İNFORMASİYA HÜQUQ POZUNTULARININ QARŞISININ ALINMASINA DAİR UNİVERSAL VƏ REGİONAL NORMALARIN TƏHLİLİ

Hüseyn Əlizadə*

Xülasə

Qlobal olaraq bir-biri ilə əlaqəli olan dünyada İnternet üzərindən törədilən pozuntular tez-tez bir dövlətin yurisdiksiyasını aşır ki, bu da bütün beynəlxalq birlik üçün təhlükədir. Bu qlobal problem regional və ya dövlətdaxili qanunlarla həll edilə bilmədiyi üçün beynəlxalq həll və çoxtərəfli yanaşma tələb olunur. Bütün yurisdiksiyalarda informasiya hüquq pozuntuları ilə mübarizə aparmaq üçün hüquq-mühafizə orqanlarının hüquqi və prosedur vasitələrə malik olması lazımdır, rəqəmsal sübutların toplanması və təmin edilməsi qaydaları beynəlxalq bir standart ətrafında bütün yurisdiksiyalarda uyğun olmalıdır. Məqalədə bu kimi istiqamətlərdə təhlillər aparılmış, universal və regional normalar müqayisə olunmuş, təklif və tövsiyələr irəli sürülmüşdür.

Açar sözlər: *informasiya hüquq pozuntusu, beynəlxalq əməkdaşlıq, regional əməkdaşlıq, formal və qeyri-formal əməkdaşlıq.*

1. İnformasiya hüquq pozuntularına qarşı beynəlxalq əməkdaşlıq formaları

Kiberməkanda törədilən bir pozuntunun araşdırılması əksər hallarda bir çox fərqli dövlətin hüquq sistemini əhatə edir və cinayətkarların ədalət mühakiməsinə çıxarılması üçün sıx beynəlxalq əməkdaşlıq tələb olunur. Azərbaycan bu əməkdaşlığı nümayiş etdirən bir sıra rəsmi və qeyri-rəsmi mexanizmlərin üzvüdür. Bura müxtəlif Konvensiyaların, xüsusilə Budapeşt Konvensiyasının ratifikasiyası, o cümlədən əsas şəbəkələrin və çoxtərəfli forumların üzvü olmaq daxildir. İnformasiya-hüquq pozuntularının beynəlxalq-hüquqi tənzimlənməsində cinayət-hüquqi aspektlərə daha çox yer verilir, əsas etibarilə kibercinayətlərin hüquqi çərçivəyə salınmasına cəhd göstərilir. İnternetin yarandığı ilkin dövrlərdən bu cür addımlar atılmağa başlanmışdı. Məsələn, 1986-cı ildə İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (OECD) "Kompüterlə əlaqəli cinayətlər: Hüquq siyasətinin təhlili" adlı nəşrində beynəlxalq məlumat şəbəkələrini qorumaq üçün ümumi cinayət və cinayət-prosessual normalarının yaradılmasının vacibliyini vurğuladı. Hesabatda dövlətlərin aşağıdakı əməlləri kriminallaşdırması zərurəti qeyd edildi: kompüter dələduzluğu və saxtakarlıq; kompüter proqramlarının və məlumatların dəyişdirilməsi; müəllif hüquqlarının pozulması; kompüterlərin və ya rabitə sistemlərinin fəaliyyətinə və ya digər funksiyalarına manea yaradılması.

Ümumiyyətlə, beynəlxalq əməkdaşlıq formal və qeyri-formal ola bilər. Formal əməkdaşlığa universal və regional səviyyədə qəbul edilmiş konvensiyalar və sazişlər daxildir. Elektron sübutların qeyri-sabit olması səbəbindən kibercinayətlər sahəsində cinayət işləri üzrə beynəlxalq əməkdaşlıq vaxtında

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

cavab verməyi və kompüter məlumatlarının qorunması kimi xüsusi istintaq hərəkətləri tələb etməyi tələb edir. 2013-cü ildə olan məlumatlara görə, kibercinayət hadisələrində ərazi xaricində sübutlar əldə etmək üçün ənənəvi əməkdaşlıq formalarının istifadəsi üstünlük təşkil edir, ölkələrin 70%-dən çoxu bu məqsədlə rəsmi qarşılıqlı hüquqi yardım istəklərindən istifadə edirdi. Belə rəsmi əməkdaşlıq çərçivəsində müraciətlərin demək olar ki, 60 faizi hüquqi əsas kimi ikitərəfli sənədlərdən istifadə edirdi. Çoxtərəfli alətlər halların 20 faizində istifadə olunurdu. [6, s.28] Lakin hal-hazırda çoxtərəfəli alətlər üstünlük təşkil etməyə başlayıb. Qeyd etdiyimiz kimi, Budapeşt Konvensiyası bariz nümunədir.

İnkişaf etmiş dövlətlərdə bir çox uğurlu nəticələr olmasına baxmayaraq, inkişaf etməkdə olan dövlətlərdə lazımi qanunvericilik ya bu beynəlxalq standartla kifayət qədər uyğun gəlmir, ya da sadəcə mövcud deyil. Əslində, Konvensiya infrastruktur ölkələrindən daha çox inkişaf etməkdə olan ölkələrə faydası baxımından daha dəyərlidir.

Hal-hazırda Budapeşt Konvensiyası beynəlxalq cinayətlərin ümumi minimum standartlarını qurmaq, daha aşağı standartlara malik yurisdiksiyalar üzrə fəaliyyət göstərən cinayətkarların qarşısını almaq, yeganə beynəlxalq vasitəni və ölkələr üçün hüquq-mühafizə orqanları arasında beynəlxalq əməkdaşlıq baxımdan ən yaxşı çıxış yollarını təqdim edir. Buna baxmayaraq, xüsusən də inkişaf etməkdə olan ölkələrdə Konvensiyaya davamlı olaraq artan dəstək heç bir şəkildə zəmanət vermir və ya qaçılmazdır. Konvensiya, ənənəvi olaraq BMT-nin qurumları tərəfindən İnternetin tənzimlənməsində daha çox rol oynamağa meylli olan müəyyən dairələrin müqaviməti ilə qarşılaşır. [11, s.110]

Ümumiyyətlə, Konvensiya qəbul olunduğu gündən birmənalı qarşılanmır. Konvensiya ilə bağlı mübahisələr üç geniş kateqoriyanı əhatə edir: [11, s.113]

Konvensiyanı ratifikasiya edən dövlətlərə baxdıqda, artıq onun regional xarakter daşıması arqumentinin əsassız olduğu görünür. İnkişaf etməkdə olan dövlətlərin iştirak etməməsinə gəldikdə isə, inkişaf etməkdə olan dövlətlər öz yurisdiksiyası daxilində kiberməkanda törədilən pozuntuların qarşsını almaq imkanına malik deyil. Çünki ənənəvi hüquq pozuntularından fərqli olaraq, kibermühitdə törədilən əməllərin qarşısının alınması üçün təhlükəsiz informasiya in-

frastrukturunun da olması mütləq şərtdir. Bu səbəbdən, Konvensiyanın inkişaf etmiş ölkələri inkişaf etməkdə olan ölkələrlə əməkdaşlıq etməyə çağırışı həmin dövlətlər üçün xüsusi faydaya malikdir.

Konvensiyanın köhnəlməsi arqumenti bəzi tənzimetmə məsələlərində özünü doğruldur. Çünki həqiqətən də bəzi təsnifat məsələləri dövrün tələblərinə uyğun gəlmir.

Lakin bir məqamı da qeyd etməliyik ki, Budapeşt Konvensiyasının özü hələ də bir çox dövlətlər tərəfindən ratifikasiya edilməmişdir. Məsələn, Braziliya, Rusiya, Çin, o cümlədən Latın Amerikası, Orta Şərq və Asiya-Sakit okean ölkələrinin əksəriyyəti hazırlanmasında iştirak etmədikləri üçün Budapeşt Konvensiyasını imzalamamışlar. Bu da Konvensiyanın effektivliyini azaldır, çünki Konvensiyanı ratifikasiya edən 66 dövlət [15] dünyanın internet istifadəçilərinin yarısından azını təşkil edir.

Hətta, bəzi müəlliflər 2012-ci ildə Braziliyanın Salvador şəhərində keçirilmiş BMT-nin Cinayətlərin qarşısının alınması və Cinayət Ədaləti üzrə on ikinci Konqresində Çin, Hindistan, Cənubi Koreya və bir sıra digər regional ölkələr tərəfindən yeni bir qlobal kibercinayət müqaviləsi təklifini dəstəkləyir və bu addımın yeni, daha əhatəli bir konvensiya üçün yaxşı bir zəmin yarada biləcəyini vurğulayırlar. [16, s.543]

Bundan əlavə, BMT Baş Assambleyası tərəfindən 22 yanvar 2001-ci ildə qəbul edilmiş "İnformasiya texnologiyalarından cinayətkar şəkildə sui-istifadə ilə mübarizə" haqqında Qətnamədə [3] BMT dövlətləri informasiya texnologiyalarından cinayətkar şəkildə sui-istifadə ilə mübarizə səylərində aşağıdakı tədbirləri nəzərə almağa dəvət edir:

- informasiya texnologiyalarından cinayətkar məqsədlərlə sui-istifadə edənlər üçün "sığınacaq" rolunu oynayan hüquqi tənzimləmə və təcrübələrin aradan qaldırılması;
- informasiya texnologiyalarından sui-istifadə cinayətləri ilə bağlı beynəlxalq işlərin araşdırılması və təqibində hüquq-mühafizə orqanlarının əlaqələndirilməsi və əməkdaşlığının təminatı;
- informasiya texnologiyalarından cinayətkar məqsədlərlə sui-istifadə halları ilə bağlı məlumat mübadiləsinin aparılması;
- hüquq-mühafizə orqanlarının əməkdaşlarının informasiya texnologiyalarından sui-istifadə hallarının qarşısının alınması üçün təlimatlandırılması və məlumatlandırılması;
- verilənlərin və kompüter sistemlərinin konfidensiallığının, tamlığının və əlyetərliyinin təminatı və İKT-dən cinayətkar məqsədlərlə sui-istifadənin cəzalandırılmasının hüquqi tənzimlənməsi;
- istintaq zamanı elektron məlumatların qorunması və onların əlyetərliyinin təminatı;
- informasiya texnologiyalarından cinayətkar məqsədlərlə sui-istifadə cinayətlərinin vaxtında araşdırılmasını və bu kimi hallarda sübutların vaxtında

toplanmasını və mübadiləsini təmin edən qarşılıqlı yardım rejimlərinin formalaşdırılmaısı;

- geniş ictimaiyyət arasında informasiya texnologiyalarından cinayətkar şəkildə sui-istifadə edilməsinin qarşısının alınması və onunla mübarizə aparılmasının vacibliyi barədə maarifləndirmənin təşkili;

- informasiya texnologiyalarının onlardan sui-istifadə hallarının qarşısının alınmasına və aşkarlanmasına, cinayətkarların izinə düşülməsinə və sübutların toplanmasına yardımçı olmağa xidmət edən dizaynda hazırlanması;

- informasiya texnologiyalarının cinayətkar məqsədlərlə sui-istifadə edilməsinə qarşı mübarizənin həm fərdi azadlıqların, həm də konfidensiallığın qorunması nəzərə alınmaqla aparılması.

Qeyri-formal əməkdaşlığa gəldikdə, vəziyyət bir qədər fərqlidir. Kiberpozuntular üçün heç bir manea törətməyən sərhədlər və tez-tez qanunsuz fəaliyyətlərini dərhal xəbərdar etməklə ört-basdır etməyə kömək edən şəraitdə kibercinayətkarlıqla effektiv mübarizə aparmaq üçün milli hüquq-mühafizə orqanlarını birləşdirən beynəlxalq səlahiyyətlə malik, daimi fəaliyyət göstərən fəal reaksiya şəbəkəsi tələb olunur. "Cinayət heç vaxt yatmaz" deyə, ayrı-ayrı ölkələr hər günün hər saatı üçün əlaqə məlumatları aktual olaraq saxlanıla bilər. 24/7 şəbəkələrinin səmərəli işləməsi üçün milli nöqteyi-nəzərdən olan səlahiyyətlilər yerli tənzimləmələrinin daha böyük beynəlxalq sistemlərlə necə kəsişdiyini və qarşılıqlı əlaqədə olduğu və kibercinayətkar davranış barədə minimum texniki biliyə malik olmalı, eləcə də və xarici dillərdə ünsiyyət qurma qabiliyyətinə malik olmalıdırlar. [4, s.206-207]

Adı	**İdarə edən təşkilat**	**Yaradılma əsası və tarixi**	**Üzvlər**	**Fəaliyyəti**
G8 24/7 Verilənlərin Mühafizəsi Şəbəkəsi [8]	G8 High-Tech Crime Subgroup	1999-cu ildə Lyon-Roma High Tech Crime Subgroup (HTCSG) tərəfindən təklif edilmişdir.	70	Məqsədi elektron sübutlarla bağlı araşdırmalara təcili yardım tələb edən hadisələr üçün kiber ixtisaslaşdırılmış əlaqə nöqtələri yaratmaqdır.
Budapeşt Konvensiyası 24/7 Yüksək Texnologiyalı Cinayət Nöqtələri	Avropa Şurası	2015-ci ildə Budapeşt Konvensiyasının 35-ci maddəsinə əsasən yaradılmışdır.	55	Məqsədi kompüter sistemləri və kompüter verilənləri ilə əlaqədar cinayətlərin istintaqı və ya

Şəbəkəsi [2]				digər icraatın aparılması məqsədilə və ya cinayətlərə dair sübutların elektron formada toplanması üçün təxirəsalınmaz yardımın göstərilməsini təmin etməklə əlaqələrin yaradılmasıdır.
INTERPOL I-24/7 Qlobal Polis Rabitə Sistemi [9]	INTERPOL	2015-ci ildə INTERPOL tərəfindən yaradılmışdır.	136	Məqsdi üzv dövlətlərin hüquq-mühafizə orqanlarının əməkdaşlarının istənilən zaman cinayət məlumat bazasına birbaşa daxil olmaqla təcili polis məlumatlarını paylaşmasına şərait yaradılmasıdır.

Əsas üç 24/7 şəbəkələr aşağıdakılardır:

24/7 kooperativ şəbəkələri digər yurisdiksiyalarda olan elektron sübutların mühafizəsinə kömək edə bilsə də, hüquq-mühafizə orqanı dəfələrlə elektron şəbəkələrə daxil olmaq və əlaqə qeydləri kimi kompüter məlumatlarını sürətlə qorumaq üçün mexanizmlərin olmamasından əziyyət çəkir. Belə ki, ayrı-ayrı dövlətlərin səlahiyyətli şəxslərinin əvəzinə kibercinayətkarlar da sistemə daxil ola bilirlər. Ona görə də məlumatların paylaşılamsı və daha operativ mühfizə-sində müxtəlif informasiya mərkəzlərinin rolu daha asan və zəmanətlidir. Məsələn, INTERPOL-un Qlobal İnnovasiya Kompleksi, Evropolun Avropa Kibercinayətkarlıq Mərkəzi, AB-nin Məhkəmə Əməkdaşlıq Birliyi, ABŞ Milli Kiber-Ədliyyə və Təlim Birliyi kimi bir neçə qlobal məlumat paylaşma və koordinasiya mərkəzini misal göstərmək olar.

2. İnformasiya hüquq pozuntularının qarşsının alınması üzrə regional əməkdaşlıq və regional təsisatlar

İnformasiya hüquq pozuntularının qarşısının alınması üzrə regional təsisatların rolu çox böyükdür. Onlardan bir neçə haqqında qısaca məlumat verək:

Niderlandın Haaqa şəhərində yerləşən bir Avropa Birliyi (AB) agentliyi olan *Evropol*, ilk növbədə üzv dövlətlərin hüquq-mühafizə orqanlarına daxili təhlükəsizlik məsələləri ilə əlaqəli, təhlükəsiz kəşfiyyat dəyişikliklərinin asanlaşdırılması üçün bir mexanizm təqdim edərək, cinayətkarlıq və terrorizmlə mübarizədə üzv dövlətlərə kömək etməklə məşğuldur. Bütün iştirakçı dövlətlər AB üzvləridir. AB-yə üzv olmayan dövlət ortaqlıqları ya "operativ", ya da "strateji" hesab olunur. Əməliyyat tərəfdaşlığı şəxsi məlumat mübadiləsi də daxil olmaqla ortaqlar və Evropol arasında məlumat mübadiləsinə imkan verir. Əməliyyat tərəfdaşları arasında Avstraliya, ABŞ və INTERPOL yer alır. [14] Lakin bir dövlət kibercinayətlərə dair kəşfiyyat məlumatlarını paylaşmağa qərar verərsə, Evropol bütün digər üzv dövlətləri kəşfiyyatlarını da paylaşmağa məcbur edəcək siyasi səlahiyyətə sahib deyil. Bir üzv dövlət kəşfiyyat məlumatlarını paylaşmamağı seçərsə, Evropol bir dövləti bu məlumatı paylaşmağa məcbur edə bilməz. Bu səbəbdən, təşkilat daxilində Europol üzv dövlətlərinin həyata keçirdiyi bir çox hərəkət tamamilə könüllüdür.

Evropol AB-nin özünün, həm də bir çox siyasətçilərin nöqteyi-nəzərindən kibercinayətkarlığa qarşı mübarizə aparan mərkəzi qurum hesab edilir. Evropolun həyata keçirdiyi əməliyyatlar üç əsas kateqoriyadan ibarətdir:

- kəşfiyyat məlumatlarının paylaşımı, təhlil və yerlərdəki dəstək də daxil olmaqla əməliyyat dəstəyi;
- təhsil və maarifləndirmə işi;
- çoxtərəfli/birgə fəaliyyətləri əlaqələndirmək və ya belə fəaliyyətlərdə iştirak etmək.

Evrojust kibercinayətləri ən az beş və ya altı il müddətinə azadlıqdan məhrumetmə cəzası ilə sanksiyalaşdırılmasını tövsiyə edir. [17] Kibercinayətlər Evrojustın ümumi işinin əhəmiyyətli bir hissəsini təşkil edən və sürətlə inkişaf edən bir cinayət sahəsidir. 2019-cu ildə Evropol və Evrojust beş fərqli sahəyə ayrılan kibercinayətkarlıqla mübarizədə mövcud inkişafları və ümumi çətinlikləri müəyyən edən və təsnif edən ortaq bir hesabat nəşr etdi:

1. Verilənlərin itkisi: elektron məlumatlar bütün kibercinayət sahələrində uğurlu araşdırmaların açarıdır, lakin bu cür məlumatları əldə etmək imkanları əhəmiyyətli dərəcədə məhdudlaşdırılmışdır.

2. Məkanın itirilməsi: son tendensiyalar hüquq-mühafizə orqanlarının artıq cinayətkarın fiziki yerini, cinayət infrastrukturunu və ya elektron sübutları müəyyən edə bilməyəcəyi bir vəziyyətə gətirib çıxarmışdır.

3. Milli hüquq çərçivələrlə bağlı çətinliklər: Aİ üzv dövlətlərində daxili hüquqi çərçivələrdəki fərqlər çox vaxt beynəlxalq kibercinayətlərin araşdırılmasında ciddi maneələr olduğunu sübut edir.

4. Beynəlxalq əməkdaşlığın qarşısındakı maneələr: beynəlxalq kontekstdə sübutların sürətlə paylaşılması üçün ortaq hüquqi çərçivə mövcud deyil (sübutların qorunması üçün olduğu kimi). Sərhədlərarası ünsiyyət və sürətli məlumat mübadiləsi üçün daha yaxşı bir mexanizmə ehtiyac olduğu aydındır.

5. Dövlət-özəl tərəfdaşlığının çətinlikləri: kibercinayətkarlıqla mübarizə üçün özəl sektorla əməkdaşlıq mühüm əhəmiyyət kəsb edir, lakin heç bir standartlaşdırılmış qarşılıqlı əlaqə qaydaları yoxdur və bu səbəbdən araşdırmalara mane ola bilər. [5]

Qeyri-formal əməkdaşlıq daha geniş miqyasda törədilən pozuntuların qarşısının vaxtında alınmasında uğurlu nəticələr verir. Məsələn, BlackShades əməliyyatını misal göstərə bilərik: BlackShades alıcılara kompüterləri yoluxdurmağa və nəzarət etmələrinə imkan verən zərərli proqramlar hazırlayan və satan bir təşkilat idi. Məsələn, bir alıcı ən az 2000 kompüteri yoluxdurmuş, qurbanların vebkameralarını qadın və qızların şəkillərini çəkmək üçün idarə etmişdi. ABŞ FTB-si bəzi müstəqil araşdırmalara başlamış olan bir neçə AB üzvü ilə əlaqə yaratdı. BlackShades zərərli proqramlarının satıcıları və istifadəçiləri bu dünya araşdırması zamanı on altı dövlətin məhkəmə və hüquq-mühafizə orqanları tərəfindən hədəfə alındı. 2013-cü ilin noyabr ayından başlayaraq əməliyyata qoşulan Evrojust məlumat paylaşımı və hərəkətlərin əlaqələndirilməsini genişləndirdi və 2014-cü ilin may ayında əməliyyat artıq on altı dövləti (Niderland, Belçika, Fransa, Almaniya, Böyük Britaniya, Finlandiya, Avstriya, Estoniya, Danimarka, İtaliya, Xorvatiya, Amerika Birləşmiş Ştatları, Kanada, Çili, İsveçrə və Moldova) əhatə edirdi. Bu müddət ərzində müxtəlif dövlətlərdə 359 evdə axtarış aparıldı, 97 adam həbs edildi və 1100-dən çox məlumat saxlama qurğusu qeyri-qanuni fəaliyyətlərdə istifadə edildiyi ehtimal edildi. BlackShades veb saytında olduğu kimi, xeyli miqdarda nağd pul, qanunsuz odlu silah və narkotik maddələr də ələ keçirildi. Eurojust hər bir dövlətdə araşdırmaların vəziyyətinə ümumi baxış keçirməklə və məhkəmə yardımı göstərməklə əlaqədar dövlətlərə kömək etdi və cinayət təqibi üçün optimal dövləti təyin etməkdə də əsas rol oynadı. [13]

Həmçinin qaranlıq veb bazarlara qarşı mübarizədə də qeyri-rəsmi əməkdaşlıq və məlumat mübadiləsi xüsusi əhəmiyyətə malikdir. Qaranlıq veb geniş çeşidli cinayət məhsulları və xidmətlərinin ticarətində əsas hüquq təminatçısı və hüquq-mühafizə orqanlarının prioritet təhdidi olaraq qalır. 2019-cu ilin may ayında AB hüquq-mühafizə orqanları tərəfindən eyni vaxtda keçirilən qlobal əməliyyatlar nəticəsində iki məhsuldar qaranlıq veb bazar – Wall Street Market və Valhalla (Silkkitie kimi də məşhurdur) ləğv edildi. 2017-ci ildə üç ən böyük bazarın silinməsindən sonra Wall Street qalan ən böyük qanunsuz onlayn bazarlardan biri idi. Bağlandığı anda 110 000-dən çox istifadəçisi və 5400 satıcısı var idi. Niderland Milli Polisi Evropol, Evrojust və ABŞ-ın bir sıra dövlət qurumları tərəfindən dəstəklənən Alman Federal Cinayət Polisi İdarəsi Almaniyada üç şübhəli şəxsi tutdu. Polis məmurları 550 000 avrodan çox nağd pulu, həmçinin

Bitcoin və Monero kriptovalyutalarını altı rəqəmli məbləğdə ələ keçirdi. ABŞ-da ən çox satılan narkotik vasitə bazarlarından ikisinin də aktivləri həbs edildi. Finlandiya Gömrük İdarəsi, Fransa Milli Polisi və Evropolla sıx əməkdaşlıq edərək, Valhalla marketplace serverini və məzmununu ələ keçirdi. Əməliyyat nəticəsində Finlandiya gömrük işçiləri də əhəmiyyətli bir Bitcoin ələ keçirdi. Valhalla ən qədim və beynəlxalq səviyyədə tanınan Tor* ticarət saytlarından biri idi. [9, s.44]

Bir çox hallarda informasiya hüquq pozuntuları offlayn rejimdə törədilir. Belə təqdirdə, hüquq mühafizə orqanlarının rolu xüsusi əhəmiyyətə malik olacaqdır. Lakin əməkdaşlıq təmin olunmadığı vəziyyətdə uğurlu nəticədən danışmaq qeyri-mümkündür. Ona görə də bəzi müəlliflər "bölüşdürülmüş (paylanmış) məsuliyyət" ideyasını irəli sürürlər. Məsələn, Brenner hesab edir ki, hökumətin, istifadəçilərin (fərdi və təşkilati) və kompüter istehsalçılarının kibertəhlükəsizlik üçün məsuliyyəti bölüşmələri lazımdır. Onun fikrincə, real dünyadakı cinayətlərdən fərqli olaraq, kibercinayətlərin tək-tək qurbanları olmadığı, eləcə də bu cinayətlərin avtomatlaşdırılması səbəbindən, kiber cinayətkarlar çox az səy göstərərək çox sayda cinayət törədə bilərlər. Məhdud mənbələr və reaktiv strategiya səbəbindən hüquq-mühafizə orqanları bu problemlə məşğul ola bilməyəcəklər. Brenner hüquq-mühafizə orqanlarının reaktiv strategiyasını təkmilləşdirmək üçün dörd tədbir təklif edir: 1) kiber cinayətlərə dair Konvensiyanın qəbulu; 2) hüquq-mühafizə orqanlarının reaksiya zərbəsi texnikası; 3) mülki reaksiya texnikaları; 4) daha çox kadr potensialı. [1, s.1-12]

Eyni zamanda, Chang da təhlükəsizlik hadisələri haqqında məlumat paylaşarkən və erkən xəbərdarlıq sxemləri qurarkən hökumət və özəl sektor arasında kütləvi iş birliyinin zəruriliyini həll etmək üçün "viki kibercinayətlərin qarşısının alınması" ideyasını təklif edir. [16, s.539]

Əslində, müəlliflərin mövqeyi doğrudur. Çünki müxtəlif hüquq pozuntularının qarşısının alınması və məsuliyyətin müəyyən olunması hüquq-mühafizə orqanlarının işi olsa da, onların təkbaşına fəaliyyəti heç vaxt müsbət nəticələr verə bilməz. Fikrimizcə, burada üçtərəfli əməkdaşlıq olmalıdır: Dövlət orqanları (hüquq-mühafizə orqanlarının timsalında) - özəl sektor - cəmiyyətin üzvləri. Dövlət orqanlarının fəaliyyəti nə qədər yaxşı təşkil olunarsa, informasiya hüquq pozuntuları üçün bir o qədər əlverişli şərait olmaz. Özəl sektor da əsas halqadır, çünki İKT istehsalı ilə məşğul olan böyük şirkətlər özəl sektorun iştirakçılarıdır. Onların təhlükəsizlik məsələlərinin təminatında, məlumat sızmalarının qarşısının alınmasında əvəzsiz rolu vardır. O ki qaldı cəmiyyətin ayrı-ayrı üzvlərinə, onların hüquq pozuntularına yol verməməsində və eləcə də belə pozuntuların qarşısının alınmasında daha fəal və məsuliyyətli olmasını təmin etmək üçün könüllü davranış daha səmərəli ola bilər. Bu isə o deməkdir ki, dövlətin məcburi qayda-

* The Union Router – Tor. Tor brauzeri istifadəçilərə pulsuz internetə anonim giriş imkanı verir. Hər şeydə olduğu kimi, bu giriş həm yaxşı, həm də pis niyyətlə istifadə edilə bilər. Tor həm də insanlara qaranlıq internetdəki cinayətkar saytları və bazarları ziyarət etməyə icazə verir.

ları ilə yanaşı, ayrı-ayrı şəxslərdə maarifləndirmə yolu ilə çəkindirməyə nail olmaq lazımdır.

Hüquq-mühafizə orqanlarının əməkdaşları və İT işçiləri kibercinayətkarlığın effektiv şəkildə araşdırılması üçün bir komanda olaraq çalışmalıdırlar. Belə ki, İT mütəxəssisləri hacker düşüncəsini başa düşür, rəqəmsal sübutları haradan axtarmağı bilir və texnologiya ilə nələrin edilə biləcəyini və nəyin edilə bilməyəcəyini daha düzgün bilir. Hüquq-mühafizə orqanlarının əməkdaşları isə sübutların tamlığını qorumaq üçün hüquqi prosedurlardan məlumatlıdırlar.

İnformasiya hüquq pozuntuları ilə daha operativ mübarizə aparılması üçün kiberməkanın tənzimlənməsi və yurisdiksiya məsələlərinin həlli də çox vacibdir. 2019-cu ildə Internet & Jurisdiction Policy Network tərəfindən aparılmış sorğuda iştirak edən mütəxəssislərin əksəriyyəti (56%) internet üzərindəki sərhədyanı hüquqi problemlərin önümüzdəki üç ildə getdikcə daha da kəskinləşəcəyinə "qəti şəkildə razılaşdığını" ifadə etmişlər. [7]

Kiberməkanda edilən pozuntunun icraatı həddindən artıq çətinliklərlə üzləşir. Məsələn, Argentinada eyni şəxs bir sosial media saytına Finlandiyadakı bir şəxs haqqında böhtan atan bir şərh yazanda, təkcə Argentina və Finlandiya qanunlarına deyil, əlaqədə olduğu bütün ölkələrin qanunlarına tabe ola bilər. İnternetdəki ən başlıca problem insanların çox vaxt hər hansı bir fəaliyyət üçün kontekstli hüquq sisteminin bir hissəsini təşkil edən bütün əyalət qanunlarını təxmin edə bilməmələridir. Bir insan hansı dövlətlərin qanunlarının onlara tətbiq olunduğunu müəyyən edə bilsə belə, bütün bu qanunların tənzmietmə dairəsinə düşmək asan olmur.

Müxtəlif tədbirlər barədə şərhlərin verilməsi zamanı əksər müəlliflər problemə yuxarıda qeyd olunan hər iki aspektdən baxırlar. Məsələn, Benoit Dupont beş istiqamət müəyyənləşdirir: [12, s.130]

3. Nəticə

İnformasiya hüquq pozuntuları təcrid olunmuş bir məsələ deyil, yalnız qlobal kibertəhlükəsizlik şüuruna və qlobal potensialın artırılmasına ehtiyac duyan hərtərəfli, əməkdaşlıq edən, qlobal bir yanaşma ilə mübarizə edilə bilər. Texnoloji inkişaflar getdikcə bir-birinə bağlı səyləri və paylaşılan əməliyyatları mümkün hala gətirdiyi kimi, onlar da kibercinayətkarlar üçün artan potensial təqdim edir və bununla da daha böyük hüquqi çeviklik tələb edir ki, bu da qlobal kibertəhlükəsizlik səylərinin inkişaf etdirilməsində nəzərə alınmalıdır.

İnformasiya-hüquq pozuntularının qarşısının alınması üçün həm təşkilati, həm də maddi əsaslarla universal və regional əməkdaşlıq tələb olunur. Dövlətlərarası əməkdaşlığın əhəmiyyəti mərkəzləşmə və müstəqilliyin saxlanması ilə bağlıdır. Mərkəzləşmə təşkilati vəzifələrin hər hansı bir təşkilat tərəfindən idarə edilməsini ifadə edir. Bu cür vəzifələr əməkdaşlığın həm hüquq, həm də təcrübi tərəflərini tənzimləyir. Müstəqillik isə dövlətlərin əməkdaşlıqda sərbəstliyini nəzərdə tutur.

Maddi əsaslara gəldikdə isə, kiberməkanda törədilən pozuntuların yalnız bir dövlətin məsələsi olmadığı artıq qeyd olunmuşdur. Belə olduğu halda, bir dövlətin, xüsusilə zəif inkişaf etmiş dövlətlərin bu cür əməllərlə təkbaşına mübarizə aparması qeyri-mümkündür. Mərkəzləşmiş regional və ya beynəlxalq təsisatın olması çox vacibdir. Məsələn, Evropol kibercinayətlərlə mübarizə aparmaq üçün genişləndirilmiş əməkdaşlığın təşkilini təqdim edən bir təşkilat kimi xüsusi rola malikdir. Evropola daxil olan məlumatların çoxunun dövlət kəşfiyyat orqanları tərəfindən hazırlandığını nəzərə alaraq, Evropol daxilində genişləndirilmiş əməkdaşlığın üstünlükləri aydın görünməyə bilər. Çünki heç bir dövlət öz dövlət sirrinə aid olan məlumatların təqdim olunmasında o qədər də maraqlı olmaya bilər. Bu baxımdan, əməkdaşlığın təşkili mükəmməl səviyyədə olmalıdır. Bunun üçün regional və universal təşkilatlar təkbaşına fəaliyyət göstərməməli, İKT sahəsində məşhur istehsalçı şirkətlərlə əlaqəli iş qurmalıdırlar ki, verilənlərin təhlükəsizliyi tam təmin olunsun.

Formal və qeyri-formal əməkdaşlıq informasiya hüquq pozuntularının qarşısının alınmasında mühüm əhəmiyyət kəsb edir. Fikrimizcə, operativ reaksiyaların verilməsində qeyri-formal əməkdaşlıq daha praktik fəaliyyət göstərə bilər. Dissertasiya işində təcrübədən gətirdiyimiz misallar bunu bir daha təsdiq edir. Lakin bu əməkdaşlıq yalnız kibercinayətləri əhatə etməməli, inzibati sferada baş verən informasiya hüquq pozuntularını, hətta adi İKT səhvlərini də əhatə etməlidir.

İstinadlar:

1. Brenner SW. Distributed security: Moving away from reactive law enforcement // International Journal of Communication Law & Policy, 2005, No. 9, pp.1-42

2. Budapest Convention 24/7 High Tech Crime Points of Contact Network. https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

3. Combating the criminal misuse of information technologies. Resolution adopted by the General Assembly. 22 January 2001. https://digitallibrary.un.org/record/454952

4. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. United Nations and International Bank for Reconstitution and Development/The World Bank, 2017, 484 p.

5. Common challenges in combating cybercrime. h https://www.eurojust.europa.eu/common-challenges-combating-cybercrime-identified-eurojust-and-europol

6. Comprehensive Study on Cybercrime. United Nations, 2013, 287 p.

7. 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

8. G8 24/7 Network for Data Preservation. https://rm.coe.int/1680303ce2

9. Internet organised crime threat assessment. Europol, 2019, 62 p.

10. INTERPOL Global Police Communications System. https://www.interpol.int/How-we-work/Databases

11. Jamil Z. Global Fight Against Cybercrime: Undoing the Paralysis // Georgetown Journal of International Affairs, 2012, pp. 109-120

12. Jobel Kyle P. Vecino. United by Necessity: Conditions for Institutional Cooperation against Cybercrime // The Cyber Defense Review, Special edition: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2018, pp. 123-144

13. Operation BlackShades: An Evaluation. Eurojust, 2015 https://www.eurojust.europa.eu/operation-blackshades-evaluation

14. Operational Agreements. Europol, accessed April 29, 2018. https://www.europol.europa.eu/partners-agreements/operational-agreements.

15. Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. https://www.coe.int/en/web/cybercrime/parties-observers

16. Peter Drahos. Regulatory Theory: Foundations and applications. ANU Press: 2017, 784 p.

17. Transmission of information. https://www.eurojust.europa.eu/judicial-cooperation/tasks-and-tools-eurojust/transmission-information

АНАЛИЗ УНИВЕРСАЛЬНЫХ И РЕГИОНАЛЬНЫХ НОРМ ПРОФИЛАКТИКИ ИНФОРМАЦИОННЫХ НАРУШЕНИЙ

Гусейн Ализаде[*]

Резюме

В глобально взаимосвязанном мире киберпреступность часто выходит за пределы юрисдикции одного государства, что представляет собой угрозу для всего международного сообщества. Поскольку эта глобальная проблема не может быть решена региональным или внутренним законодательством, требуется международное решение и многосторонний подход. Во всех юрисдикциях правоохранительные органы должны иметь правовые и процедурные средства для борьбы с информационными нарушениями, а правила сбора и предоставления цифровых доказательств должны быть единообразными во всех юрисдикциях в соответствии с международным стандартом. В статье анализируются такие области, сравниваются универсальные и региональные нормы, даются предложения и рекомендации.

Ключевые слова: *информационное нарушение, международное сотрудничество, региональное сотрудничество, формальное и неформальное сотрудничество.*

ANALYSIS OF UNIVERSAL AND REGIONAL NORMS FOR THE PREVENTION OF INFORMATION OFFENCES

Huseyn Alizade[**]

Abstract

In a globally interconnected world, cybercrime often transcends the jurisdiction of one state, which is a threat to the entire international community. As this global problem cannot be resolved by regional or domestic law, an international solution and a multilateral approach are required. In all jurisdictions, law enforcement agencies must have the legal and procedural means to combat information offences, and the rules for collecting and providing digital evidence must be consistent in all jurisdictions around an international standard. The article analyzes such areas, compares universal and regional norms, and makes suggestions and recommendations.

Keywords: *information offence, international cooperation, regional cooperation, formal and informal cooperation.*

[*] Докторант кафедры ЮНЕСКО по правам человека и информационному праву юридического факультета Бакинского государственного университета

[**] Doctoral student of the UNESCO Department of Human Rights and Information Law, Faculty of Law, Baku State University