Fərdi məlumatların qorunması sahəsində beynəlxalq təcrübənin analizi

Fərhad Yusifov[1], Aysən Fərəcova[2]
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1] *farhadyusifov@gmail.com*, [2]*aysanpharajova@gmail.com*

Xülasə – **Məqalədə fərdi məlumatlar sahəsində beynəlxalq təcrübə araşdırılmışdır. Fərdi məlumatlar həssas informasiya kateqoriyasına aid edilir. Şəxsə məxsus olan məlumatların əldə edilməsi, emalı və istifadəsi onun icazəsi ilə olmalı və digər hallarda istifadəsi məhdudlaşdırılmalıdır. Beynəlxalq təcrübədə fərdi məlumatların qorunmasında istifadə olunan təhlükəsiz liman mexanizmi fərdə və ya qohumlarına, ailə üzvlərinə və s. aid olan həssas məlumatların silinməsini tələb edir. Fərdi məlumatların təhlükəsizliyinin təmin olunması sahəsində innovativ mexanizmlər kimi Estoniyada tətbiq olunan Data səfirlik və Rusiyada fərdi məlumatların ölkə hüdudlarından kənara çıxarılmaması istiqamətində görülən işlər və qəbul edilmiş qanunlar araşdırılmışdır.**

Açar sözlər— fərdi məlumatlar, məlumatların təhlükəsizlyi, fərdi məlumatların qorunması, data səfirlik

I. GİRİŞ

Texnologiyanın sürətlə inkişaf etdiyi, vətəndaşların, cəmiyyətin və ölkələrin iqtisadi, sosial, mədəni olaraq bir-birinə yaxınlaşdığı dünyada, fərd öz şəxsi məlumatlarını və hüquqlarını qorumaqda daha da çətinlik çəkir.

Əvvəllər informasiya sistemlərində və arxivlərdə saxlanılan və az sayda insanın əldə edə biləcəyi bəzi fərdi məlumatlar günümüzdə texnologiyaların inkişaf etməsi vasitəsi ilə sadəcə bir kliklə əldə edilə biləcək qədər asan olmuşdur. Başqa şəxslərin əlinə keçə biləcək məlumatların təhlükəsizliyi kimlərin hansı şərtlərdə bu məlumatları əldə edə biləcəyi və bir başqa şəxsə ya da quruma ötürə biləcəyi vacib bir mövzu halına gəlmişdir.

İnformasiya Kommunikasiya Texnologiyalarının (İKT) inkişafının vətəndaşların və ya şirkətlərin işində müsbət inkişafa səbəb olacağına əmin olunsa da, fərdi məlumatların nəzarətsiz dövriyyəsi şəxsi həyatın gizliliyinə müxtəlif təhlükələr yarada bilər. Fərdi məlumatların qorunması milli siyasət məsələsi kimi qəbul edilməli və lazım olan hüquqi və texnoloji infrastruktur sürətlə hazırlanmalıdır. Bundan əlavə, rəqəmsal texnologiyalar insan həyatının bütün sahələrində tətbiqi ola biləcək qanunsuzluqların qarşısını almaq üçün hüquqi tənzimləmələrə ehtiyac yaradır. Fərdlərin özlərinə aid olan verilənlər "fərdi məlumatlar" adlanır. Bu məlumatlar təşkilatlar tərəfindən saxlanılır, işlənilir və tələb olduqda isə üçüncü tərəflərə ötürülür.

Dövlət təşkilatları fərdi məlumat toplayıcılarıdır. Dövlət təşkilatlarına müxtəlif ictimai qurumlar, xüsusən də dövlət və özəl hüquq sektorundakı gəlir gətirən təşkilatlar və qeyri-hökumət təşkilatları daxil edilir. Peşə sahəsində isə fərdi məlumat toplayıcılarına həkim, vəkil, notarius və bankçılıq kimi peşələri aid etmək olar. Bir sözlə, cəmiyyətdə demək olar ki, hər kəs məlumat toplayır, onları qiymətləndirir və dəyişdirir.

Tədqiqat işində fərdi məlumatlar sahəsində beynəlxalq təcrübə analiz olunmuşdur. Ölkələrin təcrübəsində fərdi məlumatların saxlanılmasına, xaricə ötürülməsinə və bu proseslərin yerinə yetirilməsinə dair yanaşmalara baxılır, qəbul edilmiş qanunlar araşdırılır.

II. FƏRDİ MƏLUMATLARIN SAXLANILMASI

Fərdi məlumatlar konfidensial informasiya kateqoriyasına aid edilir. Fərdə məxsus olan məlumatların əldə edilməsi, emalı və istifadəsi onun icazəsi ilə olmalı və toplandığı məqsədlərə uyğun olaraq istifadə edilməlidir. Fərdi məlumatların saxlanmasını, onlara girişi və istifadəsini təmin etmək üçün hüquqi səviyyədə tənzimlənmiş qanunlar, müqavilələr və təhlükəsizlik infrastrukturlarından faydalanmaqla həyata keçirmək olar [1].

Nümunə kimi tibbi məlumatların de-identifikasiyası üçün ABŞ federal qanunu HIPAA-nın (Health Insurance Portability and Accountability Act – tibbi sığortanın portativliyi və hesabatlılığı) tərtib etdiyi təhlükəsiz liman mexanizmini göstərə bilərik. Təhlükəsiz liman mexanizmi fərdin və ya qohumlarının, ailə üzvlərinin və ya işə götürənlərin 18 spesifik identifikatorunun silinməsini tələb edir. Bunlara adlar, ünvanlar, tarixlər, telefon nömrələri, faks nömrələri, tibbi sığorta nömrələri, elektron poçt ünvanları, sosial sığorta nömrələri, tibbi sənədləşmə nömrələri, hesab nömrələri, lisenziya və ya 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 aiddir [2].

Bütün bu məlumatlar kompüter vasitəsi ilə ötürüldükdə həmişə çox zərərli bir yanaşma və təhlükə üçün asan bir mühit yarada bilər. Bu məlumatların köməyi ilə bəzi insanlar seçkilərdə verilən səsləri saxtalaşdıra, vergi borcunu silə, ölən bir adamın yerinə keçə, məlumatları dəyişə və s. bu kimi bir çox saxtakarlıqları yerinə yetirə bilər, ya da başqasına zərər vermək üçün məlumatlar dəyişdirilə bilər və ən vacibi ümumdünya və konstitusiya hüquqları olan şəxslərin məlumatlarının gizliliyi pozula bilər.

DOI: 10.25045/NCInfoSec.2019.06

Şəxs haqqında bədniyyətlinin əlində olan fərdi məlumatlar cinayət silahına, işdən çıxarılan işçinin əlində qisas vasitəsinə və ya rəqib şirkətə satılan mallara çevrilir. Buna görə fərdi məlumatların qorunması sahəsinə ciddi mexanizmlər işlənilməlidir. Hazırda informasiya texnologiyaları və informasiya cəmiyyəti sürətlə inkişaf edir. İnsan şəxsi ehtiyaclarından və ya zəruriyyətdən müxtəlif formalarda fərdi məlumatların təqdim edilməsini tələb edən xidmətlərdən istifadə edir. Bu baxımdan e-xidmətlərdən istifadə zaman hər bir şəxsi düşündürən əsas məsələ fərdi məlumatların təhlükəsizliyinin nə dərəcədə təmin olunmasıdır. Əgər effektiv e-dövlət həllərindən söhbət gedirsə dövlət səviyyəsində qanunvericilik bazasınan təkmilləşdirilməsi, fərdi məlumatların qorunması sisteminin işləniləməsi informsiya sizması ilə bağlı mövcud problemlərin aradan qaldırılmasına və fərdi məlumatların icazəsi ələ keçirilməsi, emalına qarşı güclü immunitetə malik vasitələr yaradılmasına imkan verər. Beynəlxalq təcrübədə fərdi məlumatların təhlükəsizliyinin təmin olunmasına dair müxtəlif yanaşmalar vardır.

III. FƏRDİ MƏLUMATLARIN QORUNMASI İLƏ BAĞLI BEYNƏLXALQ TƏCRÜBƏ

Avropa Birliyi – Avropa Birliyi dörd əsas ideyaya əsaslanır: əşyaların, şəxslərin, xidmətlərin və kapitalın sərbəst hərəkəti.

Fərdi məlumatların toplanması və işlənməsi bu dörd əsas məqsədin yerinə yetirilməsi üçün vacib olduğundan, Avropa Birliyində (AB) fərdi məlumatların qorunmasına yönəlmiş qaydalar, informasiya texnologiyalarının inkişafı ilə birlikdə AB daxilindəki ümumi bazarın tələblərini nəzərə alır və təməl hüquqlara uyğun olaraq pulsuz məlumat trafikini idarə edir. Burada məqsəd hücumun ortaya çıxması halında təşkil ediləcək qorumadan əlavə baş verə biləcək hücumlara qarşı profilaktik tədbirlərin görülməsidir. Buna görə, fərdi məlumatların qorunması və potensial hücumların minimuma endirilməsi üçün hücumdan əvvəl sistematik qorunma təmin edilməlidir [5].

Məsələn Almaniya qanunlarında, vətəndaşlara fərdi məlumatlarının hansı hallar olduqda açıqlanacağına və bu məlumatdan necə istifadə olunacağına qərar vermək səlahiyyəti verilir və bu da ona fərdi məlumatlarının kimə ötürüldüyünü idarə etməyə imkan verir. Bu vəziyyət şəxsin razılığını ön plana çıxarır, çünki bu vasitə ilə onların məlumatlarına çıxışlarını müəyyənləşdirmək hüququ verilir.

Avropa Birliyinin təşkil etdiyi təlimatın 6-cı maddəsində “Məlumatların keyfiyyəti prinsipləri” ilə bağlı xüsusi qaydalar qeyd edilmişdir. Bu prinsiplər şəxsi məlumatların qanuna və dürüstlüyə uyğun işlənməsi üçün nəzərdə tutulmuşdur:

Məqsədə sadiqlik: Məlumatların yalnızca qanuna uyğun açıq və sərhədləri bilinən məqsəd istiqamətində toplanması və işlənməsi prinsipidir. Bu prinsipə əsaslanaraq məlumatların emalından əvvəl fərd şəxsi məlumatlarının hansı məqsədlə toplandığını öyrənir.

Xüsusi Məqsədlərin mövcudluğunda məqsədin təqdim edilməsi: Məlumatın tarixi, statistik və ya elmi məqsədlər üçün işlənməsində məqsədəuyğunluq qəbul edilir. Bununla birlikdə üzv ölkələr tərəfindən kifayət qədər zəmanət tələb olunur.

Lazımlılıq prinsipi və saxlanmanın qadağan edilməsi: Emal edilən fərdi məlumatların əldə oluna biləcəyi məqsəd üçün səbəb bağlantısı olmalıdır. Toplanmış məlumatlar yalnız məqsəd üçün lazım olduqda istifadə edilə bilər. Digər tərəfdən, gələcəkdə nəzərdə tutulan məqsədə xidmət edə biləcək məlumatların saxlanması qadağandır.

Maddi gerçəklik, məlumatların yenilənməsi, silinməsi və düzəldilməsi: Məlumatların düzgünlüyünü və aktuallığını təmin etmək üçün hər hansı bir ziddiyyət olduqda məlumat silinməli və ya yenidən düzəldilməlidir.

Saxlama müddəti: Məlumatların nəzərdə tutulmuş məqsədə çatmasına qədər saxlanması qanunidir, bu müddət keçdikdən sonra, məlumatların saxlanmasını davam etdirmək üçün məlumatları anonimləşdirmək lazımdır.

Amerika Birləşmiş Ştatları – ABŞ-da fərdi məlumatların qorunması üçün qüvvəyə minmiş ən vacib hüquqi tənzimləmələrdən biri olan 1974-cü il tarixli “gizlilik aktı” adlı qanun, fərdlərin tanınmasını yerinə yetirəcək fərdi məlumatların dövlət tərəfindən qorunması, əldə edilməsi, istifadə edilməsi və paylaşılması qanunlarını özündə birləşdirir.

Fərdi məlumatların gizliliyinin qorunması ilə bağlı qeyd edilən Gizlilik Aktının əsas prinsiplərini aşağıdakı kimi ümumiləşdirmək olar:

- Fərdi məlumatlar və həssas məlumatlar xüsusi qorunmalıdır.
- Dövlət vətəndaşların fərdi məlumatlarının qorunmasına cavabdehdir
- Fərdi məlumatlar şəffaf şəkildə emal edilməli və məlumat sahibinə özünə aid olan fərdi məlumatların hansı şəkildə emal edildiyi ilə əlaqəli məlumat verilməlidir.
- Şəxsi məlumatların gizliliyini təmin etmək üçün qanunun müddəalarının effektiv şəkildə yerinə yetirilməsi və lazımi nəzarətin təmin edilməsi vacibdir.

1974-cü il tarixli Gizlilik Aktı, federal qurumlara, yuxarıda göstərilən prinsiplərə uyğunluğu təmin etmək üçün vətəndaşların fərdi məlumatlarının qorunması üçün zəruri təhlükəsizlik mexanizmini yaratmağı tövsiyyə edir. Fərdi məlumatların gizliliyinə dair müddəalar pozulduğu təqdirdə, qanun cəza müddəalarının tətbiq edilməsini tələb edir və bununla əlaqadar şəxs tərəfindən kompensasiya tələbi ilə iddia qaldırmaq da mümkündür [6].

Rusiya – Rusiya Federasiyasında fərdi məlumatların istifadəsini tənzimləyən federal qanun 2006-cı ildə qəbul edilmişdir. Qanuna müxtəlif illərdə dəyişikliklər olunsa da 2015-ci ildə qanunda fərdi məlumatların tənzimlənməsinə dair ciddi tələblər qoyulmuşdur. Belə ki, müxtəlif operatorlar tərəfindən fərdi məlumatlar ayrı-ayrı məqsədlər üçün istifadəsinin qarışısını almaq üçün qanun ölkə vətəndaşlarının fərdi məlumatlarının emalının və saxlanmasının yanlız ölkə hüdudlarında yerləşən verilənlər bazasında istifadəsinə dair operatorlar qarşısında ciddi öhdəlik qoymuşdur.

Rusiyanın təhlükəsizlik qanunu mürəkkəbdir. Bir sıra Rusiya qanunlarının birləşməsi bütün sektorlar üzrə hərtərəfli gizliliyin qorunmasını təmin edir. Rusiya qanununun AB

təlimatı ilə bir çox oxşarlığı var. Ancaq qanunun icrası məhdud görünür. Rusiya APEC (Asia-Pacific Economic Cooperation) üzvüdür, lakin APEC Sərhədsiz Gizlilik Qaydaları sistemində CBPR (Community-based participatory research) iştirak etmir.

İnformasiya texnologiyaları və İnformasiyanın qorunması vətəndaşlara ‘unudulmaq hüququ’ verir və bəzi URL-ləri axtarış nəticələrindən çıxarmaq üçün istifadə edilə bilər. Əsas tənzimləyici Telekommunikasiya, İnformasiya Texnologiyaları və Kütləvi Rabitə Sahəsində Federal Nəzarət Xidmətidir (Roskomnadzor) [7].

Rusiyada məlumatların toplanması və işlənməsi üçün Roskomnadzor-da məlumat operatorları tərəfindən rəsmi qeydiyyat tələb olunur. Sadə, birdəfəlik məlumat toplama və insan resursları məlumatları üçün istisnalar var.

Bununla birlikdə, 2015-ci ilin sentyabrından etibarən məlumat operatorları Rusiya vətəndaşlarının fərdi məlumatlarının Rusiyada yerləşən serverlərdə saxlanmaları qanuni bir tələbdir. Roskomnadzor-a bu qanunun icrası tapşırılıb. Böyük xarici məlumat bazaları operatorlarına qanuna riayət etmək üçün əlavə vaxt verilib (2016-cı ilin əvvəlinə qədər). Qanun yalnız 2015-ci ilin sentyabrından sonra toplanmış və ya yenilənən məlumatlara şamil olunur.

Estoniya **–** 2018-ci ilin sonunda Estoniya parlamenti nəhayət yeni fərdi məlumatların qorunması qanununu qəbul etməyə müvəffəq oldu. Yeni Qanun 15 yanvar 2019-cu ildə qüvvəyə mindi; burada ümumi məlumatların qorunması qaydaları hazırlanmış və əlavə edilmişdir.

Son iyirmi ildə Estoniyanın inkişafının nəticəsi kimi Dünya Bankının tərtib etdiyi 2016-ci il üzrə “Dünya inkişaf hesabatı”nda ölkə “rəqəmsal cəmiyyətə ən yaxın” adlandırılmışdır [8]. Estoniya dünyada birinci Data səfirliyini Lüksenburqda açmışdır [9]. Bu o deməkdir ki, ölkədə məlumatların qorunması sahəsində tətbiq olunan bütün qaydalar onun "Data səfirliyi"ndə də tətbiq olunmalıdır. Qeyd edək ki, Lüksenburq dövləti Estoniyanın informasiya sisteminin verilənlərinin toxunulmazlığına zəmanət vermişdir. Lüksenburqda informasiya cəmiyyətinin yüksək səviyyədə inkişafı rəqəmsal xidmətlər sahəsində əməkdaşlıq üçün geniş imkanlara yaratmışdır.

Bu yeni yanaşma, Estoniya dövlətinin yerli məlumat mərkəzlərinin təbii fəlakət, geniş miqyaslı kiberhücum, elektrik kəsilməsi və ya digər böhran vəziyyətinə görə dayandırıldığı və ya pozulduğu bir şəraitdə fəaliyyətini davam etdirməsinə imkan verir [4].

Data səfirliyi – Estoniya hökumətinin buludda genişlənməsidir və bu dövlətin ərazi hüdudlarından kənarda server resurslarına sahib olması mənasını verir. Bu informasiyanın əldə edilməsi üçün innovativ konsepsiya hesab olunur, çünki adətən dövlətlər informasiyalarını öz fiziki sərhədləri daxilində saxlayır. Data səfirliyinin resursları Estoniya dövlətinin nəzarətindədir, kiber-hücumlardan və böhran situasiyalarından blokçeyn texnologiyasının köməyi ilə mühafizə olunur və təkcə verilənlərin ehtiyat nüsxələrinin yaradılması deyil, eləcə də kritik xidmətlərin yerinə yetirilməsi imkanına malikdir [9].

“Data səfirlik” dedikdə Data mərkəzi nəzərdə tutulur. Data mərkəz Lüksenburqda verilənlərin ötürülməsi üçün ən yüksək səviyyəli - Tier 4 təhlükəsizlik səviyyəsində qorunur. Bu ənənəvi diplomatik mənada başa düşülən səfirlik deyil, lakin təsis müqaviləsi diplomatik münasibətlər haqqında Vyana Konvensiyasını nəzərə alaraq beynəlxalq hüquqda tamamilə yeni bir yanaşmadır [9]. Data mərkəz tamamilə Estoniyanın nəzarəti altındadır, lakin toxunulmazlıq kimi fiziki səfirliklərlə eyni hüquqlara malikdir.

Lüksemburq yüksək keyfiyyətli texniki imkanlarına görə, NATO standartlarına cavab verən yüksək etibarlı data mərkəzlərin olması, həm də bu yeni konsepsiya ilə işləmək üçün açıq olduğu üçün ilk Data səfirliyin yerləşdiyi yer hesab edilə bilər. Bu əməkdaşlıqla Lüksemburq və Estoniya dünyada rəqəmsal davamlılığı təmin etmək üçün unikal və innovativ bir yol seçmişlər. Bu yeni yanaşma, Estoniya dövlətinin yerli Data mərkəzlərinin təbii fəlakət, geniş miqyaslı kiber-hücum, elektrik kəsilməsi və ya digər böhran vəziyyətinə görə dayandırıldığı və ya pozulduğu bir şəraitdə fəaliyyətini davam etdirməsinə imkan verir [10]. Server Estoniya ərazisində müvafiq sistemlərin işləməməsi halında vergilər, pensiyalar, mülkiyyət hüquqları, qanunvericilik fəaliyyət və siyahıyaalma məlumatlarına əlyetərliliyinin təmin olunması üçün yaradılmışdır.

Data səfirliyin açılması 2015-ci ildə olsa da, Estoniya və Lüksemburq arasında yekun müqavilənin imzalanması 2017-ci ildə mümkün olmuşdur. Estoniya hökumətinin buludunun inkişaf etdirilməsi Cybernetica, Dell EMC, Ericsson, OpenNode və Telia kimi özəl sektor şirkətləri ilə Estoniya hökumətinin əməkdaşlığı çərçivəsində həyata keçirilmişdir [9].

Estoniya hökuməti 2019-cu ildə fərdi məlumatların istifadəsi və emalını tənzimləyən qanun qəbul etmişdir [11]. Qəbul olunmuş qanun Avropa Birliyinin reqlamentinə uyğun insanların öz fərdi məlumatlarının idarə olunması imkanlarını genişləndirir və üçüncü şəxslər tərəfində emalını tənzimləyir. Qanun qəbul olunduqdan sonra müəssisələr və təşkilatlar istifadəçilərə onların fərdi məlumatlarını necə emal etdikləri barədə daha ətraflı və aydın məlumat verməlidirlər və şəxsin tələbi ilə bu məlumatları silməlidirlər (məlumatların saxlanması üçün başqa qanuni əsaslar olmadıqda).

Fərdi məlumatların qorunması haqqında qanun böyük ictimai maraqlar səbəbindən edilərsə və jurnalist etikası prinsiplərini pozmadığı təqdirdə şəxsin fərdi məlumatlarının mediada yayımlanmasına imkan verir. Məlumatların qorunması üsullarından istifadə edildiyi təqdirdə şəxs haqqında məlumatlar elmi-tədqiqat və statistik məqsədlər üçün onun icazəsi olmadan da toplana və emal edilə bilər. Eləcə də, qanuna əsasən fərdi məlumatları emal edənlər şəxsi məlumatlara dair qanun pozuntuları barədə şəxsə məlumat vermək öhtəliyini öz üzərilərinə götürməyə məcburdurlar [12].

Fərdi Məlumatların Mühafizəsi Qanunu qanun pozuntularının qarşısının alınması, aşkarlanması və icra edilməsi və cəzanın icrası zamanı hüquq mühafizə orqanları tərəfindən fərdi işlərin aparılması, fərdi məlumatların işlənməsi üçün xüsusi əsasları nəzərdə tutur. Sonda qanunda fərdi məlumatların qorunması qaydalarının pozulması halında yeni tərtib olunan cərimələr qeyd olunur.

IV. AZƏRBAYCANDA FƏRDİ MƏLUMATLARIN QORUNMASINA DAİR HÜQUQİ TƏNZİMLƏMƏLƏR

“Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu 2010-cu ildə qəbul edilmiş, 2014 və 2018-ci illərdə müəyyən dəyişikliklər edilərək ölkədə müvafiq sahələr üzrə fəaliyyət göstərən əsas qanunvericilik aktıdır. Bu qanun fərdi məlumatların toplanılması, işlənməsi və mühafizəsi ilə bağlı münasibətləri, milli informasiya məkanının fərdi məlumatlar bölümünün formalaşdırılması, habelə fərdi məlumatların sərhəddən kənar ötürülməsi ilə əlaqədar məsələləri tənzimləyir, bu sahədə fəaliyyət göstərən dövlət və yerli özünüidarə orqanlarının, hüquqi və fiziki şəxslərin hüquq və vəzifələrini müəyyən edir. Bu qanuna əsasən qeyd etmək olar ki, fərdi məlumatlar şəxsin kimliyini birbaşa və ya dolayısı ilə tanımağa imkan verən istənilən növ məlumat hesab olunur. Fərdi məlumatların toplanılması və işlənilməsi, həmin məlumatların mühafizəsinin tam təmin olunmaması nəticəsində subyektə dəyən maddi və mənəvi ziyan və onun həcmi məhkəmə tərəfindən müəyyən edilir, qanunvericilikdə nəzərdə tutulmuş qaydada ödənilir. Bu qanunun əsas məqsədi fərdi məlumatların toplanılmasının, işlənilməsinin və mühafizəsinin qanunvericilik əsaslarını və ümumi prinsiplərini, həmin sahədə dövlət tənzimləməsinin qayda və tələblərini, fərdi məlumatların informasiya ehtiyatlarında formalaşdırılması, informasiya sistemlərinin yaradılması, informasiyanın verilməsi və ötürülməsi qaydalarını, bu prosesdə iştirak edən şəxslərin hüquqlarını, vəzifələrini və məsuliyyətinin əsaslarını müəyyən etməkdən, əsas insan və vətəndaş hüquqlarını və azadlıqlarını, o cümlədən şəxsi və ailə həyatının sirrini saxlamaq hüququnu müdafiə etməkdən ibarətdir [13].

Müasir hüquq konsepsiyası fərdin ən müqəddəs xəzinəsi hesab olunan fərdi məlumatlarının qorunması üzərində qurulub. Bu səbəblə, insanların həyatını asanlaşdırmaq üçün inkişaf etdirilən məlumatların yığılması və ötürülməsi texnologiyaları ilə fərdi hüquqların pozulmasının qarşısını almaq üçün ölkələr qanuni tənzimləmələrə müraciət etmişdirlər.

Müasir sivilizasiya səviyyəsinə çatmaq məqsədinə uyğun olaraq, ölkəmiz dünya standartlarına cavab verən, gəlirlərini ədalətli bölüşən, insan hüquqlarını, qanunun aliliyini, iştirakçı demokratiyanı, dünyəviliyi, din və vicdan azadlığını təmin edən bir dövlət olmaq üçün səylərini artırır.

NƏTİCƏ

Hər bir siyasi, hüquqi, iqtisadi və ya sosial islahat vətəndaşların həyat səviyyəsini yüksəldir və beynəlxalq iqtisadi gücünü, ölkəmizin demokratik nüfuzunu və təhlükəsizliyini artırır. Fərdi məlumatların təhlükəsizliyi, qanunun aliliyi, insan hüquqları və əsas azadlıqlar təkcə ali ümumbəşəri dəyərlər deyil, həm də iqtisadi və siyasi sabitliyin və inkişafın ən etibarlı təməlidir.

Məqalədə fərdi məlumatlar sahəsində beynəlxalq təcrübə araşdırılır. Fərdi məlumatların qorunması ilə bağlı beynəlxalq təcrübədə qəbul olunmuş qanunlara baxılması yalnız ölkələr üçün deyil, bütövlükdə cəmiyyət üçün böyük əhəmiyyət kəsb edir. Fərdi məlumatların qorunmasında təhlükəsizlik prioritet məsələlərdən biri hesab edilir. Beynəlxalq təcrübələr innovativ ideyalar irəli sürməklə effektli həllərin işlənməsini tələb edir. Məqalədə fərdi məlumatların qorunmasına dair bir sıra ölkələrin, o cümlədən Avropa Birliyi, Rusiya, Estoniya, ABŞ kimi ölkələrin təcrübəsi araşdırılmışdır. Müqayisəli təhlil zamanı inkişaf etmiş ölkələrdən olan Estoniyanın təklif etdiyi müasir mexanizmlərdən biri olan data səfirliyi ilə Rusiyanın təklif etdiyi müasir mexanizmlər arasında oxşarlıqlar görülmüş və təhlükəsizliyin qorunması üçün nümunə olaraq götürülmüşdür. Düzgün və ardıcıllıqla istifadə edilən təhlükəsizlik qanunları və mexanizmləri vətəndaş cəmiyyətinin inkişafının yüksək səviyyəyə nail olmasına şərait yaradacaqdır.

İSTİNADLAR

[1] N. Purtova, “The law of everything. Broad concept of personal data and future of EU data protection law,” 2018. https://doi.org/10.1080/17579961.2018.1452176

[2] Y. İmamverdiyev, “ E-Səhiyyədə İnformasiya Təhlükəsizliyinin Aktual Problemləri,” İnformasiya cəmiyyəti problemləri, №1, 2017, səh. 24–34.

[3] A. Lehavi, P. Larouche, M. Accetto, N. Purtova, L. Zemer, “The Human Right to Privacy and Personal Data Protection: Local-to-Global Governance in the Digital Era,” 2016. https://lawschoolsgloballeague.com

[4] Data Protectıon Laws of The World, 2017 https://www.thebackgroundinvestigator.com

[5] Communication from the Commission to the European Parliament and the Council, Data protection rules as a trust-enabler in the EU and beyond – taking stock. https://eur-lex.europa.eu

[6] S. Cobb, “Data privacy and data protection: US law and legislation,” April 2016, pp. 3-16.

[7] Personal Data Regulation in Russia: Roskomnadzor Update. 2019.

[8] World Development Report 2016: Digital Dividends, www.worldbank.org

[9] Data embassy, https://e-estonia.com

[10] Рийгикогу принял закон о создании посольства данных в Люксембурге, 2018. https://rus.err.ee

[11] Personal Data Protection Act, www.riigiteataja.ee

[12] Digital Government Factsheet 2019, Estonia. https://joinup.ec.europa.eu

[13] “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu, www.e-qanun.az

ANALYSIS OF INTERNATIONAL PRACTICES IN THE FIELD OF PERSONAL DATA PROTECTION

Farhad Yusifov[1], Aysan Farajova[2]

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

[1]farhadyusifov@gmail.com, [2]aysanpharajova@gmail.com

Abstract – The article explores international experience in the field of personal data. Personal data is classified as sensitive information category. The access, processing and use of personal information must be authorized by someone and in other cases, their use must be restricted. In international practice, the “harbour port” mechanism used to protect personal information is used by individuals or relatives, family members, etc. requires that sensitive data should be deleted. The data embassy in Estonia has been implemented as an innovative mechanism for ensuring personal data, and the work and laws adopted the protection of personal data inside its territorial boundaries in Russia have been investigated.

Keywords *– personal data, data security, personal data protection, data embassy*