Elektron Sübutların Cinayət Prosesində Hüquqi Statusu və Kiberhücumların İstintaqında Tətbiqi

Əli Təhməzov
Dövlət Təhlükəsizliyi Xidməti, Bakı, Azərbaycan
ali.tahmazov@dtx.gov.az

***Xülasə*— Məqalədə Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsinə 2026-cı ildə edilmiş dəyişikliklər fonunda elektron sübutların hüquqi statusu, onların növləri, əldə olunması və məhkəmədə istifadəsinin əsas şərtləri təhlil olunur. Xüsusilə Cinayət-Prosessual Məcəllənin 124.2.3-1-ci maddəsi ilə elektron formada sübutların ayrıca sübut növü kimi təsbit edilməsi, 133-1–133-3-cü maddələrdə elektron verilənlər, onların sübut kimi qəbul olunması və mühafizəsi ilə bağlı yeni yanaşmalar araşdırılır. Məqalədə həmçinin kiberhücumların istintaqından götürülmüş praktik nümunələr əsasında gecikmə, loq-faylların silinməsi, transsərhəd əməkdaşlıq və sübutların saxlanma-ötürülmə zəncirinin qorunması kimi problemlər göstərilir.**

Açar sözlər*— *elektron sübut; kiberhücum; elektron verilənlər; cinayət prosesi; istintaq; məhkəmə.

I. GİRİŞ

Rəqəmsallaşmanın sürətlənməsi, dövlət və özəl sektorda informasiya-kommunikasiya texnologiyalarından (İKT) geniş istifadə, eləcə də kibercinayətlərin xarakterinin mürəkkəbləşməsi cinayət prosesində elektron sübutların rolunu əhəmiyyətli dərəcədə artırmışdır. Klassik sübut mənbələri ilə müqayisədə elektron verilənlər sürətlə dəyişə, silinə, uzaqdan ötürülə və müxtəlif serverlərdə, daşıyıcılarda və bulud mühitlərində saxlanıla bilər. Bu isə həm onların hüquqi statusunun dəqiq müəyyən edilməsini, həm də əldə olunması və qorunması prosedurlarının ayrıca tənzimlənməsini zəruri edir.

Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsinə 2026-cı ildə edilmiş dəyişikliklər [1] bu sahədə prinsipial dönüş yaratmışdır. Əgər əvvəlki mərhələdə rəqəmsal mühitdən əldə olunan məlumatlar daha çox sənəd və ya maddi sübut kontekstində qiymətləndirilirdisə, hazırda qanunvericilik səviyyəsində elektron sübutları müstəqil sübut növü kimi təsbit etmişdir. Məcəllənin 124.2.3-1-ci maddəsində "elektron formada sübutlar" ifadəsinin ayrıca göstərilməsi bu baxımdan sistemli yanaşmanın başlanğıcı hesab edilə bilər [2].

Qanunvericilik yeniliyi yalnız termin əlavə etməklə məhdudlaşmır. Məcəllədə "İKT sistemi", "elektron verilənlər", "trafik verilənləri", "abunəçi məlumatları" və "məzmun verilənləri" kimi anlayışların müəyyənləşdirilməsi [3, 4] istintaq orqanları üçün həm predmet dairəsini, həm də əldə etmə obyektini daha aydın göstərir. Xüsusilə 133-1-ci maddədə elektron verilənlərin cinayət təqibi üçün əhəmiyyət kəsb edən halların müəyyən edilməsinə kömək etdiyi təqdirdə elektron formada sübut hesab edilə bilməsi, 133-1.2-ci maddədə isə onların prosessual qanunvericiliyin tələblərinə riayət edilməklə əldə edildikdə sübut kimi qəbul olunması [3] mühüm normativ əsas yaradır.

II. ELEKTRON SÜBUTLARIN QANUNİLİK ŞƏRTLƏRİ

Elektron sübutların praktiki əhəmiyyəti onların çoxsaylı mənbələrdən əldə edilə bilməsində özünü göstərir. Bunlara İKT sistemlərində saxlanılan fayllar, loq faylları, IP ünvanlarla bağlı məlumatlar, trafik verilənləri, abunəçi məlumatları, elektron yazışmalar, mobil cihazlardan çıxarılan verilənlər, server və şəbəkə qeydləri daxildir. Lakin bu məlumatların mövcudluğu öz-özlüyündə onların sübut kimi yararlılığını təmin etmir. Sübutun qanuni əsasla əldə olunması, orijinallığının qorunması, bütövlüyünün pozulmaması və saxlanma-ötürülmə zəncirinin sənədləşdirilməsi əsas şərtlər kimi çıxış edir.

Bu baxımdan elektron sübutların toplanması mərhələsində ilk tələb qanuni əsasın mövcudluğudur. Məhkəmə qərarı, istintaq hərəkəti haqqında qərar və ya qanunda nəzərdə tutulan digər prosessual əsas olmadan əldə edilən məlumatların sonradan məhkəmədə mübahisələndirilməsi ehtimalı yüksəkdir. İkinci mühüm tələb sübutun bütövlüyünün qorunmasıdır. Elektron faylların heş qiymətlərinin hesablanması, nüsxələrin çıxarılması zamanı texniki müdaxilənin minimuma endirilməsi və orijinal daşıyıcıya toxunulmaması bu tələbə xidmət edir.

Üçüncü istiqamət sübutun saxlanma və ötürülmə zənciridir. Praktikada elektron sübutların kim tərəfindən aşkar edildiyi, kim tərəfindən götürüldüyü, hansı daşıyıcıda saxlanıldığı, nə vaxt ekspertizaya təqdim olunduğu, hansı qərarla və kimin vasitəsilə ötürüldüyü ayrıca qeydə alınmalıdır. Bu zəncirin hər hansı mərhələsində qeyri-müəyyənlik yarandıqda müdafiə tərəfində sübutun etibarlılığına şübhə doğura bilər. Buna görə də elektron sübutlar üzrə texniki aktlar, baxış protokolları, qablaşdırma və möhürləmə prosesi, daşıyıcıların identifikasiyası xüsusi əhəmiyyət daşıyır.

III. ELEKTRON SÜBUTLARIN PRAKTİKİ ƏHƏMİYYƏTİ

Elektron sübutların əhəmiyyəti kibercinayətlərin istintaqı təcrübəsində daha aydın görünür. Məsələn, dövlət informasiya resursuna qarşı paylanılmış xidmətdən imtina hücumu (DDoS) [5] zamanı müxtəlif xarici IP ünvanlar müəyyən olunsa da, hüquqi yardım sorğularına cavabların gec daxil olması sübutların operativ əldə olunmasına mane olur. Bir sıra hallarda isə xidmət provayderlərində saxlanma müddətinin başa çatması səbəbindən loq məlumatlarının itirilməsi istintaqın istiqamətini zəiflədir. İcraatda olan real cinayət işinin materiallarının daha geniş təhlili göstərir ki, qeyd olunan DDoS hücumu nəticəsində sistemə qısa müddət ərzində milyonlarla sorğu daxil olmuşdur. Bu sorğuların analizi zamanı texniki baxımdan ən aktiv IP ünvanların seçilməsi xüsusi əhəmiyyət kəsb etmişdir. Aparılmış filtrasiya və texniki analiz nəticəsində müəyyən edilmiş IP

DOI: 10.25045/forensic.gov.2026.73

ünvanların müxtəlif xarici dövlətlərə aid olduğu müəyyən edilmiş və bununla əlaqədar olaraq ümumilikdə 12 xarici dövlətə hüquqi yardım sorğuları göndərilmişdir. Lakin bu sorğular üzrə cavabların əldə olunması müəyyən vaxt tələb etmiş və bu hal istintaqın operativliyinə təsir göstərmişdir. Xüsusilə qeyd edilməlidir ki, xarici dövlətin birindən daxil olmuş cavab istintaq üçün həlledici əhəmiyyət kəsb etmişdir. Həmin cavabda hücumun əsasən müəyyən provayderə məxsus server infrastrukturu üzərindən təşkil edildiyi müəyyən edilmiş və həmin resurslardan istifadə edən şəxslərin identifikasiyası istiqamətində mühüm məlumatlar əldə olunmuşdur. Bu məlumatlar əsasında istintaqın istiqaməti konkretləşdirilmiş və əlavə hüquqi yardım mexanizmləri vasitəsilə hücumda iştirak edən şəxslərdən birinin müəyyən edilməsi mümkün olmuşdur.

Nümunə kimi, həmçinin digər cinayət işi üzrə isə müəyyən edilmişdir ki, dövlət qurumuna qarşı həyata keçirilmiş kiber müdaxilə zamanı hücum edən şəxs yalnız sistemə daxil olmaqla kifayətlənməmiş, eyni zamanda bütün loq məlumatlarını silməklə sübutların qəsdən məhv edilməsinə yönəlmiş hərəkətlər etmişdir. Loq məlumatlarının silinməsi nəticəsində sistemə giriş vaxtı, istifadə olunan IP ünvanlar və həyata keçirilmiş əməliyyatlar barədə kritik məlumatlar itirilmişdir. Bu isə istintaqın gedişini çətinləşdirmiş və elektron sübutların bir hissəsinin bərpasını mümkünsüz etmişdir. Belə hallarda istintaq orqanı alternativ sübut mənbələrinə – şəbəkə trafiki, ehtiyat nüsxələr və digər dolayı sübutlara müraciət etməyə məcbur qalır ki, bu da istintaq prosesini daha mürəkkəb və vaxt aparan edir. sistemə müdaxilə edən şəxs loq faylları silməklə və izləri qəsdən yox etməklə sübut bazasını dağıdır. Bu isə antikriminalistikanın müasir forması kimi qiymətləndirilə bilər.

Cinayət-Prosessual Məcəlləsinə 2026-cı ildə edilmiş dəyişikliklər həmin problemlərin bir hissəsinin hüquqi səviyyədə həllinə yönəlmişdir. Xüsusilə 133-2 və 133-3-cü maddələrdə elektron sübutların saxlanması və elektron verilənlərin mühafizəsi ilə bağlı müddəalar istintaq orqanlarına daha çevik reaksiya imkanı verir. Bu yeniliklər məlumatların sonradan silinməsinin qarşısını almaq, provayder və ya xidmət təminatçılarının məlumatları müəyyən müddətdə qorumasını təmin etmək və sübutların itirilməsi riskini azaltmaq baxımından əhəmiyyətlidir [6].

Bununla yanaşı, yeni normativ baza bütün problemləri avtomatik aradan qaldırmır. Birincisi, elektron sübutlarla işləyən bütün istintaq subyektləri üçün vahid metodiki standartların işlənməsi vacibdir. İkincisi, transsərhəd işlərdə beynəlxalq hüquqi yardım prosedurlarının sürəti hələ də müəyyən hallarda kifayət etmir. Üçüncüsü, elektron sübutların məhkəmədə izahı üçün müstəntiq, mütəxəssis və ekspert arasında funksional koordinasiya gücləndirilməlidir. Elektron sübutların texniki mahiyyəti lazımi şəkildə izah edilmədikdə məhkəmənin onların dəyərini qiymətləndirməsi çətinləşir.

NƏTİCƏ

Nəticə etibarilə, Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində elektron sübutların ayrıca sübut növü kimi təsbit olunması müasir cinayət mühakimə icraatının rəqəmsal çağırışlara cavabı kimi qiymətləndirilməlidir. Yeni maddələr hüquqi bazanı genişləndirsə də, praktik səmərəlilik üçün həm texniki imkanların artırılması, həm də sübutların əldə olunması, mühafizəsi və məhkəmədə təqdim olunması üzrə vahid praktik yanaşmanın formalaşdırılması zəruridir. Elektron sübutların düzgün idarə olunması müasir kiberhücumların istintaqında yalnız texniki məsələ deyil, həm də ədalətli məhkəmə araşdırmasının təminatı baxımından həlledici hüquqi şərtdir.

Bununla yanaşı, müasir dövrdə rəqəmsal mühitin dinamik inkişafı elektron sübutların hüquqi tənzimlənməsinin davamlı şəkildə təkmilləşdirilməsini tələb edir. Xüsusilə süni intellekt texnologiyalarının, bulud xidmətlərinin və anonimləşdirici alətlərin geniş yayılması şəraitində sübutların identifikasiyası, mənbəyinin müəyyən edilməsi və etibarlılığının yoxlanılması daha mürəkkəb xarakter alır. Bu isə yalnız normativ dəyişikliklərlə deyil, eyni zamanda texnoloji adaptasiya və institusional inkişaf vasitəsilə həll olunmalıdır. Digər tərəfdən, elektron sübutlarla bağlı beynəlxalq təcrübənin öyrənilməsi və milli qanunvericiliyə uyğunlaşdırılması da xüsusi əhəmiyyət kəsb edir. Transsərhəd kibercinayətlərin artması fonunda dövlətlərarası əməkdaşlığın sürətləndirilməsi, məlumat mübadiləsi mexanizmlərinin optimallaşdırılması və hüquqi yardım prosedurlarının sadələşdirilməsi elektron sübutların effektiv istifadəsinə birbaşa təsir göstərir.

Nəhayət, elektron sübutların istintaqı və qiymətləndirilməsi sahəsində kadr hazırlığı məsələsi də prioritet istiqamətlərdən biri kimi çıxış edir. Müstəntiqlərin, prokurorların və hakimlərin rəqəmsal texnologiyalar üzrə bilik və bacarıqlarının artırılması, ixtisaslaşmış ekspert institutlarının inkişafı və texniki vasitələrin müasirləşdirilməsi bu sahədə əldə olunan hüquqi yeniliklərin praktik nəticəyə çevrilməsində həlledici rol oynayır.

ƏDƏBİYYAT

[1] Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi. https://e-qanun.az/framework/46950

[2] "Azərbaycan Respublikasının Cinayət Məcəlləsində və Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində dəyişiklik edilməsi haqqında" Azərbaycan Respublikasının Qanunu, 373-VIIQD. https://e-qanun.az/framework/61568

[3] Azərbaycan Respublikası Prezidentinin rəsmi internet səhifəsi. "Azərbaycan Respublikasının Cinayət Məcəlləsində və Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində dəyişiklik edilməsi haqqında" Azərbaycan Respublikasının Qanunu. URL: https://president.az/az/articles/view/71954

[4] Azərbaycan Dövlət İnformasiya Agentliyi (AZƏRTAC). "Cinayət və Cinayət-Prosessual məcəllələrində dəyişiklik edilir". https://azertag.az/xeber/cinayet_ve_cinayet_prosessual_mecellelerinde_deyisiklik_edilir-4053191

[5] Modern.az. "Elektron sübutların toplanması hüquqi çərçivəyə salınır". https://modern.az/az/parlament/576357/elektron-subutlarin-toplanmasi-huquqi-cerciveye-salinir/

[6] Labrisnetworks.com "DDoS hücumu nədir?". https://labrisnetworks.com/az/ddos-hucumlarini-anlamaq/

The Legal Status of Electronic Evidence in Criminal Proceedings and its Applıcation in the Investigation of Cyberattacks

Ali Tahmazov
State Security Service, Baku, Azerbaijan
ali.tahmazov@dtx.gov.az

Abstract - This article analyzes the legal status of electronic evidence, its classifications, methods of acquisition, and the principal requirements for its admissibility and use in court

within the context of the 2026 amendments to the Criminal Procedure Code of the Republic of Azerbaijan. Particular attention is devoted to Article 124.2.3-1 of the Criminal Procedure Code, which formally recognizes electronic evidence as an independent category of evidence, as well as to Articles 133-1 through 133-3, which introduce new legal approaches concerning electronic data, its admissibility as evidence, and its preservation. The article further examines practical challenges arising in cyberattack investigations, including delays in investigative response, deletion of log files, transnational cooperation issues, and the preservation of the chain of custody for electronic evidence, drawing on real investigative case examples.

Keywords - digital evidence; cyberattack; electronic data; criminal procedure; investigation; court.