RAQAMLI TAHDIDLARGA QARSHI HUQUQIY MEXANIZMLARNING SAMARADORLIGI

To‘lqinova Visola Ulug‘bek qizi
Toshkent davlat yuridik universiteti
Jinoiy odil sudlov fakulteti talabasi
E-mail: visolatolqinova05@gmail.com
https://doi.org/10.5281/zenodo.20393274

ARTICLE INFO

Qabul qilindi: 22-may 2026 yil
Ma’qullandi: 24-may 2026 yil
Nashr qilindi: 26-may 2026 yil

KEYWORDS

kiberjinoyatchilik, jinoyat tarkibi, raqamli dalil, virtual jinoyat, Budapesht konvensiyasi, GDPR, axborot xavfsizligi, jinoiy javobgarlik, atribusiya, kiberforensika.

ABSTRACT

Kiberjinoyatchilik bugun O‘zbekiston fuqarolarining mol-mulkiy va shaxsiy huquqlariga eng ko‘p zarar yetkazayotgan jinoyat turlaridan biriga aylandi. Amaldagi jinoyat qonunchiligi bu tahdidlarga to‘liq javob bera olmayapti: jinoyat tarkibini aniqlashda terminologik noaniqlik, elektron dalillarni to‘plashda protsessual bo‘shliqlar, transmilliy jinoyatchilarni jinoiy javobgarlikka tortishda xalqaro hamkorlik mexanizmlarining sustligi — bularning barchasi tizimli muammo sifatida namoyon bo‘lmoqda. Maqolada jinoyat huquqi ta'limotining to‘rt asosiy elementi raqamli muhit sharoitida qayta tahlil qilinadi; milliy qonunchilikning zaif nuqtalari aniq normalar va sud amaliyoti misolida ko‘rsatib beriladi; xalqaro tajriba asosida amaliy qonunchilik takliflari ishlab chiqiladi.

Bugungi kunda O‘zbekiston Respublikasida har yili o‘n minglab fuqaro kiberjinoyatchilik qurboniga aylanmoqda — banklardan noqonuniy pul o‘tkazish, ijtimoiy tarmoqlarda shaxsiyatni o‘g‘irlash, soxta veb-saytlar orqali firibgarlik bu muammoning faqat ko‘zga ko‘ringan qismi, xolos. Biroq jinoyat huquqi bu yangi hodisani qamrab olishga har doim ham tayyor emas, amaldagi qonun normalari ko‘plab hollarda kiberjinoyatchi ustidan ish qo‘zg‘atish uchun yetarli asos bermaydi, elektron dalillarni protsessual tartibda to‘plash esa hali ham nazariy muammo bo‘lib turibdi.

Mamlakatimizning yetakchi olimlardan biri M. H. Rustambayev o‘zining ko‘p jildli “O‘zbekiston Respublikasi jinoyat huquqi kursi” kitobida jinoyat tarkibining to‘rt elementi — obyekt, obyektiv tomon, subyekt va subyektiv tomon — barcha ijtimoiy xavfli qilmishlar uchun asosiy me'zon ekanligini ta'kidlaydi[1]. Aynan mana shu to‘rt element prizmasi orqali kiber-xurujlarni jinoyat sifatida malakalashtirish masalasi bugungi kunda eng dolzarb ilmiy-amaliy masalaga aylanib bormoqda.

Xalqaro tajribaga nazar solsak, D.S.Wall kiberjinoyatchilikning an'anaviy jinoyatchililikdan asosiy farqini aniqlagan: jismoniy olam jinoyatida jabrlanuvchi va jinoyatchi orasida jismoniy yaqinlik bo‘lishi shart, raqamli olamda esa jinoyatchi boshqa qit'adan turib minglab fuqaroga bir vaqtda zarar etkazishi mumkin[2]. Bu holat “jinoyat joyi” tushunchasini,

jinoiy jarayonning territoriyalik tamoyilini va hatto jinoiy javobgarlik sub'ektini aniqlashda asosiy qiyinchilikni tug‘diradi. Ushbu muammo O‘zbekiston amaliyotida ham o‘z aksini topmog‘i lozim.

Maqolaning ilmiy muammosi shundaki, jinoyat huquqining an'anaviy metodologik ko‘rinishi kiberjinoyatchilikka nisbatan qay darajada samarali bo‘la oladi va milliy qonunchilik rivojlanib borayotgan raqamli tahdidlar bilan raqobatlasha olishini tahlil qilamiz.

Metodologiya

Tadqiqot bir-birini to‘ldiruvchi beshta ilmiy metod asosida olib borildi. Qiyosiy-huquqiy metod yordamida O‘zbekiston jinoyat qonunchiligi GDPR reglamenti va Budapesht konvensiyasi talablari bilan taqqoslandi, milliy va xalqaro modellar orasidagi umumiy hamda farqli jihatlar aniqlandi. Dogmatik metod orqali JK'ning 141^2-moddasi, “Shaxsga doir ma'lumotlar to‘g‘risida”gi qonunning 5-moddasi va Oliy Sud Plenumining 18-sonli qarori grammatik, tizimli va maqsadli talqin usullari asosida tahlil qilindi. Tizimli tahlil metodi esa Konstitutsiya, Jinoyat kodeksi maxsus qonun va Budapesht konvensiyasi o‘rtasidagi ichki bog‘liqliklarni, shuningdek ular orasidagi huquqiy bo‘shliqlarni ko‘rsatib berishga xizmat qildi. Induktiv metod yordamida CNIL/Google ishi, deepfake firibgarliklari va SIM-swap jinoyatlari kabi alohida huquqiy hodisalardan umumiy nazariy xulosalar chiqarilib, O‘zbekiston uchun qonunchilik modeli taklif etildi. Nihoyat, tarixiy-huquqiy metod orqali shaxsiy ma'lumotlarni himoya qilish qonunchiligining 1970-yillardagi Hesse modelidan (Germaniya) GDPR'ga qadar bo‘lgan evolyutsiyasi o‘rganildi va O‘zbekiston qonunchiligining rivojlanish bosqichlari shu asosda baholandi. Birlamchi manbalar sifatida normativ-huquqiy hujjatlar, sud amaliyoti va xalqaro shartnomalar; ikkilamchi manbalar sifatida milliy va xorijiy ilmiy adabiyotlardan foydalaniladi.

Natijalar va muhokama

A.Sh.Muxammedov ta'kidlaganidek, virtual jinoyatchilik zamonaviy axborot texnologiyalarining keng qo‘llanilishi natijasida shakllangan yangi turdagi ijtimoiy xavfli xatti-harakatlar bo‘lib, ular an'anaviy jinoyat huquqidagi jinoyatlar bilan har doim ham mos tushmaydi. Olim virtual jinoyatlarning uchta asosiy o‘ziga xos xususiyatini ajratib ko‘rsatadi, bular jismoniy chegara yo‘qligi, jinoyat izlarini yo‘q qilish qulayligi va bir harakat orqali bir vaqtning o‘zida ko‘plab shaxslarga zarar etkazish imkoni hisoblanadi.

Bu xususiyatlar terminologik muammoni ham keltirib chiqaradi. O‘zbekiston qonunchiligida “kiberjinoyat”, “kompyuter jinoyati”, “axborot texnologiyalari sohasidagi jinoyat” atamalari bir-birining o‘rnida befarq ishlatilmoqda. Biroq A.Sh.Muxammedov asosli ravishda ko‘rsatib berganidek, bu atamalar hajm va qamrov jihatdan bir-biridan farq qiladi: kiberjinoyat eng keng tushuncha bo‘lib, kompyuter tizimi vosita yoki nishon vazifasini o‘tagan barcha jinoyatlarni o‘z ichiga oladi [3]. Shu o‘rinda ta'kidlash joizki, O‘zbekiston Respublikasi Jinoyat kodeksida hali “kiberjinoyat” atamasi mustaqil huquqiy kategoriya sifatida o‘z ifodasini topmagan, bu esa amaliyotda jinoyatni to‘g‘ri malakalashtirish yo‘lida asosiy to‘siqlardan biriga aylanib bormoqda.

O.N.O‘rinqulov esa IIV Akademiyasi tadqiqotchisi sifatida amaliy tadqiqoti davomida shunday kiberjinoyatchilik rivojlanishi “texnologik bo‘shliq — huquqiy bo‘shliq — ijtimoiy zaiflik — tezkor moslashuv” modeli bo‘yicha sodir bo‘layotgani haqida ilmiy xulosaga keldi [4]. Bu model shuni anglatadiki, har safar texnologiya yangi imkoniyat ochganda — masalan, deepfake yoki SIM-swap — jinoyatchilar qonunchilikdagi bo‘shliqdan foydalanib oladi,

vaholanki huquqiy tartibga solish shu bo‘shliqni yopguncha sezilarli vaqt o‘tib ketadi. FBI ma'lumotlariga ko‘ra, 2024-yilda eng ko‘p tarqalgan internet jinoyatlari sifatida phishing/spoofing, tovlamachilik va shaxsiy ma'lumotlardan noqonuniy foydalanish qayd etilgan [4]. Bu hodisa O‘zbekistonda ham keng tarqalgan.

M. H. Rustamboyev jinoyat tarkibini to‘rt elementning yig‘indisi sifatida belgilaydi: obyekt (himoya qilinadigan ijtimoiy munosabatlar), obyektiv tomon (tashqi ko‘rinish), subyekt (javobgar shaxs), subyektiv tomon (aybning mavjudligi)[1]. Kiberjinoyatlar bu sxemaga qanday joylashadi? Ushbu savolga javob berish uchun har bir elementni alohida ko‘rib chiqish lozim. Obyekt masalasida O‘zbekiston Respublikasi Konstitutsiyasining 31-moddasi 3-qismida shaxsiy ma'lumotlarni himoya qilish huquqi alohida konstitutsiyaviy kafolat sifatida mustahkamlanganligi muhim qadamdir. Solove bu masalada shunday asosli fikrni olg‘a suradiki, bu axborot daxlsizligi — bu shunchaki sirning saqlanishi emas, balki shaxsning o‘ziga tegishli ma'lumotlar oqimi ustidan nazorat qilish huquqi [5]. Bunday yondashuv huquqiy nuqtayi nazardan kiberjinoyat obyekt sifatida nafaqat moddiy zarar, balki shaxsning axborot huquqiga yetkazilgan zarar ham e'tirof etilishi lozimligini ko‘rsatadi. Obyektiv tomon masalasida kiberjinoyatlar an'anaviy jinoyatlardan tubdan farq qiladi. J. Clough ta'kidlaganidek, kiber hujumda jinoyatchi ko‘pincha ketma-ket bog‘liq bosqichlarda harakat qiladi, jumladan, phishing xatini yuborish, foydalanuvchi ma'lumotlarini to‘plash, tizimga kirish va ma'lumotlarni eksfiltratsiya qilishdir [6]. Bu zanjirning har bir bo‘g‘ini mustaqil jinoyat tarkibini tashkil qilishi yoki ularning barchasi yig‘indisi bir jinoyat sifatida baholanishi mumkin. Ammo O‘zbekiston Jinoyat kodeksida bu ketma-ketlikni yaxlit qamrab oladigan maxsus norma mavjud emas. Subyekt masalasida ya'ni jinoyatchi kim degan savolda kiberjinoyatchilik «atribusiya» deb ataluvchi eng murakkab muammoni yuzaga keltiradi ya’ni Wall bu muammoni “past ta'sirli, ko‘p jabrlanuvchili” jinoyatning yangi avlodi deb ta'riflagan edi [2]. Yar va Steinmetz esa raqamli identifikatsiya o‘g‘irligining yangi shakllarini ko‘rib chiqib, VPN, TOR, botnet tarmoqlari va anonim kriptovalyuta vositasida jinoyatchi o‘zini deyarli tamoman yashira olishini ko‘rsatib bergan [12]. O‘rinqulov milliy statistika asosida shuni qayd etadiki, kiberjinoyatlarning katta qismi elektron dalillarni to‘plash va saqlash amaliyoti yetarli darajada standartlashtirilmaganligi uchun hali ham aniqlanmagan holda qolayotganini ta’kidlagan [4] Subyektiv tomon — aybdorlik shakllari masalasida O.S.Kerr muhim tadqiqotni ilgari suradi ya’ni ruxsatsiz tizimga kirish ko‘pincha “to‘g‘ridan-to‘g‘ri qasd” bilan amalga oshiriladi va buni isbotlash nisbatan oson, lekin shu kirish orqali yetkazilgan zarar qaysi maqsad bilan amalga oshirilgani — o‘g‘irlikmi, josuslikmi yoki shunchaki “qiziquvchanlik” bilan kirish-bu masalalarni sudda isbotlash juda qiyin [8].

O‘zbekiston Respublikasi JK'ning 141^2-moddasi shaxsga doir ma'lumotlarni noqonuniy qayta ishlash uchun jinoiy javobgarlikni nazarda tutadi. Biroq bu moddaning dispozitsiyasida “texnik vositalar” atamasi ishlatilgan bo‘lib, amaliyotda ushbu tushuncha qanday doirada talqin qilinishi noaniq qolmoqda. Z.N.Eshdavlatova o‘zining ilmiy asarlarida normativ bazaning yaxshi yozilgan bo‘lishining o‘zi yetarli emas — huquqni muhofaza qiluvchi organlar tomonidan elektron dalillarni to‘plashda tizimli muammolar saqlanib qolmoqdaligini bayon etgan [9]. Muammoni yanada chuqurroq tahlil qiladigan bo‘lsak, O‘zbekiston Respublikasi Oliy Sudi Plenumining «Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida»gi 18-sonli qarorining 22-bandida «axborot tizimidan foydalanib sodir etilgan firibgarlik» tushunchasi batafsil izohlanadi — ammo bu izohda ham sun'iy intellekt va deepfake kabi zamonaviy

texnologiyalar hech qayerda tilga olinmagan. Jinoyat protsessi nuqtayi nazaridan esa muammo yanada keskin ko‘rinadi. Clough ta'kidlaganidek, elektron dalillar an'anaviy ashyoviy dalillardan farqli ravishda bir necha soniyada o‘chirilishi, masofadan ko‘chirilishi yoki sirli ravishda yo‘naltirilishi mumkin [10]. Kerr bu masalada elektron dalillarni to‘plash, saqlash va sudda taqdim etish uchun maxsus protsessual qoidalar bo‘lmasa, kiberjinoyatchi sudga tortilishi deyarli imkonsiz ekanligini ta’kidlagan [11]. Aynan mana shu nuqta O‘zbekiston Jinoyat-protsessual huquqi sohasi ham ilmiy izlanishlarni talab qiladi.

2001-yildagi Budapesht konvensiyasi kiberjinoyatchilikka qarshi kurashda davlatlar o‘rtasidagi huquqiy hamkorlikning asosi hisoblanadi. Konvensiyani ratifikatsiya qilgan davlatlarda kiberjinoyatchilarni jinoiy javobgarlikka tortish imkoni sezilarli darajada yuqori, chunki ular raqamli dalillarni xalqaro tarmoq orqali tezda olish, xorijiy serverlardan ma'lumot so‘rash va jinoyatchilar ekstraditsiyasi mexanizmlaridan foydalana oladi. O‘zbekiston Respublikasi ushbu konvensiyani hali ratifikatsiya qilmagan — bu esa mamlakatimizni transmilliy kiberjinoyatlarga qarshi kurashda jiddiy cheklashlar bilan yuzlashtirmoqda. 2019-yilda Fransiya ma'lumotlarni himoya qilish organi (CNIL) Google kompaniyasiga 50 million yevro miqdorida jarima qo‘llagan. Bu voqeaning mohiyati shundaki, GDPR — Yevropa Ittifoqining «Umumiy ma'lumotlarni himoya qilish reglamenti» — nafaqat ma'muriy, balki ma'naviy saboq beradi, shuningdek, yirik raqamli korporatsiyalar ham shaxsiy ma'lumotlar sohasida millionlab yevrolik javobgarlikdan ozod emas [12]. Solove va Hartzog bu voqeani tahlil qilib, foydalanuvchi roziligini olishning ko‘pincha shakliy-rasmiy xarakter kasb etishini va bu esa huquqiy himoyani zaiflashtirishi masalasini keskin ko‘tarishgan [13]. O‘zbekiston uchun bu tajriba shuni ko‘rsatadiki, ma'muriy sanksiyalar va jinoiy javobgarlikning parallel tizimi ko‘proq samaraga erishish imkonini beradi. “Shaxsga doir ma'lumotlar to‘g‘risida”gi qonunining 5-moddasida belgilangan prinsiplar ya’ni qonuniylik, aniqlik, maxfiylik, subyektlar huquqlarining tengligi — mazmun jihatdan GDPR talablariga yaqinligi mustahkom poydevor bo‘lishi mumkin, lekin poydevordan bino qurilmasa, u poydevorligicha qolaveradi. Qonun matnining mukammalligi va uni tatbiq etishdagi instituttsional salohiyat — bu ikki narsa bir-biriga teng emasligini qonunchilik tan olishi lozim.

Xulosa

Olib borilgan tahlil shuni ko‘rsatadiki, kiberjinoyatchilik an'anaviy jinoyat huquqi kategoriyalarini inkor etmaydi, balki ularni yanada chuqurlashtirilgan va yangilangan mazmun bilan boyitishni talab qiladi. A.Sh.Muxammedov va O.N.O‘rinqulov ishlarida belgilangan asosiy muammolar — terminologik noaniqlik, protsessual bo‘shliqlar, elektron dalillar bilan ishlash standartlarining yo‘qligi, transmilliy jinoyatchilar ustidan ish yuritishdagi qiyinchiliklar — faqat akademik muammo emas, balki kundalik amaliyotda yuz minglab fuqaroni bevosita ta'sir qiluvchi holatlar ekanligini unutmaslik lozimligini alohida ta’kidlagan. Yuqoridagilardan kelib chiqib, quyidagi tavsiyalar ilgari suriladi. *Birinchidan,* Kiberjinoyatlarga qarshi Budapesht konvensiyasini ratifikatsiya qilish, *ikkinchidan,* Jinoyat kodeksiga kiberjinoyatlarning asosiy turlarini qamrab oladigan maxsus moddalar majmuasini kiritish ya’ni ruxsatsiz tizimga kirish, zararli dasturlarni tarqatish, deepfake orqali firibgarlik — bularning har biri alohida jinoyat tarkibiga ega bo‘lishi lozimligi, *uchinchidan,* Jinoyat-protsessual kodeksga elektron dalillarni to‘plash, saqlash, tekshirish va sudga taqdim etish tartibi to‘g‘risida alohida bob kiritish, *to‘rtinchidan,* “Shaxsga doir ma'lumotlar to‘g‘risida”gi qonunni foydalanuvchi roziligini olish mexanizmi jihatidan GDPR andozasiga yaqinlashtirish, *beshinchidan,* kiberforensika sohasida

maxsus mutaxassislar tayyorlash dasturlarini kengaytirish va ularning tergov jarayonidagi vakolatlarini qonun darajasida belgilash takliflari beriladi. Qonunchilik mexanizmi raqamli dunyo bilan bir tezlikda rivojlanmasa, u orqada qolaveradi. Orqada qolgan qonun esa jinoyatchiga emas, jabrlanuvchiga zarar keltiradi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Rustamboyev M. H. O‘zbekiston Respublikasi jinoyat huquqi kursi. 5 tomlik. — Toshkent: TDYU, 2006–2010. https://library.tsul.uz/uz/books/4103
2. Wall D. S. Cybercrime: The transformation of crime in the information age. — Cambridge: Polity Press, 2007. https://ssrn.com/abstract=1066922
3. Muxammedov A. Sh. Virtual jinoyatchilik tushunchasi va uning jinoiy-huquqiy tahlili // Universal Journal of Law, Finance and Applied Sciences. — 2025. — Vol. 3, Issue 29 https://scienceresearch.org.uz/index.php/UJLFAS/article/download/723/1023/1437
4. O‘rinqulov O. N. Kiberjinoyatlarning kelib chiqish va rivojlanish omillari tahlili // Scientific Review of the Problems and Prospects of Modern Science and Education: 13th international conference. — Great Britain, 2025. https://e-conferences.org/index.php/GB/article/download/886/1440/1659
5. Solove D. J. Understanding Privacy. — Cambridge, MA: Harvard University Press, 2008. ISBN: 978-0-674-027 72-5
6. Clough J. Principles of Cybercrime. 2nd ed. — Cambridge: Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781139540803
7. Yar M., Steinmetz K. F. Cybercrime and Society. 3rd ed. — London: SAGE Publications, 2019. ISBN: 978-1-5264-4065-5.
8. Kerr O. S. Computer Crime Law. 5th ed. — St. Paul: West Academic Publishing, 2018.
9. Eshdavlatova Z. N. Raqamli texnologiyalar davrida shaxsiy ma'lumotlarni muhofaza qilishning huquqiy asoslari // Ekonomika i sotsiumi. — 2022. — № 5(96)-2. https://iupr.ru/
10. Clough J. Principles of Cybercrime. 2nd ed. — Cambridge: Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781139540803
11. Kerr O. S. Computer Crime Law. 5th ed. — St. Paul: West Academic Publishing, 2018.
12. CNIL Restricted Committee. Deliberation SAN-2019-001 of 21 January 2019 — Financial penalty of 50 million euros against Google LLC. European Data Protection Board, 2019. https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en
13. Solove D. J., Hartzog W. Breached! Why Data Security Law Fails and How to Improve It. — Oxford: Oxford University Press, 2022.