BİOMETRİK MƏLUMATLARIN İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ ONLARDAN İSTİFADƏ QAYDALARI

Aytəkin İbrahimova*

Xülasə

Biometrik məlumatlar, şəxsiyyəti müəyyənləşdirmək və ya identifikasiya etmək üçün istifadə edilə bilən bir şəxsin unikal fiziki və ya davranış xüsusiyyətlərinə aid fərdi məlumatları özündə ehtiva edir. Biometrik məlumatlar artıq bu gün demək olar bir çox sahələrdə istifadə olunur. Hətta informasiya texnologiyaları o qədər inkişaf etmişdir ki, bu gün gündəlik istifadə olunan kompüter, planşet, telefon, ağıllı saat və s. kimi bir çox informasiya texnologiya vasitələrində biometrik məlumatları toplayan, emal edən, istifadə etmək bacarığı olan və saxlayan, o cümlədən məhv edən sistemlər tətbiq olunur. Bütün bunlar biometrik məlumatlara dair dəqiq hüquqi tənzimetmənin mövcud olmasını zəruri edir. Biometrik məlumatlar informasiya təhlükəsizliyi və şəxsiyyətin identifakisiyası məqsədləri üçün müxtəlif sahələrdə getdikcə daha çox istifadə olunur. Müəllif tərəfindən biometrik məlumatların informasiya təhlükəsizliyini təmin edə biləcək qaydalar təhlil edilir. Müəyyən hallarda həmin məlumatların təhlükəsiz açılması öyrənilir.

Açar sözlər: biometrik məlumatlar, fərdi məlumatlar, biometrik identifikasiya, şifrələmə, biometrik texnologiyalar, informasiya təhlükəsizliyi.

"İnformasiya hüquq münasibətlərinin inkişafi nəticə etibarilə, yeni normativ hüquqi aktların qəbulunu şərtləndirir. Məsələn, XXI əsrin əvvəllərində insanın bioloji xüsusiyyətlərinə əsasən kimliyinin müəyyən edilməsi, yəni biometrik autentifikasiya (və ya biometriya) bir çox dövlətlərin milli qanunvericiliyində biometrik informasiya haqqında hüquqi sənədlərin qəbuluna gətirib çıxarmışdır. 18 iyul 2008-ci ildə qəbul edilmiş "Biometrik informasiya haqqında" Azərbaycan Respublikası Qanunu məhz biometrik informasiya ehtiyatlarının formalaşdırılmasını və onlara dair tələbləri, biometrik identifikasiya sisteminin fəaliyyətinin təşkili və təyinatını, biometrik texnologiyaların tətbiqi sahələrini müəyyən edir və bu sahədə yaranan münasibətləri tənzimləyir." [1, s.147]

Bununla birlikdə, biometrik məlumatların toplanması və istifadəsi də məxfilik və təhlükəsizlik narahatlığını artırır. Biometrik məlumatlar həssas fərdi məlumatlar hesab olunur və xüsusi qorunma tələb olunur, çünki şəxsləri müəyyənləşdirmək üçün istifadə edilə bilər və onları dəyişdirmək çətin, hətta bəzi hallarda mümkünsüzdür. Məsələn aparılmış müvafiq araşdırmalar nəticəsində müəyyən olunmuşdur ki yaşayan insanların hər birinin barmaq izləri, üz quruluş məlumatları, genetik xüsusiyyətlərinə dair məlumatlardan üst üstə düşən yoxdur. Bu isə ümumilikdə təhlükəsizliyin təmin edilməsi üçün xüsusi əhəmiyyətli qəbul olunur. Bir çox ölkələr viza prosedurlarında şəxslərin o cümlədən biometrik məlumatlarını da toplayırlar. Bu zaman cinayət hadisələri baş verdikdə şəxsin identifikləşdirilməsi prosesi rahat olur. Hətta bu yalnız əcnəbilərə tətbiq edilmir. Artıq bir çox ölkələrdə, o cümlədən Azərbaycan Respublikasında şəxsiyyəti

* hüquq üzrə fəlsəfə doktoru, Bakı Dövlət Universitetinin Konstitusiya hüququ kafedrasının dosenti

təsdiq edən sənədin verilməsi zamanı şəxsin barmaq izi, imzası, üz quruluşunun biometrik xüsusiyyətləri kimi biometrik fərdi məlumatlar toplanılır və müvafiq informasiya ehtiyyatında saxlanılır. Bu milli təhlükəsizlik üçün olduqca əhəmiyyətli hal hesab olunur. [9, s.73]

Ümumiyyətlə, biometrik məlumatların istifadəsi təhlükəsizliyi və identifikasiyanı müxtəlif sahələrdə inkişaf etdirə bilər, eyni zamanda məxfilik və təhlükəsizlik narahatlığına diqqət yetirməyi tələb edir. Təşkilatlar fiziki şəxslərin təhlükəsizliyini və məxfiliyini təmin etmək üçün biometrik məlumatların qorunmasını prioritetləşdirməlidirlər.

"Biometrik məlumatlar müxtəlif məqsədlər üçün toplana və istifadə edilə bilər. Məsələn, girişin təlim keçmiş mütəxəssislərlə məhdudlaşdırılmalı olduğu bio-təhlükəli laboratoriyada biometrik skanerlə heç bir fiziki təması nəzərdə tutmayan girişə nəzarət üçün tor qişa və ya irsin tanınması sistemi istifadə edilə bilər. Digər misal, lazımi bacarıqlara/təhlükəsizlik sertifikatlarına malik olan tikinti sahəsində çalışan işçilər tərəfindən girişə nəzarət və davamiyyətin qeydə alınması sistemlərinin istifadəsi ola bilər. Bəzi hallarda, ilkin daxil olduqdan sonra həssas kompüter sistemlərinin istifadəçilərinin şəxsiyyətlərini davamlı olaraq yoxlamaq üçün üz tanıma və ya yazma ritm analizatoru işə salına bilər. Müəyyən bir növ biometrik məlumatın toplanıb-toplanmaması onların toplanmasının məqsədindən və bu cür məlumatların toplanma yollarından asılıdır." [30]

Burada meydana çıxan əsas əhəmiyyətli məsələ biometrik məlumatlar və onların istifadə qaydasının müəyyənləşdirilməsidir. Əvvəla biometrik məlumatlara anlayış verilməsi daha düzgün olardı.

Geniş təhlil nəticəsində müəyyən olunur ki, biometrik məlumatlara müxtəlif normativ aktlarda anlayış verilmişdir. Odur ki, biometrik məlumatlar dairəsinin müəyyən olunmasını və onların hüquqi rejiminin müəyyənləşdirilməsində kömək edir. Biometrik informasiya və biometrik məlumatlara Azərbaycan Respublikasının qanunvericiliyində də anlayış verilmişdir. "Biometrik informasiya haqqında" Azərbaycan Respublikası Qanunun 1-ci maddəsinə əsasən biometrik informasiya dedikdə identifikasiya və verifikasiya məqsədi ilə informasiya sistemlərində toplanılan, saxlanılan, işlənilən və ötürülən biometrik məlumatlar başa düşülür. [31] Öz növbəsində həmin maddədə biometrik məlumatlara da anlayış verilmişdir. Belə ki, Qanuna əsasən biometrik məlumatlar identifikasiya edilmiş və ya identifikasiya olunan fiziki şəxsin fizioloji xüsusiyyətlərini xarakterizə edən, onu birmənalı və ya digər məlumatlarla uzlaşdıraraq identifikasiya etməyə imkan verən, müvafiq standartlar tətbiq olunan və maddi daşıyıcıda əks etdirilən fərdi məlumatlardır. Belə biometrik məlumatlara aşağıdakı məlumatlar aid edilə bilər:

- əl-barmaq və ovuc izləri,
- üz təsviri,
- gözün qüzehli və tor qişası,
- səs fraqmenti və onun akustik parametrləri,

- dezoksiribonuklein turşusu (DNT) analizinin nəticələri,
- bədən ölçüləri,
- bədənin xüsusi əlamətlərinin və fiziki çatışmazlıqlarının təsviri,
- yazı xətti və imzası və s.[31]

Bu məlumatların siyahısında qeyd olunmayan amma fiziki şəxsin trasoloji izləri, daktiloskopik məlumatları da aid edilə bilər. Qanunun normasının məzmunundan göründüyü kimi biometrik məlumatların bir sıra spesifik xüsusiyyətləri mövcuddur. [10, s.378] Qanunvericiliyimizə nəzər salaraq qeyd edə bilərik ki, biometrik məlumatların spesifik xüsusiyyətləri aşağıdakılardır:

- biometrik məlumatlar identifikasiya edilmiş və ya identifikasiya olunan fiziki şəxsə aid olur,
- həmin fiziki şəxsin fizioloji xüsusiyyətlərini xarakterizə edə bilir,
- onu birmənalı və ya digər məlumatlarla uzlaşdıraraq identifikasiya etməyə imkan verir,
- müvafiq standartlar tətbiq olunan və maddi daşıyıcıda əks etdirilir
- fərdi məlumatların bir növüdür.

Avropa İttifaqı çərçivəsində qəbul edilmiş Ümumi Məlumatların Mühafizəsi Qaydalarında (GDPR) da biometrik məlumatlara anlayış verilmişdir. Belə ki, həmin Qaydaların (GDPR) 4-cü maddəsinə əsasən Biometrik məlumat dedikdə fiziki şəxsin onu identifikləşdirməyə imkan verən və ya bunu təsdiq edən, fiziki, psixoloji və davranış xüsusiyyətlərinin xüsusi texniki emalı nəticəsindən meydana çıxan üz görünüşləri və ya daktiloskopik məlumatlar kimi fərdi məlumatlar başa düşülür. [32] Həmin Qaydalarda verilən anlayışa əsasən isə məlumatın biometrik məlumat kateqoriyasına aid edilməsi üçün aşağıdakı spesifik xüsusiyyətlərə malik olması tələb olunur:

- məlumat fiziki şəxsi identifikləşdirməyə imkan verməli və ya bunu təsdiq etməlidir;
- şəxsin fiziki, psixoloji və davranış xüsusiyyətlərinin xüsusi texniki emalı nəticəsində meydana çıxmalıdır;
- fərdi məlumat olmalıdır.

İnformasiya sistemləri, texnologiyaları və onların təminat vasitələrinin yaradılması, istifadəsi barəsində hüquqa zidd olmayan qərarın verilməsində bərabərlik prinsipi mühüm əhəmiyyətə malikdir. Başqa sözlə, irqindən, etnik mənsubiyyətindən, dinindən, dilindən, cinsindən, mənşəyindən, əmlak vəziyyətindən, qulluq mövqeyindən, əqidəsindən, siyasi partiyalara, həmkarlar ittifaqlarına və digər ictimai birliklərə mənsubiyyətindən asılı olmayaraq bütün vətəndaşlar, eləcə də təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatlar informasiya sistemləri, texnologiyaları və onların təminat vasitələrinin yaradılması və istehsalında bərabər hüquqlara malikdirlər. Digər subyektlərdən fərqli olaraq, dövlətin üzərinə informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin yaradılması və istehsalı sahəsində pozitiv öhdəliklər qoyulmuş, müvafiq dövlət orqanları üçün informasiya sistem-

ləri, texnologiyaları və onların təminat vasitələri elmi və təcrübi-layihə işlərinin aparılmasına şərait yaratmasına dair vəzifə müəyyən edilmişdir. Məsələn, informasiya təhlükəsizliyinin təmin edilməsində mühüm rola malik olan biometrik eyniləşdirmə sisteminin inkişafi bu gün dövlətin qarşısında dayanan vacib məsələlərdən biridir. [17, s.276] Bu amil cəmiyyətdə ictimai-siyasi və sosial hüquqi münasibətlərin tələbidir. Belə ki, internet mühitində baş verən pozuntuların əsas səbəblərindən biri məhz subyekt haqqında identifikasiya mexanizmlərinin etibarlı və şəffaf olmamasıdır. Məhz bu sosial sifarişə cavab olaraq, BMT-nin Təhlükəsizlik Şurasının biometrik identifikasiyanın həyata keçirilməsi, yeni nəsil sənədlərin tətbiqi haqqında Qətnaməsinə müvafiq olaraq, Azərbaycanda da "Biometrik eyniləşdirmə sisteminin yaradılması haqqında" Dövlət Proqramı qəbul olunmuşdur. Göründüyü kimi, mövcud sosial tələb əsasında informasiyalaşdırmanın aparıcı istiqamətlərinin, onun inkişafi üçün müvafiq tədbirlərin reallaşdırılması, informasiya sistemlərinin yaradılması müvafiq hakimiyyət orqanları tərəfindən müəyyən edilir, sistemlər yaradılır və ya yaradılması üçün münbit şərait formalaşdırılır". [1, s.245]

Azərbaycan Respublikasında biomterik informasiya ilə əlaqədar ictimai münasibətlərin tənzimləyən xüsusi normativ hüquqi aktın mövcud olması xüsusi təqdirə layiq hal kimi qiymətləndirilməlidir. Növbəti mərhələdə isə biometrik məlumatların istifadə edilməsi qaydasının müəyyən edilməsi də zəruridir. Biometrik məlumatlara verilən anlayışdan və onun spesifik xüsusiyyətlərindən göründüyü kimi biometrik məlumatlar da fərdi məlumatlar kateqoriyasıan aid edilir. Odur ki, demək olar ki, fərdi məlumatların istifadəsi ilə bağlı qanunvericiliklə müəyyən edilmiş hüquqi rejim eyni zamanda biometrik məlumatlara da şamil edilir.

"Biometrik alqoritmlər əslində nümunə tanıma sistemləridir. Artıq qeyd edildiyi kimi, nümunənin tanınması anomaliyaların aşkarlanması və xəstəliklərin diaqnostikası üçün də istifadə olunur. Texniki standartlaşdırmanın müəyyən səviyyəsinə baxmayaraq, hər bir alqoritm məlumatı orijinal şəkildə emal edir. Üstəlik, toplanmış biometrik məhsulların emalı üçün çoxlu sayda alqoritmlər mülkiyyətə məxsusdur və buna görə də təbiətinə görə məxfidir. Biometrik sistemlərin istifadəçiləri üçün onlar haqqında hansı məlumatların toplandığını və onların sonrakı necə işləndiyini müəyyən etmək, əsasən, qeyri-mümkündür. Onlar biometrik sistemi işlədən subyekt tərəfindən onlara verilən zəmanətlərə etibar etməlidirlər. Eyni zamanda, biometrik sistemdən istifadə edən subyektlərlə bu sistemə daxil olan fiziki şəxslərin maraqlarının eyni olmasına ehtiyac yoxdur. Bu maraqlar hətta bir-birinə zidd ola bilər. Zəmanətlər etibarlı olmaya da bilər". [26, s.300]

"Belə ki, biometrika "bioloji orqanizmin konstitusiyasının və ya fəaliyyətinin və ya davranışının fərdi aspektləri" haqqında məlumat daxil olmaqla geniş bir termindir. [20] Geniş mənada belə biometrik məlumatlar müxtəlif məqsədlər üçün qiymətləndirilə və əlavə məlumat əldə edilə bilər. əvvəlki bölmələrdə təq-

dim edildiyi kimi. "Şəxs haqqında onun məlum xüsusiyyətlərinə və ya meyllərinə əsaslanan məlumatın fərdiləşdirilməsi prosesi" profilləşdirmə adlanır. [27, s.178]

Profilin yaradılması üçün biometrik məlumatlardan istifadənin təhlükələri və riskləri artıq ədəbiyyatda ümumiləşdirilmişdir. Şəxsin unikal identifikatorlarının profilləşdirmə üsulları ilə birləşdirilməsi informasiyanın öz müqəddəratını təyinetmə hüququnu poza, bəşəriyyəti əsarət altına ala bilər və ayrıseçkiliyə səbəb ola bilər." [18, s.349]

"Biometrik məlumatların işlədilməsinin (emalının, istifadəsinin) məxfiliyə təsiri ciddidir. Biometrik məlumatların emalı təkcə qanunlardan yayınma və ya bəzən onların səmərəsiz icrası kimi bütün şəxsi məlumatların emalı üçün ümumi olan təhdidlərə deyil, həm də nəzarət olunmayan sahəsinin azalması ilə nəticələnən anonimliyin itirilməsi təhlükələrinə, eləcə də yüksək həssas məlumatların hətta məlumat subyektinə məlum olmayan həssas məlumatlar bilmədən təmin edilməsi təhlükələrinə məruz qalır. Üstəlik, bu məlumat biometrik məlumatların xüsusi təbiətinə görə fərdi olaraq unikal şəkildə əlaqələndiriləcəkdir. Digər verilənlər bazaları arasında biometrik məlumatların çarpaz istinad edilməsi və digər nəzarətçilərə əlavə məlumatların təqdim edilməsi zəifliyi əhəmiyyətli dərəcədə artırır. Biometrikanı bu qədər populyar edən əsas xüsusiyyət onun rahatlığı və gözəgörünməzliyidir. Bu problemin həlli xüsusilə telefon və noutbuklarda istifadə olunan cari biometrik sistemlərin sınaqdan keçirilməsi, biometrika üzrə texniki standartlara riayət edilməsi və biometrikanın müstəqil sertifikatının yayılması üçün müstəqil proqram təminatının hazırlanmasından ibarətdir." [26, s.304;305]

Biometrik məlumatların istifadəsi adətən aşağıdakı mərhələləri əhatə edir:

Biometrik məlumatların toplanması və qeydiyyatı: Bu, şəxsin biometrik məlumatlarının emal edilməsi, istifadə olunması və onun etibarlı bir verilənlər bazasında saxlamaq üçün həmin məlumatları təqdim etdiyi bir prosesidir. Bu ilkin mərhələdir. Biometrik məlumat informasiya ehtiyyatında saxlanılan fərdi məlumatlar məhz bu proseslə əldə olunur. Qeydiyyat zamanı şəxsin biometrik məlumatları, barmaq izi skanerləri, üz tanınması kameraları və ya irs analizinin həyata keçirə bilən skanerlər kimi xüsusi cihazlardan istifadə edərək toplanılır. Biometrik məlumatlar sonra rəqəmsal şablona çevrilir və etibarlı bir verilənlər bazasında saxlanılır. Bu verilənlər bazasının mühafizəsi üçün xüsusi təhlükəsizlik tədbirləri görülməlidir. [13, s.201]

Toplanılmış və ya mövcud biometrik məlumatlardan identifikasiyanın həyata keçirilməsi (doğrulama) məqsədi ilə istifadəsi: Bir şəxsin biometrik məlumatları qeydiyyatdan keçdikdən sonra, identifikasiya məqsədləri üçün istifadə edilə bilər. Doğrulama, sonrakı identifikasiya cəhdi ərzində fərd tərəfindən təqdim olunan biometrik məlumatlar ilə (informasiya ehtiyyatında şəxsin adına qeydiyyata alınmış biometrik məlumatın rəqəsmal şablonu) sistemə təqdim edilən biometrik məlumatları (identifikasiya məqsədi ilə biometrik məlumatların təqdim edilməsi zəruri olduğu hallarda şəxs tərəfindən təqdim edilən biometrik məlumatların rəqəmsal şablona çevrilmiş versiyası) müqayisə etməyi əhatə edir. Biometrik məlumatlar uyğun gəlirsə, fərdə platformaya, cihaza və ya mühafizə

olunan digər bir yerə giriş imkanı verilir. Əgər təqdim edilən nümunə saxlanılan şablonla eynilik təşkil edirsə identifikasiya prosesi tamamlanmış olur və bununla da şəxsin şəxsiyyəti müyyən edilir (identifikləşir). Belə ki, bəzi hallarda biometrik məlumatlar yoxlama məqsədləri üçün istifadə olunur. Doğrulama, əvvəllər bir verilənlər bazasında saxlanılan bir istinad biometrik şablonu ilə biometrik məlumatlarını müqayisə etməklə bir şəxsin şəxsiyyətini təsdiqləməyi əhatə edir. Doğrulama, bir şəxsin şəxsiyyətinin sərhəd nəzarəti və ya hüquq mühafizə orqanlarında olduğu kimi təsdiqlənməli olduğu vəziyyətlərdə çox vaxt istifadə olunur. Bu kimi hallar təhlükəsizliyin təmin edilməsi üçün xüsusi əhəmiyyət daşıyır. [9, s.86]

Biometrik məlumatların saxlanıldığı informasiya ehtiyyatlarına nəzarət və onun idarəedilməsi: Biometrik məlumatlar etibarlı şəkildə saxlanılmalı və məlumatların bütövlüyünü və düzgünlüyünü təmin etmək üçün lazımi şəkildə idarə edilməlidir. Buraya şifrələmə, giriş nəzarəti və monitorinq sistemləri kimi müvafiq təhlükəsizlik tədbirlərinin icazəsiz giriş və ya biometrik məlumatların oğurlanmasından qorunması üçün monitorinq sistemlərinin həyata keçirilməsini əhatə edir. Bundan əlavə, onun düzgünlüyünü və uyğunluğunu təmin etmək üçün unikallığı dəyişə bilən biometrik məlumatlar mütəmadi olaraq yenilənməlidir. Məsələn üz şəkli, səs fraqmenti və s. [10, s.578]

Ümumiyyətlə, biometrik məlumatların istifadəsi konfidensiallığın və təhlükəsizlik narahatlığının diqqətlə nəzərdən keçirilməsini tələb edir. Təşkilatlar fərdlərin təhlükəsizliyini və məxfiliyini təmin etmək üçün biometrik məlumatların toplanması, saxlanması və idarə edilməsi üçün müvafiq prosedurları həyata keçirməlidirlər. Bundan əlavə, şəxslərə biometrik məlumatların toplanması və istifadəsi barədə məlumat verilməlidir və məlumatlı razılıq vermək imkanı təmin olunmalıdır.

Biometrik məlumatlar öz unikallıq xüsusiyyətinə görə təmamilə müxtəlif sahələrdə istifadə olunur. Belə ki, müxtəlif elm sahələrinin, həmçinin ictimai sferaların predmetini təşkil edən və qeyri müəyyən qalan məsələlər məhz biometrik məlumatlardan istifadə edilməsi ilə aydınlaşdırıla bilər. Əvvəla bəzi biometrik məlumatlar ömrü boyu dəyişilməzliyi və unikallığı ilə seçilir. Bu biometrik məlumatlar şəxslərin identifikləşdirilməsi prosesində əsrarəngiz rol oynayır. Məsələn şəxsin əl izi, üz izi, DNK məlumatları kimi fərdi unikal məlumatlar. Bunlar cinayət prosesi, kriminalistika, əməliyyat axtarış fəaliyyəti kimi sahələrdə qarşıya qoyulmuş məsələlərin həllinin təmin edilməsində əhəmiyyətli rola malikdir. Digər şəxsdən götürülən genetik məlumatları özündə əks etdirən nümunələrin üzrəində aparılan analiz nəticələri müəyyən sosiologiya ilə bağlı sualların cavablandırılmasına xidmət edir. Məsələn müəyyən ərazidə yaşayan şəxslərin gen xəritəsinin çıxarılması, demoqrafik məslələrə dair keçmişə dair təsəvvürün formalaşdırılması və s. [19, s.64] Həmçinin şəxsin genetik məlumatlarını özündə əks etdirən biometrik məlumatlar bəzi mülki mübahisələrin həllində xüsusi rol oynayır. Buna misal olaraq, atalığın mübahisələndirilməsi, atalığın müəyyən edilməsi, vərəsəlik üzrə münasibətlərə dair qaldırılan iddialar barədə

mülki işlər göstərilə bilər. Göründüyü kimi, biometrik məlumatlardan istifadə mülki hüquq münasibətlərində də geniş istifadə olunur. Tibbi məqsədlər və sfera üçün də biometrik məlumatların toplanması, emalı, saxlanması və tədqiqi geniş yayılmışdır. Belə ki, şəxsin biometrik məlumatları vasitəsi ilə bir çox xəstəliklərin diaqnozu qoyula bilir. Həmçinin şəxsin davranış və psixoloji xüsusiyyətlərinə dair biometrik məlumatlar psixologiya və psixoterapiya sahəsində mütəxəssislər tərəfindən geniş istifadə olunur. [24, s.465]

Digər tərəfdən, müəyyən mənada dəyişə bilən biometrik məlumatlardan da müxtəlif məqsədlər üçün istifadə edilir. Məsələn şəxsin fizioloji quruluşu barədə biometrik məlumatlar, yəni onun çəkisi, boyu, bədən quruluşu, əlinin və ayağının ölçüsü bəzi cinayətlərin açılması və kriminalistik tədqiqatda xüsusi əhəmiyyəti ilə fərqlənir. Həmçinin ayaq izləri, əl izləri, ayaq izlərindən ibarət trayektoriya və bu kimi digər trasoloji izlər trasologiya, məhkəmə ekspertizası və kriminalistika elmləri üzrə aparılan tədqiqatlarda əhəmiyyətli obyekt kimi çıxış edir. [3] Biometrik məlumatlar fərdi məlumatların təhlükəsizliyini və məxfiliyini təmin etmək üçün xüsusi diqqət tələb edən həssas formasıdır. Biometrik məlumatlar fərdləri müəyyən etmək və onların şəxsiyyətini təsdiqləmək üçün istifadə oluna bilər ki, bu da onu kibercinayətkarlar üçün dəyərli hədəfə çevirir. Buna görə də, şəxslərin məxfiliyinin və şəxsiyyətinin identifikasiya prosesində özünün qoruması üçün biometrik məlumatların təhlükəsizliyini təmin etmək vacibdir. Bu xüsusi informasiya təhlükəsizliyi tədbirlərin görülməsini tələb edir. [4, s.174]

Biometrik məlumatların təhlükəsizliyini təmin etmək üçün təşkilatlar biometrik məlumatlara icazəsiz giriş və ya oğurluqdan qorunmaq üçün şifrələmə, girişə nəzarət və monitorinq sistemləri kimi müvafiq təhlükəsizlik tədbirlərini həyata keçirməlidir. Bundan əlavə, təşkilatlar biometrik məlumatların toplanması, saxlanması və idarə edilməsi üçün aydın siyasət və prosedurlar yaratmalıdırlar. Məsələn, biometrik məlumatlar yalnız müəyyən məqsədlər üçün toplanmalıdır və fərdlər öz biometrik məlumatlarının toplanması və istifadəsi barədə məlumatlandırılmalıdırlar. Biometrik məlumatları əldə olunan şəxsin razılığı alınmalıdır. Ona məxsus biometrik məlumatlar yalnız qanunla müəyyən edilmiş qaydada və həddə razılığı olmadan əldə oluna, istifadə oluna, emal edilə, toplana, ötürülə və məhv edilə bilər. Həmçinin informasiya təhlükəsizliyinin təmin edilməsi məqsədi ilə şəxsin yazılı razılığında ona məxsus biometrik məlumatlardan hansı həddə və platforma və ya sistemlərdə istifadə edilməsinin göstərilməsi məqsədəmüvafiq olardı. [7, s.10]

Bundan əlavə, biometrik məlumatlar məhdud girişi olan təhlükəsiz yerdə saxlanmalıdır. Tranzit və istirahət zamanı biometrik məlumatları qorumaq üçün şifrələmədən istifadə edilməlidir. Biometrik məlumatlara giriş iş vəzifələrini yerinə yetirmək üçün girişə ehtiyacı olan səlahiyyətli şəxslərlə məhdudlaşdırılmalıdır. Həmçinin səlahiyyətləri olmayan və ya şəxsiyyəti identifikləşdirilməyən şəxslərin hücumları nəticəsində biometrik informasiya ehtiyyatlarına giriş əldə olunduqdan sonra informasiya ehtiyyatı sistemi mövcud biometrik məlumatların avtomatik silinməsi və ya istifadəyə yararsız hala salınması informasiya təhlü-

kəsizliyinin təmin edilməsi üçün əlverişli addımdır. Bunun tətbiq edildiyi platforma və informasiya ehtiyyatlarında saxlanılan biometrik məlumatların surətlərinin çıxarılması və tamamilə ayrı yerdə saxlanılması da zəruridir. Bu, biometrik məlumatların itirilməsi və məhvi kimi informasiya təhlükəsizliyinə yönələn hədlərə qarşı tətbiq edilən uğurlu təhlükəsizlik tədbiri kimi qiymətləndirilə bilər. [11]

"Həm milli, həm də beynəlxalq səviyyədə informasiya təhlükəsizliyinin təmin olunmasında biometrik informasiya texnologiyaları da böyük imkanlara malikdir. Təcrübədən məlumdur ki, informasiya-kommunikasiya sistemlərində, xüsusən də internet mühitində baş verən cinayətlərin, qeyri-etik davranışın əsas səbəblərindən biri istifadəçilərin zəruri hallarda identifikasiyası mexanizmlərinin mükəmməl olmamasıdır. 2001-ci ilin 11 sentyabrında ABŞ-da baş verən terror hadisəsindən sonra BMT-nin Təhlükəsizlik Şurası insanların onlara məxsus biometrik məlumatlara əsasən identifikasiyasının həyata keçirilməsi, yeni nəsil sənədlərin tətbiqi haqqında qətnamə qəbul etmişdir. Hal-hazırda bir sıra dövlətlərdə Beynəlxalq Mülki Aviasiya Təşkilatı, Beynəlxalq Dəniz Təşkilatı, Beynəlxalq Əmək Təşkilatı, Beynəlxalq Standartlaşdırma Təşkilatı və digər qurumlar tərəfindən qəbul edilmiş yeni standartlara, Beynəlxalq Miqrasiya Təşkilatının tövsiyələrinə uyğun olaraq, biometrik texnologiyaları nəzərdə tutan elektron pasportların istehsalı və tətbiqi, biometrik identifikasiya sistemlərindən sərhədkeçmə nəzarətində və əməliyyat-axtarış fəaliyyətinin həyata keçirilməsində, ictimai asayişin mühafizəsində istifadəsi təşkil edilmişdir. İdarələrarası və dövlətlərarası informasiya sistemləri yaradılmış, müəyyən təcrübə toplanmış, müvafiq proqram-texniki vasitələrin istehsalçıları arasında ixtisaslaşma və rəqabət güclənmişdir. Bu sahədə konkret layihələrin icrasına, müvafiq blankların və proqram-texniki vasitələrin istehsalına başlanılmışdır. " [1, s.405]

Biometrik məlumatların müntəzəm saxlanması və idarə edilməsi də onların təhlükəsizliyinin təmin edilməsi üçün vacibdir. Biometrik məlumatlar mütəmadi olaraq yenilənməlidir və icazəsiz girişin və ya sui-istifadənin qarşısını almaq üçün lazım olmadıqda məhv edilməlidir.

Xülasə, biometrik məlumatların təhlükəsizliyi fərdlərin məxfiliyini və şəxsiyyətini qorumaq üçün çox vacibdir. Təşkilatlar müvafiq təhlükəsizlik tədbirləri həyata keçirməli və biometrik məlumatların toplanması, saxlanması və idarə olunması üçün aydın siyasət və prosedurlar yaratmalıdırlar. Biometrik məlumatların müntəzəm saxlanması və idarə edilməsi də onların təhlükəsizliyinin təmin edilməsi üçün vacibdir.

"Biometrik texnologiyaların tətbiqi pasport-viza və şəxsiyyəti təsdiq edən digər sənədlərin mühafizə dərəcəsinin və şəxsin başqa fərdi məlumatlarla sənəd almasına nəzarətin gücləndirilməsini, kritik infrastrukturun və digər obyektlərin mühafizə rejiminin təkmilləşdirilməsini, identifikasiya işlərinin dəqiqliyini və müxtəlif informasiya resurslarında şəxs barədə fərdi məlumatların kompleks əlaqələndirilməsini təmin edir. Məhz ona görə də bir çox müəlliflər hesab edirlər ki, milli eyniləşdirmə sisteminin iki vacib elementinin - biometrik eyniləşdirmə sisteminin və elektron imza infrastrukturunun yaradılması, onların imkanlarının

səmərəli şəkildə birləşdirilməsi və istifadəsi təkcə bu problemin həllində deyil, ümumiyyətlə, informasiya məkanının təhlükəsizliyinin təmin edilməsində mühüm rol oynayacaqdır. 2007-ci ildə "Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007-2012-ci illər üçün Dövlət Proqramı" qəbul olunmuşdur ki, bu Proqram əsasında şəxsin şəkli, barmaq izi, səs, DNT və digər biometrik məlumatlar üzrə informasiya sistemləri arasında məlumat mübadiləsinin təşkili - fərdi məlumatlar, o cümlədən biometrik informasiya, həmçinin miqrasiyanın monitorinqi, informasiya təminatı və mühafizəsi sahələrində normativ hüquqi bazanın beynəlxalq standartlara uyğun təkmilləşdirilməsi, biometrik informasiya sahəsində standartlaşmanın və sertifikatlaşdırmanın təşkili, biometrik texnologiyalar əsasında elektron pasport-viza və şəxsiyyəti təsdiq edən digər sənədlərin istehsalının və tətbiqinin təşkili, şəxsin başqa fərdi məlumatlarla sənəd alması imkanının aradan götürülməsi, toplanan informasiyanın dəqiqliyinin təmin olunması, yeni nəsil pasport-viza sənədlərinin fərdiləşdirilməsi ilə şəkil, barmaq izi və digər biometrik məlumatlar üzrə milli informasiya resurslarının formalaşdırılması, mövcud biometrik məlumatların standartlara uyğunlaşdırılması, səs və DNT üzrə biometrik məlumatların qeydiyyatı və istifadəsi üzrə aparıcı xarici dövlətlərin təcrübəsinin və qabaqcıl texnologiyaların mənimsənilməsi, bu sahədə fəaliyyətin təşkili və s. bu kimi istiqamətləri əhatə edir. Hesab etmək olar ki, yaxın gələcəkdə onlayn biometrik servislərin tətbiqi cəmiyyətin təhlükəsizliyinin yüksək səviyyədə təmin olunması üçün geniş imkanlar yaradacaqdır." [1, s.406]

Göründüyü kimi, informasiya təhükəsizliyi aspektindən deyil həmçinin milli, ictimai və dövlət təhlükəsizliyinin təmin edilməsi baxımından da biometrik məlumatlardan istifadə, onları emal etmə, saxlama və ötürmə bacarığı olan informasiya texnologiya vasitələri və tətbiqetmələrdən istifadə zəruridir. Biometrik məlumatlar həmçinin cinayətkarlıqla mübarizədə də misligörülməmiş unikal effektiv təsirə malikdir. Bununla şübhəli şəxslərin və ya əvvəllər məhkum olunmuş şəxslərdən əldə olunmuş biometrik məlumatların şablonları qarşılaşdırıla və bağlı cinayətlərin açılması ilə nəticələnə bilir.

Biometik məlumatlardan informasiya təhlükəsizliyi sferasında identifikasiya və verifikasiya üsulu kimi istifadəsində məhz bu qeyd olunan məsələlərə də anlayış verilməsi vacibdir. Belə ki, bu terminlərə anlayış "Biometrik informasiya haqqında" Azərbaycan Respublikası Qanununda öz əksini tapmışdır. Həmin Qanunun 1-ci maddəsinə əsasən, biometrik texnologiyalar dedikdə informasiya prosesləri zamanı istifadə edilən biometrik məlumatlarla əlaqədar olan informasiya texnologiyaları başa düşülür. Həmçinin biometrik identifikasiya biometrik informasiya ehtiyatında verilmiş biometrik məlumatın mənsub olduğu şəxsin müəyyənləşdirilməsi üçün aparılan sorğu-axtarış işləri üzrə tədbirlərini özündə ehtiva edir. Verilmiş biometrik məlumatla biometrik informasiya ehtiyatında olan biometrik məlumatın müqayisəsi üzrə tədbirlərə biometrik verifikasiya deyilir. Biometrik identifikasiya sisteminin fəaliyyəti biometrik informasiya ehtiyatlarının təyinatına, sorğu, axtarış və müqayisə işləri üz-

rə tələbata əsasən müvafiq dövlət orqanları tərəfindən təşkil edilir və biometrik məlumatların növlərinə uyğun olaraq yaradılan biometrik informasiya xidmətləri vasitəsilə həyata keçirilir. Həmin Qanuna əsasən biometrik informasiya xidmətlərinə aşağıdakılar aiddir:

- üz təsviri üzrə identifikasiya və müşahidə xidməti;
- əl-barmaq və ovuc izləri üzrə identifikasiya və daktiloskopik qeydiyyatı xidməti;
- səs üzrə identifikasiya, analiz və konvertasiya xidməti;
- kağız üzərində yazı xətti və imza üzrə identifikasiya və analiz xidməti;
- DNT üzrə analiz və identifikasiya xidməti;
- fərdi identifikasiya nömrəsi ilə bağlı nəzarət və təhlükəsizlik xidməti;
- gözün qüzehli və tor qişası üzrə identifikasiya və analiz xidməti.

Biometrik informasiya xidmətlərinin yerləşdiyi obyektlər qanunvericiliklə nəzərdə tutulmuş qaydada hüquqi, təşkilati və proqram-texniki vasitələrlə, nəzarət sistemləri ilə mühafizə olunur. [31] Burada xüsusilə bruto-force qeyd olunmalıdır. "Brute-force" - istifadəçinin hər hansı e-mail hesabına və ya digər hesabındakı şifrələr toplusuna edilən hücumdur. Bu zaman istifadəçiyə aid olan məlumatlardan (məsələn, ad, soyad, valideyn və ya övladın adı və doğum tarixləri, maşın nömrəsi, telefon nömrəsi və s.) istifadə edərək manual (əl ilə bir-bir) və ya avtomatik şəkildə müxtəlif vasitələrlə hesabdakı şifrlər yoxlanılır və şifrə (parol) tapılır. Bəs brute-force hücumunun məqsədi nədir? - Social engineering kimi bu hücumlar da istifadəçi haqqında məlumatların toplanması və sonradan həmin məlumatların qeyri-qanuni məqsədlərlə istifadəsi məqsədini daşıyır. Elektron təhlükəsizlik Mərkəzinin tövsiyələrinə görə, belə hücumlardan qorunmaq üçün şifrələrin təhlükəsizliyi qaydalarına riayət olunmalıdır. Məsələn, sosial şəbəkələrdə, maillərdə və ya digər hesablarda eyni şifrə istifadə olunmaması. [2] Çünki belə hal bir hesabdakı şifrənin sındırıldığı halda digər hesabların da "ələ keçməsi"nə gətirib çıxara bilər. Eyni zamanda, yaxşı olar ki, şifrələrin qoyulması zamanı istifadəçi özünə aid məlumatlardan istifadə etməsin. Məsələn, bir qayda olaraq, şifrə qismində ad və ona bitişik formada doğum tarixinin ili, ayı və ya günü istifadə olunur. Belə tip şifrələrin aşkar olunması daha asan olduğu üçün cinayətkarın işi də asanlaşmış olur. Ona görə də istifadəçilərin bu cür şifrələrdən uzaq olması daha məqsədəmüvafiq hesab edilir. Bundan əlavə, istifadəçiyə məxsus şifrənin bədniyyətlinin əlinə keçməməsi üçün ikiqat autentifikasiyadan istifadə olunması müasir və uğurlu bir vasitə kimi qiymətləndirilir. İlkin dövrlərdə daha çox şifrənin yığılması və sonradan mobil qurğuya sms (mesaj) gəlməsi üsulu tətbiq edilirdisə, 2015-ci ildən etibarən ikiqat autentifikasiya üçün ikiqat biometrik şifrələrdən istifadəyə başlandı. Bu o deməkdir ki, yalnız bioloji markerə çevrilmiş barmaq izi deyil, eyni zamanda gözün torlu qişası da identifikasiya üçün istifadə olunur. Mobil bankçılıqda geniş yayılmış bu üsul artıq yeni telefonların son modellərində tətbiq edilir. Hesab edirik ki, biometrik məlumatlar eyniləşdirmə üçün daha "etibarlı" xarakterə malikdir və bu sahədə

tədqiqatların davam etdirilməsi və təcrübəyə tətbiqi informasiya təhlükəsizliyinin təminatında əvəzsiz rola malik ola bilər. Digər tərəfdən isə müxtəlif şifrələrin yadda saxlanmasına nisbətdə biometrik məlumatlardan istifadə etməklə eyniləşdirmə daha asan və rahat olar". [1, s.416; 417]

Göründüyü kimi, biometrik məlumatlar unikal xarakterinə görə girişə icazə sistemlərində şəxsin identifikləşdirilməsi prosesində daha asan və hədəf yönümlüdür. Məhz biometrik məlumatlar və onları dəstəkləyən texnologiyalar informasiya təhlükəsizliyinin təmin edilməsində xüsusi rol oynayır. Hətta onu da qeyd etmək olar ki, məhz bu məlumatlar və sistemlər vasitəsi ilə informasiya təhlükəsizliyi bir çox risklərdən sığortalanır. İnformasiya sistemlərinə və ehtiyyatlarına qanunsuz giriş halları demək olar ki, sıfira enir. Belə ki, giriş sistemlərində identifikəşdirmə üsulu kimi parol, istifadəçi adı və ya digər şifrələrdən istifadə edilməsinə nisbətdə biometrik məlumatlardan istifadə edilməsi informasiya təhlükəsizliyi baxımından daha təhlükəsizdir. Çünki kiberhücumçular və ya informasiya ehtiyyatına qanunsuz giriş əldə etmək istəyən şəxslər birinci halda müəyyən texnoloji üsul və vasitələrdən istifadə etməklə bunu bacara bilirlər. Lakin biometrik məlumatların unikal xarakter və xüsusiyyəti belə qanunsuz girişlərin qarşısını alır. [12, 248]

Qeyd olunanlar biometrik məlumatların və biometik tenologiyaların informasiya təhlükəsizliyinin təmin edilməsi üçün istifadəsinin əhəmiyyətini bir daha təsdiq edir. Məhz informasiya təhlüksizliyinin müasir rəqəmsal informasiya cəmiyyətində az riskli və daha rahat təmin edilməsinin ən əlverişli üsullarından biri biometrik texnologiya, sistem və məlumatlardan istifadəni özündə ehtiva edir. Bununla bir çox informasiya təhlükəsizliyi problemi öz həllini tapır. Nəticədə daha təhlükəsizlik informasiya ehtiyyatı sistemi qurula bilir. Bundan əlavə olaraq bir çox sahələrdə xüsusi mühafizəsi təmin edilən ərazilərə, binalara və digər obyektlərə giriş üsulu biometrik texnologiyalardan istifadə və biometrik məlumatların identifikasiyası və verifikasiyası vasitəsi ilə həyata keçirilir.

İstinadlar:

1. Əliyev Ə.İ., Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S. İnformasiya hüququ. Dərslik. Bakı: Nurlar, 2019, 448 s.

2. İnformasiya təhlükəsizliyi və ona qarşı yönəlmiş hücumlar. // Elektron Təhlükəsizlik Mərkəzinin rəsmi saytı. https://www.cert.az/news/2016/informasiya-tehlukesizliyi-ve-ona-qarsi-yonelmis-hucumlar

3. К вопросу о латентности киберпреступлений. https://infourok.ru/statya-k-voprosu-latentnosti-kiberprestupleniy-1460496.html

4. Платошин Ю.А.Сущность латентной преступности. // Право и образование, 2011, №5, с. 171-176.

5. Рассолов И.М. Право и Интернет: Теоретические проблемы. Москва: Норма, 2009, 383 с.

6. Телешина Н.Н. Виртуальная пространства как новая юридическая конструкция: к постановке проблемы. // Юридическая техника, 2013, №7 (Ч.2), с. 740-747.

7. Туликов А. Интеллектуальная собственность в киберпространстве: правообладатели и общество готовы к диалогу. // Интеллектуальная собственность в киберпространстве: Сборник аналитических материалов проекта "Право и общество в цифровую эпоху". МОО ВПП ЮНЕСКО "Информация для всех". Составитель: Евгений Альтовский, 2006, с. 9-12.

8. Creation of a global culture of cybersecurity: resolution / United Nations General Assembly (UNGA) Resolution 57/239, 31 January 2003. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unga-creation-global-culture-cybersecurity

9. Darrel C. Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces. // Michigan Telecommunications and Technology Law Review, 1998, Volume 4, Issue 1, p. 69-103.

10. Debra Littlejohn Shinder. Scene of the Cybercrime: Computer Forensics Handbook. Canada: Syngress Publishing, Inc., 2002, 749 p.

11. Dorothy J. Glancy. The invention of the right to privacy. // Arizona Law Review, 1979, Volume 21 (1), http://law.scu.edu/wp-content/uploads/Privacy.pdf

12. Dutfield G. Global intellectual property law: commentary and materials / Graham Dutfield [and others]. Northampton, MA: Edward Elgar Pub., 2005, pp. 238-252.

13. Fiordalisi E. The Tangled Web: Cross-Border Conflicts of Copyright Law in the Age of Internet Sharing. // Loyola University Chicago International Law Review, 2015, Vol. 12, İssue 2, pp. 197-213.

14. Gibson W. Burning chrome. Canada, 1982. http://project.cyberpunk.ru/lib/burning_chrome/

15. Gibson W. Neuromancer. First edition, 1984, 271 p.

16. John Arquilla and David Ronfeldt. Cyberwar is coming! // National Security Research Division. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

17. Human Rights in the Global Information Society (Information Revolution and Global Politics). Edited by Rikke Frank Jorgensen, London: The MIT Press Cambridge, Massachusets, 2006, 323 p.

18. KINDT, E. J. Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis . Dor-drecht: Springer, 2013. See p. 349, 351-352

19. Martin C. Libicki. What Is Information Warfare? Washington, 1995, 104 p.

20. MATEJKA, J., KRAUSOVÁ, A., GÜTTLER, V. Biometrické údaje a jejich právní režim. Revue pro právo a technolo-gie. 2018, Vol. 9, No. 17, [2018-07-10]. Available at: <https://journals.muni.cz/revue/article/view/8801/pdf>

21. National information society policy: A template. Developed by The Information For All Programme of UNESCO. Paris November 2009, 143 p.

22. Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech". / Adopted on 30 October 1997 by Committee of Ministers of Council of Europe. https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-97-20-of-the-committee-of-ministers-to-member-states-on-hate-speech-?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/

23. Recommendations of the Electronic Security Center for the prevention and elimination of the consequences of information security incidents. // Electronic Security Center, 2014. https://www.cert.az/s/u/document/tovsiye.pdf,

24. Richard R. Bartle. Designing Virtual Worlds. New Riders, 2003, 741 p.

25. Samuel D. Warren, Louis D. Brandeis. The Right to Privacy. // Harvard Law Review, 1890, Vol. 4, No. 5, p. 193-220.

26. Solarczyk Krausová, Alžběta & Hazan, Hananel & Matejka, Ján. (2018). Biometric data vulnerabilities: Privacy implications. Lawyer Quarterly. 8. 295-306. P.300

27. Understanding Cybercrime: A Guide For Developing Countries. ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector Draft April 2009, 225 p.

28. W.Lambert Gardiner. Virtual Reality/Cyberspace: Challenges to Communication Studies//Canadian Journal of Communication, 1993, Vol 18 (3). http://www.cjc-online.ca/index.php/journal/article/view/762/668

29. William L.Prosser. Privacy. // California Law Review, 1960, Volume 48 (3), p. 383-423.

30. https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf15.02. 2023

31. https://e-qanun.az/framework/15144 . 10.09.2023

32. https://gdpr-info.eu/art-4-gdpr/ . 10.02.2023.

33. http://virtualaz.org/

34. http://www.dictionary.com/browse/virtual-environment

35. http://www.virtualkarabakh.az/index.php?lang=3

36. https://www.eff.org/cyberspace-independence

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИОМЕТРИЧЕСКИХ ДАННЫХ И ПРАВИЛА ИХ ИСПОЛЬЗОВАНИЯ

Айтекин Ибрагимова*

Резюме

Биометрические данные включают личную информацию об уникальных физических или поведенческих характеристиках человека, которые могут быть использованы для идентификации или идентификации. Сегодня биометрические данные уже используются практически во многих областях. Даже информационные технологии развились настолько, что сегодня компьютер, планшет, телефон, смарт-часы и т. д. используются ежедневно. Системы сбора, обработки, использования и хранения биометрических данных, в том числе уничтожения, применяются во многих инструментах информационных технологий. Все это делает необходимым четкое правовое регулирование биометрических данных. Биометрические данные все чаще используются в различных сферах для обеспечения информационной безопасности и идентификации личности. Автор анализирует правила, которые могут обеспечить информационную безопасность биометрических данных. В определенных случаях изучается безопасное раскрытие таких данных.

Ключевые слова: биометрические данные, персональные данные, биометрическая идентификация, шифрование, биометрические технологии, информационная безопасность.

* д.ф.п.п., доцент кафедры конституционного права Бакинского государственного университета

INFORMATION SECURITY OF BIOMETRIC DATA AND RULES OF THEIR USE

Aytekin Ibrahimova*

Abstract

Biometric data includes personal information about a person's unique physical or behavioral characteristics that can be used for identification or identification. Biometric data is already used in almost many fields today. Even the information technology has developed so much that today the computer, tablet, phone, smart watch, etc. are used daily. Systems that collect, process, use and store biometric data, including destruction, are applied in much information technology tools. All this makes it necessary to have a clear legal regulation on biometric data. Biometric data is increasingly used in various fields for information security and identity identification purposes. The rules that can ensure information security of biometric data are analyzed by the author. In certain cases, the safe disclosure of such data is studied.

Keywords: biometric data, personal data, biometric identification, encryption, biometric technologies, information security

* Ph.D, Associate Professor of the Constitutional Law Department of Baku State University