УГОЛОВНОЕ ПРАВО И УГОЛОВНЫЙ ПРОЦЕСС

ӘОЖ 347/9
DOI: 10.54649/2077-9860-2024-4-68-72

Н.Д. Тлешалиев [1]
[1] Ph.D, қауымдастырылған профессор,
Каспий қоғамдық университеті
Қазақстан Республикасы , Алматы қ.
E-mail: nurlan.tleshaliev@mail.ru

Б.С. Утаев[2]
[2]Каспий қоғамдық университеті
Қазақстан Республикасы, Алматы қ.

ҮШІНШІ ТҰЛҒАЛАРДЫҢ ИЕЛІГІНДЕГІ, ОНЫҢ ІШІНДЕ ШЕТЕЛДЕ ОРНАЛАСҚАН ДЕРЕКТЕРДІ ЖИНАУ ЕРЕКШЕЛІКТЕРІ

Аңдатпа

Мақалада үшінші тұлғалардың иелігіндегі, оның ішінде шетелде орналасқан деректерді жинау ерекшеліктерінің кейбір мәселелері қарастырылған. Жаһандану және белсенді ақпарат алмасу жағдайында үшінші тұлғалардың қолындағы деректерге қол жеткізу мәселесі мемлекеттік органдар үшін де, жеке тұлғалар үшін де өзекті бола бастады. Мұндай деректерді жинаудың құқықтық және технологиялық аспектілері, оның ішінде жеке ақпаратты қорғау және халықаралық стандарттарға сәйкестік мәселелері қарастырылады.

Түйінді сөздер: автоматтандыру, ақпараттандыру, қылмыстар, қылмыстық құқық бұзушылық, азаматтық талап, кінәні мойындау, электрондық мемлекеттік қызмет интеграторы, деректерді жинау, үшінші тұлғалар, жеке деректерді қорғау, жаһандану.

Н.Д.Тлешалиев[1]
[1] PhD, ассоциированный профессор,
Каспийский общественный университет,
Республика Казахстан, г. Алматы
E-mail: nurlan.tleshaliev@mail.ru

Б.С. Утаев[2]
[2]Каспийский общественный университет,
Республика Казахстан, г. Алматы

ОСОБЕННОСТИ СБОРА ДАННЫХ, НАХОДЯЩИХСЯ В РАСПОРЯЖЕНИИ ТРЕТЬИХ ЛИЦ, В ТОМ ЧИСЛЕ РАСПОЛОЖЕННЫХ ЗА ГРАНИЦЕЙ

Аннотация

Статья рассматривает некоторые аспекты особенности сбора данных, находящихся в распоряжении третьих лиц, в том числе расположенных за границей. В условиях глобализации и активного обмена информацией, проблема доступа к данным, находящимся у третьих лиц, становится

актуальной для государственных органов, а также и для частных лиц. Рассматриваются правовые, технологические аспекты сбора таких данных, включая вопросы защиты персональной информации, соблюдения международных стандартов.

Ключевые слова: автоматизация, информатизация, преступления, уголовный проступок, гражданский иск, признание вины, сервисный интегратор "электронного правительства", сбор данных, третьи лица, защита персональных данных, глобализация.

N.D. Tleshaliyev[1]
[1]Ph.D, Associate Professor,
Caspian Public University,
Republic of Kazakhstan, Almaty
E-mail: nurlan.tleshaliev@mail.ru

B.S. Utaev[2]
[2]Caspian Public University
Republic of Kazakhstan, Almaty

FEATURES OF COLLECTING DATA AT THE DISPOSAL OF THIRD PARTIES, INCLUDING THOSE LOCATED ABROAD

Annotation

The article examines some aspects of the features of collecting data held by third parties, including those located abroad. In the context of globalization and active exchange of information, the problem of access to data held by third parties becomes relevant for government agencies, as well as for individuals. The legal and technological aspects of collecting such data are considered, including issues of protecting personal information and compliance with international standards.

Keywords: automation, informatization, crimes, criminal offense, civil claim, admission of guilt, service integrator of "electronic government", data collection, third parties, protection of personal data, globalization.

Террористер мен ұйымдасқан қылмыскерлер өздерінің қылмыстық әрекеттерін жасау үшін интернетті, әлеуметтік желілерді және шифрлау функциясы бар жедел хабар алмасу жүйелерін көбірек қолданатындықтан, мұндай қызметтерді жеткізушілерден дәлелдер алу өте маңызды.

Қызмет көрсетушілерде сақталатын электрондық дәлелдемелер қылмыстың жасалғанын растау, айыптаушы байланыстар туралы мәліметтерді ашу және құқық бұзушылардың орналасқан жерін анықтау үшін пайдаланылуы мүмкін. Мұндай электрондық дәлелдемелерді алу белгілі бір кінәлі адамды құдалауды, сондай-ақ ауыр қылмыс жасаған адамдарды жауапқа тартуды қамтамасыз етуге көмектеседі.

К.Н. Евдокимов пікірінше, кейде тергеушінің деректерді сақтайтын құрылғыға тікелей немесе қашықтан қол жеткізуге және қажетті тергеу әрекеттерін жасауға мүмкіндігі болмайды. Егер деректер үлкен күрделі жабдықта сақталса (мысалы, интернет-қызметтердің ірі жеткізушісінің жабдықтарында), онда оларға кейде оның иелерінің көмегінсіз және көмегінсіз қол жеткізу мүмкін емес. Мұндай жағдайларда үшінші тұлғалармен, мысалы, жүйелік журналдар мен тіркеу деректері болуы мүмкін хостинг қызметтерін жеткізуші компаниямен ынтымақтастық орнату ұсынылады [1, 25 б.].

И.Ю.Лоскутов, үшінші тұлғалар қылмыстың жасалғанын көрсететін және қылмыстық істі тіркеуге негіз болатын электрондық дәлелдемелерді жинап, біраз уақыт сақтай алады. Интернеттің үлкен көлемін және желіде минут сайын жасалатын транзакциялар санын ескере отырып, шектеулі ресурстары бар құқық қорғау органдары бүкіл веб-кеңістікті қамти алмайды. Интернет желісіндегі кейбір деректер жалпыға қолжетімді болғанымен, басқа деректерге қол жеткізу шектеулі және оны алу үшін тіркеу деректерін білу қажет. Егер қылмыс жасау үшін жабық байланыс арналары (мысалы, электрондық пошта) пайдаланылса, онда мұндай арнаға қол жеткізе алатын адам құқық қорғау органдарына жүгінгенше, олардың бұл әрекеттерді қадағалауға немесе қажетті дәлелдерді алуға мүмкіндігі жоқ [2, 45 б.].

Кейде Интернет арқылы компьютерлік қылмыс жасаған адамды анықтау өте қиын. Көбінесе күдікті туралы тек оның IP –мекенжайы, MAC-мекен –жайы (ортаға кіруді басқару Мекен-жайы (Media Access Control address) - бұл желідегі құрылғыны анықтайтын ерекше Сан), электрондық пошта мекенжайы, домендік атау немесе интернет бүркеншік аты ("ник"). Жеке тұлғаны IP мекен-жайы бойынша анықтау үшін маманға интернет-провайдердің қолында болатын мәліметтер қажет. Интернет қызметтерін (электрондық пошта, хостинг қызметтері) жеткізушілер көбінесе қылмыскердің виртуалды тұлғасы мен белгілі бір жеке тұлға арасында байланыс орнатуға көмектесетін жалғыз ақпарат көзі болып табылады. Сондықтан Тәуелсіз деректер иелері көбінесе тергеудің негізгі буыны болып табылады [3].

Қылмыскерлерді анықтау үшін дерекқорды пайдалану қылмыстық процестің стандартты процедурасы болып табылады. Көптеген елдердегі саусақ іздері мен ДНҚ дерекқорлары тергеудің сәтті болуын қамтамасыз ететін негізгі нүктелердің бірі болып табылады. Сонымен қатар, электронды дәлел ретінде пайдаланылуы мүмкін мәліметтер базасы құқық қорғау органдарына немесе мемлекеттік ұйымдарға емес, Интернет желісінің жұмысын қамтамасыз ететін көптеген жеке компанияларға тиесілі. Бұл мұндай компаниялармен ынтымақтастықты сақтау өте маңызды екенін білдіреді. Сонымен қатар, пайдаланушылардың сәйкестендіру деректері туралы орталықтандырылған ақпараттың болмауына байланысты интернет-провайдерлерге бірыңғай деректер алмасу стандарттарын әзірлеу өте қиын. Әрқайсысы сұралған деректерді тіркеудің, деректерді ұсынуға сұраныстардың басымдылығын анықтаудың және желідегі құқық бұзушылармен күресудің өзіндік әдістерін қолданады [4].

Егер құқық қорғау органдары мен деректердің тәуелсіз иесі арасында тұрақты диалог орнатылса, онда бұл түсініспеушіліктерді болдырмауға көмектеседі, деректерді ұсынуға сұраныстардың басымдылығын анықтауға мүмкіндік береді және ынтымақтастық мәдениетін нығайтуға ықпал етеді. Сонымен қатар, құқық қорғау органдарымен сенімді қарым-қатынас орнатқан қызмет көрсетушілер байланыс орнатуға және анықталған бұзушылықтар туралы хабарлауға дайын [5].

Құқық қорғау органдарына интернет-қызметтерді жеткізушілермен және Интернет желісін пайдаланушылар туралы деректерге ие басқа адамдармен тұрақты кездесулер өткізу ұсынылады. Бұл кездесулерді ынтымақтастықтың өзекті мәселелерін талқылау үшін ғана емес, сонымен қатар ықтимал тенденциялар мен қауіптерді Стратегиялық талдау үшін де пайдалануға болады. Сонымен қатар, құқық қорғау органдары мен жеке компаниялардың өкілдері үшін бірлескен тренингтер өткізуге болады: бұл тараптарға өзара көзқарастардан арылуға көмектеседі және сенімді атмосфераны құруға ықпал етеді.

"Байланыс туралы" Қазақстан Республикасы Заңының 2-бабының 18-тармағына сәйкес: "байланыс операторы-Қазақстан Республикасының аумағында тіркелген, байланыс қызметтерін көрсететін және (немесе) байланыс желілерін пайдаланатын жеке немесе заңды тұлға [6].

Қазақстан Республикасы цифрлық даму, Қорғаныс және аэроғарыш өнеркәсібі министрлігінің "Телекоммуникация комитеті" республикалық мемлекеттік мекемесінің 06.12.2019 жылғы №28-1-28/2734 жауабына сәйкес байланыс операторы байланыс қызметтерін көрсету жөніндегі қызмет басталған сәттен бастап "байланыс туралы" Заңның 16-1-бабы тәртібімен уәкілетті органға хабарлама жібереді. Аталған комитеттің қоса берілген кестесіне сәйкес Қазақстанда 119 байланыс операторы тіркелген.

"Байланыс операторларының абоненттер туралы қызметтік ақпаратты жинауды және сақтауды жүзеге асыру қағидаларын бекіту туралы" 2010 жылғы 30 наурыздағы № 246 Үкімет қаулысының 5-бабына сәйкес оператор абоненттер туралы қызметтік ақпаратты екі жыл бойы жинауды және сақтауды қамтамасыз етеді, олар аяқталғаннан кейін ақпарат жойылады. Оператор абоненттер туралы қызметтік ақпаратты жинау және сақтау жөніндегі міндеттерді бұзғаны үшін Қазақстан Республикасының заңдарында көзделген жауаптылықта болады [7].

Алайда, біздің елімізде қылмыстық құдалау органы байланыс операторларына заңнамалық деңгейде жүгіну кезінде үлкен кедергіге ие, атап айтқанда, байланыс операторлары қылмыстық құдалау органы мен қадағалау органының қызметтік ақпарат берудегі заңды талаптарын елемейді.

"Байланыс туралы" Қазақстан Республикасының 2004 жылғы 05 шілдедегі

№567 Заңы Қазақстан Республикасының аумағында байланыс саласындағы қызметтің құқықтық негіздерін белгілейді, осы қызметті реттеу жөніндегі мемлекеттік органдардың өкілеттіктерін, байланыс қызметтерін көрсететін немесе пайдаланатын жеке және заңды тұлғалардың құқықтары мен міндеттерін айқындайды.

Қазақстан Республикасының "Байланыс туралы" №567 Заңының 15-бабының 1-бөлігіне сәйкес өз қызметін республика аумағында жүзеге асыратын байланыс операторлары Қазақстан Республикасының заңнамасына сәйкес жедел-іздестіру қызметін, байланыс желілерінде қарсы барлау қызметін жүзеге асыратын органдарға жедел-іздестіру, қарсы барлау іс-шараларын жүргізудің ұйымдастырушылық және техникалық мүмкіндіктерін қамтамасыз етуге міндетті. барлық байланыс желілері, абоненттер туралы қызметтік ақпаратқа қол жеткізу [6].

ҚР "Байланыс туралы" Заңының 15-бабына сәйкес заң шығарушы байланыс желілерінде жедел-іздестіру және қарсы барлау іс-шараларын жүргізудің ұйымдастырушылық және техникалық мүмкіндіктерін жедел-іздестіру және қарсы барлау қызметін жүзеге асыратын органдарға ғана ұсынады [6].

"Байланыс туралы" ҚР Заңының 2 - бабының 2-тармағына сәйкес абоненттер туралы қызметтік ақпарат-байланыс желілерінде қарсы барлау қызметін және жедел-іздестіру іс-шараларын жүргізу мақсаттарына ғана арналған және өзіне: 1). Абоненттік нөмірлер иелерінің жеке сәйкестендіру нөмірлері (жеке тұлғалар үшін) немесе бизнес-сәйкестендіру нөмірлері (заңды тұлғалар үшін) туралы мәліметтерді қоса алғанда, абоненттік нөмірлертуралыақпарат;2).Ұялыбайланыстың абоненттік құрылғылары иелерінің жеке сәйкестендіру нөмірлері (жеке тұлғалар үшін) немесе бизнес-сәйкестендіру нөмірлері (заңды тұлғалар үшін) туралы мәліметтерді қоса алғанда, ұялы байланыстың абоненттік құрылғыларының сәйкестендіру кодтары туралы ақпарат; 3). Биллингтік мәліметтер (абоненттерге алынған қызметтер туралы мәліметтер); 4). Техникалық регламенттің талаптарына сәйкес желідегі абоненттік құрылғының орналасқан жері; 5). Деректерді беру желісіндегі мекенжайлар; 6). Деректерді беру желісіндегі интернет-ресурстарға жүгіну мекенжайлары; 7). Интернет-ресурстың идентификаторлары; 8). Деректер желісінің хаттамалары [6].

"Байланыс туралы" заңда сотқа дейінгі тергеп-тексеруді немесе прокурорлық қадағалауды жүзеге асыратын адамдардың құқықтары жоқ. Сотқа дейінгі тергеп-тексеруді және прокурорлық қадағалауды жүзеге асыратын адамдардың "байланыс туралы" заңда болмауы байланыс операторларының абоненттер туралы заңды талап етілетін қызметтік ақпаратты беруден негізсіз бас тартуына негіз болып табылады. Дәлелді бөлімде байланыс операторлары сотқа дейінгі тергеп-тексеруді және прокурорлық қадағалауды жүзеге асыратын адамдардың талабы жедел-іздестіру іс-шараларын және қарсы барлау қызметін жүргізумен байланысты болмағандықтан, байланыс операторы талапты орындаудан бас тартуға мәжбүр екенін көрсетеді [8].

Қазақстан Республикасы қылмыстық процестік кодексінің 34-бабының 5-бөлігіне сәйкес " қылмыстық құдалау органының заңға сәйкес қойған талаптары барлық мемлекеттік органдардың, ұйымдардың, лауазымды адамдар мен азаматтардың орындауы үшін міндетті және ол белгілеген мерзімде, бірақ үш тәуліктен кешіктірілмей орындалуы тиіс. Көрсетілген талаптарды дәлелсіз себептермен орындамау заңмен белгіленген жауапкершілікке әкеп соғады [9].

Осыған байланысты, қылмыстық құдалау органдары мен қадағалау органының абоненттер туралы қызметтік ақпарат алу құқықтарын нақты көрсете отырып, "байланыс туралы" Қазақстан Республикасының Заңына өзгеріс енгізу қажеттілігі туындайды.

"Кселл" АҚ, "Сеть Казахстан" ЖШС, "BTCOM infocommunications" ЖШС, "ASTEL" АҚ және басқа да байланыс операторларының жауаптарына сәйкес абоненттер туралы қызметтік ақпаратты жинау және сақтау жүйелеріне қол жеткізу ҚР ҰҚК-не берілді, осыған байланысты абоненттер туралы қызметтік ақпаратты бере алмайды, өйткені олар қол жеткізе алмайды.

Қазақстан Республикасы Ұлттық қауіпсіздік Комитеті уәкілетті департаментінің 23.02.2021 жылғы шығыс үшін берген жауабына сәйкес. № 5/1/7473 қызығушылық танытқан IP-мекен-жаймен байланыс орнатқан "Кселл" АҚ абоненттеріне қатысты ақпарат алынды. "Инженерлік-техникалық орталық" АҚ байланыс операторының желісінде деректерді беру желісінде қызметтік ақпаратты жинау және сақтау құралдары жоқ. Осыған байланысты сұралған ақпаратты алу үшін көрсетілген операторды мекен-жайына жүгіну қажет.

Ақпараттық қауіпсіздік инциденттерін зерттеу тәжірибесін арттыру мақсатында қылмыстық құқықтағы қылмыстық құдалау органдары диссертант барлық тіркелген Ақпараттық қауіпсіздік инциденттерін зерттеуге және қылмыстық құқық жазықтығында одан әрі зерттеу үшін мәліметтерді мамандандырылған және құқық қорғау органдарына беруге бағытталған ақпараттық қауіпсіздікті ұлттық үйлестіру орталығының қызметін кеңейту бөлігінде "Ақпараттандыру туралы" Заңға өзгерістер енгізуді ұсынады.

Пайдаланылған кайнар көздерінің тізімі:

1. Евдокимов К.Н. Актуальные вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации //Российский следователь. – 2015.–№ 10. – С.25-32.
2. Лоскутов И.Ю. Преступления в сфере информационных технологий в проекте новой редакции Уголовного кодекса Республики Казахстан// Сборник Материалов Международно-практической конференции «Актуальные вопросы развития уголовного законодательства в рамках разработки нового уголовного кодекса РК» (Алматы, 20 сентября 2012 года). – С. 45-54.
3. Ақпараттандыру туралы Қазақстан Республикасының Заңы 2015 жылғы 24 қарашадағы № 418-V ҚРЗ.
4. Киберқауіпсіздік тұжырымдамасын ("Қазақстанның киберқалқаны") бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы.
5. Ақпараттандыру саласындағы ақпараттық қауіпсіздік https://egov.kz/cms/kk/cyberspace
6. Байланыс туралы Қазақстан Республикасының 2004 жылғы 5 шілдедегі N 567 Заңы.
7. "Байланыс операторларының абоненттер туралы қызметтік ақпаратты жинауды және сақтауды жүзеге асыру қағидаларын бекіту туралы" 2010 жылғы 30 наурыздағы № 246 Үкімет қаулысы
8. Об утверждении Плана мероприятий по реализации Концепции кибербезопасности ("Киберщит Казахстана") до 2022 года Постановление Правительства Республики Казахстан от 28 октября 2017 года № 676. www.adilet.kz
9. Қазақстан Республикасының Қылмыстық-процестік кодексі Қазақстан Республикасының Кодексі 2014 жылғы 4 шілдедегі № 231-V ҚРЗ.

References:

1. Evdokimov K.N. Aktualnye voprosy ugolovno-pravovoy kvalifikatsii prestupleny v sfere kompyuternoy informatsii //Rossysky sledovatel. – 2015.–№ 10. – S.25-32.
2. Loskutov I.Yu. Prestupleniya v sfere informatsionnykh tekhnology v proyekte novoy redaktsii Ugolovnogo kodeksa Respubliki Kazakhstan// Sbornik Materialov Mezhdunarodno-prakticheskoy konferentsii «Aktualnye voprosy razvitiya ugolovnogo zakonodatelstva v ramkakh razrabotki novogo ugolovnogo kodeksa RK» (Almaty, 20 sentyabrya 2012 goda). – S. 45-54.
3. Aқparattandyru turaly Қazaқstan Respublikasynyң Zaңy 2015 zhylғy 24 қarashadaғy № 418-V ҚRZ.
4. Kiberқauipsizdik tұzhyrymdamasyn ("Қazaқstannyң kiberқalқany") bekitu turaly Қazaқstan Respublikasy Ykimetinің 2017 zhylғy 30 mausymdaғy № 407 қaulysy.
5. Aқparattandyru salasyndaғy aқparattyқ қauipsizdik https://egov.kz/cms/kk/cyberspace
6. Baylanys turaly Қazaқstan Respublikasynyң 2004 zhylғy 5 shildedegi N 567 Zaңy.
7. "Baylanys operatorlarynyң abonentter turaly қyzmettik aқparatty zhinaudy zhәne saқtaudy zhүzege asyru қaғidalaryn bekitu turaly" 2010 zhylғy 30 nauryzdaғy № 246 Ykimet қaulysy
8. Ob utverzhdenii Plana meropriyaty po realizatsii Kontseptsii kiberbezopasnosti ("Kibershchit Kazakhstana") do 2022 goda Postanovleniye Pravitelstva Respubliki Kazakhstan ot 28 oktyabrya 2017 goda № 676. www.adilet.kz
9. Қazaқstan Respublikasynyң Қylmystyқ-protsestik kodeksi Қazaқstan Respublikasynyң Kodeksi 2014 zhylғy 4 shildedegi № 231-V ҚRZ.