Kibertəhlükəsizliyin Təmin Edilməsində Cinayət-Hüquqi Vasitələrin Rolu və Rəqəmsal Dayanıqlılığın Qorunması

Kamran Xəlilov
Bakı Dövlət Universiteti, Bakı, Azərbaycan
kamran.khalilov.isa@bsu.edu.az

***Xülasə*— Bu tədqiqat kibertəhlükəsizliyin təmin edilməsində cinayət hüquqi mexanizmlərin rolunu təhlil edir. Rəqəmsal sübutun dəyişdirilə bilən xarakteri, transsərhəd yerləşməsi və texnoloji mürəkkəbliyi istintaq və məhkəmə mərhələsində xüsusi prosessual təminatların tətbiqini zəruri edir. Tədqiqat normativ və doktrinal təhlil əsasında göstərir ki, əməlin yalnız cinayət məsuliyyəti yaradan hüquq pozuntusu kimi müəyyən edilməsi kifayət deyil. Sübutların qanuni qaydada əldə olunması, qorunması və məhkəmədə etibarlı qiymətləndirilməsi hüquqi reaksiyanın effektivliyini müəyyən edən əsas amillərdir. Nəticə etibarilə, rəqəmsal dayanıqlılıq texniki müdafiə tədbirləri ilə yanaşı, hüquqi sabitlik, beynəlxalq əməkdaşlıq və effektiv və balanslı cinayət-prosessual mexanizmlərin tətbiqindən asılıdır.**

Açar sözlər*— *kibertəhlükəsizlik; kibercinayətlər; rəqəmsal sübut; cinayət-prosessual təminatlar; hüquqi dayanıqlılıq.

I. GİRİŞ

Rəqəmsal texnologiyaların ictimai və iqtisadi münasibətlərə dərin inteqrasiyası kibertəhlükəsizliyi yalnız texniki müdafiə anlayışı ilə məhdudlaşdırmağa imkan vermir. İnformasiya sistemlərinə yönəlmiş hücumlar dövlət idarəçiliyinə, maliyyə sektoruna, kritik infrastruktura və şəxsi məlumatların qorunmasına birbaşa təsir göstərir. Bu baxımdan kibertəhlükəsizlik anlayışı təkcə texniki müdafiə məsələsi kimi deyil, həm də hüquqi sabitlik və ictimai təhlükəsizlik kontekstində qiymətləndirilməlidir [1].

Rəqəmsal mühitdə baş verən hüquq pozuntuları klassik cinayət modellərindən fərqli xüsusiyyətlərə malikdir. Hüquqa zidd müdaxilə çox vaxt maddi iz buraxmır, nəticələr isə dərhal aşkar olunmaya bilər. Hücumun təsiri texniki sistemlərlə məhdudlaşmır, hüquqi münasibətlərin sabitliyinə və ictimai etimada birbaşa təsir göstərir. Bu reallıq kibertəhlükəsizliyin yalnız preventiv deyil, eyni zamanda reaksiya mexanizmləri baxımından da təhlilini zəruri edir. Cinayət-hüquqi mexanizmlər kibermühitdə hüquqi müdaxilənin əsas formalarından biridir. Lakin onların rolu yalnız hüquq pozuntusunun sanksiyalaşdırılması ilə məhdudlaşmır. Hüquqi sistemin operativ reaksiya qabiliyyəti, hüquqi müəyyənlik səviyyəsi və ədalətli proses təminatları rəqəmsal mühitdə dayanıqlılığın formalaşmasına birbaşa təsir göstərir. Əgər hüquqi mexanizm gecikmiş, qeyri-müəyyən və ya formal xarakter daşıyırsa, texniki müdafiə tədbirləri uzunmüddətli təhlükəsizliyi təmin edə bilməyəcəkdir.

Rəqəmsal dayanıqlılıq anlayışı bu baxımdan kompleks xarakter daşıyır. O, sistemin yalnız texniki bərpa imkanını deyil, hüquqi reaksiyanın legitimliyini, proporsionallığını və tətbiq qabiliyyətini də ehtiva edir. Hüquqi sabitlik olmadan rəqəmsal mühitdə davamlı təhlükəsizlik mümkün deyildir. Bu isə kibertəhlükəsizlik və cinayət-hüquqi mexanizmlər arasında funksional əlaqənin sistemli şəkildə araşdırılmasını zəruri edir.

Tədqiqatın məqsədi kibertəhlükəsizliyin təmin edilməsində cinayət-hüquqi vasitələrin struktur rolunu müəyyən etmək və rəqəmsal dayanıqlılıq konsepsiyasını hüquqi müstəvidə əsaslandırmaqdır. Bu məqsədlə normativ yanaşma, doktrinal təhlil və müqayisəli hüquqi baxış metodlarından istifadə olunur. Araşdırma kibertəhlükəsizliyi yalnız texniki müdafiə kateqoriyası kimi deyil, hüquqi təhlükəsizlik fenomeni kimi qiymətləndirir və cinayət-hüquqi mexanizmlərin bu sistemdə tutduğu yeri konseptual çərçivədə müəyyənləşdirir.

II. KİBERTƏHLÜKƏSİZLİYİN CİNAYƏT-HÜQUQİ ÇƏRÇİVƏSİ VƏ NORMATİV UYĞUNLUQ

Kibertəhlükəsizliyin hüquqi təminatı ilk növbədə cinayət tərkiblərinin düzgün təsnifatının müəyyən edilməsi ilə başlayır. Dövlət informasiya sistemlərinə qanunsuz müdaxilə, məlumatların dəyişdirilməsi və sistemlərin fəaliyyətinin pozulması kimi əməlləri cinayət kimi tanımaqla müdafiə mexanizmini formalaşdırır. Azərbaycan Respublikasının Cinayət Məcəlləsində informasiya sistemlərinə və kompüter məlumatlarına qarşı yönəlmiş əməllər ayrıca maddələrdə nəzərdə tutulmuşdur [2]. Bu normativ baza kibermühitdə hüquqi müdaxilənin əsasını təşkil edir. Bununla yanaşı, normanın mövcudluğu onun effektiv tətbiqini avtomatik təmin etmir. Kibercinayətlər çox vaxt transsərhəd xarakter daşıyır və bir hadisə bir neçə yurisdiksiyanı əhatə edə bilir. Bu vəziyyət cinayət tərkibinin müəyyən edilməsi və sübutların toplanılması prosesində əlavə çətinlik yaradır. Buna görə də, "Kibercinayətkarlıq haqqında" Budapeşt Konvensiyası (2001) məhz bu reallığı nəzərə alaraq kriminalizasiya ilə yanaşı, beynəlxalq əməkdaşlıq mexanizmlərini də hüquqi sistemin ayrılmaz elementi kimi müəyyən etmişdir [3].

Avropa İttifaqında informasiya sistemlərinə hücumlarla bağlı minimal cinayət-hüquqi standartların müəyyən edilməsi və elektron sübutlara çıxış üzrə yeni hüquqi mexanizmlərin qəbul edilməsi göstərir ki, normativ çərçivə yalnız cinayət tərkiblərinin təsviri ilə məhdudlaşmamalıdır [4,5]. Hüquqi sistem rəqəmsal məlumatın sürətli ötürülməsi və saxlanma

DOI: 10.25045/cyber.gov.2026.39

modellərinə uyğunlaşmalı, sübutların operativ qorunması üçün prosedur alətlər təqdim etməlidir. Bu baxımdan normativ aydınlıq yalnız maddi hüquq səviyyəsində deyil, prosessual mexanizmlərlə birlikdə qiymətləndirilməlidir.

Doktrinal ədəbiyyatda da qeyd olunur ki, kibercinayətlərin effektiv qarşısının alınması cinayət-hüquqi mexanizmlərin çəkindirici təsiri ilə sıx bağlıdır [1,6]. Əgər hüquqi sistem real tətbiq qabiliyyətinə malik deyilsə və cinayət təqibi nəticəsiz qalırsa, normativ çərçivə formal xarakter daşımağa başlayır. Bu isə rəqəmsal mühitdə hüquqi risklərin artmasına səbəb olur. Kibertəhlükəsizliyin cinayət-hüquqi çərçivəsi yalnız kriminalizasiya ilə məhdudlaşmır. Normativ yetərlilik maddi hüquq normalarının mövcudluğu, beynəlxalq uyğunluq və praktik tətbiq imkanları ilə birlikdə qiymətləndirilməlidir. Rəqəmsal mühitdə dayanıqlılığın hüquqi təminatı bu elementlərin qarşılıqlı əlaqəsi ilə formalaşır.

A. İbtidai istintaq mərhələsində rəqəmsal sübutun prosessual təminatları və hüquqi risklər

Kibercinayətlərin istintaqında əsas sübut mənbəyi rəqəmsal məlumatlardır. Elektron yazışmalar, server qeydləri, istifadəçi fəaliyyətinə dair log məlumatları və digər rəqəmsal izlər cinayət işində faktiki halların müəyyən edilməsinə xidmət edir. Lakin, bu sübutların hüquqi qiymətləndirilməsi klassik maddi sübut modelindən fərqlənir və xüsusi metodoloji yanaşma tələb edir [6]. Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsinin 124-cü maddəsinə əsasən sübut cinayət işi üzrə əhəmiyyət kəsb edən halları müəyyən edən məlumatlardır. Həmin Məcəllənin 125-ci maddəsi isə sübutun qəbuledilənliyini onun qanuni yolla əldə olunması ilə əlaqələndirir [7]. Bu iki norma rəqəmsal sübutlara da tam şəkildə şamil olunur. Lakin praktikada əsas çətinlik məhz burada yaranır. Belə ki, rəqəmsal sübutun “məlumat” kimi mövcudluğu ilə onun “prosessual sübut” kimi tanınması eyni şey deyildir.

Rəqəmsal sübutun birinci xüsusiyyəti onun dəyişdirilə bilən xarakter daşımasıdır. Elektron məlumatlar fiziki izlərdən fərqli olaraq asanlıqla silinə, köçürülə və dəyişdirilə bilər. Bu səbəbdən sübutun bütövlüyünün qorunması məsələsi xüsusi əhəmiyyət kəsb edir. Elmi ədəbiyyatda da vurğulanır ki, rəqəmsal sübutun toplanması və saxlanması mərhələləri sənədləşdirilmiş və ardıcıl qaydada aparılmalıdır [8]. Hüquqi baxımdan burada əsas məsələ texniki mexanizmin necə işləməsi deyil, sübutun əldə olunması və saxlanması prosesinin sənədləşdirilməsidir. Əgər istintaq materiallarında sübutun kim tərəfindən, nə vaxt və hansı qaydada götürüldüyü aydın göstərilmirsə, sonradan onun dəyişdirilmədiyini əsaslandırmaq çətinləşir. Bu baxımdan prosessual qaydalara riayət olunması yalnız formal tələb deyil, sübutun qiymətləndirilməsində müsbət qərarların qəbulu üçün əsas şərtdir [6].

İkinci mühüm xüsusiyyət sübutun əldə olunma üsuludur. Elektron daşıyıcının axtarışı və götürülməsi zamanı qanunda nəzərdə tutulan prosedur tələblərinə riayət olunmalıdır. Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi axtarış, götürmə və digər istintaq hərəkətlərinin qanuni qaydada, yəni məhkəmə qərarı əsasında aparılmasını tələb edir [7]. Bununla belə, rəqəmsal sübutların itirilməsinin və ya dəyişdirilməsinin qarşısını almaq üçün milli qanunvericilikdə rəqəmsal məlumatların operativ qorunması mexanizmi nəzərdə tutulmalıdır. Budapeşt Konvensiyasının 16-cı maddəsinə uyğun olaraq, müstəntiq məhkəmə qərarı alınanadək təxirəsalınmaz hallarda provayderə məlumatların silinməməsi və dəyişdirilməməsi barədə təcili göstəriş verə bilməlidir [3]. Bu tədbir qısa müddət üçün tətbiq edilməli və sonradan məhkəmə nəzarəti ilə təsdiqlənməlidir. Belə mexanizm xüsusilə transsərhəd işlərdə sübutların qorunmasına xidmət edə bilər. Həmçinin elektron məlumat daşıyıcılarının götürülməsi zamanı müdaxilənin həcmi konkret cinayət işi ilə əlaqəli məlumatların həddində, daha dəqiq desək, irəli sürülmüş və ya sürüləcək ittihamın həddində məhdudlaşdırılmalıdır. Əks halda şəxsi həyatın toxunulmazlığı və məlumatların qorunması prinsipləri pozula bilər. İnsan hüquqları üzrə məhkəmə təcrübəsində müdaxilənin proporsionallığı ədalətli məhkəmə hüququnun tərkib hissəsi kimi qiymətləndirilmişdir [9].

Üçüncü xüsusiyyət kimi, rəqəmsal sübutun sənədləşdirilməsi istintaq mərhələsində xüsusi əhəmiyyət daşıyır. Sübutun əldə olunma şəraiti, vaxtı və texniki proseduru dəqiq göstərilmədikdə onun bütövlüyünün qorunması barədə şübhə yarana bilər. Beynəlxalq metodoloji sənədlər və forensika üzrə tədqiqatlar sübutun ardıcıl və izlənəbilən prosedurla qorunmasının zəruriliyini vurğulayır [8,10]. Xüsusilə bulud mühitində saxlanılan məlumatların əldə edilməsi zamanı mənşənin və dəyişməzliyin əsaslandırılması daha mürəkkəb xarakter daşıyır [11].

İbtidai istintaq mərhələsində digər mühüm məsələ sübuta çıxış və onu mübahisələndirmək imkanıdır. İstintaq orqanları ixtisaslaşmış texniki imkanlara malik olduğu halda müdafiə tərəfi eyni səviyyədə texniki resurslara sahib olmaya bilər. Bu baxımdan müdafiə tərəfi də rəqəmsal sübutun əldə olunma və analiz metodologiyasını yoxlamaq hüququna malik olmalıdır. Bu vəziyyət sübutun yoxlanılması və ekspertiza nəticələrinin qiymətləndirilməsi prosesində balansın pozulmasına səbəb ola bilər [12]. Əgər müdafiə tərəfi sübutun necə əldə edildiyini və hansı şərtlərdə saxlanıldığını araşdıra bilmirsə, bu zaman “silahların bərabərliyi” (equality of arms) prinsipi formal xarakter daşıya bilər [13]. Buna görə də, ədalətli məhkəmə prinsipinin reallaşması müdafiə tərəfinin sübutla tanış olmaq və onu mübahisələndirmək imkanının real şəkildə təmin edilməsini tələb edir.

Bundan başqa, rəqəmsal sübutun mənşəyinin müəyyən edilməsi ayrıca diqqət tələb edir. Rəqəmsal mühitdə istifadəçi hesabları, IP ünvanlar və digər identifikasiya vasitələri həmişə birbaşa şəxsi göstərmir. Bu səbəbdən həmin izlə konkret şəxsin hərəkəti arasında səbəbli əlaqəni əsaslandırmalıdır. Əks halda sübut yalnız ehtimal xarakterli qalır və təqsirin sübuta yetirilməsi üçün yetərli olmaya bilər.

Digər tərəfdən, müasir dövrdə “deepfake” və digər manipulyasiya üsulları da sübutların qiymətləndirilməsini çətinləşdirir. Audio və video materialın dəyişdirilməsi artıq texniki baxımdan mümkündür və bu risk hüquqi müstəvidə də müzakirə olunur [14]. Lakin, burada yenə də əsas məsələ texnologiyanın özü deyil, sübutun mənbəyinin və bütövlüyünün prosessual şəkildə təsdiqlənməsidir. Məhkəmə rəqəmsal sübutu qiymətləndirərkən onun əldə olunma qaydasını, saxlanma ardıcıllığını və dəyişdirilmədiyini təsdiqləyən prosessual sənədləşməni nəzərə almalıdır. Xüsusilə

sübutun əldə edilməsindən məhkəməyə təqdim olunmasına qədər olan mərhələdə bütövlüyün qorunması və müdaxilə risklərinin aradan qaldırılması hüquqi qiymətləndirmənin əsas meyarlarından biridir [13].

Transsərhəd element istintaq mərhələsində əlavə çətinlik yaradır və məlumatların xarici platformalardan əldə olunması milli prosedur qaydalarının beynəlxalq əməkdaşlıq mexanizmləri ilə uzlaşdırılmasını tələb edir [15]. Məlumat xarici serverlərdə saxlanıldıqda beynəlxalq hüquqi yardım prosedurlarına riayət olunması zəruridir. Elektron sübutlara çıxış üzrə beynəlxalq mexanizmlərin yenilənməsi bu sahədə hüquqi koordinasiyanın əhəmiyyətini artırmışdır [16]. Prosedur qaydalarının pozulması nəticəsində əldə edilmiş məlumatın məhkəmədə istifadəsi sual altına düşə bilər.

Beləliklə, rəqəmsal sübutun hüquqi xüsusiyyətləri göstərir ki, kibercinayətlərin istintaqında əsas məsələ texniki imkan deyil, prosessual dəqiqlikdir. Sübutun hüquqi dəyəri onun məzmunu ilə yanaşı, qanunauyğun əldə olunması, sənədləşdirilməsi və etibarlılığının əsaslandırılması ilə müəyyən edilir. Bu səbəbdən ibtidai istintaq mərhələsində prosessual təminatlar həlledici əhəmiyyət daşıyır və qanuni əldə olunma, proporsionallıq və müdafiə hüququnun təmin edilməməsi rəqəmsal sübutun məhkəmədə dayanıqlılığını zəiflədə bilər.

B. Məhkəmə baxışında rəqəmsal sübutların qiymətləndirilməsi

İbtidai istintaq mərhələsində toplanmış rəqəmsal sübutlar məhkəmə baxışında qiymətləndirilir. Bu mərhələdə əsas məsələ sübutun mövcudluğu deyil, onun qanunauyğun əldə olunması və etibarlılığıdır. Məhkəmə sübutun iş üzrə halların müəyyən edilməsinə nə dərəcədə təsir etdiyini nəzərə alaraq daxili inam formalaşdırır. Cinayət-Prosessual Məcəlləsinin 145-ci maddəsinə əsasən hər bir sübut mənsubiyyəti, mümkünlüyü, mötəbərliyi üzrə qiymətləndirilməlidir. Cinayət təqibi üzrə toplanmış bütün sübutların məcmusuna isə ittihamın həlli üçün onların kifayət etməsinə əsasən qiymət verilməlidir. Həmçinin sübutlar məhkəmə tərəfindən daxili inam əsasında qiymətləndirilir [7]. Daxili inam subyektiv fikir deyil. O, iş üzrə bütün sübutların hərtərəfli və obyektiv araşdırılmasına əsaslanmalıdır. Rəqəmsal sübutlarda bu xüsusilə vacibdir, çünki elektron məlumat dəyişdirilə və ya manipulyasiya oluna bilər [17].

Doktrinal baxımdan rəqəmsal mühitdə sübutun hüquqi qiymətləndirilməsi ilkin mərhələdə iki əsas meyar üzrə həyata keçirilməlidir: Sübutun qəbuledilən və etibarlı olması. Qəbuledilənlik sübutun qanuni üsulla əldə olunmasına aiddir. Bu meyarın pozuntusu sübutun hüquqi qüvvəsini tamamilə aradan qaldıra bilər. Etibarlılıq isə onun həqiqiliyinə, dəyişdirilmədiyinə və texniki manipulyasiyaya məruz qalmadığına dair əsaslandırılmış qənaətin mövcudluğunu ifadə edir. Bu meyarın pozulması isə sübutun indandırıcılığı ilə əlaqədar məhkəmənin daxili inamına təsir edə və son nəticədə gözlənilən hüquqi nəticə doğurmaya bilər [18]. Avropa İnsan Hüquqları Məhkəməsinin təcrübəsində də sübutun əldə olunma üsulu ədalətli məhkəmə hüququnun qiymətləndirilməsində mühüm amil kimi nəzərə alınmışdır. Bu yanaşma rəqəmsal sübutlara da şamil olunur [9].

Məhkəmə təcrübəsi də göstərir ki, rəqəmsal sübutların qəbul olunması və qiymətləndirilməsi zamanı məhkəmələr texniki əsaslandırmanı və prosedur qanuniliyini paralel şəkildə nəzərə alırlar. ABŞ məhkəməsinin Gates Rubber Company v. Bando Chemical Industries işində elektron məlumatların sübut kimi qəbul edilməsində ekspert izahlarının və texniki metodların hüquqi əsaslandırılmasının vacibliyi vurğulanmışdır [19]. Böyük Britaniya Ali Məhkəməsinin R v. Elliott and McKee qərarında isə elektron cihazdan əldə edilmiş məlumatların avtomatik olaraq etibarsız hesab edilməməsi, lakin onların düzgün hüquqi prosedur çərçivəsində təqdim edilməsinin zəruriliyi qeyd edilmişdir [20].

Avropa İnsan Hüquqları Məhkəməsinin təcrübəsində də sübutun əldə olunma üsulu ədalətli məhkəmə hüququnun qiymətləndirilməsində mühüm amil kimi qəbul edilir. Məhkəmə qeyd edir ki, sübutun qanunsuz əldə olunması avtomatik olaraq Konvensiyanın 6-cı maddəsinin pozuntusu demək deyil, lakin ümumi prosesin ədalətliliyi qiymətləndirilərkən bu hal nəzərə alınmalıdır [21]. Bu yanaşma rəqəmsal sübutlara da şamil olunur və sübutun əldə olunma üsulu ilə onun məhkəmədə istifadəsi arasında balansın qorunmasını tələb edir.

Bununla da, aydın olur ki, məhkəmə baxışında rəqəmsal sübutların qiymətləndirilməsi zamanı sübutun qanunauyğun əldə olunması, metodoloji şəffaflıq və müdafiə hüququnun real təminatı olmadan rəqəmsal sübutun inandırıcılığı zəifləyə bilər. Bu isə cinayət-hüquqi reaksiyanın effektivliyinə birbaşa təsir göstərir.

III. RƏQƏMSAL DAYANIQLILIĞIN HÜQUQİ MODELİ VƏ İNKİŞAF İSTİQAMƏTLƏRİ

Rəqəmsal mühitdə dayanıqlılıq anlayışı cinayət-hüquqi mexanizmlərin effektiv işləməsi ilə sıx bağlıdır. Hücum baş verdikdən sonra hüquqi sistem sürətli və qanunauyğun reaksiya verm ədikdə texniki müdafiə tədbirləri öz preventiv təsirini itirir [8]. Bu baxımdan rəqəmsal dayanıqlılıq üçün vahid hüquqi model üç əsas struktur elementi üzərində qurulmalıdır: normativ müəyyənlik, prosessual sabitlik və institusional legitimlik.

A. Normativ müəyyənlik

Kibercinayətlərin kriminalizasiyası hüquqi müdafiənin ilkin şərtidir. Lakin yalnız cinayət tərkiblərinin mövcudluğu rəqəmsal dayanıqlılığı təmin etmir. Hüquqi norma tətbiq edilə bilən, aydın və texnoloji dəyişikliklərə uyğunlaşa bilən olmalıdır. Normanın qeyri-müəyyənliyi və ya fərqli interpretasiyası hüquqi sabitliyi zəiflədir və praktik tətbiqi çətinləşdirir. Rəqəmsal mühitdə cinayət tərkiblərinin texnoloji neytrallıq prinsipi əsasında formalaşdırılması hüquqi sistemin uzunmüddətli dayanıqlılığı üçün vacibdir. Əks halda hər yeni texnoloji inkişaf normativ boşluq yarada bilər və hüquqi reaksiya gecikə bilər.

B. Prosessual sabitlik

Rəqəmsal dayanıqlılığın əsasını təşkil edən ikinci element prosessual mexanizmlərin sabitliyidir. Hüquqi sistem yalnız cinayət faktını müəyyən etməklə kifayətlənməməli, sübutun operativ qorunması, əldə olunması və məhkəmə baxışında

etibarlı qiymətləndirilməsi üçün sabit mexanizm yaratmalıdır. Bu baxımdan prosessual sabitlik bir neçə alt-komponentdən ibarətdir: rəqəmsal sübutun qanuni və operativ qorunması mexanizmləri; istintaq hərəkətlərinin məhkəmə nəzarəti ilə həyata keçirilməsi; sübutun əldə olunma və saxlanma mərhələlərinin izlənəbilən formada sənədləşdirilməsi; müdafiə və ittiham tərəfləri arasında real prosessual balansın təmin edilməsi. Əgər sübutun əldə olunması mərhələsində pozuntu baş verirsə və ya müdafiə tərəfi sübutun analiz metodologiyasını yoxlamaq imkanından məhrumdursa, bu halda hüquqi model formal xarakter alır. Prosessual mexanizmlərin sabitliyi məhz sübutun məhkəmə mərhələsində hüquqi sınaqdan keçə bilmə qabiliyyəti ilə ölçülür.

C. İnstitusional legitimlik

Hüquqi modelin üçüncü elementi institusional bacarıq və legitimlikdir. Rəqəmsal sübutların effektiv toplanması və qiymətləndirilməsi yalnız normativ mexanizmlərlə deyil, həm də ixtisaslaşmış kadr potensialı və metodoloji standartların tətbiqi ilə mümkündür. Əgər hüquqi mexanizm insan hüquqlarının tələbləri ilə uzlaşmırsa, xüsusilə şəxsi həyatın toxunulmazlığı və müdafiə hüququ lazımi səviyyədə təmin olunmursa, hüquqi reaksiya legitimliyini itirir. Hüquqi legitimliyin zəifləməsi isə preventiv təsirin azalmasına və kibermühitdə etimadın sarsılmasına səbəb olur. Bu səbəbdən rəqəmsal dayanıqlılıq yalnız cəza mexanizminin sərtliyi ilə deyil, hüquqi müdaxilənin proporsionallığı və ədalətliliyi ilə ölçülməlidir. Hüquqi sistem nə qədər sürətli reaksiya verirsə-versin, əgər bu reaksiya insan hüquqları ilə üst-üstə düşmürsə, uzunmüddətli dayanıqlılıq təmin edilə bilməz.

Bununla da rəqəmsal dayanıqlılığın hüquqi modeli normativ müəyyənlik, prosessual sabitlik və institusional bacarıq üzərində qurulur. Texniki müdafiə və cinayət-hüquqi reaksiya bir-birini tamamlayan elementlər kimi çıxış edir. Rəqəmsal mühitdə uzunmüddətli təhlükəsizlik yalnız bu mexanizmlərin qarşılıqlı və balanslı fəaliyyəti ilə mümkün olur.

NƏTİCƏ

Rəqəmsal mühitdə təhlükəsizlik anlayışı hüquqi mexanizmlərin effektivliyi ilə bilavasitə əlaqəlidir. Tədqiqat nəticəsində müəyyən edilmişdir ki, kibercinayətlərə qarşı mübarizədə həlledici amil yalnız kriminalizasiya deyil, hüquqi reaksiyanın sistemli və tətbiq edilə bilən mexanizmə çevrilməsidir. Xüsusilə rəqəmsal sübutun dəyişdirilə bilməsi, uzaq serverlərdə saxlanılması və texniki mürəkkəbliyi sübut mexanizmlərinin klassik modeldən fərqli şəkildə qurulmasını tələb edir. Araşdırma göstərir ki, rəqəmsal dayanıqlılıq normativ müəyyənlik, prosessual sabitlik və institusional legitimliyin qarşılıqlı təsiri nəticəsində formalaşır. Hüquqi çərçivə aydın olmadıqda tətbiq qeyri-müəyyənləşir. Prosessual mexanizmlər sabit işləmədikdə sübutun hüquqi dəyəri zəifləyir. İnstitusional imkanlar yetərli olmadıqda isə normativ mexanizm formal xarakter daşıyır. Bu elementlərin hər biri rəqəmsal mühitdə hüquqi sabitliyin təmin olunmasında müstəqil, lakin bir-biri ilə əlaqəli rol oynayır.

Beləliklə, rəqəmsal dayanıqlılıq texniki davamlılıq anlayışından daha geniş məna daşıyır və hüquqi sistemin adaptivliyi, balanslı müdaxiləsi və sübut mexanizmlərinin işləkliyi ilə müəyyən olunur. Cinayət-hüquqi mexanizmlər bu kontekstdə təhlükəsizliyin təmin edilməsində əsas hüquqi dayaqlardan biri kimi çıxış edir.

ƏDƏBİYYAT

[1] D. S. Wall, Cybercrime: The transformation of crime in the information age. Cambridge, U.K.: Polity Press, 2007.

[2] Azərbaycan Respublikasının Cinayət Məcəlləsi, 30 dekabr 1999. Council of Europe, Convention on cybercrime. Budapest, Hungary, Nov. 23, 2001.

[3] European Parliament and Council of the European Union, Directive 2013/40/EU on attacks against information systems, Aug. 12, 2013.

[4] European Parliament and Council of the European Union, Regulation (EU) 2023/1543 on European production orders and European preservation orders for electronic evidence in criminal proceedings, Jul. 12, 2023.

[5] E. Casey, Digital evidence and computer crime: Forensic science, computers, and the internet, 3rd ed. London, U.K.: Academic Press, 2011.

[6] Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi, 14 iyul 2000.

[7] ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2012.

[8] European Court of Human Rights, Bykov v. Russia, Application no. 4378/02, Grand Chamber judgment, Mar. 10, 2009.

[9] A. W. Malik et al., “Cloud digital forensics: Beyond tools, techniques, and challenges,” Sensors, vol. 24, no. 2, Art. no. 433, 2024, doi: 10.3390/s24020433

[10] O. I. Abiodun et al., “Data provenance for cloud forensic investigations: Security and privacy issues,” Journal of King Saud University – Computer and Information Sciences, vol. 34, no. 10, 2022.

[11] K. Kent, S. Chevalier, T. Grance, and H. Dang, Guide to integrating forensic techniques into incident response, NIST Special Publication 800-86, Gaithersburg, MD, USA, 2006.

[12] R. Stoykova, “The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations,” Computer Law & Security Review, vol. 49, Art. no. 105801, 2023, doi: 10.1016/j.clsr.2023.105801

[13] R. Chesney and D. Citron, “Deepfakes and the new disinformation war,” Foreign Affairs, vol. 98, no. 1, pp. 147–155, 2019.

[14] S. Carrera, M. Stefan, and V. Mitsilegas, Cross-border data access in criminal proceedings and the future of digital justice. Brussels, Belgium: CEPS, 2020.

[15] A. Sachoulidou, “Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift,” European Journal of Criminology, 2024, doi: 10.1177/20322844241258649

[16] B. Carrier and E. H. Spafford, “Getting physical with the digital investigation process,” International Journal of Digital Evidence, vol. 2, no. 2, pp. 1–20, 2003.

[17] A. Ashworth and M. Redmayne, The criminal process. 4th ed. Oxford, U.K.: Oxford University Press, 2010.

[18] Gates Rubber Co. v. Bando Chemical Industries, Ltd., 167 F.R.D. 90 (D. Colo. 1996).

[19] R v. Elliott and McKee [2013] EWCA Crim 144.

[20] European Court of Human Rights, Schenk v. Switzerland, Application. No. 10862/84, Judgment of 12 July 1988.

The Role of Criminal Law Mechanisms in Ensuring Cybersecurity and Protecting Digital Resilience

Kamran Khalilov

Baku State University, Baku, Azerbaijan

Abstract— This study examines the role of criminal law mechanisms in ensuring cybersecurity. The mutable nature, cross-border location, and technological complexity of digital evidence require specific procedural safeguards at both the investigation and trial stages. Based on normative and doctrinal analysis, the study demonstrates that defining conduct merely as a criminal offense is not sufficient. The lawful collection, preservation, and reliable judicial evaluation of evidence are decisive factors in determining the effectiveness of legal response. Consequently, digital resilience depends not only on technical protective measures but also on legal stability, international cooperation, and the effective and balanced application of criminal procedural mechanisms.

Keywords— cybersecurity; cybercrime; digital evidence; criminal procedural safeguards; legal resilience.