AXBOROT TEXNOLOGIYALARIDAN FOYDALANIB SODIR ETILADIGAN FIRIBGARLIK JINOYATINING OBYEKTIV TOMONINI BELGILASHDAGI AMALIY MUAMMOLAR

Xalmuratov Muxammed Jumabayevich
Berdaq nomidagi Qoraqalpoq davlat universiteti stajyor-o'qituvchisi
e-mail: xalmuratovmuxammed@gmail.com

Annotatsiya: Ushbu maqola raqamli transformatsiya va virtual makon sharoitida axborot texnologiyalaridan foydalangan holda sodir etiladigan firibgarlik jinoyatlarining obyektiv tomonini kvalifikatsiya qilishning fundamental nazariy va amaliy muammolarini tadqiq etishga bag'ishlangan.

Kalit so'zlar: Kiberfiribgarlik, obyektiv tomon, aldash, axborot texnologiyalari, kiberxavfsizlik, kripto-aktivlar.

Zamonaviy jinoyat huquqi dogmatikasida axborot texnologiyalaridan foydalanib sodir etiladigan firibgarlik jinoyatining obyektiv tomonini to'g'ri kvalifikatsiya qilish tergov va sud amaliyotidagi eng ziddiyatli masalalardan biri bo'lib qolmoqda. An'anaviy mulkiy jinoyatlardan farqli o'laroq, kiber-makonda jinoyatchi va jabrlanuvchi o'rtasida to'g'ridan to'g'ri vizual yoki jismoniy muloqotning (kontaktning) mavjud emasligi sababli, qilmishning xususiyati, sodir etish usuli hamda jinoiy harakat va ijtimoiy xavfli oqibat o'rtasidagi sababiy bog'lanish zanjirida jiddiy ontologik va tarkibiy o'zgarishlar yuzaga keladi. Firibgarlikning obyektiv tomonidagi markaziy va hal qiluvchi belgi bu – "aldash" yoxud "ishonchni suiiste'mol qilish" hisoblanib, klassik yondashuvda ushbu harakatlar doimo inson jabrlanuvchi ongi, irodasi va voqelikni idrok etish qobiliyatiga qaratilgan bo'lishi shart. O'zbekiston Respublikasi Oliy sudi Plenumining tushuntirishlariga binoan, firibgarlikdagi aldash yoki ishonchni suiiste'mol qilish harakatlari mulkni yoki unga bo'lgan huquqni aybdorning egaligiga ixtiyoriy va ongli ravishda topshiradigan aqli raso shaxsga nisbatan sodir etilishi shart. Binobarin, voqelik mohiyatini anglay olmaydigan shaxslardan masalan, yosh bolalar yoki ruhiy kasalligi ma'lum shaxslardan aldov yo'li bilan mulkni olish firibgarlik emas, balki yashirin ravishda talon-toroj qilish, ya'ni o'g'rilik jinoyati sifatida baholanishi lozim.

Biroq, kiberfiribgarlik holatlarida qilmishning usuli (modus operandi) bevosita axborot tizimlariga, dasturiy kodlarga va tarmoq infratuzilmasiga yo'naltirilgan bo'ladi. O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasini qo'llashda huquqni muhofaza qiluvchi organlar uzoq vaqt davomida moddaning eski tahrirdagi 2-qismi "v" bandi "kompyuter texnikasi

vositalaridan foydalanib” va 3-qismi “g” bandi “axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib” normalarini o‘zaro chegaralashda muayyan amaliy chalkashliklarga duch kelib kelishayotgan edi [4]. Ushbu tizimli muammolar va qonun amaliyotidagi tushunmovchiliklarni huquqiy jihatdan bartaraf etish maqsadida O‘zbekiston Respublikasining 2026-yil 22-iyundagi O‘RQ-1155-sonli Qonuni bilan Jinoyat kodeksining 168-moddasiga tub o‘zgartirishlar kiritildi. Mazkur islohotga ko‘ra, 168-modda uchinchi qismining eski tahrirdagi “v” va “g” bandlari almashtirilib yagona norma doirasida birlashtirilib, kiberfiribgarlik harakatlari to‘g‘ridan-to‘g‘ri 168-modda uchinchi qismi “v” bandi “axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan bo‘lsa” ostida kvalifikatsiya qilinadigan bo‘ldi [5]. Bu o‘zgarish sud-tergov amaliyotida “kompyuter texnikasi” va “axborot tizimi” tushunchalari o‘rtasidagi sun’iy farqlarni butunlay yo‘q qilib, virtual makonda mulkiy ishonchni suiiste’mol qilish harakatlariga nisbatan yagona va mantiqiy huquqiy mezonlarni shakllantirishga xizmat qiladi.

Bundan tashqari, axborot texnologiyalari vositasida mulkni talon-toroj qilish jinoyatlarining obyektiv tomonidagi eng katta muammo insonni aldash va kompyuter tizimining zaifliklaridan yashirin foydalanishni to‘g‘ri ajratish chegaralash hisoblanadi. Agar jinoyatchining qasddan yuborgan elektron xabari fishing havolasi bevosita jabrlanuvchining ongiga ta’sir qilib, u aldov oqibatida o‘z ixtiyori bilan bank parollari yoki raqamli aktivlarini masalan, kriptovalyutani ko‘chirib bersa, bu firibgarlikning obyektiv tomonini tashkil etadi. Negaki, bu yerda jabrlanuvchi mulk o‘z egaligidan chiqib ketayotganligini ongli ravishda idrok etadi va ixtiyoriy ravishda o‘tkazadi. Aksincha, agar jinoyatchi inson ishtirokisiz to‘g‘ridan-to‘g‘ri dasturiy ta’minotni yoki algoritmni o‘zgartirib, tizimni chetlab o‘tsa va bank kartasidan mablag‘larni yechib olsa, mantiqan va huquqan axborot tizimini “aldash” mumkin bo‘lmaganligi sababli, bunday qilmishda firibgarlik tarkibi mavjud bo‘lmaydi. Binobarin, ta’sir jabrlanuvchining ongiga emas, balki to‘g‘ridan-to‘g‘ri kompyuter ma’lumotlariga qaratilgan ushbu holat axborot tizimidan foydalanib sodir etilgan o‘g‘rilik JK 169-moddasi 3-qismi “b” bandi – “qonunga xilof ravishda ruxsatsiz axborot tizimiga kirib yoki undan foydalanib” jinoyati sifatida kvalifikatsiya qilinishi lozim.

Jinoyatning obyektiv tomonidagi uchinchi muhim element – ijtimoiy xavfli qilmish va kelib chiqqan moddiy zarar o‘rtasidagi obyektiv sababiy bog‘lanishdir [6]. Kiberfiribgarlikda pul mablag‘larining yoki virtual aktivlarning bir necha soniya ichida transchegaraviy tarmoqlar, turli xorijiy elektron hamyonlar yoki mikser xizmatlari orqali taqsimlab yuborilishi oqibatida sababiy bog‘lanishni aniqlash va isbotlash jarayoni texnik hamda

yurisdiksiyaviy jihatdan keskin murakkablashadi. Jabrlanuvchining mulki uning ixtiyoridan hisob varag‘idan chiqqan vaqtdan boshlab, to u jinoyatchining yoki uchinchi shaxslarning real tasarrufiga o‘tguniga qadar bo‘lgan oraliqdagi raqamli tranzaksiyalar zanjiri firibgarlik jinoyatining tamom bo‘lgan vaqtini to‘g‘ri belgilashda jiddiy to‘siq bo‘lib xizmat qiladi. Amaldagi Plenum qarori talablariga muvofiq, firibgarlik yo‘li bilan olingan naqd bo‘lmagan pul mablag‘lari aybdorning yoki boshqa shaxsning hisob varag‘iga o‘tkazilib, u ushbu mablag‘larni tasarruf etish imkoniyatiga ega bo‘lgan paytdan boshlab jinoyat tamom bo‘lgan deb hisoblanadi [2]. Biroq kiber-muhitdagi ko‘p bosqichli va anonim tranzaksiyalar zanjiri ushbu jinoiy oqibatning aynan qaysi lahzada va kimning real tasarrufida yuzaga kelganini isbotlashda tergov organlariga o‘ziga xos murakkabliklarni tug‘diradi. Milliy qonunchilikda ushbu kiber-tahdidlarga qarshi kurashish mexanizmlari O‘RQ-899-sonli Qonun kripto-aktivlar aylanmasi sohasidagi javobgarlik hamda PQ-153-sonli Prezident qarori droplar javobgarligi, banklar va moliya muassasalarining kiberxavfsizlik talablariga rioya etishi bo‘yicha moddiy javobgarligi bilan huquqiy jihatdan qat’iy va tizimli ravishda takomillashtirildi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Adxamov N.A. Kompyuter texnikasi vositalaridan foydalangan holda sodir etilgan talon-taroj jinoyatlarini kvalifikatsiya qilish muammolari // IQRO JURNALI. – 2023. – Jild 4. – № 1. – B. 242-248.
2. O‘zbekiston Respublikasi Oliy sudi Plenumining “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-sonli qarori. – Toshkent, 2023-yil 23-iyun. URL: https://lex.uz/en/docs/-6523582.
3. Серик А.С. Правовые основы предотвращения кибермошенничества: состояние и перспективы развития: дис. ... магистр права (7М04208 - “Право IT”). – Нур-Султан, 2022. – 53 с.
4. Nurmanov X.R. Onlayn banklar faoliyati sohasida firibgarlikni kvalifikatsiya qilish masalalari // Yurisprudensiya huquqiy ilmiy-amaliy jurnali. – 2025. – Jild 5. – № 4. – B. 147-155.
5. O‘zbekiston Respublikasining Jinoyat kodeksi [Elektron resurs] // Qonunchilik ma’lumotlari milliy bazasi. URL: https://lex.uz/docs/-111453.
6. Kabulov R. Jinoyatlarni kvalifikatsiya qilish: Darslik. – Toshkent: O‘zbekiston Respublikasi IIV Akademiyasi, 2012. – B. 45-48.