Fərdi məlumatların “qara bazar”ının xüsusiyyətləri və yaratdığı problemlər

Rasim Mahmudov
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
rasimmahmudov@gmail.com

***Xülasə*— Məqalədə fərdi məlumatların “qara bazar”ının mahiyyəti, xüsusiyyətləri araşdırılır. “Qara bazar”da alqı-satqı obyekti olan məlumat və xidmət növləri, texnologiyalar və onların qiymət siyasəti şərh olunur, həmçinin “qara bazar”da əldə edilən fərdi məlumatların hansı məqsədlər üçün istifadə edildiyi müəyyənləşdirilir. Eyni zamanda, bu cür məlumatların qeyri-qanuni əldə edilməsi və satılmasının şəxsi, korporativ və milli maraqlar baxımından yaratdığı problemlər göstərilir.**

Açar sözlər— fərdi məlumatlar; fərdi məlumatların “qara bazar”rı; fərdi məlumatların qiyməti; fərdi məlumatların oğurlanması.

I. GİRİŞ

Fərdi məlumatların dəyəri, əhəmiyyəti artdıqca, onlara olan tələbat da artır. Fərdi məlumatlardan istifadə ilə bağlı hüquqi məsuliyyət normaları, məhdudiyyətlər olduğu üçün onlardan qeyri-leqal biznes və kriminal məqsədlərlə istifadəyə olan tələbat bu sahənin “qara bazarı”nın formalaşmasına rəvac verir.

Müasir informasiya təhlükəsizliyi texnologiyaları və vasitələrinin tətbiqi standart kiberhücumlardan mühafizəni, əsasən, təmin edir. Ona görə də kibercinayətkarlar daim mövcud mühafizə sistemlərini aşıb keçmək üçün yeni-yeni imkanlar, üsullar axtarırlar. Belə üsullardan biri də “qara bazar” vasitəsi ilə müvafiq məlumatların ələ keçirilməsidir [1].

“Qara bazar”da insanların başqalarından gizli saxlamaq istədikləri istənilən fərdi məlumatları - şəxsiyyət vəsiqəsinin, sürücülük vəsiqəsinin, sığorta şəhadətnaməsinin, kredit kartın, sağlamlıq kartının, bank hesabının, VÖEN-in, mobil telefon məlumatları, e-poçt ünvanı, ev və ya iş ünvanı və s. satıla bilər Kibercinayətkarlar bu cür məlumatlardan sosial mühəndislik üsullarını tətbiq etməklə dələduzluq, şantaj, qəsbkarlıq üçün istifadə edirlər.

Tədqiqatçılar hələ 1990-cı illərdə fərdi məlumat bazarının formalaşmasını proqnozlaşdırsalar da, həmin vaxtlar elm və hüquq ictimaiyyətinin nümayəndələri bu ideyaya ehtiyatla yanaşırdılar. Onlar hesab edirdilər ki, şəxsi həyatın toxunulmazlığı hüququ və onun reallaşdırılmasının mövcud mexanizmləri fərdi məlumatların bir ticarət predmeti olmasına imkan verməyəcək [2].

Hazırda bir çoxları hələ də şəxsi həyatın toxunulmazlığını insanın ayrılmaz hüququ hesab edirlər. Konfidensiallığın qorunması texnologiyaları bu hüquqların təmin olunmasına yönəlsə də, fərdi məlumatların bazarı başqa istiqamətdə inkişaf edir.

Bir çox ekspertlər fərdi məlumatların “qara bazarı”nın getdikcə daha da inkişaf edəcəyini proqnozlaşdırırlar. Sürətlə inkişaf edən bu “qara” biznes qlobal hakerlər cəmiyyəti, zərərli proqram təminatı hazırlayanlar tərəfindən dəstəklənir. Deməli, fərdi məlumatların “qara bazar”ı həm də zərərli, yaxud kriminal proqram təminatı bazarının inkişafını stimullaşdırır [3].

ABŞ-da “qara bazar”ın məhsullarına daha çox maraq göstərirlər. 2019-cu ildə bu ölkədə fərdi məlumatların əldə edilməsi üçün 15,2 milyard dollar xərclənib. Dünyada fərdi məlumatların ən böyük “qara bazar”ı ABŞ-dadır. Belə ki, qlobal bazarın təxminən 60%-i Birləşmiş Ştatların payına düşür. Müvafiq Çin bazarı 2,4 milyard dollarla dünyada 2-ci yerdə qərarlaşır. Növbəti 3 yeri uyğun olaraq Böyük Britaniya, Kanada və Fransa tutur [4].

Məqalədə fərdi məlumatların “qara bazar”ının mahiyyəti, xüsusiyyətləri araşdırılır. “Qara bazar”da alqı-satqı obyekti olan məlumat və xidmət növləri, texnologiyalar və onların qiymət siyasəti şərh olunur. Həmçinin “qara bazar”da əldə edilən fərdi məlumatların hansı məqsədlər üçün istifadə edildiyi müəyyənləşdirilir. Eyni zamanda, bu cür məlumatların qeyri-qanuni əldə edilməsi və satılmasının şəxsi, korporativ və milli maraqlar baxımından yaratdığı problemlər göstərilir.

II. FƏRDİ MƏLUMATLARIN “QARA BAZAR”ININ ƏSAS XİDMƏTLƏRİ

“Qara bazar” dedikdə, ənənəvi olaraq əmtəə və xidmətlərin qanunsuz olaraq mübadilə edildiyi yer başa düşülür. Elə əmtəə və xidmət növləri var ki, əslində, qanun onların satışına icazə verir. Lakin bəzi hallarda bu proses rəsmiləşdirilmədən (lisenziya almadan, vergi uçotuna dayanmadan, yaxud digər zəruri tələbləri ödəmədən) həyata keçirilir. Bu halda, müvafiq əmtəə və xidmətlərin alqı-satqısı “qara bazar” kateqoriyası altına düşür.

Elə əmtəə və xidmətlər də mövcuddur ki, onların satışı, ümumiyyətlə, qanunla qadağandır (məsələn, narkotika, insan alveri və s.). Fərdi məlumat sahiblərinin icazəsi olmadan onların alqı-satqısına da qanunla icazə verilmir. Ona görə də bu cür məlumatların qanunsuz alqı-satqısı da “qara bazar” kateqoriyasına aid edilir.

DOI: 10.25045/NCInfoSec.2019.09

Fərdi məlumatların “qara bazar”ında konkret olaraq aşağıdakı xidmətlər təklif olunur [5]:

- real zaman rejimində mobil abonentin yerinin müəyyənləşdirilməsi;
- real zaman rejimində mobil abonenti əhatə edən şəxslərin müəyyən ediloməsi;
- abonentin mobil telefonla ünsiyyət qurduğu şəxslərin siyahısı və digər məlumatlar;
- şəxsin hərəkəti zamanı olduğu coğrafi məkanlar və zamanlar və trayektoriyalar haqqında məlumatlar;
- şəxsə aid mülklər, bank hesabları və s. haqqında məlumatlar;
- İnternet xidmətlərindən istifadə zamanı provayderlərin serverlərində toplanan fərdi məlumatlar və s.

III. “QARA BAZAR”DA QİYMƏT SİYASƏTİ

“Qara bazar”da fərdi məlumatların qiymətləri insanların sosial statusundan və maliyyə imkanlarından asılı olaraq dəyişir. Bu “qara” əmək bazarının insan resurslarını formalaşdırmaq üçün xüsusi hakerlik kursları təşkil olunur. Əksər hallarda ödənişlər kriptovalyuta ilə aparıldığından bu cür kibercinayətkarlıqla mübarizə aparmaq çox çətin olur [1].

“Qara bazar”da fərdi məlumatların qiymətlərinin formalaşmasına təsir edən 4 əsas faktoru fərqləndirmək olar:

Birincisi, normal iqtisadiyyatda olduğu kimi, “qara bazar”da da tələb və təklif qanunları işləyir.

İkinci faktor hesab balansıdır - əgər kredit kartı kifayət qədər əlyetərli kreditə malikdirsə, onun qiyməti baha olacaq.

Üçüncü faktor sədaqət kartlarının (ing. *cards loyalty*) yüksək bal stabilliyinə malik olmasıdır ki, bu da onların qiymətini qaldırır.

CƏDVƏL I. FƏRDİ MƏLUMATLARIN “QARA BAZAR”INDA TƏKLİF OLUNAN BƏZİ PROQRAM VƏ XİDMƏTLƏRİN QİYMƏTLƏRİ [5]

Proqram və ya xidmətin adı	**Qiyməti**
Akkauntların “sındırılması” proqramları	10-15$
Parolun oğurlanması	50$
Bank botnetləri	aylıq icarə - 750- 1200$ aylıq dəstək – 150$
Chrome , FireFox, Internet Explorer, Opera, Edge brauzerlərinin trafikləri	gündəlik – 2000$ aylıq – 15000$
Zərərli Android proqramının yüklənməsi	1500$
DDoS-hücumlar	həftəlik 500-1200$
Bankomat skimmerləri	700-1500$
Dərsliklərin əldə edilməsi	5-50$

Nəhayət, fərdi məlumatların dəyəri məlumatların təkrar istifadə edilməsindən asılı ola bilər. Yəni təkrar istifadə edə bilmək imkanı həmin məlumatların dəyərini artırır. Məsələn, “qara bazar”ın müştərilər bir dəfə istifadə edilə bilən hədiyyə kartı ilə müqayisədə dəfələrlə istifadə edilə bilən kredit kartı üçün daha çox pul ödəyirlər.

Fərdi məlumatların qeyri-qanuni satışı bir çox hallarda onlayn qaydada həyata keçirilir. Bu cür qeyri-leqal xidməti həyata keçirmək üçün *DarkNet* gizli şəbəkəsindən geniş istifadə edilir. Bu şəbəkəyə xüsusi proqram təminatı vasitələrinin köməyi ilə giriş əldə etmək mümkündür. Həmin şəbəkəyə daxil olanların anonimliyi qorunur və onlardan tələb edilir ki, alq;-satqı bitkoin və digər kriptovalyutalar vasitəsi ilə həyata keçirilsin [5].

“Qara bazar”da, adətən, korporativ məlumatlar fərdi məlumatlardan daha qiymətli olur. Ona görə də hazırda müəssisə və təşkilatlarda toplanan və saxlanılan fərdi məlumatlar bədniyyətlilərin hədəfinə daha çox tuş gəlir.

Kibercinayətkarlar hər hansı oğurlanmış məlumatları bazara çıxarmazdan əvvəl onları çeşidləyirlər və inventarlaşdırırlar. Bahalı hesab etdikləri məlumatlara daha yüksək qiymət qoyurlar. Az dəyərli hesab etdiklərini isə bir yerə yığaraq toplu şəkildə kiçik ödənişlər müqabilində satışa çıxarırlar.

Hakerlər və “qara bazar” vasitəçiləri oğurlanmış fərdi məlumatların alqı-satqı proseslərini mümkün qədər sürətlə həyata keçirməyə çalışırlar. Çünki məlumat sahibləri oğurluqdan xəbər tutan kimi əks tədbirlər görməyə çalışırlar.

İstənilən fərdi məlumatlar aktual, mötəbər və dolğundursa, biznes üçün qiymətli resurs sayılır. Bütün bu xüsusiyyətlərə malik olan fərdi məlumatlar “qara bazar”da yüksək tələbata malikdir. Lakin bu cür məlumatlar qanuni yollarla əldə edilmədiyinə görə onları dəqiqləşdirmək qeyri-mümkündür.

IV. “QARA BAZAR”DA FƏRDİ MƏLUMATLARI NƏ ÜÇÜN ALIRLAR?

“Qara bazar”da fərdi məlumatları müxtəlif fəaliyyət istiqamətləri üçün alırlar. Amma əksər hallarda son məqsəd eynidir – gəlir əldə etmək. Sadəcə olaraq, fərdi məlumatlar vasitəsi ilə qeyri-qanuni gəlir əldə etməyin yolları müxtəlifdir.

Big data analitiksına əhəmiyyət verən şirktlərin artması, marketinq proseslərinin avtomatlaşdırılması üçün proqram təminatlarının hazırlanması “qara bazar”da fərdi məlumatlara olan tələbatı sürətlə artırmaqdadır. Rəqəmsal marketinqdə aşağıdakı məqsədlərin reallaşdırılmasına xidmət edən məlumatlara daha çox tələbat hiss olunur [6]:

- onlayn şirkətlərin effektivliyinin artırılması;
- reklam şirkətlərinin dəqiq hədəflənməsi;
- istifadəçilərin profillərinin və maraqlarının analizi;
- ən yaxşı məhsulların və xidmətlərin işlənib hazırlanması.

Əldə edilən fərdi məlumatların analizi əsasında kommersiya şirkətləri hədəf auditoriyasını müəyyənləşdirir, fərdiləşdirilmiş, ünvanlı reklam texnologiyalarını tətbiq edirlər.

Belə ki, insanlar İnternetdə müxtəlif axtarış sistemlərindən, sosial şəbəkələrdən, onlayn servislərdən istifadə edərkən onların arzu və istəkləri, ehtiyacları, həyat tərzi, hobbiləri haqqında məlumatlar toplanır və onlar reklam-marketinq fəaliyyəti üçün çox faydalı məlumatlara çevrilir.

Daha çox rast gəlinən hallardan biri də başqalarının kredit kartlarını, bank hesablarını və s. maliyyə məlumatlarını oğurlayaraq onların pullarının mənimsənilməsidir. Bu cür məlumatların əldə edilməsi üçün fiziki və virtual mühitə xas olan müxtəlif texnologiyalardan istifadə edilir.

Bəzi hallarda fərdi məlumatlar saxta sənədlər düzəldib satmaq üçün lazım olur. Digər hallarda müəyyən insanların fərdi məlumatlarını ələ keçirdikdən sonra onları şantaj edərək pul tələb edirlər. Həmçinin kriminal qruplar kiminsə hansısa bahalı mülkü barədə məlumat əldə edərək onu ələ keçirmək üçün fəaliyyətə keçirlər.

Fərdi məlumatlar siyasi mübarizə predmeti də ola bilər. Belə ki, siyasi rəqiblər əks tərəfin fərdi məlumatlarını qeyri-leqal yolla əldə edərək onların siyasi nüfuzunu aşağı salmaq üçün istifadə edə bilərlər.

Fərdi məlumatlar xarici kəşfiyyat orqanları üçün siyasi-ideoloji məqsədlər üçün də istifadə edilə bilər. Bu halda fərdi məlumatlar milli təhlükəsizliyin obyektinə çevrilir.

V. “QARA BAZAR”IN YARATDIĞI PROBLEMLƏR

Fərdi məlumatların “qara bazar”ının formalaşması və inkişafı dövlət, müəssisə və təşkilatlar, vətəndaşlar üçün bir sıra problemlərə yol açır. Əvvəla, “qara bazar”a daxil olan fərdi məlumatlar qeyri-qanuni yollarla, kriminal üsullarla, hüquqi və fiziki şəxslərə ziyan vurmaqla əldə edilir. İkincisi, həmin fərdi məlumatlardan bir çox hallarda sağlam məqsədlər üçün deyil, zərərli məqsədlər üçün istifadə edilir.

Fərdi məlumatların oğurlanması onların sahibləri üçün bir sıra neqativ nəticələrə səbəb ola bilər. Aparılan bir sorğunun nəticələrinə görə, fərdi məlumatları oğurlanan şəxslərin 40%-i gecələr normal yata bilmədiklərini, 65%-i əsəb hissləri keçirdiklərini, 69%-i təhlükə və qorxu hissləri yaşadıqlarını bildiriblər. Rəyi soruşulanların 7%-i isə intihar etmək həddinə çatdıqlarını söyləyiblər. Oğurluq qurbanlarının 15%-i zərərlərini ödəmək üçün şəxsi əşyalarını satıblar, 7%-i isə bunun üçün kredit götürüblər [7].

Fərdi məlumatların oğurlanması biznes qurumlarına daha çox ziyan vurur. Faktlar göstərir ki, bu, şirkətlər üçün daimi bir riskdir və həmişə bu cür neqativ hallara qarşı hazır olmaq lazımdır.

Məlumat sızıntısı ilə qarşılaşan şirkətlər üçün bunun ən böyük maliyyə itkisi reputasiyanın itirilməsidir. Bu cür hallardan sonra şirkətlər gərək müştəri etimadını qaytarmaq, uzunmüddətli maliyyə təsirlərini azaltmaq üçün zəruri tədbirlər görsün. Məlumat sızıntılarının əksəriyyəti kiberhücumlar nəticəsində baş verir. Bu cür insidentləri araşdırmaq və aşkara çıxarmaq böyük vaxt aparır.

Şirkətlər etiraf edirlər ki, məlumat sızmalarının müəyyənləşdirilməsi və qarşısının alınmasına nə qədər çox vaxt sərf edilirsə, bir o qədər xərc tələb edilir. Bu cür xərclərin həcmi ilbəil artır. Bu cür təhlükələrin aşkarlanması və qarşısının alınması üçün şəxsi təcrübədən istifadə etmək və texnoloji vasitələrə investisiya qoyuluşlarını artırmaq lazımdır [3].

Səhiyyə və maliyyə xidmətləri kimi güclü tənzimlənən sahələrdə məlumat sızmaları daha baha başa gəlir. Çünki bu sahələrdə müvafiq insidentlər nəticəsində reputasiyanın və müştərinin itirilməsi səviyyəsi və ehtimalı daha yüksək olur.

Fərdi məlumatlar “qara bazar” vasitəsi ilə xarici kəşfiyyat orqanlarının əlinə düşərsə, bu halda milli təhlükəsizlik üçün ciddi problemlər yarana bilər.

NƏTİCƏ

Fərdi məlumatların “qara bazarı” ilə effektli mübarizə aparmaq üçün müvafiq qanunvericiliyin təkmilləşdirilməsi, kibercinayətkarlıqla mübarizə tədbirlərinin gücləndirilməsi vacibdir.

Texnoloji səviyyədə fərdi məlumatların mühafizəsinin gücləndirilməsi ilə bağlı müvafiq dövlət siyasətini həyata keçirən qurumların, eləcə də, vətəndaşlara müxtəlif xidmətlər göstərən müəssisə və təşkilatların üzərinə mühüm vəzifə düşür.

Vətəndaşların özləri fərdi məlumatlarının qayğısına qalmalı, onlarla düzgün davranmalı, virtual mühitin xüsusiyyətlərini nəzərə almalıdır. Onların informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələsinə xüsusi diqqət yetirmək lazımdır.

Bunlarla yanaşı, fərdi məlumatların Big data ehtiyacları üçün səmərəli istifadəsi üçün onların şəxssizləşdirilməsi (adsızlaşdırılması) mexanizmlərinin işlənilib həyata keçirilməsi də zəruridir.

Hazırda müvafiq beynəlxalq hüquqi instansiyalarda insanların öz fərdi məlumatlarından gəlir əldə edə bilmələri üçün müvafiq hüquqi mexanizmlərin yaradılması məsələsi müzakirə olunur. Bunun üçün, ilk növbədə, hər kəsin öz fərdi məlumatlarına dair mülkiyyət hüququ əldə etməsi vacibdir.

Nəzərə almaq lazımdır ki, fərdi məlumatların xüsusi çəkiyə malik olduğu böyük verilənlər öz strateji əhəmiyyətinə, faydalarına görə neft ehtiyatları ilə müqayisə edilir. Deməli, elə etmək lazımdır ki, həm insanların şəxsi toxunulmazlıq hüququ yüksək səviyyədə qorunsun, həm də onların fərdi məlumatlarından faydalı məqsədlər üçün istifadə etmək mümkün olsun.

İSTİNADLAR

[1] R.Əliquliyev, R.Mahmudov, “Milli mentalitet kontekstində fərdi məlumatların həssaslığı və onların təhlükəsizliyinin təmin edilməsi məsələləri”, İnformasiya cəmiyyəti problemləri, 2019, №2, s. 117-128.

[2] P. Samuelson, Privacy as intellectual property?. Stanford Law Review, 2000, pp. 1125–1173.

[3] M.Nuncic, “The Black Market for Data”, https://www.ontrack.com

[4] A.Fontinelle, “How Black Markets Work”, 2019, https://www.investopedia.com

[5] Armor, “The Black Market Report”, 2018, 16 p.

[6] S.Spiekermann, R.Böhme, “The challenges of personal data markets and privacy”, Electronic Markets, June 2015, https://www.eprofing.springer.com/journals/printpage

[7] G.Cook, “How Much Is My Identity Worth on the Black Market?” https://www.findreviews.com

CHARACTERISTICS AND CHALLENGES OF PERSONAL DATA “BLACK MARKET”

Rasim Mahmudov

Institute of Information Technology of ANAS, Baku, Azerbaijan

rasimmahmudov@gmail.com

Abstract— The essence and characteristics of personal data “Black market” are explored in this article. The article interprets the types of information and services, technologies and pricing policies that are the subjects of the sale on the “Black market”. It also defines the purpose of the use of the personal data obtained in the “Black market”. Moreover, the problems caused by the illegal acquisition and sale of such information, in terms of personal, corporate and national interests, are highlighted.

Keywords— *personal data; personal data “Black market”; price of personal data; personal data theft*