QANUN № 08 (382), 2026, s.162-170

İbrahimzadə Lalə İlqar qızı,
Azərbaycan Resplublikasının Ədliyyə Nazirliyinin Məhkəmə Ekspertizası Mərkəzinin
"Cinayət prosesi; kriminalistika və məhkəmə ekspertizası; əməliyyat-axtarış fəaliyyəti" ixtisaslaşması üzrə doktorantı
E-mail: laleibrahimzade37@gmail.com
Ünvan: Bakı şəhəri, Səbail rayonu, Xaqani küçəsi 24

UOT 343.1
DOI: https://doi.org/10.30546/2218-9130.008.382.2026.1161

KİBERCİNAYƏTLƏRİN İBTİDAİ İSTİNTAQI ZAMANI İNSAN HÜQUQLARININ MÜDAFİƏSİNİN HÜQUQİ TƏMİNATLARI

Açar sözlər: *kibercinayətkarlıq, ilkin istintaq, insan hüquqları, rəqəmsal sübutlar, elektron sübutlar, şəxsi həyatın toxunulmazlığı hüququ, ədalətli məhkəmə araşdırması, sübutların saxlanma və ötürülmə zənciri, süni intellekt, blokçeyn.*

Ключевые слова: *киберпреступность, предварительное расследование, права человека, цифровые доказательства, электронные доказательства, неприкосновенность частной жизни, справедливое судебное разбирательство, chain of custody, искусственный интеллект, блокчейн.*

Keywords: *cybercrime, preliminary investigation, human rights, digital evidence, electronic evidence, right to privacy, fair trial, chain of custody, artificial intelligence, blockchain.*

Giriş

Cəmiyyətin rəqəmsallaşması cinayət hüququ və cinayət-prosessual hüquq üçün yeni reallıqlar yaratmışdır. Əvvəllər cinayət hadisəsinin sübut olunması daha çox şahid ifadələri, maddi sübutlar, sənədlər və ekspert rəyləri əsasında həyata keçirilirdisə, hazırda cinayətlərin böyük bir hissəsində elektron izlər mühüm əhəmiyyət daşıyır. Mobil telefon məlumatları, IP ünvanları, elektron yazışmalar, sosial media paylaşımları, elektron ödəniş məlumatları, bulud yaddaşı, müşahidə kameraları, üz tanıma sistemləri və digər rəqəmsal məlumatlar istintaq üçün əhəmiyyətli sübut mənbələrinə çevrilmişdir. Müasir cinayət mühakiməsində rəqəmsal sübutlar təkcə kibercinayətlərin deyil, həm də ənənəvi cinayətlərin araşdırılmasında mühüm sübut mənbələrindən birinə çevrilmişdir və hüquqmühafizə orqanlarının qarşısında yeni texniki və prosessual vəzifələr yaratmışdır [12, s.18].

Kibercinayətlərin xüsusiyyəti ondan ibarətdir ki, belə cinayətlərdə sübutlar çox vaxt fiziki məkanda deyil, rəqəmsal mühitdə formalaşır. Bu sübutlar asanlıqla dəyişdirilə, silinə, kopyalana, başqa yurisdiksiyaya ötürülə və ya şifrələnə bilər. Ona görə də onların əldə olunması və qiymətləndirilməsi ənənəvi sübutlarla müqayisədə daha mürəkkəbdir. Rəqəmsal sübut müasir cinayət prosesində əhəmiyyətli yer tutsa da, onun dəyişkənliyi, asanlıqla manipulyasiya edilə bilməsi və müxtəlif texniki sistemlərdə saxlanılması məhkəmələr üçün ciddi hüquqi və praktiki çətinliklər yaradır.

Digər tərəfdən, rəqəmsal sübutların toplanması çox vaxt şəxsin şəxsi həyatına geniş müdaxilə ilə müşayiət olunur. Bir mobil telefonun və ya kompüterin araşdırılması nəticəsində şəxsin yal-

nız cinayət işi ilə bağlı məlumatları deyil, ailə həyatı, şəxsi münasibətləri, maliyyə vəziyyəti, sağlamlıq məlumatları, hərəkət trayektoriyası və sosial əlaqələri barədə də geniş informasiya əldə edilə bilər. Rəqəmsal sübutlardan istifadə cinayət ədalət mühakiməsi üçün üstünlük yaratsa da, bu sübutların çox vaxt böyük həcmdə şəxsi məlumat ehtiva etməsi şəxsi həyatın toxunulmazlığı hüququnun qorunmasını xüsusi aktuallaşdırır.

Şəxsi məlumatların emalı zamanı qanunilik, məqsədlə məhdudluq, məlumatların minimallaşdırılması və təhlükəsizlik prinsipləri Avropa Şurasının "Şəxsi məlumatların avtomatlaşdırılmış qaydada emalı zamanı şəxslərin müdafiəsi haqqında" 1981-ci il Konvensiyasında da təsbit olunmuşdur [10].

Bu baxımdan kibercinayətlərin ibtidai istintaqı zamanı əsas məsələ yalnız sübutların tez və effektiv əldə olunması deyil, həmin prosesin hüquqi, şəffaf, mütənasib və müdafiə tərəfi üçün mübahisələndirilə bilən olmasıdır. İstintaqın effektivliyi insan hüquqlarının məhdudlaşdırılması üçün ümumi əsas kimi qəbul edilə bilməz. Əksinə, rəqəmsal sübutların gücü artdıqca, onların əldə olunması və istifadəsinə dair hüquqi təminatlar da gücləndirilməlidir.

Rəqəmsal sübut anlayışı və kibercinayətlərin istintaqında onun rolu. Rəqəmsal sübut dedikdə, elektron və ya rəqəmsal formada mövcud olan, cinayət hadisəsinin törədilməsi, cinayətin subyekti, cinayətin mexanizmi, zərərçəkmiş şəxs, hadisənin yeri, vaxtı və digər sübut əhəmiyyətli hallar barədə məlumat verən informasiya başa düşülür. Bu məlumat kompüterdə, mobil telefonda, serverdə, bulud yaddaşında, sosial media platformasında, elektron poçtda, müşahidə sistemində və ya digər rəqəmsal mühitdə saxlanıla bilər. Rəqəmsal sübutların əsas xüsusiyyətləri onların asanlıqla kopyalana bilməsi, dəyişdirilməsi ehtimalı və bütövlüyünün xüsusi kriminalistik metodlarla qorunmasının zəruriliyidir [7, s. 45-46].

Rəqəmsal sübutların əsas kateqoriyaları kompüterdə saxlanılan məlumatlar, internet və şəbəkə məlumatları, mobil cihaz sübutları, bulud əsaslı sübutlar, ağıllı cihaz məlumatları, blockchain (blokçeyn) və paylanmış reyestr qeydləri kimi təsnif olunur [21, s. 38]. Bu təsnifat göstərir ki, rəqəmsal sübutlar yalnız kompüter fayllarından ibarət deyil. Onlar eyni zamanda IP loqlarını, server qeydlərini, GPS məlumatlarını, mesajlaşma tətbiqlərinin yazışmalarını, kriptovalyuta əməliyyatlarını, ağıllı ev cihazlarının qeydlərini və digər texnoloji izləri əhatə edir [5, s.10-11].

Kibercinayətlərin istintaqında rəqəmsal sübutların rolu iki istiqamətdə özünü göstərir. Birincisi, bu sübutlar cinayətin törədilmə mexanizmini müəyyən etməyə kömək edir. Məsələn, qanunsuz giriş, məlumatların silinməsi, saxta profil yaradılması, zərərli proqramın yerləşdirilməsi və ya elektron ödənişlərin yönləndirilməsi kimi əməllərin sübut olunması çox vaxt yalnız rəqəmsal izlər vasitəsilə mümkündür. İkincisi, rəqəmsal sübutlar təqsirləndirilən şəxsin kimliyini, əlaqələrini, hərəkət trayektoriyasını və cinayətlə bağlı rolunu müəyyən etmək üçün istifadə olunur.

Lakin rəqəmsal sübutların yüksək sübutetmə potensialı onların avtomatik olaraq etibarlı və qanuni hesab olunması demək deyildir. Əksinə, bu sübutların dəyişdirilə bilməsi, kontekstdən çıxarıla bilməsi, texniki səhvlərə məruz qalması və bəzən avtomatlaşdırılmış sistemlər tərəfindən yanlış təhlil edilməsi onların xüsusi prosessual təminatlar əsasında qiymətləndirilməsini tələb edir. Rəqəmsal sübutların artan rolu onların emalı zamanı "prosedur dəqiqliyi hüququ"nun (procedural accuracy right) formalaşdırılmasını aktual edir və bu yanaşma ədalətli məhkəmə araşdırması hüququnun rəqəmsal dövrə uyğun inkişafı kimi əsaslandırılır [23, s.18-20].

Şəxsi həyatın toxunulmazlığı hüququ və rəqəmsal sübutların toplanması. Kibercinayətlərin ibtidai istintaqı zamanı ən çox təsirə məruz qalan hüquqlardan biri şəxsi həyatın toxunulmazlığı hüququdur. Rəqəmsal mühitdə şəxsin həyatına dair məlumatların həcmi olduqca genişdir. Telefon və kompüterlərdə saxlanılan fotoşəkillər, yazışmalar, sənədlər, bank məlumatları, internet axtarış tarixçəsi, yerləşmə

məlumatları və şəxsi qeydlər dövlət orqanlarının müdaxiləsi üçün həssas sahələrdir.

Avropa İnsan Hüquqları Konvensiyasının 8-ci maddəsinə əsasən hər kəsin şəxsi və ailə həyatına, mənzilinə və yazışmalarına hörmət hüququ vardır. Bu hüquqa dövlət müdaxiləsi yalnız qanunla nəzərdə tutulduğu, legitim məqsəd daşıdığı və demokratik cəmiyyətdə zəruri olduğu halda mümkündür. Kibercinayətlərin istintaqında elektron cihazlara baxış, məlumatların götürülməsi, yazışmaların əldə edilməsi, IP məlumatlarının istənilməsi və digər tədbirlər məhz bu hüququn məhdudlaşdırılması ilə bağlıdır [8].

Şəxsi həyatın toxunulmazlığı hüququ beynəlxalq insan hüquqları sistemində də mühüm yer tutur. Mülki və Siyasi Hüquqlar haqqında Beynəlxalq Paktın 17-ci maddəsinə əsasən heç kəs öz şəxsi və ailə həyatına, mənzilinə və yazışmalarına qanunsuz və ya özbaşına müdaxiləyə məruz qalmamalıdır [15].

Bu sahədə Avropa İnsan Hüquqları Məhkəməsinin təcrübəsi xüsusi əhəmiyyət daşıyır. AİHM-in yanaşmasına görə, rəqəmsal sübutun əldə olunması özlüyündə qanunsuz hesab edilmir, lakin belə sübutun şəxsi həyat hüququnun pozulması ilə əldə edilməsi onun cinayət prosesində istifadəsini problemli edir. Bu baxımdan Benedik v. Slovenia işi mühüm əhəmiyyət daşıyır. Həmin işdə hüquq-mühafizə orqanları məhkəmə qərarı olmadan dinamik IP ünvanı ilə bağlı abunəçi məlumatlarını əldə etmişdilər. AİHM bu müdaxilənin kifayət qədər aydın, əlçatan və qabaqcadan proqnozlaşdırıla bilən hüquqi əsasının olmadığını müəyyən etmiş və Konvensiyanın 8-ci maddəsinin pozulduğu qənaətinə gəlmişdir [4].

Digər mühüm iş Glukhin v. Russia qərarıdır. Bu işdə şəxsin üz tanıma texnologiyası vasitəsilə müəyyən edilməsi və sonradan inzibati məsuliyyətə cəlb olunması məsələsi araşdırılmışdır. Məhkəmə qeyd etmişdir ki, üz tanıma kimi texnologiyalardan istifadə yalnız qanuni əsas, zərurilik, mütənasiblik və adekvat təminatlar olduqda mümkündür. Əks halda, belə texnologiyalar yalnız şəxsi həyat hüququna deyil, həm də ifadə və toplaşmaq azadlığına çəkindirici təsir göstərə bilər [11].

Bu yanaşmadan belə nəticə çıxır ki, rəqəmsal sübutların toplanması zamanı hüquq-mühafizə orqanları istintaq maraqlarını əsas gətirərək şəxsin bütün rəqəmsal həyatına məhdudiyyətsiz müdaxilə edə bilməzlər. Müdaxilə konkret cinayət işi ilə əlaqəli, qanuni, zəruri və mütənasib olmalıdır. Axtarışın hüdudları əvvəlcədən müəyyənləşdirilməli, yalnız iş üçün əhəmiyyətli məlumatlar götürülməli və şəxsi həyatla bağlı artıq məlumatların istifadəsi məhdudlaşdırılmalıdır.

Ədalətli məhkəmə araşdırması və müdafiə tərəfinin rəqəmsal sübutlara çıxışı. Rəqəmsal sübutların istifadəsi yalnız şəxsi həyat hüququ ilə bağlı deyil, həm də ədalətli məhkəmə araşdırması hüququ ilə sıx bağlıdır. Konvensiyanın 6-cı maddəsi hər kəsə ədalətli məhkəmə araşdırması hüququ verir. Bu hüququn əsas elementləri sırasında tərəflərin bərabərliyi, müdafiə hüququ, sübutları mübahisələndirmək imkanı və məhkəmə prosesində real iştirak hüququ dayanır [8].

Rəqəmsal sübutlar müdafiə tərəfi üçün xüsusi çətinliklər yaradır. Bir çox hallarda belə sübutların əldə olunması və təhlili mürəkkəb texniki metodlardan, xüsusi proqram təminatından və ekspert biliklərindən asılıdır. Müdafiəçi və təqsirləndirilən şəxs təqdim olunan rəqəmsal sübutun necə əldə edildiyini, hansı proqramla təhlil olunduğunu, hansı alqoritmin tətbiq edildiyini və nəticənin nə dərəcədə etibarlı olduğunu qiymətləndirmək imkanına malik olmaya bilər.

Bu problem "prosedur dəqiqliyi hüququ" konsepsiyası ilə izah olunur. Rəqəmsal sübutların emalı zamanı müdafiə tərəfi yalnız sübutun nəticəsi ilə tanış olmaqla kifayətlənməməli, həm də sübutun əldə olunma, emal və təhlil mərhələlərinə dair zəruri məlumatlara çıxış əldə etməlidir. Bu hüquq üç əsas elementlə əlaqələndirilir:

Birincisi, şəxs etibarsız rəqəmsal sübut emalından müdafiə olunmalıdır. Yəni sübutun texniki baxımdan düzgün əldə edilməsi,

dəyişdirilməməsi və təhlil olunması sənədlərlə təsdiq edilməlidir.

İkincisi, müdafiə tərəfinin sübutun hərəkət zəncirinə, istifadə olunan metodlara və nəticələrin izahına çıxış hüququ olmalıdır.

Üçüncüsü, müdafiə tərəfi rəqəmsal sübutun emalının həlledici mərhələlərində iştirak etmək və ya ən azı həmin mərhələlərin sonradan yoxlanılmasını tələb etmək imkanına malik olmalıdır [23, s.17].

Bu yanaşma rəqəmsal sübutların yalnız texniki obyekt kimi deyil, həm də müdafiə hüquqlarına təsir edən prosessual institut kimi qəbul edilməsini zəruri edir. Əgər müdafiə tərəfi sübutun etibarlılığını yoxlaya bilmirsə, tərəflərin bərabərliyi və sübutları mübahisələndirmək hüququ formal xarakter alır.

"Chain of custody" ("Sübutun hərəkət zənciri") mexanizmi insan hüquqlarının təminatı kimi. Rəqəmsal sübutların etibarlılığını təmin edən əsas mexanizmlərdən biri "chain of custody", yəni sübutun hərəkət zənciridir. Bu anlayış sübutun aşkar edilməsindən məhkəməyə təqdim olunmasına qədər keçdiyi bütün mərhələlərin sənədləşdirilməsini ifadə edir. Sübutu kim əldə etmişdir, harada saxlamışdır, kim ona baxmışdır, hansı dəyişikliklər aparılmışdır, hansı proqramlardan istifadə olunmuşdur - bütün bu sualların cavabı sənədləşdirilməlidir.

Ənənəvi maddi sübutlarda chain of custody daha çox fiziki nəzarət və saxlanma qaydaları ilə bağlıdır. Rəqəmsal sübutlarda isə bu mexanizm daha mürəkkəbdir. Çünki rəqəmsal sübut fiziki daşıyıcıdan ayrıla, kopyalana, təsdiqlənə, bulud mühitində saxlanıla və müxtəlif proqramlar vasitəsilə emal edilə bilər. Buna görə rəqəmsal sübutun bütövlüyünü qorumaq üçün texniki və prosessual tədbirlər birlikdə tətbiq olunmalıdır [19, p.145-146].

Chain of custody və forensic integrity (Sübutun hərəkət zənciri və kriminliastik bütövlük) rəqəmsal sübutların qəbuledilənliyinin əsas şərtlərindən biri kimi çıxış edir. Rəqəmsal sübutlarla bağlı proses müəyyən etmə, qoruma, toplama, araşdırma, təhlil, təqdim etmə və yoxlama mərhələlərindən ibarətdir. Bu mərhələlərdən hər hansı birində sənədləşdirmə aparılmadıqda, sübutun etibarlılığı şübhə altına düşür [5, s.11].

Blockchain əsaslı chain of custody mexanizmi sübutun mənşəyi, davamlılığı və mübahisələndirilə bilməsi baxımından faydalı texniki vasitə ola bilər. Bununla belə, blockchain sübutun məzmununun həqiqiliyini avtomatik sübut etmir; o yalnız müəyyən hadisələrin qeydiyyatını, dəyərlərini, zaman möhürlərini və giriş-çıxış tarixçəsini daha şəffaf və dəyişdirilməsi çətin formada saxlaya bilər [13, s.12].

Bu yanaşma olduqca vacibdir. Çünki hüquqmühafizə orqanları texnologiyaya həddindən artıq etibar etməməlidirlər. Blockchain və ya hər hansı digər texniki sistem sübutun hüquqi qiymətləndirilməsini əvəz etmir. O, yalnız məhkəməyə və müdafiə tərəfinə sübutun necə hərəkət etdiyini yoxlamaq imkanı verən əlavə təminatdır. Bu baxımdan chain of custody insan hüquqlarının müdafiəsi mexanizmi kimi çıxış edir, çünki o, şəxsin əsassız və manipulyasiya olunmuş sübutlarla məhkum edilməsinin qarşısını almağa xidmət edir.

Transsərhəd rəqəmsal sübutlar və yurisdiksiya problemləri. Kibercinayətlərin böyük əksəriyyəti transsərhəd xarakter daşıyır. Cinayəti törədən şəxs bir ölkədə, zərərçəkmiş başqa ölkədə, server üçüncü ölkədə, xidmət provayderi isə dördüncü ölkədə yerləşə bilər. Bu hal rəqəmsal sübutların əldə olunmasını ciddi şəkildə çətinləşdirir.

Rəqəmsal sübutlar cinayət araşdırmalarının əksəriyyətində mühüm rol oynayır və bir çox hallarda belə sübutlar başqa yurisdiksiyalarda yerləşir. Transsərhəd cinayət araşdırmalarında hüquqi çərçivələrin müxtəlifliyi, əməkdaşlıq mexanizmlərinin ləngliyi və texniki mürəkkəblik səbəbindən sübutların vaxtında əldə olunması çətinləşir [6, s. 5-15].

Rəqəmsal kriminalistika (digital forensics – rəqəmsal ekspertiza) kompüter cinayətləri ilə mübarizə vasitəsindən çıxaraq, demək olar ki, bütün cinayət növlərinin araşdırılmasında istifadə olunan müstəqil elmi və praktik fəaliyyət sahəsinə çevrilmişdir [17, s.16].

Bu sahədə əsas beynəlxalq mexanizmlərdən biri Kibercinayətkarlıq haqqında Budapeşt Konvensiyasıdır. Konvensiya kibercinayətlərlə mübarizə və elektron sübutların əldə olunması sahəsində dövlətlərarası əməkdaşlığın hüquqi əsaslarını müəyyən edir. Lakin texnologiyaların inkişafı, bulud xidmətlərinin genişlənməsi və məlumatların müxtəlif ölkələrdə saxlanılması səbəbindən Konvensiyanın ilkin mexanizmləri artıq bütün problemləri həll etmir [9].

Buna görə Budapeşt Konvensiyasına İkinci Əlavə Protokol qəbul edilmiş və elektron sübutların daha çevik əldə olunması üçün yeni əməkdaşlıq mexanizmləri nəzərdə tutulmuşdur [22].

Avropa müstəvisində Avropa İstintaq Əmri, MLAT mexanizmləri, e-Evidence təşəbbüsləri və digər alətlər tətbiq olunur. Bununla belə, MLAT mexanizmləri çox vaxt ləng işləyir, eyni zamanda müxtəlif ölkələrin sübutların qəbuledilənliyi, məlumatların qorunması və insan hüquqları standartları arasında fərqlər qalmaqdadır [8].

Transsərhəd rəqəmsal sübutların əldə olunmasında əsas insan hüquqları problemləri aşağıdakılardır:

• Birincisi, məlumatların hansı ölkənin qanunvericiliyinə əsasən əldə olunması məsələsi həmişə aydın olmur. Bu, şəxsin hansı hüquqi müdafiə vasitələrindən istifadə edə biləcəyini müəyyən etməyi çətinləşdirir.

• İkincisi, bir ölkədə qanuni sayılan istintaq tədbiri başqa ölkədə şəxsi həyatın və ya müdafiə hüququnun pozulması kimi qiymətləndirilə bilər.

• Üçüncüsü, xidmət provayderləri ilə birbaşa əməkdaşlıq bəzən məhkəmə nəzarətindən yayınma riski yaradır.

• Dördüncüsü, müdafiə tərəfi xarici yurisdiksiyada əldə olunmuş sübutun qanuniliyini və etibarlılığını mübahisələndirməkdə ciddi çətinliklərlə üzləşir.

Bu səbəbdən transsərhəd rəqəmsal sübutlarla bağlı beynəlxalq əməkdaşlıq yalnız effektivlik prinsipi əsasında deyil, həm də insan hüquqları, şəffaflıq, mütənasiblik və müdafiə imkanları əsasında qurulmalıdır.

Süni intellekt və rəqəmsal ekspertiza vasitələrinin yaratdığı risklər. Son illərdə süni intellekt və avtomatlaşdırılmış analiz sistemləri cinayət araşdırmalarında daha geniş tətbiq olunur. Üz tanıma, davranış analizi, böyük məlumat bazalarının emalı, əlaqə şəbəkələrinin müəyyən edilməsi və risk proqnozlaşdırılması kimi vasitələr istintaqı sürətləndirsə də, insan hüquqları baxımından yeni risklər yaradır.

Rəqəmsal ekspertiza və süni intellekt sistemləri çox vaxt kifayət qədər tənzimlənmir və onların nəticələri hüquq-mühafizə orqanları tərəfindən avtomatik olaraq etibarlı qəbul edilir. Bu isə müdafiə tərəfinin vəziyyətini çətinləşdirir. Çünki müdafiə tərəfi alqoritmin necə işlədiyini, hansı məlumatlardan istifadə etdiyini, hansı səhv ehtimalının mövcud olduğunu və nəticənin necə formalaşdığını bilməyə bilər [14, s.38-40].

Süni intellektin istifadəsi zamanı əsas risklər aşağıdakılardır:

• alqoritmik qərəz;

• istifadə olunan məlumat bazalarının natamam və ya qeyri-dəqiq olması;

• qərarların izah edilə bilməməsi;

• hüquq-mühafizə orqanlarının texnologiyaya həddindən artıq etibar etməsi;

• müdafiə tərəfinin nəticəni mübahisələndirmək imkanlarının məhdudluğu;

• şəxsi həyat və məlumatların qorunması hüququna geniş müdaxilə.

Bu problemlər xüsusilə üz tanıma sistemlərində özünü göstərir. Glukhin v. Russia işi göstərdi ki, üz tanıma texnologiyalarından hüquqi əsas olmadan və adekvat nəzarət mexanizmləri tətbiq edilmədən istifadə olunması Konvensiyanın 8-ci maddəsinin pozulmasına səbəb ola bilər [22].

Süni intellekt əsaslı sübutların istifadəsi zamanı müdafiə tərəfinə alqoritmin ümumi iş prinsipi, istifadə olunan məlumatların mənbəyi, səhv ehtimalı və tətbiq olunmuş texniki metodlar barədə məlumat verilməlidir. Bu, mənbə kodunun hər zaman tam açıqlanması demək deyil. Lakin ən azı sübutun etibarlılığını yoxlamağa

imkan verən audit izi, metodoloji izah və ekspertiza imkanları təmin edilməlidir.

Blockchain əsaslı sübut idarəetməsi və hüquqi məhdudiyyətlər. Blockchain texnologiyası rəqəmsal sübutların bütövlüyünün təmin olunması üçün perspektivli vasitə kimi təqdim olunur. Bu texnologiya məlumatların dəyişdirilməsinin çətinləşdirilməsi, zaman möhürlərinin yaradılması, sübutun hərəkət tarixçəsinin qeydə alınması və audit imkanlarının artırılması baxımından faydalıdır.

Blockchain əsaslı chain of custody modelində üç əsas element fərqləndirilir: mənşə, davamlılıq və mübahisələndirilə bilmə. Mənşə sübutun haradan və hansı şəraitdə əldə olunduğunu, davamlılıq sübut üzərində aparılan bütün hərəkətlərin qeydiyyatını, mübahisələndirilə bilmə isə müdafiə tərəfinin bu qeydləri yoxlamaq və sorğulamaq imkanını ifadə edir [15].

Bununla belə, blockchain texnologiyasının hüquqi məhdudiyyətləri də vardır. Birincisi, blockchain yalnız qeydə alınmış məlumatın dəyişdirilmədiyini göstərə bilər, lakin həmin məlumatın ilkin olaraq doğru olub-olmadığını sübut etmir. İkincisi, əgər sübut qanunsuz yolla əldə olunubsa, onun blockchain sistemində qeydiyyata alınması bu qanunsuzluğu aradan qaldırmır. Üçüncüsü, sistemin kim tərəfindən idarə edildiyi, giriş hüquqlarının necə verildiyi və məlumatların məxfiliyinin necə qorunduğu hüquqi baxımdan ciddi əhəmiyyət daşıyır.

Bu səbəbdən blockchain sübutların hüquqi qiymətləndirilməsini əvəz edən mexanizm deyil, yalnız sübutun bütövlüyünü və hərəkət tarixçəsini yoxlamağa kömək edən əlavə texniki vasitədir. Məhkəmə yenə də sübutun qanuni yolla əldə olunmasını, işə aidliyini, etibarlılığını və müdafiə tərəfinin onu mübahisələndirmək imkanını qiymətləndirməlidir [13, s.12].

Azərbaycan qanunvericiliyi baxımından əsas problemlər və təkmilləşdirmə istiqamətləri. Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində sübutlar, istintaq hərəkətləri və ekspertiza ilə bağlı ümumi prosessual normalar nəzərdə tutulmuş, elektron məlumatların sübut kimi istifadə olunmasına imkan verən hüquqi mexanizmlər formalaşdırılmışdır [3]. Lakin rəqəmsal sübutların ayrıca anlayışı, onların toplanması, saxlanılması, emalı, ekspertizası və məhkəmədə qiymətləndirilməsi üzrə ətraflı və sistemli mexanizmlərin daha da inkişaf etdirilməsinə ehtiyac vardır.

Bundan əlavə, Azərbaycan Respublikasının "Fərdi məlumatlar haqqında" Qanunu fərdi məlumatların toplanması, emalı və mühafizəsi zamanı şəxsin hüquq və azadlıqlarının qorunmasına yönəlmiş mühüm hüquqi təminatlar müəyyən edir. Rəqəmsal sübutların əldə olunması və istifadəsi prosesində bu təminatların nəzərə alınması şəxsi həyatın toxunulmazlığı hüququnun müdafiəsi baxımından xüsusi əhəmiyyət daşıyır [1].

Eyni zamanda, Azərbaycan Respublikasının "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunu informasiya təhlükəsizliyi, məlumatların mühafizəsi və informasiya münasibətlərinin hüquqi əsaslarını müəyyən edir ki, bu da rəqəmsal sübutlarla bağlı fəaliyyət zamanı hüquqi çərçivənin mühüm elementlərindən biri kimi çıxış edir [2].

Bu sahədə əsas problemləri aşağıdakı kimi qruplaşdırmaq olar:

- Birincisi, rəqəmsal sübut anlayışının qanunvericilikdə ayrıca və dəqiq müəyyən edilməməsi praktikada qeyri-müəyyənlik yaradır. Elektron məlumatların bəzən sənəd, bəzən maddi sübut, bəzən də ekspertiza obyekti kimi qiymətləndirilməsi vahid yanaşmanın formalaşmasını çətinləşdirir.
- İkincisi, rəqəmsal sübutların toplanması zamanı şəxsi həyatın toxunulmazlığı və şəxsi məlumatların qorunması ilə bağlı xüsusi prosessual təminatlar daha aydın şəkildə təsbit edilməlidir. Elektron cihazlara baxış və məlumatların götürülməsi zamanı istintaq orqanlarının səlahiyyətlərinin hüdudları konkret müəyyən olunmalıdır. Şəxsi məlumatların emalı zamanı qanunilik, məqsədlə məhdudluq, məlumatların minimallaşdırılma-

sı və təhlükəsizlik prinsipləri GDPR-də də əsas tələblər kimi nəzərdə tutulmuşdur (20).

• Üçüncüsü, chain of custody mexanizminin qanunvericilikdə və istintaq təcrübəsində sistemli tətbiqi təmin edilməlidir. Sübutun kim tərəfindən, hansı tarixdə, hansı texniki vasitə ilə əldə olunması, necə saxlanılması və hansı dəyişikliklərə məruz qalması sənədləşdirilməlidir.

• Dördüncüsü, rəqəmsal ekspertiza alətlərinin sertifikatlaşdırılması, ekspertlərin ixtisaslaşması və istifadə olunan proqramların etibarlılığının yoxlanılması mexanizmləri gücləndirilməlidir.

• Beşincisi, müdafiə tərəfinin rəqəmsal sübutlara real çıxış imkanı təmin edilməlidir. Müdafiəçi yalnız hazır ekspert rəyi ilə tanış olmamalı, həm də sübutun əldə olunma və emal prosesini yoxlamaq üçün zəruri məlumatlara çıxış əldə etməlidir.

• Altıncısı, transsərhəd elektron sübutların əldə olunması zamanı beynəlxalq əməkdaşlıq mexanizmləri insan hüquqları təminatları ilə birlikdə tətbiq edilməlidir.

Bu istiqamətlərdə aparılacaq islahatlar həm kibercinayətlərlə mübarizənin effektivliyini artırar, həm də cinayət prosesində insan hüquqlarının müdafiəsini gücləndirər.

Kibercinayətlərin ibtidai istintaqı zamanı insan hüquqlarının müdafiəsi müasir cinayət-prosessual hüququn ən aktual məsələlərindən biridir. Rəqəmsal sübutlar cinayətlərin açılması və təqsirkar şəxslərin məsuliyyətə cəlb olunması üçün mühüm vasitə olsa da, onların toplanması və istifadəsi şəxsi həyatın toxunulmazlığı, yazışma sirri, şəxsi məlumatların qorunması, ədalətli məhkəmə araşdırması və müdafiə hüququ ilə sıx bağlıdır.

Nəticə. Aparılan təhlil göstərir ki, rəqəmsal sübutların hüquqi tənzimlənməsi yalnız sübutların texniki baxımdan düzgün əldə olunmasını deyil, həm də onların insan hüquqları baxımından qanuni, şəffaf, mütənasib və mübahisələndirilə bilən olmasını təmin etməlidir. Rəqəmsal sübutun gücü onun məhkəmədə avtomatik qəbul olunması üçün əsas ola bilməz. Əksinə, belə sübutlar yüksək texniki mürəkkəbliyə malik olduğuna görə daha ciddi prosessual nəzarət və müdafiə imkanları tələb edir [16, s. 236].

Bu baxımdan aşağıdakı hüquqi təminatlar xüsusi əhəmiyyət daşıyır:

• rəqəmsal sübutların toplanmasına məhkəmə nəzarətinin təmin edilməsi;

• şəxsi həyata müdaxilənin zərurilik və mütənasiblik prinsipləri əsasında aparılması;

• chain of custody mexanizminin məcburi sənədləşdirilməsi;

• müdafiə tərəfinin sübutun mənşəyi, emal prosesi və ekspertiza nəticələri barədə məlumat almaq hüququ;

• süni intellekt və avtomatlaşdırılmış sistemlərin şəffaf və yoxlanıla bilən istifadəsi;

• transsərhəd sübutların əldə olunmasında beynəlxalq insan hüquqları standartlarına əməl edilməsi; rəqəmsal ekspertiza alətlərinin və metodlarının etibarlılıq baxımından yoxlanılması (18, p.86-87).

Nəticə etibarilə, kibercinayətlərin ibtidai istintaqında insan hüquqlarının müdafiəsi istintaqın effektivliyinə manea kimi deyil, onun legitimliyinin əsas şərti kimi qiymətləndirilməlidir. Hüquqi dövlət şəraitində cinayətkarlıqla mübarizə yalnız nəticəyə yönəlmiş fəaliyyət olmamalı, həm də həmin nəticəyə aparan prosesin hüquqa uyğunluğunu təmin etməlidir. Rəqəmsal dövrdə ədalətli cinayət mühakiməsi məhz bu balansın qorunmasından asılıdır.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT SİYAHISI:

1. Azərbaycan Respublikasının "Fərdi məlumatlar haqqında" Qanunu, 11 may 2010-cu il, № 998-IIIQ.

2. Azərbaycan Respublikasının "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunu, 3 aprel 1998-ci il, № 460-IQ.

3. Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi. Bakı: Hüquq ədəbiyyatı, son nəşr.

4. Benedik v. Slovenia, Application no. 62357/14, European Court of Human Rights, Judgment of 24 April 2018.

5. Bhatti, N. The Use of Digital Evidence in Criminal Proceedings // American Journal of Social Law. 2026. Vol. 5, No. 1. P. 10–19.

6. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., Patsakis, C. SoK: Cross-border Criminal Investigations and Digital Evidence // arXiv:2205.12911. 2022. 24 p.

7. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Burlington: Academic Press, 2011. 838 p.

8. Convention for the Protection of Human Rights and Fundamental Freedoms. Rome, 4 November 1950.

9. Convention on Cybercrime (Budapest Convention). Council of Europe, Budapest, 23 November 2001.

10. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 1981.

11. Glukhin v. Russia, Application no. 11519/20, European Court of Human Rights, Judgment of 4 July 2023.

12. Goodison, S. E., Davis, R. C., Jackson, B. A. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Santa Monica, California: RAND Corporation, 2015. 32 p.

13. Haji, I. A., Mohammed, S. D., Mousa, K. M. Blockchain Based Chain of Custody and Digital Evidence Legality in Post-Conflict Prosecutions // Frontiers in Blockchain. 2026. 16 p.

14. Horsman, G. Digital Evidence: A Review of the Admissibility of the Automated Forensic Tool // Forensic Science International: Digital Investigation. 2019. Vol. 29. P. 36–45.

15. International Covenant on Civil and Political Rights. United Nations, 16 December 1966.

16. Mason, S., Seng, D. Electronic Evidence and Electronic Signatures. London: University of London Press, 2021. 604 p.

17. Pollitt, M. M. History, Historiography and the Hermeneutics of the Hard Drive // Advances in Digital Forensics IX. 2013. P. 3–17.

18. Prysiazhniuk, I. Use of Digital Evidence in Criminal Process: Some Issues of Right to Privacy Protection // Visegrad Journal on Human Rights. 2023. No. 5. P. 81–88.

19. Quick, D., Choo, K. K. R. Digital Forensics and Cloud Storage // Digital Investigation. 2014. Vol. 11, No. 2. P. 140–149.

20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

21. Ruan, K., Carthy, J., Kechadi, T., Baggili, I. Cloud Forensics: An Overview // Advances in Digital Forensics IX. IFIP Advances in Information and Communication Technology. Vol. 410. Berlin, Heidelberg: Springer, 2013. P. 35–46.

22. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. Council of Europe, 2021.

23. Stoykova, R. A. A Governance Model for Digital Evidence in Criminal Proceedings // Computer Law & Security Review. 2024. Vol. 55. Article 106040.

Ибрагимзаде Лала Ильгар гызы,
соискатель ученой степени в Центре судебной экспертизы
Министерства юстиции Азербайджанской Республики,
специализация: «Уголовный процесс; криминалистика и судебная экспертиза;
оперативно-розыскная деятельность»

ПРАВОВЫЕ ГАРАНТИИ ЗАЩИТЫ ПРАВ ЧЕЛОВЕКА ПРИ ПРЕДВАРИТЕЛЬНОМ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

РЕЗЮМЕ

В данной статье рассматриваются правовые гарантии защиты прав человека при предварительном расследовании киберпреступлений. Быстрое развитие информационно-коммуникационных технологий усилило значение цифровых доказательств в уголовном процессе, одновременно создав серьезные риски для неприкосновенности частной жизни, тайны переписки, защиты персональных данных и права на справедливое судебное разбирательство. В статье анализируются понятие и особенности цифровых доказательств, пределы вмешательства в частную жизнь, возможности стороны защиты оспаривать цифровые доказательства, механизм chain of custody, получение трансграничных электронных доказательств, а также использование искусственного интеллекта и блокчейн-ориентированного управления доказательствами. Делается вывод, что правовое регулирование цифровых доказательств должно рассматриваться не только как технический и процессуальный вопрос, но и как важный механизм защиты прав человека и обеспечения легитимности уголовного судопроизводства.

Ibrahimzada Lala Ilgar
Doctoral candidate, Forensic Expertise Center of the
Ministry of Justice of the Republic of Azerbaijan,
“Criminal procedure; criminalistics and forensic expertise;
operational-search activity” specialty

LEGAL GUARANTEES FOR THE PROTECTION OF HUMAN RIGHTS DURING THE PRELIMINARY INVESTIGATION OF CYBERCRIMES

SUMMARY

The article examines the legal guarantees for the protection of human rights during the preliminary investigation of cybercrimes. The rapid development of information and communication technologies has increased the importance of digital evidence in criminal proceedings, while also creating serious risks for privacy, confidentiality of correspondence, personal data protection and the right to a fair trial. The article analyzes the concept and characteristics of digital evidence, the limits of interference with private life, the defense’s ability to challenge digital evidence, the chain of custody mechanism, cross-border access to electronic evidence, and the use of artificial intelligence and blockchain-based evidence management. It is concluded that the legal regulation of digital evidence should be regarded not only as a technical and procedural matter, but also as an essential mechanism for protecting human rights and ensuring the legitimacy of criminal proceedings.

Redaksiyaya daxilolma tarixi: 17.08.2026
Təkrar işlənməyə göndərilmə tarixi: 20.08. 2026
Çapa qəbul olunma tarixi: **23.08.2026**