгіленген тәртібін сақтамауды ақтамайды. Сондықтан цифрлық дәлелдемелерді бағалау қылмыстық-процестік заңнамада көзделген жалпы талаптарды сақтай отырып, олардың технологиялық ерекшеліктерін ескеруге негізделуі қажет.

Зерттеу барысында цифрлық ақпаратты алу мен зерттеуге қатысатын маман және сарапшы функцияларын ажыратудың маңызы да анықталды. Маманның техникалық көмегі ақпаратты дұрыс алу, көшіру және сақтау әрекеттерін қамтамасыз етуге бағытталса, арнайы ғылыми білімді қажет ететін мәселелер сараптамалық зерттеу арқылы шешілуі тиіс. Бұл айырмашылықты сақтау цифрлық ақпаратпен жұмыс істеу нәтижелерінің процестік мәртебесін дұрыс айқындауға ықпал етеді.

Осылайша, зерттеудің төртінші ғылыми нәтижесі цифрлық ортадағы дәлелдемелердің авторлық ұғымын қалыптастыру және олардың жол берілетіндігін бағалаудың өзара байланысты құқықтық әрі техникалық өлшемдерін жүйелеу болып табылады. Ұсынылған тәсіл цифрлық ақпаратты дәлелдеме ретінде пайдаланудың құқықтық айқындығын арттыруға, процестік қателіктердің алдын алуға және дәлелдемелерді сотта жан-жақты тексеру мүмкіндігін қамтамасыз етуге бағытталған.

5. Қылмыстық іс материалдары мен жарияланатын сот актілерінде дербес деректерді міндетті түрде иесіздендірудің арнайы қылмыстық-процестік тетігі ғылыми тұрғыдан негізделді.

Қылмыстық сот ісін жүргізу барысында дербес деректерді қорғау мәселесі ақпаратты жинау және сақтау кезеңдерімен ғана шектелмейді.

Қылмыстық іс материалдарын рәсімдеу, олардың көшірмелерін беру және сот актілерін жариялау кезінде де адамның жеке өміріне қатысты мәліметтердің негізсіз таралу тәуекелі туындайды. Бұл мәселе дербес деректерді заңсыз жинау, өңдеу және таратуға байланысты қылмыстық істер бойынша ерекше өзекті, өйткені құқыққа қайшы әрекеттердің мән-жайларын дәлелдеу үшін алынған ақпараттың өзі кейіннен қайта жария етілуі мүмкін.

Зерттеу барысында сот төрелігінің жариялылығы мен адамның жеке өміріне қол сұғылмаушылық құқығы өзара қарама-қарсы құндылықтар ретінде қарастырылмауға тиіс екені негізделді. Сот актілерінің ашықтығын қамтамасыз ету қоғамның сот төрелігіне деген сенімін арттыруға ықпал етеді, алайда жариялылық қағидасын іске асыру адамның жеке басын сәйкестендіруге мүмкіндік беретін мәліметтерді шектеусіз тарату қажеттігін білдірмейді. Осыған байланысты жарияланатын ақпараттың мазмұны оның қоғамдық маңыздылығы мен дербес деректер субъектілерінің құқықтарын қорғау талаптарына сәйкес айқындалуы тиіс.

Жүргізілген зерттеу нәтижесінде жарияланатын сот актілерінде және қылмыстық іске қатысы жоқ тұлғаларға заңды негізде берілетін іс материалдарының көшірмелерінде дербес деректерді міндетті түрде иесіздендірудің арнайы процестік тетігін енгізу ұсынылды. Оның ғылыми жаңалығы иесіздендіруді ақпаратты техникалық редакциялау тәсілі ретінде ғана емес, қылмыстық іс жүргізу барысында дербес деректердің қайталама жария етілуін болдырмауға бағытталған дербес құқықтық кепілдік ретінде қарастыруында.

Ұсынылған тетік дербес деректерді анықтау, олардың жариялану қажеттілігін бағалау, тұлғаны тікелей немесе жанама сәйкестендіруге мүмкіндік беретін мәліметтерді бүркемелеу, жариялауға арналған редакцияланған нұсқаны қалыптастыру және толық түпнұсқаны шектеулі қолжетімділік режимінде сақтау кезеңдерін қамтиды. Аталған кезеңдердің бірізділігі ақпараттың жариялануынан туындайтын құқықтық тәуекелдерді алдын ала бағалауға мүмкіндік береді.

Зерттеу барысында дербес деректерді иесіздендіруді адамның аты-жөні немесе жеке сәйкестендіру нөмірі сияқты тікелей сәйкестендіру белгілерін алып тастаумен ғана шектеу жеткіліксіз екені анықталды. Кейбір жағдайларда адамның тұрғылықты жері, жұмыс орны, байланыс мәліметтері, туыстық қатынастары, цифрлық аккаунттары немесе нақты оқиғаға қатысты өзге де деректер тұлғаны жанама түрде анықтауға мүмкіндік береді. Сондықтан иесіздендірудің тиімділігі жарияланатын мәліметтердің жиынтық мазмұнын бағалаумен қамтамасыз етілуі тиіс.

Сонымен бірге ұсынылған тетік қылмыстық іс бойынша дәлелдемелердің түпнұсқаларын өзгертуге немесе олардың мазмұнын бұрмалауға негіз болмауы қажет. Иесіздендірілген нұсқа ақпаратты жариялау немесе тиісті тұлғаларға беру мақсатында қалыптастырылғанымен, толық түпнұсқа қылмыстық іс материалдарында заңда белгіленген тәртіппен сақталуға тиіс. Бұл талап дәлелдемелердің тұтастығын және олардың кейіннен тексерілу мүмкіндігін қамтамасыз етеді.

Иесіздендірудің қолданылу шектерін айқындау кезінде қорғау тарапының және қылмыстық процеске қатысатын өзге де уәкілетті тұлғалардың құқықтарын сақтау ерекше маңызға ие. Аталған рәсім күдіктінің, айыпталушының немесе қорғаушының іс материалдарымен заңда белгіленген көлемде танысу құқықтарын негізсіз шектеуге пайдаланылмауы тиіс. Сондықтан жарияланатын ақпаратқа қатысты қорғау талаптары мен процеске қатысушылардың дәлелдемелерге қол жеткізу құқықтарының арасындағы айырмашылық нақты сақталуы қажет.

Осылайша, зерттеудің бесінші ғылыми нәтижесі қылмыстық іс материалдарындағы дербес деректердің негізсіз жария етілуінің алдын алуға бағытталған міндетті иесіздендіру тетігін ғылыми тұрғыдан негіздеумен сипатталады. Ұсынылған тәсіл сот төрелігінің ашықтығын қамтамасыз ету, дәлелдемелердің тұтастығын сақтау және адамның жеке өміріне қол сұғылмаушылық құқығын қорғау арасындағы теңгерімді нығайтуға мүмкіндік береді.

6. Шетелдік юрисдикцияда сақталған цифрлық мәліметтерді алу және сақтау кезінде халықаралық ынтымақтастықты жеделдетудің арнайы қылмыстық-процестік тетіктері негізделді.

Дербес деректерді заңсыз жинау, өңдеу және тарату әрекеттерінің цифрлық ортада жасалуы қылмыстық құқық бұзушылықтың аумақтық шектерін анықтауды және дәлелдемелік ақпаратты алуды күрделендіреді. Қазіргі ақпараттық инфрақұрылым жағдайында қылмыстық құқық бұзушылыққа қатысты мәліметтер бір мемлекеттің аумағында қалыптасып, басқа мемлекеттің аумағындағы серверлерде сақталуы немесе бірнеше цифрлық платформа арқылы берілуі мүмкін. Мұндай жағдайда ұлттық тергеу органдарының дәлелдемелерді алу мүмкіндігі халықаралық құқықтық ынтымақтастық рәсімдерінің тиімділігіне тәуелді болады.

Зерттеу барысында дәстүрлі халықаралық құқықтық көмек рәсімдерінің ұзақтығы мен цифрлық ақпараттың өзгеру немесе жойылу жылдамдығы арасындағы сәйкессіздік маңызды практикалық мәселе ретінде анықталды. Ақпараттық жүйелердің журналдары, желілік қосылымдар туралы мәліметтер, уақытша сақталатын техникалық жазбалар және өзге де цифрлық іздер белгілі бір мерзімнен кейін автоматты түрде жойылуы мүмкін. Сондықтан тиісті ақпаратты алу туралы халықаралық сұратудың кеш жіберілуі қылмыстық іс бойынша маңызы бар мәліметтердің жоғалу тәуекелін арттырады.

Осы мәселені шешу мақсатында зерттеуде трансшекаралық цифрлық ақпаратпен жұмыс істеудің екі өзара байланысты кезеңін ажыратуға негізделген ғылыми тәсіл ұсынылды. Бірінші кезең цифрлық мәліметтерді шұғыл сақтап қоюға бағытталса, екінші кезең оларды тиісті халықаралық-құқықтық және ұлттық қылмыстық-процестік рәсімдер арқылы алуды қамтиды.

Ұсынылған тәсілдің ғылыми жаңалығы мәліметтерді сақтап қою мен оларды дәлелдеме ретінде алуды дербес құқықтық рәсімдер ретінде ажыратуында. Ақпаратты шұғыл сақтап қою оның мазмұнымен автоматты

түрде танысуға немесе оны тергеу органына тікелей беруге құқықтық негіз болып табылмайды. Бұл рәсімнің негізгі мақсаты мәліметтерді заңды түрде алу туралы шешім қабылданғанға дейін олардың жойылуын немесе өзгертілуін болдырмау болып табылады.

Зерттеу нәтижесінде цифрлық ақпаратты сақтап қою туралы шұғыл сұратулардың стандартталған нысандарын әзірлеу, халықаралық құқықтық көмек туралы сұрауларды электрондық түрде жолдау мүмкіндіктерін дамыту, тәулік бойы жұмыс істейтін ұлттық байланыс тетігін жетілдіру және шетелдік құзыретті органдармен өзара іс-қимылдың ұйымдастырушылық рәсімдерін нақтылау ұсынылды.

Халықаралық тәжірибені салыстырмалы талдау барысында киберқылмысқа қарсы іс-қимыл және дербес деректерді қорғау саласындағы халықаралық құқықтық құралдардың цифрлық ақпаратты сақтау мен алудың тиімді рәсімдерін қалыптастырудағы маңызы анықталды. Атап айтқанда, Киберқылмыс туралы Будапешт конвенциясында, оған Екінші қосымша хаттамада және дербес деректерді қорғау саласындағы халықаралық стандарттарда көзделген құқықтық тәсілдер ұлттық заңнаманы жетілдіру үшін салыстырмалы-құқықтық бағдар ретінде қарастырылды. Бұл ретте халықаралық құралдарды қолдану олардың Қазақстан Республикасы үшін құқықтық мәртебесін және тиісті ұлттық құқықтық негіздердің болуын ескере отырып жүзеге асырылуға тиіс.

Ұсынылған тетіктер шетелдік ақпараттық жүйелерге шектеусіз қол жеткізуді немесе халықаралық құқықтық көмек рәсімдерін айналып өтуді көздемейді. Олардың мақсаты цифрлық ақпараттың сақталуын қамтамасыз ететін шұғыл шаралар мен мәліметтерді заңды түрде алудың кейінгі рәсімдері арасындағы байланысты жетілдіру болып табылады. Мұндай тәсіл дәлелдемелердің жоғалу тәуекелін төмендетуге, халықаралық ынтымақтастықтың жеделдігін арттыруға және алынған ақпараттың ұлттық қылмыстық процесте пайдаланылуының заңдылығын қамтамасыз етуге мүмкіндік береді.

Осылайша, зерттеудің алтыншы ғылыми нәтижесі трансшекаралық цифрлық мәліметтерді шұғыл сақтап қою мен оларды кейіннен заңды түрде алудың кезеңдік моделін ғылыми тұрғыдан негіздеумен сипатталады. Бұл модель халықаралық ынтымақтастықтың тиімділігін арттыруға және цифрлық дәлелдемелермен жұмыс істеу кезінде адамның құқықтарын қорғаудың қажетті кепілдіктерін сақтауға бағытталған.

Зерттеу барысында қалыптастырылған ғылыми тұжырымдардың негізділігі нормативтік-құқықтық, салыстырмалы-құқықтық, статистикалық және эмпирикалық талдау нәтижелерімен айқындалады.

Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің мәліметтері бойынша 2021–2025 жылдары Қазақстан Республикасы Қылмыстық кодексінің 147-бабының 3–5-бөліктері бойынша 302 қылмыстық құқық бұзушылық тіркелген. Олардың саны 2021 жылы 35 жағдайды, 2022 жылы 39 жағдайды, 2023 жылы 66 жағдайды, 2024 жылы 64 жағдайды және 2025 жылы 98 жағдайды құраған.

Осылайша, қарастырылған кезеңде тіркелген құқық бұзушылықтар саны 2,8 есеге артқан.

Аталған құқық бұзушылықтардың құрылымында Қылмыстық кодекстің 147-бабының 5-бөлігі бойынша 154 жағдай немесе 51,0%, 4-бөлігі бойынша 77 жағдай немесе 25,5%, 3-бөлігі бойынша 71 жағдай немесе 23,5% тіркелген. Бұл мәліметтер дербес деректерге қатысты қылмыстық қол сұғушылықтарды тергеп-тексеру мәселелерінің өзектілігін көрсетеді. Сонымен бірге тіркелген құқық бұзушылықтар санының өзгеруі қылмыстылықтың нақты таралу деңгейімен қатар құқық бұзушылықтарды анықтау, тіркеу және құқықтық саралау практикасына да байланысты болуы мүмкін екенін ескеру қажет.

Сот статистикасын зерттеу нәтижесінде 2021–2025 жылдары Қылмыстық кодекстің 147-бабы бойынша 53 адамның сотталғаны, олардың 41-і немесе 77,4%-ы аталған баптың 5-бөлігі бойынша жауаптылыққа тартылғаны анықталды. Тіркелген қылмыстық құқық бұзушылықтар мен сотталған адамдардың саны әртүрлі статистикалық есепке алу бірліктері болғандықтан, бұл көрсеткіштер тікелей салыстырылмайды. Дегенмен олардың жиынтық талдауы құқықтық саралау, дәлелдеу нысанасын анықтау және цифрлық мәліметтерді процестік тұрғыдан бағалау мәселелерін зерттеудің қажеттілігін негіздейді.

Зерттеу шеңберінде Алматы қаласында тергеушілер, прокурорлар мен тергеу судьялары, қорғаушылар, дерек ұстаушы ұйымдардың өкілдері және дербес деректер субъектілерінен тұратын бес топ бойынша 850 респонденттің қатысуымен сауалнама жүргізілді. Оның нәтижелері дербес деректерді қылмыстық процесте пайдаланудың бірыңғай стандарттарын қалыптастыру қажеттігін көрсетті. Респонденттер топтары бойынша мұндай стандарттарды қолдау деңгейі 67,4%-дан 78,6%-ға дейінгі аралықта болды. Сонымен қатар сауалнама барысында цифрлық дәлелдемелерді бекіту тәртібін нақтылау және дербес деректердің қайталама жария етілуінің алдын алу мәселелерінің практикалық маңыздылығы анықталды.

Аталған эмпирикалық нәтижелер диссертацияда ұсынылған ғылыми тұжырымдардың құқық қолдану практикасындағы нақты қажеттіліктермен байланысын көрсетеді. Сонымен бірге сауалнама Алматы қаласында жүргізілгендіктен, алынған нәтижелер зерттеуге қатысқан респонденттер топтарының ұстанымдарын сипаттайды және бүкіл Қазақстан бойынша репрезентативті көрсеткіш ретінде қарастырылмайды.

Жүргізілген зерттеудің нәтижелерін жинақтау дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің кешенді қылмыстық-процестік моделін қалыптастыруға мүмкіндік берді. Аталған модель дербес деректердің құқықтық мәртебесін айқындауды, оларды пайдаланудың сараланған режимін, дерек ұстаушылардан мәліметтерді құпияландырылған тәртіппен алуды, цифрлық дәлелдемелерді бағалаудың бірыңғай өлшемдерін, дербес деректерді иесіздендірудің арнайы кепілдіктерін және

трансшекаралық цифрлық ақпаратты алу тетіктерін өзара байланысты жүйе ретінде біріктіреді.

Ұсынылған модельдің негізгі ерекшелігі сотқа дейінгі тергеп-тексерудің тиімділігін қамтамасыз ету мен адамның жеке өміріне қол сұғылмаушылық құқығын қорғауды өзара байланысты қылмыстық-процестік міндеттер ретінде қарастыруында. Бұл тәсіл дәлелдемелерді жинау қажеттілігін адамның құқықтарын қорғау талаптарынан бөліп қарастырмай, олардың арасындағы құқықтық теңгерімді қамтамасыз етуге бағытталған.

Зерттеудің теориялық маңыздылығы қылмыстық процесс ғылымындағы дербес деректердің құқықтық табиғаты, цифрлық ортадағы дәлелдемелердің ерекшеліктері, ақпаратты алу мен пайдаланудың құқықтық шектері және адамның жеке өмірін қорғаудың процестік кепілдіктері туралы ғылыми түсініктерді дамытуымен сипатталады. Ұсынылған авторлық анықтамалар мен ғылыми тұжырымдар цифрлық ақпаратты қылмыстық процесте пайдаланудың ғылыми-әдіснамалық негіздерін одан әрі жетілдіруге мүмкіндік береді.

Зерттеудің практикалық маңыздылығы қалыптастырылған ғылыми нәтижелерді Қазақстан Республикасының қылмыстық-процестік заңнамасын жетілдіруде, сотқа дейінгі тергеп-тексеру органдарының қызметінде, прокурорлық қадағалау мен сот бақылауы практикасында, дерек ұстаушылармен ақпарат алмасу рәсімдерін ұйымдастыруда және құқық қорғау органдары қызметкерлерінің кәсіби даярлығында пайдалану мүмкіндігімен айқындалады.

Сонымен қатар зерттеу нәтижелері цифрлық технологиялардың одан әрі дамуына байланысты дербес деректерді қорғау мәселелерін тұрақты ғылыми зерделеу қажеттігін көрсетті. Атап айтқанда, жасанды интеллект құралдары арқылы алынған ақпараттың дәлелдемелік мәртебесін айқындау, автоматтандырылған өңдеу нәтижелерінің тексерілуін қамтамасыз ету, трансшекаралық ақпарат алмасудың құқықтық кепілдіктерін жетілдіру және цифрлық дәлелдемелердің ұзақ мерзімді сақталуын қамтамасыз ету болашақ ғылыми зерттеулердің маңызды бағыттары болып табылады.

Қорытындылай келе, диссертациялық зерттеудің негізгі ғылыми нәтижесі дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің тиімділігін арттыру мен адамның жеке өміріне қол сұғылмаушылық құқығын қорғау арасындағы теңгерімді қамтамасыз етуге бағытталған арнайы қылмыстық-процестік кепілдіктердің кешенді жүйесін ғылыми тұрғыдан негіздеу болып табылады. Ұсынылған алты ғылыми тұжырым осы жүйенің өзара байланысты элементтерін құрайды және дербес деректерді дәлелдемелік мақсатта пайдаланудың құқықтық шектерін нақтылауға, цифрлық ақпаратпен жұмыс істеудің процестік тәртібін жетілдіруге және қылмыстық сот ісін жүргізуде адамның құқықтары мен заңды мүдделерін қорғауды күшейтуге бағытталған.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Қазақстан Республикасының Конституциясы: 2026 жылы 15 наурызда республикалық референдумда қабылданған [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/K2600000000 (қол жеткізген күні: 15.03.2026).

2. «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/Z1300000094 (қол жеткізген күні: 17.02.2026).

3. Президент Бас прокуратурада жиын өткізді [Электрондық ресурс] // Ақорда: Қазақстан Республикасы Президентінің ресми сайты. – URL: https://www.akorda.kz/kz/prezident-bas-prokuraturada-zhiyn-otkizdi-2604726 (қол жеткізген күні: 17.02.2026).

4. Қазақстан Республикасының 2026 жылғы 9 қаңтардағы № 255-VIII ҚРЗ Цифрлық кодексі [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/K2600000255 (қол жеткізген күні: 17.02.2026).

5. Мухамадиева Г.Н., Алимкулов Е.Т., Жанибеков А.К., Жұмадилова Н.С. Қазақстан Республикасындағы заң шығару қызметінің нормативтік құқықтық негізін талдау: проблемалар, қайшылықтар және жетілдіру жолдары // Eurasian Scientific Journal of Law. – 2025. – № 3(12). – Б. 7–16.

6. Қазақстан Республикасының 2014 жылғы 4 шілдедегі № 231-V ҚРЗ Қылмыстық-процестік кодексі [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/K1400000231 (қол жеткізген күні: 17.02.2026).

7. Zhumadilova N., Zhanibekov A., Taubayev B., Adilgazy S., Assanova S. The Effectiveness of Criminal Law Provisions on the Illegal Circulation of Personal Data in the Context of Digitalization: Challenges and Approaches to Legislative Improvement // Journal of Applied Security Research. – https://doi.org/10.1080/19361610.2025.2604136

8. Салимгерей А.А., Дуйсенов Е.Э., Байдаулетова А.И., Жұмадилова Н.С. Закон Республики Казахстан «Об искусственном интеллекте»: проблемы реализации и образованности населения // Вестник КазНУ. Серия юридическая. – 2025. – № 3(115). – Б. 43–52.

9. General Data Protection Regulation (GDPR) [Электрондық ресурс] // URL: https://gdpr-info.eu (қол жеткізген күні: 17.02.2025).

10. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg, 28 January 1981 [Electronic resource]. – URL: https://rm.coe.int/1680078b37 (accessed: 10.05.2025).

11. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). Strasbourg, 10 October 2018 [Electronic resource]. – URL: https://rm.coe.int/16808ac918 (accessed: 10.05.2026).

12. Бисалиев М.С. «Международно-правовые аспекты защиты личной информации в глобальном и национальном информационном пространстве»:

дис. ... доктор философии (PhD): 8D04201 – Международное право / КазНУ имени аль-Фараби. – Алматы, 2025. – 195 с.

13. Бундин М.В. «Персональные данные в системе информации ограниченного доступа»: дис. ... кандидат юридических наук: 12.00.13 – Информационное право / Институт законодательства и сравнительного правоведения. – Москва, 2017. – 218 с.

14. Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. ... канд. юрид. наук. – Владивосток, 2017. – 220 с.

15. Хохлова Е.В. Незаконные действия с персональными данными: уголовно-правовое исследование: дис. ... канд. юрид. наук: 5.1.4. – Белгород, 2023. – 255 с.

16. Амиров А.М. Прокурорский надзор за соблюдением законности в сфере персональных данных и их защиты: дис. ... доктора философии (PhD). – Косшы, 2025. – 210 с.

17. Ахметова С.Б. Государственно-правовая защита персональных данных в Республике Казахстан: дис. ... доктора философии (PhD): 8D04203 – Юриспруденция / КазНУ имени аль-Фараби. – Алматы, 2026. – 189 с.

18. Дигай Д.А. Правовое регулирование обеспечения доступа к информации (национальное законодательство и международный опыт): дис. ... доктора философии (PhD): 8D04201 – Юриспруденция. – Талдыкорган, 2026. – 180 с.

19. Қазақстан Республикасының 2014 жылғы 3 шілдедегі № 226-V ҚРЗ Қылмыстық кодексі [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/K1400000226 (қол жеткізген күні: 01.02.2025).

20. Қазақстан Республикасының 2014 жылғы 5 шілдедегі № 235-V ҚРЗ Әкімшілік құқық бұзушылық туралы кодексі [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/K1400000235 (қол жеткізген күні: 01.02.2025).

1. Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитеті. №10 «Сот актілері шығарылған адамдардың саны туралы» статистикалық есептер, 2021–2025 жылдар.

2. Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитеті. №11 «Қылмыстық құқық бұзушылық жасаған сотталғандардың құрамы туралы» статистикалық есептер, 2021–2025 жылдар.

3. Борчашвили И.Ш. Комментарий к Уголовному кодексу Республики Казахстан: общая и особенная части. – 2-е изд. – Алматы: Жеті жарғы, 2007. – 989 с.

4. Неприкосновенность частной жизни: сборник материалов круглого стола / Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – Астана, 2018. – 333 с.

5. Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің міндетін атқарушының 2020 жылғы 21 қазандағы № 395/НҚ бұйрығы «Дербес деректерді жинау, өңдеу қағидаларын

бекіту туралы» [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/V2000021498 (қол жеткізген күні: 18.01.2026).

6. Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2023 жылғы 12 маусымдағы № 179/НҚ бұйрығы «Меншік иесінің және (немесе) оператордың, сондай-ақ үшінші тұлғаның дербес деректерді қорғау жөніндегі шараларды жүзеге асыру қағидаларын бекіту туралы» [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/V2300032810 (қол жеткізген күні: 15.01.2026).

7. «Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V ҚРЗ Заңы [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/Z1500000418 (қол жеткізген күні: 15.09.2026).

8. «Ақпаратқа қол жеткізу туралы» Қазақстан Республикасының 2015 жылғы 16 қарашадағы № 401-V ҚРЗ Заңы [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/Z1500000401 (қол жеткізген күні: 21.09.2025).

9. «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы № 370-II Заңы (2026 жылғы 9 қаңтардағы № 255-VIII ҚРЗ Цифрлық кодекспен 2026 жылғы 12 шілдеден бастап күші жойылды) [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/Z030000370_ (қол жеткізген күні: 15.12.2025).

10. Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы «Киберқауіпсіздік тұжырымдамасын ("Қазақстанның киберқалқаны") бекіту туралы» [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/P1700000407 (қол жеткізген күні: 15.12.2025).

11. «Қазақстан Республикасының ұлттық қауіпсіздігі туралы» Қазақстан Республикасының 2012 жылғы 6 қаңтардағы № 527-IV Заңы [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/Z1200000527 (қол жеткізген күні: 15.12.2025).

12. «Байланыс туралы» Қазақстан Республикасының 2004 жылғы 5 шілдедегі № 567-II Заңы [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/Z040000567_ (қол жеткізген күні: 15.12.2025).

13. «Халық денсаулығы және денсаулық сақтау жүйесі туралы» Қазақстан Республикасының 2020 жылғы 7 шілдедегі № 360-VI ҚРЗ Кодексі [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/K2000000360 (қол жеткізген күні: 15.12.2025).

14. Қазақстан Республикасы Денсаулық сақтау министрінің 2021 жылғы 14 сәуірдегі № ҚР ДСМ-30 бұйрығы «Цифрлық денсаулық сақтау субъектілерінің дербес медициналық деректерді жинау, өңдеу, сақтау, қорғау және беру қағидаларын бекіту туралы» (ҚР Әділет министрлігінде 2021 жылғы 15 сәуірде № 22550 болып тіркелген) [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/V2100022550 (қол жеткізген күні: 15.12.2025).

15. «Мемлекеттік құпиялар туралы» Қазақстан Республикасының 1999 жылғы 15 наурыздағы № 349-I Заңы [Электрондық ресурс] // URL: https://adilet.zan.kz/kaz/docs/Z990000349_ (қол жеткізген күні: 15.04.2026).

16. «Прокуратура туралы» Қазақстан Республикасының Конституциялық заңы, 2022 жылғы 5 қарашадағы № 155-VII ҚРЗ

[Электрондық ресурс] // URL: адилеттегі құжат нөмірін тексеру қажет (қол жеткізген күні: 15.12.2025).

17. Kuner C. Transborder Data Flows and Data Privacy Law. – Oxford: Oxford University Press, 2013. – DOI: 10.1093/acprof:oso/9780199674619.001.0001.

18. Bygrave L.A. Data Privacy Law: An International Perspective. – Oxford: Oxford University Press, 2014. – DOI: 10.1093/acprof:oso/9780199675555.001.0001.

19. Greenleaf G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. – Oxford: Oxford University Press, 2014.

20. Смолькова И.В. Проблемы охраняемой законом тайны в уголовном процессе: дис. ... докт. юрид. наук: 12.00.09. – Иркутск, 1998. – 404 с.

21. Смолькова И.В. Защита персональных данных в уголовном судопроизводстве // Правовое государство: теория и практика. – 2025. – Т. 21, № 1(79). – Б. 134–142. – DOI: 10.33184/pravgos-2025.1.15.

22. S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008, judgment of 4 December 2008.

23. Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13, 62322/14 and 24960/15, ECHR 2021, judgment of 25 May 2021.

24. Қазақстан Республикасы Жоғарғы Соты. Қылмыстық істер бойынша дәлелдемелерді бағалаудың кейбір мәселелері туралы: 2006 жылғы 20 сәуірдегі № 4 нормативтік қаулы. URL: https://adilet.zan.kz/kaz/docs/P06000004S_

25. Kerr O.S. Digital Evidence and the New Criminal Procedure // Columbia Law Review. 2005. Vol. 105. P. 279–318. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=594101

26. Carrier B., Spafford E.H. Getting Physical with the Digital Investigation Process // International Journal of Digital Evidence. 2003. Vol. 2, No. 2. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/2666

27. Garfinkel S.L. Digital forensics research: The next 10 years // Digital Investigation. 2010. Vol. 7, Supplement. P. S64–S73. DOI: 10.1016/j.diin.2010.05.009. URL: https://dfrws.org/presentation/digital-forensics-research-the-next-10-years/

28. Quick D., Choo K.-K.R. Impacts of increasing volume of digital forensic data: A survey and future research challenges // Digital Investigation. 2014. Vol. 11, No. 4. P. 273–294. DOI: 10.1016/j.diin.2014.09.002. URL: https://www.sciencedirect.com/science/article/pii/S1742287614001066

29. Ruan K., Carthy J., Kechadi T., Crosbie M. Cloud Forensics: An Overview // Advances in Digital Forensics VII. 2011. P. 35–46. URL: https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview

30. NIST. NIST Cloud Computing Forensic Science Challenges. NISTIR 8006. 2020. DOI: 10.6028/NIST.IR.8006. URL: https://csrc.nist.gov/pubs/ir/8006/final

31. Herman M. et al. NIST Cloud Computing Forensic Reference

Architecture. NIST SP 800-201. 2024. DOI: 10.6028/NIST.SP.800-201. URL: https://csrc.nist.gov/pubs/sp/800/201/final

32. Қазақстан Республикасы Бас Прокуроры. Қылмыстық құқық бұзушылықтар туралы арызды, хабарды немесе баянатты қабылдау және тіркеу, сондай-ақ Сотқа дейінгі тергеп-тексерулердің бірыңғай тізілімін жүргізу қағидаларын бекіту туралы: 2014 жылғы 19 қыркүйектегі № 89 бұйрық. Мемлекеттік тіркеу № 9744. URL: https://adilet.zan.kz/kaz/docs/V1400009744

33. National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders. 2nd ed. Washington, DC, 2008. NCJ 219941. URL: https://nij.ojp.gov/library/publications/electronic-crime-scene-investigation-guide-first-responders-second-edition

34. Brezinski D., Killalea T. Guidelines for Evidence Collection and Archiving. RFC 3227. 2002. DOI: 10.17487/RFC3227. URL: https://www.rfc-editor.org/rfc/rfc3227.html

35. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST SP 800-86. 2006. DOI: 10.6028/NIST.SP.800-86. URL: https://csrc.nist.gov/pubs/sp/800/86/final

36. ISO/IEC 27043:2015. Information technology – Security techniques – Incident investigation principles and processes. Geneva: ISO, 2015. URL: https://www.iso.org/standard/44407.html

37. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61 Rev. 3. 2025. DOI: 10.6028/NIST.SP.800-61r3. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final

38. NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. 2024. DOI: 10.6028/NIST.CSWP.29. URL: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final

39. Durand A., Gashinsky I., Lee D., Sheppard S. Logging Recommendations for Internet-Facing Servers. RFC 6302. 2011. DOI: 10.17487/RFC6302. URL: https://www.rfc-editor.org/rfc/rfc6302.html

40. Court of Justice of the European Union. Patrick Breyer v Bundesrepublik Deutschland. Case C-582/14. Judgment of 19 October 2016. ECLI:EU:C:2016:779. URL: https://curia.europa.eu/juris/liste.jsf?num=C-582%2F14

41. Buchholz F., Spafford E. On the role of file system metadata in digital forensics // Digital Investigation. 2004. Vol. 1, No. 4. P. 298–309. DOI: 10.1016/j.diin.2004.10.002. URL: https://www.sciencedirect.com/science/article/pii/S1742287604000829

42. Klyne G., Newman C. Date and Time on the Internet: Timestamps. RFC 3339. 2002. DOI: 10.17487/RFC3339. URL: https://www.rfc-editor.org/rfc/rfc3339.html

43. National Institute of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Washington, DC, 2004. NCJ 199408. URL: https://www.ojp.gov/library/publications/forensic-examination-digital-evidence-

guide-law-enforcement

44. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012. URL: https://www.iso.org/standard/44381.html

45. Ayers R., Brothers S., Jansen W. Guidelines on Mobile Device Forensics. NIST SP 800-101 Rev. 1. 2014. DOI: 10.6028/NIST.SP.800-101r1. URL: https://csrc.nist.gov/pubs/sp/800/101/r1/final

46. SWGDE. Best Practices for Computer Forensic Acquisitions. 17-F-002, Version 2.1. 2025. URL: https://www.swgde.org/documents/published-complete-listing/17-f-002-best-practices-for-computer-forensic-acquisitions/

47. SWGDE. Best Practices for Digital Evidence Collection. 18-F-002, Version 2.0. 2025. URL: https://www.swgde.org/documents/published-complete-listing/18-f-002-2-0/

48. OHCHR; Human Rights Center, University of California, Berkeley. Berkeley Protocol on Digital Open Source Investigations. New York; Geneva: United Nations, 2022. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

49. ISO/IEC 27050-1:2019. Information technology – Electronic discovery – Part 1: Overview and concepts. Geneva: ISO, 2019. URL: https://www.iso.org/standard/78647.html

50. Kent K., Souppaya M. Guide to Computer Security Log Management. NIST SP 800-92. 2006. DOI: 10.6028/NIST.SP.800-92. URL: https://csrc.nist.gov/pubs/sp/800/92/final

51. Gerhards R. The Syslog Protocol. RFC 5424. 2009. DOI: 10.17487/RFC5424. URL: https://www.rfc-editor.org/rfc/rfc5424.html

52. Australian Signals Directorate's Australian Cyber Security Centre et al. Best Practices for Event Logging and Threat Detection. 2024. URL: https://www.cyber.gov.au/business-government/detecting-responding-to-threats/event-logging/best-practices-for-event-logging-and-threat-detection

53. Dykstra J., Sherman A.T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques // Digital Investigation. 2012. Vol. 9, Supplement. P. S90–S98. URL: https://dfrws.org/presentation/acquiring-forensic-evidence-from-infrastructure-as-a-service-cloud-computing/

54. SWGDE. Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers. 23-F-004, Version 1.1. 2025. URL: https://www.swgde.org/documents/published-complete-listing/23-f-004-best-practices-for-digital-evidence-acquisition-preservation-and-analysis-from-cloud-service-providers/

55. Jansen W., Grance T. Guidelines on Security and Privacy in Public Cloud Computing. NIST SP 800-144. 2011. DOI: 10.6028/NIST.SP.800-144. URL: https://csrc.nist.gov/pubs/sp/800/144/final

56. Guttman B., White D.R., Williams S., Walraven T. Digital Evidence Preservation: Considerations for Evidence Handlers. NIST IR 8387. 2022. DOI: 10.6028/NIST.IR.8387. URL: https://www.nist.gov/publications/digital-evidence-

preservation-considerations-evidence-handlers

57. NIST. Secure Hash Standard (SHS). FIPS PUB 180-4. 2015. DOI: 10.6028/NIST.FIPS.180-4. URL: https://csrc.nist.gov/pubs/fips/180-4/upd1/final

58. Adams C., Cain P., Pinkas D., Zuccherato R. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). RFC 3161. 2001. DOI: 10.17487/RFC3161. URL: https://www.rfc-editor.org/rfc/rfc3161.html

59. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022. URL: https://www.iso.org/standard/27001

60. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva: ISO, 2022. URL: https://www.iso.org/standard/75652.html

61. NIST. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5. 2020. DOI: 10.6028/NIST.SP.800-53r5. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

62. McCallister E., Grance T., Scarfone K. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). NIST SP 800-122. 2010. DOI: 10.6028/NIST.SP.800-122. URL: https://csrc.nist.gov/pubs/sp/800/122/final

63. Сот-сараптама қызметі туралы: Қазақстан Республикасының 2017 жылғы 10 ақпандағы № 44-VI ҚРЗ Заңы. URL: https://adilet.zan.kz/kaz/docs/Z1700000044

64. Қазақстан Республикасы Конституциялық Соты. 2014 жылғы 4 шілдедегі Қазақстан Республикасы Қылмыстық-процестік кодексінің 80-бабы екінші бөлігінің Қазақстан Республикасының Конституциясына сәйкестігін қарау туралы: 2023 жылғы 20 шілдедегі № 24-НҚ нормативтік қаулы. URL: https://adilet.zan.kz/kaz/docs/S2300000024

65. ISO/IEC 27041:2015. Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method. Geneva: ISO, 2015. URL: https://www.iso.org/standard/44405.html

66. ISO/IEC 27042:2015. Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. Geneva: ISO, 2015. URL: https://www.iso.org/standard/44406.html

67. Lyle J.R., Guttman B., Butler J.M., Sauerwein K., Reed C., Lloyd C.E. Digital Investigation Techniques: A NIST Scientific Foundation Review. NIST IR 8354. 2022. DOI: 10.6028/NIST.IR.8354. URL: https://doi.org/10.6028/NIST.IR.8354

68. Brunty J. Validation of forensic tools and methods: A primer for the digital forensics examiner // WIREs Forensic Science. 2023. Vol. 5. e1474. DOI: 10.1002/wfs2.1474. URL: https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1474

69. Hughes N., Karabiyik U. Towards reliable digital forensics investigations through measurement science // WIREs Forensic Science. 2020. Vol. 2, No. 4. e1367. DOI: 10.1002/wfs2.1367. URL: https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1367

70. Horsman G. Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics // Computers & Security. 2018. Vol. 73. P. 294–306. URL: https://research.tees.ac.uk/en/publications/framework-for-reliable-experimental-design-fred-a-research-framew/

71. Sunde N., Dror I.E. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward // Digital Investigation. 2019. Vol. 29. P. 101–108. DOI: 10.1016/j.diin.2019.03.011. URL: https://phs.brage.unit.no/phs-xmlui/bitstream/handle/11250/2675988/1-s2.0-S1742287619300441-main.pdf?isAllowed=y&sequence=1

72. Garfinkel S., Farrell P., Roussev V., Dinolt G. Bringing science to digital forensics with standardized forensic corpora // Digital Investigation. 2009. Vol. 6, Supplement. P. S2–S11. DOI: 10.1016/j.diin.2009.06.016. URL: https://dfrws.org/sites/default/files/session-files/2009_USA_paper-bringing_science_to_digital_forensics_with_standardized_forensic_corpora.pdf

73. Casey E. The chequered past and risky future of digital forensics // Australian Journal of Forensic Sciences. 2019. Vol. 51, No. 6. P. 649–664. DOI: 10.1080/00450618.2018.1554090. URL: https://www.tandfonline.com/doi/abs/10.1080/00450618.2018.1554090

74. SWGDE. Considerations for Focused Collection of Digital Evidence. 14-F-003, Version 2.0. 2025. URL: https://www.swgde.org/documents/published-complete-listing/14-f-003-2-0/

75. SWGDE. Best Practices for Computer Forensic Examinations. 18-F-001, Version 2.0. 2025. URL: https://www.swgde.org/documents/published-complete-listing/18-f-001-2/

76. Chandramouli R., Hibbard E. Guidelines for Media Sanitization. NIST SP 800-88 Rev. 2. 2025. DOI: 10.6028/NIST.SP.800-88r2. URL: https://csrc.nist.gov/pubs/sp/800/88/r2/final

77. Жедел-іздестіру қызметі туралы: Қазақстан Республикасының 1994 жылғы 15 қыркүйектегі № 154-XIII Заңы. URL: https://adilet.zan.kz/kaz/docs/Z940004000_

78. Қазақстан Республикасы Жоғарғы Соты. Жасырын тергеу әрекеттерін санкциялау туралы: 2020 жылғы 11 желтоқсандағы № 5 нормативтік қаулы. URL: https://adilet.zan.kz/kaz/docs/P200000005S

79. Жасырын тергеу әрекеттерін жүргізу қағидаларын бекіту туралы: ҚР Ішкі істер министрінің 2014 жылғы 12 желтоқсандағы № 892, Қаржы министрінің 2014 жылғы 12 желтоқсандағы № 565, Мемлекеттік күзет қызметі бастығының 2014 жылғы 15 желтоқсандағы № 146, Мемлекеттік қызмет істері және сыбайлас жемқорлыққа қарсы іс-қимыл агенттігі төрағасының 2014 жылғы 12 желтоқсандағы № 62 және Ұлттық қауіпсіздік комитеті төрағасының 2014 жылғы 18 желтоқсандағы № 416 бірлескен бұйрығы. Мемлекеттік тіркеу № 10027. URL: https://adilet.zan.kz/kaz/docs/V14C0010027

80. United Nations. International Covenant on Civil and Political Rights. Adopted 16 December 1966. United Nations Treaty Series. Vol. 999. P. 171. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

81. UN Human Rights Committee. General Comment No. 16: Article 17, Right to Privacy. 1988. HRI/GEN/1/Rev.9 (Vol. I). URL: https://www.ohchr.org/sites/default/files/Documents/HRBodies/TB/HRI-GEN-1-REV-9-VOL-I_en.pdf

82. European Court of Human Rights. Roman Zakharov v. Russia [GC]. Application No. 47143/06. Judgment of 4 December 2015. URL: https://hudoc.echr.coe.int/eng?i=001-159324

83. European Court of Human Rights. Benedik v. Slovenia. Application No. 62357/14. Judgment of 24 April 2018. URL: https://hudoc.echr.coe.int/eng?i=001-182455

84. European Court of Human Rights. Trabajo Rueda v. Spain. Application No. 32600/12. Judgment of 30 May 2017. URL: https://hudoc.echr.coe.int/eng?i=001-174630

85. European Court of Human Rights. Saber v. Norway. Application No. 459/18. Judgment of 17 December 2020. URL: https://hudoc.echr.coe.int/eng?i=001-206519

86. Court of Justice of the European Union. H.K. v Prokuratuur. Case C-746/18. Judgment of 2 March 2021. ECLI:EU:C:2021:152. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0746

87. Court of Justice of the European Union. La Quadrature du Net and Others. Case C-470/21. Judgment of 30 April 2024. ECLI:EU:C:2024:370. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0470

88. European Court of Human Rights. Podchasov v. Russia. Application No. 33696/19. Judgment of 13 February 2024. URL: https://hudoc.echr.coe.int/eng?i=001-230854

89. European Court of Human Rights. Yüksel Yalçınkaya v. Türkiye [GC]. Application No. 15669/20. Judgment of 26 September 2023. URL: https://hudoc.echr.coe.int/eng?i=002-14187

90. UN Human Rights Committee. General Comment No. 32: Article 14, Right to Equality before Courts and Tribunals and to a Fair Trial. 2007. CCPR/C/GC/32. URL: https://docs.un.org/en/CCPR/C/GC/32

91. Council of Europe. Convention on Cybercrime. ETS No. 185. Budapest, 23 November 2001. URL: https://rm.coe.int/1680081561

92. Council of Europe. Explanatory Report to the Convention on Cybercrime. ETS No. 185. Budapest, 23 November 2001. URL: https://rm.coe.int/16800cce5b

93. Council of Europe. Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. Ресми тізім. URL: https://www.coe.int/en/web/cybercrime/parties-observers

94. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. CETS No. 224. Strasbourg, 12 May 2022. URL: https://rm.coe.int/1680a49dab

95. Council of Europe. Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime. CETS No. 224. 2022. URL: https://rm.coe.int/1680a49c9d

96. European Parliament; Council of the European Union. Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings // OJ L 191. 28.07.2023. P. 118–180. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj

97. European Parliament; Council of the European Union. Directive (EU) 2023/1544 of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings // OJ L 191. 28.07.2023. P. 181–190. URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj

98. European Parliament; Council of the European Union. Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for criminal law enforcement purposes // OJ L 119. 04.05.2016. P. 89–131. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj

99. United Nations General Assembly. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. Resolution A/RES/79/243 of 24 December 2024, annex. URL: https://digitallibrary.un.org/record/4071955?ln=en

100. Court of Justice of the European Union. M.N. (EncroChat). Case C-670/22. Judgment of 30 April 2024. ECLI:EU:C:2024:372. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0670

101. Warren S.D., Brandeis L.D. The Right to Privacy // Harvard Law Review. 1890. Vol. 4, No. 5. P. 193–220. URL: https://doi.org/10.2307/1321160

102. Nissenbaum H. Privacy as Contextual Integrity // Washington Law Review. 2004. Vol. 79. P. 119–158. URL: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

103. Solove D.J. A Taxonomy of Privacy // University of Pennsylvania Law Review. 2006. Vol. 154, No. 3. P. 477–560. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622

104. Koops B.-J. The trouble with European data protection law // International Data Privacy Law. 2014. Vol. 4, No. 4. P. 250–261. URL: https://research.tilburguniversity.edu/en/publications/the-trouble-with-european-data-protection-law/

105. Hildebrandt M. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar, 2015. URL: https://www.e-elgar.com/shop/gbp/smart-technologies-and-the-end-s-of-law-9781849808767.html

106. OECD. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. 1980; revised 2013. OECD/LEGAL/0188. URL: https://legalinstruments.oecd.org/public/doc/114/body-text.en.html

107. Council of Europe. Practical Guide on the Use of Personal Data in the Police Sector. Consultative Committee of Convention 108. 2018. URL: https://www.coe.int/en/web/data-protection/-/newly-adopted-practical-guide-on-the-use-of-personal-data-in-the-police-sector-how-to-protect-personal-data-while-combatting-crime-

108. Council of Europe. Recommendation No. R (87) 15 regulating the use of personal data in the police sector. 17 September 1987. URL: https://rm.coe.int/cmrec-87-15-regulating-the-use-of-personal-data-in-the-police-sector/1680a43b58

109. European Court of Human Rights. Z v. Finland. Application No. 22009/93. Judgment of 25 February 1997. URL: https://hudoc.echr.coe.int/fre?i=001-62593

110. European Court of Human Rights. Avilkina and Others v. Russia. Application No. 1585/09. Judgment of 6 June 2013. URL: https://hudoc.echr.coe.int/eng?i=001-120071

111. Court of Justice of the European Union. Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police). Case C-205/21. Judgment of 26 January 2023. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0205

112. EDPB. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2. 17 May 2023. URL: https://www.edpb.europa.eu/documents/guideline/guidelines-052022-on-the-use-of-facial-recognition-technology-in-the-area-of_en

113. NIST. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. Version 1.0. January 2020. URL: https://www.nist.gov/privacy-framework/privacy-framework

114. Brooks S., Garcia M., Lefkovitz N., Lightman S., Nadeau E. An Introduction to Privacy Engineering and Risk Management in Federal Systems. NIST IR 8062. 2017. URL: https://csrc.nist.gov/pubs/ir/8062/final

115. Қылмыстық сот ісін электрондық форматта жүргізу жөніндегі нұсқаулықты бекіту туралы: Қазақстан Республикасы Бас Прокурорының 2018 жылғы 3 қаңтардағы № 2 бұйрығы. Мемлекеттік тіркеу № 16268. URL: https://adilet.zan.kz/kaz/docs/V1800016268

116. Cavoukian A., Taylor S., Abrams M.E. Privacy by Design: essential for organizational accountability and strong business practices // Identity in the Information Society. 2010. Vol. 3. P. 405–413. DOI: 10.1007/s12394-010-0053-z. URL: https://link.springer.com/article/10.1007/s12394-010-0053-z

117. EDPB. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Final version. 20 October 2020. URL: https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_en

118. Hu V.C. et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST SP 800-162. 2014; updated 2019. URL: https://csrc.nist.gov/pubs/sp/800/162/upd2/final

119. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207. 2020. URL: https://csrc.nist.gov/pubs/sp/800/207/final

120. Temoshok D. et al. Digital Identity Guidelines: Authentication and Authenticator Management. NIST SP 800-63B-4. 2025. URL: https://csrc.nist.gov/pubs/sp/800/63/b/4/final

121. European Court of Human Rights. M.M. v. the United Kingdom. Application No. 24029/07. Judgment of 13 November 2012. URL: https://hudoc.echr.coe.int/eng?i=001-114517

122. European Court of Human Rights. Gaughran v. the United Kingdom. Application No. 45245/15. Judgment of 13 February 2020. URL: https://hudoc.echr.coe.int/eng?i=001-200817

123. European Court of Human Rights. Catt v. the United Kingdom. Application No. 43514/15. Judgment of 24 January 2019. URL: https://hudoc.echr.coe.int/eng?i=001-189658

124. Court of Justice of the European Union. Direktor na Glavna direktsia Natsionalna politsia pri MVR – Sofia. Case C-118/22. Judgment of 30 January 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0118

125. Ұлттық архив қоры және архивтер туралы: Қазақстан Республикасының 1998 жылғы 22 желтоқсандағы № 326-I Заңы. URL: https://adilet.zan.kz/kaz/docs/Z980000326_

126. European Court of Human Rights. Surikov v. Ukraine. Application No. 42788/06. Judgment of 26 January 2017. Ресми хабарлама. URL: https://hudoc.echr.coe.int/eng?i=003-5609735-7090499

127. ISO/IEC 27701:2025. Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance. Geneva: ISO, 2025. URL: https://committee.iso.org/standard/27701

128. Адвокаттық қызмет және білікті заң көмегі туралы: Қазақстан Республикасының 2018 жылғы 5 шілдедегі № 176-VI ҚРЗ Заңы. URL: https://adilet.zan.kz/kaz/docs/Z1800000176

129. European Parliament; Council of the European Union. Directive 2012/13/EU of 22 May 2012 on the right to information in criminal proceedings. URL: https://eur-lex.europa.eu/eli/dir/2012/13/oj

130. European Parliament; Council of the European Union. Directive 2013/48/EU of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and related rights upon deprivation of liberty. URL: https://eur-lex.europa.eu/eli/dir/2013/48/oj

131. European Court of Human Rights. Rowe and Davis v. the United Kingdom [GC]. Application No. 28901/95. Judgment of 16 February 2000. URL: https://hudoc.echr.coe.int/eng?i=001-58496

132. European Court of Human Rights. Jasper v. the United Kingdom [GC]. Application No. 27052/95. Judgment of 16 February 2000. URL: https://hudoc.echr.coe.int/eng?i=001-58495

133. Қазақстан Республикасы Жоғарғы Соты. Прокурордың, қылмыстық қудалау органдарының әрекеттеріне (әрекетсіздігіне) және шешімдеріне жасалған шағымдарды соттардың қарауы туралы (ҚПК-нің 106-бабы): 2012 жылғы 27 маусымдағы № 3 нормативтік қаулы. URL: https://adilet.zan.kz/kaz/docs/P120000003S

134. EDPB. Guidelines 01/2022 on data subject rights – Right of access. Version 2.1. 17 April 2023. URL: https://www.edpb.europa.eu/documents/guideline/guidelines-012022-on-data-subject-rights-right-of-access_en

135. EDPB. Guidelines 10/2020 on restrictions under Article 23 GDPR. Version 2.1. 13 October 2021. URL: https://www.edpb.europa.eu/documents/guideline/guidelines-102020-on-restrictions-under-article-23-gdpr_en

136. Қылмыстық процеске қатысушы адамдарды мемлекеттік қорғау туралы: Қазақстан Республикасының 2000 жылғы 5 шілдедегі № 72-II Заңы. URL: https://adilet.zan.kz/kaz/docs/Z000000072_

137. European Court of Human Rights. Doorson v. the Netherlands. Application No. 20524/92. Judgment of 26 March 1996. URL: https://hudoc.echr.coe.int/eng?i=001-57972

138. European Court of Human Rights. Van Mechelen and Others v. the Netherlands. Applications Nos. 21363/93, 21364/93, 21427/93, 22056/93. Judgment of 23 April 1997. URL: https://hudoc.echr.coe.int/eng?i=001-58030

139. United Nations General Assembly. Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power. Resolution 40/34. 29 November 1985. URL: https://www.ohchr.org/sites/default/files/victims.pdf

140. UNODC. Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime. New York: United Nations, 2008. URL: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/Good_Practices_for_the_Protection_of_Witnesses_in_Criminal_Proceedings_Involving_Organized_Crime.pdf

141. United Nations. Convention on the Rights of the Child. 20 November 1989. United Nations Treaty Series. Vol. 1577. P. 3. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

142. UN Committee on the Rights of the Child. General comment No. 25 (2021) on children's rights in relation to the digital environment. CRC/C/GC/25. 2 March 2021. URL: https://docs.un.org/en/CRC/C/GC/25

143. European Court of Human Rights. Volodina v. Russia (No. 2). Application No. 40419/19. Judgment of 14 September 2021. Ресми хабарлама. URL: https://hudoc.echr.coe.int/eng?i=003-7116031-9638379

144. European Court of Human Rights. Buturugă v. Romania. Application No. 56867/15. Judgment of 11 February 2020. Ресми хабарлама. URL: https://hudoc.echr.coe.int/eng?i=003-6635916-8811383

145. European Court of Human Rights. K.U. v. Finland. Application No. 2872/02. Judgment of 2 December 2008 // Reports of Judgments and Decisions. 2008-V. URL: https://ks.echr.coe.int/documents/d/echr-ks/reports_recueil_2008-v

146. Қазақстан Республикасы Жоғарғы Соты. Қылмыстық істер бойынша сот ісін жүргізудің жариялылығы қағидатын сақтау туралы: 2002 жылғы 6 желтоқсандағы № 25 нормативтік қаулы. URL: https://adilet.zan.kz/kaz/docs/P02000025S_

147. European Court of Human Rights. L.L. v. France. Application No. 7508/02. Judgment of 10 October 2006. Information Note No. 90. URL: https://hudoc.echr.coe.int/eng?i=002-3113

148. European Court of Human Rights. Vicent Del Campo v. Spain. Application No. 25527/13. Judgment of 6 November 2018. Information Note No. 223. URL: https://ks.echr.coe.int/documents/d/echr-ks/clin_november_2018_eng

149. Масс-медиа туралы: Қазақстан Республикасының 2024 жылғы 19 маусымдағы № 93-VIII ҚРЗ Заңы. URL: https://adilet.zan.kz/kaz/docs/Z2400000093

150. Council of Europe. Recommendation Rec(2003)13 on the provision of information through the media in relation to criminal proceedings. 10 July 2003. URL: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-rec-2003-13-of-the-committee-of-ministers-to-member-states-on-the-provision-of-information-through-the-media-in-relation-to-criminal-pr

151. European Parliament; Council of the European Union. Directive (EU) 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings. URL: https://eur-lex.europa.eu/eli/dir/2016/343/oj

152. European Court of Human Rights. Bédat v. Switzerland [GC]. Application No. 56925/08. Judgment of 29 March 2016. URL: https://hudoc.echr.coe.int/eng?i=001-161898

153. European Court of Human Rights. Axel Springer AG v. Germany [GC]. Application No. 39954/08. Judgment of 7 February 2012. URL: https://hudoc.echr.coe.int/eng?i=001-109034

154. European Court of Human Rights. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC]. Application No. 931/13. Judgment of 27 June 2017. URL: https://hudoc.echr.coe.int/eng?i=001-175121

155. Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. WP216. 10 April 2014. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

156. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization // UCLA Law Review. 2010. Vol. 57. P. 1701–1777. URL: https://www.uclalawreview.org/pdf/57-6-3.pdf

157. Narayanan A., Shmatikov V. Robust De-anonymization of Large Sparse Datasets // Proceedings of the 2008 IEEE Symposium on Security and Privacy. 2008. P. 111–125. DOI: 10.1109/SP.2008.33. URL: https://collaborate.princeton.edu/en/publications/robust-de-anonymization-of-large-sparse-datasets/

158. Sweeney L. k-anonymity: A model for protecting privacy // International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2002. Vol. 10, No. 5. P. 557–570. URL: https://cyberlaw.stanford.edu/content/files/dataprivacy/projects/kanonymity/kanonymity.pdf

159. Garfinkel S.L. De-Identification of Personal Information. NIST IR 8053. 2015. URL: https://www.nist.gov/publications/de-identification-personal-information

160. Garfinkel S. et al. De-Identifying Government Datasets: Techniques and Governance. NIST SP 800-188. 2023. URL: https://csrc.nist.gov/pubs/sp/800/188/final

161. ENISA. Pseudonymisation techniques and best practices. 2019. URL: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

162. Dwork C. Differential Privacy // Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science. Vol. 4052. P. 1–12. URL: https://www.microsoft.com/en-us/research/publication/differential-privacy/

163. EDPB. Guidelines 01/2021 on Examples regarding Personal Data Breach Notification. 3 January 2022. URL: https://www.edpb.europa.eu/documents/guideline/guidelines-012021-on-examples-regarding-personal-data-breach-notification_en

164. Құқықтық актілер туралы: Қазақстан Республикасының 2016 жылғы 6 сәуірдегі № 480-V ҚРЗ Заңы. URL: https://adilet.zan.kz/kaz/docs/Z1600000480

165. UN High Commissioner for Human Rights. The right to privacy in the digital age. A/HRC/39/29. 3 August 2018. URL: https://digitallibrary.un.org/record/1640588/files/A_HRC_39_29-EN.pdf

166. OHCHR. The right to privacy in the digital age. A/HRC/51/17. 4 August 2022. URL: https://digitallibrary.un.org/record/3985679/files/A_HRC_51_17-EN.pdf

167. EDPS. Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit. 11 April 2017. URL: https://www.edps.europa.eu/press-publications/press-news/press-releases/2017/privacy-friendly-policymaking-made-easier-edps_en

168. EDPS. Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. 19 December 2019. URL: https://www.edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

169. Court of Justice of the European Union. Bezirkshauptmannschaft Landeck (Attempt to access personal data stored on a mobile telephone). Case C-548/21. Judgment of 4 October 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0548

170. ISO/IEC 29134:2023. Information technology – Security techniques – Guidelines for privacy impact assessment. Geneva: ISO, 2023. URL: https://www.iso.org/standard/86012.html

171. NIST. Assessing Security and Privacy Controls in Information Systems and Organizations. NIST SP 800-53A Rev. 5. 2022; Release 5.2.0, 2025. URL: https://csrc.nist.gov/pubs/sp/800/53/a/r5/final

172. OECD. Declaration on Government Access to Personal Data Held by Private Sector Entities. 14 December 2022. OECD/LEGAL/0487. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

173. Жасанды интеллект туралы: Қазақстан Республикасының 2025 жылғы 17 қарашадағы № 230-VIII ҚРЗ Заңы. URL: https://adilet.zan.kz/kaz/docs/Z2500000230

174. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. 2023. URL: https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10

175. CEPEJ. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. 2018. URL: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment

176. Court of Justice of the European Union. Ligue des droits humains ASBL v Conseil des ministres. Case C-817/19. Judgment of 21 June 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62019CJ0817

177. CEPEJ. Guidelines on how to drive change towards Cyberjustice: Stock-taking of tools deployed and summary of good practices. CEPEJ(2016)13. 7 December 2016. URL: https://www.coe.int/en/web/cepej/documentation/cepej-documents/guidelines

178. OECD. Regulatory Impact Assessment. OECD Best Practice Principles for Regulatory Policy. Paris: OECD Publishing, 2020. DOI: 10.1787/7a9638cb-en. URL: https://www.oecd.org/en/publications/regulatory-impact-assessment_7a9638cb-en.html

179. United Nations Statistics Division. Manual for the Development of a System of Criminal Justice Statistics. Studies in Methods. Series F, No. 89. New York: United Nations, 2003. URL: https://unstats.un.org/unsd/demographic-social/standards-and-methods/?topics=Crime+Statistics

180. HM Treasury; Evaluation Task Force. The Magenta Book: Central Government guidance on evaluation. Updated 15 May 2026. URL: https://www.gov.uk/government/publications/the-magenta-book/magenta-book-central-government-guidance-on-evaluation-html

ҚОСЫМША А

Ғылыми-зерттеу жұмысының нәтижелерін Қазақстан Республикасы Бас прокуратурасының практикалық қызметіне енгізу туралы АКТ

Астана қ. **«28» қыркүйек 2026 жыл**

Осы акт Жұмадилова Назерке Серікжанқызының 8D04203 – «Құқықтану» білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесін алу үшін дайындалған «Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің қылмыстық-процестік мәселелері» тақырыбындағы диссертациялық зерттеу нәтижелерінің Қазақстан Республикасы Бас прокуратурасының практикалық қызметіне енгізілгенін растайды.

1. Ғылыми-зерттеу жұмысының атауы: «Дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің қылмыстық-процестік мәселелері».

2. Ғылыми нәтиженің түрі: дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеру кезінде дәлелдемелерді жинау, бекіту, зерттеу және бағалау, жеке өмірге қолсұғылмаушылықты қамтамасыз ету және прокурорлық қадағалауды жетілдіру жөніндегі ғылыми негізделген қорытындылар мен практикалық ұсынымдарды қамтитын диссертациялық жұмыс.

3. Тапсырыс беруші: әл-Фараби атындағы Қазақ ұлттық университеті.

4. Жұмысты орындаушы: Жұмадилова Назерке Серікжанқызы.

5. Жұмысты орындау негізі: 8D04203 – «Құқықтану» білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесін алу үшін дайындалған диссертациялық зерттеу шеңберінде бекітілген докторанттың жеке жұмыс жоспары.

6. Енгізу туралы мәліметтер: зерттеу нәтижелері Қазақстан Республикасы Бас прокуратурасының қызметінде осы санаттағы істер бойынша сотқа дейінгі тергеп-тексерудің заңдылығына прокурорлық қадағалауды жүзеге асыру, процеске қатысушылардың құқықтарын қорғау, өтінішхаттар мен шағымдарды қарау, сондай-ақ дәлелдемелерді алу мен бекітудің процестік тәртібін және құқық қолдану практикасын талдау барысында пайдаланылуда.

7. Енгізу тиімділігі туралы мәліметтер: зерттеу нәтижелерін пайдалану дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексерудің заңдылығын қамтамасыз етуге, прокурорлық қадағалаудың тиімділігін арттыруға, процестік шешімдер мен әрекеттердің заңдылығын тексеру сапасын жақсартуға ықпал етеді.

Автор әзірлеген ғылыми-практикалық ұсынымдар:

- сотқа дейінгі тергеп-тексеру материалдары мен процестік шешімдерге прокурорлық баға берудің негізділігін арттыруға;
- дербес деректерді заңсыз жинауға, өңдеуге және таратуға байланысты қылмыстық құқық бұзушылықтар бойынша дәлелдеуге жататын мән-жайларды толық анықтауға;
- цифрлық ақпаратты алу мен бекіту кезінде қылмыстық-процестік нысанның сақталуын, ақпараттың тұтастығы мен анықтығын тексеруге;
- дәлелдемелерді алу, бекіту немесе сақтау тәртібінің бұзылуына байланысты

оларды жол берілмейтін деп тану тәуекелін төмендетуге;

- жәбірленушілердің, күдіктілердің, айыпталушылардың және қылмыстық процеске өзге де қатысушылардың құқықтарын тиісінше қорғауға;
- ақпараттық жүйелердегі дербес деректерге құқыққа қайшы қол жеткізумен байланысты бұзушылықтарды анықтау тиімділігін арттыруға;
- операторлармен, провайдерлермен, интернет-платформалармен және өзге де дерек ұстаушылармен өзара іс-қимылдың заңдылығын бағалаудың бірыңғай тәсілдерін қалыптастыруға;
- қылмыстық қудалау мүдделері мен жеке өмірге қол сұқпаушылықтың конституциялық кепілдіктері арасындағы тепе-теңдікті сақтауға мүмкіндік береді.

Енгізілген нәтижелердің практикалық маңызы дербес деректердің заңсыз айналымына байланысты құқық бұзушылықтарды тергеп-тексеру тиімділігін арттырумен қатар, қылмыстық сот ісін жүргізуде жеке адамның құқықтары мен бостандықтарын қорғауға бағытталуымен айқындалады.

Диссертациялық зерттеу нәтижелері Қазақстан Республикасы прокуратура органдарының қызметінде талдамалық материалдар, прокурорлық қадағалау актілері, әдістемелік ұсынымдар, құқық қолдану практикасына шолулар, сондай-ақ дербес деректерді қорғау саласындағы қылмыстық-процестік заңнаманы және құқық қолдану практикасын жетілдіру жөніндегі ұсыныстарды дайындау кезінде пайдаланылуы мүмкін.

Осы акт диссертациялық зерттеу нәтижелерінің практикалық маңызын және оларды Қазақстан Республикасы прокуратура органдарының қызметінде қолдану мүмкіндігін растайды.

Қазақстан Республикасы Бас прокуратурасының
Сотқа дейінгі тергеп-тексерудің және
қылмыстық қудалаудың заңдылығын қадағалау
қызметі басқармасының бастығы **І.М. Ескалиев**

ҚОСЫМША Б

Дербес деректерге қатысты дәлелдемелерді жинау: тергеу практикасы (респонденттер санаты: тергеуші, анықтаушы, жедел уәкіл).

I. Жалпы мәлімет

A1. Сіздің лауазымыңыз:

□ тергеуші
□ анықтаушы
□ жедел уәкіл
□ басқа: _____

A2. Қызмет өтіліңіз (жыл):

□ 0–3
□ 4–7
□ 8–12
□ 13 және одан жоғары

A3. Соңғы 12 айда дербес деректерді заңсыз жинаумен, өңдеумен және таратумен байланысты істер/материалдармен жұмыс істеу жиілігі:

□ ешқашан
□ 1–2 рет
□ 3–5 рет
□ 6–10 рет
□ 10 реттен көп

II. Дәлелдеу пәні және СДТТ ұйымдастыру

A4. Мұндай істер бойынша дәлелдеу пәнін айқындаудағы ең негізгі қиындықтарды көрсетіңіз (бірнеше жауап мүмкін):

□ дербес деректердің нақты санатын/көлемін анықтау
□ деректерді өңдеудің/таратудың нақты тәсілін бекіту
□ заңды негіздің (келісім, заң, өкілеттік) бар-жоғын дәлелдеу
□ дерек ұстаушы/оператор рөлін айқындау
□ электрондық іздердің жойылып кетуі (логтардың сақталмауы)
□ субъектіні (кінәліні) сәйкестендіру
□ басқа: _____

A5. СДТТ-ді ұйымдастыруда қандай процестік шешімдер ең күрделі болады?

□ қылмыстық құқық бұзушылық туралы арыз/хабарламаны қабылдау және тіркеу
□ іс жүргізуді бастау туралы шешім қабылдау
□ тергеу нұсқаларын жоспарлау және дәлелдеу пәнін құрылымдау
□ дерек ұстаушылардан ақпаратты жедел алу
□ электрондық тасымалдаушыларды алу/қарау/зерттеу
□ ЖТӘ қолдану қажеттілігін негіздеу
□ басқа: _____

III. Дерек ұстаушылардан ақпарат алу және дәлелдемелерді бекіту

A6. Дерек ұстаушылардан (операторлар, провайдерлер, ұйымдардың

АЖ әкімшілері және т.б.) ақпарат алу арнасы көбіне қандай?
□ ресми сұрату (қағаз/электрондық құжат айналымы)
□ ақпараттық жүйелер арқылы интеграцияланған арна
□ электрондық пошта арқылы (ресми домен)
□ жедел байланыс/хат алмасу (қосымша түсіндірумен)
□ басқа: _____
А7. Ақпаратты алу мерзімі әдетте қанша уақыт алады?
□ 0–24 сағат
□ 2–3 күн
□ 4–7 күн
□ 8–14 күн
□ 14 күннен көп
А8. Алынған электрондық материалды бекіту кезінде сіз міндетті түрде көрсететін реквизиттер (бірнеше жауап):
□ дерек көзі/дерек ұстаушы (атауы)
□ алу уақыты және алу арнасы
□ алынған файл/жазба атауы, көлемі, формат(тар)
□ идентификаторлар (телефон нөмірі, аккаунт, IP және т.б.)
□ қоса берілген материалдардың тізбесі (тасымалдаушы, көшірме)
□ басқа: _____
А9. Төмендегі пікірмен келісу деңгейіңізді белгілеңіз: «Дерек ұстаушылардан алынатын деректер көлемі дәлелдеу пәнімен шектелуі тиіс (артық деректерді алмау/минимизациялау)».

1 – мүлдем келіспеймін	2 – келіспеймін	3 – бейтарап	4 – келісемін	5 – толық келісемін

IV. ЖТӘ және цифрлық ортадағы дәлелдемелер
А10. Жасырын тергеу әрекеттерін (ЖТӘ) қолдануға көбіне не себеп болады? (бірнеше жауап)
□ ашық процестік тәсілдермен деректерді алу мүмкін болмауы
□ деректердің жойылып кету тәуекелі
□ қылмыстық құқық бұзушылықтың жасырын тәсілмен жасалуы
□ байланыс арналары/аккаунттар бойынша ақпараттың қажет болуы
□ басқа: _____
А11. Цифрлық ортадағы дәлелдемелердің жол берілетіндігіне күмән туғызатын ең жиі себептер қандай? (бірнеше жауап)
□ алу рәсімінің процестік нысаны сақталмаған
□ дерек көзі анық емес (кім/қай жүйе қалыптастырған)
□ тұтастыққа кепіл жоқ (өзгеруі мүмкін)
□ уақыт белгісі/логтар сәйкес келмейді
□ маманның/арнайы білімнің жеткіліксіз пайдаланылуы
□ басқа: _____
V. Ұсыныстар
А12. ҚПК-те немесе ведомстволық әдістемеде нақтылауды қажет ететін үш мәселені атаңыз:
1) _____

2) _____
3) _____

А) «Жылдамдық» және «жойылу тәуекелі»

А13. Деректердің жойылып кетуіне әкелетін негізгі фактор (1 жауап):

□ сақтау мерзімі қысқа (лог retention)
□ сұрату ұзақ рәсімделеді
□ провайдер/ұйым ішкі келісімдері ұзақ
□ техникалық құзырет жетіспейді
□ басқа: ___

А14. Қандай деректер түрі ең «тез жоғалады»? (1 жауап)

□ мессенджер жазбалары
□ call detail records
□ IP/сессия логтары
□ CCTV/бейне
□ банктік транзакция метадеректері
□ басқа: ___

А15. Электрондық материалды бекіту кезінде ең жиі қате қай жерде кетеді? (1 жауап)

□ алу/тексеру хаттамасы
□ қосымшаларды сипаттау
□ дерек көзін көрсету
□ тұтастықты растау
□ маман/IT қатыстырмау
□ басқа: ___

А16. Нақты істе «артық дерек» алынған жағдай болды ма?

□ жоқ □ сирек □ кейде □ жиі □ өте жиі

А17. Артық дерек алынса, оны «бөліп» сақтау/редакциялау жасала ма?

□ ешқашан □ сирек □ кейде □ жиі □ өте жиі

ҚОСЫМША В

Қадағалау және санкциялау практикасы
Респонденттер санаты: прокурор, тергеу судьясы

I. ЖТӘ қолданудың негізділігі

В1. ЖТӘ бойынша өтінішхаттар/материалдарда ең жиі кездесетін кемшіліктер (бірнеше жауап):

□ негіздеменің жеткіліксіздігі (қажеттілік дәлелденбейді)
□ мақсат пен көлемнің дәл айқындалмауы
□ баламалы ашық тәсілдердің қаралмауы
□ мерзім/объект/идентификаторлардың нақтыланбауы
□ қолданылатын шараның қажет мөлшермен шектелетіні негізделмеуі
□ басқа: _____

В2. Төмендегі пікірмен келісу деңгейіңізді белгілеңіз: «Дербес деректерді алуға бағытталған ЖТӘ-де деректер көлемі дәлелдеу пәнімен қатаң шектелуі тиіс».

1 – мүлдем келіспеймін	2 – келіспеймін	3 – бейтарап	4 – келісемін	5 – толық келісемін

II. Электрондық дәлелдемелердің жол берілетіндігін бағалау

В3. Электрондық дәлелдемелерді бағалауда шешуші өлшемдерді маңыздылығы бойынша 1–5 ретімен қойыңыз (1 – ең маңызды):

□ алу рәсімінің заңдылығы (процестік нысан)
□ дерек көзі мен қалыптасу тетігінің анықтылығы
□ тұтастық (өзгермегендігі)
□ тексерілгіштік (қайта тексеру мүмкіндігі)
□ қатыстылық және жеткіліктілік

III. Құпиялылық және жария ету тәуекелі

В4. Сотқа дейінгі тергеп-тексеру деректерін жария ету тәуекелі ең жоғары саты (бір жауап):

□ сотқа дейінгі тергеп-тексеру
□ істі сотқа дайындау
□ үкімнің (шешімнің) заңды күшіне енуі және оны орындау
□ анық айта алмаймын

В5. ҚПК-ті жетілдіру қажет деп санайтын негізгі бағыттарды белгілеңіз (бірнеше жауап):

□ дерек ұстаушылардан ақпарат алу тәртібін нақтылау
□ электрондық дәлелдемелер бойынша процестік бекіту стандартын нақтылау
□ дербес деректерді қорғаудың арнайы процестік режимін енгізу
□ іс материалдарына қолжетімділікте деректерді шектеу/редакциялау тетіктері
□ ЖТӘ қолдану кезінде мөлшерлестік/минимизация талаптарын күшейту
□ басқа: _____

В6. ЖТӘ материалдарында қай компонент жиі жетіспейді? (бір жауап)

□ қажеттілік (necessity)
□ мөлшерлестік/минимизация (proportionality)
□ балама ашық тәсілдерді талдау
□ объект/идентификатор нақтылығы
□ мерзім негіздемесі

В7. ЖТӘ арқылы алынатын деректер көлемін шектеудің ең дұрыс тәсілі (1 жауап)

□ нақты идентификаторлармен шектеу (IP/ID/№)
□ уақыт диапазонымен шектеу
□ дерек түрімен шектеу (тек метадерек)
□ тұлғалар шеңберімен шектеу
□ аралас

В8. Ортақ стандартты қай деңгейде бекіткен дұрыс?

□ ҚПК-де
□ ведомстволық әдістемеде
□ Жоғарғы Сот нормативтік қаулысында
□ бірлескен регламентте

ҚОСЫМША Г

Қорғау тарапының процестік тәуекелдер бағасы
Респонденттер санаты: адвокат, заң консультанты, судья (қылмыстық істер), қорғау тарапының өкілдері.

I. Электрондық дәлелдемелер және даулар

С1. Электрондық дәлелдемелерге қатысты қандай негіздер бойынша жиі қарсылық білдіріледі? (бірнеше жауап)

□ алу рәсімінің заңсыздығы/процестік нысан сақталмауы
□ дереккөзі анық емес
□ тұтастыққа күмән
□ идентификация (аккаунт/нөмір) дәлелденбеген
□ маман қорытындысының/техникалық түсіндірменің болмауы
□ басқа: _____

С2. Төмендегі пікірмен келісу деңгейіңізді белгілеңіз: «Электрондық дәлелдемелердің жол берілетіндігін бағалау үшін ортақ өлшемдер (стандарт) қажет».

1 – мүлдем келіспеймін	2 – келіспеймін	3 – бейтарап	4 – келісемін	5 – толық келісемін

II. Іс материалдарына қолжетімділік және дербес деректер

С3. Іс материалдарымен танысу кезінде артық дербес деректердің болуы қандай тәуекел тудырады? (бірнеше жауап)

□ деректердің үшінші тұлғаларға таралуы
□ жәбірленуші/куәларға қысым көрсету тәуекелі
□ тараптардың құқықтарының теңгеріміне кері әсер
□ процестің созылуы (артық материал)
□ тәуекел жоқ/елеусіз

С4. Қолдануға орынды деп санайтын тетіктер (бірнеше жауап):

□ қолжетімділікті саралау (тек қажет бөлігі)
□ көшірмелерде деректерді редакциялау/деперсонализациялау
□ дербес деректерді бөлек қосымша ретінде сақтау
□ көшірмелеуді шектеу (процестік тәртіппен)
□ басқа: _____

ҚОСЫМША Д

Дерек ұстаушылармен өзара іс-қимыл: сұрату тәртібі, сақталым және жауапкершілік
Респонденттер санаты: дерек ұстаушылар (операторлар, провайдерлер, ұйымдардың ақпараттық жүйе әкімшілері, комплаенс/қауіпсіздік бөлімдері).

I. Сұратулар мен өзара іс-қимыл
D1. Сізге құқық қорғау органдарынан деректерге қатысты сұратулар қаншалықты жиі түседі?
□ ешқашан
□ сирек
□ кейде
□ жиі
□ өте жиі
D2. Сұратулардың мазмұны қаншалықты нақты (қажетті деректер, мерзім, формат, құқықтық негіз көрсетілуі)?
□ мүлдем нақты емес
□ ішінара нақты
□ толық нақты
D3. Деректерді беру кезінде негізгі қиындықтар (бірнеше жауап):
□ сұратудағы идентификаторлардың нақтыланбауы
□ мерзімнің өте қысқалығы
□ құқықтық негіздің түсініксіздігі
□ қауіпсіз арнаның болмауы/шектеулілігі
□ деректер көлемін шектеу қажеттілігі (минимизация)
□ лог/метадеректерді сақтау мерзімдерінің жеткіліксіздігі
□ басқа: _____
II. Қауіпсіздік және верификация
D4. Деректерді беру фактісі және берілген материалдар құрамы ішкі журналда (логта) тіркеле ме?
□ иә, толық
□ ішінара
□ жоқ
□ айту қиын
D5. ҚПК деңгейінде нақтылауды қажет ететін тетіктерді белгілеңіз (бірнеше жауап):
□ сұратудың стандартты құрылымы (мақсат, көлем, мерзім)
□ қауіпсіз арна және техникалық формат талаптары
□ деректердің тұтастығын растау (верификация) рәсімі
□ артық деректерді бермеу/бөлек беру тәртібі
□ басқа: _____

ҚОСЫМША Е

Дерек ұстаушылармен өзара іс-қимыл: сұрату тәртібі, сақталым және жауапкершілік
Респонденттер санаты: деректер субъектілері (жәбірленушілер немесе дербес деректері заңсыз тараған деп есептейтін тұлғалар).

I. Оқиға және салдар
Е1. Сіздің дербес деректеріңіз қай салада тарады деп ойлайсыз? (бірнеше жауап)
□ банк/қаржы қызметтері
□ медицина/денсаулық сақтау
□ мемлекеттік қызметтер
□ жұмыс/HR
□ әлеуметтік желі/мессенджер
□ басқа: _____
Е2. Қандай салдар/зиян болды? (бірнеше жауап)
□ алаяқтық әрекеттер/қоңыраулар көбейді
□ қаржылық шығын
□ беделдік/психологиялық зиян
□ қорқыныш, сенімсіздік
□ салдар жоқ/білмеймін
□ басқа: _____
II. Құқық қорғау органына жүгіну және сенім
Е3. Сіз құқық қорғау органына жүгіндіңіз бе?
□ иә
□ жоқ
Е4. Жүгінбеуге негізгі себеп (бір жауап):
□ сенімсіздік
□ дәлел жоқ деп ойладым
□ процестің ұзақтығы
□ қайтадан деректерім таралып кетеді деп қорықтым
□ басқа: _____
Е5. Төмендегі пікірмен келісу деңгейіңізді белгілеңіз: «Іс материалдарына қолжетімділік кезінде менің деректерім қайта таралуы мүмкін деп қауіптенемін».

1 – мүлдем келіспеймін	2 – келіспеймін	3 – бейтарап	4 – келісемін	5 – толық келісемін

Е6. Қандай тетіктер сіздің сеніміңізді арттырады? (бірнеше жауап)
□ іс материалдарында артық деректерді алып тастау/қысқарту
□ көшірмелерде деректерді редакциялау/деперсонализациялау
□ қолжетімділікті шектеу және бақылау
□ деректерді жария еткені үшін жауаптылықтың нақты қолданылуы
□ басқа: _____