FİZİKİ ŞƏXSLƏRİN İNFORMASİYA-HÜQUQİ MƏSULİYYƏTİ

Əlizadə Hüseyn Oktay oğlu,
Bakı Dövlət Universiteti Hüquq Fakültəsi İnsan hüquqları və informasiya hüququ UNESCO kafedrasının doktorantı.
e-mail:huseyn.alizade.95@bk.ru

Rəqəmsal dövrün tələbindən irəli gələrək, müxtəlif dövlətlərdə istifadə olunan yeni informasiya-hüquq pozuntularının milli hüquq sistemlərində tətbiq olunan normalar müstəvisində şərh olunması mümkün olmur. Çünki müqayisə zamanı mövcud normaların müəyyən etdiyi elementlər arasında uyğunsuzluq yaranır. Habelə, robotların elektron şəxsiyyət kimi tanınması reallığı fiziki şəxslərin hüquqi məsuliyyəti ilə bağlı tənzimləmələri dövrün aktuallığına çevirmişdir. Məqalədə qeyd olunan istiqamətlərdə tədqiqat aparılmış, hüquqi və praktiki təklif və tövsiyələr irəli sürülmüşdür.

Açar sözlər: informasiya hüquq pozuntusu, fiziki şəxs, informasiya-hüquqi məsuliyyət, robot, elektron şəxsiyyət, beynəlxalq tənzimetmə, milli hüquqi baza.

Qeyd edək ki, tədqiqat mövzusu aşağıdakı bəndlər üzrə aparılmışdır:

1. **"Eyniyyətin (şəxsiyyətin) oğurlanması" və informasiya-hüquqi məsuliyyət**

İnformasiya hüquq pozuntularına dair fiziki şəxslərin məsuliyyətinin müəyyən olunması üzrə əsas problem onların sürətlə yeni növlərinin meydana gəlməsidir. Hətta bir çox hallarda mövcud pozuntunun hansı növə aid ediləcəyi problem yaradır. Bununla bağlı, eyniyyətin oğurlanması xüsusi qeyd olunmalıdır. Bir şəxsin qeydə alınmış rəqəmsal şəxsiyyətindən başqa bir şəxs tərəfindən vicdansız şəkildə sui-istifadə etmək ədəbiyyatda "eyniyyətin (şəxsiyyətin) oğurlanması" (theft of identity) kimi adlandırılır. Ümumi dələduzluq cinayətlərindən fərqli olaraq, oğurluq həmin şəxsi cinayətin qurbanı olaraq təyin edir. Rəqəmsal eyniyyətin (şəxsiyyətin) oğurlanmasını dələduzluq saya bilmərik. Çünki dələduzluq bir sıra saxtakarlıq hərəkətlərinə tətbiq edilir və bir şəxsin rəqəmsal şəxsiyyətinin mənfəət və ya zərər əldə etmək məqsədilə vicdansız şəkildə istifadə edildiyi halda tətbiq olunur. Lakin qeyd etdiyimiz cinayətlər yalnız gəlir əldə etmək üçün törədilmir. Bunun əksinə çıxış edən Alex Steel oğurluğun obyektinə qeyri-maddi mülkiyyəti də daxil edərək genişləndirirməyin faydasız olduğunu vurğulayır və qeyri-maddi mülkiyyətdən sui-istifadə hallarının ən yaxşı şəkildə dələduzluq kimi qiymətləndirilməli olduğunu söyləyir.[12, p. 575]

Eyniyyətin (şəxsiyyətin) oğurlanması bir şəxsin qeydiyyatdan keçmiş tranzaksiya şəxsiyyətinin başqa bir şəxs tərəfindən qanunsuz olaraq istifadə edilməsidir. Misal olaraq, şəxsin bank kartının şifrəsinin ələ keçirilməsi, mail adresinin şifrəsinin ələ keçirilməsini göstərə bilərik. Deməli, rəqəmsal eyniyyətin (şəxsiyyətin) oğurlanması hər hansı bir şəxsə

məxsus olan fərdi məlumatların qanunsuz yolla əldə olunmasıdır. Əgər bu məlumatlar maliyyə vəsaitləri ilə bağlı olarsa, əməlin dələduzluq və ya oğurluq kimi tövsif olunması problemli məsələdir. Ənənəvi yanaşmaya nəzər salsaq, burada etibardan sui-istifadə etmə olmadığı üçün dələduzluq kimi qiymətləndirilməsi düzgün olmayacaqdır. Oğurluq gizli talamadır və burada törədilmə üsulunu qanunverici açıq qoymuşdur. Oğurluğun müasir üsullarla törədilməsi istisna olunmur. Lakin burada da bir çox tətbiqetmə çətinlikləri ola bilər. Əgər hər hansı bir kart məlumatları əldə olunubsa, talama obyektinin dəyərini müəyyən etmək mümkün olacaq. Mail adres və s. məlumatlarının əldə olunması başqa məqsədlərlə də icra oluna bilir. Belə olduğu halda, əməlin oğurluq kimi qiymətləndirilməsi nə dərəcədə düzgündür? – Rəqəmsal eyniyyətin (şəxsiyyətin) oğurluğunu oğurluğun bir növü kimi qəbul edən tədqiqatçılar məsələni mənimsəmə ilə əlaqələndirirlər. C.Sullivana görə, başqa bir şəxs tərəfindən sui-istifadə həmin şəxsi mülkiyyətindən həmişəlik məhrum etmək məqsədi ilə mənimsəmə deməkdir. Sui-istifadə fərdin eksklüziv istifadə və tranzaksiya şəxsiyyətinə nəzarət hüququnun nəzərə alınmamasıdır.[13, p. 108]Maraqlı cəhət ondadır ki, "eyniyyətin (şəxsiyyətin) oğurluğu" özü bir anlayış olaraq yanlış ifadədir. Çünki burada şəxs öz tranzaksiya şəxsiyyəti üzrə məlumatlardan tam məhrum edilmir. Oğurluq ənənəvi olaraq başqasının şəxsi əmlakını bu əmlakdan daimi olaraq məhrum etmək məqsədi ilə mənimsənilməsini nəzərdə tutur. Heç bir fiziki sənəd və ya bir şey almadan, bir şəxsin fərdi məlumatlarına qanunsuz daxil olmaq və istifadə etmək bu məlumatı istifadə etmək qabiliyyətindən məhrum etməyəcəkdir. Ona görə də şəxsi məlumatların mənimsənilməsi daimi məhrumiyyətə səbəb ola bilməz. Lakin əgər söhbət sırf tranzaksiya eyniyyətindən (şəxsiyyətindən), yəni maliyyə əməliyyatları üçün nəzərdə tutulan fərdi məlumatlardan gedirsə, bu zaman tövsif dəyişə bilər. Tranzaksiya eyniyyəti (The transaction ID) hər bir əməliyyatı təyin edən xüsusi nömrələr toplusudur. Onun köməyi ilə bank işçiləri müştəri tərəfindən edilən satınalmanı müəyyən edə bilər. Tranzaksiya eyniyyəti həmişə unikaldır, yəni eyni olan heç bir tranzaksiya eyniyyəti yoxdur. Bu əməliyyat açarı ümumiyyətlə sistemin uğurlu bir açar olaraq təyin etməsindən sonra yaranır. Tipik olaraq, açar rəqəmlərdən və hərflərdən ibarətdir (12-18 rəqəmli kod). Müştəri müəyyən bir ödəniş üçün axtarış etmək istəsə, tranzaksiya eyniyyəti lazımdır.[15]Beləliklə, tranzaksiya eyniyyəti hüquqi xarakter verən sxem altında xüsusi funksiyalara malikdir. Bu da bu eyniyyətin mülkiyyət olduğunu qəbul etmək, bir şəxsin zərər vurmaq niyyətində olduğu və ya ehtiyatsızlıq etdiyi hallarda cinayətdən zərər görmə cinayətinin sui-istifadə halında tətbiq edilməsinə imkan verir. İndi isə problemə öz milli hüquq sistemimiz aspektindən şərh verək. Eyniyyət oğurluğunun predmetini hər bir halda konkret şəxsə aid olan məlumatlar təşkil edir ki, bu məlumatlar informasiya sistemlərinə yerləşdirilmişdir. Respublikamızda bu cür məlumatlar hamısı fərdi məlumatlar adı altında birləşdirilmişdir. Deməli, eyniyyət oğurluğunun predmetini fərdi məlumatların bir növü təşkil edir. O ki qaldı bu cür fərdi məlumatların ələ keçirilməsi və

müxtəlif məqsədlər üçün istifadəsinə, oğurluq əmlakın gizli talanmasıdır. Burada şəxsin sonradan həmin əmlakı hansı məqsədlə istifadə edəcəyinin heç bir əhəmiyyəti yoxdur. Önəmli olan hər hansı bir şəxsə məxsus əmlakın qanunsuz ələ keçirilməsidir. Əgər fərdi məlumatlar qanunsuz yolla maddi gəlir əldə etmək və ya maddi ziyan vurmaq məqsədilə, yaxud da başqa qanunsuz əməliyyatın icrası üçün ələ keçirilirsə, bu cür əldə etmə hər bir halda oğurluq kimi qiymətləndirilə bilməz. Çünki əmlakdan tam məhrumetmə yoxdur. Yalnız maddi ziyan vurulduğu halda oğurluq olması mümkündür. Məsələn, şəxsin kart məlumatlarını ələ keçirən cinayətkar onlayn alış-veriş etmişdir. Əgər şəxs müxtəlif profil məlumatlarını əldə edib başqa şəxsi təhqir etmək üçün həmin profildən istifadə etmişdirsə, artıq burada oğurluqdan söhbət gedə bilməz. Bu zaman artıq CM-nin 272-ci maddəsində təsbit olunmuş qanunsuz ələ keçirmə əməli kimi qiymətləndirmə etmək lazımdır. Bu mövqeni ona görə təqdim edirik ki, oğurluq daha ağır sanksiya ilə cəzalandırılır. 272-ci maddənin isə sanksiyası nisbətən yüngül cəza nəzərdə tutmuşdur. Şəxsin fərdi məlumatlarını ələ keçirməklə onlayn qaydada onu talamaq bir qədər sərt cəzalandırılmalıdır. (272-ci maddənin özü də qüsurludur, bu barədə ətraflı aidiyyəti olan paraqraflarda şərh verilir).

Burada başqa bir problem ümumiyyətlə, eyniyyətin oğurluğunun predmeti ilə bağlıdır. Qeyd etdiyimiz kimi, milli qanunvericilik aspektindən bu predmeti fərdi məlumatlar təşkil edir. Məhz hansı fərdi məlumat növündən söhbət getməsi qaranlıq qalır. Məsələn, giriş şifrəsini fərdi məlumatların "İnformasiya əldə etmək haqqında" Qanunun 38-ci maddəsinin hansı bəndinə aid edə bilərik? Ümumiyyətlə, şəxsi eyniləşdirməyə imkan verən məlumatların konkret dairəsi necə müəyyən oluna bilər? – "Fərdi məlumatlar haqqında" Qanuna əsasən, müəyyən mənada fərdi identifikasiya nömrəsinə istinad edək. Vahid təkrarolunmaz kod olan bu FİN bütün eyniləşdirmə məlumatlarını ehtiva edirmi? Azərbaycan Respublikası Nazirlər Kabinetinin 4 aprel 2011-ci il tarixli 49 nömrəli qərarı ilə təsdiq edilmiş "Fərdi məlumatların informasiya sistemlərinə fərdi identifikasiya nömrəsinin daxil edilməsi və istifadə olunması Qaydaları"nın 2-ci bəndində göstərilən siyahı heç də tam deyil. Məsələn, burada ümumvətəndaşlıq pasportu və ya sürücülük vəsiqəsi kimi digər eyniləşdirici sənədlərlə bağlı məlumatlar daxil edilməmişdir. Hesab edirik ki, ümumi redaktələrin edilməsi və FİN-ə daxil olan məlumatların dairəsinin konkretləşdirilməsi lazımdır.

Əmələn maddi tərəfinə gəldikdə isə, AR CM-nin 177-ci maddəsinə 2013-cü ildə edilmiş dəyişikliyə əsasən, oğurluğun İKT-dən istifadə etməklə törədilməsi tövsifedici hal kimi nəzərdə tutulmuşdur. İlk olaraq onu qeyd edək ki, bu halın ağırlaşdırıcı hal kimi qəbul edilməsi özü mübahisəlidir. Çünki rəqəmsal əsrdə informasiya cəmiyyətinin əksər üzvləri üçün İKT-dən istifadə və onun imkanlarından müxtəlif məqsədlər üçün istifadə çox asan bir haldır. Ona görə İKT-dən istifadə sadəcə olaraq oğurluğun bir üsulu qismində tanınsa, daha yaxşı olar. Başqa bir məsələ isə verilənlərin oğurlanmasının oğurluq kimi tövsif olunub-olunmamasındadır. AR Ali Məhkəməsinin şərhinə görə, əsas məqam

varlanma ilə bağlıdır. Əgər informasiya sistemlərinə daxil olmaqla, pul vəsaiti ələ keçirilirsə, artıq dələduzluq deyil, oğurluğa və müvafiq kibercinayət əməlinə (maddə 271 və ya maddə 273) görə məsuliyyət yaranacaqdır.[1]Bəs sadəcə informasiya sistemlərinə daxil olmaqla verilənlər ələ keçirilərsə və başqa qeyri-qanuni məqsədlər üçün istifadə olunarsa, həmin verilənlərin əldə olunması oğurluq sayılacaqmı? – Ali Məhkəməyə istinadən xeyr. Bu yanaşmanı düzgün hesab edirik. Çünki oğurluğun əsas məsədi varlanmadır. Şəxsin başqa qeyri-qanuni məqsədlərlə eyniyyəti oğurlaması oğurluğun ənənəvi məzmununa uyğun gəlmir. Bu halda həmin qeyri-qanuni məqsədin kriminallaşdırıldığı əmələ və müvafiq kibercinayət maddəsinə görə məsuliyyət yaranacaqdır.

2. Fiziki şəxslərin informasiya-hüquqi məsuliyyətinin müəyyən olunmasında İKT-nin rolu

Fiziki şəxslərin hüquqi məsuliyyətinin müəyyən olunmasında əsas etibarilə İKT-nin özünün istifadəsi nəticəsində uğurlu nəticələr əldə etmək olur. Bir təcrübi misala baxaq: Dennis Rader 1974-1991 illəri arasında Kanzas ştatının (ABŞ) Vikita şəhərində 10 cinayət törətmişdir. Cinayətlərdə polisin əlində olan yeganə dəlil cinayət yerində tapılan taxta lövhələrdə (BTK - Bind, Torture and Kill, yəni Bağla, İşgəncə et və Öldür) həkk olunmuş imzası və DNT nümunələridir. Ancaq illərlə davam edən araşdırma nəticəsində heç bir nəticə əldə edilə bilməmişdir. BTK cinayətlərini törədərkən, eşidilməsini, məşhurlaşmasını, ancaq sirr olaraq qalmasını planlaşdırmışdı. Səssizliyini uzun müddət saxlasa da, müəyyən vaxtlarda Kanzasdakı media qrupları ilə əlaqə saxlayır və özünə uyğun mesajlar verirdi. Bütün etdiklərinə baxmayaraq, tutulmadığı üçün BTK-nın bir müddət sonra hətta polis məmuru ola biləcəyi müzakirə edildi, hətta bir neçə polis şöbəsində bütün polislərin DNT nümunələri götürüldü və cinayətdən əldə edilənlərlə müqayisə edildi. Lakin bir nəticəyə gəlmək mümkün olmadı. Bütün bu araşdırmalar davam edərkən, BTK hələ də özünəməxsus bir oyun qururdu. 2005-ci ilin fevral ayında Vikita televiziya stansiyalarından biri olan KSAS-a bənövşəyi, şəffaf bir disket göndərildi. Diskdə 3*5 sm ölçüdə etiket var və içərisində yalnız "test.rtf" adlı bir mətn faylı yazılmışdı. Faylda "Disketdəki etiketi oxuyun!"[6]qeyd olunmuşdu. Əvvəlcə bunu anlaya bilməyən polis "Çöl Fırtınası" Əməliyyatında iştirak etmiş və 1998-ci ildən Vikita polis idarəsinin kibercinayətlər bölməsində çalışan keçmiş əsgər 39 yaşlı Randi Stouna disketin rəqəmsal ekspertizası üçün müraciət etdi. Randi Stoun disketi və içindəki faylı araşdırdıqdan sonra, disketin Vikitanın Lüteran Kilsəsində istifadə edildiyini və əvvəlki istifadəçisinin "Dennis" adlı bir adla daxil olduğunu aşkar etdi. O, dərhal Vikitanın Lüteran Kilsəsinin rəsmi saytına daxil olaraq oradakı işçilərin siyahısına baxdı. İşçilərdən birinin adının Dennis Rader olduğu müəyyən olundu. Dennis Rader dərhal tutuldu və DNT nümunələri cinayət yerindən götürülənlərlə uyğun gəldi.[11]Nəticədə otuz bir il ərzində həllini tapmayan iş təxminən on beş dəqiqədə həll edildi.[3, s. 153]

Fiziki şəxslərin informasiya-hüquqi məsuliyyəti də hüquqi şəxslər kimi sahəvi normalarla tənzimlənir. Hüquqi şəxslərdən fərqli

olaraq, fiziki şəxslər istifadəçi qismində məsuliyyət daşıyırlar. Qısa sözlə desək, informasiya sistemlərinin işləməsi və onlarda toplanan verilənlərin mühafizəsi üçün informasiya sahibləri və ya mülkiyyətçilər məsuliyyət daşıyırsa, həmin sistemlərdən əldə olunan informasiyadan istifadəyə görə istifadəçilər məsuldurlar. Belə məsuliyyətin təyin olunmasında əsas məqsəd digər şəxslərin hüquq və azadlıqlarının qorunmasından ibarətdir. Çünki əksər hallarda açıq informasiya elan olunur və onun informasiya sistemində əldə edilməsinə ehtiyac qalmır. İnformasiya sorğusu əsasən mühafizə olunan məlumatlar üçün verilir. Şəxs əldə etdiyi həmin informasiyanı icazəsiz açıqlayarsa və ya bundan başqa məqsədlər üçün istifadə edərsə, müvafiq məsuliyyət yaranacaqdır. Problem ondadır ki, informasiya ehtiyatlarından istifadə qaydalarını pozma xətasının (İXM 371-maddə) cinayət ekvivalenti nəzərdə tutulmamışdır. İnformasiyanı əldə edən şəxsin həmin informasiyadan istifadə qaydalarını pozma verilənlər əleyhinə cinayətlərin heç birinə aid edilə bilməz. Deməli, qanunverici əldə olunmuş informasiyanın məzmunundan asılı olaraq, ictimai təhlükəliliyi müəyyən etmiş və müxtəlif sirlərin yayılmasına görə cinayət məsuliyyəti nəzərdə tutmuşdur. Məsələn, vəkillik fəaliyyəti ilə məşğul olan şəxs öz müştərisinin boşanma işi üzrə qarşı tərəfin əmlakı barədə müvafiq orqana sorğu ilə müraciət etmişdir. Mülkiyyətə dair məlumatlar fərdi məlumat sayıldığı üçün vəkil bu məlumatların özbaşına yayılmasına, açıqlanmasına yol verməməlidir. Bundan əlavə, hüquqi qaydada da müəyyən olunmuşdur ki, vəkilə öz peşə fəaliyyəti zamanı məlum olan məlumatların konfidensiallığını qorumalıdır və bu məlumatlar vəkil sirrini təşkil edir. Deməli, bu vəziyyətdə vəkilin fərdi məlumatları açıqlaması vəkil sirrinin yayılmasına görə məsuliyyət yaradır. Buna uyğun kriminallaşdırılmış əməl olmadığı üçün fərdi məlumatlara dair dispozisiyaya (156-cı maddənin 2.1-ci bəndi) istinad etmək lazımdır. Hüquqi ziddiyyətlər də elə buradan irəli gəlir. Müxtəlif konfidensial məlumatları təsnifləşdirən qanunverici həmin məlumatların yayılmasına görə məsul olan şəxslər üçün məsuliyyət differensiasiyasını etmir.

Lakin inzibati xətalar üzrə qayda fərqlidir. Burada sorğuçunun qulluq vəzifəsini bəhanə etməklə şəxsi məqsədlə informasiya əldə etməsi və ya qulluq vəzifəsinin icrası zamanı əldə etdiyi informasiyanı digər məqsədlər üçün istifadəsi inzibati məsuliyyəti formalaşdırır (AR İXM-in 374.4-cü maddəsi).

Fiziki şəxslərin informasiya-hüquqi məsuliyyətinin digər forması müxtəlif zərərli proqramların yayılmasına görə yaranır. Budapeşt Konvensiyasında (6-cı maddə) verilənlər əleyhinə cinayətlərin törədilməsi məqsədilə hazırlanmış istənilən qurğu, kompüter proqramları, informasiya sistemlərinə daxil olmaq üçün lazım olan şifrələr, kodlar və oxşar verilənlərə sahib olmaq, eləcə də onları istehsal etmək, satmaq, əldə etmək və başqa formalarda istifadəyə təqdim etmək cinayət kimi qəbul edilir. Lakin Azərbaycan Respublikasının Konvensiyanın ratifikasiyası zamanı verdiyi Qeyd-şərtdə bu cür əməllər yalnız o halda cinayət sayılır ki, ictimai təhlükəli nəticəyə, daha dəqiq desək, əhəmiyyətli zərərə səbəb olsun. Qalan hallarda belə pozuntular az əhəmiyyətli təhlükəyə malik ol-

duğundan digər hüquqi məsuliyyət növləri ilə cəzalandırıla bilər.

Cinayət Məcəlləsinə əlavə edilmiş 273-1-ci maddə qeyd olunan əməlin əhəmiyyətli zərərlə nəticələndiyi hallar üçün cinayət məsuliyyəti nəzərdə tutur. Lakin bu əməllər heç bir zərərə səbəb olmadığı formal tərkiblə AR İXM-də inzibati xəta kimi daxil edilməmişdir. Deməli, müxtəlif zərərli proqramı istehsal edən şəxs hələ onu aktivləşdirməmişdirsə, məsuliyyətdən söhbət gedə bilməz.

Eyni qaydaya müxtəlif xarici dövlətlərin təcrübəsində də rast gəlinir Məsələn, 2008-ci ildə Nanjing İctimai Təhlükəsizlik Bürosu (PSB) onlayn oyunlar oynayan kompüter istifadəçilərinin hesab məlumatlarını əldə etmək üçün hazırlanmış "Young Lady" adlı bir Troya atı proqramı hazırladığı, satdığı və ya istifadə etdiyi iddia edilən 10 şübhəli şəxsi tutdu. Nanjing PSB-yə görə, Troya atı proqramı Çin bazarında 40-dan çox məşhur onlayn oyun saytının istifadəçi hesabı məlumatlarını əldə etmək üçün istifadə edilmişdir.

Bu işdən sonra məhkəmələr tərəfindən oxşar işlərin sayı artdı. Məsələn, Jiangsu əyalətindəki Xuzhou məhkəməsi onlayn oyunların istifadəçi adlarını və şifrələrini oğurlamaq üçün hazırlanmış virusların yazılması və yayılmasındakı rollarına görə on bir nəfərə üç ilə qədər həbs cəzası vermişdi. Cinayətkarlara 833.000 RMB (121.980 ABŞ dolları) məbləğində cərimə də tətbiq olunmuşdu.[10]

Əgər hər hansı bir virus proqramı hələ heç bir zərərə səbəb olmayıbsa, hansı məsuliyyət formasının tətbiqi problemli məsələdir. Məsələn, COVİD-19 virusu ilə əlaqədar cəmiyyətdə yaranan "təlaş"dan istifadə edən bədniyyətlilər 2020-ci ildə CovidLock ransomware proqramını yaratmışlar. Bu proqram zərər çəkmiş faylları yoluxduraraq xəstəlik haqqında daha çox məlumat verməyi vəd edir. Problem ondadır ki, CovidLock quraşdırıldıqdan sonra Android cihazlarından olan məlumatları şifrələyir və zərərçəkənlərə məlumat girişini rədd edir.[7]

Beləliklə, hər bir halda zərərli proqramın hazırlanması və onunla bağlı əməliyyatlar əhəmiyyətli zərərə səbəb olduğu halda məsuliyyət yaradır. Məntiqi baxımdan da bu doğru yanaşmadır.

3. Süni intellekt və fərdi hüquqi məsuliyyət problemi

Son illərdə süni intellektin tətbiqi bununla hüquqi məsuliyyət məsələsini aktuallaşdırmışdır.

Əksər xarici dövlətlər süni intellektin tətbiqinə dair inkişaf planlarında və ya strategiyalarında məsuliyyətlə bağlı istiqamətləri rəhbər tuturlar. Məsələn, Almaniyanın Federal Hökumət üçün Milli Süni İntellekt Strategiyasında (2018) Süni intellektin məsuliyyətli inkişafı və istifadəsini qorumaq üç əsas məqsəddən birini təşkil edir, Danimarkanın Rəqəmsal İnkişaf (2018) və Süni İntellekt (2019) üzrə Milli Strategiyaları məsuliyyət prinsipini irəli sürülmüş altı prinsip sırasında nəzərdə tutur[2, s. 42] və s.

2017-ci ildən Avropa Parlamenti tərəfindən robotların "elektron şəxsiyyət" kimi tanınması, yəni "Robot texnikası üzrə mülki-hüquqi qaydalar üzrə Komissiyanın təkliflərinə dair Avropa Parlamentinin 16 Fevral 2017-ci il tarixli Qərarında[8]robotlar üçün konkret

hüquqi statusun yaradılması və onların məsuliyyətinin müəyyən olunması hüquqi tənzimetmənin yenidən işlənib hazırlanmasını bir daha tələb etdi.

Avropa Parlamenti bütün süni intellekt sistemlərinin deyil, yalnız aşağıdakı xüsusiyyətlərə malik olan ağıllı robotların elektron şəxsiyyət kimi tanınmasını təklif edir:

– sensorlar vasitəsilə və/və ya ətraf mühitlə məlumat mübadiləsi (əlaqələrarası), bu məlumatların dövriyyəsi və təhlili yolu ilə muxtariyyətin mövcudluğu;
– təcrübədən irəli gələn və qarşılıqlı təsir yolu ilə özünü öyrənmənin olması;
– çox az olsa belə, fiziki dəstəyin olması;
– davranış və hərəkətlərini ətraf mühitə uyğunlaşdırmaq bacarığının mövcudluğu;
– bioloji mənada həyatın olmaması.[8]

Akademik ədəbiyyatda, məsələn, hazırda süni intellekt sistemlərinin mülki məsuliyyəti üçün təklif olunan yeganə həll yolu heyvanların vurduğu ziyana bənzətməklə süni intellekt üçün ciddi məsuliyyət müddəalarını tətbiq etməkdir. Süni intellekt sistemləri üçün mülki məsuliyyətə ümumi yanaşma üçün təsirli və işlək bir həll axtarılarkən, heyvanlar üçün ciddi məsuliyyət haqqında milli müddəalar müzakirə üçün maraqlı bir zəmin yaradır.[14, p. 32]

Əsas nəzəri mövqeləri ümumiləşdirsək, həm xətaya əsaslanan, həm də ciddi məsuliyyət rejimi zərər risklərinin azaldılmasını nəzərdə tutsa da, təşviqetmə üçün ciddi problemlər yaradır. Belə ki, süni intellekt sistemlərinin istehsalı üzrə onlarda baş verən xətalara görə daha sərt məsuliyyət sistemi ilə mal və ya xidmət istehsalçıları və ya təchizatçılarının müştəriyə daha yüksək qayğı göstərməsinə nail olmaq olar. Amma belə sistem eyni zamanda fəaliyyət səviyyəsini aşağı sala və potensial olaraq yeniliyə mənfi təsir göstərə bilər. Bununla bağlı, "məsuliyyət innovasiyaların qarşısını alır" iddiası ilə çıxış edən əksər tədqiqatçılar sərt məsuliyyətə qarşı çıxırlar.[14, p. 36]

A.Gallaso və H.Luo bu arqumenti inkişaf etdirir və öz yanaşmalarını empirik sübutlarla dəstəkləyirlər. Son araşdırmalarında tibbi implantlar nümunəsi ilə məsuliyyət rejimlərinin innovasiyalara təsiri ilə bağlı məsələni xüsusi olaraq həll edən müəlliflərə görə, öhdəlik riski yenilik təşviqlərini soyutsa da, riskləri azaldan texnologiyaların inkişafına stimul verə, pis nəticənin olma ehtimalını azalda bilər. Beləliklə, Gallaso və Luo məsuliyyət qaydalarının müəyyən olunmasının mütləq yeniliyə mənfi təsir etmədiyi qənaətinə gəlirlər.[4]

Süni intellekt sistemlərinin tətbiqi üzrə hüquqi tənzimetmədəki problemləri şərh edən müəlliflər robotların hüquqi məsuliyyətinin tanınmasını qəti şəkildə qəbul etmirlər: Ənənəvi olaraq, cinayət könüllü cinayətkar hərəkət və ya hərəkətsizlik (actus reus) və cinayət etmək niyyəti (men rea) ilə törədilir. Robotların insanabənzər iradə sərbəstliyi və ya əxlaqi mənada zəngin bir düşüncəyə sahib olduğunu etiraf etsək, hüquqi tənzimetmədə köklü dəyişiklik etmək lazım olacaqdır.[2, s. 92-93]

Müəlliflərin yanaşması ilə tam razılaşmaq olar. Tramvay Yanaşması ilə bağlı şərhlər də bir daha təsdiq edir ki, robotların "mənə-

vilik" meyarına cavab verməsindən hələ söhbət gedə bilməz. 2017-ci ildə Həyatın Gələcəyi İnstitutunun (Future of Life Institute) təşkilatçılığı keçirilmiş Asilomar Konfransının nəticəsində qəbul olunmuş "Asilomar Süni İntellekt Prinsipləri"ndə də[9]məsuliyyət prinsipi elan olunmuşdur. Bu prinsipə əsasən, süni intellekt sistemlərinin qeyri-təyinati, qeyri-hüquqi məqsədlərlə istifadə olunması, süni intellektin tətbiqi nəticəsində yaranan hər hansı maddi və mənəvi zərərə görə istehsalçı şirkət, proqram təminatını həyata keçirən şirkət, mexanizmin sahibi və ya digər aidiyyəti üzrə subyektlər məsuliyyət daşıyırlar. Məsuliyyət həcmi ölçüləbilən olmalı, həddi əvvəlcədən müəyyən olunmalıdır.

4. Nəticə

İnformasiya-hüquq pozuntuları ilə mübarizə, həmçinin onların artma səbəblərinin də minimuma endirilməsi təqdirdə uğurla nəticələnə bilər. Bu səbəblər, bir tərəfdən kiberməkanın hüquqi və texniki tənzimlənməsində problemlərlə əlaqədardırsa, digər tərəfdən ayrı-ayrı şəxslərin məlumatlılıq səviyyəsinin aşağı olmasından asılıdır. Təbii ki, burada maarifləndirmənin də rolu əvəzsizdir. Hələ 2010-cu illərdə əksər alimlər ali təhsil müəsssisələrində informasiya təhlükəsizliyi və informasiya hüququ kimi fənlərin keçirilməsi zərurətindən bəhs edirdilər. Artıq 2015-ci ildən Hüquq fakültəsinin İnsan hüquqları və informasiya hüququ UNESCO kafedrasında "İnformasiya hüququ" magistr ixtisasının yaradılması, o cümlədən bakalavr pilləsində "İnformasiya hüququ", "Kibertəhlükəsizlik hüququ" kimi fənlərin tədrisi alqışalayiq haldır. Bununla belə, bu tədbirlərlə kifayətlənməməli, daha qabaqcıl və müasir ümumi yanaşmalar və əməkdaşlıq təmin edilməli, regionlarda da informasiya hüquqi biliklərin aşılanması üzrə tədbirlər həyata keçirilməlidir. Çünki kiberməkanda törədilən pozuntular hər gün və inkişaf edən informasiya texnologiyaları ilə yenilənir.

İnformasiya hüquq pozunutlarına görə məsuliyyətin təyin olunmasında mütləq şəkildə sanksiya kimi həbs (inzibati xəta) və ya azadlıqdan məhrumetmə (cinayət) tətbiq edilməsi məqsədəmüvafiq deyil. Əksinə, bu cür əməllərdə əgər böyük miqdarda maddi, fiziki və ya mənəvi ziyan vurulmamışdırsa, cərimə və alternativ başqa yeni cəzalar daha effektiv ola bilər. Məsələn, ABŞ-da "kompüterdən müəyyən müddətə istifadə etməmək" kimi cəzalar tətbiq olunur. Fikrimizcə, şəxsin törətdiyi infiormasiya-hüquq pozuntusuna görə onu azadlıqdan məhrum etmək əvəzinə cərimə etməklə və İKT-dən istifadəsinə qadağalar qoymaqla daha uğurlu nəticə əldə etmək olar.

Son dövrlərdə süni intellekt sistemlərindən istifadə, insanabənzər robotların hüquqi statusunun tanınması məsuliyyət məsələlərinin də tənzimlənməsini zəruri etmişdir. Hesab edirik ki, bu cür robotları fiziki şəxslərlə bərabər səviyyədə məsuliyyətə cəlb etmək nə nəzəri, nə də təcrübi baxımdan səmərəli ola bilməz. Bu, tədricən məsuliyyəti "robotların üzərinə qoymaqla" xaosla nəticələnəcəkdir. Ona görə də süni intellekt sistemlərinin törətdiyi pozuntulara görə məsuliyyət istehsalçının, satınalmadan sonra isə müvafiq müqavilə şərtlərinə uyğun olaraq alıcının üzərinə qoyulmalıdır.

İstifadə olunmuş ədəbiyyat:

1. "Dələduzluq cinayətlərinə dair işlər üzrə məhkəmə təcrübəsi haqqında" Azərbaycan Respublikası Ali Məhkəməsi Plenumunun Qərarı. 11 iyun 2015-ci il, bənd 16. http://supremecourt.gov.az/post/view/756
2. Gülnaz Rzayeva, Aytəkin İbrahimova. Süni intellekt, insan hüquqları və fərdi məlumatların təhlükəsizliyi. Dərs vəsaiti. Bakı: Nurlar, 2021,200 s.
3. Hüseyin Akarslan. Bilişim suçlari, bilişim yoluyla işlenen suçlar ve adli bilişim ayrimi. Yüksek Lisanz Tezi. Ankara, 2011, 184 s.
4. A.Galasso and H.Luo. Punishing Robots: Issues in the Economics of Tort Liability and Innovation in Artificial Intelligence. http://individual.utoronto.ca/galasso/research_files/Papers/GalassoLuo_Chapter_2018.pdf
5. Brenner SW. Distributed security: Moving away from reactive law enforcement // International Journal of Communication Law & Policy, 2005, No. 9, pp. 1-42
6. BTK killer sends message. https://www.history.com/this-day-in-history/btk-killer-sends-message
7. CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware. https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#
8. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html
9. Future of Life Institute 2017 Asilomar Conference. https://ai-ethics.com/2017/08/11/future-of-life-institute-2017-asilomar-conference/
10. Jihong Chen and Bing Cheng. The first "Trojan horse" case prosecuted in China. https://journals.sas.ac.uk/deeslr/article/download/1931/1868/
11. Reagan Brad. Computer Forensics: The New Fingerprinting. http://www. popularmechanics.com/technology/how-to/computer-security/2672751
12. Steel A. Intangible Property as Theft // Sydney Law Review, 2008, Volume 30 (4), pp. 575-614
13. Sullivan C. Digital Identity: An Emergent Legal Concept. University of Adelaide Press, 2011, 178 p.
14. Tatjana Evas. Civil liability regime for artificial intelligence: European added value assessment. EPRS, 2020, 220 p.
15. Transaction ID. https://ikajo.com/glossary/transaction-id

INFORMATION-LEGAL LIABILITY OF INDIVIDUALS

Alizade Huseyn Oktay oglu,
PhD student of the UNESCO Department of Human Rights and Information Law, Faculty of Law, Baku State University.
e-mail: huseyn.alizade.95@bk.ru

Due to the requirements of the digital age, it is impossible to interpret the new information-legal violations used in different countries in accordance with the norms applied in national legal systems. Because during the comparison there is a discrepancy between the elements defined by the existing norms. In addition, the reality of the recognition of robots as electronic entities has made the regulation of the legal liability of individuals relevant.

Research has been conducted in the areas mentioned in the article, and legal and practical suggestions and recommendations have been made.

Keywords: information offence, individual, information-legal responsibility, robot, electronic identity, international regulation, national legal framework.

ИНФОРМАЦИОННО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ ФИЗИЧЕСКИХ ЛИЦ

Ализаде Гусейн Октай оглы,
аспирант кафедры ЮНЕСКО по правам человека и информационному праву юридического факультета Бакинского государственного университета.
e-mail: huseyn.alizade.95@bk.ru

В связи с требованиями цифровой эпохи невозможно интерпретировать новые информационно-правовые нарушения, используемые в разных странах, в соответствии с нормами, применяемыми в национальных правовых системах. Потому что при сравнении есть несоответствие между элементами, определенными существующими нормами. Кроме того, признание роботов электронными объектами сделало актуальным регулирование юридической ответственности физических лиц. Проведены исследования по указанным в статье направлениям, даны правовые и практические предложения и рекомендации.

Ключевые слова: информационное нарушение, физическое лицо, информационно-правовая ответственность, робот, электронная идентификация, международное регулирование, национальная правовая база.

BİREYLERİN BİLGİ VE HUKUKİ SORUMLULUĞU

Alizade Hüseyin Oktay oğlu,
Bakü Devlet Üniversitesi Hukuk Fakültesi UNESCO
İnsan Hakları ve Bilgi Hukuku Bölümü doktora öğrencisi.
e-posta: huseyn.alizade.95@bk.ru

Dijital çağın gerekleri nedeniyle farklı ülkelerde kullanılan yeni bilgi-hukuk ihlallerini ulusal hukuk sistemlerinde uygulanan normlara göre yorumlamak mümkün değildir. Çünkü karşılaştırma sırasında mevcut normların tanımladığı unsurlar arasında bir farklılık vardır. Ayrıca robotların elektronik varlıklar olarak tanınması gerçeği, bireylerin hukuki sorumluluğunun düzenlenmesini de ilgili hale getirmiştir. Makalede belirtilen alanlarda araştırmalar yapılmış, yasal ve pratik öneriler ve önerilerde bulunulmuştur.

Anahtar kelimeler: bilgi ihlali, birey, bilgi-yasal sorumluluk, robot, elektronik kimlik, uluslararası düzenleme, ulusal yasal çerçeve.