Big data mühitində fərdi məlumatların təhlükəsizliyi

Məkrufə Hacırəhimova[1], Aybəniz Əliyeva[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
makrufa@science.az, [2]aliyeva.a.s@mail.ru

***Xülasə*—Big data insanlara rahatlıqla bərabər müəyyən risklər də gətirir. Verilənlərin toplanması, saxlanması və istifadəsi prosesində fərdi məlumatların asanlıqla sızması və gizli verilənlərin aşkar edilməsi fərdi məlumatların məxfiliyinin qorunması üçün problemlər yaradır. İşdə fərdi məlumatların təhlükəsizlik problemləri və səbəbləri tədqiq olunur, fərdi verilənlərin məxfiliyinin qorunmasına dair bəzi prinsiplər nəzərdən keçirilir.**

Açar sözlər— big data; big data analitika; fərdi məlumatların qorunması; verilənlərin gizliliyi; informasiya təhlükəsizliyi

I. GİRİŞ

Rəqəmsal verilənlər dövrünün meydana gəlməsi Big data-nın insanların həyat tərzinə, iş və təhsil vərdişlərinə getdikcə daha çox təsir etməsi, eyni zamanda insanlara rahatlıq gətirməsi ilə yanaşı, insanların bir çox informasiya təhlükəsizliyi təhdidləri və problemləri ilə üz-üzə qalmasına səbəb olur. Fərdi məlumatların təhlükəsizliyi belə problemlərdən biridir. Big data dövründə, davamlı olaraq böyük həcmdə fərdi məlumatlar daxil edilir, eyni zamanda, fərdi məlumatların qanunsuz əldə edilməsi, yayılması və tətbiq vasitələri sürəkli olaraq ortaya çıxır. Bu məlumatların İnternet mühitində fırıldaqçılıq məqsədləri üçün istifadəsi insanların həyatı üçün böyük fəsadlar və hətta əhəmiyyətli iqtisadi zərərlər yarada bilər. Müasir dünyada çoxlu sayda şirkətlər hər gün milyardlarla fərdi məlumatı istifadə edərək böyük gəlir əldə edirlər. Bəzi qiymətləndirilmələrə görə təkcə Avropa İttifaqında məlumatların ticarəti üzrə ixtisaslaşdırılmış, "verilənlərin brokerləri" adlandırılan 50-yə yaxın böyük şirkət fəaliyyət göstərir [1]. Bir sıra ölkələr təşkilatlardan fərdi məlumatların qorunmasını tələb edən qanun və qaydalar qəbul etsələr də, fərdi məlumatların sızması hadisələri adi hal almışdır. Fərdi məlumatların oğurluğu üzrə Resurs Mərkəzi (Identity Theft Resource Center) [2] və Açıq Təhlükəsizlik Fondunun (Open Security Foundation) [3] statistikasına görə, fərdi məlumatlarla əlaqəli qayda pozuntuları getdikcə çoxalmış və son zamanlarda milyonlarla fərdi məlumat yazılarının itməsinə səbəb olmuşdur.

Bir sıra təşkilatlar fərdi məlumatların qorunması sistemlərini yaratmağa kömək etmək üçün tövsiyələr təklif edirlər. 1995-ci ildə Avropa Parlamenti Komissiyası, Avropa İttifaqına üzv olan ölkələrdən İqtisadi əməkdaşlıq və inkişaf təşkilatının (Organisation for Economic Co-operation and Development – OECD) qaydalarını təsdiq edən fərdi məlumatların qorunması qanunları (və ya qaydaları) olmayan ölkələrə fərdi məlumatların ötürülməsini qadağan edən direktiv (Directive 95/46/EC) qəbul etdi [4].

27 aprel 2016-cı il tarixdə Avropa Parlamentinin və Şurasının qərarı ilə fərdi məlumatların mühafizəsi ilə əlaqədar olaraq Məlumatların Qorunmasının Ümumi Qanunu (General Data Protection Regulation – GDPR) qəbul edilmişdir. Bu nizamnaməyə uyğun olaraq ad və soyad, şəxsiyyət vəsiqəsinin nömrəsi, doğum tarixi, yaşayış yeri, e-mail və telefon, IP-ünvanı kimi fərdi məlumatlar praktiki olaraq sərbəst girişə malikdirlər. Lakin xüsusi kateqoriyalara aid olan fərdi məlumatlar, xüsusi halda irq və milliyyət, siyasi baxışlar, dini, biometrik məlumatlar (barmaq izləri, gözün torlu qişası, səsin yazısı və s.), sağlamlıq haqqında məlumatlar və genetik məlumatların emalı GDPR-ın ümumi qaydalarına görə qadağan edilmişdir. Verilənlərin subyektləri nəzərdə tutulmuş məqsədlər üçün göstərilən fərdi məlumatların emalına öz razılığını verməlidir. Eyni zamanda fərdi məlumatların xüsusi kateqoriyalarının emalı mümkün olduqda belə onların məxfiliyinin qorunmasına riayət edilməlidir. Məxfiliyin meyarları Avropa Birliyinin və ya üzv dövlətin hüquqları və ya milli səlahiyyətli orqanlar tərəfindən nəzərdə tutulmuş normalarla təyin edilir [3].

Hazırda bir çox ölkələrdə, o cümlədən Azərbaycanda fərdi verilənlərin qorunması üzrə qanun [5] fəaliyyət göstərir. Verilənlərin qorunması qanunlarının əksəriyyəti OECD Təlimatlarının [6] rəhbər prinsiplərinə uyğun olaraq işlənib hazırlanmışdır. OECD Təlimatları müəyyən edilmiş prinsiplərlə verilənlərin toplanması, verilənlərin keyfiyyəti, məqsədin spesifikasiyası, istifadənin məhdudlaşdırılması, təhlükəsizliyə təminat, açıqlıq, fərdi iştirak və hesabatlılığı əhatə edir.

II. BIG DATA VƏ FƏRDİ MƏLUMATLAR

Fərdi məlumatlar, identifikasiya olunmuş şəxsə aid olan məlumatlardır. Big data dövründə fərdi məlumatlarla bağlı yaranan problemləri dərk etmək üçün ilk növdədə ondakı yeniliyin və fərqliliyin nə olduğunu anlamaq vacibdir. Big data konsepsiyası kifayət qədər tanınsa da, tam yaxşı başa düşülmür və "ümumiləşdirilmiş, dəqiq olmayan bir termin" kimi təsvir edilir [7, 8]. Big data adətən “həcm, sürət və müxtəliflik” kimi xüsusiyyətləri ilə müəyyən edilir. Big data böyük həcmdə verilənlər yığımı ilə bərabər verilənlərin analizi və istifadəsi üsullarındakı dəyişikliyi də özündə birləşdirir.

DOI: 10.25045/NCInfoSec.2019.34

Biğ data dövründə təşkilatlar üçün yüksək dəyər ifadə edən fərdi məlumatlar daha çox istifadə olunur. Big data-nın meydana gəlməsi müəssisə və təşkilatların qərarların qəbulu prosesini yaxşılaşdırmasına və verilənlərin analizinə yeni yanaşmanın tətbiqi hesabına yeni imkanlar əldə etməsinə şərait yaradır. Big data verilənlərin analizinin ənənəvi formalarını dəyişdirdi və böyük verilənlərin analitikası (Big data analytics, BDA) adlanan yeni bir proqnozlaşdırıcı yanaşma yaratdı [9]. Böyük verilənlərin analitikası verilənlərin ənənəvi analizindən fərqlənən üç əsas xüsusiyyətə – alqoritmlərdən istifadə, “bütün verilənlər”dən istifadə və verilənlərin təkrar istifadəsinə (repurposing data) malikdir [6, 8].

Fərdi məlumatların analitikasının aparılması üçün müxtəlif mənbələrdən istifadə olunur. "Əşyaların İnterneti"nin bir hissəsini təşkil edən obyektlərin istifadə dairəsi genişləndikcə yaranan fərdi məlumatların da həcmi artır. Bu fərdi məlumatlar həm dövlət, həm də özəl şirkətlər üçün olduqca dəyərlidir.

Digər bir zəngin mənbə, İnternet forumlarda, sosial şəbəkələrdə, icmal saytlarında, xəbər qruplarında və bloqlarda əlyetərli olan böyük həcmdə sosial məlumatlardır. İnternetin insanlara verdiyi imkanların hesabına fərdi məlumatların həcmi əhəmiyyətli dərəcədə artır.

Beləliklə, toplanmış verilənlər fərdlərin hobbiləri, bəyənmələr və bəyənməmələri, sağlamlıq vəziyyəti, sosial və ailə şəbəkələri, siyasi görüşləri, elektron cihazlardan və məişət texnikasından istifadə də daxil olmaqla, insanların həyatının əksər aspektlərinə aydınlıq gətirir. Yeni korrelyasiyaları axtarmaq üçün bu böyük həcmdə verilənlərin öyrənilməsi (mining) fərdi məlumatlar üçün bir çox potensial tətbiqlərə səbəb olur. Belə tətbiqlərdən biri problemlərin yeni həll yollarının axtarılmasıdır (korrelyasiyalar müəyyən bir konkret problemin mümkün həllini təklif edə bilər). Korrelyasiyalar insanların davranışına təsir etməklə, ayrı-ayrı şəxslərə aid qərarların qəbuluna, müəyyən risklər və ya təhdidlərin qabaqcadan aradan qaldırılmasına yönəldilmiş üsulları da təklif edə bilərlər.

III. FƏRDİ VERİLƏNLƏRİN POTENSİAL İMKANLARI VƏ ZƏRƏRLƏRİ

A. Fərdi verilənlərin Potensial Faydaları

Fərdi məlumatların potensial faydaları məntiqi olaraq onun potensial istifadəsi ilə bağlıdır. Kommersiya baxımından verilənlər olduqca qiymətli bir aktiv və "dəyər yaratmaq mənbəyidir" [8]. Xüsusilə, pərakəndə satış sektoru insanların nəyi və nə vaxt alacağı ilə bağlı proqnoz verməyi asanlaşdıran bir vasitə olaraq fərdi verilənlərin analizindən istifadə edir. Nümunə üçün, ABŞ-da Wal-Mart ticarət mərkəzi maliyyələşməni tənzimləmək və mağazada satışın uyğun vaxtını proqnozlaşdırmaq üçün demoqrafik və hava məlumatları ilə birlikdə satış, qiymət və iqtisadi göstəricilər haqqındakı verilənləri də istifadə edir. Pərakəndə satışda da malların qiymətlərini tələb və təklif əsasında tənzimləmək üçün fərdi məlumatlardan istifadə olunur. ABŞ-da “Stage Stores” pərakəndə satış şəbəkəsi hər hansı bir mağazada konkret bir malın qiymətini azaltmağın ən yaxşı vaxtını elan edən “endirim optimallaşdırması” üçün böyuk həcmdə fərdi məlumatlardan istifadə edir [8].

Böyük həcmli fərdi məlumatların daha bir istifadəsi pərakəndə satışda tələbə uyğun olaraq reklamın anında həyata keçirilməsinə kömək etməsidir. Başqa sözlə, fərdi məlumatlar kredit risklərinin qiymətləndirilməsində və sığorta nəticələrinin proqnozlaşdırılmasında istifadə olunur. “İnsanların analitikası” (“istedadların analizi”) sahələri hansı namizədlərin işə götürüləcəyi, işçilərin əmək məhsuldarlığının yaxşılaşdırılması, işçinin işdən çıxması və ya işdən çıxarılmasına dair proqnozlar verməyə imkan verir.

İnsanların sağlamlığı və təhlükəsizliyi baxımından Big data xəstəliyin yayılması və ya təbii fəlakətlərin baş verməsi kimi məsələlərdə proqnozların verilməsinə yardım edə bilər. Həmçinin xəstəliyin diaqnozunda və dərmanların mənfi təsirlərinin müəyyən edilməsində kömək edə bilər, yol qəzaları və tıxacların baş vermə ehtimalını təxmin etməyə kömək edə bilər. Böyük verilənlər təhlükəsizlik və hüquq mühafizə risklərini də müəyyənləşdirməyə kömək edə bilər.

Fərdi məlumatlar özəl istehlakçılar üçün xidmət və məhsulların təqdimini asanlaşdırır, aviaşirkət biletləri kimi mal və ya xidmətlərin alışı üçün ən uyğun vaxtı təyin etməklə istehlakçıların imkanlarını genişləndirə bilər [8].

B. Fərdi Verilənlərin Potensial Ziyanları

Fərdi məlumatların yayılması nəticəsində yaranan zərərlər iki qrupa ayrılır. Birincisi, bütün böyük verilənlər üçün ümumi xarakter daşıyır və verilənlərdəki çatışmazlıqlar, tətbiq olunan analitik alətlər və ya müəyyən edilmiş nümunələrin həqiqi korrelyasiyalara malik olmaması səbəbindən yanlışlığa gətirən potensial imkanları ilə bağlıdır. İkincisi, onun gizliliyi pozmaq imkanı ilə bağlıdır. Bu özlüyündə bir zərərdir, eyni zamanda əlavə təhdidlərə səbəb ola bilər [4,8].

İnsan hüquqlarının əsasını təşkil edən dəyərlərin qorunmasında məxfilik başlıca rol oynadığından fərdi məlumatların məxfiliyinin qorunması vacibdir. Böyük fərdi məlumatlar məxfiliyə zərər yetirir, çünki bu, ayrı-ayrı şəxslərin fərdi məlumatlarına nəzarəti həyata keçirmək qabiliyyətini aradan qaldırır və bununla da insanın öz seçiminə uyğun olaraq həyatını yaşamaq və nizamlamaq hüquqlarını pozur [7,8].

Boyd və Crawford tərəfindən qeyd edildiyi kimi [10] İnternet mənbələrindən əldə olunan verilənlər dəstləri çox vaxt etibarlı deyil, itkilərə meyllidir və çox sayda verilənlər dəsti birlikdə istifadə edildikdə bu xətalar və boşluqlar daha da artır. Belə məlumatlar ədalətsiz qərarların qəbuluna səbəb ola bilər və fərdi şəxslərin ləyaqətinə xələl gətirə bilər.

Digər bir məsələ, fərdi məlumatlar əsasında fərdin zəif cəhətlərinin aşkar edilməsi və müəyyən məqsədlər üçün istifadəsi ilə bağlıdır. Məsələn, 2016-cı ildə ABŞ-da prezident seçkilərinin nəticələrinə təsir etmək üçün namizədə qarşı siyasi kompaniyada onun istifadəsi buna bir nümunədir [8, 11] . Fərdi məlumatlar əsasında qərarların qəbulu ayrı-ayrı şəxslərə qarşı haqsızlığa və ayrı-seçkiliyə səbəb ola bilər. Bəzi sektorlarda bu

cür təcrübələr adi hal alsa da, fərdi məlumatların əlyetərliyi sığorta sektoru kimi sahələrdə də belə halların yaranmasına şərait yaradır.

Fərdi məlumatlarla bağlı fəaliyyəti asanlaşdırmaq üçün tələb olunan fərdi məlumatların geniş şəkildə toplanması da digər bir problem yarada bilər, insanların oğurluğa və saxtakarlığa məruz qalmasına səbəb ola bilər.

IV. FƏRDİ MƏLUMATLARIN GİZLİLİYİNİN QORUNMASI PROBLEMLƏRİ

Təhlükəsizlik nöqteyi-nəzərindən böyük verilənlər üçün ən böyük problem istifadəçinin məxfiliyinin qorunmasıdır. Böyük verilənlərin bir çox hallarda çoxlu sayda fərdi məlumatları özündə birləşdirməsi istifadəçilərin məxfiliyinə çox böyük təhlükə yaradır. İstifadəçilərin məxfiliyi aşağıdakı hallarda pozula bilər [6]:

a) *Kənar verilənlər yığımı ilə birləşdirildikdə fərdi məlumatlar istifadəçilər haqqında yeni faktların ortaya çıxmasına səbəb ola bilər.* Bu faktlar gizli ola bilərlər və başqalarına açıqlanmamalıdır.

b) *Fərdi məlumatlar bəzən biznesə dəyər əlavə etmək üçün toplanır və istifadə olunur.* Məsələn, fərdi alış-veriş vərdişləri bir çox şəxsi məlumatları üzə çıxara bilər.

c) *Həssas məlumatlar düzgün şəkildə qorunmayan bir yerdə saxlanılır və emal olunur.* Bu halda saxlama və emal mərhələlərində məlumatların sızması baş verə bilər.

Fərdi məlumatların qorunması üzrə mövcud qanun və qaydalar adətən fərdi məlumatların məxfiliyinin və transsərhəd axınlarının qorunması üzrə OECD Təlimatlarına əsaslanır. Bir təşkilat və ya məlumat toplayıcısı verilənlər subyektlərinin fərdi məlumatlarını toplamaq və ya istifadə etmək istəyirsə OECD-nin aşağıdakı qaydalarına əməl etməlidir [4] :

• Toplama və məhdudiyyət (Collection and limitation) – Şəxsi məlumatların toplanmasında məhdudiyyətlər olmalıdır. Bundan əlavə, məlumatlar verilənlərin subyektlərinin razılığı ilə qanuni və ədalətli üsullarla əldə edilməlidir.

• Məlumatların keyfiyyəti (Data quality) – Toplanan məlumatlar aktual, dəqiq və tam olmalıdır.

• Məqsədin spesifikasiyası (Purpose specification) – Məlumat toplanarkən məqsəd dəqiq müəyyən olunmalı və açıqlanmalıdır.

• İstifadə məhdudiyyəti (Use limitation) – Toplanmış məlumatların sonrakı istifadəsi məlumat toplanarkən açıqlanan məqsədlərə uyğun olmalıdır.

• Təhlükəsizlik tədbirləri (Security safeguards) – Fərdi məlumatlar səmərəli təhlükəsizlik tədbirləri ilə qorunmalıdır.

• Açıqlıq (Openness) – Fərdi məlumatlarla bağlı hadisələr (inkişaflar), təcrübələr və siyasət açıq olmalıdır.

• Fərdi iştirak (Individual participation) – Məlumat subyektləri özləri haqqında məlumat almaq hüququna və bu məlumatların düzgünlüyünə etiraz etmək hüququna malikdirlər.

• Hesabatlılıq (Accountability) – Təşkilat yuxarıda göstərilən prinsiplərə uyğun olaraq məlumatın subyekti qarşısında məsuliyyət daşıyır.

Verilənlərin qorunması üçün əsas tələblərdən biri fərdi məlumatların emalının qanuna uyğunluğunun təmin edilməsidir.

Big data və verilənlərin müasir analiz metodları ayrı-ayrı fərdlərin şəxsi həyatının məxfiliyinin qorunmasının ənənəvi yollarını təsirsiz hala gətirir [11]. Fərdi şəxslər Big data analitikada məlumatların istifadəsi və açıqlanmasına az nəzarət edirlər [4]. Big data analitika insanların sağlamlıq, siyasi görüşləri və s. ilə bağlı meyllərini qabaqcadan proqnozlaşdıran qanunauyğunluqları və tendensiyaları üzə çıxarmağa imkan verir. Qanunla və ya fərdin razılığı ilə icazə verilən fərdi verilənlər konkret bir məqsədə xidmət edərsə, qorunması şərti ilə emal oluna bilərlər. Lakin Big data-nın tətbiqləri üçün bunu yoxlamaq çətindir. Məqsədin məhdudlaşdırılması prinsipi Big data erası üçün artıq uyğun deyildir [13].

V. BIG DATA MÜHİTİNDƏ MƏQSƏDİN SPESİFİKASİYASI VƏ İSTİFADƏNİN MƏHDUDLAŞDIRILMASI PRİNSİPİ

Məqsədin spesifikasiyası və istifadənin məhdudlaşdırılması verilənlərin qorunmasının hər hansı bir aktında mövcud olan prinsiplərdən biridir. Bu prinsiplər verilənlərin qorunmasının ənənəvi sütunlarıdır. İstehlakçıların verilənlərinin qorunması sahəsində isə "bildiriş və razılıq" adlanan model verilənlərin qanuni emalı üçün ən çox istifadə olunan mexanizmlərdən biridir [6, 8].

Bu prinsip iki addımlı bir yanaşmanı özündə birləşdirir [6]: a) fərdi məlumatlar müəyyən olunmuş, açıq və qanuni məqsədlər (orijinal məqsədlər) üçün əldə edilməli; və sonra isə b) orijinal məqsədə uyğun olmayan başqa bir məqsəd (yeni məqsəd) üçün istifadə edilməməlidir. Beləliklə, toplanan hər hansı bir fərdi məlumat bu prinsipə uyğun olmalıdır.

Big data məqsədin məhdudlaşdırılması prinsipinə problem yaradir və bu prinsip Big data analitikanın inkişafı üçün bir maneədir [4]. Məqsədin spesifikasiyasının məhdudlaşdırılması ilə bağlı qeyd olunan bu vacib məqamlar [6] “bildiriş və razılıq” modelinin effektivliyinə mənfi təsir göstərir. Məsələn, Big data analitika yeni məqsədlər üçün istifadə edilə bilən gözlənilməyən korrelyasiyaları aşkar edən müxtəlif alqoritmlərdən istifadə edərək verilənlərin analizini həyata keçirməyə imkan verir. Buna görə məqsədin məhdudlaşdırma prinsipi təşkilatın imkanlarını və innovasiya fəaliyyətini məhdudlaşdırır.

Aşağıda məqsədin spesifikasiyası və məhdudlaşdırma prinsipi ilə əlaqəli iki əsas məsələ nəzərdən keçirilmişdir.

A. Verilənlərin təkrarlanması (Repurpose Data)

İlk popblem verilənləri yeni məqsədlər üçün istifadə edərkən yaranır. Big data verilənlərin təkrar istifadəsini özündə birləşdirir ki, bu da verilənlərin təkrarlanmasına səbəb olur. Big data analitika fərdi verilənlərin toplanması yolu ilə dəyərli bilikləri aşkarlamaq imkanına malikdir. Bu halda çox böyük verilənlər dəstləri məqsədin məhdudlaşması prinsipinə problem yaradır [6].

Bu prinsipə görə, toplanmış fərdi məlumatları prediktiv analiz üçün istifadə edən təşkilatlar verilənlərin toplanmasının orijinal məqsədi ilə bu analizin uyğunluğunu təmin etməlidirlər [6,12]. İnsanlar məlumatları başqaları ilə paylaşdıqda, onlar bu məlumatların hansı məqsədlərlə istifadə olunacağına dair təbii bir gözləntiyə sahibdirlər.

Bundan əlavə, Big data analitika müxtəlif məqsədlər üçün, bəzi hallarda isə başqa bir təşkilat tərəfindən əldə olunan verilənləri də təkrar istifadə edir. Bu, toplanmış verilənlərin orijinal məqsədə uyğun olmayan məqsədlər üçün istifadə edilməyəcəyinə dair məxfilik prinsipinə ziddir. Məqsədin məhdudlaşdırılması prinsipinə görə fərdi verilənlər müəyyən, açıq və qanuni məqsədlər üçün əldə edilməli və orijinal məqsədə uyğun olan digər məqsədlər üçün sonradan emal edilməməlidir.

B. Big data analitikanın yaratdığı yeni fərdi məlumatlar

İkinci problem, böyük verilənlərin analizi zamanı yaranan yeni fərdi məlumatların məqsədini müəyyənləşdirməyə ehtiyac olduqda ortaya çıxır. Təkrarlanma ilə yanaşı, big data analitika da yeni fərdi məlumatlar yaratmaq potensialına malikdir [6, 8].

Big data analitikanın yaratdığı yeni fərdi məlumatların emalı üçün verilənlərin subyektlərindən razılığın alınması vacibdir. Big data analitika vasitəsilə fərdi məlumatlarda istinad olunan yaş, seçim və həyat tərzi kimi xüsusiyyətlərinə görə fərdlər məhsul və ya xidmət təklifləri ala bilərlər. bilər. Sosial media verilənləri və fərdlər haqqında digər məlumatlar isə fərdi şəxsin kredit reytinqini təyin edərkən, onun həyat tərzini öyrənmək üçün analiz edilə bilər [6, 13].

NƏTİCƏ

Son texnoloji nailiyyətlər və biznes fəaliyyətinin inkişafı fərdi məlumatların toplanması, saxlanmasıı və istifadəsi imkanlarını artırır. Xüsusilə, Big data dövründə əvvəlkindən daha çox fərdi verilənlər toplanır, analiz olunur və istifadə edilir. Eyni zamanda Big data analitika verilənlərin analizinin ənənəvi formalarını dəyişdirdi və tədqiqatlara yeni prediktiv yanaşma gətirdi. Bundan sonra fərdi məlumatlarla bağlı məxfilik və məlumatların qorunması problemləri daha qabarıq şəkildəi ortaya çıxır. Aparılan tədqiqatlar göstərir ki, fərdi verilənlərin qorunması ilə bağlı irəli sürülmüş bəzi prinsiplər Big data erasında özünü doğrultmur. Belə ki, Big data verilənlərin qorunmasının əsasını təşkil edən məqsədin spesifikasiyası və istifadənin məhdudlaşdırılması prinsiplərinə problem yaradir, eyni zamanda bu prinsip Big data analitikanın inkişafı üçün bir maneədir. Big data analitika toplanmış verilənlərin orijinal məqsədə uyğun olmayan məqsədlər üçün istifadə edir ki, bu da fərdi verilənlərin məxfiliyinə xələl gətirir.

Beləliklə, fərdi məlumatların ənənəvi qorunması prinsiplərinin məhdudiyyətləri yeni metodologiyanın işlənilməsini tələb edir. Böyük verilənlər üçün profil qanunun hazırlanması bu halda daha məntiqli qərar hesab oluna bilər.

İSTİNADLAR

[1] Ch. Chi, T. Liu, X. u, Sh. Shi, “Research on the security of personal information in the era of Big Data,” The Inter. Conference on Artificial Intelligence for Communications and Networks, July 2019, pp 107-114 .

[2] Identity Theft Resource Center (ITRC). Data Breaches., https://www.idtheftcenter.org/data-breaches

[3] The risk based security (RBS) and the open security foundation (OSF). DatalossDB, https://blog.datalossdb.org

[4] S.C. Cha, K.H. Yeh, “Data-driven security risk assessment scheme for personal data protection,” IEEE Access, 2018, vol. 6, pp. 50510-50517.

[5] Fərdi məlumatlar haqqında Azərbaycan Respublikasinin Qanunu, http://www.e-qanun.az/framework/19675

[6] N. A. Ghani, S. Hamid, N.I. Udzir, “Big data and data protection: Issues with purpose limitation principle,” Int J. Advance Soft Computing Applications, 2016, vol. 8, no. 3, pp. 116-121.

[7] K. Crawford, J. Schultz, “Big data and due process: Toward a framework to redress predictive privacy harms”, Boston College Law Review, 2014, vol 55, pp. 93- 96.

[8] M. Paterson, M. Mcdonagh, “Data protection in an era of Big data: The challenges posed by big personal data,” Monash University Law Review, 2018, vol 44, no 1, pp. 1-31.

[9] M. S. Hajirahimova, “Big data technologies and information security challenges,“ Problems of of Information Technology, 2016, vol. 13, no. 1, pp. 49-56.

[10] D. Boyd, K. Crawford, “Critical questions for Big data: Provocations for a cultural, technological, and scholarly phenomenon,” Information, Communication & Society, 2012, vol. 15, pp.667–700.

[11] D. Zhang, “Big data security and privacy protection,” Advances in Computer Science Research, 2018, vol. 77, pp.275-278.

[12] L. Zhou, W. Gu, Ch. Huang, Y. Bai, “Research on information security in big data era,” The 6th International Conference on Computer-Aided Design, Manufacturing, Modeling and Simulation, 2018.

[13] Y. Sun, “Personal information security in the era of Big Data,” Proceedings of the 2nd International Conference on Artificial Intelligence and Engineering Applications, 2017, pp. 619-626.

PERSONAL INFORMATION SECURITY IN BIG DATA ENVIRONMENT

Makrufa Hajirahimova[1], Aybeniz Aliyeva[2]

[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]makrufa@science.az, [2]aliyeva.a.s@mail.ru

Abstract – Big data brings convenience to people and brings certain risks. In the process of data collection, storage, and use, it can easily lead to the leakage of personal information and discovery of confidential data which it create the problems for privacy protection of personal data. This paper have been investigated the challenges and causes of data security, some core principles of privacy protection of personal information are considered.

Keywords *– Big data; big data analytics; protection of personal information; data security; information security*