İNFORMASİYA HÜQUQU

İNFORMASİYA HÜQUQ POZUNTULARI VƏ İNFORMASİYA-HÜQUQİ MƏSULİYYƏT: QARŞILIQLI ƏLAQƏLƏRİN NƏZƏRİ VƏ TƏCRÜBİ ASPEKTLƏRİ

Hüseyn Əlizadə*

Xülasə

Hal-hazırda əksər dövlətlərin qanunvericiliyi informasiya texnologiyaları sahəsindəki pozuntuların qiymətləndirilməsinə vahid yanaşmanın olmaması ilə xarakterizə olunur. Bundan əlavə, elmi-texniki tərəqqinin nailiyyətlərinin tətbiqi və istifadəsini tənzimləyən qanunvericiliyin mükəmməl olmaması, texnoloji tərəqqinin müxtəlif aspektlərinin hüquqi tənzimlənməsinə yanaşmalarda tənzimləyici bazanın bölünməsi ümumi hüquqi problem olaraq qalmaqda davam edir. Bu da informasiya hüquq pozuntularının artmasına və bir çox hallarda latent qalmasına gətirib çıxarır. Məqalədə informasiya-hüquq pozuntuları və informasiya-hüquqi məsuliyyətlə bağlı problemlərin hüquqi və təcrübi aspektdən təhlili aparılmış, təklif və tövsiyələr irəli sürülmüşdür.

Açar sözlər: *informasiya hüquq pozuntusu, beynəlxalq normalar, milli qanunvericilik, İKT, informasiya-hüquqi məsuliyyət.*

İnformasiya-hüquq pozuntularının aktual problem olaraq tədqiqatı informasiya cəmiyyətinin formalaşmasından sonra başlandı. Yarandığı ilkin dövrlərdə uğurlu nəticələr əldə olunacağı gözlənilən bu cəmiyyətdə müxtəlif neqativ halların mövcud olması da qaçılmaz idi. Hələ XX əsrin 50-ci illərində informasiyanı bizim və hisslərimizin ətraf mühitə qarşı uyğunlaşması prosesində əldə olunan məlumatlar kimi müəyyənləşdirən [6, s.31] informasiya nəzəriyyəsinin banisi Norbert Viner avtomatlaşdırma və İKT-nin tətbiqi üzrə təhlükələrin mövcudluğu ilə bağlı problemlər ortaya qoydu. Vinerin söylədiyi həmin təhlükələr zaman keçdikcə informasiya hüquq pozuntuları olaraq geniş yayılmağa başladı.

İnternet bu gün gündəlik həyatın ehtiyaclarına uyğun olaraq bütün sahələrə nüfuz etmiş və dünyanın hər yerindən insanları əlaqələndirmişdir. Bir-birinə vahid qlobal şəbəkə ilə bağlı olan müasir dünyada kiberməkanın mövcudluğu dövlətlərin hökmranlığını itirmək riski ilə yanaşı, konkret sərhədlərin də olması artıq mübahisəli bir fakta çevrilmişdir. Çünki mərkəzi idarəetmənin olmadığı bu sahədə sui-istifadə hallarının qarşısını almaq və ya onlarla mübarizə aparmaq çox çətindir və bir dövlətin tənzimləməsi kifayət etmir. Amnesty International-ın hesabatına görə, Google və Facebook şirkətləri əşyaların interneti texnologiyası və ağıllı şəhər dizaynı infrastrukturu olan ağıllı məişət texnikası vasitəsilə evlərimizdə vaxt keçirdiyimiz məkanları şəxsi bir məkana çevirirlər və bu yolla insanların fərdi məlumatlar toplanır. [5] Ona görə də informasiya hüququ pozuntularının qarşısının alınması yalnız bir istiqamətdən vacib deyil, həmçinin digər insan hüquqlarının təminatı üçün mühüm əhəmiyyət kəsb edir.

* Baku Dövlət Universitetinin Hüquq fakültəsinin İnsan hüquqları və informasiya hüququ UNESCO kafedrasının doktorantı

İKT-nin inkişafı nəticəsində meydana gələn kiberpozuntuların səbəb olduğu və ya ola biləcəyi ziyanın aşkar edə bilməməsi, keyfiyyət və kəmiyyət baxımından hesablanmayan məlumatların miqdarı kimi səbəblər informasiya hüquq pozuntularının artmasına səbəb olur. Lakin bunu statistik rəqəmlərdə görmək də çox çətindir. Çünki bir çox pozuntular hələ də kriminallaşdırılmadığı və yaxud aşkar edilməməsi səbəbindən latent qalır və rəsmi statistikada öz əksini tapmır. Bu səbəblərdən, informasiya hüquq pozuntuları kontekstində hüquqi tənzimləmələrin effektivliyi baxımından bir çox problemlər mövcuddur. Məsələ burasındadır ki, kiberməkanda törədilən əməllərin insan ölümü ilə nəticələnən hər hansı bir istintaq materialı və ya məhkəmə təcrübəsi ilə bağlı statistik məlumatlara rast gəlinmir. Heç bir dövlət informasiya müharibəsinə hüquqi anlayış verməmiş, rəsmi olaraq informasiya müharibəsi elan etməmiş və ya belə müharibəni dəstəklədiyini açıqlamamışdır. Lakin buna baxmayaraq, kiberməkanda günbəgün artan informasiya hüquq pozuntularının vurduğu ziyanın hesablanması hədsiz çətinliklər yaradır. Çünki bu cür pozuntular, xüsusilə də kibercinayətlər əksər hallarda bir şəxsə deyil, minlərlə, milyonlarla insana qarşı yönəlmiş olur. Burada ilk növbədə, müxtəlif kompüter və şəbəkələrin sıradan çıxmasına, məhvinə gətirib çıxaran əməllərin vurduğu iqtisadi ziyan qeyd olunmalıdır ki, bu ziyan hər il artan dinamika ilə dəyişir. Cybersecurity Ventures-in məlumatına görə, qlobal kibercinayətlər üzrə xərclərin 2015-ci ildə mövcud olmuş 3 trilyon ABŞ dollarından 2025-ci ilə qədər illik 10,5 trilyon ABŞ dollarına çatacağı, önümüzdəki beş il ərzində ildə 15 % artacağı gözlənilir. [3] Bu rəqəmlər vurulan və vurulacaq iqtisadi zərərin hansı səviyyədə böyük olacağını təsdiq edir. Həmçinin dövlət sirrini təşkil edən informasiya sistemlərinə qanunsuz daxil olmalar və s. bu kimi əməllər nəticə etibarilə müxtəlif dövlətlərə siyasi ziyan da vurmuş olur. Fərdi məlumatların oğurlanması ilə qeyri-qanuni yolla gəlir əldə olunmasına yönəlmiş müxtəlif informasiya hüquq pozuntuları bilavasitə insan hüquq və azadlıqlarına qəsd etdiyi üçün bu cür pozuntularla bağlı insan amili də ön plana çəkilməlidir. Qeyd olunan səbəblərdən, onların qarşısının alınması, məsuliyyət məsələsinin həlli aktual problem hesab olunur.

Hətta son dönəmdə Rəqəmsal İpək Yolunun çəkilişinə başlanılması özü də respublikamızda kiberməkanın hüquqi tənzimlənməsini, xüsusilə də informasiya hüquq pozuntularına görə məsuliyyət məsələlərinin hüquqi həllini zəruri edir. Region üzrə dövlətlərin internet bağlantısı tələbatının bu üsulla Azərbaycan vasitəsilə ödənilməsini nəzərdə tutan layihə respublikamızın kiberməkanda tranzit ölkəyə çevrilməsinə şərait yaradacaqdır.

Kibercinayətkarlıqla mübarizə hər zaman İKT şəbəkəsi istifadəçilərinin sayı, İnternetin transsərhəd xüsusiyyətləri və mərkəzləşdirilməmiş arxitekturası sayəsində kompleks bir məsələ olmuşdur. Həm ənənəvi, həm də yalnız onlayn fəaliyyət göstərən kiberməkanda mütəşəkkil cinayətkar qruplar qanunvericilərdən və hüquq-mühafizə orqanlarından bir neçə addım qabaqda qalırlar və ehtimal ki, qalmağa davam edəcəklər. Çünki kiberməkanda olan texnoloji yeni-

liklər heç də həmişə qanuni məqsədlər üçün istifadə olunmur. Hətta, 2019-cu ildə aparılmış hesablamalara görə, sorğuda iştirak edən mütəxəssislərin 69%-i internetdəki sui-istifadə hallarının, daha dəqiq desək informasiya hüquq pozuntularının artdığını qəti şəkildə təsdiq etmişdir. [4]

İnformasiya-hüquq pozuntuları ilə bağlı ziddiyyət bu pozuntuların ənənəvi şərhi ilə müasir izahı arasında mövcuddur. Ənənəvi olaraq, informasiya əsas etibarilə KİV və xəbərlərlə əlaqələndirildiyi üçün informasiya hüquq pozuntuları da bu kontekstdən şərh olunurdu. Müasir cəmiyyətdə kiberməkanın formalaşması informasiya hüquq pozuntularının yalnız bu məkanda törədildiyi və İKT ilə əlaqədar olduğu mövqeyini formalaşdırmışdır. Hesab edirik ki, belə dar yanaşma qəbul edilməyərək informasiya məkanının daha geniş anlayış olması məqbul sayılmalıdır. Çünki informasiya cəmiyyətində informasiya həyatımızın ayrılmaz hissəsinə çevrilmişdir. Belə olduğu halda, kibercinayətlərin özünün də dar mənada şərhi hüquqi baxımdan düzgün sayılmır. Kiberməkanda və İKT ilə əlaqəli pozuntuların fərqləndirilməsi bilavasitə obyektdən asılı olaraq müəyyən olunmalıdır ki, bu obyekti müxtəlif sistemlərdə qeydə alınmış informasiya, yəni verilənlər təşkil edir. Ona görə də respublikamızın cinayət qanunvericiliyində kibercinayətlərə aid sanksiyaların nəzərdə tutulduğu fəslin adını bir qədər uğursuz saymaq olar. Bu, Budapeşt Konvensiyası müstəvisində də qarışıqlıq yaradır. Konvensiya kibercinayətləri qüsurlu olsa da, geniş mənada qəbul edərək, kiberməkanda törədilən əməllər kimi qiymətləndirir. Fikrimizcə, Konvensiyanın belə mövqeyi kiberməkanda törədilən əməllərin transsərhəd xarakter daşıması və ümumilikdə onların yurisdiksiya məsələlərinin tənzimlənməsi üçün vahid beynəlxalq-hüquqi çərçivəyə ehtiyacın olmasından irəli gəlir. Lakin qeyd etdiyimiz fəsil bilavasitə verilənlərə qəsd edən əməlləri nəzərdə tutur. Ona görə də fəslin adının "Verilənlər (və yaxud da Kompüter verilənləri) əleyhinə cinayətlər" kimi adlandırmaq daha məqsədəuyğundur. Bir-birindən çox fərqli statusu olan cinayətlərin eyni sanksiya ilə cəzalandırılmasını tələb edəcəyi üçün bütün İKT-dən istifadə edilməklə törədilən bütün cinayətləri kibercinayət daxilində birləşdirmək düzgün olmazdı. Bundan əlavə, bu fərq qoyulmadıqda, kibercinayətlərin əhatə dairəsi o dərəcədə genişlənəcək ki, gələcəkdə təcrübə üçün çox böyük problemlər yaranacaqdır.

Ümumi olaraq, kibercinayətlərin anlayışı nə beynəlxalq, nə milli tənzimetmədə verilmədiyi səbəbi ilə hüquq ədəbiyyatında müxtəlif şərhlərin verilməsinə gətirib çıxarmışdır. Əksər tədqiqatçılar kibercinayətlər dedikdə, İKT-yə qəsd edən və İKT vasitəsilə törədilən əməlləri başa düşürlər. Lakin İKT vasitəsilə törədilən əməllərin də kibercinayət sayılması hüquq elminin ənənəvi baxışları üçün ciddi problemlərə gətirib çıxara bilər. İnformasiya sistemindən verilənlərin qanunsuz ələ keçirilməsi ilə kiberməkanda hər hansı bir şəxsin təhqir olunmasının eyni ad - kibercinayət altında birləşdirilməsi məntiqi və praktiki baxımdan düzgün deyil. Bu halı bir çox cinayətlərə tətbiq etmək olar. Ona görə də kibercinayət üçün ən vacib element qəsd obyekti götürülməlidir. Məsələn, bank məlumatlarını qanunsuz ələ keçirməklə talamanı kibercinayət kimi deyil, oğur-

luq kimi qiymətləndirmək lazımdır. Lakin əgər müvafiq əməli nəzərdə tutan dispozisiyada İKT-dən istifadə tərkib elementi kimi təsbit olunamışdırsa, o zaman əmələ cinayətlərin məcmusu kimi tövsif vermək lazım olacaqdır.

Fikrimizcə, bu məsələ BMT-nin Cinayətkarlığın qarşısının alınması və Cinayət Ədliyyəsi üzrə XIII Konqresində maraqlı və tutarlı əsaslandırma edilmişdir. Yeni cinayət formalarının müəyyənləşdirilməsi üzrə problemlərin, xüsusilə də terminologiya probleminin mövcudluğu qeyd olunur və "yeni yaranan cinayət formaları" ifadəsinə müraciət edilir. Kibercinayətlər də bu yeni cinayət formalarına daxil edilərək bildirilir ki, "kibercinayət" termini həm kompüter sistemlərinin və ya məlumatların cinayətin obyekti olduğu cinayətləri, həm də kompüter sistemləri və ya məlumatların cinayət vasitələrini təmsil etdiyi cinayətləri, məsələn şəxsiyyətlə əlaqəli cinayətin əksər formalarını əhatə edir. Yeni cinayət formaları yalnız yeni səbəb və ya cinayət üsullarını əhatə etmir, eyni zamanda aşkarlanması daha çətin ola biləcək yeni qurban növlərinə yönəldilə bilər. Kompüter zərərli proqramlarının paylanması kimi kibercinayətlər eyni zamanda çox sayda qurbana təsir edə bilər. Fərdi konkret qurbanın nümayiş etdirilməsini tələb edən cinayət ədalət sistemləri bu sahədə xüsusi çətinliklərlə üzləşə bilər. [2, s.4]

Nəticə

İnformasiya texnologiyaları sürətlə dəyişir və eyni zamanda informasiya sahəsində pozuntuların törədilmə üsulları, ümumilikdə təbiəti də dəyişir. Lakin qanunvericilik bu dəyişikliklərlə tam uyğunlaşa bilmir. Ona görə də informasiya sahəsində normalarda konkretliyə yol verilməməlidir ki, gələcək dəyişikliklərə cavab verə bilsin. "Kiberhücum", "kibermüharibə", "kibercasusluq", "kibercinayət" kimi anlayışların beynəlxalq səviyyədə qəbul edilmiş vahid tərifləri yoxdur. Eyni zamanda, dövlətlərin qəbul etdiyi jus cogens qaydaları kiberhüquq sahəsində yaradılmamışdır. Əslində, inkişaf etmiş ölkələrin internetdən asılılığının artması nəticəsində internetdəki çatışmazlıqlar düşmən dövlətlərin hücumları üçün uyğun bir mühit yaratmışdır. Belə ki, internetin yaratdığı təhlükəsizlik boşluqları səbəbindən inkişaf etmiş dövlətlər daha az inkişaf etmiş dövlətlərə qarşı müxtəlif kiberpozuntular icra edir. Beynəlxalq hüquq sahəsində tərifin olmamasının nəticələrindən biri də budur. Dövlətlərarası münaqişələrə səbəb ola biləcək kiberhücumların beynəlxalq hüquqda heç bir ekvivalentinin olmaması əhəmiyyətli bir çatışmazlıqdır.

Digər bir vacib problem kiberməkanda törədilən pozuntuların internetin transsərhəd təbiətindən irəli gələrək, yurisdiksiya məsələlərini aşması ilə bağlıdır. Ona görə də belə pozuntuların qarşısının alınması üçün mövcud qanunvericilik bazasının möhkəmləndirilməsi, köhnə beynəlxalq və milli normaların yenilənməsi və uyğunlaşdırılması ilə yanaşı, həm də milli səviyyədə sektorlararası əməkdaşlıq, həm də elektron mühitdə törədilən cinayətlərin aşkarlanması, istintaqı və qarşısının alınması sahəsində beynəlxalq əməkdaşlığın inkişafı tələb olunur. Burada kibermühitdə törədilən əməllərin mütəşəkkilliyi də nəzərə alınma-

lıdır. Bir çox dövlətlərdə mütəşəkkil kibercinayətkarların fəaliyyətlərinə cavab vermək üçün lazımi tənzimetmə mövcud deyil. Ona görə də problemin həlli qlobal səviyyədə mümkün ola bilər. Çünki İnternet şəbəkəsi qlobal bir şəbəkədir. Qlobal strategiyanın olmaması ilə yaxın gələcəkdə problemin daha da dərinləşməsi ehtimalı çox yüksəkdir. Bu baxımdan, problemi həll etməyin yolu həm milli, həm də beynəlxalq səviyyədə səylərin koordinasiyası və uyğunlaşdırılmasını ehtiva edən uzunmüddətli tədbirlər planının hazırlanması ola bilər.

İstinadlar:

1. Əliyev Ə.İ., Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S. İnformasiya hüququ. Dərslik. Bakı: Nurlar, 2019, 448 s.

2. Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime. Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, Doha, 12-19 April 2015, Working paper prepared by the Secretariat, 20 p.

3. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

4. Dan Jerker B. Svantesson. Internet & Jurisdiction Global Status Report 2019. https://digital-strategy.ec.europa.eu/en/library/internet-and-jurisdiction-global-status-report-2019

5. Surveillance giants: How the business model of google and facebook threatens human rights. https://www.amnesty.org/en/documents/pol30/1404/2019/en/

6. Винер Н. Кибернетика и общество. Москва: Изд-во иностранной литературы, 1958, 200 с.

ИНФОРМАЦИОННО-ПРАВОВЫЕ НАРУШЕНИЯ И ИНФОРМАЦИОННО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ: ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ВЗАИМООТНОШЕНИЯ

Гусейн Ализаде[*]

Резюме

В настоящее время в законодательстве большинства стран отсутствует единый подход к оценке нарушений в сфере информационных технологий. Кроме того, общей правовой проблемой остается несовершенство законодательства, регулирующего применение и использование достижений научно-технического прогресса, разделение нормативной базы на подходы к правовому регулированию различных аспектов технического прогресса. Это приводит к увеличению информационных нарушений и во многих случаях остается латентным. В статье анализируются проблемы, связанные с информационно-правовыми нарушениями и информационно-правовой ответственностью с юридической и практической точки зрения, даются предложения и рекомендации.

Ключевые слова: *информационно-правовые нарушения, международные нормы, национальное законодательство, ИКТ, информационно-правовая ответственность.*

[*] докторант Бакинского государственного университета

INFORMATION OFFENCES AND INFORMATION-LEGAL LIABILITY: THEORETICAL AND PRACTICAL ASPECTS RELATIONS

Huseyn Alizade*

Abstract

Currently, the legislation of most countries is characterized by a lack of a unified approach to the assessment of violations in the field of information technology. In addition, the imperfection of the legislation governing the application and use of the achievements of scientific and technological progress, the division of the regulatory framework in approaches to the legal regulation of various aspects of technological progress remain a common legal problem. This leads to an increase in information violations and in many cases remains latent. The article analyzes the problems related to information offences and information-legal responsibility from the legal and practical point of view, makes suggestions and recommendations.

Keywords: *information offence, international framework, national legislation, ICT, information-legal responsibility.*

* Ph.D Candidate, Baku State Universitety