HÜSEYN ƏLİZADƏ
Baku Dövlət Universitetinin Hüquq Fakültəsinin
İnsan hüquqları və informasiya
UNESCO kafedrasının doktorantı
huseyn.alizade.95@bk.ru

HÜQUQİ ŞƏXSLƏRİN İNFORMASİYA-HÜQUQİ MƏSULİYYƏTİ: AZƏRBAYCAN RESPUBLİKASINDA ELEKTRON İDARƏETMƏNİN FORMALAŞDIRILMASI VƏ İNFORMASİYA-HÜQUQİ MƏSULİYYƏT İNSTİTUTUNA YENİ YANAŞMA

Açar sözlər: informasiya-hüquqi məsuliyyət, informasiya hüquq pozuntusu, sanksiya, inzibati xəta, cinayət, delikt.

Ключевые слова: информационно-правовая ответственность, информационное нарушение, санкция, административное правонарушение, преступление, деликты.

Keywords: information-legal responsibility, information violation, sanction, administrative violation, crime, delict.

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.

Mövcud qanunvericilikdə informasiya texnologiyaları sahəsindəki pozuntuların qiymətləndirilməsinə vahid yanaşmanın olmaması, istifadə olunan konseptual aparatda birlik və nəticədə gözlənilən nəticəni verməyən uyğunsuz və sistemsiz dəyişikliklərin tətbiqi ilə xarakterizə olunur. Bundan əlavə, elmi və texnoloji 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. Məqalədə bu kimi problemlər təhlil olunmuş, təklif və tövsiyələr irəli sürülmüşdür.

İnformasiya-hüquq pozuntularının araşdırılması üzrə ən vacib məsələ pozuntunun həqiqətən də törədildiyini müəyyən etmək və məsuliyyəti tətbiq etməkdir. Hamımız "bir qanun olmalıdır" ifadəsini eşitmişik, lakin törədilmiş hərəkəti xüsusi olaraq təsvir edən bir qanun olmadıqda, bu hərəkət nə qədər "səhv" görünsə də, hüquqi məsuliyyət məsələsi açıq qalır. Kibercinayətlər üzrə hüquqi tənzimetmədə elementlər o qədər də dəqiq müəyyən edilməmişdir. Həyatımızı idarə edən kompleks qanunlar sistemini və bir-biri ilə necə qarşılıqlı əlaqədə olduğunu başa düşmək bu cinayətlərin aşkar edilməsi üçün vacibdir.

Ümumi anlamda, hüquqi məsuliyyət hüquq pozuntusunun törədilməsinə görə yaranır və dövlət məcburiyyəti xarakteri daşıyır, hüquqi qaydada müəyyən olunmuş sanksiyada ifadə olunur. Ənənəvi olaraq, hüquq pozuntularının xarakterindən asılı olaraq dörd növ – cinayət, inzibati, mülki və intizam məsuliyyəti fərqləndirilir. Lakin müasir dövrdə beynəlxalq-hüquqi məsuliyyət, konstitusiya-hüquqi məsuliyyət kimi anlayışlara

da rast gəlinir. Tədqiqat mövzusu çərçivəsində birinci təsnifata əsasən təhlil aparılcaqdır.

Ümumiyyətlə, informasiya hüquq pozuntularına dair təcrübədə kibercinayətlərə daha az diqqət yetirilir. Cinayət təqibləri və məhkumluqların artması ilə müqayisədə mülki məhkəmə proseslərində görünən artım demək olar ki, az müşahidə edilir. Məhz bundan çıxış edərək, bəzi müəlliflər (Jonatan Mayer) informasiya hüquq pozuntularının tənzimlənməsi üzrə gərəksizlik məsələsini gündəmə gətirirlər. Onların şərhinə görə, birincisi, bir kiber hüquq pozuntusu eyni qanuni sxem çərçivəsində digər kibercinayət əməlləri ilə üst-üstə düşərək daxili baxımdan artıq ola bilər. İkincisi, kiber hüquq pozuntular, həmçinin xaricdən artıq ola bilər və mülki iddialarla və ya cinayət ittihamları ilə üst-üstə düşə bilər [7, s. 1485-1486]. Deməli, J.Mayer daxili və xarici gərəksizlik problemini ayırır və öz mövqeyini ABŞ qanunvericiliyi (Kompüter dələduzluğu və sui-istifadəsi haqqında Akt) əsasında şərh edir: Məlumatların əldə olunması və dələduzluq cinayətləri tez-tez üst-üstə düşür, çünki məhkəmələr Kompüter dələduzluğu və sui-istifadəsi haqqında Aktın dələduzluq cinayətinin əsas elementlərini ön plana çəkirlər. Eyni zamanda, müxtəlif "zərər" iddiaları bir məlumat alma və ya bir dələduzluq iddiası ilə birləşdirilir. Bu, "zərər" anlayışının geniş şərh olunmaqla məlumatların surətinin çıxarılması və məzmununun dəyişdirilməsi əməliyyatlarını birlikdə əhatə etməsi təcrübəsi ilə bağlıdır. Həm də onu nəzərə almalıyıq ki, bu tip şikayətlər əksər hallarda dələduzluqla bağlı verilir, mobil telefonlarda kilidin açılması ilə məlumatların əldə olunması hallarına çox az rast gəlinir (13.65 %). Məsələnin mahiyyəti onunla bağlıdır ki, başqasının şifrəsinin əldə olunması və istifadəsi dələduzluq sayılır. Belə olduğu halda, şifrə ticarəti kimi cinayət dələduzluqla müqayisədə gərəksiz kimi görünür [7, s. 1485-1486]. Həqiqətən də bir çox hallarda informasiya hüquq pozuntuları digər cinayətlərin və ya mülki deliktlərin "kölgəsində" nəzərdən qaçırılmış olur.

İnformasiya-hüquq pozuntularına görə mülki-hüquqi məsuliyyət əksər hallarda hüquqi şəxslər arasında yaranmış mübahisələrdən doğur. Çünki fiziki şəxslər adətən, bir-birinə qarşı İKT-dən istifadə etməklə təhqir və böhtan əməllərinə yol verirlə və bu da kriminallaşdırılmışdır. Məsələn, 2021-ci il aprel ayının məlumatına görə, Google şirkəti Chrome-a qarşı 5 milyard dollar həcmində mülki iddia qaldırılmışdır. İddiaya görə, Google İncognito Rejimi gizli axtarış sessiyası zamanı istifadəçiləri izləmiş, yəni onların məlumatlarının toplanılması, müdaxiləsi kimi əməliyyatlarla konfidensiallıq qaydalarını pozmuşdur [3].

İnformasiya hüquqi məsuliyyətin fiziki və hüquqi şəxslər üzrə bölünməsi xüsusi praktiki əhəmiyyətə malikdir. Bu, tətbiq olunacaq müvafiq inzibati və ya cinayət sanksiyasının müəyyən olunmasında, eləcə də mülki mübahisənin həllində mühüm rol oynayır. İnformasiya cəmiyyətinin ilkin dövrlərində daha çox fiziki şəxslər informasiya hüquq pozuntularına meylli idilərsə, tədricən kriminal təşkilatlar İKT-nin təqdim etdiyi "rahat və münasib" imkanlardan istifadə etməyə başladılar. Nəticə etibarilə mütəşəkkil cinayətkarlığın bir növü olaraq kibercinayətkarlıq inkişafa başladı ki, bu da məsuliyyətin müəyyən olunmasına öz təsirini göstərir.

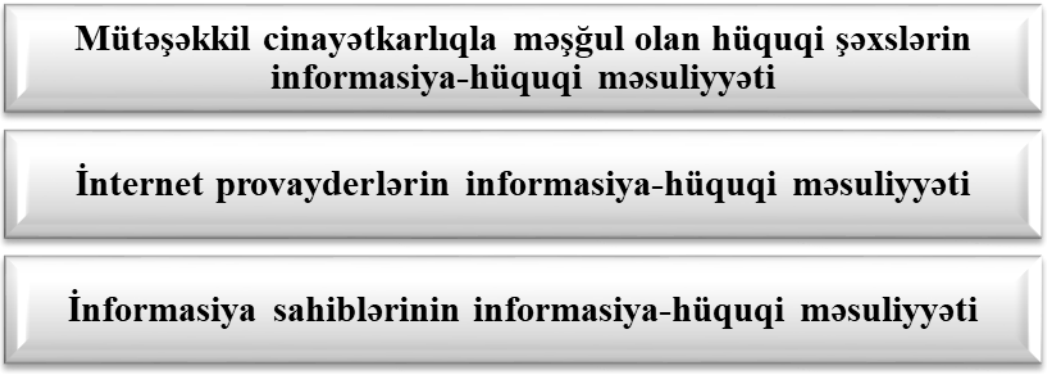
Hüquqi şəxslərin informasiya-hüquqi məsuliyyətinə dair beynəlxalq normalardan olan Avropa Parlamenti və Şurasının "İnformasiya sistemlərinə qarşı hücumlar və 2005/222/JHA Şurasının Çərçivə Qərarının dəyişdirilməsi haqqında" 12 avqust 2013-cü il Direktivində göstərilir ki, hüquqi şəxsin nümayəndəlik, hüquqi şəxs adından qərar qəbul etmək və hüquqi şəxs daxilində nəzarəti həyata keçirmək səlahiyyəti daşıyan şəxslər tərəfindən onların xeyrinə törədilmiş 3-8-ci maddələrdə göstərilən cinayətlərə (informasiya sistemlərinə qeyri-qanuni daxil olma, qeyri-qanuni müdaxilə, verilənləri qeyri-qanuni ələ keçirmə, cinayət törətmək üçün istifadə olunan vasitələr, təhrik, kömək və razılıq və cəhd) görə məsuliyyətə cəlb olunmasını təmin etmək üçün lazımi tədbirləri görürlər. Burada hüquqi şəxs – qüvvədə olan qanuna görə hüquqi şəxs statusu daşıyan, lakin dövlət səlahiyyətini həyata keçirən orqanları və ya ictimai qurumları və ya ictimai beynəlxalq təşkilatları əhatə etməyən bir təşkilat deməkdir. Qeyd olunan məsuliyyət 3-8-ci maddələrdə göstərilən cinayətlərin hər hansı birini törədən və ya onlara köməkçi olan fiziki şəxslərə qarşı cinayət işini is-

tisna etmir. Direktivə uyğun olaraq, üzv dövlətlər məsuliyyət daşıyan hüquqi şəxsin effektiv, mütənasib və çəkindirici sanksiyalarla və ya digər tədbirlərlə cəzalandırılmasını təmin etmək üçün lazımi tədbirləri görməlidirlər [6].

Budapeşt Konvensiyası da bununla bağlı özünəməxsus tənzimləmə nəzərdə tutur. Birincisi, Konvensiya hər hansı hüquqi şəxsin adından qərarlar vermək, nəzarət funksiyalarını həyata keçirmək, hüquqi şəxsin təmsil etmək kimi səlahiyyətlərə malik olan şəxsin hüquqi şəxsin xeyrinə törətdiyi pozuntulara görə həm fiziki şəxsin özünün, həm də müvafiq hüquqi şəxsin məsuliyyətinin müəyyən olunmasını dövlətlərdən tələb edir. İkincisi, burada yalnız cinayət-hüquqi deyil, digər məsuliyyət növlərindən də söhbət gedir. Üçüncüsü, hüquqi şəxslərin məsuliyyətinin müəyyən olunmasını Konvensiya yüngülləşdirici vəziyyət kmi qiymətləndirməyərək, bunun şəxsin fiziki şəxs kimi məsuliyyətini istisna etmədiyini xüsusi vurğulayır (12-ci maddə).

Respublikamızda hüquqi şəxslərin məsuliyyətinin əsas xüsusiyyətlərindən biri burada cəzaların iştirakçı fiziki şəxslərlə yanaşı, hüquqi şəxsin özünə də cinayət-hüquqi tədbir kimi tətbiq olunmasıdır. Lakin bu, informasiya hüququnun tədqiqat obyekti olmadığı üçün bununla bağlı məqamlara toxunmamağı məqsədəuğun sayırıq.

Ümumilikdə, informasiya hüquq pozuntuları üzrə hüquqi şəxslərin məsuliyyəti aşağıdakı istiqamətlərdə təhlil olunmalıdır:



Sxem 1.1. Hüquqi şəxslərin informasiya-hüquqi məsuliyyəti

Məlum olduğu kimi, transmilli xarakter daşıyan kiberməkanda mütəşəkkil cinayətkar qrupların fəaliyyəti asanlıqla idarə oluna bilir. Belə olduğu halda, kibercinayətlərin mütəşəkkil cinayətlərə aid olub-olmaması mübahisə doğurur. McCusker bu problemi məntiq və praqmatizm arasındakı ziddiyyət kimi xarakterizə edir. Burada məntiq ənənəvi mütəşəkkil cinayətkarlığın kiberməkanda hər hansı bir az riskli və yüksək gəlirli qanunsuz biznesdə olduğu kimi cinayətkar fəaliyyətə girəcəyini təsdiqləyirsə, praqmatizm ənənəvi cinayətkarlığın bu sahəyə qədəm qoymasının zəruriliyini və investisiyaların geri qaytarılmasını təmin etmək və istənilən maddi səmərə əldə etmək qabiliyyətini sual altına alır [9, s. 257].

Tarixən XXI əsrin əvvəllərində, yəni İKT-nin inkişafının ilkin dövrlərində əksər tədqiqatçılar kibercinayətlərin mütəşəkkil cinayət olmadığını israrla vurğulayırdılar. Səbəb qismində isə mütəşəkkil cinayətkarlığın oflayn rejimdə fəaliyyət göstərməyə davam etmə imkanının şəbəkədən heç bir asılılığının olmaması göstərilirdi [11, s. 49].

Lakin hal-hazırda kiberməkan artıq uşaq istismarı, qanunsuz narkotik və odlu silah ticarəti, insan alveri, qeyri-qanuni miqrasiya, çirkli pulların yuyulması, müxtəlif dələduzluq formaları və s. bu kimi cinayətlərin törədilməsi geniş imkanlar yaratmışdır. Ona görə də sanki mütəşəkkillik və tarnsmillilik kibercinayətlərin iki növünü formalaşdırır: kiberməkanda törədilməyə meyl edən ənənəvi mütəşəkkil cinayətkarlıq və mütəşəkkil cinayətkarlığın yeni bir forması, yəni kiberməkanda təşkilati formada törədilən kibercinayətlər.

Mütəşəkkil cinayətkar qrupların başlıca xüsusiyyəti onların peşəkar, ixtisaslaşmış virtual cinayətkarlar tərəfindən qurulmasıdır. Əslində, İnternet, cinayətkarlığın yeni və köhnə təşkilati formalarının bir-birlərini narahat etmədən yanaşı yaşaya biləcəyi platformanı təmsil edir. Ənənəvi mütəşəkkil cinayətkar qrupların qara bazarda bəzi az və ya qeyri-qanuni mallara nəzarət etmək üçün şiddətlə aktivləri və əraziləri üzərində inhisarçılığı qoruduğu məlumdur. Rəqəmsal kölgə iqtisadiyyat üçün bir məhsulu təmsil edən oğurlanmış, qeyri-maddi məlumatlarla, kibercinayətkarlar coğrafi ərazilər üzərində nəzarət tələb etmirlər. Burada cinayətkarlar arasında daha az şəxsi təmasa və daha az intizam tətbiq edilməsinə və nəticədə rəsmi bir təşkilatın yaradılmasına daha az ehtiyac vardır [11, s. 53]. Eyni zamanda, mütəşəkkil cinayət qruplarının ənənəvi funksional bölgüsü mütəşəkkil kibercinayətlər üçün yararsız da ola bilər.

Ənənəvi mütəşəkkil cinayətkar qruplarla kibercinayətkarlıq qrupları arasındakı digər böyük fərq yenə də avtomatlaşdırma üsuludur. Başqa sözlə, qrupun gücü fərdlərin sayında deyil, proqram təminatının gücündə ifadə olunur. Kiberməkanda fəaliyyət göstərən cinayətkar qrupların ənənəvi mütəşəkkil cinayətkar qruplarla müqayisədə daha çevik olduqlarını qəbul etmək olar və bu da qrupun üzvlərinin çevikliyi səbəbi ilə məhdud müddətə üzv olmağa imkan verir.

İKT-nin inkişafı nəticəsində kiberməkanda qeyri-qanuni məqsədlərlə gəlir əldə olunması o qədər sürətlə arıb ki, artıq hal-hazırda kiberməknada "qara bazar"lar fəaliyyət göstərir. Məlum olduğu kimi, qara bazarlar Nyu-Cersidən Nigeriyaya, Çinə və Cənub-Şərqi Asiyaya qədər bütün dünyada fəaliyyət göstərən fəaliyyətlər toplusudur. Bazar dedikdə, rəqəmsal əsasda cinayətləri əhatə edən mal və ya xidmətlər üçün ixtisaslaşmış və qeyri-ixtisaslaşmış təchizatçıların, satıcıların, potensial alıcıların və vasitəçilərin toplanması nəzərdə tutulur. Haker bazarları zamanla inkişaf etmişdir və indi bir çox formalarda mövcuddur. Onlar 2000-ci illərin əvvəlindən ortalarına qədər kredit kartı məlumatlarını əhatə edən mal və xidmətlərə diqqət yetirdilər. Sonra e-ticarət hesabları, sosial media və digər sahələr üçün vasitəçiyə qədər genişləndilər. Bu günlərdə bəziləri hələ bir məhsula və ya xüsusi bir xidmətə həsr olunur, bəziləri isə hücumun tam dövrü üçün bir sıra mal və xidmətlər təklif edir, bəziləri bir çox məhsul təklif edən, lakin birpəncərəli alış-verişi tamamlamayan "vitrinlər" dir. Bəzi satıcılar çoxsaylı bazarlarda reklam verirlər, digərləri yalnız bir neçə onlayn forumda qalırlar. Tək forumlarda və ya mağazalarda olsa da, müxtəlif məhsullara müxtəlif səviyyələrdə giriş vardır [8, s. 4-5].

Bəs kiberməkanda qara bazar necə işləyir? Troyan yaradıldıqdan sonra nə baş verir? Pul necə əldə edilir və yuyulur? Federal Təhqiqatlar Bürosu bu yaxınlarda onlayn talama və dələduzluq yolu ilə qazanc gətirən ən çox yayılmış rəqəmləri təsvir etmək üçün kibercinayətkarlıq biznesində aktiv olan fərqli "peşəkar mövqeləri" təsnifləşdirmişdir [12]:

- **Proqramçılar** – kibercinayətlər törətmək üçün istifadə olunan zərərli proqramı işləyib hazırlayırlar;
- **Distribyutorlar** – oğurlanmış verilənləri (məlumatları) satır və digər mütəxəssislər tərəfindən təqdim olunan mallar üçün vauçer rolunu oynayırlar;
- **Texniki mütəxəssislər – s**erverlər, şifrələmə texnologiyaları, verilənlər bazaları və s. daxil olmaqla cinayətkar təşkilatın İKT infrastrukturunu qoruyurlar;
- **Hakerlər** – tətbiqlərin, sistemlərin və şəbəkənin zəifliklərini axtarır və bundan istifadə edirlər;
- **Dələduzlar** – fişinq və spam kimi müxtəlif sosial mühəndislik sxemləri yaradır və tətbiq edirlər;
- **Host sistem təminatçıları** – qanunsuz məzmun serverlərinin və saytlarının təhlükəsiz yerləşdirilməsini təklif edirlər;
- **Kassirlər** – silinən hesablara nəzarət edir və digər cinayətkarlara ödənişlə ad və hesab təqdim edirlər;
- **Pul qatırları** – bank hesabları arasında pul köçürmələrini həyata keçirirlər;
- **Tellerlər** – rəqəmsal valyuta xidmətləri və fərqli dünya valyutaları vasitəsilə qanunsuz qazanılmış gəlirlərin köçürülməsi və yuyulmasını həyata keçirirlər;

- **Təşkilat rəhbərləri** – əksər hallarda texniki bacarığı olmayan şəxslərdir ki, komandanı toplayır və hədəfləri seçirlər.

Kiberməkanda qara bazarın işləməsi və burada pozuntuların törədilməsi müəyyən texniki mərhələlər üzrə icra olunur. Birinci növbədə, istifadəçilərin internet təhlükəsizliyini pozmaq üçün zərərli proqram yaradılır. Unutmamalıyıq ki hər Troyan, virus, bot və başqa digər zərərli proqramların arxasında qanunsuz mqəsədlər dayanır. Zərərli proqramın yaradılmasının əsas məqsədi "qurbanlar"ın cəlb edilməsidir. Bu da müxtəlif üsullarla edilir. Məsələn, qanunsuz onlayn malların reklamı.

Növbəti mərhələ verilənlərin satışı və çirkli pulların yuyulmasıdır. Sual yaranır? Niyə cinayətkarlar bank məlumatları əsasında pulları birbaşa əldə etmirlər və onun yuyulmasına davam edirlər? – Çünki verilənlər trafiki birbaşa oğurlamaqdan daha təhlükəlidir. Əksər hallarda kibercinayətlər bir neçə dövlətin sərhədini aşa bilir. Yəni cinayətkar ABŞ-da kompüter arxasında əyləşib, Azərbaycanda hər hansı bir şəxsin bank məlumatları əsasında pul vəsaitlərini talaya bilər. Əgər talama birbaşa olarsa, onun izinə düşmək və aşkar etmək çox asanlıqla mümkün olar. Amma arada vasitəçilər olduğu halda əsl cinayətkarın tapılması çətin olur. Məhz qara bazarlar da bunun üçün fəaliyyət göstərir.

Son zamanlar terrorçuluq kimi təhlükəli əməllərin törədilməsində kiberməkanda istifadə bütün dünya ictimaiyyətinin diqqətini hüquqi şəxslərin kibercinayətkarlığına qarşı mübarizəyə yönəltmişdir. Hətta, bəzi tədqiqatçılar "Kibercinayətkarlıqla Mübarizə Qanunu"nun hazırlanmasını təklif edirlər: Bu qanunla zəruri çatışmazlıqlar aradan qaldırılmalı və kiberterrorçuluqla mübarizə ilə bağlı qaydalar daxil edilməlidir. Bundan əlavə, ədliyyə binalarında xüsusi "İnformasiya Prokurorluqları" və "İnformasiya Məhkəmələri"nin yaradılması bu cinayətlərlə mübarizə sahəsində təcrübə gətirəcəyi üçün əhəmiyyətli bir inkişaf olacaq [1, s. 135].

Hüquqi şəxslərin informasiya-hüquqi məsuliyyətinin növbəti istiqaməti kimi ***internet provayderlərin məsuliyyətini*** qeyd etdik. "Bilməmək xoşbəxtlikdir" deyiminə istinad edən əksər internet provayderlər məsuliyyətini inkar etməyə çalışırlar. Ümumilikdə, qəbul olunur ki, provayderlər müştərinin fəaliyyətinin məzmununa daxil olan informasiyaya görə heç bir məsuliyyət daşımamalıdırlar. Çünki onların əsas məqsədi internetə çıxış imkanlarının təmin olunmasıdır. Lakin burada həmin provayderin fəaliyyətinin sırf texniki xarakterdə olması mütləq şərtdir. Məsələn, bir neçə il əvvəl internetlə bağlı Prodigy ilə əlaqəli məhkəmə işində Prodigy müştərilərindən birinin Prodigy müzakirə qrupunda (və ya bülleten lövhəsində) verdiyi ifadələrə əsaslanaraq böhtan ittihamı ilə məhkəməyə verildi. Bu işdə müştərisinin böhtan atan ifadələrinə görə Prodigy -nin məsuliyyət daşıyıb-daşımadığını müəyyən edərkən, New York ştatının hakimi Prodigy-nin kitab mağazası və ya kitabxana kimi bir məlumatın "paylayıcısı" olub-olmadığını və ya Prodigy-nin "naşir" olub-olmadığını müəyyən edərkən, ikincinin üzərində mövqeyini bildirir. Sadəcə bir distribyutor olaraq, Prodigy bəyanata görə məsuliyyət daşımır. Bunun əksinə olaraq, Prodigy naşir sayılsa (məlumatın məzmununa daha çox nəzarət etməklə), Prodigy məsuliyyət daşıyacaq. Ən çox onlayn xidmət təminatçılarını şoka salan bir qərarda, hakim Prodigy-nin forumlarını izləmək və senzura etmək üçün çox yaxşı təbliğat aparmasının nəticəsi olaraq, Prodigy-nin bir nəşriyyat olduğunu və böhtan atan ifadəyə görə məsuliyyət daşıdığını qəbul etdi. Prodigy hakimin qərarını geri götürmək üçün hərəkət etsə də, hakim bunu rədd etdi [10]. Çünki onlayn olsa belə, əgər hər hansı bir forumdan söhbət gedirsə, deməli məsuliyyət yaranacaqdır.

Məzmunundan asılı olmayaraq İnternet vasitəsilə ünsiyyət aktları, hər biri bir operator tərəfindən idarə olunan çox fərqli fiziki və məntiqi elementlərdən ibarət kompleks bir texnoloji infrastrukturdan keçir. Bu operatorların iştirakı, ümumi rabitə xidmətləri ilə bağlı qaydalar və ya İnternetlə əlaqəli xidmətlərin göstərilməsi hər bir müvafiq ərazinin qaydalarına tabedir. Eyni şəkildə, iş birləşmələrini tənzimləyən milli qaydalara və onların bazar payına uyğun olaraq tənzimləyici fərqlər var. Bu cür fərqlərin aktuallığı ondadır ki, hər bir əməliyyat metodu fərqli bir məsuliyyət formasına səbəb ola bilər. Hər bir operatorun mövcud texniki mərhələlərdən birinə nəzarət etməsi və nəticədə üçüncü şəxslərin hüquqlarını pozan iddia

edilən cinayət məzmununun və ya məzmunun dövriyyəsinə icazə vermək üçün texniki imkanlara malik olduğu halda, vasitəçi ünsiyyəti asanlaşdıracaq. Məntiqlə bu vasitəçinin bu cür ünsiyyətin dövriyyəsinin qarşısını almaq üçün lazımi texniki imkanları da olacaq. Bu baxımdan, İnternet xidmətlərini funksional xüsusiyyətlərinə görə fərqləndirmək olar [5, s. 2-3]:

1) son istifadəçinin kompüterini İnternetə qoşan, kabellərdən və ya simsiz texnologiyadan istifadə edən və ya avadanlığın İnternetə çıxışını asanlaşdıran bir giriş provayderi;

2) kompüterlə giriş provayderi ilə hostinq provayderləri arasında qarşılıqlı əlaqəyə imkan verən tranzit provayder (onun funksiyası yalnız məlumatların ötürülməsidir);

3) öz məqsədləri üçün və ya üçüncü şəxslərin istifadəsi üçün nəzərdə tutulan, tranzit provayderlərə çıxışı olan, boş yer və ya "serverləri" olan hostinq provayder;

4) veb səhifələr, xidmətlər, e-poçt, fərqli son istifadəçilər arasındakı əlaqə və zehnin təsəvvür edə biləcəyi digər imkanlar daxil olmaqla son istifadəçilərə ən müxtəlif məlumatları təqdim etmək üçün yuxarıdakı infrastrukturdan istifadə edən məzmun provayderi.

Bölgünün müəyyən çatışmazlıqları vardır. İlk öncə qeyd edək ki, Azərbaycanda iki termindən – internet və host provayderindən istifadə edilir. Tranzit provayderinə gəldikdə isə, dünya təcrübəsində internet şəbəkələrinin internet üzərindən birbaşa və dolayı olaraq əlaqələndirilməsinə və tranzit adlandırılmasına imkan verən iki növ qarşılıqlı əlaqə var. Bu iki termin bəzən bir-birini əvəz edir, amma eyni deyil. Bu baxımdan, tranzit provayderinə də hüquqi anlayış verilməsi daha yaxşı olardı.

Respublikamızda internet xidməti telekommunikasiya xidmətinin bir növü sayılır ("Telekommunikasiya haqqında" Qanunun 23-cü maddəsi). Belə olduğu halda, internet provayderlərin məsuliyyəti qeyd olunan normativ hüquqi aktla tənzimlənir. Provayderlərin məsuliyyəti birinci növbədə uçota alınma üzrə qaydaların pozulması ilə bağlıdır. Lakin bu, informasiya-hüquqi məsuliyyət hesab oluna bilməz. Çünki bilavasitə predmetini inzibati-idarəetmə qaydalarının pozulması təşkil edir. Lakin internet provayderi tərəfindən yayılan informasiya ilə bağlı pozuntular bilavasitə informasiya-hüquqi aspektə daxildir. Milli qanunvericiliyimizə əsasən, başqa qayda nəzərdə tutulmadığı tədqirdə, ötürülən məlumatların məzmununa görə operatorlar və provayderlər məsuliyyət daşımır (43-cü maddə).

Bəs internet informasiya ehtiyatında informasiya ilə bağlı pozuntulara görə məsuliyyət kimin üzərinə düşəcəkdir? – Bununla bağlı, qanunverici yetərincə ətraflı tənzimləmə etmişdir. Əsasən, aşağıdakı istiqamətlərdə normalar müəyyən olunmuşdur:

- *İnformasiya qanunvericiliyində internet informasiya ehtiyatında informasiyanın yayılması ilə bağlı qaydaların müəyyən olunması və həmin qaydaların pozulmasına görə məsuliyyət.* Bu məsuliyyətin subyektlərinə yalnız informasiya ehtiyatının sahibi deyil, həmçinin host və internet provayderlər də daxildir. Lakin onların məsuliyyət formaları fərqlidir. Belə ki, sırf texniki məsələlər üzrə məsuliyyət provayderlərin üzərinə düşürsə, qalan məzmun məsələləri üzrə məsuliyyət internet ehtiyatının sahibi üçün nəzərdə tutulur.

"İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunun 13-2-ci maddəsinə uğun olaraq, yayılması qanunla qadağan edilən informasiyanın yerləşdirilməsinə yol verilməməlidir. Azərbaycan Respublikasının Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi yayılması qadağan edilən informasiyanın internet informasiya ehtiyatında yerləşdirilməsi hallarını bilavasitə aşkar etdikdə və ya fiziki, hüquqi şəxslərdən, yaxud dövlət qurumlarından daxil olmuş əsaslandırılmış məlumatlar əsasında müəyyən etdikdə, bu barədə internet informasiya ehtiyatının və onun domen adının sahibinə və host provayderə yazılı xəbərdarlıq edir. Xəbərdarlıq edildiyi vaxtdan 8 saat ərzində yayılması qadağan edilən informasiya internet informasiya ehtiyatından götürülməlidir. Əks halda, Nazirlik həmin orqanın yerləşdiyi yer üzrə rayon (şəhər) məhkəməsinə internet informasiya ehtiyatına müraciətin məhdudlaşdırılması barədə müraciət edir. Məhkəmə internet informasiya ehtiyatına müraciətin məhdudlaşdırılması barədə müraciətə 5 günədək müddətdə baxır və qərar qəbul edir. Qərar

qəbul edildikdən dərhal sonra qüvvəyə minir və qərardan şikayətin verilməsi onun icrasını dayandırmır. Məhkəmə internet informasiya ehtiyatına müraciətin məhdudlaşdırılması haqqında qərar qəbul etdikdə, Azərbaycan Respublikası Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi həmin informasiya ehtiyatını "Yayılması qadağan edilən informasiyanın yerləşdirildiyi informasiya ehtiyatlarının Siyahısı"na daxil edir. İnternet informasiya ehtiyatı "Yayılması qadağan edilən informasiyanın yerləşdirildiyi informasiya ehtiyatlarının Siyahısı"na daxil edildikdən dərhal sonra host provayder və internet provayderlər internet informasiya ehtiyatına müraciəti məhdudlaşdırmalı və bu barədə internet informasiya ehtiyatının sahibinə məlumat verməlidirlər.

Qanunverici host provayder üçün də birbaşa qayda təyin etmişdir ki, yayılması qanunla qadağan olunan informasiya aşkar etdikdə, bu cür pozuntuların qarşısını alsın.

Beləliklə, respublikamızda internet və host provayderlərin də yayılan informasiyanın məzmununa görə müəyyən mənada informasiya-hüquqi məsuliyyəti nəzərdə tutulmuşdur. Müasir dövrdə müxtəlif süzgəclər vasitəsilə "təhlükəli kontent"in aşkar edilməsinin çox asan olması provayderlərin məsuliyyətinin müəyyən olunması üçün əsas və səbəb ola bilər. Bu, həm də pozuntuların vaxtında qarşısının alınmasına xidmət edə bilər.

- *İnzibati qanunvericilikdə informasiya-hüquqi məsuliyyətin müəyyən olunması.* Yuxarıda qeyd etdiyimiz kontekstdən qadağan olunmuş informasiyanın yayılması ilə bağlı qaydaları pozan hüquqi şəxslər inzibati məsuliyyətə cəlb edilirlər (AR İXM-in 388-1-ci maddəsi). Burada yalnız ehtiyatın sahibi deyil, həmçinin provayder, eləcə də istifadəçilər hər bir öz funskional təyinatına uyğun şəkildə məsuliyyət daşıyırlar. İXM-ə əsasən, sanskiya yalnız o halda tətbiq oluna bilər ki, həmin əməl cinayət kimi məsuliyyət yaratmasın.
- *Cinayət qanunvericiliyində informasiya-hüquqi məsuliyyətin müəyyən olunması.* Maraqlı məqam ondadır ki, AR İXM-in Cinayət Məcəlləsinə göndəriş etməsinə baxmayarq, burada konkret qadağan olunmuş informasiyanın yayılmasına görə məsuliyyət müəyyən edən norma yoxdur. Sadəcə olaraq, qanunla müəyyən edilmiş siyahıya daxil olan məlumatların yayılması ilə bağlı müxtəlif əməllər kriminallaşdırılmışdır. Məsələn, hüquqi şəxs öz saytında terrorçuluğu təbliğ edirsə, arıtq bilavasitə cinayət məsuliyyəti (214-2) yaranmış olacaqdır. Cinayət Məcəlləsinin xüsusi normalarını təhlil edərək, qanunda sadalanan məlumatların hər birinin müxtəlif maddələr üzrə cinayət əməli kimi nəzərdə tutulduğu qənaətinə gələ bilərik.

Cinayət-hüquqi aspektlə bağlı digər problemli cəhət yeni əlavə olunan bənd və normaların bir qədər qüsurlu olmasından irəli gəlir. Məsələn, 148-ci maddədən əlavə, 148-1-ci maddə (internet informasiya ehtiyatında saxta istifadəçi adlar, profil və ya hesablardan istifadə edərək böhtan atma və ya təhqir etmə) tərkib kimi müəyyən olunmuşdur. Əgər burada yalnız İKT-dən istifadə əlaməti olsa idi, belə əlavənin edilməsinə heç bir gərək qalmayacaqdı. Lakin söhbət saxtakarlıqdan getdiyi üçün artıq şəxsi həyata müdaxilə və s. pozuntular da ortaya çıxır. Bu baxımdan, saxta profillə edilən bu cür pozuntular daha təhlükəli ola bilər. Amma bu fakt da həmin əməllərin yeni bir tərkib kimi təsbit olunmasına əsas vermir. Yaxşı olardı ki, saxta profillərdən istifadə etmə tövsifedici hal kimi hər iki cinayəti nəzərdə tutan dispozisiyalara əlavə olunsun.

Nəhayət, hüquqi şəxslərin informasiya-hüquqi məsuliyyətinin digər istiqaməti ***informasiya sahiblərinin məsuliyyətidir.*** Bu məsuliyyət forması informasiya sahiblərinin informasiyanın əlyetərliyini təmin etməməsindən irəli gəlir. "İnformasiya əldə etmək haqqında" Azərbaycan Respublikası Qanununun III fəsli informasiya sorğusunun təmin edilməsi ilə bağlı məsələləri tənzimləyir. Həmin tənzimləmələrin pozulduğu təqdirdə, informasiya sahibi müvafiq məsuliyyət daşıyır ki, pozuntular həm qaydalara riayət etməməkdə ifadə oluna bilər, həm də istifadəçi hüquqlarını əsassız məhdudlaşdırmaqla özünü büruzə verə bilər (maddə 13 və 20). Bununla yanaşı, vəzifəli şəxslərin də əsassız məhdudlaşdırmalara görə məsuliyyəti müəyyən olunmuşdur. Bu da ondan irəli gəlir ki, elektron idarəetməyə keçən respublikamızda bütün məlumatlar elektron formaya keçirilir. Belə olduğu vəziyyətdə vətəndaşlar üçün həmin məlumatların əlyetərliyi tam formada təmin

olunmalıdır. Həmçinin konfidensiallıq və məxfilik qaydaları da gözlənməlidir.

Milli məhkəmə təcrübəsində informasiya sorğusunun icrasından imtina ilə bağlı yetərincə faktlar mövcuddur [2]. Həmin işlərin ümumiləşdirilməsinə əsasən, qeyd etmək lazımdır ki, əksər hallarda müxtəlif sirlərin hüquqi rejiminə daxil olan məlumatların verilməməsi əsası ilə sorğuya imtina edilir. Bu da qanunvericilikdə olan ziddiyyətlərdən irəli gəlir.

Onu da nəzərə almalıyıq ki, informasiya cəmiyyətinin əsas xüsusiyyətini bütün üzvlərin informasiya proseslərində aktivliyini təmin etmək təşkil edir ki, bunun da əsasında informasiya sahəsində hüquqlar dayanır. Bu baxımdan, informasiya sorğusunun təminatı üzrə informasiya sahiblərinin hüquq pozuntuları bilavasitə həmin hüquqlara qəsd etmiş olur. Ona görə də Ombudsmanın fəaliyyətini tənzimləyən normalar informasiya əldə etmək hüququ pozulan şəxslərin şikayət verməsi üçün hüquqi imkanlar təqdim edir (Azərbaycan Respublikasının İnsan hüquqları üzrə müvəkkili (ombudsman) haqqında" Qanunun 13-1-ci maddəsi). Müvafiq olaraq, Ombudsmanın Aparatında tərkibində "İnformasiya əldə etmək hüququnun təmini sektoru və Təhlil və monitorinqlər sektoru" fəaliyyət göstərən "İnformasiya əldə etmək hüququnun müdafiəsi şöbəsi" yaradılmışdır. Hətta Müvəkkilin Avropa Şurası ilə birlikdə keçirdiyi Tvinninq layihəsində üçüncü komponent "İnformasiya əldə etmək haqqında" Qanunun milli hüquqda implementasiyası sahəsində Ombudsman İnstitutunun imkanlarının gücləndirilməsi olmuşdur [4].

Qeyd etmək lazımdır ki, son dövrlərdə respublikamızda elektron sənəd dövriyyəsinin daha çox üstünlük təşkil etməsi elektron sənəd mübadiləsi zamanı informasiya təhlükəsizliyinin təminatı problemini gündəmə gətirir. "Elektron imza və elektron sənəd haqqında" 9 mart 2004-cü il tarixli AR Qanunu elektron sənədlərlə bağlı konkret qaydalar müəyyənləşdirir. Məsələn, Qanunda elektron sənədlərin saxlanması və mühafizəsi üçün imperativ qaydaların müəyyən edilməsi, eləcə də elektron imza ilə bağlı sertifikatlaşdırmanın nəzərdə tutulması mahiyyət etibarilə elektron sənəd dövriyyəsində "informasiya sızma"sının, informasiyanın müxtəlif məqsədlərlə məhvinin və korlanmasının qarşısını alır. Lakin onu da qeyd etməliyik ki, informasiyanın müəyyən müddətdən sonra əhəmiyyətini itirməsindən irəli gələrək, onun daşıyıcılarının qanuni qaydada məhv edilməsi və ya utilizasiyası da mümkündür. Mövcud qanunvericilik aktlarında informasiyanın məhvi ilə bağlı normalar əsas etibarilə kağız daşıyıcılarda əks olunan məlumatlara şamil edildiyi üçün elektron məlumatların məhv edilməsi ilə bağlı bir çox çətinliklər vardır. Bu baxımdan, məsuliyyət məsələlərinin düzgün həlli, informasiya sisteminin mühafizəsinin operativ təşkili məqsədilə elektron sənəd dövriyyəsi ilə bağlı normalara yenidən baxılmalı, mümkün redaktələr edilməlidir.

Nəticə

Tədqiqat zamanı informasiya-hüquqi məsuliyyət iki kontekstdən şərh olunmuşdur:

- Məzmun baxımdan: mülki, inzibati, cinayət və intizam məsuliyyəti.
- Subyekt baxımdan: fiziki və hüquqi şəxslərin məsuliyyəti.

İnformasiya-hüquqi məsuliyyətlə bağlı ən problemli məqam qanunvericiliyin əksər normalarında İKT-dən istifadənin ağırlaşdırıcı hal hesab edilməsidir. Rəqəmsallaşmanın dinamikasını nəzərə alaraq, İKT-nin tətbiqini ağırlaşdırıcı hal kimi qəbul etmək məntiqə uyğun sayıla bilməz. Belə tətbiq də digər üsullardan biri kimi qəbul edilməlidir.

Bundan əlavə, dövrün tələbindən irəli gələrək, müxtəlif dövlətlərdə istifadə olunan yeni pozuntuların, məsələn, eyniyyət oğurluğunun milli hüquq sistemimizdə tətbiq olunan normalar müstəvisində şərh olunması mümkün olmur. Çünki müqayisə zamanı mövcud normaların müəyyən etdiyi elementlər arasında uyğunsuzluq yaranır. Fikrimizcə, hər üç sahədə məsuliyyətin müəyyən olunması zamanı konkretləşdirməyə deyil, daha çox ümumi elementlərə üstünlük verilməsi daha düzgündür.

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 bö-

yük 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. Alper Güneş. Bilişim suçları və idarenin hukuki sorumluluğu. Yüksek Lisanz Tezi. Konya, 2015, 171 s.
2. Azərbaycan Respublikası adından Azərbaycan Respublikası Ali Məhkəməsinin İnzibati-İqtisadi Kollegiyasının Qərarı. http://sc.supremecourt.gov.az/storage/Inzibat/2019/9_3498+17.12.2019.pdf
3. Chrome-un "İncognito" (Gizli) rejimi istifadəçilərinin veb tarixçəsindəki məlumatları toplaması iddiası ilə Google şirkətinə qarşı 5 milyard dollar dəyərində mülki iddia qaldırılıb. https://cert.gov.az/az/article-view/73
4. İnformasiya əldə etmək hüququnun təmin edilməsi. Azərbaycan Respublikasının İnsan Hüquqları üzrə Müvəkkilinin (Ombudsman) rəsmi saytı. https://ombudsman.az/az/view/pages/46
5. Claudio Ruiz Gallardo and J. Carlos Lara Gálvez. Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America. https://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/02-Liability_Internet_Service_Providers_exercise_freedom_expression_Latin_America_Ruiz_Gallardo_Lara_Galvez.pdf
6. Directive 2013/40/EU of the European Parliament and of The Council of 12 August 2013 "On attacks against information systems and replacing Council Framework Decision 2005/222/JHA". https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF
7. Jonathan Mayer. Cybercrime litigation // University of Pennsylvania Law Review, May 2016, Vol. 164, No. 6, pp. 1453-1507
8. Lillian Ablon, Martin C. Libicki and Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. RAND Corporation, 2014, 63 p.
9. McCusker R. Transnational organised crime: Distinguishing threat from reality // Crime Law and Social Change, 2006, No. 46, pp. 257-273
10. Stratton Oakmont, Inc. v. Prodigy Services Co., 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995). https://h2o.law.harvard.edu/cases/4540
11. Tatiana Tropina. Transnational Organized Crime: Analyses of a Global Challenge to Democracy. Transcript Verlag, 2013, 308 p.
12. The cyber-crime black market: Uncovered. Panda Security Report, 2014. https://www.pandasecurity.com/en/mediacenter/src/uploads/2014/07/The-Cyber-Crime-Black-Market.pdf

Гусейн Ализаде

ИНФОРМАЦИОННО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ ЮРИДИЧЕСКИХ ЛИЦ: ФОРМИРОВАНИЕ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА В АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКЕ И НОВЫЙ ПОДХОД К ИНСТИТУТУ ИНФОРМАЦИОННО-ПРАВОВОЙ ОТВЕТСТВЕННОСТИ

Резюме

Такие причины, как невозможность идентифицировать ущерб, причиненный или который может быть причинен кибер-нарушениями в результате развития ИКТ, количество информации, не рассчитанной с точки зрения качества и количества, увеличивают информационные нарушения. Однако увидеть это в статистике очень сложно. Потому что многие нарушения остаются скрытыми, потому что они еще не криминализованы, не выявлены и не отражены в официальной статистике.

Действующее законодательство характеризуется отсутствием единого подхода к оценке нарушений в сфере информационных технологий, единством используемого понятийного аппарата и применением несоответствующих и бессистемных изменений, не приносящих ожидаемых результатов. 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. В статье анализируются такие проблемы, даются предложения и рекомендации.

Huseyn Alizade

INFORMATION-LEGAL RESPONSIBILITY OF LEGAL ENTITIES: FORMATION OF E-GOVERNMENT IN THE REPUBLIC OF AZERBAIJAN AND NEW APPROACH TO THE INSTITUTE OF INFORMATION-LEGAL RESPONSIBILITY

Summary

Reasons such as the inability to detect the damage caused or likely to be caused by cyber-violations as a result of the development of ICT, the amount of information that is not calculated in terms of quality and quantity, lead to an increase in information violations. However, it is very difficult to see this in the statistics. Because many violations remain latent because they have not yet been criminalized or detected, and are not reflected in official statistics.

The current legislation is characterized by the lack of a unified approach to the assessment of violations in the field of information technology, the unity of the conceptual apparatus used and the application of inappropriate and unsystematic changes that do not yield the expected results. 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 remains a common legal problem. The article analyzes such problems and makes suggestions and recommendations.