DOI: 10.30546/120124.2026.001.1116

Kibercinayətlərin istintaqı kontekstində rəqəmsal suverenliyin konstitusion əsasları

Elşad Nəsirov,
Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyasının rəisi.
Elektron ünvan: elshad_nasirov@yahoo.com

Kamran Xəlilov,
Bakı Dövlət Universitetinin doktorantı və Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyasının müəllimi.
Elektron ünvan: xalilovkamran75@gmail.com

Xülasə

Rəqəmsal texnologiyaların inkişafı cinayətkarlığın xarakterini və miqyasını dəyişmiş, kibercinayətkarlıqla mübarizə dövlətin təhlükəsizliyinin təmin edilməsində prioritet istiqamətlərdən birinə çevrilmişdir. Kibercinayətlərin istintaqı zamanı sübutların müxtəlif dövlətlərin ərazisində yerləşməsi və məlumat mübadiləsinin beynəlxalq xarakter daşıması ənənəvi ərazi yurisdiksiyası anlayışının tətbiqini çətinləşdirir və yeni hüquqi yanaşmaların formalaşdırılmasını zəruri edir. Bu şəraitdə dövlətin istintaq fəaliyyəti ilə bağlı səlahiyyətlərinin konstitusion əsaslarının müəyyən edilməsi xüsusi əhəmiyyət kəsb edir. Məqalənin məqsədi kibercinayətlərin istintaqı çərçivəsində dövlətin səlahiyyətlərinin konstitusion çərçivəsini müəyyənləşdirmək və bu sahədə hüquqi tənzimləmənin əsas istiqamətlərini sistemli şəkildə təhlil etməkdir. Tədqiqat normativ-hüquqi və doktrinal təhlil metodlarına əsaslanır, həmçinin beynəlxalq məhkəmə təcrübəsi və müqayisəli hüquqi yanaşma nəzərə alınır. Araşdırmada cinayət yurisdiksiyasının hüdudları, beynəlxalq əməkdaşlıq çərçivəsində sübutların əldə olunması mexanizmləri, məhkəmə nəzarəti və mütənasiblik prinsipi konstitusion baxımdan qiymətləndirilir. Təhlil göstərir ki, rəqəmsal mühit dövlət suverenliyinin həyata keçirilməsi mexanizmlərinin dəyişən hüquqi reallıqlar kontekstində yenidən formalaşdırılmasını tələb edir. Kibercinayətlərin effektiv istintaqı dövlətin konstitusiya ilə müəyyən edilmiş təhlükəsizlik funksiyasının tərkib hissəsi olmaqla yanaşı, hüquqi dövlət prinsipi, normativ müəyyənlik və fundamental hüquqların qorunması ilə uzlaşdırılmış şəkildə həyata keçirilməlidir. Tədqiqatın elmi yeniliyi rəqəmsal şəraitdə istintaq səlahiyyətlərinin konstitusion əsaslandırılmasına və dövlətin bu sahədə fəaliyyətinin sistemli modelinin təqdim edilməsinə yönəlmişdir.

Açar sözlər: *rəqəmsal suverenlik, kibercinayətlərin istintaqı, konstitusion əsaslar, dövlət suverenliyi, cinayət yurisdiksiyası, hüquqi dövlət prinsipi, mütənasiblik prinsipi.*

Giriş

Müasir dövrdə kibercinayətlərin artması və rəqəmsal mühitdə istintaq fəaliyyətinin genişlənməsi dövlət suverenliyinin həyata keçirilmə formalarının konstitusion baxımdan yenidən qiymətləndirilməsini zəruri edir. İnformasiya və kommunikasiya texnologiyalarının geniş tətbiqi nəticəsində kibercinayətlər artıq yalnız müəyyən fiziki ərazidə baş vermir, eyni zamanda transmilli xarakter daşıyaraq müxtəlif yurisdiksiyalar arasında həyata keçirilir. Bu isə dövlətlərin cinayət hüququ çərçivəsində istintaq səlahiyyətlərini həyata keçirmə metoduna birbaşa təsir göstərir. Xüsusilə rəqəmsal sübutların müxtəlif ölkələrdə yerləşməsi ənənəvi ərazi prinsipinə əsaslanan istintaq mexanizmlərini mürəkkəbləşdirir və yeni hüquqi suallar yaradır.

Rəqəmsal mühitdə istintaq fəaliyyəti yalnız texniki məsələ deyil, həm də konstitusion əhəmiyyət daşıyan hüquqi problemdir. Dövlət kibercinayətlərlə mübarizə apararkən bir tərəfdən təhlükəsizlik funksiyasını həyata keçirir, digər tərəfdən isə fundamental hüquq və azadlıqların qorunması öhdəliyini daşıyır. Bu səbəbdən rəqəmsal mühitdə is-

tintaq səlahiyyətlərinin həyata keçirilməsi hüquqi dövlət prinsipi, hüquqi müəyyənlik və mütənasiblik meyarları əsasında qiymətləndirilməlidir.

Transmilli xarakter daşıyan sübutların əldə olunması və mübadiləsi üzrə mexanizmlər və beynəlxalq əməkdaşlıq alətləri mövcud olsa da, onların tətbiqi hər bir dövlətin konstitusion sistemi daxilində əsaslandırılmalıdır. Rəqəmsal mühit dövlət suverenliyinin həyata keçirilmə formasını dəyişir və istintaq səlahiyyətlərinin hüquqi əsaslarının daha dəqiq müəyyən edilməsini tələb edir. Bu baxımdan əsas məsələ istintaq fəaliyyətinin hansı çərçivədə və hansı hədlər daxilində reallaşdırılmalı olduğunu aydınlaşdırmaqdır.

Bu tədqiqatın məqsədi kibercinayətlərin istintaqı kontekstində dövlətin cinayət yurisdiksiyası və prosessual səlahiyyətlərinin konstitusion əsaslarını sistemli şəkildə təhlil etməkdir. Tədqiqat rəqəmsal mühitdə istintaq fəaliyyətinin həyata keçirilməsini hüquqi dövlət prinsipi çərçivəsində qiymətləndirir və bu sahədə konstitusion legitimlik meyarlarını müəyyənləşdirməyə yönəlir.

Metodoloji baxımdan araşdırma normativ, hüquqi, doktrinal və müqayisəli təhlilə əsaslanır. Konstitusiya normaları, cinayət və cinayət-prosessual qanunvericilik və beynəlxalq hüquqi mexanizmlər qarşılıqlı əlaqədə qiymətləndirilmiş, İnsan Hüquqları üzrə Avropa Məhkəməsinin (bundan sonra – İHAM) və Avropa İttifaqı Ədalət Məhkəməsinin (bundan sonra – AİƏM) presedentləri analitik çərçivə kimi istifadə edilmişdir. Seçilmiş yanaşma rəqəmsal mühitdə istintaq səlahiyyətlərinin konstitusion əsaslarının həm nəzəri, həm də praktik müstəvidə sistemli şəkildə araşdırılmasına imkan verir.

Bu kontekstdə məqalənin əsas tədqiqat sualları aşağıdakılardır:

Kibercinayətlərin istintaqı kontekstində dövlət suverenliyi hansı konstitusion prinsiplərə əsaslanır?

Rəqəmsal mühitdə transmilli səviyyədə sübut əldə olunması prosesi dövlətin cinayət yurisdiksiyasının sərhədlərinə necə təsir göstərir?

Dövlətin istintaq səlahiyyətlərinin həyata keçirilməsi hüquqi dövlət prinsipi və mütənasiblik meyarları ilə necə uzlaşdırılmalıdır?

Tədqiqatın elmi yeniliyi üç əsas istiqamətdə özünü göstərir. Birincisi, rəqəmsal suverenlik anlayışı informasiya siyasəti və texnoloji idarəetmə kontekstindən çıxarılaraq cinayət-prosessual səlahiyyətlər müstəvisində təhlil olunur. Bu yanaşma suverenliyi yalnız siyasi müstəqillik kimi deyil, istintaq fəaliyyətinin konstitusion əsasını təşkil edən hüquqi institut kimi təqdim edir. İkincisi, məqalədə kibercinayətlərin istintaqı kontekstində dövlətin prosessual hakimiyyəti sistemli şəkildə modelləşdirilir. Bu çərçivədə yurisdiksiya, sərhədlərarası sübut mübadiləsi üzrə mexanizmlər və məhkəmə nəzarətinin funksional rolu vahid konstitusion çərçivə daxilində əlaqələndirilir. Üçüncüsü, tədqiqat rəqəmsal mühitdə istintaq səlahiyyətlərinin hüquqi əsaslandırılmasını dövlət hakimiyyətinin konstitusion legitimliyinin mühüm elementi kimi nəzərdən keçirir. Bu yanaşma təhlükəsizlik məqsədləri ilə fundamental hüquqların qorunmasını vahid konstitusion çərçivədə qiymətləndirir və onların qarşılıqlı balansını əsas götürür.

Klassik suverenlik anlayışı və cinayət yurisdiksiyası

Suverenlik dövlət hakimiyyətinin hüquqi mahiyyətini müəyyən edən fundamental kateqoriyadır. Klassik hüquq nəzəriyyəsində suverenlik dövlətin müəyyən ərazi daxilində ali və müstəqil hakimiyyətə malik olması kimi izah olunur. Bu hakimiyyət normativ xarakter daşıyır və qanun yaratma, tətbiq etmə və məcburetmə səlahiyyətlərini özündə əhatə edir. Suverenlik dövlət hakimiyyətinin hüquqi əsaslarını və onun realizəsinin sərhədlərini müəyyən edən normativ kateqoriya kimi çıxış edir. Konstitusion dövlət modelində isə həmin kateqoriya birbaşa konstitusiya ilə müəyyən olunur və ali normativ səlahiyyət kimi öz hüquqi ifadəsini tapır. Dövlət hakimiyyətinin təşkili, səlahiyyət bölgüsü və icra mexanizmləri birbaşa konstitusiya ilə müəyyən edilir və bütün dövlət orqanlarının fəaliyyəti həmin ali hüquqi çərçivəyə uyğun olmalıdır. Bu baxımdan suverenlik hüquqi dövlət prinsipi ilə vəhdətdə çıxış edir və onun tətbiqi hüquqi müəyyənlik, mütənasiblik və məhkəmə nəzarəti mexanizmləri ilə məhdudlaşdırılır. Bununla da suverenlik sərhədsiz hakimiyyət deyil, normativ legitimliklə şərtlənmiş səlahiyyət formasıdır.

Beynəlxalq hüquq doktrinasında suverenlik dövlətlərin hüquqi bərabərliyi və ərazi bütövlüyü prinsipləri ilə əlaqələndirilir. Belə ki, BMT Nizamnaməsinin 2-ci maddəsi dövlətlərin suveren bərabərliyini təsbit etməklə digər dövlətlərin daxili səlahiyyətlərinə müdaxiləni qadağan edir. Lakin müasir beynəlxalq hüquq mühitində suverenlik tam təcrid olunmuş hakimiyyət kimi deyil, qarşılıqlı tanınma və əməkdaşlıq mexanizmləri ilə uzlaşdırılmış institut kimi çıxış edir. Bu xüsusiyyət cinayət hüququnun tətbiqi sahəsində xüsusilə əhəmiyyətlidir.

Cinayət yurisdiksiyası suverenliyin konkret təzahür formasıdır. Dövlət cinayət məsuliyyətini müəyyən etmək, istintaq aparmaq və cəza tətbiq etmək səlahiyyətinə malikdir və bu səlahiyyət onun ali hakimiyyətinin hüquqi ifadəsidir. Yurisdiksiya anlayışı dövlətin şəxslər, əməllər və hadisələr üzərində hüquqi hakimiyyətini ifadə edir. Bu hakimiyyət norma yaratma və icra xarakterli komponentlərdən ibarətdir. Dövlət müəyyən davranışı cinayət kimi tanımaq hüququna malik olsa da, həmin normanın faktiki tətbiqi prosessual mexanizmlər və konstitusion məhdudiyyətlər daxilində həyata keçirilir. Bu fərqləndirmə suverenliyin praktik sərhədlərini müəyyən edən mühüm nəzəri alət kimi çıxış edir.

Ənənəvi olaraq cinayət yurisdiksiyası ərazi prinsipi əsasında qurulur. Dövlət öz ərazisində törədilmiş və ya nəticəsi həmin ərazidə baş vermiş cinayət əməllərinə münasibətdə cinayət təqibini həyata keçirmək hüququna malikdir. Ərazi prinsipi dövlətin cinayət-hüquqi hakimiyyətinin məkan baxımdan hüdudlarını müəyyən edir və cinayət təqibinin legitimliyini təmin edir. Bununla yanaşı, beynəlxalq hüquqda şəxsi bağlılıq meyarına əsaslanan yurisdiksiya formaları da qəbul edilir. Dövlət öz vətəndaşlarının xarici ərazilərdə törətdiyi cinayət əməllərinə görə cinayət məsuliyyəti tətbiq edə bilər. Bu yanaşma doktrinada aktiv şəxsi yurisdiksiya kimi xarakterizə olunur və dövlətlə cinayət əməlini törədən şəxs arasındakı vətəndaşlıq bağlılığına əsaslanır. Eyni zamanda dövlət öz vətəndaşlarına qarşı xaricdə törədilmiş cinayətlərə münasibətdə də yurisdiksiya həyata keçirə bilər. Bu model passiv şəxsi yurisdiksiya kimi tanınır və dövlətin öz vətəndaşlarının hüquq və mənafelərini qorumaq funksiyası ilə əsaslandırılır. Bu mexanizmlər suverenliyin yalnız coğrafi məkan baxımından deyil, həm də hüquqi bağlılıq əsasında reallaşdığını göstərir.

Universal yurisdiksiya prinsipi beynəlxalq ictimaiyyət üçün xüsusi təhlükəlilik dərəcəsinə malik cinayətlərə münasibətdə dövlətlərə ərazi və vətəndaşlıq meyarlarından asılı olmayaraq cinayət təqibi həyata keçirmək imkanı verir. Genosid, insanlığa qarşı cinayətlər və müharibə cinayətləri üzrə yurisdiksiya tətbiqi beynəlxalq cinayət hüququnda formalaşmış və geniş qəbul olunmuş mexanizmdir. Müasir beynəlxalq hüquq ədəbiyyatında universal yurisdiksiya dövlətlərin ağır beynəlxalq cinayətlərə qarşı kollektiv məsuliyyəti kontekstində təhlil olunur. Bu yanaşma çərçivəsində dövlətlərin belə cinayətlərə münasibətdə tədbir görməsi beynəlxalq hüquqi öhdəliklərlə əlaqələndirilir və suverenliyin beynəlxalq hüquq sistemi daxilində həyata keçirilməsinin xüsusi forması kimi izah edilir. Deməli, universal yurisdiksiya institutu dövlətlərin beynəlxalq cinayətlərlə mübarizə sahəsində səlahiyyət və öhdəliklərinin qarşılıqlı əlaqəsini ifadə edir və suverenliyin beynəlxalq hüquqi mühitdə funksional şəkildə reallaşdırılması mexanizmlərindən biri kimi qiymətləndirilir.

Cinayət yurisdiksiyası institutunun legitimliyi hüquqi dövlət prinsipi ilə təmin edilir. Dövlətin istintaq və məcburetmə səlahiyyətləri qanunla müəyyən edilməli, normativ baxımdan aydın və proqnozlaşdırıla bilən olmalı və effektiv məhkəmə nəzarəti ilə müşayiət olunmalıdır. İHAM-in presedent hüququnda müdaxilə tədbirlərinin "qanunla nəzərdə tutulmuş" olması tələbi normanın əlçatanlığını və proqnozlaşdırıla bilənliyini ehtiva edir. Bu yanaşma suveren hakimiyyətin hüquqi çərçivə daxilində və normativ əsaslara söykənərək həyata keçirilməsini təmin edir.

Bununla belə, klassik yurisdiksiya modeli cinayət davranışının fiziki məkana bağlı olduğu fərziyyəsinə əsaslanır. Bu modeldə əməl, nəticə və sübut eyni və ya bir-biri ilə coğrafi əlaqədə olan məkan daxilində baş verir. Rəqəmsal mühitdə isə vəziyyət fərqlidir. Elektron məlumatlar eyni vaxtda müxtəlif dövlətlərin serverlərində saxlanıla bilər, kommunikasiya axınları bir neçə yurisdiksiyanı əhatə edə bilər və istintaq üçün əhəmiyyətli sübut fiziki obyekt formasında mövcud olmaya

bilər. Bu xüsusiyyətlər ərazi prinsipinin tətbiqində normativ və praktik çətinliklər yaradır.

Beləliklə, suverenlik və cinayət yurisdiksiyası qarşılıqlı bağlı institutlardır. Suverenlik dövlətə cinayət hüququ tətbiq etmək səlahiyyəti verir, yurisdiksiya isə bu səlahiyyətin konkret hüquqi mexanizmini təşkil edir. Lakin rəqəmsal mühit klassik ərazi modelinə əsaslanan yurisdiksiya mexanizminin tətbiqini mürəkkəbləşdirir və suverenliyin funksional interpretasiyasını zəruri edir. Bu nəzəri baza dövlətin istintaq fəaliyyətinin konstitusion əsaslarını anlamaq üçün fundamental əhəmiyyət daşıyır və rəqəmsal mühitdə bu səlahiyyətlərin tətbiqinin qiymətləndirilməsi üçün metodoloji çərçivə yaradır.

Rəqəmsal mühitdə istintaq fəaliyyətinin xüsusiyyətləri və konstitusion əsaslandırmanın vacibliyi

Azərbaycan Respublikasında rəqəmsal istintaqın hüquqi modeli

Rəqəmsal mühitdə istintaq səlahiyyətlərinin legitimliyi ilk növbədə Azərbaycan Respublikası Konstitusiyasının müəyyən etdiyi fundamental prinsiplər çərçivəsində qiymətləndirilməlidir. Azərbaycan Respublikasının Konstitusiyası hüquqi dövlət modelini qəbul etməklə dövlət hakimiyyətinin fəaliyyətini hüquqla məhdudlaşdırılmış səlahiyyət kimi müəyyən edir. Bu prinsip rəqəmsal mühitə də eyni intensivliklə tətbiq olunur. Dövlətin kibercinayətlərlə mübarizə aparmaq səlahiyyəti mövcuddur, lakin həmin səlahiyyət konstitusion çərçivə daxilində əsaslandırılmalıdır. Nəzərə almaq lazımdır ki, Konstitusiya rəqəmsal istintaq səlahiyyətini birbaşa təsbit etmir. Bu akt dövlət hakimiyyətinə təhlükəsizlik funksiyasını həyata keçirmək imkanı verir və həmin səlahiyyətin konkret məzmunu qanunvericilik vasitəsilə formalaşdırılır. Bu, rəqəmsal müdaxilənin konstitusion deyil, törəmə normativ səlahiyyət kimi qiymətləndirilməsini şərtləndirir.

Konstitusiyanın 12-ci maddəsində insan və vətəndaş hüquq və azadlıqlarının təmin olunması dövlətin ali məqsədi kimi müəyyən edilmişdir. Bu norma rəqəmsal istintaq tədbirlərinin hüquqi qiymətləndirilməsi üçün meyar rolunu oynayır və müdaxilənin cinayət təqibi ilə yanaşı, insan və vətəndaş hüquqlarının qorunması funksiyası ilə uzlaşdırılmasını zəruri edir. Eyni zamanda 94-cü maddə cinayət məsuliyyətinin və cinayət-prosessual mexanizmlərin yalnız qanunla müəyyən edilə biləcəyini təsbit etməklə istintaq səlahiyyətlərinin normativ əsasını konstitusion səviyyədə müəyyənləşdirir. Konstitusiyanın 32-ci maddəsi şəxsi həyatın toxunulmazlığını və məlumatların qanunsuz toplanmasının yolverilməzliyini təsbit edir.

Hesab edirik ki, rəqəmsal mühitdə elektron yazışmalara, şəbəkə (trafik) məlumatlarına və şəxsi informasiya daşıyıcılarına çıxış bu maddənin tətbiq sferasına daxildir. Bu baxımdan müdaxilə yalnız qanuni əsasla və məhkəmə nəzarəti çərçivəsində mümkündür. Konstitusion model müdaxilənin formasını deyil, onun hüquqi əsasını və məqsədini qiymətləndirir. Bu isə rəqəmsal istintaq tədbirlərinin klassik axtarış və baxış tədbirləri ilə eyni hüquqi meyarlarla qiymətləndirilməsini şərtləndirir.

Konstitusiyanın sözügedən müddəalarının mühüm xüsusiyyəti hüquq və azadlıqların məhdudlaşdırılmasının yalnız qanunla və legitim məqsəd naminə mümkün olmasıdır. Dövlət təhlükəsizliyi və ictimai asayiş kimi məqsədlər rəqəmsal istintaq tədbirlərinin əsaslandırılmasında legitim məqsəd kimi çıxış edə bilər. Lakin müdaxilə zəruri və mütənasib olmalıdır. Mütənasiblik prinsipi rəqəmsal mühitdə xüsusi əhəmiyyət kəsb edir, çünki elektron məlumatlar böyük həcmdə şəxsi və kontekstual informasiya ehtiva edə bilər. Bu səbəbdən müdaxilənin həcmi ilə gözlənilən nəticə arasında rasional balans qorunmalıdır.

Konstitusiyada təsbit olunmuş məhkəməyə müraciət hüququ, müdafiə hüququ və qanunsuz üsulla əldə edilmiş sübutların yolverilməzliyi rəqəmsal sübutların toplanması və istifadə edilməsi prosesində əsas hüquqi təminatlar sırasında yer alır. Bu konstitusion müddəalar istintaq fəaliyyətinin həyata keçirilmə qaydalarını və sübutların prosessual dövriyyəsini hüquqi çərçivəyə salır. Azərbaycan Konstitusiyası rəqəmsal istintaq fəaliyyətini mövcud hüquqi dövlət modelinin tərkib hissəsi kimi nəzərdə tutur və onu ümumi konstitusion prinsiplər sisteminə daxil edir.

Azərbaycan Respublikasında dövlətin kibercinayətlərlə mübarizə sahəsində istintaq səlahiyyətləri Konstitusiya ilə yanaşı, Cinayət Məcəlləsi,

Cinayət-Prosessual Məcəllə və bu sahədəki digər normativ hüquqi aktlarla müəyyən edilir.

Qeyd etmək lazımdır ki, rəqəmsal mühitdə hüquqi tənzimləmənin təkmilləşdirilməsi istiqamətində son dövrlərdə mühüm normativ dəyişikliklər həyata keçirilmişdir. Belə ki, "Azərbaycan Respublikasının Cinayət Məcəlləsində və Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində dəyişiklik edilməsi haqqında" Azərbaycan Respublikasının 2026-cı il 3 mart tarixli 373-VIIQD nömrəli Qanunu ilə cinayət və cinayət-prosessual qanunvericilikdə aparılmış dəyişikliklər nəticəsində həm Cinayət Məcəlləsində kibercinayətlərə dair müddəaların terminoloji və məzmun baxımından müasirləşdirilməsi, həm də Cinayət-Prosessual Məcəllədə elektron sübutlar və rəqəmsal mühitlə bağlı anlayışların sistemli şəkildə təsbit olunması təmin edilmişdir. Bu dəyişikliklər maddi hüquqla prosessual mexanizmlər arasında əlaqənin gücləndirilməsi və rəqəmsal cinayətkarlığa qarşı mübarizənin hüquqi əsaslarının inkişaf etdirilməsi baxımından mütərəqqi addım hesab olunmalıdır.

Hər şeydən öncə Azərbaycan Respublikasının Cinayət Məcəlləsində (bundan sonra - CM) kibercinayətlərin ayrıca fəsil şəklində təsbit olunması yalnız cinayət siyasətinin texniki elementi deyil, həm də dövlətin konstitusion funksiyasının hüquqi ifadəsi kimi qiymətləndirilə bilər. Konstitusion hüquq nəzəriyyəsinə görə, dövlət yalnız hüquqlara müdaxilə etməmək öhdəliyi daşıyan passiv subyekt deyil, eyni zamanda fərdləri real və aktual təhlükələrdən qorumaq vəzifəsi olan aktiv hüquqi aktordur. Hüquq ədəbiyyatında bu yanaşma dövlətin pozitiv öhdəliyi kimi izah olunur. Yəni dövlət təkcə azadlıqları məhdudlaşdırmamalı, həm də onları cinayət xarakterli müdaxilələrdən effektiv şəkildə müdafiə etməlidir.

Rəqəmsal mühitdə İKT sistemlərinə qanunsuz müdaxilə, elektron verilənlərin dəyişdirilməsi və ya silinməsi, eləcə də kibermühitlə əlaqəli digər hüquq pozuntuları şəxsi həyatın toxunulmazlığına, mülkiyyət maraqlarına və informasiya təhlükəsizliyinə birbaşa təhdid yaradır. Bu baxımdan kibercinayətlərin CM-də kriminalizasiyası dövlətin hüquqları qorumağa yönəlmiş müdafiə funksiyasının maddi hüquqi mexanizmi kimi çıxış edir. Lakin cinayət hüququnun özü də konstitusion məhdudiyyətlər daxilində fəaliyyət göstərməlidir. Konstitusion hüququn əsas prinsiplərindən biri hüquqi müəyyənlikdir. Bu prinsip tələb edir ki, cinayət məsuliyyəti yaradan davranış aydın, dəqiq və proqnozlaşdırıla bilən şəkildə müəyyən edilsin. Şəxs əvvəlcədən bilməlidir ki, hansı hərəkət və ya hərəkətsizlik cinayət hüquqi nəticə doğurur. Rəqəmsal mühitdə istifadə olunan anlayışların texniki xarakter daşıması və sürətlə dəyişməsi bu sahədə terminoloji və tətbiqi dəqiqliyin daim diqqətdə saxlanılmasını zəruri edir. Əgər kibercinayət tərkibləri həddən artıq geniş və ya qeyri-dəqiq formalaşdırılarsa, bu, istintaq orqanlarının normanı geniş şərh etməsinə imkan yarada bilər və nəticə etibarilə fundamental hüquqlara müdaxilənin dairəsini genişləndirə bilər.

Bu kontekstdə dolayı müdaxilə anlayışı xüsusi əhəmiyyət kəsb edir. Dolayı müdaxilə o deməkdir ki, norma formal olaraq hüququ qadağan etməsə də, onun qeyri-müəyyən tətbiqi nəticəsində şəxslər hüquqlarını ehtiyatla və məhdud şəkildə həyata keçirməyə meyil göstərə bilərlər. Hüquq nəzəriyyəsində bu hal çox vaxt "soyuducu effekt" anlayışı ilə izah olunur. Sadə ifadə ilə desək, əgər şəxslər hüquqi sərhədlərin aydın olmaması səbəbindən qanuni fəaliyyətlərini belə riskli hesab edərək onlardan çəkinirlərsə, bu, hüququn praktik həyata keçirilməsinə dolayı mənfi təsir deməkdir. Rəqəmsal mühitdə informasiya mübadiləsi və texniki fəaliyyət sahəsində bu riskin daha həssas formada təzahür etməsi ehtimalı nəzərə alınmalıdır. Buna görə də, kibercinayət normalarının tətbiqində dəqiqlik, konkretlik və hüquqi müəyyənlik meyarlarının qorunması xüsusi əhəmiyyətə malikdir.

CM-in məkana görə tətbiqi məsələsi də rəqəmsal mühitdə konstitusion əhəmiyyət daşıyır. Kibercinayətlərdə əməl bir dövlətdə baş verə, nəticə digər dövlətdə yarana, məlumat isə üçüncü ölkənin serverində saxlanıla bilər. Bu vəziyyət dövlətin yurisdiksiya səlahiyyətinin klassik ərazi modeli ilə məhdudlaşmadığını göstərir. Lakin yurisdiksiya səlahiyyətinin genişlənməsi avtomatik olaraq müdaxilə səlahiyyətinin sərhədsiz olması demək deyil. Ekstraterritorial tətbiq mexanizmləri yalnız formal suverenlik anlayışı ilə deyil, mütənasiblik prinsipi ilə uzlaşdırılmalıdır. Mütənasiblik prinsipi konstitusion hüquqda əsas qiymətləndirmə meyarlarından biri kimi tələb edir ki, dövlətin müdaxiləsi legitim məqsədə yönəlsin, həmin məqsədə

nail olmaq üçün zəruri olsun və fundamental hüquqlara müdaxilənin intensivliyi ilə əldə edilən ictimai fayda arasında rasional balans qorunsun. Rəqəmsal daşıyıcıların böyük həcmdə məlumat saxlaması və sübutun istənilən fayl strukturu daxilində yerləşə bilməsi səbəbindən rəqəmsal axtarışlar praktik olaraq geniş informasiya spektrini əhatə edə bilir və bu xüsusiyyət ənənəvi fiziki axtarışlardan fərqli olaraq müdaxilənin real əhatə dairəsini əhəmiyyətli dərəcədə artırır. Bu baxımdan belə müdaxilənin həcmi ilə konkret istintaq fəaliyyətinin məqsədi arasındakı əlaqə mütənasiblik prinsipi çərçivəsində xüsusilə diqqətlə qiymətləndirilməlidir. Əks halda istintaq səlahiyyəti faktiki olaraq ümumi nəzarət mexanizminə çevrilə bilər ki, bu da konstitusion tənzimləməni poza bilər.

Bununla da müəyyən olunur ki, CM rəqəmsal mühitdə cinayət təqibinin maddi hüquqi əsasını formalaşdırır. Lakin bu əsas yalnız aşağıdakı şərtlərlə konstitusion baxımdan legitim hesab edilə bilər: cinayət tərkiblərinin aydın və dəqiq formalaşdırılması; müdaxilənin legitim məqsədə yönəlməsi; tətbiqin zəruri və mütənasib olması; maddi və prosessual mexanizmlər arasında balansın qorunması. Əslində, rəqəmsal mühit ayrıca fövqəladə hüquqi rejim formalaşdırmır. Konstitusion prinsiplər sadəcə olaraq yeni texnoloji reallıqlar kontekstində tətbiq olunur və istintaq səlahiyyətləri həmin ümumi hüquqi qaydalar daxilində həyata keçirilir.

Prosessual baxımdan Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi (bundan sonra – CPM) cinayət prosesinin məqsədini, prinsiplərini və istintaq orqanlarının səlahiyyət dairəsini müəyyən edir. Lakin rəqəmsal mühitdə sübutların əldə olunması və istifadəsi ənənəvi sübut modelindən mahiyyətcə fərqləndiyi üçün klassik prosessual mexanizmlərin bu sahəyə mexaniki tətbiqi əlavə hüquqi əsaslandırma tələb edir. Rəqəmsal sübut fiziki obyekt deyil, dinamik, dəyişdirilə bilən və çoxaldıla bilən məlumat strukturu kimi mövcuddur.

CPM-də sübut anlayışı geniş şəkildə təsbit edilmişdir. Uzun müddət elektron sübutların ayrıca normativ kateqoriya kimi sistemli şəkildə müəyyən edilməməsi praktikada hüquqi müəyyənlik probleminə səbəb olmuşdur. Lakin 2026-cı il 3 mart tarixli 373-VIIQD nömrəli Qanunla edilmiş dəyişikliklərlə elektron formada sübutların ayrıca sübut növü kimi normativ tanınması milli cinayət-prosessual sistemdə rəqəmsal sübutların hüquqi statusunun müəyyən edilməsi baxımından mühüm mərhələ kimi qiymətləndirilə bilər. Bu dəyişiklik hüquqi müəyyənliyin gücləndirilməsi və rəqəmsal mühitdə əldə olunan məlumatların sübut kimi qəbul edilməsinin normativ əsasının yaradılması baxımından əhəmiyyətlidir.

Bununla belə, elektron sübutların hüquqi statusunun əsasən "elektron verilənlər" anlayışı üzərindən müəyyən edilməsi onların spesifik texniki və funksional xüsusiyyətlərini tam əhatə etmir. Müasir hüquq ədəbiyyatında qeyd olunduğu kimi, rəqəmsal sübutlar klassik maddi sübutlardan fərqli olaraq dinamik, çoxaldıla bilən və tez dəyişdirilə bilən xarakterə malikdir və bu xüsusiyyətlər onların əldə olunması, saxlanılması və qiymətləndirilməsi üçün ayrıca metodoloji çərçivənin mövcudluğunu zəruri edir. Elektron məlumatlar metaməlumat daşıyır, uzaq serverlərdə saxlanıla bilər, müxtəlif yurisdiksiyalarda yerləşən sistemlərdə paralel şəkildə və bir neçə nüsxədə mövcud ola bilər. Bu xüsusiyyətlər sübutun autentikliyinin, mənşəyinin və bütövlüyünün qiymətləndirilməsini əhəmiyyətli dərəcədə mürəkkəbləşdirir və klassik sübut doktrinasının tətbiqini məhdudlaşdırır.

Əlavə olaraq, qanunvericiliyə edilmiş sonuncu dəyişikliklərə qədər CPM-in 135-ci maddəsi elektron daşıyıcılardakı məlumatları sənəd kateqoriyası altında ümumiləşdirsə də, rəqəmsal sübutun əldə olunması və surətinin çıxarılması üzrə texniki prosedurlar ayrıca normativ mexanizm kimi sistemləşdirilməmişdi. Halbuki beynəlxalq praktikada rəqəmsal sübutların qorunması üzrə konkret prosedur standartlar formalaşmışdır. Xüsusilə məlumatın ilkin vəziyyətinin qorunması, onların bütövlüyünün kriptoqrafik üsulla identifikasiyası (heş) və texniki ekspertiza prosedurlarının sənədləşdirilməsi sübutun sonradan məhkəmədə etibarlı hesab olunması üçün mühüm əhəmiyyət kəsb edir.

CPM-ə edilmiş son dəyişikliklər çərçivəsində elektron verilənlərin sübut kimi tanınması, onların saxlanılması və mühafizəsi ilə bağlı mexanizmlərin nəzərdə tutulması, habelə informasiya və kom-

munikasiya texnologiyaları sistemi, xidmət provayderi və müxtəlif növ elektron verilənlərə dair anlayışların daxil edilməsi rəqəmsal sübutların hüquqi mühitinin daha sistemli və strukturlaşdırılmış şəkildə formalaşdırılmasına xidmət edir. Bu yanaşma rəqəmsal sübutların yalnız nəticə kimi deyil, həm də onların formalaşdığı texnoloji mühitlə qarşılıqlı əlaqədə qiymətləndirilməsi baxımından müsbət hüquqi inkişaf kimi dəyərləndirilə bilər. Eyni zamanda bu dəyişikliklər rəqəmsal mühitdə fəaliyyət göstərən subyektlərin və məlumat növlərinin hüquqi təsnifatını təmin etməklə cinayət-prosessual fəaliyyətin daha sistemli həyata keçirilməsi üçün əsas yaradır. Bununla belə, mövcud tənzimləmənin tətbiqi prosesində rəqəmsal sübutların əldə olunması, surətinin çıxarılması, emalı və texniki baxımdan etibarlılığının yoxlanılması ilə bağlı metodoloji yanaşmaların daha da dəqiqləşdirilməsi və praktik mexanizmlərlə zənginləşdirilməsi perspektiv olaraq aktuallığını qoruyur. Bu baxımdan normativ çərçivənin mərhələli şəkildə texniki və metodoloji elementlərlə tamamlanması hüquqi sistemin effektivliyinin artırılmasına töhfə verə bilər.

Beynəlxalq praktikada bu sahədə formalaşmış yanaşmalar rəqəmsal sübutlarla işləmənin daha strukturlaşdırılmış metodoloji əsaslara söykəndiyini göstərir. Məsələn, ISO/IEC 27037 standartı rəqəmsal sübutların identifikasiyası, toplanması, əldə olunması və qorunması mərhələlərini fərqləndirərək hər bir mərhələ üzrə konkret prosedur yanaşmalar müəyyən edir və sübutun dəyişdirilmədən əldə olunmasını əsas prinsip kimi qəbul edir. ABŞ Milli Standartlar və Texnologiya İnstitutunun NIST SP 800-86 sənədində rəqəmsal sübutların toplanması və analizinin mərhələli şəkildə həyata keçirilməsi və təhlükəsiz saxlanılması üzrə metodoloji yanaşmalar təqdim olunur. Böyük Britaniyada tətbiq edilən ACPO prinsipləri məlumatın ilkin vəziyyətinin qorunması, əməliyyatların şəffaf sənədləşdirilməsi və audit izlənilə bilənliyi kimi tələbləri ön plana çıxarır. Avropada ENFSI təlimatları isə rəqəmsal ekspertiza prosesində keyfiyyət təminatı və standartlaşdırılmış prosedurların tətbiqinin vacibliyini vurğulayır. Bu yanaşmalar göstərir ki, rəqəmsal sübutların etibarlılığı yalnız onların hüquqi tanınması ilə deyil, həm də əldə olunma və işlənmə prosesinin texniki baxımdan yoxlanıla bilən, izlənilə bilən və təkrarlana bilən olması ilə təmin edilir. Xüsusilə məlumatın ilkin vəziyyətinin qorunması, onların bütövlüyünün kriptoqrafik üsullarla (məsələn, heş vasitəsilə) identifikasiyası, istifadə olunan texniki vasitələrin və metodların qeyd olunması, eləcə də bütün prosesin ardıcıl şəkildə sənədləşdirilməsi sübutun sonradan məhkəmədə etibarlı hesab olunması üçün həlledici əhəmiyyət kəsb edir. Bu baxımdan yalnız prosessual sənədləşdirmə ilə kifayətlənmək əvəzinə texniki səviyyədə də sübutun dəyişdirilmədiyini təsdiq edən mexanizmlərin inkişaf etdirilməsi hüquqi sistemin davamlılığı baxımından əhəmiyyətlidir.

Rəqəmsal sübutların etibarlılığı ilə bağlı əsas mexanizmlərdən biri "saxlanma zənciri" (chain of custody) prinsipidir. Bu prinsip sübutun əldə olunduğu andan məhkəməyə təqdim edilənədək onun kim tərəfindən, hansı üsulla və hansı şəraitdə saxlanıldığını ardıcıl şəkildə sənədləşdirməyi tələb edir. Beynəlxalq standartlarda bu zəncirin hər mərhələsinin izlənilə bilən olması, sübut üzərində aparılmış bütün əməliyyatların audit mexanizmləri vasitəsilə yoxlanıla bilməsi və hər hansı dəyişiklik riskinin minimuma endirilməsi əsas tələb kimi çıxış edir. Mövcud qanunvericilikdə elektron sübutların tamlığının qorunmasına yönəlmiş tələblər nəzərdə tutulsa da, saxlanma zəncirinin daha strukturlaşdırılmış və mərhələli şəkildə tətbiqi ilə bağlı yanaşmaların inkişaf etdirilməsi gələcək hüquqi təkmilləşdirmə istiqamətlərindən biri kimi qiymətləndirilə bilər. Bu isə həm sübutların məhkəmədə qiymətləndirilməsinin etibarlılığını artırar, həm də tərəflər arasında prosessual balansın daha effektiv təmin olunmasına xidmət edə bilər.

Ümumilikdə 2026-cı il 3 mart tarixli 373-VIIQD nömrəli Qanunla edilmiş dəyişikliklərlə rəqəmsal sübutların normativ müstəvidə tanınması və ilkin hüquqi çərçivəsinin formalaşdırılması baxımından mühüm institusional addım kimi qiymətləndirilə bilər. Bununla yanaşı, beynəlxalq təcrübə nəzərə alınmaqla metodoloji və texniki yanaşmaların mərhələli şəkildə inkişaf etdirilməsi, xüsusilə sübutların əldə olunması, emalı və yoxlanılması proseslərinin daha da standartlaşdırılması hüquqi sistemin effektivliyinin artırılması baxımından yüksək əhəmiyyətə malik istiqamətlərdən biri kimi çıxış edir.

Rəqəmsal mühitdə istintaq səlahiyyətlərinin tətbiqi yalnız daxili prosessual mexanizmlərlə məhdudlaşmır, həm də yurisdiksiya məsələsini aktuallaşdırır. Elektron məlumatların fiziki məkandan asılı olmaması və müxtəlif ölkələrin serverlərində saxlanıla bilməsi klassik ərazi prinsipinin praktik tətbiqini mürəkkəbləşdirir və adi daxili istintaq işlərini faktiki olaraq transsərhəd araşdırmaya çevirə bilir. Elektron sübuta çıxış məqsədilə tətbiq edilən ərazi hüdudlarından kənar (ekstraterritorial) tədbirlərin əsas xüsusiyyəti ondan ibarətdir ki, dövlət müvafiq hüquqi mexanizmlər çərçivəsində başqa dövlətlərin ərazisində yerləşə bilən məlumat infrastrukturu vasitəsilə sübuta çıxış əldə etməyə yönəlir. Rəqəmsal mühitdə məlumatın fiziki yerləşdiyi yer ilə ona nəzarət edən provayderin hüquqi mənsubiyyəti üst-üstə düşməyə bilər. Bu səbəbdən istintaq orqanları məlumatın saxlanılması, qorunması və təqdim edilməsi barədə göstərişləri birbaşa xidmət provayderlərinə ünvanlamaqla sübuta operativ çıxış əldə etməyə çalışırlar. Bu yanaşmanın mahiyyəti sürətli və effektiv istintaq təmin etməkdir. Bununla yanaşı, belə mexanizmlər müxtəlif dövlətlərin yurisdiksiyası ilə əlaqəli məlumatlara çıxışı əhatə etdiyində suverenlik, məhkəmə nəzarəti və müdafiə hüququ kimi konstitusion təminatların tətbiq dairəsinin daha dəqiq müəyyən edilməsini aktuallaşdırır. Problemin mərkəzində texniki imkanla hüquqi səlahiyyət arasındakı uyğunluğun təmin edilməsi dayanır. Belə hallarda əsas məsələ istintaqın effektivliyinin təmin olunması ilə yanaşı, müdaxilənin hüquqi əsasının, əhatə dairəsinin və nəzarət mexanizmlərinin aydın və balanslı şəkildə müəyyən edilməsidir. Əks təqdirdə, transsərhəd elektron sübuta çıxış mexanizmlərinin tətbiqi zamanı hüquqi müəyyənliyin təmin olunması və fundamental hüquqların qorunması ilə bağlı əlavə qiymətləndirmə zərurəti yarana bilər.

Bundan əlavə, rəqəmsal sübutların əldə olunması tez-tez geniş həcmli məlumatların toplanmasını tələb edir. Bu isə müdaxilənin həcmi ilə konkret cinayət faktı arasındakı əlaqənin daha dəqiq və əsaslandırılmış şəkildə qiymətləndirilməsini aktuallaşdırır. Xarici mənbəli doktrinada qeyd olunur ki, rəqəmsal mühitdə aparılan axtarışlar ənənəvi fiziki axtarışlardan daha geniş informasiya əldə etmə imkanı yaradır və buna görə də daha yüksək əsaslandırma standartı tələb edə bilər. Bu yanaşma konstitusion mütənasiblik və hüquqi müəyyənlik prinsipləri ilə uzlaşır.

Maddi hüquqla prosessual mexanizmlər arasında uyğunluq konstitusion legitimliyin mühüm elementidir. CM-də kibercinayətlərin dairəsinin geniş müəyyən edilməsi bu cinayətlərin istintaqı üzrə prosessual təminatların eyni dərəcədə konkretləşdirilməsini aktuallaşdırır və bu istiqamətdə maddi hüquqla prosessual mexanizmlər arasında normativ uyğunluğun daha da gücləndirilməsi zərurətini ortaya qoyur. Əlavə olaraq, rəqəmsal sübutların məhkəmə mərhələsində istifadəsi ədalətli məhkəmə hüququ ilə birbaşa bağlıdır. Elektron məlumatların müdafiə tərəfi üçün yoxlanıla bilən və mübahisələndirilə bilən olması konstitusion təminatın əsas elementidir. Müdafiə tərəfinin sübutun texniki xüsusiyyətlərini və əldə olunma qaydasını qiymətləndirmə imkanlarının təmin edilməsi prosessual balansın effektiv həyata keçirilməsi baxımından mühüm əhəmiyyət kəsb edir və bu sahədə əlavə təminatların əhəmiyyətini artırır.

Azərbaycan Respublikasında informasiya və fərdi məlumatlara dair qanunvericilik rəqəmsal mühitin ayrı-ayrı elementlərini müxtəlif hüquqi aktlar vasitəsilə tənzimləyir. Lakin bu aktların istintaq fəaliyyəti ilə qarşılıqlı əlaqəsinin daha aydın və sistemli şəkildə müəyyən edilməsi praktik baxımdan əhəmiyyət kəsb edir. Rəqəmsal sübutun əldə edilməsi prosesində eyni məlumat həm cinayət-prosessual münasibətin obyekti, həm də fərdi məlumatların qorunması rejiminin predmeti kimi çıxış edə bilər. Bu vəziyyət paralel hüquqi rejimlərin əlaqələndirilmiş şəkildə tətbiqini zəruri edir.

Azərbaycan Respublikasının "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" 1998-ci il 3 aprel tarixli 460-IQ nömrəli Qanunu əsasən informasiya sistemlərinin təhlükəsizliyinə və dövlət orqanlarının texniki öhdəliklərinə yönəlmişdir. Cinayət-prosessual müstəvidə isə diqqət konkret sübuta çıxışın hüquqi əsaslarına və həmin sübutun dövriyyə qaydasına yönəlir. "Fərdi məlumatlar haqqında" 2010-cu il 11 may tarixli 998-IIIQ nömrəli Qanun isə məlumatların emalı və saxlanılması üzrə ümumi rejimi müəyyən edir. Rəqəmsal istintaq zamanı məlumatların müvəqqəti saxlanılması, nüsxəsinin çıxarılması və ekspertiza məqsədilə işlənməsi xüsusi hüquqi və-

ziyyət yaradır və məlumatın hansı normativ çərçivəyə daxil edildiyini dəqiqləşdirməyi tələb edir.

Bu aktların təhlili mövzu üçün təsadüfi deyil. Rəqəmsal istintaq fəaliyyətində məlumatların geniş həcmdə toplanması, avtomatlaşdırılmış emalı və üçüncü şəxslərdən əldə edilməsi praktik olaraq konstitusion təminatların tətbiq sahəsini genişləndirir. Normativ səviyyələr arasında aydın koordinasiya olmadıqda müdaxilənin həddinin qeyri-müəyyən qalması, məlumatların emalı məqsədinin geniş şərh edilməsi və prosessual təminatların maddi hüquqla uzlaşmaması kimi risklər yarana bilər. Bu isə hüquqi müəyyənliyin zəifləməsinə və fundamental hüquqların müdafiəsində sistemli boşluqların formalaşmasına səbəb ola bilər. Xüsusilə rəqəmsal mühitdə məlumatın eyni zamanda həm sübut, həm də fərdi məlumat kimi qiymətləndirilməsi onun hüquqi rejiminin dəqiqləşdirilməsini zəruri edir. Əks halda istintaq orqanları tərəfindən tətbiq edilən mexanizmlər məlumatların qorunması rejimindən kənar qalmaq riski daşıya bilər. Bu vəziyyət konstitusion səviyyədə hüquqların müdafiəsi ilə dövlətin təhlükəsizlik funksiyası arasında uzlaşmanın təmin olunmasının vacibliyini göstərir. Məhz bu səbəbdən informasiya və fərdi məlumatlara dair normativ aktların analizi rəqəmsal istintaq səlahiyyətlərinin konstitusion əsaslandırılmasının ayrılmaz hissəsidir. Bu təhlil maddi hüquq, prosessual mexanizmlər və məlumatların qorunması rejimi arasında sistemli uyğunluğun təmin olunub-olunmadığını müəyyən etməyə imkan verir və rəqəmsal suverenliyin konstitusion çərçivədə necə realizə olunduğunu aydınlaşdırır.

Göründüyü kimi, normativ aktlar arasında sistemli əlaqələndirmənin gücləndirilməsi çox mühüm istiqamətdir. İnformasiya təhlükəsizliyi, fərdi məlumatların qorunması və cinayət-prosessual mexanizmlər arasında funksional uyğunluq təmin edilmədikdə, maddi hüquqla prosessual mexanizmlər arasında disbalans yarana bilər. Bu isə istintaq səlahiyyətlərinin tətbiqində qeyri-vahid praktika və fundamental hüquqlara müdaxilə riskinin artması ilə nəticələnə bilər. Rəqəmsal transformasiya şəraitində məlumatların texnoloji xüsusiyyətləri hüquqi tənzimləmənin statik deyil, çevik və adaptiv olmasını zəruri edir. Süni intellekt sistemləri, avtomatlaşdırılmış emal və böyük verilənlər mühiti istintaq fəaliyyətinin həm metodologiyasını, həm də hüquqi qiymətləndirmə meyarlarını yenidən düşünməyi tələb edir.

Bu kontekstdə müəlliflərdən Hildebrandt vurğulayır ki, hüquqi təminatlar yalnız normativ mətn səviyyəsində qalmamalı, alqoritmlərin daxili məntiqinə inteqrasiya olunmalıdır. Süni intellekt əsaslı istintaq alətləri tətbiq edildikdə, hüquq bu prosesə kənardan nəzarətlə kifayətlənə bilməz və birbaşa texniki arxitekturaya daxil edilməlidir. Şəxsi həyatın toxunulmazlığı və ya təqsirsizlik prezumpsiyası kimi əsas prinsiplər elə bir formaya salınmalıdır ki, alqoritmin özü bu məhdudiyyətləri daxili texniki maneə kimi qəbul etsin. Çünki rəqəmsal mühitdə fərdlər normalardan daha çox kodlar tərəfindən təsirə məruz qalır. Bu fərqi parkın girişinə "otun üzərinə çıxmaq qadağandır" lövhəsinin vurulması (norma əsaslı hüquq) ilə otluğun ətrafına keçilməz hasarın çəkilməsi (kod əsaslı hüquq) misalı ilə müqayisə etmək olar. Sonuncu halda parkın arxitekturası qaydanın pozulmasını fiziki olaraq mümkünsüz edir və hüquqi qorumanı bir növ avtomatlaşdırır.

Bununla da müəlliflər hesab edirlər ki, rəqəmsal mühitdə hüquqi müdafiə deklarativ deyil, funksional xarakterdə olmalıdır. Rəqəmsal mühitin sürəti və intensivliyi şəraitində hüquqi nəzarət yalnız insan amili ilə effektiv təmin olunmadığından, konstitusion prinsiplər texnoloji sistemlərin arxitekturasında da əksini tapmalıdır. Bu yanaşma doktrinada “kod əsaslı tənzimləmə” (code-based regulation) kimi xarakterizə olunur. Məsələn, istintaq orqanlarının istifadə etdiyi proqram təminatı elə qurula bilər ki, müvafiq məhkəmə qərarı sistemə elektron qaydada daxil edilmədən məlumatlara çıxış texniki olaraq mümkünsüz olsun. Lakin nəzərə alınmalıdır ki, kod insan səhvlərini minimuma endirmək və normativ tələblərin icrasını avtomatlaşdırmaq baxımından effektiv vasitə olsa da, onun dizaynı və tətbiqi üzərində hüquqi nəzarət mütləqdir. Əks halda texnoloji həllərin özləri şəffaflıq problemləri, alqoritmik qərəzlilik və ya hüquqların həddindən artıq məhdudlaşdırılması kimi yeni risklər yarada bilər.

Bu şəraitdə normativ aktlar arasında sistemli uyğunluğun təmin edilməsi və prosedur dəqiqləşdirmələrin aparılması uzunmüddətli konstitusion sabitlik üçün mühüm əhəmiyyət kəsb edir. Belə yanaşma dövlətin təhlükəsizlik funksiyasının ef-

fektiv icrasını hüquqi dövlət prinsipi ilə uzlaşdırır və rəqəmsal mühitdə istintaq səlahiyyətlərinin davamlı və proqnozlaşdırıla bilən əsaslarla həyata keçirilməsinə imkan yaradır.

Müəlliflər belə nəticəyə gəlirlər ki, rəqəmsal mühitdə istintaq səlahiyyətlərinin konstitusion əsaslandırılması üç fundamental elementə söykənməlidir:

Qanunilik – müdaxilə açıq normativ əsasla müəyyən olunmalıdır;

Məhkəmə nəzarəti və prosedur təminatı – fundamental hüquqlara müdaxilə institusional nəzarət altında həyata keçirilməlidir;

Mütənasiblik – müdaxilə vahid məqsədə uyğun və zəruri həddə olmalıdır.

Bu çərçivə rəqəmsal mühitdə dövlətin təhlükəsizlik funksiyasını konstitusion legitimliklə birləşdirir. Azərbaycan modelində rəqəmsal sahə ayrıca fövqəladə hüquqi zona kimi deyil, mövcud konstitusion sistemin davamı kimi qəbul olunur. Bu isə rəqəmsal istintaq səlahiyyətlərinin tətbiqini hüquqi dövlət prinsipi daxilində saxlayır və normativ sabitliyi təmin edir.

Rəqəmsal istintaq üzrə beynəlxalq hüquqi modelin əsas cəhətləri

Rəqəmsal mühitdə istintaq səlahiyyətlərinin legitimliyi artıq yalnız milli hüquq sistemi ilə müəyyən edilmir. Kibercinayətlərin transmilli xarakteri, məlumatların sərhədlərarası hərəkəti və bulud infrastrukturlarının qlobal yerləşməsi dövlətlərin istintaq səlahiyyətlərini beynəlxalq hüquqi mexanizmlərlə uzlaşdırmasını zəruri etmişdir [51]. Bu kontekstdə beynəlxalq hüquqi çərçivə üç əsas istiqamət üzrə formalaşmışdır: cinayət-hüquqi harmonizasiya, transmilli sübut mübadiləsi və fundamental hüquqların qorunması.

Beynəlxalq səviyyədə rəqəmsal mühitin istintaq səlahiyyətlərinin müəyyən edilməsində ilk sistemli sənədlərdən başlıcası 2001-ci ildə qəbul edilmiş və Avropa Şurasının təşəbbüsü ilə hazırlanmış "Kibercinayətkarlıq haqqında" Budapeşt Konvensiyası hesab edilir. Konvensiya Azərbaycan Respublikasının 2009-cu il 30 sentyabr tarixli 874-IIIQ nömrəli Qanunu ilə ratifikasiya edilmişdir. Konvensiyanın ən mühüm elementi istintaq səlahiyyətlərinə dair xüsusi prosedur normalarının müəyyən edilməsidir. Buraya elektron məlumatların sürətli qorunması, şəbəkə (trafik) məlumatlarının saxlanılması, kompüter sistemlərinə çıxış və məlumatların real vaxt rejimində əldə edilməsi kimi mexanizmlər daxildir. Bu yanaşma rəqəmsal sübutların sürətlə dəyişdirilə və ya silinə bilən xarakterini nəzərə alaraq operativ və preventiv istintaq ehtiyaclarını təmin etməyə yönəlmişdir.

Eyni zamanda Konvensiya fundamental hüquqlara hörmət prinsipini ayrıca vurğulayır və müdaxilə tədbirlərinin milli hüquq sistemlərində qüvvədə olan insan hüquqları və konstitusion təminatlarla uyğunlaşdırılmasını tələb edir. Bu müddəa istintaq alətlərinin tətbiqini iştirakçı dövlətlərin daxili hüquqi standartları ilə əlaqələndirir və onların icrasını konstitusion nəzarət müstəvisinə daxil edir. Nəticədə beynəlxalq səviyyədə prosedur çərçivə müəyyən edilir, lakin həmin tədbirlərin hüquqi sərhədlərinin konkretləşdirilməsi milli hüquq sistemləri vasitəsilə həyata keçirilir. Rəqəmsal sübutların transmilli mübadiləsi istintaq fəaliyyətində iki əsas çətinlik yaradır. Məlumatın saxlandığı yer, xidmət təminatçısının yerləşdiyi ölkə və istintaq aparan dövlətin səlahiyyət dairəsi çox vaxt eyni olmur. Bu, ərazi prinsipinə əsaslanan klassik mexanizmlərin rəqəmsal mühitdə tətbiqini mürəkkəbləşdirir. Digər tərəfdən elektron məlumatların dəyişkən və tez silinə bilən xarakteri qarşılıqlı hüquqi yardım prosedurlarının zaman baxımından gecikməsi ilə uyğunlaşmır və sübutun qorunması risk altına düşür.

Konvensiya bu riskləri nəzərə alaraq, sübutun ilkin mərhələdə qorunmasına yönəlmiş hüquqi alətlər təqdim edir. "Sürətli qorunma" mexanizmi elektron məlumatın dərhal təqdim edilməsinə deyil, onun mövcud vəziyyətinin saxlanılmasına yönəlir. Bu tədbirin hüquqi mahiyyəti sübutun dəyişdirilməsi və ya silinməsi ehtimalının qarşısını almaq məqsədilə məlumatın müəyyən müddət ərzində qorunmasını təmin etməkdən ibarətdir. Məlumatın istintaq orqanına ötürülməsi isə ayrıca prosessual qərar və müvafiq hüquqi əsas tələb edir. Bu baxımdan sürətli qorunma sübutun əldə edilməsindən əvvəl tətbiq olunan təminat xarakterli tədbir kimi qiymətləndirilir və sonrakı müdaxilə mərhələsinin hüquqi əsasını formalaşdırır.

Konvensiyanın sonrakı inkişaf mərhələsi olan İkinci Əlavə Protokol isə transmilli sübut müba-

diləsinin sürətləndirilməsinə yönəlmişdir. Bu Protokol elektron sübutlara çıxış üçün birbaşa və operativ mexanizmlər təqdim edir və klassik qarşılıqlı hüquqi yardım modelinin ləngliyini aradan qaldırmağa çalışır. Mövcud dəyişiklik istintaq səlahiyyətinin beynəlxalq tətbiq mexanizmini daha funksional və çevik formaya gətirir. Normativ baxımdan İkinci Əlavə Protokol suverenliyin tətbiq modelini yenidən şərh edir. Dövlətlər formal ərazi hakimiyyətindən imtina etmədən sübut mübadiləsində birbaşa əməkdaşlıq mexanizmlərinə razılıq verirlər. Bu, suverenliyin zəifləməsi deyil, onun koordinasiyalı və qarşılıqlı etimada əsaslanan tətbiqidir. Beləliklə, rəqəmsal istintaq artıq tək dövlət aktı deyil, çoxtərəfli normativ sistemin elementi kimi formalaşır. Eyni zamanda Protokol fundamental hüquqların qorunması mexanizmlərinə xüsusi istinad edir və müdaxilələrin mütənasiblik və qanunilik prinsipləri ilə uyğunlaşdırılmasını tələb edir. Bu isə göstərir ki, beynəlxalq səviyyədə istintaq səlahiyyətinin genişləndirilməsi paralel olaraq hüquqi təminat mexanizmlərinin də gücləndirilməsini zəruri edir.

Son dövrlərdə beynəlxalq hüquqi çərçivənin inkişafı yalnız regional mexanizmlərlə məhdudlaşmayaraq, daha geniş çoxtərəfli platformaya keçid etmişdir. Bu istiqamətdə BMT səviyyəsində 2024-cü ildə qəbul edilmiş "Kibercinayətkarlığa qarşı" Konvensiya rəqəmsal mühitdə cinayətkarlıqla mübarizə və elektron sübutlara çıxış məsələlərinin qlobal miqyasda vahid hüquqi yanaşma əsasında tənzimlənməsi tendensiyasını əks etdirir. Bu sənəd transmilli cinayətlərin araşdırılması zamanı elektron sübutların toplanması, qorunması və dövlətlərarası mübadiləsi ilə bağlı mexanizmlərin universal hüquqi çərçivədə formalaşdırılmasına yönəlmişdir və bununla da rəqəmsal istintaq fəaliyyətinin yalnız regional əməkdaşlıq alətləri ilə deyil, daha geniş normativ sistem daxilində həyata keçirilməsinin əhəmiyyətini göstərir. Bu kontekstdə Azərbaycan Respublikasının Konvensiyanın hazırlanması və qəbul edilməsi prosesində fəal iştirak etməsi, eləcə də onu ilkin mərhələdə ratifikasiya edən dövlətlər sırasında yer alması rəqəmsal mühitdə hüquqi tənzimləmənin inkişafına yönəlmiş çoxtərəfli əməkdaşlıq modelinə inteqrasiyanın göstəricisi kimi qiymətləndirilə bilər. Bu yanaşma milli hüquq sisteminin beynəlxalq standartlarla uyğunlaşdırılması ilə yanaşı, transmilli istintaq fəaliyyətinin həyata keçirilməsində hüquqi koordinasiyanın gücləndirilməsinə xidmət edir.

Eyni zamanda BMT-nin Narkotiklər və Cinayətkarlığa qarşı Mübarizə Ofisinin (UNODC) sənədlərində vurğulanır ki, kiberməkanda məlumatlara çıxış digər dövlətlərin suveren hüquqlarına müdaxilə riskini daşıyır və buna görə də beynəlxalq əməkdaşlıq mexanizmləri əsas rol oynayır. Bu, konstitusion baxımdan dövlətin istintaq səlahiyyətlərini həyata keçirərkən beynəlxalq hüquqi öhdəlikləri nəzərə almalı olduğunu göstərir. Belə düşünülə bilər ki, rəqəmsal istintaq fəaliyyəti ikiqat legitimlik tələb edir: daxili konstitusion legitimlik; beynəlxalq hüquqi uyğunluq. Əgər bu iki səviyyə arasında tarazlıq qorunmazsa, dövlətin rəqəmsal istintaq fəaliyyəti hüquqi mübahisə predmetinə çevrilə bilər.

Rəqəmsal mühitdə cinayətlərin istintaqının effektiv aparılması Avropa İttifaqında da klassik ərazi prinsipinin yenidən şərhini zəruri etmişdir. Belə ki, 2023-cü ildə qəbul edilmiş 1543 saylı Reqlament (Regulation (EU) 2023/1543) kibercinayətlərin istintaqında elektron sübutların əldə olunması və qorunması üçün Avropa Qoruma Mexanzimləri kimi tanınan (European Production Order; European Preservation Order) hüquqi alətləri müəyyən etmişdir. Bu mexanizm vasitəsilə bir üzv dövlətin səlahiyyətli orqanı digər üzv dövlətdə fəaliyyət göstərən xidmət təminatçısından birbaşa elektron məlumat tələb edə bilir. Beləliklə, sübutun fiziki yerləşdiyi ərazi istintaqın hüquqi imkanlarını məhdudlaşdıran əsas faktor olmaqdan çıxır. Bu tənzimləmə normativ baxımdan istintaq səlahiyyətinin operativ institusionallaşdırılması kimi qiymətləndirilə bilər. Ərazi prinsipinin klassik sərhədləri qorunmaqla yanaşı, qarşılıqlı tanınma və etimad prinsipi əsas mexanizmə çevrilir. Üzv dövlətlərin qərarları əlavə diplomatik təsdiq mexanizmi olmadan icra edilir. Bu tənzimləmə istintaq səlahiyyətinin yalnız milli çərçivədə deyil, Avropa İttifaqı daxilində qarşılıqlı tanınma prinsipi əsasında həyata keçirildiyini göstərir.

Reqlament məlumatın növünə görə fərqli müdaxilə səviyyələri müəyyən edir və bəzi hallarda məhkəmə nəzarətini tələb edir. Belə ki, Avropa İttifaqı modelində məlumat növləri arasında normativ diferensiasiya xüsusi əhəmiyyət kəsb edir.

Hüquqi tənzimləmədə şəbəkə (trafik) məlumatları, abunəçi məlumatları və məzmun məlumatları eyni müdaxilə səviyyəsində qiymətləndirilmir. Şəbəkə (trafik) məlumatları əlaqənin vaxtı, müddəti və istiqaməti kimi texniki göstəriciləri əhatə edir, abunəçi məlumatları istifadəçinin identifikasiya məlumatlarını müəyyən edir, məzmun məlumatları isə kommunikasiya və yazışmanın birbaşa məzmununu təşkil edir. Bu kateqoriyalar arasında fərq yalnız texniki xarakter daşımır, müdaxilənin konstitusion intensivliyini müəyyən edən hüquqi meyar kimi çıxış edir. Məzmun məlumatları şəxsi həyatın toxunulmazlığı və yazışma sirri ilə birbaşa bağlı olduğu üçün daha yüksək səviyyədə müdaxilə hesab edilir və buna uyğun olaraq daha ciddi əsaslandırma və nəzarət mexanizmləri tələb edir. Digər tərəfdən, şəbəkə (trafik) və abunəçi məlumatları üzrə müdaxilə səviyyəsi daha diferensial qiymətləndirilir. Bu yanaşma istintaqın operativliyini zəiflətmədən müdaxilənin mütənasibliyini məlumatın xarakterinə uyğun şəkildə təmin etməyə yönəlmişdir.

Eyni paket daxilində qəbul edilmiş 1544 saylı Direktiv xidmət təminatçıları üçün konkret hüquqi öhdəliklər müəyyən edir və onların Avropa İttifaqı daxilində hüquqi nümayəndə təyin etməsini tələb edir. Bu tənzimləmə 2023-cü il tarixli 1543 saylı Reqlamentlə nəzərdə tutulan Avropa təqdimetmə qərarı və Avropa qoruma qərarının icrasını təmin edən hüquqi əsasları möhkəmləndirir. Hüquqi mahiyyət baxımından Avropa təqdimetmə qərarı səlahiyyətli orqan tərəfindən qəbul edilən və digər üzv dövlətdə fəaliyyət göstərən xidmət təminatçısına birbaşa ünvanlanan məcburi hüquqi göstərişdir. Bu qərar müəyyən elektron məlumatın təqdim edilməsini tələb edir və qarşılıqlı tanınma prinsipi əsasında icra olunur. Avropa qoruma qərarı isə məlumatın dərhal ötürülməsini deyil, onun müəyyən müddət ərzində saxlanılmasını təmin edən prosessual təminat tədbiridir. Bu qərarın məqsədi sübutun dəyişdirilməsi və ya silinməsi ehtimalının qarşısını almaqdır. Hər iki halda xidmət təminatçısı hüquqi öhdəlik daşıyan subyekt kimi çıxış edir və qərarın icrası normativ əsasla təmin olunur. Bu yanaşma istintaq səlahiyyətinin tətbiq sahəsini genişləndirərək xidmət təminatçılarını hüquqi münasibətin birbaşa tərəfinə çevirir və rəqəmsal mühitdə sübuta çıxış prosesini dövlət və özəl subyektlərin iştirak etdiyi vahid hüquqi sistem daxilində təşkil edir. Nəticə etibarilə Avropa İttifaqının elektron sübut modeli istintaq səlahiyyətinin həyata keçirilməsini çoxsəviyyəli hüquqi münasibətlər müstəvisində qurur və rəqəmsal mühitdə səlahiyyətin realizə formasını struktur baxımından yenidən müəyyənləşdirir.

Bu iki tənzimləmə birlikdə Avropa İttifaqında rəqəmsal istintaqın çoxsəviyyəli modelini formalaşdırır. Bir tərəfdən operativ və birbaşa sübut əldə etmə mexanizmi yaradılır, digər tərəfdən isə fundamental hüquqların qorunması və institusional nəzarət mexanizmləri saxlanılır. Bu yanaşma rəqəmsal mühitdə istintaq səlahiyyətlərinin konstitusion əsaslandırılmasının Avropa modeli kimi qiymətləndirilə bilər.

Məhkəmə praktikası isə göstərir ki, dövlətin rəqəmsal mühitdə məlumat toplama və elektron sübut əldə etmə səlahiyyəti legitimdir, lakin bu legitimlik hüquqi dövlət prinsipi və fundamental hüquqlar sistemi ilə uzlaşdırılmış şəkildə həyata keçirilməlidir.

Hələ ötən əsrin 70-ci illərində İnsan Hüquqları üzrə Avropa Məhkəməsində baxılan "Klass və digərləri Almaniyaya qarşı" işində açıq şəkildə bildirilmişdir ki, demokratik cəmiyyətdə gizli nəzarət tədbirləri tamamilə istisna edilə bilməz. Dövlət təhlükəsizlik funksiyasını həyata keçirərkən müəyyən hallarda məxfi istintaq vasitələrinə müraciət edə bilər. Sonrakı illərdə rəqəmsal mühitin inkişafı bu cür presedent yanaşmasının oxşar işlərdə də tətbiqini zəruri hala gətirdi. Məsələn, 2015-ci il tarixli "Zakharov Rusiyaya qarşı" işində kommunikasiya nəzarətinə dair mühüm prinsip müəyyən edildi: dövlət təhlükəsizlik və cinayətkarlıqla mübarizə məqsədilə gizli nəzarət mexanizmləri tətbiq edə bilər, lakin bu mexanizmlər aydın normativ baza, prosedur təminatlar və effektiv nəzarət mexanizmi ilə müşayiət olunmalıdır. Məhkəmə burada dövlət səlahiyyətini inkar etməyərək onun hüquqi çərçivədə həyata keçirilməsinin zəruriliyini vurğulamışdır. "Szabó və Vissy Macarıstana qarşı" və "Big Brother Watch və digərləri Birləşmiş Krallığa qarşı" işləri bu yanaşmanı daha da inkişaf etdirmişdir. Xüsusilə Böyük Palatanın qərarında Məhkəmə genişmiqyaslı məlumat toplama mexanizmlərini tam şəkildə qadağan etməmiş, lakin çoxsəviyyəli təminatlar mo-

delini tələb etmişdir. Bu modelə normativ əsas, icra mərhələsində prosedur nəzarəti və sonradan məhkəmə baxışı daxildir. Bu yanaşma göstərir ki, məsələ istintaq səlahiyyətinin mövcudluğu deyil, onun düzgün konstitusion meyarlarla təmin edilməsidir.

Bundan başqa, "Bărbulescu Rumıniyaya qarşı" işində məhkəmə rəqəmsal kommunikasiya üzərində nəzarətin şəxsin məxfilik gözləntisi ilə uzlaşdırılması məsələsinə toxunmuşdur. Qərar göstərir ki, rəqəmsal yazışmalar müasir hüquq sistemində konstitusion qorunan sahəyə daxildir. Bu presedent istintaq səlahiyyətinin tətbiqində məxfilik hüququnun nəzərə alınmasının zəruri olduğunu təsdiq edir. Dövlətin təhlükəsizlik və cinayət təqibi məqsədi legitimdir, lakin müdaxilə ölçülü və əsaslandırılmış olmalıdır. Avropa İttifaqı Ədalət Məhkəməsinin Digital Rights Ireland işi, Tele2 Sverige işi və La Quadrature du Net işi işləri məlumatların kütləvi saxlanılması və istifadə mexanizmlərinin hüquqi sərhədlərini müəyyən etmişdir. Bu qərarlar dövlətin ağır və xüsusilə ağır cinayətlərlə mübarizə və milli təhlükəsizlik məqsədilə məlumat saxlamasını prinsip etibarilə legitim hesab edir, lakin belə tədbirlərin ümumi və qeyri-məhdud xarakter almamasını tələb edir. Burada əsas meyar məqsədlə müdaxilə arasında rasional əlaqənin mövcudluğu və konkretləşdirilmiş tətbiq mexanizminin təmin edilməsidir.

"Demirhan və digərləri Türkiyəyə qarşı" işində Məhkəmə rəqəmsal sübutların məhkəmə prosesində istifadəsi zamanı müdafiə hüququnun təmin olunmasına xüsusi diqqət yetirmişdir. Qərar göstərir ki, istintaq mərhələsində əldə edilmiş elektron məlumatların məhkəmə baxışında istifadəsi yalnız onların yoxlanıla bilməsi və müdafiə tərəfinə real çıxış imkanının təmin edilməsi şərti ilə konstitusion standartlara uyğun hesab edilə bilər. Bu yanaşma istintaq səlahiyyətinin son mərhələdə ədalətli məhkəmə hüququ ilə əlaqələndirilməsini təmin edir.

İnsan Hüquqları üzrə Avropa Məhkəməsinin presedentlərinin təhlili göstərir ki, rəqəmsal mühitdə istintaq orqanlarının səlahiyyət həddi konstitusion meyarlar əsasında qiymətləndirilir və məhkəmə praktikası hüquqi dövlət çərçivəsində balanslaşdırılmış yanaşma təqdim edir. Dövlətin təhlükəsizlik funksiyası qorunur, onun həyata keçirilməsi fundamental hüquqlar sistemi ilə uzlaşdırılır və hüquqi nəzarət mexanizmləri ilə müşayiət olunur. Transmilli elektron sübutlara birbaşa çıxış mexanizmləri və rəqəmsal məlumatların dövlətlərarası mübadiləsinin yeni formaları nisbətən son dövrün normativ inkişafının nəticəsidir və bu sahədə formalaşmış geniş məhkəmə praktikası hələ tam mövcud deyil. Bununla belə, rəqəmsal məlumatlara müdaxilə ilə bağlı tətbiq olunan konstitusion meyarlar transmilli tədbirlərin qiymətləndirilməsində də istifadə olunur.

Beləliklə, beynəlxalq hüquqi təcrübə göstərir ki, rəqəmsal mühitdə istintaq səlahiyyəti müasir cinayətkarlıqla mübarizənin zəruri alətidir. Elektron sübutların artması və transsərhəd məlumat axını dövlətlərin klassik istintaq mexanizmlərini yenidən qurmasını zəruri etmişdir. Bu zərurət hüquqi sistemlərdə istintaq səlahiyyətinin ləğvinə deyil, onun daha dəqiq və sistemli şəkildə tənzimlənməsinə gətirib çıxarmışdır. Dövlətin təhlükəsizlik və cinayət təqibi funksiyası legitim məqsəd kimi qəbul olunur. Lakin bu səlahiyyət aydın normativ əsas, məqsədyönlü tətbiq və effektiv nəzarət mexanizmi ilə müşayiət olunmalıdır. Rəqəmsal mühitdə konstitusion legitimlik bu üç elementin vəhdəti ilə təmin edilir.

Nəticə və təkliflər

Rəqəmsal mühitdə istintaq səlahiyyətlərinin müqayisəli təhlili göstərir ki, fərqləndirici amil normativ bazanın həcmi və ya texniki xüsusiyyətlərdən daha çox, bu səlahiyyətlərin hansı hüquqi çərçivə daxilində əsaslandırılması ilə bağlıdır. Elektron sübutun hüquqi statusu, transmilli məlumatlara çıxış mexanizmləri və fundamental hüquqların prosedur təminatı bu çərçivənin legitimlik əsaslarını formalaşdıran başlıca komponentlər kimi çıxış edir.

Azərbaycan Respublikasında rəqəmsal istintaq mövcud konstitusion və prosessual sistem daxilində inkişaf etmişdir və ayrıca müstəqil hüquqi rejim kimi deyil, ümumi istintaq mexanizminin tərkib hissəsi kimi tətbiq olunur. Bu yanaşma normativ ardıcıllığın qorunmasına, hüquqi sabitliyin təmin olunmasına və konstitusion prinsiplərin vahid tətbiqinə imkan yaradır. Eyni zamanda beynəlxalq və Avropa təcrübəsində rəqəmsal mühit üzrə pro-

sedur mexanizmlərinin daha strukturlaşdırılmış şəkildə formalaşdırıldığı müşahidə olunur. Elektron sübutların əldə olunması, saxlanılması və transmilli mübadiləsi ilə bağlı xüsusi hüquqi alətlərin mövcudluğu istintaq fəaliyyətinin operativliyini artırmaqla yanaşı, fundamental hüquqların müdafiəsini daha konkret prosedur çərçivəsində təmin edir.

Aparılan müqayisə göstərir ki, müxtəlif yanaşmalar eyni hüquqi prinsiplərə əsaslansa da, onların normativ ifadə forması və tətbiq intensivliyi müəyyən fərqlər göstərir. Azərbaycan modeli mövcud hüquqi çərçivəyə və son normativ inkişaflara əsaslanaraq, rəqəmsal istintaqın həyata keçirilməsini ümumi hüquqi sistem daxilində təmin edir, beynəlxalq yanaşmada isə bu prinsiplər daha detallı prosedur mexanizmlərlə konkretləşdirilir. Hər iki halda məqsəd hüquqi dövlət prinsipi çərçivəsində təhlükəsizlik maraqları ilə fundamental hüquqlar arasında tarazlığın qorunmasıdır.

Nəticə etibarilə rəqəmsal mühitdə istintaq səlahiyyətlərinin konstitusion əsaslandırılması təhlükəsizlik funksiyası ilə fundamental hüquqlar arasında qarşıdurma deyil, onların uzlaşdırılmasını nəzərdə tutan hüquqi mexanizmlər sistemi kimi çıxış edir. Bu kontekstdə Azərbaycan Respublikasında formalaşmış yanaşma mövcud konstitusion çərçivə daxilində hüquqi sabitliyin qorunmasına yönəlmişdir və onun gələcək inkişafının da bu prinsiplər əsasında davam etdirilməsi məqsədəuyğun hesab edilə bilər.

Məhz bu çərçivədə rəqəmsal istintaq mexanizminin daha da dəqiqləşdirilməsi məqsədilə bir sıra inkişaf istiqamətləri və təkliflər irəli sürülə bilər.

1. Elektron sübutların tətbiqi və məhkəmədə qiymətləndirilməsi üzrə vahid metodoloji çərçivənin hazırlanması – cinayət-prosessual qanunvericiliyə edilmiş son dəyişikliklər elektron sübutların hüquqi statusunu və onların əldə olunması ilə bağlı əsas mexanizmləri müəyyən etməklə rəqəmsal mühitdə istintaq fəaliyyətinin normativ əsaslarını gücləndirmişdir. Bununla yanaşı, elektron sübutların əldə olunması, surətinin çıxarılması, saxlanılması və autentifikasiyası üzrə prosedurların vahid metodoloji yanaşma əsasında konkretləşdirilməsi onların etibarlılığını və tətbiq vahidliyini artırmaqla yanaşı, müdaxilənin hüquqi əsaslarının daha şəffaf və proqnozlaşdırıla bilən şəkildə müəyyən edilməsinə xidmət edir. Bu çərçivədə məlumatların bütövlüyünün qorunması, əldə olunma ardıcıllığının sənədləşdirilməsi və saxlanma prosesinin izlənilə bilənliyinin təmin edilməsi əsas elementlər kimi çıxış edir. Rəqəmsal sübutların məhkəmə mərhələsində qiymətləndirilməsi isə müdafiə tərəfinin həmin sübutun əldə olunma qaydasını və texniki xüsusiyyətlərini yoxlamaq, ona etiraz etmək və zəruri hallarda alternativ ekspertiza tələb etmək imkanları ilə təmin olunmalıdır ki, bu da sübutların obyektiv qiymətləndirilməsi, prosessual balansın qorunması və hüquqi müəyyənliyin təmin edilməsi üçün zəruri şərtdir. Bütün bunlar rəqəmsal sübutlarla bağlı prosedur mexanizmlərin yalnız texniki və prosessual deyil, eyni zamanda konstitusion təminatların realizə olunduğu kompleks hüquqi çərçivə kimi formalaşdırılmasını zəruri edir.

2. Rəqəmsal məlumatlara çıxış üzrə diferensial müdaxilə modelinin formalaşdırılması – qanunvericiliyə edilmiş son dəyişikliklər nəticəsində CPM-də elektron verilənlərin müxtəlif kateqoriyalar üzrə (xüsusilə trafik, abunəçi və məzmun məlumatları) fərqləndirilməsi üçün hüquqi əsas formalaşmışdır. Bununla belə, rəqəmsal mühitdə bütün məlumat növləri eyni hüquqi mahiyyətə və eyni dərəcədə məxfilik həssaslığına malik deyil. Bu baxımdan şəbəkə (trafik) məlumatları (əlaqənin vaxtı, davametmə müddəti və istiqaməti barədə texniki göstəricilər), abunəçi məlumatları (istifadəçinin identifikasiya və qeydiyyat məlumatları) və məzmun məlumatları (kommunikasiyanın birbaşa məzmunu) arasında normativ fərqləndirmənin aparılması məqsədəuyğun hesab oluna bilər. Bu bölgü yalnız texniki təsnifat deyil, müdaxilənin hüquqi intensivliyini müəyyən edən meyar kimi çıxış edir.

Məzmun məlumatları birbaşa şəxsi həyatın və yazışma sirrinin mahiyyətinə toxunduğu üçün daha yüksək müdaxilə səviyyəsi hesab oluna bilər. Şəbəkə (trafik) və abunəçi məlumatları isə dolayısı ilə şəxsi sferaya təsir göstərsə də, onların məxfilik dərəcəsi fərqli qiymətləndirilə bilər. Bu səbəbdən məlumat növünə uyğun olaraq məhkəmə icazəsinin şərtlərinin, nəzarət mexanizmlərinin və əsaslandırma standartlarının normativ səviyyədə konkretləşdirilməsi müdaxilənin mütənasibliyini daha aydın çərçivəyə sala bilər. Belə diferensial model bir tərəfdən istintaqın operativliyini təmin etməyə

imkan verər, digər tərəfdən isə daha həssas məlumatlara münasibətdə konstitusion təminatların gücləndirilməsini təmin edər. Nəticədə müdaxilə ilə hüquqi nəzarət arasında daha balanslı və proqnozlaşdırıla bilən mexanizm formalaşar ki, bu da həm hüquqi müəyyənliyi artırar, həm də istintaq səlahiyyətlərinin legitimliyini möhkəmləndirər.

3. Transmilli fəaliyyət üzrə operativ prosedur çərçivənin dəqiqləşdirilməsi – kibercinayətlərin transmilli xarakteri nəzərə alındıqda, elektron sübutların əldə olunmasında vaxt amili xüsusi əhəmiyyət kəsb edir. Mövcud normativ çərçivədə elektron məlumatların qorunması və təqdim edilməsi ilə bağlı mexanizmlər nəzərdə tutulsa da, onların tətbiq ardıcıllığının və operativlik səviyyəsinin daha aydın prosedur qaydalarla konkretləşdirilməsi praktik baxımdan faydalı ola bilər. Xüsusilə məlumatın silinməsi və ya dəyişdirilməsi riskinin mövcud olduğu hallarda tətbiq edilən qoruma tədbirlərinin prosedur çərçivəsinin daha dəqiq müəyyən edilməsi məqsədəuyğun ola bilər. Bu tədbirlərin məlumatın dərhal qorunmasını təmin edən, lakin onun təqdim edilməsini ayrıca hüquqi prosedurla şərtləndirən mexanizm kimi strukturlaşdırılması istintaqın operativliyini artırmaqla yanaşı, sonrakı mərhələdə məhkəmə nəzarətinin təmin olunmasına da imkan yaradır. Eyni zamanda elektron sübutlarla bağlı beynəlxalq sorğular üzrə prosedur mərhələlərinin və cavab müddətlərinin daha konkret müəyyən edilməsi, o cümlədən sorğunun qəbul edilməsi, icraya götürülməsi və nəticənin təqdim edilməsi proseslərinin ardıcıllığının normativ səviyyədə dəqiqləşdirilməsi hüquqi müəyyənliyin gücləndirilməsinə töhfə verə bilər. Bu yanaşma operativlik ilə hüquqi nəzarət arasında balansın daha effektiv şəkildə təmin olunmasına xidmət edir.

4. Elektron cinayət təqibində texnoloji proseslər üzərində hüquqi nəzarətin həyata keçirilməsi – rəqəmsal mühitdə istintaq fəaliyyəti yalnız hüquqi qərarların qəbul edilməsi ilə məhdudlaşmır. Bu fəaliyyət məlumatların toplanması, seçilməsi və təhlili kimi mərhələləri əhatə edən texnoloji proseslər vasitəsilə həyata keçirilir. Məlumatlar proqram təminatları vasitəsilə emal olunur, müəyyən meyarlar üzrə seçilir və analiz edilir. Bu proseslər istintaqın nəticəsinə birbaşa təsir göstərir. Buna görə nəticə yalnız hüquqi qiymətləndirmədən deyil, məlumatların necə seçildiyi və emal edildiyi ilə də müəyyən olunur. Mövcud hüquqi mexanizmlər əsasən qəbul edilən qərarların qanuniliyinə nəzarət edir. Lakin rəqəmsal mühitdə qərar artıq texnoloji mərhələlərdən keçərək formalaşır. Bu mərhələlər hüquqi baxımdan tənzimlənmədikdə, nəzarət yalnız qəbul edilmiş qərarın qiymətləndirilməsi ilə məhdudlaşır və müdaxilənin real hüdudları texniki vasitələrin işləmə qaydaları ilə müəyyən edilir. Bu səbəbdən təklif olunur ki, hüquqi nəzarət yalnız qərarın özünə deyil, onun formalaşdığı texnoloji mərhələlərə də şamil edilsin. Burada hüquqi nəzarət dedikdə müdaxilənin qanuni əsaslarının yoxlanılması ilə yanaşı, onun həyata keçirildiyi texnoloji proseslərin də hüquqi çərçivədə saxlanılması nəzərdə tutulur. Bu məqsədlə texnoloji vasitələrin tətbiqi qanuni əsaslarla əlaqələndirilməli, məhkəmə qərarı tələb olunan hallarda belə qərar olmadan avtomatlaşdırılmış müdaxilə istisna edilməli, təxirəsalınmaz hallarda isə sonradan məhkəmə nəzarəti təmin olunmalıdır. Belə yanaşma müdaxilənin sərhədlərini aydınlaşdırır, özbaşına müdaxilə riskini azaldır və hüquqi normaların real tətbiqini təmin edir. Bu model rəqəmsal suverenliyin konstitusion əsaslar çərçivəsində həyata keçirilməsinə və fundamental hüquqlar ilə istintaq səlahiyyətləri arasında balansın qorunmasına xidmət edir.

5. İnformasiya və fərdi məlumatlara dair qanunvericilik aktları ilə cinayət-prosessual mexanizmlər arasında funksional uyğunluğun dərinləşdirilməsi – rəqəmsal cinayət təqibi zamanı fərdi məlumatların emalı ilə bağlı hüquqi münasibətlərin yaranması nəzərə alınaraq, bu sahədə normativ yanaşmaların daha aydın uzlaşdırılması hüquqi müəyyənliyin təmin olunmasına xidmət edir. Xüsusilə istintaq məqsədilə əldə edilmiş məlumatların yalnız konkret cinayət işi çərçivəsində istifadəsinin hüdudlarının, həmin məlumatların saxlanılma müddətinin və sonrakı mərhələdə silinməsi və ya arxivləşdirilməsi ilə bağlı prosedurların daha konkret müəyyən edilməsi məqsədəuyğun ola bilər. Bu yanaşma sübut əhəmiyyətini itirmiş məlumatların dövriyyəsinin tənzimlənməsinə və məlumatların emalının nəzarətli şəkildə həyata keçirilməsinə imkan yaradır. Bu istiqamətdə normativ dəqiqləşdirmə məxfilik prinsipləri ilə təhlükəsizlik maraqları arasında balansın daha sistemli şəkildə qorunmasına xidmət edə bilər.

İstifadə edilmiş ədəbiyyat siyahısı:

1. Azərbaycan Respublikasının Cinayət Məcəlləsi // 30 dekabr 1999-cu ildə qəbul edilmişdir (dəyişiklik və əlavələrlə). – Bakı: Qanun, – 2024. – 520 s.
2. Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi // 14 iyul 2000-ci ildə qəbul edilmişdir (dəyişiklik və əlavələrlə). – Bakı: Qanun, – 2024. – 768 s.
3. Azərbaycan Respublikasının Konstitusiyası // 12 noyabr 1995-ci ildə qəbul edilmişdir (dəyişiklik və əlavələrlə). – Bakı: Qanun, – 2016. – 48 s.
4. "Azərbaycan Respublikasının Cinayət Məcəlləsində və Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində dəyişiklik edilməsi haqqında" Azərbaycan Respublikasının Qanunu // 3 mart 2026-cı il, № 373-VIIQD.
5. Əsgərov, Z.A. Konstitusiya hüququ. Dərslik / Z.A.Əsgərov. – Bakı: Bakı Universiteti nəşriyyatı, – 2024. – 608 s.
6. "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu // 11 may 2010-cu il, № 998-IIIQ.
7. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu // 3 aprel 1998-ci il, № 460-IQ.
8. American Law Institute. Restatement (Third) of the Foreign Relations Law of the United States. – Washington, D.C.: American Law Institute, – 1987. – 1230 p.
9. Ashworth, A., Zedner, L. Preventive Justice / A.Ashworth, L.Zedner. – Oxford: Oxford University Press, – 2014. – 312 p.
10. Barak, A. Proportionality: Constitutional Rights and Their Limitations / A.Barak. – Cambridge: Cambridge University Press, – 2012. – 638 p.
11. Bingham, T. The Rule of Law / T.Bingham. – London: Allen Lane, – 2010. – 224 p.
12. Casey, E. Digital Evidence and Computer Crime / E.Casey. – Amsterdam: Academic Press, – 2011.–704 p.
13. Cassese, A. International Criminal Law / A.Cassese. – Oxford: Oxford University Press, – 2013. – 472 p.
14. Crawford, J. Brownlie's Principles of Public International Law / J.Crawford. – Oxford: Oxford University Press, – 2019. – 872 p.
15. Fredman, S. Human Rights Transformed: Positive Rights and Positive Duties / S.Fredman. – Oxford: Oxford University Press, – 2008. – 304 p.
16. Grimm, D. Sovereignty: The Origin and Future of a Political and Legal Concept / D.Grimm. – New York: Columbia University Press, – 2015. – 240 p.
17. Hildebrandt, M. Law as Computation in the Era of Artificial Legal Intelligence // Critical Analysis of Law, – 2016. Vol. 3, No. 1, – p. 1–17.
18. Kerr, O.S. Searches and Seizures in a Digital World // Harvard Law Review, – 2005. Vol. 119, No. 2, – p. 531–585.
19. Kerr, O.S. Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data // Texas Tech Law Review, – 2015. Vol. 48, No. 1, – p. 1–35.
20. Loughlin, M. Foundations of Public Law / M.Loughlin. – Oxford: Oxford University Press,–2010.–544 p.
21. Ryngaert, C. Jurisdiction in International Law / C.Ryngaert. – Oxford: Oxford University Press, – 2015. – 256 p.
22. Sachoulidou, A. Cross-border Access to Electronic Evidence in Criminal Matters: The New EU Legislation // New Journal of European Criminal Law, – 2024. Vol. 15, No. 3, – p. 256–274.
23. Schabas, W.A. An Introduction to the International Criminal Court / W.A.Schabas. – Cambridge: Cambridge University Press, – 2017. – 576 p.
24. Schauer, F. Fear, Risk and the First Amendment: Unraveling the "Chilling Effect" // Boston University Law Review, – 1978. Vol. 58, – p. 685–732.
25. Shaw, M.N. International Law / M.N.Shaw. – Cambridge: Cambridge University Press, – 2021. – 1032 p.
26. Stoykova, R. The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations // Computer Law & Security Review, – 2023. Vol. 49, – p. 104-120.

27. Svantesson, D.J.B. Solving the Internet Jurisdiction Puzzle / D.J.B.Svantesson. – Oxford: Oxford University Press, – 2017. – 256 p.
28. Yeung, K. Algorithmic Regulation: A Critical Interrogation // The Oxford Handbook of Law, Regulation and Technology / ed. R. Brownsword, E. Scotford, K. Yeung. – Oxford: Oxford University Press, – 2020. – p. 844–873.
29. Bărbulescu v. Romania // Judgment of the European Court of Human Rights [Grand Chamber], application no. 61496/08. – Strasbourg: 2017.
30. Big Brother Watch and Others v. the United Kingdom // Judgment of the European Court of Human Rights [Grand Chamber], applications nos. 58170/13, 62322/14 and 24960/15. – Strasbourg: 2021.
31. Demirhan and Others v. Türkiye // Judgment of the European Court of Human Rights, application no. 25445/20. – Strasbourg: 2025.
32. Digital Rights Ireland Ltd v Minister for Communications // Judgment of the Court of Justice of the European Union, joined cases C-293/12 and C-594/12. – Luxembourg: 2014.
33. Klass and Others v. Germany // Judgment of the European Court of Human Rights, application no. 5029/71. – Strasbourg: 1978.
34. La Quadrature du Net and Others // Judgment of the Court of Justice of the European Union, joined cases C-511/18, C-512/18 and C-520/18. – Luxembourg: 2020.
35. Malone v. the United Kingdom // Judgment of the European Court of Human Rights, application no. 8691/79. – Strasbourg: 1984.
36. Roman Zakharov v. Russia // Judgment of the European Court of Human Rights [Grand Chamber], application no. 47143/06. – Strasbourg: 2015.
37. Szabó and Vissy v. Hungary // Judgment of the European Court of Human Rights, application no. 61496/08. – Strasbourg: 2016.
38. Tele2 Sverige AB v Post- och telestyrelsen // Judgment of the Court of Justice of the European Union, joined cases C-203/15 and C-698/15. – Luxembourg: 2016.
39. Association of Chief Police Officers (ACPO). Good Practice Guide for Digital Evidence. – London: ACPO, – 2012. – URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (last access: 20.02.2026).
40. Council of Europe. Convention on Cybercrime (ETS No.185) // Strasbourg: – 2001. – URL: https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf (last access: 27.01.2026).
41. Council of Europe. Explanatory Report to the Convention on Cybercrime // Strasbourg: – 2001. – URL: https://rm.coe.int/16800cce5b (last access: 14.02.2026).
42. Council of Europe. Second Additional Protocol to the Convention on Cybercrime // Strasbourg: – 2022. – URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol/-/asset_publisher/isHU0Xq21lhu/content/opening-coecyber2ap (last access: 14.01.2026).
43. Directive (EU) 2023/1544 of the European Parliament and of the Council. – 2023. – URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj/eng (last access: 25.02.2026).
44. European Network of Forensic Science Institutes (ENFSI). Best Practice Manual for the Forensic Examination of Digital Technology. – 2015. – URL: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf (last access: 24.02.2026).
45. ENISA. Privacy and Data Protection by Design – from policy to engineering // Heraklion: ENISA, – 2014. – 95 p.
46. International Organization for Standardization (ISO). ISO/IEC 27037:2012 Digital Evidence Guidelines. – Geneva: ISO, – 2012. – URL: https://www.iso.org/standard/44381.html (last access: 17.02.2026).
47. National Institute of Standards and Technology (NIST). Guide to Integrating Forensic Techniques into Incident Response (SP 800-86). – 2006. – URL: https://csrc.nist.gov/pubs/sp/800/86/final (last access: 28.02.2026).
48. Regulation (EU) 2023/1543 of the European Parliament and of the Council. – 2023. – URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng (last access: 12.03.2026).

49. United Nations. Charter of the United Nations // San Francisco: – 1945. – URL: https://www.un.org/en/about-us/un-charter/full-text (last access: 15.01.2026).
50. United Nations. Convention against Cybercrime // New York: – 2024. – URL: https://www.unodc.org/unodc/en/cybercrime/convention/home.html (last access: 05.03.2026).
51. UNODC. Comprehensive Study on Cybercrime // Vienna: – 2013. – URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last access: 02.03.2026).
52. Козлова, Е.И., Кутафин, О.Е. Конституционное право России: учебник / Е.И.Козлова, О.Е.Кутафин. – Москва: Норма, – 2014. – 592 с.
53. Марченко, М.Н. Теория государства и права: учебник / М.Н.Марченко. – Москва: Проспект, – 2016. – 640 с.

Constitutional Foundations of Digital Sovereignty in the Context of Cybercrime Investigation

Elshad Nasirov,
Chief of the Academy named after Heydar Aliyev of the State Security Service.
Email: elshad_nasirov@yahoo.com

Kamran Khalilov,
PhD candidate at Baku State University and Lecturer at the Heydar Aliyev Academy of the State Security Service
Email: xalilovkamran75@gmail.com

Abstract

The rapid advancement of digital technologies has fundamentally transformed the nature and scale of criminal activity, making the prevention and investigation of cybercrime one of the principal priorities of contemporary state security policy. The transnational character of cybercrime, together with the location of digital evidence across multiple jurisdictions and the cross-border exchange of electronic data, challenges the application of traditional concepts of territorial jurisdiction and necessitates the development of new legal approaches. Against this background, defining the constitutional foundations of the State's investigative powers has become a matter of particular legal significance. This article examines the constitutional framework governing the exercise of State powers in the investigation of cybercrime and provides a systematic analysis of the principal directions of legal regulation in this field. The research is based on normative and doctrinal legal analysis, supplemented by a comparative legal approach and an examination of relevant international judicial practice. Particular attention is devoted to the constitutional limits of criminal jurisdiction, mechanisms for obtaining digital evidence through international cooperation, judicial oversight of investigative measures, and the application of the principle of proportionality. The analysis demonstrates that the digital environment requires a reconceptualization of the legal mechanisms through which State sovereignty is exercised in light of evolving technological and legal realities. While the effective investigation of cybercrime constitutes an integral component of the State's constitutionally mandated security function, the exercise of investigative powers must remain consistent with the rule of law, the principle of legal certainty, and the effective protection of fundamental rights and freedoms. The scientific novelty of the study lies in the development of a constitutional framework for the exercise of investigative powers in the digital environment and in proposing a coherent legal model for the State's exercise of such powers within the context of cross-border cybercrime **i**nvestigations.

Keywords: *digital sovereignty; cybercrime investigation; constitutional framework; State sovereignty; criminal jurisdiction; digital evidence; international judicial cooperation; rule of law; legal certainty; principle of proportionality.*

Конституционные основы цифрового суверенитета в контексте расследования киберпреступлений

Эльшад Насиров,
Начальник Академии Службы Государственной Безопасности имени Гейдара Алиева.
Электронная почта: elshad_nasirov@yahoo.com

Камран Халилов,
Докторант Бакинского Государственного Университета и Преподаватель Академии Службы Государственной Безопасности имени Гейдара Алиева.
Электронная почта: xalilovkamran75@gmail.com

Резюме

Развитие цифровых технологий изменило характер и масштабы преступности, борьба с киберпреступностью стала одним из приоритетных направлений обеспечения безопасности государства. При расследовании киберпреступлений размещение доказательств на территории различных государств и международный характер обмена информацией затрудняют применение понятия традиционной территориальной юрисдикции и требуют формирования новых правовых подходов. В этих условиях особое значение имеет определение конституционных основ полномочий государства, связанных со следственной деятельностью. Целью статьи является определение конституционных рамок полномочий государства в рамках расследования киберпреступлений и систематический анализ основных направлений правового регулирования в этой сфере. Исследование основывается на методах нормативно-правового и доктринального анализа, а также учитывается международная судебная практика и сравнительно-правовой подход. В расследовании с конституционной точки зрения конституционно оцениваются пределы уголовной юрисдикции, механизмы получения доказательств в рамках международного сотрудничества, судебный контроль и принцип пропорциональности. Анализ показывает, что цифровая среда требует переформатирования механизмов реализации государственного суверенитета в контексте меняющихся правовых реалий. Эффективное расследование киберпреступлений должно осуществляться в сочетании с принципом правового государства, нормативной определенностью и защитой фундаментальных прав, являясь частью конституционно определенной функции безопасности государства. Научное новшество исследования направлено на конституционное обоснование полномочий следствия в цифровых условиях и представление системной модели деятельности государства в этой сфере.

Ключевые слова: *цифровой суверенитет, расследование киберпреступлений, конституционные основы, государственный суверенитет, уголовная юрисдикция, принцип правового государства, принцип пропорциональности.*

Məqalənin redaksiyaya daxil olma tarixi: 20.04.2026
Çapa qəbul tarixi: 18.06.2026