İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi problemləri

Ramiz Şıxəliyev
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

***Xülasə*— İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi şəxsi həyatın toxunulmazlığının təmin edilməsi üçün çox vacib məsələdir. Lakin qlobal İnternet mühitində bu məsələnin həlli çox çətin problemdir. Çünki İnternet istifadəçiləri marketinq və elektron kommersiya, sosial media, bulud və s. kimi çoxlu sayda elektron xidmətlərdən və həmçinin mobil İnternet vasitələrindən istifadə edirlər və onların fərdi məlumatları müxtəlif mənbələrdə (xidmətlərdə, bazalarda və s.) yerləşir. Bu mənbələrdə yerləşən fərdi məlumatlara qarşı təhdidlər də müxtəlif olur. Belə bir paylanmış qlobal mühitdə fərdi məlumatların təhlükəsizliyinin monitorinqi üçün vahid bir mexanizmin yaradılması çox çətin məsələdir. Məqalə İnternet mühitində fərdi məlumatların təlükəsizliyinin monitorinqi problemlərinin analizinə həsr olunmuşdur. Analiz nəticəsində, fərdi məlumatların təhlükəsizliyinin monitorinqi məsələsinin onların yerləşdiyi mənbələrdən asılı olaraq müəyyən edilməsi və intellektual texnologiyaların (multi-agent texnologiyasından) istifadəsi ilə paylanmış monitorinq sisteminin yaradılması məqsədəuyğun hesab edilmişdir.**

Açar sözlər— fərdi məlumatlar, fərdi məlumatların kateqoriyaları, şəxsi həyatın toxunulmazlığı, fərdi məlumatların təhlükəsizliyinin monitorinqi

I. GİRİŞ

Rəqəmsal texnologiyaların istifadə sahəsinin genişlənməsi dövlət xidmətləri, səhiyyə, ticarət və s. sahələrdə fərdi məlumatların təhlükəsizliyinin təmin edilməsi problemlərinin yaranmasına gətirib çıxarmışdır. Belə ki, bu xidmətlərdən istifadə zamanı istifadəçilər həm könüllü, həm də bilməyərəkdən öz fərdi məlumatlaını daxil edirlər. Bu halda, heç şübhə yoxdur ki, rəqəmsal texnologiyaların istifadəsinin üstünlüyünə baxmayaraq istifadəçilərin şəxsi həyatının toxunulmazlığına təhlükə yaranır. Xüsusilə də istifadəçilər İnternet mühitində elektron xidmətlərdən, sosial şəbəkələrdən istifadə zamanı böyük risklərə məruz qalırlar. Məsələn, istifadəçilər Facebook, Twitter, Instagram, MySpace və s. kimi sosial şəbəkələrdən, bulud xidmətindən, bloqlardan, vakansiyalar üzrə veb-saytlardan, smartfonlardan, elektron ticarətdən və s. istifadə etdikdə öz fərdi məlumatlarını daxil edirlər. Bununla yanaşı, həm dövlət, həm də özəl sektor istifadəçilərin fərdi məlumatlarından öz məqsədləri üçün istifadə edirlər və çox zaman bu məlumatlar insanların xəbəri olmadan toplanır. Bununla da istifadəçinin fərdi məlumatlarının yeni bir ekosistemi meydana çıxır. Təbii ki, istifadə edilən rəqəmsal texnologiyaların və xidmətlərin sayı artdıqca istifadəçilər öz fərdi məlumatları üzərindəki nəzarəti demək olar ki itirirlər.

Bu gün fərdi məlumatların təhlükəsizliyinin təmin edilməsinin mexanizmlərinin olmaması fərdi məlumatların təhlükəsizliyinin tez-tez pozulmasına səbəb olur. Çox zaman fərdi məlumatların təhlükəsizliyinin pozulması hallarının müəyyən edilməsi mümkün olmur. Buna görə də, elektron xidmətlər yaradılarkən və istifadə edilərkən fərdi məlumatların təhlükəsizliyinin təmin edilməsi və ona nəzarət məsələləri mütləq tələb kimi nəzərə alınmalıdır. Yəni elektron xidmətlər istifadə edilərkən, fərdi məlumatların təhlükəsizliyinin təmin edilməsi və ona nəzarət mexanizmləri olmalıdır. Bir sözlə, rəqəmsal texnologiyaların istifadəsi zamanı fərdi məlumatların təhlükəsizliyinin monitorinqi imkanlarının olması çox vacib məsələdir. Təhlükəsizliyin monitorinqi istifadəçilərin fərdi məlumatlarının tam təhlükəsizliyini təmin etməyə imkan verməlidir. Lakin, digər tərəfdən, elə fərdi məlumatların təhlükəsizliyinin monitorinqinin özü istifadəçilərin şəxsi həyatının toxunuzmaqlığına təhlükə yarada bilər. Hətta şəbəkə trafikinin monitorinqi istifadəçilərin şəxsi həyatının toxunuzmaqlığına təhlükə yarada bilər, çünki verilənlərin analizi və klassifikasiyanın müasir üsullarının köməyi ilə şəbəkə trafikindən də fərdi məlumatlar əldə etmək olar [1].

Qeyd etmək lazımdır ki, bu gün qlobal İnternet mühitində istifadəçilərin fərdi məlumatlarının təhlükəsizliyinin bütövlükdə təmin edilməsi çox çətin məsələdir və bu mühitdə fərdi məlumatların təhlükəsizliyinin bütövlükdə monitorinqi üçün vasitə və imkan yoxdur.

İşin məqsədi İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi problemlərinin analizidir.

II. FƏRDİ MƏLUMATLARIN KATEQORİYALARI

Fərdi məlumatların təhlükəsizliyinin təmin edilməsi zamanı əsas məsələlərdən biri bu məlumatların kateqoriyalarının müəyyən edilməsidir. Verilənlərin mühafizəsinin təmin edilməsi hüququ Avropa Birliyinin Verilənlərin Mühafizəsinin Ümumi Qaydalarına (EU GDPR – European Union General Data Protection Regulation) görə əsas insan hüququ kimi qəbul edilmişdir [2]. EU sənədində fərdi məlumatlar belə müəyyən olunmuşdur: “Fərdi məlumatlar” identifikasiya olunmuş və ya identifikasiya olunan fiziki şəxsə (“məlumat subyektinə”, img.

DOI: 10.25045/NCInfoSec.2019.25

“data subject”) aid olan istənilən informasiyadır; identifikasiya olunan fiziki şəxs, birbaşa və ya dolayı yolla, xüsusən də ad, şəxsiyyət nömrəsi, yeri haqqında məlumat, onlayn identifikator və ya fiziki, fizioloji, genetik, əqli, iqtisadi, mədəni və ya sosial kimliyi kimi identifikatorlar vasitəsilə identifikasiya oluna bilən şəxsdir. Bir sözlə, fərdi məlumat konkret (canlı) şəxsin identifikasiya edilməsinə səbəb ola biləcək hər hansı bir məlumatdır. Bu, ad kimi açıq şəkildə identifikasiya edilə bilən məlumatlar, həmçinin yaş, boy, çəki, sərvət, iş yeri, şirkət, şəhər və s. kimi məlumatların kombinasiyası da ola bilər. Çünki bu məlumatların kombinasiyası şəxsi identifikasiya etməyə imkan verir.

EU GDPR fərdi məlumatların xüsusi kateqoroyalarını müəyyən edir ki, bunlara irqi və ya etnik mənşə, siyasi baxışlar, dini və ya fəlsəfi inanclar, həmkarlar ittifaqı üzvlüyü, genetik məlumatlar, biometrik məlumatlar, sağlamlıq məlumatları, cinsi həyat və cinsi orentasiya aiddir. Bu kateqoriadan olan fərdi məlumatlar əlavə vasitələrlə mühafizə olunmalıdır. Fərdi məlumat subyektinin açıq razılığı, əsaslı səbəblər və ya müəyyən istisnaslar olmadıqda toplanıla və emal oluna bilməz. Ancaq o fərdi məlumatlar emal oluna bilər ki, məlumat subyekti tərəfindən birmənalı şəkildə açıqlanmış olsun.

Fərdi məlumatlara misal kimi şəxsə aid olan müxtəlif məlumatları göstərmək olar. Məsələn, ad, soyad, təvəllüd, foto, telefon nömrəsi, ev ünvanı (küçə, şəhər, poçt indeksi və s.), elektron poçt ünvanı, bank hesab nömrəsi, kredit kartının nömrəsi, pasportun nömrəsi və fərdi identifikasiya nömrəsi, sosial sığorta kartının nömrəsi, vergi ödəyici nömrəsi, nəqliyyat vasitəsinin dövlət nömrə nişanı, IP-ünvan, “cookie” identifikatoru, olduğu yeri haqqında məlumat, əl yazısı, loqin və parol, sosial media profili identifikatoru, mobil cihaz identifikatorları, məşğulluq haqqında məllumat, vəzifəsi, təhsili haqqında məlumat və s. Həmçinin xüsusi fərdi məlumatlar müəyyən olunmuşdur ki, onlara cinsi, irqi/etnik mənsubluğu, doğulduğu yer/şəhər/ölkə, həyat yoldaşının adı, sağlamlıq haqqında məlumat, tibbi qeydlər və s. məlumatlar aid edilir.

EU GDPR həmçinin “nəzarətçi” (controller) və “prosessor” (processor) anlayışlarını müəyyən etmişdir. Bu anlayışlar fərdi məlumatların monitorinqi üçün çox vacib anlayışlardır və məlumat subyekti, nəzarətçi və prosessor arasındakı münasibətləri müəyyən etməyə imkan verir.

“Nəzarətçi” dedikdə fərdi məlumatların emalının məqsəd və vasitələrini təyin edən fiziki və ya hüquqi şəxs, dövlət orqanı, agentlik və ya digər qurum başa düşülür.

“Prosessor” dedikdə isə nəzarətçi adından fərdi məlumatları emal edən fiziki və ya hüquqi şəxs, dövlət orqanı, agentlik və ya digər qurum başa düşülür.

III. FƏRDİ MƏLUMATLARA QARŞI TƏHDİDLƏRİN MƏNBƏLƏRİ

Yeni informasiya texnologiyalarının inkişafı və geniş istifadəsi fərdi məlumatların təhlükəsizliyinə təhdidlər yaradır və nəticədə fərdin şəxsi həyatının toxunulmazlığına təhlükə yaranır [3]. Bu təhdidlərin mənbələri müxtəlif ola bilər. Məsələn, çox zaman, fərdi məlumatları toplayan tərəflər şəxslərin xəbəri olmadan (və yaxud onlara məlumat vermədən) onların fərdi məlumatlarını toplayırlar. Bu zaman üçüncü tərəf həmin məlumatları ələ keçirə və istifadə edə bilər, yəni şəxslər öz fərdi məlumatlarının təhlükəsizliyi haqqında məlumatsız olurlar. Buna görə də, səxslərin icazəsi və onların məlumatlandırılması fərdi məlumatların toplanması, emalı və yayılması üçün çox vacib tələblərdir və bu da sui-istifadələrin qarşısını ala bilər. Fərdi məlumatların təhlükəsizliyinə qarşı təhdidlərin yaranmasının digər bir mənəbəyi bu məlumatların olduğu verilənlər daşıyıcıları, məsələn, aparat vasitələri, proqram təminatı, əlaqə kanalları və s. ilə bağlıdır.

Fərdi məlumatların təhlükəsizliyinə qarşı təhdidlərin yaranmasının digər bir mənbəyi isə yeni İnternet texnologiyalarının (məsələn, Əşyaların İnterneti, ing. Internet of Things (IoT), mobil texnologiyaların (Mobil İnternetin) və s.), həmçinin böyük verilənlər (ing.Big Data) fenomeninin yaranması ilə bağlıdır. Məsələn, IoT insan həyatının bütün sahələrini əhatə edir – evlərdə, xəstəxanalarda və s. sahələrdə istifadə edilir və IoT çərçivəsində qurğularda olan fərdi məlumatlara ciddi təhdidlər yarana bilər. Bu gün IoT qurğularına qarşı müxtəlif hücum növləri mövcuddur [4]. Böyük verilər texnologiyası müxtəlif sahələrdə, məsələn, sosial şəbəkələrdə, tibbi kartlarda və s. toplanmış verilənlərin emalı üçün istifadə edilir və nəticədə fərdi məlumatlara və şəxsi həyatın toxunulmazlığına təhdid yarana bilər [5].

Fərdi məlumatların təhlükəsizliyinə qarşı təhdidlərin yaranması mənbələrindən biri də müxtəlif İnternet xidmətlərinin yaranması və istifadəsidir. Məsələn, marketinq və elektron kommersiya, sosial media, bulud və s. xidmətlərin istifadəsi. Məlumdur ki, bu xidmətlərin istifadəsi zamanı, xüsusilə də sosial medianın [6] və bulud xidmətlərinin [7] istifadəsi zamanı istifadəçilərin fərdi məlumatları toplanır və onlara qarşı təhdidlər yarana bilər.

IV. FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİNİN MONİTORİNQİ PROBLEMLƏRİ

İnternet mühitində fərdi məlumatların təhlükəsizliyinin təmin edilməsinin vacib elemenlərindən biri onun monitorinq edilməsidir. Fərdi məlumatların təhlükəsizliyinin monitorinqi problemi aydın görünsə də, mümkün vahid həll yolunun tapılması çətin məsələ olaraq qalır.

Bu gün istənilən şəxsin fərdi məlumatları müxtəlif mənbələrdə (xidmətlərdə, bazalarda və s.) ola bilər və bu məlumatlara qarşı müxtəlif təhdidlər ola bilər. Bu zaman monitorinq məsələsinə sırf texniki məsələ kimi baxılması düzgün olmaz. Çünki o, həm də şəxsi həyatın toxunulmazlığı məsələsini əhatə edir. Yəni fərdi məlumatların təhlükəsizliyinin monitorinqi mexanizminin yaradılması zamanı mütləq şəxsi həyatın toxunulmazlığının təmin edilməsi məsələsi nəzərə alınmalıdır – bu məsələni həyata keçirən komponent olmalıdır. Bununla yanaşı fərdi məlumatların təhlükəsizliyinin

monitorinqinin həyata keçirilməsini tənzimləyən standartlar, mexnizmlər və davranış kodeksləri işlənilməlidir. Bu standartlar maraqlı tərəflərin iştirakı ilə, müəssisə, regional və yaxud da beynəlxalq səviyyələrdə işlənilə bilər. Bu zaman hansı məlumatların toplanması, kimin toplaması, məlumatın həcmi, kimin və hansı əsaslarla bu məlumatlara giriş hüququ əldə etməsi, məlumatların toplanması və saxlanması müddəti və s. nəzərə alınmalıdır. Bununla yanaşı şəxsi həyatın toxunulmazlığının təmin edilməsi üçün internet-provayderlər müvaviq tələblərə uyğunlaşmaq üçün öz şəbəkə monitorinq infrastrukturlarını yeniləməlidirlər.

Məlumdur ki, şəbəkələrin monitorinqi üçün əsasən iki sinif monitorinq sistemləri istifadə edilir. Birinci sinfə şəbəkənin diaqnostikası, planlaşdırılması və xidmət keyfiyyətinin təmin edilməsi kimi sistemlər daxildir. Bu sistemlər adətən passiv şəkildə toplanmış verilənləri emal edir və aqreqasiya olunmuş verilənləri əldə edir. Əldə edilmiş verilənlər müxtəlif şəbəkə problemlərinin həlli üçün istifadə edilir. Məsələn, yüklənmə, məhsuldarlıq, resursların istifadəsi, planlaşdırma, xidmət səviyyəsi haqqında razılaşmanın (ing. service level agreement – SLA) və s. şəbəkə problemlərinin müəyyən edilməsi üçün istifadə edilir. Bu zaman məlumat paketlərində olan əhəmiyyətli informasiyaya (ing. packet payload) tam şəkildə giriş tələb olunmur və şəxsi həyatın toxunulmazlığı məsələsi anonimliyin qorunmasından ibarət olur. İkinci sinif monitorinq sistemlərinə müdaxilələrin aşkarlanması sistemləri aiddir və şəbəkə təhlükəsizliyinə yönəlmişdir. Əsasən trafikin klassifikasiyasını həyata keçirir. Buna görə də bu sistemlər məlumat paketlərinin dərin yoxlanmasına və bu paketlərdə göndərilən əhəmiyyətli informasiyanın detallı şəkildə analizinə əsaslanır. Bu halda şəxsi həyatın toxunulmazlığının təmin edilməsi çox çətin məsələyə çevrilir.

Yuxarıda deyilənləri nəzərə alaraq, qeyd etmək lazımdır ki, fərdi məlumatların təhlükəsizliyinin monitorinqi məsələsinin onların yerləşdiyi mənbələrdən asılı olaraq müəyyən edilməsi və intellektual texnologiyaların (multi-agent texnalogiyasından) istifadəsi ilə paylanmış monitorinq sisteminin yaradılması daha məqsədəuyğun olardı.

NƏTİCƏ

İnformasiya və kommunikasiya texnologiyalarının sürətlə inkişafı və geniş istifadəsi (xüsusilə də İnternetin) elektron xidmətlərin sayının və elektron formadakı informasiyanın həcminin həddindən çox artmasına gətirib çıxarmışdır. Bu şəraitdə, şəxsi həyatın toxunulmazlığının təmin edilməsi üçün fərdi məlumatların təhlükəsizliyi çox vacib və çətin məsələyə çevrilmişdir.

Bu gün rəqəmsal mühitdə fərdi məlumatların təhlükəsizliyinin təmin edilməsi üçün hüquqi baza yaradılmışdır. Buna misal olaraq Avropa Birliyinin Verilənlərin Mühafizəsinin Ümumi Qaydalarını göstərmək olar. Bununla yanaşı texniki və texnoloji bazanın da olması çox vacibdir və bunlardan biri fərdi məlumatların təhlükəsizliyinin monitorinqi mexanizminin və vasitələrinin işlənməsidir.

İnternet mühitində fərdi məlumatların təhlükəsizliyinin təmin edilməsi üçün onların təhlükəsizlik vəziyyəti qiymətləndirilməlidir, yəni monitorinq edilməlidir. Lakin bu zaman şəxsi həyatın toxunulmazlığı ilə bağlı problemlər yarana bilər. Buna görə İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi zamanı yaranan problemlərin analizi çox vacibdir.

İSTİNADLAR

[1] G. Bianchi, E. Boschi, F. Gaudino, L. Koutsoloukas, et al. “Privacy-preserving network monitoring: Challenges and solutions,” ICT Mobile Summit, pp. 1-10, 2008.

[2] https://eugdpr.org/the-regulation

[3] E. Y. Yıldırım, A. Eşref “The threats and risks in personal data security,” Proceedings of the International Conference on Computer Science and Engineering, pp. 610-615, 2017.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao “A survey on security and privacy issues in Internet-of-Things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, 2017.

[5] B. B. Rad, N. Akbarzadeh, P. Ataei, and Y. Khakbiz “Security and privacy challenges in Big data era,” International Journal of Control Teory and Applications, vol. 9, no. 43 , pp. 437-448, 2016.

[6] X. Liang, Z. Kuan, and X. Shen “Security and privacy in mobile social networks: Challenges and solutions,” IEEE Wireless Communications, pp. 33-41, 2014.

[7] H. Takabi, B. D. Joshi, G.J. Ahn “Security and privacy challenges in cloud computing environments,” IEEE Security and Privacy Magazine, vol. 8, no. 6, pp. 24–31, 2011.

PROBLEMS OF MONITORING OF PERSONAL DATA SECURITY IN INTERNET ENVIRONMENT

Ramiz Shikhaliyev

Institute Information Technology of ANAS, Baku, Azerbaijan

ramiz@science.az

Abstract– Monitoring the security of personal information in the Internet environment is a very important issue to ensure the inviolability of privacy. But in the global Internet environment, this is a very difficult problem. This is because Internet users use marketing and e-commerce, social media, cloud, and so on. They use a large number of electronic services, including mobile Internet, and their personal information is stored in various sources (services, databases, etc.). The threats to the personal data contained in these sources also vary. Creating a single mechanism for monitoring the security of personal data in such a distributed global environment is a difficult task. The article is devoted to the analysis of the problems of monitoring the privacy of personal information in the Internet. As a result of the analysis, the article notes the feasibility of establishing a distributed monitoring system with the use of intelligent technology (multi-agent technology) to identify the issue of monitoring personal data security depending on the source of their location.

Keywords– *personal data, categories of personal data, privacy, monitoring of personal data security*