Elnur Hümbətov. Əşyaların interneti və mobil tətbiqlərin istifadəsi üzrə əsas hüquqi problemlər // Ali Məhkəmənin Bülleteni, 2024 (N° 1), səh. 1-9

DOI: 10.30546/120124.2024.1.03.

ƏŞYALARIN İNTERNETİ VƏ MOBİL TƏTBİQLƏRİN İSTİFADƏSİ ÜZRƏ ƏSAS HÜQUQİ PROBLEMLƏR

Hümbətov Elnur Akif oğlu

Bakı Dövlət Universitetinin
İnsan hüquqları və informasiya hüququ UNESCO
kafedrasının müəllimi,
hüquq üzrə fəlsəfə doktoru
elnur_88@inbox.ru

Xülasə

Mc Luhanın "Biz alətlərimizi formalaşdırırıq, sonra alətlərimiz bizi formalaşdırır", ifadəsində deyildiyi kimi, texnologiyalar istifadə olunduqca cəmiyyətdə dəyişikliklərə səbəb olur. Belə ki, Əşyaların internetinin formalaşması və ağıllı əşyaların insanların gündəlik həyatında daha çox istifadə olunması, eləcə də müxtəlif mobil tətbiqlərin sayının günbəgün artması bu yeni tendensiyaların insan hüquq və azadlıqları üçün yaratdığı təhlükələrin vaxtında qarşısının alınmasını tələb edir. Bu zaman həmin texnologiyaların tətbiqi zamanı riayət olunmalı prinsiplərin dairəsinin əvvəlcədən dəqiq müəyyən olunması və təminat mexanizmlərinin işlənib hazırlanması xüsusi əhəmiyyət kəsb edir.

Məqalədə konkret faktlar üzərində cari hüquqi problemlər təhlil edilərək, onların qarşısının alınması üzrə təklif və tövsiyələr işlənib hazırlanmışdır.

Açar sözlər: Əşyaların interneti, mobil tətbiqlər, hüquqi tələblər, standartlar, insan hüquqları, ağıllı əşyalar.

1.1. Giriş

Biz mobil tətbiqlər əsrində yaşayırıq. Hələ 2000-ci illərdə informasiya cəmiyyəti quruculuğuna dair ilkin beynəlxalq sənədlər qəbul edilərkən informasiya və kommunikasiya texnologiyalarının (bundan sonra - İKT) istifadəsini asanlaşdıran mobil əlavələrin inkişaf etdirilməsi əsas prioritet istiqamətlər sırasında yer almışdı. Azərbaycan Respublikasında da elektron Azərbaycan dövlət proqramlarında mobil tətbiqlərin geniş istifadəsi üçün imkanların yaradılması məsələsi hər zaman xüsusi qeyd olunurdu. Bu gün nəinki ölkəmizdə, bütün dünya dövlətlərində mobil tətbiqlərdən çox asan və rahat olduğu üçün geniş formada istifadə olunur. Dünyada 6,3 milyarddan çox smartfon istifadəçisi və Android və iOS platformalarında yeddi milyondan çox proqramla mobil proqramlar sənayesinin sürətlə inkişaf etməsi təəccüblü deyil. "Grand View Research"ə görə, qlobal mobil proqramlar bazarı 2022-ci ildə 206,85 milyard dollar dəyərində qiymətləndirilmişdir və 2023-cü ildən 2030-cu ilə qədər 13,8% CAGR ilə artmağı gözlənilir (19).

Artıq təxminən 10 milyard cihazın qarşılıqlı əlaqəyə malik olduğu təxmin edilir və 2025-ci ilə qədər bu rəqəmin 25 milyarda çatacağı gözlənilir (6). Əşyaların internetinin (bundan sonra – Əİ) iqtisadi təsiri çox böyük olacaq, 2025-ci ildə ildə 11,1 trilyon ABŞ dolları və 2035-ci ildə isə 12,3 trilyon dollara çatacağı gözlənilir (10). İnternet bağlantısının 5G mobil rabitə standartı ilə asanlaşdırılacağı gözlənilir. 5G mövcud 4G LTE5-dən 100 dəfəyə qədər sürətli olacaq, ucdan-uca gecikmə 1 milli saniyəyə enəcək ki, bu da məlumatların fasiləsiz ötürülməsindən asılı olan uzaqdan əməliyyatlara və ya özü idarə olunan avtomobillərə imkan verə bilər. 5G və digər qarşılıqlı fəaliyyət standartlarının Əşyaların internetinin potensial dəyərinin 40%-ni təşkil etdiyi təxmin edilir (17, p. 17).

Əİ və əlaqəli texnologiyaların ortaya çıxması artıq əhəmiyyətli sosial-texniki dəyişikliyə səbəb olmuşdur və bu, çox güman ki, hələ də davam edəcək. Bu dəyişiklik cəmiyyət üçün, xüsusən də aşağıdakı sahələrdə əhəmiyyətli faydalar gətirir: əlillərin daha müstəqil həyat sürməsinə kömək etmək; səhiyyədə; yaşlılara qulluq zamanı; daha səmərəli və dayanıqlı infrastruktur, nəqliyyat, sənaye və kənd təsərrüfatında. Bununla belə, Əİ və mobil tətbiqlər gündəlik həyatımızda fayda gətirə bilsə də, insanlar Əİ cihazlarından və mobil tətbiqlərdən istifadə etməklə fərdi məlumatların açıqlanması, dövlət və korporativ maraqlar tərəfindən arzuolunmaz nəzarət, fiziki xəsarətlər kimi bir sıra risklərə məruz qalırlar.

1.2. Əşyaların internetinin insan hüquqlarının qorunmasında yaratdığı problemlər və onların həlli yolları

Bu gün Əİ-nin hələ də razılaşdırılmış tərifi yoxdur. Onun mənası müxtəlif maraqlı tərəflər arasında geniş şəkildə fərqlənə bilər və zaman keçdikcə təkamül etmiş və edəcəkdir. Azərbaycan qanunvericiliyində Əİ-yə dair heç bir hüquqi yanaşmaya rast gəlmək mümkün deyil. Lakin Cinayət-Prosessual Məcəllədə nəzərdə tutulan elektron nəzarət vasitələri əslində Əİ-yə bariz nümunədir (maddə 156-1) ki, bunlara elektron qolbaq, mobil nəzarət qurğusu, ev nəzarət stansiyası və ev siqnal ötürücüsü daxildir.

İnformasiya-Kommunikasiya Texnologiyalarının Tətbiqi və Tədrisi Mərkəzinin verdiyi anlayışa görə, Əşyaların interneti (Internet of Things, IoT) müxtəlif əşyaların və qadcetlərin insan müdaxiləsi olmadan bir-biri ilə IP qoşulması üzərindən qarşılıqlı əlaqəyə girdiyi şəbəkədir (1). Məsələn, son illərdə tibbdə geniş istifadə olunan bədəndə (body-worn) daşınan (wearable) bir çox cihazlar vardır ki, onlar insanın fizioloji parametrlərini ölçərək məsafədən ötürmək qabiliyyətinə malikdir. Bu tip ağıllı əşyalar eynək, saat, üzük, qolbaq, baş örtüyü və s. geyim əşyaları formasında da təqdim olunur (2, s. 21).

Deməli, Əİ internetə qoşulmuş və həmişə aktiv olmaq potensialına malik cihazlar şəbəkəsidir. Əİ cihazlarının canlılar, fiziki dünya, digər Əİ cihazları və digər hesablama cihazları və ya sistemləri ilə qarşılıqlı əlaqəsi ola bilər. Bir çox Əİ cihazları həmçinin bir və ya bir neçə aşağıdakı atributlara malikdir: aktiv tutum (fiziki aləmdə hərəkət etmək qabiliyyəti), uyğunlaşma (kontekstdən xəbərdarlıq), ünvanlılıq (unikal ünvan), canlılarla əlaqə, muxtariyyət, asılılıq (uzaqdan xidmətlər və ya infrastruktur), geoyerləşmə qabiliyyəti, identifikasiya (unikal cihaz identifikatoru/lar), mobillik və ya daşınma qabiliyyəti, əməliyyat, iqtisadi və sosial təsir, şəbəkənin yerləşdirilməsi, yayılması, istifadə nümunəsi, görünmə qabiliyyəti, dəyişkənlik və zəiflik (14, p. 3).

İstehlakçılar, vətəndaşlar, biznes və dövlət sektoru üçün problemləri müəyyən edərkən, Əİ cihazlarının və onların iştirak etdiyi sistemlərin əsas mürəkkəb və bir-biri ilə əlaqəli təbiətini nəzərə almaq vacibdir. Bütün Əİ cihazları fiziki obyektdən və ya canlıdan, kompüter prosessoru şəklində aparatdan və proqram təminatından ibarətdir. Bir çox Əİ cihazları daha böyük bir Əİ cihazının içərisində yerləşə bilər və ya daha böyük, paylanmış sistemin elementlərini təşkil edə bilər. Əşyaların interneti cihazlarından yaranan problemlər tək bir Əİ cihazına və ya Əşyaların interneti cihazının iştirak etdiyi ekosistemin bütün və ya bəzi elementlərinə aid ola bilər. Aparat, proqram təminatı, obyekt və ya xidmətin bu elementlərinin hər hansı biri və ya hamısı müxtəlif qurumlar tərəfindən fərdi satışın bir hissəsi kimi (məsələn, ağıllı evdə) və ya ictimaiyyət tərəfindən istifadə olunan sistemlərin bir hissəsi kimi (məsələn, ağıllı şəhərlərdə) təmin edilə bilər.

Əşyaların internetinin geniş istifadəsi müasir dövrün hüquq doktrinası üçün yeni anlayışlar formalaşdırmışdır. Məsələn, son zamanlar insansız fərdi məlumatlar haqqında danışılır ki, bu məlumatlar bir-birinə bağlı olan obyektlərin insan müdaxiləsi olmadan hərəkətə gətirilməsi və fəaliyyəti nəticəsində topladığı məlumatları əhatə edir (12, p. 155).

Əşyaların interneti cihazlarının tətbiqinin insan hüquqlarına, daha dəqiq desək, şəxsi toxunulmazlıq hüququ, təhlükəsizlik, ayrı-seçkiliyə yol verilməməsi və bərabər rəftar, eləcə də məlumat, fikir və ifadə azadlığı kimi siyasi hüquqlara mənfi təsir göstərdiyi hallara çox rast gəlinir. Məlumata əsaslanan ayrı-seçkilik qəsdən və ya planlaşdırılmamış ola bilər. Xüsusi narahatlıq doğuran sahələrdən biri alqoritmik ayrı-seçkilikdir ki, burada maşın öyrənməsində istifadə olunan çox vaxt nisbətən kiçik və yaxud seçmə məlumat dəstləri ictimai qərəzləri ehtiva edir. Məsələn, irq, cins, sağlamlıq vəziyyəti, sosial-iqtisadi vəziyyət və məşğulluq imkanları, mənzil, polis və cəza siyasəti kimi sahələrə təsir edən digər dəyişənlər üzrə toplanmış məlumatlar əsasında alqoritmik ayrı-seçkiliklə bağlı əhəmiyyətli faktlar ortaya çıxır. 2017-ci ilin əvvəlində "Amazon" maşın öyrənməsindən istifadə edən işə götürmə vasitəsinin istifadəsindən və sonrakı inkişafından imtina etdi, çünki onlar bunun proqram tərtibatçısı işlərinə və digər texniki yazılara namizədləri gender baxımından neytral şəkildə qiymətləndirilmədiyini aşkar etdilər. İddialara görə, bu, istifadə

edilən təlim məlumat dəstinin xarakteri ilə bağlı olmuşdur (14, p. 15).

"Amazon"un qabaqcıl Əİ cihazı olan "Amazon Echo"dan yaranan mümkün insan hüquqları pozuntularını araşdıran R.Pakzadın tədqiqatı maraq doğurur. Universal ev köməkçisi kimi işləmək üçün nəzərdə tutulmuş ilk səslə aktivləşdirilmiş cihaz olan "Amazon Echo" gündəlik tapşırıqlarınızı "Google" və ya "Apple" təqviminizdən oxuya bilir. Siqnal və ya taymer qurmaq və ya istehlak məhsulları üçün alış-veriş etmək üçün "Echo" kömək etmək imkanına malikdir. "Echo", həmçinin "Philips Hue Lamp" və ya "Google Nest" termostatı kimi üçüncü tərəfin İnternetə qoşulmuş cihazları ilə əlaqə saxlayır (18). "Amazon Echo" hazırda öz ətraf mühitinin daimi qeydi ilə məşğul olmur və bunun əvəzinə "Alexa" adını söyləməklə işə salınır, bundan sonra əmrlər bulud əsaslı serverdə qeyd olunur və daxil olur. Buna baxmayaraq, sistemin hazırkı tətbiqi onun istifadəçilərinin, xüsusən də uşaqların hüquqları və məlumat təhlükəsizliyi ilə bağlı ciddi suallar doğurur. Bundan əlavə, "Alexa"nın həmişə açıq təbiəti onu cihazın daxili mikrofonundan xüsusi müşahidə cihazı kimi istifadə edə bilən hakerlərə (və ya hətta istifadəçilərin ailə üzvlərinə) qarşı həssas edir.

"Echo" şəxsi cihaz deyil, ailə cihazıdır. Evdə hər kəs ondan istifadə edə bilər. Buraya telefon və ya veb-saytdan istifadə edən böyüklərdən fərqli olaraq, konfidensiallıqlarının pozulmasına razılıq verə bilməyən yetkinlik yaşına çatmayanlar da daxildir. Başqa sözlə, istifadəçilər "Amazon"un konfidensiallığı məhdudlaşdıran xidmətinə həvəslə qoşula bilər, lakin bununla belə, onlar ev təsərrüfatlarının bütün sakinlərini dövlət və ya digər üçüncü tərəfin nəzarətinə potensial olaraq məruz qoyacaqlarından xəbərsiz ola bilərlər.

Bundan əlavə, məlum olduğu kimi, 2011-ci ildən BMT-nin İnsan Hüquqları Şurası tərəfindən yekdilliklə qəbul edildikdən sonra BMT-nin Rəhbər Prinsipləri şirkətlərə siyasətin insan hüquqlarına təsirinin nə ola biləcəyini anlamaq üçün siyasət hazırlamazdan əvvəl səy göstərməklə insan hüquqlarına hörmət etməyi tapşırmışdır (BMT Rəhbər Prinsip 17). Lakin müəlliflərin şərhinə görə, "Amazon" heç də bu öhdəliyinə tam riayət etmir. Birincisi, Əİ cihazları böyük miqdarda hesablama gücü tələb edir ki, onlar emal edilmək üçün məlumatları bulud əsaslı serverə ötürməklə əldə edirlər. Beləliklə, məlumatlar fiziki cihazınızı tərk edir və "Amazon S3"ə (Sadə Saxlama Xidməti) keçir. "Amazon"un konfidensiallıq siyasəti səhifəsində bu müştəri məlumatlarının "Amazon" serverlərində nə qədər qalacağı göstərilmir.

Digər tərəfdən, "Echo" qonaqları və məlumatlı razılıq verməyən digər insanların səslərini qeyd edə bilər. Xüsusən də "Echo" tez-tez əlaqəsiz söhbət zamanı "Alexa" tətik sözünü eşitdiyinə inandığına görə (sözsüz ki, Alec, Alex, Alexis və ya Lex bu baxımdan xüsusilə həssasdır) belə qeydiyyatı işə salacaqdır. "Amazon" indiyə qədər "Echo" istifadəçilərini bu cür hallardan xəbərdar etməmişdir. Bu baxımdan, "Google Home"un konfidensiallıq siyasəti daha qabaqcıl sayıla bilər. Çünki burada istifadəçilərə qonaqları olduqda "Google Home"u söndürmələrini və ya qonaqları cihaz və səslərinin yazıla biləcəyi barədə məlumatlandırmalarını yönləndirən tövsiyələri ehtiva edir (9).

"Echo"nun xidmətlərini genişləndirmək və təkmilləşdirmək üçün "Amazon" üçüncü tərəflərlə əməkdaşlıq etməlidir. Məsələn, siz "ridesharing" şirkəti olan "Uber"ə zəng etmək üçün "Alexa"dan istifadə etdiyiniz zaman bulud əsaslı məlumatlarınızın bir hissəsi "Uber" tərəfindən göndərilir və istifadə olunur. Bu, hakerlər üçüncü tərəf tərtibatçılarına qoşulmuş Əİ cihazlarına giriş əldə edə bildikləri halda, məlumatların əldə edilməsi və manipulyasiya edilməsi ilə bağlı potensial təhlükəsizlik riski yaradır. İnternet şəbəkəsinin həddən artıq yüklənməsini əhatə edən DDoS hücumları nəticədə məlumat ötürülməsinin dayandırılmasına səbəb olur. "Paypal", "Netflix", "Twitter" və "Spotify" kimi veb-saytlar üçün internet kəsilməsinə səbəb olan Dyn məlumat mərkəzinə edilən kiberhücum Əİ ilə bağlı belə bir pozulma halının bariz nümunəsidir (18). NPR-nin texnologiya müxbiri Aliah Seliuxun sözlərinə görə: Dyn deyir ki, onların məlumat mərkəzlərinə qarşı hücumlar internetə qoşulan müxtəlif cihazlarla əlaqəli on milyonlarla IP ünvanlarından qaynaqlanır. Məsələn, qapalı dövrəli TV kameraları, DVR-lər, marşrutlaşdırıcılar kimi əşyalar (11).

Bütün bunları nəzərə alaraq, "Amazon"un öz istifadəçilərinə üçüncü tərəflərin potensial təhlükələri barədə məlumat verməməsi və öz konfidensiallıq siyasətində - "Amazon"un bu cür məhsullar üçün heç bir məsuliyyəti və ya öhdəliyi yoxdur ifadəsi məsuliyyətdən kənar dayanması insan hüquq və azadlıqlarının qorunması baxımdan BMT-nin 17-ci Rəhbər Prinsipinə uyğun gəlmir.

İlk baxışdan adi cihaz kimi görünən ağıllı cihazlar bir çox zərərli proqramlar üçün münbit mənbə rolunu oynaya bilər. Hələ 2016-cı ilin iyun ayında "Akamai" çoxsaylı internet cihazlarını və ev internet marşrutlaşdırıcılarını hədəf alan zərərli proqram ştammını izləməyə başladığını bildirirdi (4). Bütün dünyada yayılmış "Mirai" adlı bu zərərli proqram 600.000 həssas Əİ cihazını yoluxdurmuşdu. Qurğuları pozmaq üçün "Mirai"nin ilkin versiyası yalnız 64 tanınmış sabit dəstdən istifadə edirdi. Bu hücum çox aşağı texnologiyalı olsa da, son dərəcə effektiv olduğunu sübut etdi. "Akamai"nin şərhinə görə, əgər daha çox şəbəkə əsas gigiyena qaydalarına əməl etsə idi (məsələn, etibarsız protokolların bloklanması) "Mirai" kimi botnetlərin yayılması üçün şərait olmazdı (13, p. 337).

2018-ci ilin may ayı ərzində ABŞ-ın Ticarət Departamentləri və Dövlət Təhlükəsizliyi Departamentləri birlikdə Prezidentə İnternet və Kommunikasiya Ekosisteminin Botnetlərə və Digər Avtomatlaşdırılmış Paylanmış Təhdidlərə Qarşı Dayanıqlığının Artırılmasına dair Hesabatı dərc etdilər. Hesabatda daha sonra qeyd edilir ki, botnetlərin təsirlərini sıfıra endirmək üçün həddən artıq gücə malik olan şəbəkə provayderləri kimi ənənəvi DDoS azaldılması üsulları botnetlərdən qorunmaq üçün nəzərdə tutulmuşdur. Orijinal "Mirai" variantı zəif cihaz parollarından istifadə edərək nisbətən sadə olsa da, daha mürəkkəb botnetlər vardır. Məsələn, "Reaper" botneti cihazların uzun siyahısından istifadə etmək üçün məlum kod zəifliklərindən istifadə edir və bu günə qədər görülən ən böyük DDoS hücumlarından biri nisbətən qaranlıq olan "MemCacheD" proqram təminatında yeni aşkar edilmiş boşluqdan istifadə edib. Bu nümunələr bu ölçüdə və əhatə dairəsində botnetlərin yaratdığı riskləri, həmçinin gözlənilən yeniliyi və gələcək hücumların artan miqyasını və mürəkkəbliyini açıq şəkildə nümayiş etdirir (20).

Əşyaların interneti kibertəhlükəsizliyi həssas edir ki, bu da əlaqəni ələ keçirmək, manipulyasiya etmək və ya bloklamaq istəyi ilə əlaqədardır. İT sahəsinin mütəxəssisləri hesab edirlər ki, bir çox hallarda İnternet bağlantıları növündən (WiFi, Bluetooth, mobil rabitə, peyk və ya mikrodalğalı soba) və ya buluda necə qoşulmasından asılı olmayaraq, Əİ proqramından məlumat axtarmaq, emal etmək və ya qəbul etmək üçün təyin edilmiş digər serverlər və xidmətlərdə aşkar edilmiş zəifliklər səbəbindən fərdi məlumatların təhlükəsizliyini qorumaq mümkün olmur. Belə zəifliklərə misal olaraq, sənədsiz protokollar, etibarsız protokollar, zəif şifrələr və ya arxa qapılar (qanuni istifadəçilərin autentifikasiyasından yayınmanın müxtəlif üsulları) daxildir(12, p. 157). Məhz belə problemlərin qarşısının alınması məqsədilə Əİ cihazlarından istifadə və məsuliyyətin müəyyən olunması konkret prinsiplərə əsaslanmalıdır. Ümumilikdə məlumatların emalı prinsipləri ilk mövqeni tutur ki, Əşyaların interneti fərdi məlumatları müvafiq qanunvericiliklə müəyyən edilmiş qaydalara uyğun emal edir. Məsələn, qanuni və ədalətli emal, adekvat, müvafiq və dəqiq məlumatların emalı qaydası, məlumatların təhlükəsizliyi və konfidensiallıq prinsipi həm beynəlxalq normalarda, həm də milli hüquq normalarında öz əksini tapmış imperativlərdir. Qanuni, ədalətli, şəffaf emal prinsipi məlumatların işlənməsinin qanunauyğunluq, vicdanlılıq çərçivəsində və prosedurların məqsədini, informasiyanın emalı mərhələlərini, məlumatın işlənmə mərhələsini və məlumatın işlənmə məqsədini bilməyə imkan verən qaydada həyata keçirilməsini tələb edən qaydanı təşkil edir. Bu birinci qaydanın təməl daşı emalla əlaqədar olan şəxsin razılığı ilə təmsil olunur. Razılıq olmadıqda, fərdi məlumatların emalı qadağandır, müstəsna hallar qanunla məhdud şəkildə qeyd olunur.

Bundan əlavə, daha konkret prinsiplər də qeyd olunmalıdır ki, onlara da riayət olunması insan hüquq və azadlıqlarının təminatı baxımdan zəruridir:

• Emal məqsədinin məhdudlaşdırılması prinsipi xüsusi, açıq və qanuni məqsədlər üçün aidiyyəti şəxslərin şəxsi məlumatlarının toplanmasını nəzərdə tutur.

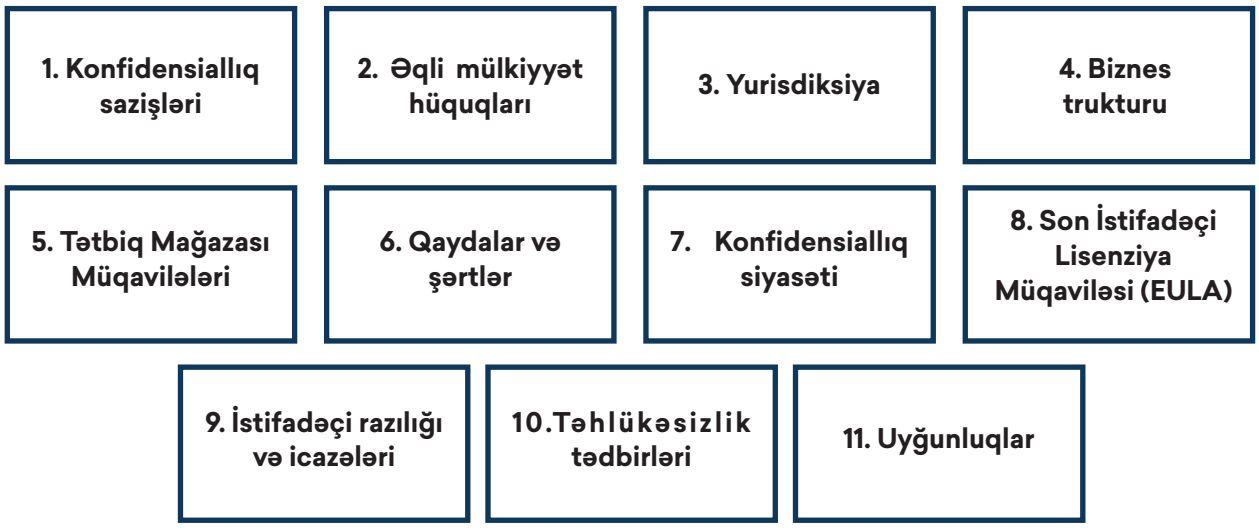
• Məlumatların minimuma endirilməsi prinsipi onların toplandığı məqsədlə məhdudlaşan adekvat, müvafiq məlumatların emalı qaydasını müəyyən edir.
• Məlumatların dəqiqliyi prinsipi məlumatların dəqiq işlənməsini tələb edir. Emal əməliyyatlarının obyekti olan məlumatların düzgünlüyünün şərti məsul şəxslərin yenilənmiş məlumatları emal etmək öhdəliyini doğurur.
• Məlumatın saxlanma müddətinin məhdudlaşdırılması prinsipi yalnız müəyyən edilmiş müddətə çata bilən emalın məqsədindən irəli gəlir. Emal əməliyyatlarının son anından sonra məlumatların anonimləşdirilməsi öhdəliyi işə düşür. Bununla da aidiyyəti şəxs müəyyən edilmir və ya müəyyən edilə bilməz.
• Məlumatların təhlükəsizliyi, tamlığı və konfidensiallığı prinsipi məlumat subyektinin emal üçün müxtəlif qurumlara etibar etdiyi (və ya işin razılığı olmadan həyata keçirilən) məlumatların icazəsiz girişdən, yayınmalardan təhlükəsiz olmasının təmin edilməsini nəzərdə tutur.

Beləliklə, texnologiyaya çıxış və ona nəzarət etmək güc sahibi olmaq kimi qiymətləndirilir və bu gün yüksək texnologiya və məlumatlara çıxış siyasi, iqtisadi və hərbi üstünlük deməkdir. Siyasi gücün Əİ vasitəsilə texnologiyada daha çox cəmləşəcəyi və ərazinin özündən daha az asılı olacağı ehtimal olunur (15, p. 269). Sivilizasiyanın əsasını maşınlara həvalə etmişik deyən Qudmanın fikirləri ilə (8, p. 39) razılaşsaq, texnologiyanın hara getdiyini və bunun bir sıra sosial məsələlər və münasibətlər üçün nə demək olduğunu başa düşmək üçün yaxşı təchiz edilmiş və ya təlim keçmiş mütəxəssislər komandasına ehtiyac vardır.

1.3. Mobil tətbiqlərin istifadəsi üzrə əsas hüquqi istiqamətlər

Mobil proqramlar və ya tətbiqlər smartfonlar və ya planşetlər kimi mobil cihazlarda işləmək üçün hazırlanmış və yerləşdirilən proqramlardır. Mobil proqram ekosistemi xüsusilə mürəkkəbdir, bir çox müxtəlif tərəflər mobil cihazda proqramın işlənib hazırlanmasında və yerləşdirilməsində iştirak edir. Bunlara proqram tərtibatçıları, proqram təminatçıları, əməliyyat sistemi istehsalçıları, cihaz istehsalçıları, mobil proqram tərtibatçılarının öz proqramlarına inteqrasiya etdiyi proqram təminatını təmin edən üçüncü tərəf xidmət təminatçıları, eləcə də bulud xidməti təminatçıları daxildir (3).

Peeyush Singh mobil tətbiqlərin inkişafı zamanı nəzərə alınmalı 11 hüquqi aspekti müəyyənləşdirmişdir (19):



Sual yaranır: Bəs hüquqi tələblər dedikdə, hansı əsaslar nəzərdə tutulur? – Bura həm mobil tətbiqin sahəsindən asılı olaraq mövcud normalar (məsələn, səhiyyəyə dair tətbiqlər üçün beynəlxalq səhiyyə hüququnun müddəaları), həm də hər bir halda verilənlərin qorunması məsələsi gündəmdə olduğu üçün bununla bağlı beynəlxalq-hüquqi mətnlər daxildir. Xüsusilə qeyd etməliyik ki, mobil proqramların hazırlanması sahəsində Ümumi Məlumatların Qorunması Qaydasına (GDPR) uyğunluq təkcə hüquqi zərurət deyil, həm də istifadəçi etibarının və məlumat təhlükəsizliyinin təməl daşıdır. Tətbiq tərtibatçıları fərdi məlumatların necə toplandığını, işlənməsini və saxlanmasını tənzimləyən tələblərin mürəkkəb mənzərəsini idarə etməlidirlər. GDPR-nin təsiri dərindir, ilkin dizayndan tutmuş mobil tətbiqetmənin gündəlik əməliyyatlarına qədər bütün proseslərə təsir edir:

1. Məlumatların minimuma endirilməsi: Tərtibatçılar yalnız proqramın funksionallığı üçün ciddi şəkildə zəruri olan məlumatları toplamalıdırlar.
2. Razılıq: İstifadəçilərin məlumatlarını emal etməzdən əvvəl onlardan açıq razılıq almaq vacibdir. Məsələn, dil öyrənmə proqramı istifadəçilərdən nitqin tanınması funksiyaları üçün mikrofonlarının istifadəsinə razılıq vermələrini xahiş etməlidir.
3. Şəffaflıq: Məlumat istifadəsi siyasətləri ilə bağlı aydın ünsiyyət vacibdir. Elektron ticarət proqramı fərdiləşdirilmiş tövsiyələr üçün müştəri məlumatlarının necə istifadə edildiyini açıqlamalıdır.
4. Verilənlərlə bağlı subyektiv hüquqlar: İstifadəçilər öz məlumatlarına daxil olmaq, düzəltmək və silmək hüququna malikdirlər. Sosial media proqramı istifadəçilərə məlumatlarını idarə etmək üçün asan alətlər təqdim etməlidir.
5. Dizayn üzrə məlumatların qorunması: Təhlükəsizlik tədbirləri proqrama sıfırdan inteqrasiya edilməlidir. Məsələn, mesajlaşma proqramı bütün prosesi əhatə edən (end-to-end) şifrələməni həyata keçirməlidir.
6. Məlumatların təhlükəsizliyinin pozulması barədə bildiriş: Məlumatların təhlükəsizliyinin pozulması halında tərtibatçılardan səlahiyyətlilərə və təsirə məruz qalan istifadəçilərə dərhal məlumat vermələri tələb olunur.
7. Transsərhəd məlumat ötürülməsi: Məlumatların ötürülməsi zamanı əlavə təminatlara ehtiyac vardır. Bulud saxlama proqramı müxtəlif ölkələrdə yerləşən serverlərdə saxlanılan məlumatların adekvat qorunmasını təmin etməlidir.

Bu müddəalara riayət etməklə proqram tərtibatçıları nəinki hüquqauyğun fəaliyyət göstərirlər, həm də başlanğıc ekosistemində rəqabət üstünlüyünə çevrilə bilən istifadəçi məlumatlarını qorumaq öhdəliyini nümayiş etdirirlər (16).

Mobil proqramlardan istifadə vasitəsilə fərdlər üçün konfidensiallıq və məlumatların qorunması risklərini qiymətləndirərkən, emalın baş verdiyi konteksti anlamaq risk mənbələrini, emalın fərdə potensial təsirini və azaldılmasının həyata keçirilməsinə dair məhdudiyyətləri müəyyən etmək üçün vacibdir. Proqramlar xüsusi funksionallıq təmin etmək üçün yaradıla bilər (məsələn, oyun və ya fitnes proqramları), lakin üçüncü tərəf xidmətlərini də birləşdirə bilər. Bunlar istifadəçilərə oyun xalları və ya gündəlik məşq fəaliyyəti kimi məlumatlarını paylaşmağa imkan verən sosial şəbəkə xüsusiyyətləri ola bilər. Tətbiq tərtibatçıları və üçüncü tərəf xidmət təminatçıları arasında potensial məlumat mübadiləsi səbəbindən proqram sosial şəbəkə funksiyasını və ya üçüncü tərəfin reklam xidmətlərini birləşdirdikdə daha yüksək məlumatların qorunması və konfidensiallıq riskləri ola bilər. Bundan əlavə, bəzi yurisdiksiyalarda yetkinlik yaşına çatmayanların məlumatlarının işlənməsi üçün daha sərt məlumatların qorunması qaydaları olduğu üçün proqram uşaqlara deyil, böyüklərə yönələrsə, onlara ünvanlanmış onların yaş qruplarına uyğun müxtəlif məlumatların qorunması riskləri yaranır.

Avropa İttifaqının Kibertəhlükəsizlik Agentliyinə (ENISA) görə, mobil proqramlarla bağlı iki əsas risk mənbəyi vardır: a) onların təbiəti, şəxsi mobil istifadəçi cihazlarında (əl cihazları) işləyən proqram təminatına malik olması və b) mobil inkişaf və paylama mühitinin xüsusiyyətləri (7).

Əİ cihazları fərdi istifadəçilər üçün risk yarada biləcək bir sıra xüsusiyyətlərə malikdir. ENISA hesab edir ki, bunlar müxtəlif şəxsi və ya həssas məlumatların toplanmasına imkan verən bir sıra sensorlarla təchiz edilmiş cihazlara aid ola bilər. ENISA-nın məlumatına görə, bu cihazlar demək olar ki, həmişə aktivdir və müxtəlif identifikatorları, o cümlədən cihaz ID, metadata və geolokasiya məlumatlarını ehtiva edir ki, bu da cihazın və fərdi istifadəçilərin müxtəlif cihazlar və ya proqramlarda izlənilməsini təmin edə bilər (7).

Mobil tətbiqlərin həyata keçirilməsinin müxtəlif yolları var:

• Spesifik (native) tətbiqlər. Bu proqramlar tətbiq bazarı (tətbiq mağazası), məsələn, "Google Play" vasitəsilə quraşdırılır və xüsusi platforma (məsələn: Android, Windows telefonu və ya iOS) üçün hazırlanır. Bu cür proqramlar GPS, akselerometr, kamera, bildiriş sistemi və s. daxil olmaqla, bütün cihaz imkanlarından istifadə edə bilər.

• Veb tətbiqlər. Veb tətbiqlər adətən brauzerdə işləyir və adətən HTML5-də yazılır. Onlara brauzerdəki veb-səhifələr kimi daxil olmaq olar və onlar istifadəçi cihazında işə salınan hər cür yeniləmədən azaddır. Bu tətbiqlərdən bəzilərində səhifəyə əlfəcin yaradaraq əsas ekrana ikona əlavə etmək imkanı var.

• Hibrid tətbiqləri. Bu tətbiqlər spesifik və veb tətbiqinin birləşməsindən yaranır. Hibrid proqramlar veb tətbiqləri ilə eyni şəkildə işləyir, lakin native proqramlar kimi cihaza endirilir. Veb proqramları kimi tərtibatçılar, adətən HTML5, CSS və JavaScript-də hibrid proqramlar yazır. Hibrid proqramlar bir konteyner daxilində kod işlədir. Cihazın brauzer mühərriki cihaza məxsus avadanlıqlara daxil olmaq üçün HTML, "JavaScript" və yerli API-ləri təqdim edir. Hibrid proqram, adətən veb tətbiqi kimi oxşar naviqasiya elementlərini paylaşsa da, tətbiqin oflayn işləyə bilməyəcəyi onun funksionallığından asılıdır. Əgər proqram verilənlər bazasından dəstəyə ehtiyac duymursa, tərtibatçılar onu oflayn rejimdə işlədə bilərlər.

Proqramın tipologiyası konfidensiallıq və təhlükəsizlik tələblərinin necə həyata keçirildiyinə birbaşa təsir göstərə bilər. Avtomatik olaraq yaradılan tətbiqlərin sayı getdikcə artır. Müxtəlif növ proqramların konfidensiallıq və məlumatların qorunmasına təsirləri ilə bağlı əlavə tədqiqatlar proqram tərtibatçıları üçün dəqiq tövsiyələrin hazırlanması üçün mühüm əsas verəcəkdir.

1.4.Nəticə

Virtual məkanın müasir inkişaf tendensiyalarından biri də Əşyaların internetinin formalaşmasıdır. Elm və texnika o qədər sürətlə inkişaf edir ki, artıq virtual məkanda insanlar arasında deyil, əşyalar arasında qarşılıqlı əlaqə yaradılır və bu əlaqə bir çox hallarda insanların faydası üçün yaradılmış olsa belə, onların hüquqlarının pozulması və buna qarşı mübarizə mövzusunu gündəmə gətirir. Əşyaların internetinin yaranması və ağıllı obyektlər tərəfindən yaradılan məlumatların emalının qabaqcıl texnoloji imkanları ilə yeni iqtisadi dəyərlər formalaşdırılır. Lakin bu, o demək deyil ki, bu hadisələr avtomatik olaraq yeni qanunvericiliyin qəbulunu tələb edir. Sadəcə olaraq, Əşyaların internetinin meydana gətirdiyi insan hüquq və azadlıqları üçün təhlükələrin qarşısının alınması tədbirləri gücləndirilməlidir. Məsələn, fərdi məlumatların qorunması ənənəvi olaraq qəbul olunmuş bir hüquqdur. Əşyaların internetinin geniş formada tətbiqi bu hüququn qorunması üçün müasir tədbirlərin işlənib hazırlanmasını zəruri edir. Tədqiqat zamanı konkret ağıllı əşyalar (məsələn, Echo) üzərində müxtəlif hüquq və azadlıqların pozulması halları təhlil olunmuş və bununla bağlı təcrübi təkliflər təqdim olunmuşdur. Belə təkliflərdən ən başlıcası ağıllı əşyaları istehsal edən şirkətlərin konfidensiallıq siyasətlərinin təkmilləşdirilməsi və istifadəçilərin mövcud və gözlənilən təhlükələr barədə öncədən məlumatlandırılması ilə bağlıdır.

Mobil tətbiqlərdən istifadə zamanı müvafiq sənaye standartlarına və qaydalara əməl etmək zəruridir. Çünki əsas standartlara əməl edilməməsi hüquqi sanksiyalar və işgüzar nüfuzun zədələnməsi ilə nəticələnə bilər. Həmçinin süni intellekt texnologiyalarının tətbiqlərdə artan inteqrasiyası ilə etik istifadəni, məlumatların konfidensiallığını və qərar qəbul etmə proseslərində ədaləti təmin etmək üçün süni intellektlə bağlı qaydalara riayət etmək də məcburi hala gəlmişdir.

Qanunauyğunluğun təmin edilməsi və etik mülahizələrin həlli sərfəli proqram hazırlamaq istəyən şirkətlər üçün çox vacibdir. Hüquqi tələblərə riayət etmək hüquqi riskləri minimuma endirmək və əqli mülkiyyət hüquqlarını qorumaq üçün vacibdir. "Appinventiv" (5) kimi mötəbər mobil proqram inkişaf etdirmə şirkəti ilə əməkdaşlıq hüquqi mürəkkəblikləri idarə etməyə kömək etməklə yanaşı, tətbiqin hazırlanmasında hüquqi məsələləri səmərəli şəkildə idarə edə bilər.

İstifadə olunmuş ədəbiyyat siyahısı:

1. Əşyaların interneti: əldə edilən təcrübə və perspektivlər. https://www.iktlab.az/article/esyalarin-interneti-elde-edilen-tecrube-ve-perspektivler
2. Gülnaz Rzayeva, Aytəkin İbrahimova. Süni intellekt, insan hüquqları və fərdi məlumatların təhlükəsizliyi. Dərs vəsaiti. Bakı: "Nurlar" nəşriyyatı, 2020, 211 s.
3. A guide to data protection in mobile applications. 2021. https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-guide-data-protection-mobile-apps.pdf
4. Akami Technologies, Inc., AKAMAI's [STATE OF THE INTERNET] / SECURITY: Q3 2016 REPORT 6 (Martin McKeay ed., 2016). https://www.akamai.com/us/en/multimedia/documents/ state-of-the-intemet/q3-2016-state-of-the-inteet-security-report.pdf [https://perma.ec/5NTL-397S]
5. Appinventiv. https://appinventiv.com/about/
6. Commission, Advancing the Internet of Things in Europe, SWD(2016) 110 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN
7. ENISA. Privacy and data protection. 2017. https://www.enisa.europa.eu/about-enisa/data-protection
8. Goodman, M. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World, New York: Anchor Books, 2016, 608 p.
9.Google, Guests & Google Home.
https://support.google.com/googlehome/answer/7177221?hl=en&ref_topic=7173611
10. IHS Economics & HIS Technology, 2017, The 5G Economy: How 5G Technology Will Contribute to the Global Economy, January. https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf
11. Internet of Things' Hacking Attack Led To Widespread Outage Of Popular Websites. NPR.org. http://www.npr.org/2016/10/22/498954197/internet-outage-update-internet-of-things-hackingattack-led-to-outage-of-popula
12. Jugastru, Calina. Internet of Things and the Protection of Personal Data // Acta Universitatis Lucian Blaga, 2017. Vol. 2017, No. 1, pp. 152-162.
13. Lawrence J. Trautman, Mohammed T. Hussein, Louis Ngamassi, Mason J. Molesky. Governance of the Internet of Things (IoT) // Jurimetrics, 2020, Vol. 60, No. 3, pp. 315-352.
14.Manwaring, K and Hall, C. Legal, social and human rights challenges of the Internet of Things in Australia. Input paper for the Horizon Scanning Project "The Internet of Things" on behalf of the Australian Council of Learned Academies, 2019, 29 p. file:///C:/Users/User/Downloads/SSRN-id3464277.pdf
15. Milivojevic, Sanja and Elizabeth Marie Radulski. The "Future Internet and Crime: Towards a Criminology of the Internet of Things. // CRIMEN: Casopis za Krivicne Nauke, 2020, No. 3, pp. 255-271.
16. Mobile legal and regulatory issues: GDPR and Mobile Apps: Ensuring Compliance in Your Startup. https://fastercapital.com/content/Mobile-legal-and-regulatory-issues--GDPR-and-Mobile-Apps--Ensuring-Compliance-in-Your-Startup.html
17. Nikolic, Igor. Competition Law and Policy for the Internet of Things // Union University Law School Review (Pravni Zapisi), 2022. Vol. 13, No. 1, pp. 16-53.

18. Pakzad, Roya. Amazon's Echo: The Adverse Human Rights Impact of the Internet of Things. https://www.academia.edu/32381714/Amazon_s_Echo_The_Adverse_Human_Rights_Impact_of_the_Internet_of_Things
19. Peeyush Singh. Top 11 Legal Issues to Consider to Protect Your App in 2024. https://appinventiv.com/blog/legal-issues-in-mobile-app-development/
20. U.S. DEP'T OF Commerce & U.S. Dep't of homeland sec., A report to the president on enhancing the resilience of the internet and communications ecosystem against botnets and other automated, distributed threats, 2018. https://csrc.nist.gov/ CSRC/media/Publications/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to -the-president/final/documents/eo_1 3800_botnetreport_-_fmalv2.pdf

Key legal issues related to the Internet of Things and the use of mobile applications

Abstract

In McLuhan's words, "We shape our tools, then our tools shape us, and as technology is used it causes change in society." Thus, the emergence of the Internet of Things and the increasing use of smart objects in people's daily lives, as well as the daily increase in the number of various mobile applications, require timely prevention of the threats that these new trends pose to human rights and freedom. At this time, it is especially important to clearly define the principles that must be followed when using these technologies and to develop safety mechanisms.

The article analyzes current legal problems based on specific facts, and also develops proposals and recommendations for their prevention.

Keywords: Internet of things, mobile applications, legal requirements, standards, human rights, smart objects.

Основные правовые вопросы, связанные с Интернетом вещей и использованием мобильных приложений

Аннотация

По словам МакЛюэна, - Мы формируем наши инструменты, затем наши инструменты формируют нас, а по мере использования технологий они вызывают изменения в обществе. Таким образом, формирование Интернета вещей и рост использования смарт-объектов в повседневной жизни людей, а также ежедневное увеличение количества различных мобильных приложений требуют своевременного предотвращения угроз, которые эти новые тенденции создают для прав человека и свободы. В настоящее время особенно важно точно определить круг принципов, которым необходимо следовать при применении этих технологий, и разработать механизмы безопасности.

В статье анализируются актуальные правовые проблемы на основе конкретных фактов, а также разрабатываются предложения и рекомендации по их предотвращению.

Ключевые слова: Интернет вещей, мобильные приложения, требования законодательства, стандарты, права человека, умные объекты.

Məqalənin redaksiyaya daxil olma tarixi: 07.05.2024
Çapa qəbul tarixi: 23.08.2024