# Big Data və Fərdi Məlumatların Təhlükəsizliyi

Yadigar İmamverdiyev
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
*yadigar@lan.ab.az*

***Xülasə* — Big data üçün fərdi məlumatların təhlükəsizliyi kritik əhəmiyyətli məsələdir. Bu işdə Big data texnologiyalarının fərdi məlumatlara yaratdığı təhdidlər və bu təhdidləri qarşılamaq üçün fərdi məlumatlar sahəsində qanunvericiliyin təkmilləşdirilməsi çağırışları analiz edilir. Big data texnologiyalarında fərdi məlumatların təhlükəsizliyi üçün mövcud texnoloji yanaşmalar analiz edilir və müvafiq elmi tədqiqat istiqamətləri haqqında məlumat verilir.**

***Açar sözlər — Big data; fərdi məlumatlar; fərdi məlumatların təhlükəsizliyi; diferensial gizlilik***

## I. GİRİŞ

Fərdi məlumatlar – şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatlardır [1]. Fərdi məlumatlar toplandığı andan mühafizə olunmalı və yalnız toplandığı məqsədlər üçün istifadə edilməlidir. Konfidensial fərdi məlumatlar qanunla müəyyən olunmuş hallar istisna olmaqla, üçüncü şəxslərə yalnız subyektin razılığı əsasında verilə bilər.

Big Data texnologiyaları fərdlər barəsində toplanan məlumatların dairəsini və mənbələrini hədsiz dərəcədə genişləndirir. Müxtəlif sosial-iqtisadi aktorlar istifadəçilər haqqında olduqca çox fərdi məlumatlar – istifadəçinin veb-saytlardakı və sosial şəbəkələrdəki davranışı, istifadəçi ilə əlaqəsi olan şəxslərin davranışları və əlaqələri, onların alış-veriş davranışları və s. Toplayırlar. Bundan başqa, sosial şəbəkədə ünsiyyətin emosional çalarlarını da analiz etmək mümkündür. İstifadəçinin sosial mediada nə yazdığı ilə yanaşı, necə yazdığı da analiz edilir. Bir sözlə, potensial istifadəçi barəsində vacib və ya lazımsız görünən hər bir məlumat toplanır və onun “360 dərəcəlik” profili yaradılır [2-4].

Nəticədə Big Data texnologiyaları şəxsi həyatın toxunulmazlığı baxımından ciddi problemlər yaradır. Lakin universal, heç nə ilə məhdudlaşdırılmayan hüquqlar yoxdur. Xüsusi halda, vətəndaşların şəxsi həyatının toxunulmazlığı hüquqları, məsələn, təhlükəsizliyin təmin olunması və ciddi cinayətlərlə mübarizə sahəsində cəmiyyətin qanuni maraqları ilə məhdudlaşdırılır.

Hələ 1967-ci ildə filosof Marşall Maklyuen qeyd edirdi ki, «insanın beşikdən qəbrədək hərtərəfli izlənilməsinə xidmət edən elektrik informasiya qurğuları insanın şəxsi sirlərini qorumaq cəhdləri ilə cəmiyyətin məlumat ehtiyacları arasında olduqca ciddi dilemma yaradır» [5]. ABŞ Milli Təhlükəsizlik Agentliyinin fəaliyyəti haqqında E. Snoudenin açıqlamaları göstərdi ki, Maklyuenin «ciddi dilemması» reallığa çevrilib – müasir izləmə texnologiyaları və Big Data analitikası sayəsində insanların şəxsi həyatının toxunulmazlığı böyük təhlükə altındadır [6].

Big Data texnologiyaları strateji, taktiki və operativ səviyyələrdə yaxşı əsaslandırılmış mürəkkəb qərarların qəbul edilməsinə və müxtəlif funksional sahələrdə yeni həllərin və məhsulların yaradılmasına şərait yaradır. Buna görə Big Data texnologiyaları, onların biznes perspektivləri, tətbiqləri və böyük miqyaslı yüksək məhsuldarlıqlı intellektual analiz sahəsində bir çox tədqiqat işləri aparılmışdır. Lakin Big Data müstəsna faydalı məlumatlar versə də, verilənlərin toplanması, saxlanması, saxlanma müddəti, təhlükəsizliyi və gizliliyi ilə bağlı yeni problemlər də yaradır və bu problemlər yalnız son illər tədqiqatçıların diqqətini cəlb etməkdədir [7,8].

Bu işin məqsədi Big Data baxımından fərdi məlumatların təhlükəsizliyi üzrə elmi-praktiki tədqiqatların müasir vəziyyətini analiz etmək və aktual tədqiqat istiqamətlərini müəyyən etməkdir.

## II. BİG DATA: FƏRDİ MƏLUMATLARIN MƏNBƏLƏRİ

Ənənəvi informasiya texnologiyaları strukturlaşdırılmış verilənlərdən istifadə edir və bunun nəticəsində yaxın vaxtlara kimi IT-bazarın liderləri verilənlər bazalarını idarəetmə sistemlərinin istehsalçıları idi (Oracle, SAP və s.). Lakin hazırda mühüm yerdəyişmə baş verməkdədir – verilənlərin çox sayda yeni mənbələri meydana çıxır, təkcə sosial şəbəkə servislərini və mobil texnologiyaları yada salmaq kifayətdir. Bu verilənlər çox zaman strukturlaşdırılmayıb, olduqca müxtəlif formatlara malikdirlər, böyük sürətlə yaranırlar və həcmləri kəskin sıçrayışla artır. Belə informasiya axınının mövcud texnologiyalarla emalı mümkün deyil və yeni texnologiyalar tələb edilir. Big Data texnologiyaları müxtəlif mənbələrdən alınmış strukturlaşdırılmamış verilənlərin real zamanda emalını mümkün edir.

Biliyin, informasiyanın əsas qeyri-maddi aktiv olduğu sahələr – maliyyə, satış, marketinq, idarəetmə sahələri böyük həcmdə toplanan fərdi məlumatların əsas istehlakçılarıdır. Son dövrlər hüquq-mühafizə orqanları və milli təhlükəsizliyi təmin edən strukturlar cinayətkar və terrorçu elementlərin daha dəqiq aşkarlanması üçün Big Data ideyalarından istifadə edilməsində maraqlıdırlar. Müşahidə kameralarının məlumatları, sosial şəbəkələrdəki yazışmalar və paylaşılan multimedia məlumatları, veb-saytların loq-faylları, mobil və ənənəvi rabitə ilə danışıqlar, elektron xidmətlərin tranzaksiyaları yaxşı məlum olan Big Data mənbələridir.

Big Data texnologiyalarının marketinq məqsədləri üçün istifadəsinə yol açanlar onlayn-topdansatış mağazalarıdır.

Oflayn mağazalardan fərqli olaraq, onların İnternet sayəsində öz alıcılarının davranışı ilə bağlı bütün verilənləri analiz etmək üçün unikal imkanları var. Onlar olduqca müxtəlif verilənlər – müştərinin veb-saytlardakı və sosial şəbəkələrdəki davranışı, müştərinin əlaqəli olduğu şəxslərin davranışları, alış-veriş davranışları, kredit tarixçələri və s. haqqında müxtəlif məlumatlar toplayırlar.

Big data verilənlərinin 15-20%-i "Əşyaların İnterneti", o cümlədən, çoxsaylı telefonlar, planşetlər və digər qurğular tərəfindən generasiya edilir. "Əşyaların İnterneti" tərəfindən generasiya edilən verilənlərin payı 2020-ci ildə 40%-ə çatacaq.

Müasir tibb texnologiyaları tibbi yardımın göstərilməsi ilə bağlı böyük həcmdə verilənlər generasiya edir (şəkillər, video, real vaxt rejimində monitorinq). Artıq bu gün daşınan elektronika və sensor texnologiyaları insanın sağlamlıq vəziyyəti haqqında verilənləri real zamanda təqdim edə bilirlər. Sensor texnologiyaları mütəxəssislərə xroniki xəstəliyi olan pasiyentlərin vəziyyətini uzaqdan monitorinq etməyə və onlara vaxtında kömək göstərməyə imkan verir [9].

Tibbi sənədlərin ənənəvi formalardan elektron formalara keçirilməsi nəticəsində də böyük həcmdə fərdi məlumatlar informasiya sistemlərinə daxil olur.

Dövlət sektoru da çox böyük həcmdə verilənlər toplayır və bu verilənlərin 70%-i strukturlaşdırılmayıb, müxtəlif sənədlər – planlar, hesabatlar, ərizələr, şikayətlər, təkliflər… şəklində saxlanır. Bu verilənlərin həcmi daim artır və dünya üzrə illik artım sürəti 30%-dir. Vətəndaşlar daim bu və ya digər şəkildə dövlət orqanları ilə ünsiyyətdə olurlar, elektron dövlətin formalaşdırılması sayəsində bu ünsiyyətin intensivliyi və nəticədə e-xidmət sistemlərində toplanan fərdi məlumatların həcmi kəskin şəkildə artır.

## III. BİG DATA VƏ FƏRDİ MƏLUMATLARA TƏHLÜKƏLƏR

Big Data texnologiyalarından istifadə etmək imkanı olan müxtəlif subyektlər fərdi məlumatları toplayırlar. Bu zaman bir sıra suallar meydana çıxır. Məsələn, şirkətlərin qanuni yolla hansı verilənləri toplamaq hüququ var?

Fərdi verilənlər çox zaman fərdlərin razılığı olmadan toplanır və çox nadir hallarda fərdlərin bu verilənlərin aqreqasiyasına və başqa məqsədlər üçün istifadə edilməsinə razılığı alınır. Bu fərdi məlumatların sui-istifadə ssenariləri olduqca rəngarəngdir.

İnsanların öz fərdi məlumatlarına nəzarət etmək və idarə etmək imkanları yoxdur. Fərdi məlumatların həcmi artdıqca istifadəçilərin hansı məlumatları, nə zaman, kiminlə paylaşdıqlarına nəzarət etmələrinə imkan verən mexanizmlər əlyetər olmalıdır.

Daha bir təhlükə ondadır ki, Big Data texnologiyaları sayəsində şirkətlər haqqımızda həssas və şəxsi faktları bizdən almadan, müxtəlif mənbələrdən topladıqları məlumatları birləşdirməklə birbaşa nəticə çıxararaq əldə edə bilərlər.

Big Data texnologiyaları məhsuldarlığı yüksəltmək və yeni biznes-prosesləri təkmilləşdirmək məqsədilə əməkdaşlar haqqında müfəssəl məlumatlar toplamaq üçün istifadə edilir. Lakin əməkdaşların daim izlənməsi təşkilatlarda gərgin atmosfer yarada bilər.

Bundan başqa, böyük həcmdə multimedia verilənlərinin yayılması genişləndikcə açıq və konfidensial verilənlər arasında sərhədlər yox olur. Video-verilənləri sosial şəbəkələrə yükləməyə imkan verən onlayn proqramlar insanı mahiyyətcə videokameraya çevirir. Lakin video-müşahidə kameralarından fərqli olaraq smartfonlar, məsələn, təsadüfən kadra düşən şəxslər üçün konfidensiallığın qorunmasını təmin etmirlər. Məsələn, Bostonda partlayışların təhqiqatı zamanı bir neçə nəfər terror aktının törədildiyi yerdə çəkilmiş fotoşəkillərin sosial şəbəkə saytlarında yerləşdirilməsindən sonra şübhəlilər sırasına düşmüşdü.

De-identifikasiya yanaşması təklikdə fərdi məlumatların təhlükəsizliyi üçün yetərli həll deyil. Əlavə mənbələrdən verilənlər cəlb etməklə məlumatların re-identifikasiya edilməsi imkanları da kifayət qədər realdır [10].

Bəzi fərdi məlumatlar şəxs barəsində qərar qəbul edilməsi, onun diskriminasiyası üçün istifadə edilə bilər.

Big Data fərq qoymadan bütün verilənləri toplamağa imkan verir. Verilənlər yeni kəşflər ediləcəyini, yeni məhsullar və servislər yaradılacağını vəd edirlər. Lakin bu verilənlərin gigiyenası üzrə “birinci qanuna” ziddir: verilənləri, xüsusilə də fərdi məlumatları ehtiyac olmadan toplamayın və saxlamayın. Bu qanunu Big Data əsrində ləğv etmək lazımdır, yoxsa hər yerdə hər veriləni toplamaq lazımdır; yaxud verilənlərin toplanmasını məhdudlaşdırmaq Big Data potensialını məhdudlaşdırırmı?

Big Data və fərdi məlumatların təhlükəsizliyi problemləri üzrə Gizliliyin Gələcəyi Forumunun və Stenford Internet və Cəmiyyət Mərkəzinin birgə təşkil etdiyi “Big Data and Privacy: Making Ends Meet” seminarının əsərlər toplusu yaxşı mənbədir [11]. Bu toplu aşağıdakı əsas suallardan bəzilərinə ünvanlanıb: Big Data yeni çağırışlar gətirirmi, yoxsa sadəcə verilənlərin tənzimlənməsi müzakirələrini yenidən gündəmə gətirir? Big data vətəndaş azadlıqlarına təhdid törədən prinsipcə yeni imkanlar yaradırmı? De-identifikasiya və digər texnoloji və ya inzibati tədbirlər gizlilik risklərini yetərincə azaldırmı? Verilənlərin minimallaşdırılması kimi gizlilik konsepsiyaları Big Data sahəsində hansı rolu oynamalıdır? Digər sahələrdə alınmış hansı dərslər tətbiq edilə bilər?

Massaçusets Texnologiya İnstitutunda “Big Data və fərdi məlumatların təhlükəsizliyi problemləri üzrə işçi qrup” (MIT Big Data Privacy Working Group) 2013-cü ildən başlayaraq bir neçə seminar keçirmişdir. Həmin işçi qrup fərdi məlumatların təhlükəsizliyində Big data texnologiyalarının təbiətindən irəli gələn aşağıdakı xüsusiyyətləri diqqətə çatdırır [12]:

**Miqyas:** Verilənlərin həcminin nəhəng olması gizlilik siyasətlərinin yaradılmasına, idarə edilməsinə və tətbiqinə ciddi problemlər yaradır.

**Müxtəliflik:** Big Data toplanmasına, idarə edilməsinə və istifadəsinə müxtəlif iştirakçılar cəlb edilir və onların məqsəd və hədəflərindəki fərqlər ziddiyyətlərə gətirib çıxarır.

**İnteqrasiya:** Verilənlərin idarə edilməsi texnologiyalarının inkişafı ilə (məsələn, bulud servisləri) müxtəlif verilənlər

topluları arasında inteqrasiya artır və məntiqi çıxarışlar əsasında fərdlər və onların davranışları haqqında yeni informasiya almaq imkanı genişlənir.

**Digər iştirakçılara təsiri:** Məlumatların bir çox hissəsi təkcə hədəf subyektə deyil, həm də digər, çox zaman istəməyərəkdən iştirak edən şəxslərə aid ola bildiyindən, məntiqi çıxarış nəticəsində alınmış yeni informasiya da gizliliyin subyekti olmayan digər şəxslərə aid ola bilər.

**Yeni informasiya üçün yeni siyasətin zəruriliyi:** Birləşdirilən verilənlər yeni məntiqi nəticələr verdikdə yeni informasiya və ya anlayışlar ortaya çıxır. Hər bir verilənlər toplusu mövcud gizlilik siyasətinə və həyata keçirilmə mexanizmlərinə malik ola bilər, lakin yeni məlumatlar üçün rekvizitlərin, uyğun gizlilik siyasətlərinin və müvafiq reallaşdırma mexanizmlərinin avtomatik yaradılmasına ehtiyac vardır.

Təşkilat daxilində fərdi məlumatların təhlükəsizliyi ilə bağlı aşağıdakı tövsiyələri vermək olar [12]:

- fərdi məlumatların təhlükəsizliyi risklərini qiymətləndirmək üçün təşkilat daxilində yeni rollar yaradılmalıdır;
- Big Data layihələrinin başlanğıc mərhələsində fərdi məlumatların təhlükəsizliyi riskləri qiymətləndirilməlidir;
- ilkin mərhələdən başlayaraq istifadəçilər üçün şəffaflıq təmin edilməlidir – verilənlərin toplanmasının məqsədlərini və gələcək istifadə potensialını aydın göstərmək zəruridir;
- verilənlərin saxlanması mühiti müntəzəm qiymətləndirilməli və istifadə modellərinin öyrənilməsi təmin edilməlidir;
- təhlükəsizlik mexanizmləri verilənlərə yaxın yerləşdirilməli və fərdi məlumatların bütün növləri üçün şifrələmədən istifadə edilməlidir;
- təşkilatlar mövcud və potensial müştərilərinin etimadını qorumaq üçün fərdi məlumatların qanun və etik normalar çərçivəsində istifadə edilməsini və istənilən növ konfidensial fərdi məlumatlara müraciətlərin qeydiyyata alınmasını və monitorinq edilməsini təmin etməlidirlər.

## IV. BİG DATA VƏ FƏRDİ MƏLUMATLAR ÜZRƏ QANUNVERİCİLİYİN TƏKMİLLƏŞDİRİLMƏSİ

Big Data texnologiyalarının inkişafı fərdi məlumatların təhlükəsizliyinin təmin edilməsinin qanunvericilik bazasına yenidən baxılmasını zəruri edir [13]. Bu sahədə Avropa təşəbbüslərinə nəzər salmaq vacibdir.

Avropa Komissiyası 2015-ci ilin sonuna qədər fərdi məlumarların qorunması sahəsində yeni Avropa qanununun (General Data Protection Regulation, GDPR) qəbulu üçün lazım olan bütün razılaşmalara nail olmağı planlaşdırır [14]. Qüvvədə olan "EU Data Protection Directive 95/46/EC" təlimatından fərqli olaraq, yeni qanun Avropa Birliyinə üzv-ölkələrdə səsvermə keçirilmədən "birbaşa" qüvvəyə minəcək və icrası məcburi olacaq.

Fərdi məlumatların qorunması sahəsində dəyişikliklərə ehtiyac həm də Avropa iqtisadiyyatının rəqabət qabiliyyətinin yüksəldilməsi ilə əlaqəlidir. Bəzi qiymətləndirilmələrə görə, Avropa vətəndaşlarının fərdi məlumatlarının illik dəyəri 2020-ci ildə təxminən 1 trilyon avroya çatacaq. Ona görə fərdi məlumatların emalı sahəsində yüksək Avropa standartlarının bərqərar edilməsi biznesin inkişafına xidmət etməyə yönəlib. Məqsəd Big Data və bulud servislərinin Avropada inkişafını dəstəkləməkdir. Hansı ölkədən gəlmələrinə baxmayaraq, Avropada fəaliyyət göstərən bütün şirkətlərə fərdi məlumatların emalı üzrə eyni qaydalar tətbiq ediləcək. Eyni zamanda, kiçik şirkətlərin fərdi məlumatlar bazarına girişi də asanlaşdırılır. Qanunun fərdi məlumatların emalı sahəsində pərakəndəliyi aradan qaldıracağı və inzibati xərcləri ildə təxminən 2,3 milyard avro azaldacağı da gözlənilir [14].

Avropa Birliyinə üzv-ölkələr üçün yeni, vahid qanunvericilik fərdi məlumatların qorunması üzrə tələblərin icrası ilə bağlı xərcləri, xüsusilə kiçik və orta müəssisələr üçün əhəmiyyətli dərəcədə azaltmağa imkan verəcək. Beləliklə, vahid qanunvericilik təşkilatların hakimiyyətlə qarşılıqlı əlaqəsini elə təşkil etməyə imkan verəcək ki, fərdi məlumatların qorunması üzrə qeydiyyat ölkəsindəki təşkilat vahid əlaqə nöqtəsinə çevriləcək. Müvafiq olaraq, yeni qanunvericilik Avropa Birliyinə üzv-ölkələrin güc strukturları arasında fərdi məlumatların mübadiləsini də sadələşdirəcək.

Vətəndaşlara öz fərdi məlumatlarına baxmaq və düzəliş etmək hüququ, verilənlərin emalına etiraz etmək hüququ, verilənlərin sızması baş verdikdə məlumatlandırılmaq hüququ, unudulmuş olmaq hüququ (yəni, fərdi məlumatlarının operator tərəfindən dərhal, izafi rəsmiyyət olmadan məhv edilməsini tələb etmək hüququ) verilir. Bu hüquqların başqa şəxslərin və təşkilatların hüquq və azadlıqlarına, bütövlükdə cəmiyyətin maraqlarına zidd olmaması gözləniləcək. Vətəndaşlar üçün əsas faydalar vətəndaşların fərdi məlumat operatorlarına etibarının artmasından yaranacaq, bu onlara daha geniş onlayn-xidmətlərdən istifadə etməyə imkan verəcək (və eyni zamanda bu iqtisadiyyatın "elektron" sektorunun artmasına imkan yaradacaq).

Autentifikasiyanın gücləndirilməsi yeni qanunun tələblərinin qanunauyğun nəticəsidir. Fərdi məlumatların itkisi haqqında məcburi məlumat verilməsi və fərdi məlumatların itkisinə görə yüksək cərimələr qaçılmaz olaraq "fərdi məlumatların emalı zamanı daha enerjili müdafiə tədbirlərinin" görülməsinə gətirib çıxaracaq [15].

GDPR layihəsinin mətnində göstərilir ki, yeni qanunu pozmuş təşkilatlar ümumi gəlirin 2 %-inə kimi cərimələnə bilərlər. Əgər şirkət məlumat itkisinin qarşısını almaq üçün bütün mümkün tədbirləri gördüyünü sübut edə bilsə, onda daha yumşaq cəza tətbiq ediləcək.

Ehtimal olunur ki, fərdi məlumatların qorunması sahəsində Avropa Birliyinin yeni islahatları sanksiyalar rejiminin xeyli sərtləşməsinə gətirib çıxaracaq. Bununla əlaqədar olaraq, biznes dairələri Avropa qanunvericilərindən və nəzarət orqanlarından yeni qanunun daha aydın şərhini, xüsusi halda təhlükəsizlik tələblərinə uyğunluq üçün çoxpilləli

autentifikasiya və ya digər müdafiə tədbirləri daxil olmaqla, hansı tədbirlərin qəbul edilməsinin zəruri olduğunu aydınlaşdırmağı tələb edəcəklər.

Son illər ölkəmizdə fərdi məlumatlar sahəsində bir sıra normativ hüquqi aktlar qəbul edilmişdir, o cümlədən "Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında" 1981-ci il yanvarın 28-də Strasburq şəhərində imzalanmış Konvensiya müvafiq bəyanatlarla təsdiq edilmiş (2009-cu il) və "Fərdi məlumatlar haqqında" Azərbaycan Respublikası Qanunu qəbul edilmişdir (2010-cu il). Bununla yanaşı, Big Data reallıqlarını nəzərə almaqla fərdi məlumatlar üzrə milli qanunvericiliyin təkmilləşdirilməsinə zərurət yaranır.

## V. FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİ ÜZRƏ TEXNOLOJİ YANAŞMALAR

Analiz göstərir ki, aşağıdakı istiqamətlərdə praktiki həllərin işlənilməsi zəruridir [16]: 1) Big Data verilənlərinin təhlükəsiz və gizliliyin qorunması ilə toplanması və emalı; 2) Big Data analizinin təhlükəsiz mühitdə və gizliliyin qorunduğu şəkildə həyata keçirilməsi; və 3) Big Data sistemləri üçün verilənlərin saxlanılması siyasətinin təhlükəsiz (və gizlilik rejimində) tətbiqi. Əgər bu həllər lazımi səviyyədə olmasa, insanların öz fərdi məlumatlarını Big Data sistemlərinə təqdim etməsi istəyi azalır.

"Fərdi məlumatların təhlükəsizliyinə cavabdeh təşkilatlar adətən de-identifikasya üsullarından, o cümlədən, anonimlik (*anonymization*), təxəllüs (*pseudonymization*), şifrləmə (*encryption*), açar-kodlaşdırma (*key-coding*) və s. istifadə edirlər. Anonimlik ad, ünvan və sosial təhlükəsizlik nömrələrini silməklə gizliliyi təmin edirsə, təxəllüs bu informasiyanı ləqəb və süni identifikasiya ilə əvəz edir. Açarla kodlaşdırma fərdi məlumatları kodlaşdırır və onların dekodlaşdırılması üçün açar yaradır" [17,18].

Tibbi məlumatların de-identifikasiyası üçün ABŞ federal qanunu HIPAA (Health Insurance Portability and Accountability Act – tibbi sığortanın portativliyi və hesabatlılığı) iki metod irəli sürür [9]:

- ***Təhlükəsiz liman:*** fərdin və ya qohumlarının, ailə üzvlərinin və ya işə götürənlərin 18 spesifik identifikatorunun silinməsi tələb edilir: adlar, ünvanlar, tarixlər, telefon nömrələri, faks nömrələri, tibbi sığorta nömrələri, elektron poçt ünvanları, sosial sığorta nömrələri, tibbi sənədləşmə nömrələri, hesab nömrələri, lisenziya/sertifikat nömrələri, maşın identifikatorları və seriya nömrələri, qurğu identifikatorları və seriya nömrələri, URL (universal resource locator), IP-ünvanlar, biometrik identifikatorlar, üzün tam fotoşəkilləri və identifikasiyanın başqa unikal nömrəsi, xarakteristikası və ya kodu.
- ***Statistik metod:*** müvafiq təlim görmüş şəxs identifikatorların kifayət qədər silindiyini yoxlayır.

Texnoloji yanaşmalardan biri də bu sahədə yeni kriptoqrafik alqoritmlərin işlənməsidir. Klassik şifrləmə üsulları artıq yetərli deyil və şifrlənmiş verilənlər üzərində hesablamalar aparmağa imkan verən üsulların işlənməsi tələb edilir:

***Funksional şifrləmə*** – şifrlənmiş məlumat əsasında müəyyən $f$ funksiyasının qiyməti hesablanır: $m$ açıq məlumatının şifrlənmiş mətninə əsasən $f(m)$ hesablanır, bu zaman $m$ haqqında (o cümlədən, $f$-in hesablanması zamanı aralıq nəticələr haqqında) hər hansı əlavə məlumat əldə etmək mümkün olmamalıdır. İlk funksional şifrləmə sxemi [19] yalnız funksiyaların bəzi siniflərində işləyirdi (monoton funksiyalar və skalyar hasil), hazırda istənilən funksiyaya tətbiq edilə bilən funksional şifrləmə sxemləri təklif edilib [20].

***Diferensial gizlilik*** metodu fərdi məlumatlara müraciətləri alqoritm və interfeys (etibarlı kurator kimi çıxış edir) vasitəsilə idarə edir [21]. Tədqiqatçı verilənləri analiz etmək üçün kuratora sorğu göndərir və kurator da təsadüfi küy əlavə etməklə verilənlərin konfidensiallığını qorumağa və eyni zamanda sorğulara düzgün cavab verməyə çalışır.

Diferensial gizliliyin tərifində iki $D$ və $D'$ verilənlər çoxluğuna baxılır. $D$-də verilmiş fərdin məlumatları var və bu məlumatlar $D'$-də silinib (və ya hər hansı əlaqəsi olmayan məlumatlarla əvəzlənib). Tələb olunur ki, prosesin sonunda $D$ və $D'$-ni bir-birindən fərqləndirmək mümkün olmasın. Fərqləndirməmə $\varepsilon$ parametrindən istifadə etməklə ölçülür. $\varepsilon$ parametri $D$ və $D'$-dən alınmış nəticələrin paylanmasının nə dərəcədə yaxın olmasını ölçür. $\varepsilon$ kiçik olduqda gizliliyin təhlükəsizliyi səviyyəsi yüksək olur.

Verilənlərin müxtəlif növləri üzərində analitik məsələlər üçün diferensial gizlilik alqoritmlərinin işlənməsi sahəsində bir çox tədqiqatlar mövcuddur [21,22].

***Homomorf şifrləmə*** sistemi şifrlənmiş məlumatlar üzərində məlumatları deşifrləmədən riyazi əməliyyatlar (məsələn, toplama, çıxma, birləşmə, kəsişmə) aparmağa imkan verir. Bu şifrləmə sistemi fərdi məlumatların qorunması, elektron səsvermə, maliyyə məlumatlarının emalı, tövsiyə sistemlərində tətbiq edilə bilər. Ən uğurlu hesab edilən homomorf şifrləmə sistemi 2009-cu ildə IBM şirkətinin kriptoqrafları tərəfindən təklif edilib və IBM tərəfindən patentləşdirilib [23].

***CryptoDB*** – şifrlənmiş verilənlər bazasında SQL sorğularının yerinə yetirilməsi üçün verilənlər bazasını idarəetmə sistemidir (VBİS). CryptoDB ənənəvi VBİS-lərdə (MySQL, Postgres) və tətbiqi proqramlarda dəyişiklik edilməsini tələb etmir. Eyni zamanda, CryptoDB-nin gətirdiyi əlavə yüklənmə də çox deyil: MySQL ilə müqayisədə etalon testlərə görə (TPC-C performance) məhsuldarlıq itkisi 26%-dir [24].

## NƏTİCƏ

Big Data texnologiyaları fərdi məlumatların təhlükəsizliyi baxımından ciddi problemlər yaradır. Bu texnologiyalar sayəsində fərdi məlumatlardan sui-istifadə edilməsinin mənfi nəticələri təkcə ayrı-ayrı insanların şəxsi həyatlarının gizliliyinin pozulmasında deyil, ictimai həyatda, iqtisadiyyatda və siyasətdə də özünü göstərə bilər. Bu problemlərin aradan qaldırılması üçün Big Data texnologiyalarının insan həyatında oynamağa başladığı rolu yenidən qiymətləndirmək tələb edilir.

Eyni zamanda, fərdi məlumatlar sahəsində milli qanunvericiliyin təkmilləşdirilməsi və fərdi məlumatların konfidensiallığını dəstəkləyən texnoloji alətlərin yaradılması olduqca zəruridir. Big Data sahəsində fərdi məlumatların təhlükəsizliyi üzrə bir sıra çətin texnoloji problemlərin həlli: səmərəli şifrləmə və deşifrləmə alqoritmlərinin, şifrlənmiş informasiyada axtarış metodlarının, atribut əsasında şifrləmə alqoritmlərinin işlənməsi, Big Data əlyetənliyinə, etibarlığına və tamlığına hücumların aşkarlanması metodlarının işlənməsi aktual tədqiqat problemləridir.

## ƏDƏBİYYAT

[1] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu. 11 may 2010-cu il.

[2] T. M. Payton, T. Claypoole. Privacy in the age of Big Data: Recognizing threats, defending your rights, and protecting your family. Rowman& Littlefield Publishers. 2014.

[3] C.L. Borgman. Big Data, Little Data, No Data: Scholarship in the Networked World. MIT Press. 2015.

[4] M.Smith, C.Szongott, B.Henne, G. von Voigt, “Big data privacy issues in public social media,” 6th IEEE International Conference on Digital Ecosystems Technologies (DEST), pp.1-6, 18-20 June 2012.

[5] M. McLuhan, Q. Fiore. The Medium is the Massage: An Inventory of Effects. Random House, 1967.

[6] L. Li, M. F. Goodchild and S. Barbara, “ Is Privacy Still an Issue in the Era of Big Data — Location disclosure in spatial footprints”, Proceedings of 21st International conference on Geoinformatics, IEEE, pp.1-4, 2013.

[7] CSA: Top Ten Security and Privacy Issues. November 2012.

[8] R.Alguliyev, Y.Imamverdiyev, “Big Data: Big Promises for Information Security,” IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), 2014.

[9] M. Мамедова, “Проблемы информационной безопасности персональных данных в условиях электронной медицины,” Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş “İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı” nın əsərləri, 14 may 2015, s.52-55.

[10] J. Sedayao, R. Bhardwaj and N. Gorade, “Making Big Data, Privacy, and anonymization work together in the enterprise: Experiences and issues”, IEEE International Congress on Big Data, pp.1-7, 2014.

[11] O. Tene, J. Polonetsky, “Big Data for All: Privacy and User Control in the Age of Analytics,” Northwestern Journal of Technology and Intellectual Property, Vol. 11, Issue 5, Article 1, 2013.

[12] “Big Data and Privacy: Making Ends Meet” workshop http://www.futureofprivacy.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf

[13] Big Data Privacy Working Group. Big Data Privacy Scenarios. September 2015.

[14] Reform of the data protection legal framework in the EU. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[15] E. J. Kennedy, C. Millard, “Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU member states,” Queen Mary School of Law Legal Studies Research Paper No. 194/2015.

[16] President’s Council of Advisors on Science and Technology (PCAST): Big Data and Privacy: A Technological Perspective. 2014.

[17] M. Hacırəhimova, “Big Data texnologiyalarının təhlükələri,” Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş “İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı” nın əsərləri, səh. 248-251, 2015.

[18] F. F. Zhao, L. F. Dong, K. Wang, Y. Li, “Study on Privacy Protection Algorithm Based on K-Anonymity,” Physics Procedia, Vol.33, pp. 483-490, 2012.

[19] A. Sahai, and B. Waters, “Fuzzy identity-based encryption,” Eurocrypt, pp. 457–473, 2005.

[20] S. Goldwasser, Y. Kalai; R. A. Popa; V. Vaikuntanathan, N. Zeldovich, “Reusable Garbled Circuits and Succinct Functional Encryption,” Proc. of the 35th annual ACM Symposium on Theory of Computing (STOC’13), pp. 555-564. 2013.

[21] C. Gentry, “Fully homomorphic encryption using ideal lattices,” Proceedings of the 41st annual ACM Symposium on Theory of Computing (STOC’09), pp. 169-178, 2009.

[22] C.Dwork, “Differential Privacy: A Survey of Results,” TAMC 2008, LNCS 4978, pp. 1–19, 2008.

[23] N. Mohammed, R. Chen, B. C. M. Fung, and P. S. Yu, “Differentially private data release for data mining,” Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (SIGKDD), pp. 493-501, 2011.

[24] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, “CryptDB: Protecting Confidentiality with Encrypted Query Processing, Proc. of the 23rd ACM Symposium on Operating Systems Principles (SOSP’11), pp. 85-100, October 2011.