

H Ü Q U Q L A W

UOT 343.1

MƏTANƏT ƏSGƏROVA

**Ədliyyə Nazirliyi Ədliyyə Akademiyasının Cinayət prosesi,
kriminalistika və məhkəmə ekspertizası kafedrasının müdiri,
hüquq elmləri doktoru**

e-mail: matanatasgarova@yahoo.com

ALQORİTMİK SÜBUTLARIN MÜMKÜNLÜYÜNÜN PROSESSUAL TƏMİNATLARI

Cinayət prosesinin rəqəmsallaşdırılması sübut məlumatlarının əldə edilməsi və istifadəsi üçün yeni metodların yaranmasına səbəb olmuşdur. Məhkəməyəqədərki mərhələdə süni intellekt (Sİ) videomüşahidə kameraları və görüntü bazalarından istifadə edərək üz tanıma, rəqəmsal izlərin, yazışmaların, geolokasiyanın, cihaz qeydlərinin, şəbəkə trafikinin təhlilində, cinayətkar qruplar daxilində gizli əlaqələrin müəyyən edilməsi üçün böyük verilənlərin təhlil edilməsində, cinayət törətmə ehtimalını və ya təkrar cinayət törətmə riskini qiymətləndirmək üçün polisın proqnozlaşdırıcı fəaliyyətində istifadə olunur.

Müasir texnologiyalar cinayət işləri üzrə sübutlar sistemini rəqəmsal, biometrik və analitik sahələrə doğru genişləndirir. Sübutların toplanması, təhlili və qiymətləndirilməsində alqoritmlərin və Sİ sistemlərinin istifadəsi yeni “alqoritmik sübutlar” anlayışının yaranmasına səbəb olmuşdur. Alqoritmik sübutlar dedikdə, sübut bazasının məzmununa təsir edən avtomatlaşdırılmış alqoritmlər tərəfindən əldə edilən və ya emal edilən məlumatlar başa düşülür.

Rəqəmsal hüquq sahələrarası hüquq elmi kimi formalaşmışdır, rəqəmsal mühitdə yaranan münasibətləri tənzim edir, hüquq, informasiya, kiber təhlükəsizlik, iqtisadiyyat, mühəndislik

kimi elm sahələrinin müddəalarından istifadə etməklə texnologiyaların hüquqi rejimini və subyektlərin hüquq və vəzifələrini müəyyən edir. Elektron sübutlar artıq cinayət prosesinə daxil olmuşdur, onları rəqəmsal sübutlar da adlandırırlar, iş üçün əhəmiyyəti olan və elektron formada qeydə alınmış istənilən məlumatlardır. Məsələn, elektron məktublar (e-mail), messengerlərdə çatlar (Telegram, WhatsApp), faylların metadataları (yaradılması vaxtı, müəllifi, dəyişikliklər), server qeydləri (istifadəçilərin hərəkətlərinin qeydləri), videokamera qeydləri, rəqəmsal imzalar, elektron sənədlər, sosial şəbəkələrdən, veb-saytlardan, smartfonlardan, GPS-dən və s. alınan məlumatlar elektron sübutlar qismində çıxış edə bilirlər. Onların məqsədi rəqəmsal formada qeydə alınmış müəyyən faktları, hadisəni və ya hərəkəti (məsələn, sistemə daxil olmanı, məlumat göndərməni, köçürmələri) təsdiq etmək və ya inkar etməkdir.

Alqoritmik sübutlar alqoritmlərin (o cümlədən, Sİ, maşın öyrənməsi və ya kriptografik metodların) vasitəsilə əldə edilən və ya formalaşdırılan sübutlardır. Mütəxəssislər qeyd edirlər ki, “Konstruktiv riyaziyyatda sübutlar alqoritmlərdir” [12, s.268]. Onlar sadəcə hadisəni qeyd etmirlər, əsas məqsəd faktın

özünü deyil, məlumatların etibarlılığını və ya həqiqiliyini riyazi və ya hesablama əsaslandırmasından istifadə etməklə alqoritm vasitəsilə təsdiqləməkdir. Məsələn, rəqəmsal imzanın yoxlamasında orijinallıq kriptografik metodlardan sübut olunur, dəyişməzliyi sübut etmək üçün blokçeyn zənciri təhlil edilir, proqnozlaşdırıcı analitik sistemlərdə məlumatların təhlili əsasında riskləri müəyyən edən alqoritmlər tətbiq olunur, məlumatların həqiqiliyi alqoritmlərlə yoxlanılır və s.

Avropa Şurası “alqoritmik sistemlər”i “...riyazi optimallaşdırma üsullarından istifadə edərək məlumatların toplanması, birləşdirilməsi, təmizlənməsi, çeşidlənməsi, təsnif edilməsi və nəticə çıxarılması, eləcə də seçim, prioritetləşdirmə, tövsiyələrin verilməsi və qərar qəbul edilməsi kimi bir və ya daha çox tapşırığı yerinə yetirən tətbiqlər” kimi qəbul edir [17, A(2)].

Maşın öyrənmə alqoritmləri böyük məlumat dəstlərini təhlil etmək, kommunikasiyalarda əlaqələr qurmaq, riskləri proqnozlaşdırmaq və şübhəli davranışlardakı nümunələri müəyyən etmək üçün istifadə olunur. “Maşın öyrənmə kompüter elmlərinin bir sahəsidir, kompüter proqramları sınaq əsasında öyrənilir. Alqoritm verilənləri maşını uşaqlar öz mühitində öyrəndiyi kimi, məşq prosesini yerinə yetirməyə məcbur edir. Bütövlükdə bu təlim metodlarına insanlar nəzarət edə bilirlər” [6, 69-cu bənd]. Sİ sübut məlumatlarının emalını əhəmiyyətli dərəcədə sürətləndirir, kriminalistik və kriminoloji təhlilin dəqiqliyini artırır, cinayətlərin açılmasına səmərəli kömək edir.

Lakin bu cür texnologiyaların tətbiqi alqoritmik sübutların qəbul edilməsinin ənənəvi prosedur təminatlarına uyğunluğu məsələsini aktuallaşdırır. Bu təminatlar ədalətli məhkəmə prosesinin əsasını təşkil edir və tərəflərin hüquqlarını, bərabərliyini, şəffaflığı təmin edir.

Azərbaycan Respublikası CPM-nin 125-ci maddəsinə [1] əsasən, sübutların mümkünlüyü üç meyarla müəyyən edilir: əldə olunması və yaranma mənbəyinə, həmçinin həqiqiliyinə

şübhələrin olmaması. Rəqəmsal sübutların xüsusi bir növü kimi alqoritmik sübutlar məlumatların alqoritmik təfsirinə əsaslanır və təfsirə çıxışın olmaması bu meyarların tətbiqini çətinləşdirir.

İlk yanaşmada alqoritmlərdən istifadə fundamental prosessual prinsiplərin, təqsirsizlik prezumpsiyasının, ədalətli məhkəmə araşdırması hüququnun, müdafiə hüququnun və ayrışdırıcılıq qadağan edilməsinin pozulması kimi ciddi risklər yaradır. Əsas problem alqoritmlərin şəffaf olmaması, onların məntiqinin yoxlanıla bilməməsi, qərəzli və ya natamam məlumatlara əsaslanan səhvlərin yüksək ehtimalı ilə bağlıdır. Alqoritmın işləmə məntiqini tam təhlil etmənin mümkün olmaması (“qara qutu effekti”) nəticələrin etibarlılığının yoxlanılmasını və sübutların mümkünlüyünün qiymətləndirilməsini çətinləşdirir. Sİ modellərinin əksəriyyəti qapalıdır, onların texniki fəaliyyət prinsipləri tərəflərə və məhkəməyə məlum deyildir ki, bu da çəkişmə prinsipi üçün problemlər yaradır. Belə ki, müdafiə tərəfi alqoritmlərin nəticələrini səmərəli mübahisələndirə bilmir. “Məhkəmə qərarı, tibbi qərar kimi, fundamental əsaslılığı və tətbiq edilməsi konkret halda sübut olunmayan Sİ proqramından asılı olmamalıdır” [19]. Alqoritmik sübutların müdafiə tərəfindən mübahisələndirilməsi üçün onun texniki sənədləşməyə, öyrənmə məlumatlarına və modelin metodologiyasına çıxışı olmalıdır. Əgər belə çıxış yoxdursa, qiymətləndirmə zamanı nəzərə alınmalıdır. Məsələn, ABŞ-da tətbiq edilən COMPAS (residiv riskini qiymətləndirmə sistemi), TrueAllele (DNT təhlil sistemi) sistemlərində başlanğıc kod açılmır, bu da onun düzgün işləməsini yoxlamağa imkan vermir. Buna görə də onlardan əsas sübut kimi istifadə olunması düzgün deyildir. Bu xüsusiyyətləri nəzərə alaraq, State v. Loomis işində ABŞ-ın Viskonsin Ali Məhkəməsi qərarında qeyd edir ki, “109...dairə məhkəməsi COMPAS risk qiymətləndirməsindən bəhs etsə də, Loomisin həbsdə saxlanılıb-saxlanılmaması, cəzanın ağırlığı və ya cəmiyyətdə

təhlükəsiz və effektiv şəkildə nəzarət altına alına biləcəyi barədə qərar verməkdə həlledici deyildi” [21].

Üz tanıma alqoritmləri qadınların, yaşlı insanların və etnik azlıqların üzvlərinin şəkillərini emal edərkən tez-tez yüksək səhv nisbətləri nümayiş etdirir. Joy Buolamwini və Timnit Gebru tərəfindən 2018-ci ildə keçirilmiş “Gender Shades” tədqiqatında 3 kommersiya gender-tanıma API sistemi (IBM, Microsoft, Face++) qiymətləndirilmiş və nəticələr belə olmuşdur: “...açıq dərilili kişilərdə səhv nisbəti 0,8 faiz, tünd dərilili qadınlarda isə 34,7 faiz təşkil edir” [22]. Bu səhvlər əsassız şübhələrə və ya ittihamlara səbəb ola bilər.

Bu gün alqoritmik ayrı-seçkilikdən də danışılır. Belə ki, modellər təlim nümunələrindən qərəzliliyi miras ala bilərlər. Məsələn, ABŞ-da COMPAS afroamerikalılar üçün residivizm riskinin təkrarlanması hallarına yol verilmişdir. “... hakimlər, COMPAS alqoritmik tələfindən yaradılan təqsirləndirilən şəxslərin residivizm riskinin proqnozunu alırlar. Hakimlər bu proqnozlara əsasən hərəkət edərsə, əvvəlcədən sənədləşdirilmiş irq və yaş qərəzlərindən kənara çıxmaqla belə, dolayı yolla normativ qərarları mülki proqram təminatına həvalə edirlər. ProPublica məlumat dəstindən istifadə edərək, COMPAS proqnozlarının azadlığa buraxılmaqdan əhsəxanaya salınmağı üstün tutduğunu nümayiş etdiririk. COMPAS təqsirləndirilən şəxslərə qarşı qərəzlidir” [4, s.383]. Bu cür nümunələr alqoritmik qərarların tərəflərin bərabərliyi prinsipinə uyğunluğunu şübhə altına alır.

Sİ-ə əsaslanan alqoritmik sübutlar hakimlər tərəfindən obyektiv məlumatlar kimi qiymətləndirilə bilər ki, bu da məhkəmənin mülahizəsinin məhdudlaşdırılmasına və prosesin humanizmdən kənər həyata keçirilməsinə gətirir. Ənənəvi olaraq, cinayət mühakimə icraatında məhkəmənin qəbul etdiyi qərar yalnız təqdim edilən sübutların məcmusu ilə məhdudlaşmır. Hakim sübutları dəyərləndirərkən onları hadisənin ümumi konteksti və işin

konkret hallarının dinamikası ilə birlikdə nəzərdən keçirir.

CPM-nin 145.2-ci maddəsinə əsasən, “Təhqiqatçı, müstəntiq, prokuror, hakim qanunu və vicdanını rəhbər tutaraq sübutların məcmusunun hərtərəfli, tam və obyektiv baxılmasına əsaslanmaqla öz daxili inamına görə sübutları qiymətləndirirlər.” Sİ-in vicdan, mənəvi məsuliyyət, empatiya və ya sosial konteksti anlamaq qabiliyyəti yoxdur. Hakimin mülahizəsinin, daxili inamının maşın alqoritmik ilə əvəz edilməsi ehtimal modellərinin mexaniki tətbiqinə, məlumatlarda nəzərə alınmayan unikal hallara etinasızlıq göstərilməsinə, cəzanın fərdiləşdirilməsi prinsipindən kənara çıxmağa gətirir. Alqoritmik xüsusi qəddarlığı, törətdiyi əmələ görə peşmançılığı, mərhəmət və bu kimi halları qiymətləndirməsi mümkün deyildir.

Alqoritmlərin geniş tətbiqinə etiraz edən Vincent Chiao bildirir ki, “...cinayət hüququ gündəlik mənəvi düşüncə ilə ən çox əlaqəli hüquq sahəsi kimi qəbul edilir və bu, cinayət məhkəmələrində təqsir, məsuliyyətdən yayınma, bəhanə və sair anlayışlarının əhəmiyyətindən də görünür” və proqnozlaşdırıcı alqoritmlərin istifadəsi cinayət hüququnu və ədalətin tətbiqini texnokratlara və mütəxəssislərə təhvil vermək olardı, “Bunu itki kimi qəbul etmək olar, çünki bu, cinayət hüququnu cəmiyyətin mənəvi vərdislərinin ictimai şəkildə yenidən tətbiqindən xalis sosial zərəri minimuma endirmək üçün soyuq hesablama işinə çevirərdi” [27, s.138].

Alqoritmik sübutların mümkünlüyünün digər bir problemi onların vahid texniki standartlarının olmamasıdır. Alqoritmik etibarlı işlədiyini sübut etmək və ya onun qərarlarının təkrarlana bilən və yoxlanıla bilən əsaslara söykəndiyini göstərmək üçün vahid texniki standartlar formalaşdırılmamışdır. Məsələn, ABŞ-da Daubert Standartına əsasən, məhkəmə ekspertinin elmi metodun etibarlılığını yoxlayır [5], ABŞ-da residivin proqnozlaşdırılması üçün COMPAS sistemi və İsveç və Hollandiyada

İsveçdə hazırlanmış OxRec sistemi tətbiq olunur [7, s.397]. Bu sistemlər müxtəlif metodologiyaya əsaslanırlar. Onların texniki uyğunluğu məsələsi xarici elementli işlərdə nəticələrin qiymətləndirilməsində xüsusi əhəmiyyət kəsb edir.

Doshi-Velez & Kim (2017) tərəfindən aparılan araşdırmaya əsasən bəzi şirkətlər modelin qərarlarının əsaslarını açıqlamaq üçün model interpretasiyası yanaşmasından istifadə edirlər [8], Katz et al. araşdırmasına görə (2017) bir çox firmalar alqoritmlərin riyazi şəkildə sübut olunmanı tələb edən formal doğrulama metodlarını tətbiq edir [10]. Raji & Buolamwininin araşdırmasına görə (2019) akademik müstəvidə isə daha çox yoxlanıla bilən SI prinsipi əsas götürülür [16, s.429]. Bu fərqlilik nəticəsində eyni alqoritm bir ölkədə etibarlı, digərində isə qeyri-etik və ya hüquqa zidd sayıla bilər. Müxtəlif tənzimləyici qurumlar, məsələn, Avropa İttifaqı, İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı [14], ABŞ Standartlar və Texnologiya İnstitutu (NIST) [13] fərqli terminologiya və metodologiyalardan istifadə edir.

Alqoritmlərin etibarlılığın yoxlanması, bir alqoritmın “doğru” qərar verdiyini sübut etmək texniki cəhətdən çətinidir. Dərin öyrənmə modelləri (Deep Learning) milyonlarla parametrdən ibarətdir və “qara qutu” (black box) kimi işləyir. “Explainability” alətləri (SHAP, LIME və s.) qismən izah versə də, formal olaraq sübut sayılmırlar. Formal verifikasiya (məsələn, riyazi və ya məntiq əsaslı doğrulama) metodları hələ çox məhduddur və mürəkkəb sistemlərə tətbiqi çətinidir. Bu da deməkdir ki, əgər vahid texniki çərçivə (standart) yoxdursa, onda “alqoritmik sübut” anlayışı praktiki olaraq subyektiv xarakter daşıyır.

Vahid standartların olmaması həm texniki, həm də hüquqi sahədə ciddi nəticələr doğurur. Məsələn, şirkət öz alqoritmının “ədalətli” olduğunu deyirsə, onun statistik bərabərlik, bərabərləşdirilmiş ehtimallar, yoxsa proqnozlaşdırıcı bərabərlik prinsiplərinə əsaslanmasını

bildirməlidir, çünki, onların tətbiqi fərqli nəticələr verə bilər. Avropa İttifaqı çərçivəsində qanunvericilik səviyyəsində alqoritmik şəffaflıq tələbi qoyulur, lakin bu şəffaflığın texniki olaraq necə sübut ediləcəyi hələ tam müəyyən edilməmişdir [18, 9-cu bənd]. Problemin həlli üçün beynəlxalq səviyyədə birgə qəbul olunmuş alqoritmik etibarlılıq və şəffaflıq standartlarının (məsələn, ISO və ya digər texniki standartlar hazırlayan təşkilatlar səviyyəsində) hazırlanması zəruridir.

Ancaq bu çatışmazlıqlara baxmayaraq, alqoritmlərdən “polis proqnozlaşdırılması sistemlərinin təkmilləşdirilməsində...ekspertizada...hadisə yerinin və ya marşrutun müəyyən edilməsində...həbsxanalarda məhkumların idarə edilməsində...” geniş tətbiq olunması gözlənilir [23, s.85].

Sübutların mümkünlüyünün ümumi şərtləri alqoritmik sübutlara da tətbiq edilməlidir, sübutların əldə edilməsinin mənbəyi, üsulu və prosedur forması tələblərə cavab verməlidir. Sübutların yoxlanılması proseduruna riayət edilməklə, onların həqiqiliyinin, eyniləşdirilməsinin və təkrarlanmasının müəyyən edilməsi tələblərinə uyğunluğu nəzərə alınmalıdır. Alqoritmik sübutlara digər sübutlara qarşı irəli sürülən tələbləri və onların öz xüsusiyyətlərini nəzərə almaqla qeyd edə bilərik ki, onlar mötəbərlik meyarına cavab verməlidirlər, yəni etibarlı, doğru olmalıdır, təhrif olunmamalıdır, qanuni yolla əldə edilməlidir, dəqiq və obyektiv olmalıdır, digər sübutlarla ziddiyyət təşkil etməməlidir, real hadisəni əks etdirməlidir. Adi riyazi məntiqi və ehtimal nəzəriyyəsini tətbiq etsək, alqoritmlər 95% dəqiqlik göstərsə, təkrarlama dəqiqliyi müəyyən olunur. Bu faiz alqoritmın bütün suallar arasında düzgün cavablarının payıdır. Təkrarlana bilmə üçün alqoritmlər ya eyni giriş veriləndə eyni nəticələr verməlidir, ya da təkrarlana bilməsi üçün sabit təsadüfi mənbəyə malik olmalıdır. Alqoritmlərin maşınla oxuna bilməsi mümkün olmalıdır ki, avtomatik yoxlanıla bilsin. Əlbəttə, hüquqşünas yanaşması tətbiq edildikdə, alqoritmik

sübutların etibarlılığının yüksəldilməsi ehtimalların səviyyəsinin aşağı düşməsi ilə bağlıdır. Minimum ehtimallar həmişə mövcud olacaqdır, bu minimum mütəxəssislərin kompleks tədqiqatının nəticəsində müəyyən olunmalıdır.

Alqoritmik sübutların təkrarlanması həm hüquqi və texnoloji prinsip kimi qiymətləndirilməlidir. Təqdim olunan alqoritmik nəticə yalnız o zaman mötəbər sayılır ki, alqoritm eyni verilənlərlə təkrar işləndikdə, eyni və ya ekvivalent nəticə əldə olunsun. Bu, alqoritm sabitliyini və obyektivliyini təsdiq edir. Təkrarlanma şəffaflığının və izah ediləbilənliyin tərkib hissəsidir, prosessual təminatlar sisteminə daxildir. Alqoritmik sübutların təkrarlana bilməsi üçün ilkin verilənlərin bütövlüyü və dəyişdirilməməsi, alqoritm versiyasının sabit saxlanması, tətbiq vasitələrinin (proqram, modul, cihaz) eyni olması, metodologiyanın sənədləşdirilməsi tələb olunur. Təkrarlanma prinsipi pozulduqda, alqoritmik nəticə məhkəmə tərəfindən qəbul edilə bilməz, sadəcə əlavə məlumat kimi qiymətləndirilə bilər.

Alqoritmik sübutlar rəqəmsal sferada həyata keçirilən fəaliyyətin nəticəsidir və insan hüquqları sahəsində beynəlxalq standartlara cavab verməlidir. İnsan hüquqlarını pozan normativ alətlərin və yanaşmaların yayılmasının qarşısının alınması üçün YUNESKO 2023-cü ildə “Rəqəmsal platformaların tənzim edilməsinin rəhbər prinsipləri: ifadə azadlığının və informasiyaya çıxışın təmin edilməsinə çoxtərəfli yanaşma” adlı sənəd qəbul etmiş, rəqəmsal platformaların insan hüquqlarına hörmət etmək üzrə öhdəliklərini, beş əsas uyğunluq prinsipini müəyyən etmişdir. Bu prinsiplərə gender və mədəni aspektlərin nəzərə alınaraq, risklərin təhlil edilməsi və azaldıcı tədbirlərin müəyyən edilməsi, ümumi qəbul edilmiş insan hüquqları standartlarına riayət edilməsi, şəffaflıq, istifadəçilərin hüquqlarının genişləndirilməsi və hesabatlılıq aid edilmişdir [9, 30-cu maddə]. Platformalarda məzmunla bağlı lazımi diqqətlik göstərilməli, onların dizaynında

ayrı-seçkiliyə yol verilməməli, bərabər münasibət və zərərin qarşısının alınması təmin edilməli, mədəni müxtəlifliyə hörmət edilməli, məzmunun idarə edilməsi mümkün olmalı, idarə etmə zamanı istifadə edilən alətlər, sistemlər və proseslər şəffaf olmalı, aydın və yoxlanıla bilən siyasətlərə və səmərəliliyin müəyyən edilməsi üçün ölçülərə malik olmalı, istifadəçilərə məzmunların silinməsi və ya idarə edilməsi ilə bağlı qərarlardan dərhal və müvafiq şəkildə şikayət vermək imkanını nəzərdə tutmalıdır.

Avropa İnsan Hüquqları Məhkəməsi (AİHM) alqoritmik sübutlarla bağlı işləri birbaşa araşdırmasa da rəqəmsal sübutlarla bağlı bir sıra hüquqi meyarlar müəyyən etmişdir. Roman Zakharov v. Russia işində məlumatların avtomatlaşdırılmış toplanması üzərində nəzarətin vacibliyi ilə bağlı “Məhkəmə bu nəticəyə gəlir ki, ...izləmələrin hər hansı məqamında məlumatlandırmanın olmaması hüquqi müdafiə vasitələrinin səmərəliliyinə, yaxud izləmələrlə bağlı sənədlərə yetərinə çıxış əldə etmək imkanına xələl gətirir” [20, s.302].

Ben Faiza v. France işində AİHM qeyd edir ki, “məlumat subyektinin xəbəri olmadan telefon istifadəsi ilə bağlı şəxsi məlumatların toplanması və saxlanması, 8-ci maddənin mənasında, eləcə də təqsirləndirilən şəxsin telefon danışıqlarının siyahısının cinayət prosesində istifadəsi məlumat subyektinin şəxsi həyatına və yazışmalarına hörmət hüququnun həyata keçirilməsinə müdaxilə təşkil edir.” [2, s. 66].

Etik nöqteyi-nəzərdən insana məlumatların məcmusu kimi baxıla bilməz. Sİ fərdlərin rəqəmsal fəaliyyəti, coğrafi yerləşməsi, sosial əlaqələri və internet axtarışları vasitəsilə təhlili əsasında risk profilini yaradır. Bu isə şəxsiyyətin muxtariyyətini və azadlığını pozur, şəxsi həyata müdaxilədir, insanın “rəqəmsal” kölgəsini yaradır, “rəqəmsal ikiləşmə” formalaşır ki, bu da hüquqi və sosial qərarların əsasına çevrilir, insanın cinayət-hüquqi statusuna təsir edir. İnsanın rəqəmsal kölgəsi onun real

həyatda fəaliyyətinin rəqəmsal mühitdə buraxdığı izlərin məcmusudur. Big Brother Watch v. UK işində AİHM şəxsi məlumatların geniş və avtomatlaşdırılmış şəkildə toplanmasını və alqoritmik təhlilini şəxsi həyata müdaxilə hesab etdi və bu cür müdaxilənin yalnız mütənasiblik prinsipi çərçivəsində həyata keçirilə biləcəyini vurğuladı [3, §357-364].

Avropa Şurası alqoritmlərə əsaslanan avtomatlaşdırılmış qərar qəbul edilməsinin yolverilməzliyindən və məcburi insan nəzarətinin vacibliyindən çıxış edir [17, B 5]. Profil yaradılması əməliyyatlarında şəxsin hüquqlarına müdaxilələr yalnız qanunla nəzərdə tutulmuş, zəruri və mütənasib tədbirlərlə həyata keçirilməlidir. Avtomatik sistemlər insan mülahizəsi olmadan tam azad şəkildə qərar verməməlidir. Buna görə də, hər bir avtomatlaşdırılmış qərara görə məsuliyyət daşıyan konkret subyektlər müəyyən edilməlidir. Alqoritmik sistemlər, nə qədər müstəqil işləsələr də, hüquqi subyekt statusuna malik olmadığından, hüquqi və etik baxımdan “öz-özünə məsuliyyət daşıya” bilməzlər. Qərar qəbul etmə prosesində iştirak edən bütün tərəflər, alqoritmik hazırlayan mühəndislər, onu tətbiq edən texniki əməkdaşlar, eləcə də nəticələri qiymətləndirən və təsdiqləyənlər birgə və ya fərdi qaydada məsuliyyət daşıyırlar. CEPEJ “İstifadəçi nəzarəti altında” yanaşmanın tətbiqini tövsiyə edir, istifadəçilərin məlumatlı subyektlər olmasından və verilən seçimlərə nəzarət etməsinin təmin edilməsindən çıxış edir. Ədliyyə sisteminin mütəxəssislərinin istənilən vaxt məhkəmə qərarlarını və nəticə çıxarmaq üçün istifadə edilən məlumatları nəzərdən keçirmə imkanları təmin edilməlidir, lakin onlar həmin məlumatlarla məhdudlaşdırılmamalı, konkret işin spesifik xüsusiyyətlərini nəzərə almalıdırlar. İstifadəçiyə Sİ alətləri tərəfindən təklif olunan həllərin məcburi olmaması, mövcud olan müxtəlif variantlar, hüquqi məsləhət almaq və məhkəməyə müraciət etmək hüququ barədə aydın və başa düşülən dildə məlumat verilməlidir. O, həmçinin məhkəmə prose-

sindən əvvəl və ya məhkəmə prosesi zamanı Sİ tərəfindən işin əvvəlcədən işlənməsi barədə aydın şəkildə məlumatlandırılmalı və etiraz etmək hüququna malik olmalıdır ki, onun işinə AİHK-nın 6-cı maddəsinin mənasında ədalətli məhkəmə araşdırması hüququ təmin edilməklə baxılması təmin edilsin [6, s.13].

Alqoritmik sübutların etibarlılığı yoxlanılması mümkün olan hallar sırasına aid olmalıdır. Bu alqoritmiklərin eyni və ya əsasən oxşar hallara tətbiq edildikdə dəqiq nəticələr vermə ardıcılığının müəyyən edilməsi, onlardan cinayət işlərində sübut kimi qəbul edilib-edilməməsi məsələsinin həllində məcburi nəzərə alınmalı olan xüsusiyyətlərdən biridir. Burada texniki mənada, ən azı ilkin məlumatların daxil edilməsi zamanı səhvlərin, funksiya sürüşməsinin qarşısının alınması üçün təminatlardan söhbət gedir.

Müasir məhkəmə proseslərində alqoritmiklərdən istifadə əsasında video tanıma sistemlərinin, proqnozlaşdırıcı təhlillərin, avtomatlaşdırılmış qiymətləndirmə modellərinin, rəqəmsal kriminalistika sistemlərinin köməyi əldə edilən sübutları təqdim edilməsi alqoritmik sübutların qiymətləndirilməsində məhkəmənin rolunun yüksəldilməsi məsələsini qoyur. Belə ki, məhkəmə yalnız faktları qiymətləndirməməli, həm də alqoritmik metodların etibarlılığını, şəffaflığını və məhdudiyyətlərini başa düşməli, sübutların əsasını təşkil edən alqoritmikləri nəzərdən keçirmək imkanına və hüququna malik olmalıdır. Hakimin alqoritm hazırlama metodologiyası, metodologiyanın dəqiqliyi, yanlışlığın nisbəti, istifadə olunan keyfiyyət ölçüləri və s. ilə bağlı məlumatlara çıxışı olmalıdır. Məsələn, sübutlar üz tanımaya əsaslanırsa, məhkəmənin az işıq şəraitində səhv ehtimalı, alqoritmik qərəz, yəni alqoritmik müəyyən qruplar üçün səhv etmə ehtimalı ilə bağlı məlumatlara çıxışı olmalıdır. Alqoritmik texniki cəhətdən təkmil və obyektiv görünə bilər, lakin qüsurlu ola bilər. Hakimlərin bu sübutları inamla qəbul etmələri üçün bu inamı formalaşdıran məlumatlara maneəsiz çıxışı

olmalıdır. Alqoritmik sübutlarla bağlı indiki vəziyyəti DNT analizinin tətbiqi təcrübəsi ilə müqayisə etsək, məhkəmə ekspertlərinin alqoritmik sübutlarla bağlı eyni qaydada fəaliyyətləri tələb olunur, yəni hakimə alqoritmik anlaşılan dildə izah etməlidirlər, səhvləri və ya yanlış nəticələri müəyyən etməli, nəticələrin şərhinin düzgünlüyünü yoxlamalıdırlar. Alqoritmik parametrləri və imkanları barədə məlumatların təqdim edilməsi öhdəliyi alqoritmik məlumatları təqdim edən tərəfin üzərinə qoyulmalıdır.

Alqoritmik sübutlarla bağlı prosessual hüquqların təmin edilməsində məhkəmənin rolunun gücləndirilməsi üçün məhkəmənin alqoritmə etiraz etmək, onun müstəqil yoxlanılmasını tələb etmək, avtomatlaşdırılmış nəticələrin dəqiqliyini şübhə altına almaq, orijinal məlumatlara daxil olmaq və ya onları yoxlanılmasını təmin etmək hüququ olmalıdır və alqoritmik qeyri-şəffaflığın təqsirsizlik prezumpsiyasını əvəz etməsinə yol verilməməlidir.

Alqoritmik mükəmməl, şərtsiz həqiqət mənbəyi kimi qəbul edilməsinə yol verilməməlidir.

Avtomatlaşdırılmış nəticələrdə əqləbatan şübhənin olması istənilən halda minimuma endirilməlidir, bu əlbəttə texniki məsələdir və əsas məsələ bu minimum kənarlaşmanın hədlərinin əqləbatan olmasıdır. Çünki, alqoritmik sübutlar yekun qərarın özü deyildir, ancaq onun formalaşdırılmasında iştirak edirlər. Məhkəmə hesablaşma səhvlərini, şərhin çətinliyini, səhv istifadə ehtimalını nəzərə almalıdır. Burada digər əhəmiyyətli bir məsələ də hakimlərin rəqəmsal savadlılığının yüksəldilməsidir. Çünki, lazımi rəqəmsal və alqoritmik biliklər olmadan alqoritmik sübutların düzgün qiymətləndirilməsi demək olar ki, mümkün deyildir. Əks halda hakimin qiymətləndirməsi və mülahizəsi tərəflərin sübutları təqdim etmək üsullarından və hakimi inandırmaq bacarığından asılı olacaqdır. Bu sahədə müəyyən səhvlərin olması, bir sıra hallarda qaçılmazdır. Hazırda

bir sıra ölkələrdə hakimlərin rəqəmsal hüquq sahəsində təlimlərinə başlanılmışdır. Məsələn, ABŞ Dövlət Məhkəmələri üzrə Milli Mərkəzi Thomson Reuters İnstitutu ilə birlikdə bu sahədə kurslar təklif edir [24]. Qlobal Hakimler Təşəbbüsünün xətti ilə 2022-2023-cü illərdə 4500 çox məhkəmə işçisi UNESCO-nun Süni İntellekt (Sİ) və Qanunun Aliliyi üzrə onlayn kurslarında iştirak etmişdir [25].

Alqoritmik sübutdan istifadə olunması barədə təklif verilməsi və ya təqdim edilməsi kifayət etmir, onlar yalnız məhkəmənin əsaslandırılmış qərarı ilə qəbul oluna bilər.

““Süni intellektlə neyroproqnozlaşdırma” süni intellektin bir növü hesab edilə bilər. Bu neyroproqnozlaşdırma üsulu beynin fəaliyyətindəki biomarkerləri tapmaqla gələcəkdə cinayət törətmə ehtimalı olan şəxsləri müəyyən etməyə çalışır.” [29, s.593]. “Cinayətkarlığa meyilliliyi” proqnozlaşdırmaq və ya cinayət törətmə ehtimalını qiymətləndirmək üçün Sİ-in prediktiv modellərindən istifadənin qarşısının alınması üçün qanunvericilik qaydasında tədbir görülməlidir, çünki bu modellər təqsirsizlik prezumpsiyasına uyğun gəlmir. Residiv riskinin qiymətləndirilməsi alqoritmik müəyyən sosial qruplarla bağlı göstəriciləri yüksəldir, keçmiş tutulmalar haqqında məlumatlar hüquq-mühafizə orqanlarının münasibətinin formalaşmasına, qərəzliliyinə təsir edir Alqoritmiklərin tətbiqi zamanı texniki problemləri də nəzərə almaq lazımdır. “...risk və ehtiyacların birləşməsi bu alətlərin proqnozlaşdırma dəqiqliyini azalda bilər, çünki ən güclü risk faktorlarının bəziləri kriminogen ehtiyacları adətən nəzərə alındığı şəkildə dəyişdirilə bilməz və bəzi ehtiyaclar təkrar cinayət törətmə riski ilə əlaqələndirilməyə bilər” [7, s.397].

Böyük Britaniya Kembric Universiteti və Durham Polis İdarəsi tərəfindən hazırlanan Zərərin Qiymətləndirilməsi Risk Aləti (HART) Cinayət Ədliyyə Sistemində (CJS) daxil olan işlər üzrə cinayətləri proqnozlaşdırma və polis nəzarəti şəraitində istifadə olunan alqoritmik proqnozlaşdırma alətidir. Proqnozlaşdırma

modeli gələcək cinayət riskini qiymətləndirməklə polis nəzarəti işçilərinin qərar qəbul etməsini dəstəkləyir [28].

Cinayətkar davranış ehtimalını qiymətləndirən proqnozlaşdırıcı sistemlərdən istifadə edilməsi təqsirsizlik prezumpsiyasını pozur, fərdin təqsiri sübut olunmazdan əvvəl riskli cinayətkar hesab olunur. Alqoritmlərə qarşı ədalətlik tələbini irəli sürmək o qədər də düzgün olmazdı. Ola bilər ki, texniki imkanlarına görə alqoritmlərlə əldə edilən sübutlar verilənlər baxımından düzgün qiymətləndirilmişdir. Ancaq alqoritmın ədalətli olması üçün cinayətkarın şəxsiyyətinin xüsusiyyətlərinə, cinayətin törədilməsinin hallarına və şəraitinə, yüngülləşdirici halların olmasına və s. aspektlərə diqqət yetirilməlidir. Ümumiyyətlə, proqnozlaşdırma modelinin tətbiqinin nəticələri tövsiyə xarakteri daşmalıdır, polis əməkdaşının vəzifələrini əvəz etməməlidir. Heç bir alqoritm təkrar cinayət törətməklə bağlı hər hansı məlumatı özü əldə edə bilməz. Polis əməkdaşı məlumatları olsa belə, şübhəli şəxsə bağlı məhkəmədənə qərar qəbul edə bilməz. Proqnozlaşdırma modelləri polis və məhkəmə məlumat sistemlərində əks olunan nəticələrdən istifadə etməklə qurulur və bu nəticələr o dövrdə verilən insan mühakimələrinə əsaslanır. Model reallığı əks etdirməsəydi, bu, səhv olardı və səhv nisbətləri artardı. Buna görə də alqoritmlərin qərəzli hesab edilməli olduğu qənaətinə gəlməzdən əvvəl, insan mühakiməsinin daha çox və ya daha az qərəzli olub-olmadığını nəzərə almaq lazımdır. Alqoritmlər adətən öz səhv nisbətlərini qiymətləndirə bilirlər.

Alqoritmik formalaşdırılmış məlumatların hüquqi təbiəti milli CPM-də möhkəmləndirilməmişdir. Mövcud qanunvericilik baxımından bu məlumatlar bir neçə sübut növünə aid edilə bilər, lakin bu zaman müəyyən problemlər yaranır. Məlum olduğu kimi CPM sübutların növlərinə şübhəli, təqsirləndirilən, zərər çəkmiş şəxs, şahidlərin ifadələrini, istintaq və həmçinin məhkəmə hərəkətlərinin protokol-

larını, ekspertin rəyini, maddi sübutları və digər sənədləri aid edir. Hər bir proqram və ya alqoritm tərəfindən yaradılan avtomatlaşdırılmış hesabat cinayət işi ilə əlaqəli qeydə alınmış məlumatları ehtiva edən rəqəmsal sənəd hesab edilməlidir. Çünki, alqoritmə bağlı hesabat fayl formasına malikdir (PDF, log, JSON, CSV), yəni sənədə qarşı irəli sürülən tələblərə, yəni CPM-nin 135-ci maddəsinin tələblərinə cavab verir, sənəd kimi cinayət təqibi üzrə əhəmiyyət kəsb edə bilən məlumatları hərflər, rəqəm, qrafika və digər işarə formasında özündə əks etdirir, elektron daşıyıcıdır. Problemlər onunla bağlı ola bilər ki, sənəd insan tərəfindən deyil, sistem tərəfindən yaradılır, bu da onun düzgünlüyünə görə məsuliyyət məsələsini çətinləşdirir. Həmçinin həqiqiliyinin yoxlanılması mürəkkəb bir prosesdir, alqoritm yalnız ekspertiza vasitəsilə təhlil etmək mümkündür. Məlumat mənbəyinin qeyri-müəyyənliyi ilə bağlı hesabat ilkin məlumatlar emal edildikdən sonra yaradılsa, hesabatın, yoxsa orijinal məlumat massivinin sənəd olması ilə bağlı sual yaranır.

Alqoritmədən ekspert tərəfindən tədqiqat vasitəsi kimi istifadə olunursa, onun nəticələri ekspert rəyinə daxil edilir və ekspert tədqiqatı prosedurunun ayrılmaz elementi kimi çıxış edir. CPM-nin 127-ci maddəsinə əsasən ekspertin rəyi “cinayət prosesini həyata keçirən orqanın və ya cinayət prosesi tərəflərinin ekspert qarşısında qoyduğu suallara, habelə iş materiallarının tədqiqi zamanı ortaya çıxan onun səlahiyyətlərinə aid digər halların araşdırılmasına dair nəticələridir; bu nəticələri əsaslandıran ekspertin apardığı tədqiqatın təsviridir”. Bu mənada ekspert alqoritmədən metodika və ya texniki vasitə kimi istifadə edir. CPM-nin 7-ci maddəsi ekspertin rəyinin “elmi inkişafın müasir tələblərinə uyğun olan və hamı tərəfindən qəbul edilmiş elmi dəlillər əsasında yoxlanmasına imkan verən müddəalara əsaslanmalı” olmasını müəyyən edir. Nəticəni ekspert formalaşdırır, alqoritm isə nəticənin əldə edilməsinə kömək edir. CPM-nin 97.4.1-ci

maddəsi müəyyən edir ki, ekspert “düzgünlüyü özü tərəfindən yoxlanılmamış iş materiallarının tədqiqi əsasında gəldiyi şəxsi nəticələrini, habelə kompüter proqramından və məlumat materiallarından istifadə etməklə əldə etdiyi nəticələri rəydə bir-birindən dəqiq ayırmalıdır”. Burada alqoritmın metodikanın elementi kimi validasiyası ilə bağlı problemin yaranması mümkündür, bu mənada hər bir proqram kriminalistik vasitə hesab olunmaya da bilər. Həmçinin alqoritmın parametrlərinə ekspertin çıxışı yoxdur. Məhkəmə ekspertizası fəaliyyəti haqqında Azərbaycan Respublikası Qanununa əsasən ekspertin rəyi ekspertiza təcrübəsində formalaşmış vahid elmi-metodik üsullar əsasında aparılır [11, 23-cü maddə]. Ekspertizasının aparılmasında istifadə olunan tədqiqat metodları Dövlət Reyestrinə daxil olmalıdır, həmçinin elmi-metodik materialların xüsusi fondu yaradılmalıdır. Bu metodlar elmi əsaslılıqla yanaşı, sahəvi standartlara da uyğun olmalıdır, onlara çıxış təmin edilməlidir. Hesab edirik ki, bu tələblər alqoritmik sübutların əsaslandığı alqoritmələrə və onlardan istifadə olunması metodikasına da aid edilməlidir. Alqoritmələr kommersiya sistemində istifadə olunduqda, əksər hallarda qapalı xarakter daşıyır, ona görə də bu tələblərin mənsubiyyətindən asılı olmayaraq bütün alqoritmələrə tətbiq edilməsi xüsusilə vacibdir.

Alqoritmələr CPM-nin 128-ci maddəsi mənasında maddi sübutlar kimi də baxıla bilər. CPM-nin 128.1-ci maddəsinə əsasən, “Öz xüsusiyyətinə və əlamətlərinə, mənşəyinə, aşkar edildiyi yerə və vaxtına və ya üzərində hadisənin izlərinin saxlanıldığına görə cinayət təqibi üzrə əhəmiyyət kəsb edən halların müəyyən edilməsinə kömək edən hər bir əşya maddi sübut hesab edilə bilər”. Rəqəmsal mühitdə məlumat saxlama cihazı (telefon, daşıyıcı disklər), kompüter faylları, rəqəmsal video nəzarət arxivi bu obyektlərə aid edilə bilər. Orijinal rəqəmsal daşıyıcı maddi sübut hesab edildikdə, alqoritm informasiyanı bu daşıyıcılardan çıxara və ya bərpa edə bilər, alqoritm cinayətin

izlərinə çıxışın texniki vasitəsidir. Məsələn, proqram silinmiş faylları avtomatik olaraq bərpa edir. Bu zaman fayllar maddi sübutlar, proqramlar isə alət qismində çıxış edir. Burada problemlər texniki müəyyən etmə və məlumatların modifikasiyasının sərhədlərinin müəyyən edilməsi, alqoritmın tətbiqi zamanı informasiyanın transformasiyası riski, proqramların tətbiqinin şərtlərinin dəqiq qeydə alınmasının zəruriliyi ilə bağlı ola bilər.

Alqoritmələr artıq həyatımıza daxil olmuşdur, onlardan adi həyatda və ədalət mühakiməsinin həyata keçirilməsində istifadə edilməsi qaçılmazdır. Buna görə də bu sahədə texniki maarifləndirmə tədbirləri xüsusi əhəmiyyət kəsb edir. Avropa Şurası alqoritmik sistemlərin tətbiqi ilə bağlı Üzv Dövlətlərin hökumətlərinə tövsiyə edir ki, avtomatlaşdırılmış qərar qəbul etmə sistemlərinin funksiyalarını və nəticələrini anlamaq, bu cür sistemlərin istifadəsində məlumatlı qərarlar qəbul etmək, alqoritmik sistemlərin istifadəsindən irəli gələn faydalarından yararlanmaq və bu cür sistemlərin istifadəsindən irəli gələn təhdid və risklərə məruz qalması minimuma endirmək üçün bütün fərdlərə və qruplara imkan yaratmaq üçün effektiv və uyğunlaşdırılmış media, informasiya və rəqəmsal savadlılıq proqramlarının həyata keçirilməsini təşviq etsinlər, özəl sektor, media, vətəndaş cəmiyyəti, təhsil müəssisələri və akademik və texniki qurumlar da daxil olmaqla bütün müvafiq maraqlı tərəflərlə səmərəli əməkdaşlıq etsinlər [17, B.7].

CPM alqoritmələri, avtomatlaşdırılmış sistemləri, SI, neyro-şəbəkə modellərini sübutlara aid etmir, bu isə onların statusunun mübahisələndirilməsinə gətirir. Belə ki, alqoritmələr sübut mənbəyi kimi qəbul olunarsa, onların əmələ gəlmə mənbəyi aydın olmalıdır, əks halda müdafiə hüququnu, həmçinin ittiham tərəfinin də hüququnu pozur. İttiham tərəfi alqoritmik sübutlara əsaslanaraq təqsirləndirilən şəxs barəsində tam olmayan, bəzi hallarda düzgün olmayam məlumatlar alır, öz mövqeyini onlarla möhkəmlədir. Sübut mənbəyi kimi

alqoritmlərin yoxlanılması üçün hakimlər çıxış kodlarını tədqiq etmək imkanları olmalıdır, ekspert əgər modelin tətbiqinin nəticələrindən istifadə edərsə, onun işləmə məntiqini də izah etməlidir. Hesab edirik ki, alqoritmik sübutlar hazırda digər informasiya mənbələri ilə məcmuda götürüldükdə sübut kimi qəbul olunmalıdır.

ABŞ-nın məhkəmə təcrübəsində TrueAllele Casework Sisteminin koduna çıxış əldə edilməsi ilə bağlı müdafiə tərəfi kodun əldə edilməsi barədə sorğusunu onunla əsaslandırır ki, təqsirləndirilən şəxsin Dr. Perlin-in məhkəmədə ifadə verməsindən əvvəl üzləşmə hüququ vardır, TrueAllele Casework Sistemi əsl şahiddir və həmin şahidi effektiv şəkildə çarpaz dindirmək üçün onun mənbə koduna ehtiyacı vardır. Məhkəmə “kompüter proqramını necə çarpaz dindirmək olar?” deyə soruşduqda, təqsirləndirilən şəxsin müdafiəçisi bildirdi ki, onların ekspertləri mənbə kodunu araşdırmaq imkanı əldə etdikdən sonra bu araşdırmanın nəticələrinə əsasən Dr. Perlin-ə suallar verəcəklər. Məhkəmə bu vəsatəti rədd etdi və müdafiə tərəfinin qaldırdığı məsələnin əslində açıqlama məsələsi olduğunu, mənbə kodunun yaradıcısı olan Dr. Perlin-i çarpaz dindirmək imkanının təqsirləndirilən şəxsin üzləşmə hüququnu təmin etdiyini bildirdi. Həm Dr. Perlin, həm də elektroforezi aparmış laboratoriya analitiki məhkəmədə DNT testlərinin nəticələri və statistik təhlillə bağlı ifadə verdilər [15].

Amerikanın Vətəndaş Azadlıqları İttifaqı (“ACLU”) və Electronic Frontier Foundation belə bir Amicus curiae icmalı təqdim etmişlər ki, TrueAllele geniş şəkildə başa düşülən və hərtərəfli yoxlanılmış bir texnologiyadır, yaxud mahiyyət etibarilə məxfi olan kommersiya sirlərinə, yəni mənbə koduna əsaslanan bir sistem kimi fəaliyyət göstərir. Bunların ikisi eyni anda mümkün deyildir. Əslində isə, bu ehtimalların heç biri olmaya bilər, çünki bu texnologiya ciddi, müstəqil testlərdən keçməyib və ümumiyyətlə kommersiya sirri kimi qorun-

mağa layiq hesab edilə biləcək hər hansı bir element də daşımaya bilər. Özəl bir şirkətin sırf maliyyə maraqları prosessual ədalət və üzləşmə hüququ kimi fundamental hüquqlardan üstün tutula bilməz. Cinayət işi üzrə təqsirləndirilən şəxsin prokurorun sübutlarını nəzərdən keçirmək, təhlil etmək və onlara cavab vermək hüququ vardır və ondan kriminalistik texnologiya satıcısının iddialarını kor-koranə qəbul etməsi tələb oluna bilməz. Mənbə kodunun müstəqil araşdırılması kriminalistik proqram təminatının qiymətləndirilməsində mühüm və əvəzolunmaz bir addımdır və belə araşdırmalar kriminalistik alətlərdə təkrarən səhvlər aşkar etmişdir. TrueAllele ilə eyni tip probabilistik genotipləmə texnologiyasının müstəqil araşdırılması əvvəllər ciddi səhvləri, hətta onların yaradıcılarının belə xəbərdar olmadığı səhvləri, üzə çıxarmışdır. Proqramçıların nəzərdə tutduğu abstrakt alqoritmin sadəcə olaraq təsviri və ya dizaynerin dindirilməsi müstəqil təhlili əvəz edə bilməz və cinayət təqiblərində ədalətsizliyin qarşısını almağa yönəlmiş konstitusion təminatlara tam cavab vermir. Kriminalistik proqram təminatının mənbə kodunun gizli saxlanılmasının məqsədi guya kommersiya məlumatlarının mənimsənilməsinin qarşısını almaqdır, lakin bu gizlilik eyni zamanda təqsirləndirilən şəxslərin və ictimaiyyətin həmin proqramlarda məhkumun təqsirsiz insanları belə həbsə və ya ölüm cəzasına aparacaq qüsurları üzə çıxarmasının qarşısını alır. Təkrar aparılan müstəqil araşdırmalar kriminalistik proqramlarda texnologiyanın etibarlılığını və cinayət ədliyyə sisteminə istifadəyə yararlılığını şübhə altına alan səhvlər və uyğunsuzluqlar aşkar etmişdir. Bunun nümunələrinə TrueAllele-in analoqları olan FST və STRMix daxildir, hər ikisində günahsız insanları təqsirləndirəcək dərəcədə ciddi səhvlər üzə çıxarılmışdır. Hökumət kriminalistik proqram təminatı tərəfindən yaradılmış sübutlardan istifadə etmək istədikdə, həmin proqramın mənbə kodunun açıqlanması həm cinayət işi üzrə təqsirləndirilən şəxsləri Kon-

stitusiya ilə qorunan hüquqlara, həm də ictimaiyyətin məhkəmə proseslərinə çıxış hüququna uyğun olaraq tələb olunur. Cinayət təqibi kontekstində ictimaiyyətin ədalətli və açıq məhkəmə proseslərinə dair Konstitusion təminatlara güclü marağı vardır, ictimai açıqlama əsas qayda olmalıdır. Yalnız qeyri-adi hallarda, bu işə aid olmayan hallarda, hökumət ictimaiyyətin çıxış hüququnu üstələyəcək dərəcədə ciddi məxfilik marağını əsaslandırma bilər. Belə bir vəziyyətdə məhkəmə qoruyucu qərar çıxara bilər. Belə qərarlar adətən ticarət rəqibləri arasında kommersiya məhkəmə çəkişmələrində tətbiq olunur, orada risklər daha aşağıdır və məlumatların mənimsənilməsi mümkündür. Heç vaxt müdafiə tərəfinin mənbə kodu və proqramın hazırlanma materiallarına çıxışı tamamilə rədd edilməməli, yaxud təqsirləndirilən şəxs ona qarşı irəli sürülmüş sübutlarla üzləşmək imkanından birmənalı məhrum edilməməlidir. Buna görə də Məhkəmə hökumətin sorğunu ləğv etmək (motion to quash) barədə vəsatətini rədd etməlidir. Təqsirləndirilən şəxsə prokurorun sübutlarını nəzərdən keçirmək və onlarla üzləşmək hüququ təmin edilməli və prokurorun sübut etmə yükünü müdafiə tərəfinin üzərinə keçirməsi qadağan edilməlidir. Mənbə kodu müdafiənin vəkillərindən və ekspertlərdən gizlədilə bilməz. Mülki məhkəmə çəkişmələrində, azadlıq hüququnun risk altında olmadığı və tərəflərin çox vaxt bazar rəqibləri olduğu hallarda, qoruyucu qərarların geniş tətbiqi göstərir ki, belə qərarlar kommersiya sirri sahiblərinin maraqlarını qorumaq üçün kifayət qədər təsirlidir. Bu işlərdə belə qərarlar vəkillərə və rəqib tərəfin cəlb etdiyi ekspertlərə sübutlarla tanış olmaq imkanı verir, amma məlumatın digər şəxslərə ötürülməsi məhdudlaşdırıla bilər. Bir çox federal dairə məhkəmələri patent mübahisələri üzrə model qoruyucu qərarlar qəbul etmişdir. Bu qərarlar açıq şəkildə kommersiya sirləri və mənbə kodunun qarşı tərəfin vəkillərinə və mütəxəssislərinə açıqlanmasını nəzərdə tutur. Qoruyucu qərarlar, hətta tərəflər bir-birinin mülkiyyət

məlumatlarından iqtisadi fayda əldə edə biləcək birbaşa rəqiblər olduqları hallarda belə, tətbiq olunur [26].

Alqoritmik sübutlardan istifadə cinayət mühakimə icraatının səmərəliliyini artırmaqla yanaşı, hüquqi sistemin qarşısında yeni məsuliyyətlər də qoyur. Bu məsuliyyətlərin mərkəzində isə alqoritmlərin tətbiqində ədalətlik, obyektivlik və müdafiə hüququnun təminatı dayanır. Yalnız bu şərtlər daxilində alqoritmik sübutlar cinayət prosesi üçün etibarlı və legitim vasitə kimi çıxış edə bilər. Alqoritmik sübutların mümkünlüyü tələblərindən çıxış edərək, belə hesab edirik ki, onlardan istifadə olunması texnoloji inkişafın qaçılmaz mərhələsidir, lakin iş üzrə istintaqın sürətləndirilməsi və sadələşdirilməsi təqsirləndirilən şəxslərin hüquqları hesabına əldə edilə bilməz. Buna görə də alqoritmik sübutlar üçün xüsusi hüquqi rejim tətbiq edilməlidir. Cinayət Prosesual Məcəlləsinə “alqoritmik sübutlar” anlayışı daxil edilməli, mümkünlüyünün şərtləri müəyyən edilməlidir. Sİ-dən istifadə edərək əldə edilən sübutların məcburi yoxlanılmasına və ekspert qiymətləndirməsinə tabe olması mütləq öz əksini tapmalıdır. Müdafiənin alqoritmlərə çıxış imkanı olmalıdır, bu çıxış ilk növbədə onun texniki təsvirinə və öyrənmə seçimlərinə aiddir. Qapalı və ya çıxış olmayan məlumatlara əsaslanan modellərin təqsirləndirilən şəxsə qarşı istifadə edilməsi qadağan edilməlidir. Hazırda informasiya texnologiyaları ilə bağlı texniki ekspertizalar keçirilir. Hesab edirik ki, alqoritmik sistemlərlə bağlı rəqəmsal ekspertizanın keçirilməsi mümkün olmalıdır. Cinayət prosesinin məqsədləri üçün dəqiqlik, etibarlılıq və ayrı-seçkiliyə yol verilməməsi üçün sınaqdan keçirilmiş sertifikatlaşdırılmış Sİ sistemlərindən istifadə edilməsinə yol verilməlidir, sertifikatlaşdırılmamış sistemlərin tətbiqinə görə məsuliyyət müəyyən edilməlidir.

Prosesual təminatlar, ilk növbədə, alqoritmlər vasitəsilə əldə edilən məlumatların qanuni yolla toplanmasını, təhrif edilmədən saxlanmasını, həmçinin tərəflərin bu sübut-

ların mahiyyəti ilə tanış olmaq və onları şübhə altına almaq imkanlarının təmin olunmasını tələb edir. Bununla yanaşı, alqoritmın tətbiq metodunun açıq şəkildə göstərilməsi, onun səhv ehtimalının qiymətləndirilməsi və nəticələrin digər sübutlarla müqayisəli təhlili vacibdir.

Bu çərçivədə məhkəmə yalnız o halda alqoritmik sübutu qəbul edə bilər ki, həmin sübutun istifadəsi əsaslandırılmış, prosessual qaydalara uyğun, etik çərçivədə və təqsirsizlik prezumpsiyasını pozmadan həyata keçirilsin. Alqoritmik sübutların mümkünlüyü onların məhkəmə sisteminə integrasiyasının keyfiyyətindən deyil, məhz onların tətbiqinin hüquqi tənzimlənməsi və prosessual zamanətlərlə təmin edilməsindən asılıdır.

Məhkəmə proseslərində rəqəmsal və alqoritmik texnologiyaların artan istifadəsi ilə məh-

kəmənin rolu əhəmiyyətli dərəcədə genişlənməlidir: məhkəmə alqoritmik metodların elmi əsaslılığını, şəffaflığını və etibarlılığını yoxlamaq, bu cür sübutların qəbul edilməsi üçün alqoritmlərin texniki parametrlərinin açıqlanmasını təmin etmək, ixtisaslaşmış mütəxəssisləri cəlb etmək və tərəflərə avtomatlaşdırılmış nəticələrə tənqidi şəkildə etiraz etmək imkanı vermək səlahiyyətinə malik olmalıdır.

Alqoritmik sübutların cinayət prosesində geniş tətbiqi onların təbiəti, imkanları və hüquqi aspektləri, həmçinin texniki aspektləri, məhdudiyyətləri, ayrı-seçkiliyə yol verilməsi, insan hüquqlarının qorunması ilə bağlı aspektləri barədə həm hüquqtətbiq edici təcrübənin əməkdaşları, həm də əhali arasında rəqəmsal biliklərin inkişaf etdirilməsinə yönəlmiş təhsil və məlumatlandırma fəaliyyətləri genişləndirilməlidir.

Ədəbiyyat:

1. Azərbaycan Respublikasının Cinayət-prosessual Məcəlləsi. URL: <https://e-qanun.az/framework/46950>
2. Ben Faiza v. France (application no. 31446/12). Judgment, 8 Februar 2018. URL: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%5B%22001-180657%22%5D%7D>
3. Big Brother Watch and Others v. The United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15). Judgment, 25 May 2021. URL: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%5B%22001-210077%22%5D%7D>
4. Christoph Engel et al. Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism// Artificial Intelligence and Law, – 2025.33, –p.383–404. URL: <https://doi.org/10.1007/s10506-024-09389-8>
5. Daubert Standard. URL: https://www.law.cornell.edu/wex/daubert_standard
6. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment (Adopted at the 31st plenary meeting of the CEPEJg, Strasbourg, 3-4 December 2018). URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>
7. Fazel S, Sariaslan A, Fanshawe T. Towards a More Evidence-Based Risk Assessment for People in the Criminal Justice System: The Case of OxRec in the Netherlands// Eur J Crim Pol Res., – 2022.28(3), – p.397-406. URL:doi: 10.1007/s10610-022-09520-y. Epub 2022 Jul 1. PMID: 36097585; PMCID: PMC9458683.
8. Finale Doshi-Velez, Been Kim. Towards A Rigorous Science of Interpretable Machine Learning. 2 Mar 2017. URL: <https://doi.org/10.48550/arXiv.1702.08608>
9. Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information

- through a multi-stakeholder approach. UNESCO, 2023. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000387339>
10. Katz DM, Bommarito MJ II, Blackman J. A general approach for predicting the behavior of the Supreme Court of the United States// PLOS ONE, –2017.12(4): e0174698. URL: <https://doi.org/10.1371/journal.pone.0174698>
11. Məhkəmə ekspertizası fəaliyyəti haqqında Azərbaycan Respublikası Qanunu, 18 noyabr 1999-cu il № 758-IQ. URL: <https://e-qanun.az/framework/91>
12. Newcomb, Greenleaf. Algorithms and proofs: Mathematics in the Computing Curriculum 268-272 //SIGCSE '89: Proceedings of the twentieth SIGCSE technical symposium on Computer science education. -February 23-25, 1989. Louisville, KY, USA. URL: <https://doi.org/10.1145/65293.65313>
13. NIST AI Risk Management Framework. URL: <https://www.nist.gov/itl/ai-risk-management-framework>
14. OECD AI Principles. Recommendation of the Council on Artificial Intelligence. Adopted on: 22/05/2019. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
15. People v. Wakefield (N.Y. 2022). 38 N.Y.3d 367. No. 3. Decided April 26, 2022. URL: <https://law.justia.com/cases/new-york/court-of-appeals/2022/3.html>
16. Raji, Inioluwa & Buolamwini, Joy. (2019). Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products// AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, –p. 429 – 435. DOI: 10.1145/3306618.3314244.
17. Recommendation (CM/Rec (2020)1) of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies). URL: [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016809e1154%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016809e1154%22],%22sort%22:[%22CoEValidationDate%20Descending%22]})
18. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. PE/24/2024/REV/1. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
19. Robert, Sanger. Artificial Intelligence and Criminal Law// The Colleges of Law, – Jan. 12, 2024. URL: <https://www.collegesoflaw.edu/blog/2024/01/12/artificial-intelligence-and-criminal-law/>
20. Roman Zaxarov (Roman Zakharov) Rusiyaya qarşı (Ərizə № 47143/06). Qərar, 4 dekabr 2015-ci il. URL: [https://hudoc.echr.coe.int/fre#{%22display%22:\[%220%22\],%22languageisocode%22:\[%22AZE%22\],%22apno%22:\[%2247143/06%22\],%22documentcollectionid%22:\[%22GRAND-CHAMBER%22\],%22itemid%22:\[%22001-162749%22\]}](https://hudoc.echr.coe.int/fre#{%22display%22:[%220%22],%22languageisocode%22:[%22AZE%22],%22apno%22:[%2247143/06%22],%22documentcollectionid%22:[%22GRAND-CHAMBER%22],%22itemid%22:[%22001-162749%22]})
21. State v. Loomis, 2016 WI 68. URL: <https://cases.justia.com/wisconsin/supreme-court/2016-2015ap000157-cr.pdf?ts=1468415026>
22. Study finds gender and skin-type bias in commercial artificial-intelligence systems//MIT News Office. – February 11, 2018. URL: https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212?utm_source=chatgpt.com
23. Tatia Dolidze. The Role of Artificial Intelligence in Criminal Justice - Reality and Perspective// International Journal “LAW AND WORLD “, –2024, September. Volume 10/Issue 3, – p. 80-97. <https://doi.org/10.36475/10.3.8>

24. TRI/NCSC AI Policy Consortium for Law & Courts. URL: <https://www.ncsc.org/our-centers-projects/trincsc-ai-policy-consortium-law-courts>
25. UNESCO. Training judges, lawyers and prosecutors in Artificial Intelligence and the Rule of Law. URL: <https://www.unesco.org/en/articles/training-judges-lawyers-and-prosecutors-artificial-intelligence-and-rule-law>
26. United States of America v. Lafon Ellis. Brief of Electronic Frontier and ACLU of Pennsylvania as Amici Curiae in support of defendant's opposition to government motion to quash. Case No. 2:19-cr-00369-DWA. URL: https://www.eff.org/files/2022/06/15/19-cr-00369_amicus_brief_of_eff_and_aclu_1.pdf
27. Vincent, Chiao. Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice// International Journal of Law in Context, – 2019. № 15, –p.126–139 doi:10.1017/S1744552319000077
28. Written evidence submitted by Durham Constabulary (ALG0041). Evidence on Algorithms in decision-making. URL: <https://committees.parliament.uk/writtenevidence/79959/pdf/>
29. Zico, Junius Fernando et al. The Role of Neuroprediction and Artificial Intelligence in the Future of Criminal Procedure Support Science: A New Era in Neuroscience and Criminal Justice// Yuridika, – 2023. September. Volume 38. No 3, –p.593-620. DOI: 10.20473/ydk.v38i3.46104

Açar sözlər: süni intellekt, mümkünlük, alqoritmik sübutlar, cinayət prosesi, insan nəzarəti, ayrı-seçkilik, prosessual təminatlar

Matanyat Askerova

*Academy of Justice of the Ministry of Justice,
Head of the Department of Criminal Procedure,
Forensic Science and Criminalistics, Doctor of Law*

PROCEDURAL GUARANTEES FOR THE ADMISSIBILITY OF ALGORITHMIC EVIDENCE

ABSTRACT

The purpose of the research is to determine the limits of the application of algorithmic evidence and to define the boundaries of its admissibility within criminal proceedings. The author proceeds from the necessity of establishing general legal frameworks for the use of algorithmic data as evidence. Algorithmic evidence must comply with the principles of controllability, proportionality, and minimization of interference, and must be subject to judicial evaluation.

The significance of the study lies in the fact that the widespread use of algorithmic evidence requires the development of new approaches to ensure transparency, accountability, and the humanistic character of the administration of justice. It also highlights the need to develop internationally recognized standards of algorithmic reliability and transparency (for example, at the level of ISO and other standard-setting organizations), as well as the necessity of introducing the concept of algorithmic evidence into national legislation.

The scientific novelty of the research lies in the fact that it is one of the first studies devoted to the admissibility of algorithmic evidence in the context of the evidentiary provisions of the Criminal Procedure Code of the Republic of Azerbaijan. It introduces the concept of “algorithmic evidence” into the academic discourse of national criminal procedural law and develops its conceptual dimensions. The research is situated at the intersection of criminal procedure, human rights, digital law, and it advances contemporary approaches in this field.

The study employs methods of comparative legal analysis, doctrinal interpretation of normative acts, and systemic analysis. These methods make it possible to determine the relationship between the technical autonomy of algorithmic evidence and human legal responsibility.

The results of the research may be used in legislative and law-enforcement practice, in the development of national strategies on the regulation of algorithmic evidence, and in academic programs on criminal procedure and human rights.

Keywords: *artificial intelligence, admissibility, algorithmic evidence, criminal procedure, human control, discrimination, procedural guarantees*

Матанят Аскерова

*Заведующая кафедрой Уголовного процесса,
судебной экспертизы и криминалистики
Академии Юстиции Министерства Юстиции,
доктор юридических наук*

ПРОЦЕССУАЛЬНЫЕ ГАРАНТИИ ДОПУСТИМОСТИ АЛГОРИТМИЧЕСКИХ ДОКАЗАТЕЛЬСТВ

РЕЗЮМЕ

Цель исследования состоит в определении пределов применения алгоритмических доказательств и границ их возможного использования в уголовном процессе. Автор исходит из необходимости формирования общих правовых рамок использования алгоритмических данных в качестве доказательств. Алгоритмические доказательства должны соответствовать принципам управляемости, соразмерности и минимизации вмешательства, а также подлежать оценке судом.

Значимость работы заключается в том, что широкое применение алгоритмических доказательств требует разработки новых подходов для обеспечения транспарентности, ответственности и гуманистического характера отправления правосудия, а также выработки международно признанных стандартов алгоритмической надежности и прозрачности (например, на уровне ISO и других организаций, разрабатывающих технические стандарты), и обосновывает необходимость включения понятия алгоритмических доказательств в национальное законодательство.

Научная новизна исследования заключается в том, что оно является одним из первых в контексте положений УПК Азербайджанской Республики о доказательствах, посвящённых вопросам допустимости алгоритмических доказательств, вводит понятие «алгоритмические доказательства» в научный оборот национального уголовно-процессуального права и разрабатывает его понятийные аспекты. Исследование находится на стыке уголовного процесса, прав человека, цифрового права и развивает современные подходы в данной сфере.

В ходе исследования использованы методы сравнительно-правового анализа, доктринального толкования нормативных актов и системного анализа. Эти методы позволяют определить взаимосвязь между технической автономностью алгоритмических доказательств и юридической ответственностью человека.

Результаты исследования могут быть использованы в законодательной и правоприменительной практике, при разработке национальных стратегий регулирования алгоритмических доказательств, а также в учебных программах по уголовному процессу и правам человека.

Ключевые слова: *искусственный интеллект, допустимость, алгоритмические доказательства, уголовный процесс, человеческий контроль, дискриминация, процессуальные гарантии*