XALQARO JINOYAT SUDI YURISDIKSIYASI VA RAQAMLI DALILLAR: ZAMONAVIY MUAMMOLAR VA RIVOJLANISH ISTIQBOLLARI

O'rolov Abdulla Anvar o'g'li

Termiz davlat universiteti yuridik fakulteti 3-bosqich talabasi
uralov0106@gmail.com
DOI: 10.61587/mmit.tiue.uz.v1i1.408

Annotatsiya. Ushbu ilmiy maqola zamonaviy texnologik transformatsiyalar davrida Xalqaro jinoiy sud (XJS) yurisdiksiyasi hamda raqamli dalillardan foydalanishning huquqiy mexanizmlarini chuqur tadqiq etadi. Tadqiqotda Rim statuti doirasida ochiq axborot resurslari (OSINT), koinotdan olingan tasvirlar, kriptografik aloqalar, biometrik ma'lumotlar va metaverse muhitidagi elektron izlarning huquqiy maqomi tahlil qilingan. Shuningdek, maqolada sun'iy intellekt tomonidan yaratilgan soxta kontentlar (deepfake) va kvant texnologiyalari kabi yangi avlod tahdidlari sharoitida protsessual ishonchlilikni saqlash masalalari ko'rib chiqiladi. Al-Werfalli kabi xalqaro pretsedentlar misolida dalillarning autentifikatsiyasi va daxlsizligi muammolari o'rganilgan. Tadqiqot yakunida XJS faoliyatini raqamlashtirish, maxsus tahliliy tuzilmalar yaratish va post-kvant himoya tizimlarini joriy etishga oid qonunchilik takliflari shakllantirilgan.

Kalit so'zlar: *Rim statuti, Xalqaro jinoiy sud, elektron isbotlash, kiber-yurisdiksiya, OSINT, sun'iy intellekt xavfsizligi, Berkeley protokoli, metaverse tahlili, kvant kriptografiyasi, protsessual qonuniylik.*

JURISDICTION OF THE INTERNATIONAL CRIMINAL COURT AND DIGITAL EVIDENCE: CONTEMPORARY CHALLENGES AND DEVELOPMENT PROSPECTS

Abdulla Anvar ugli Orolov

3rd-year student, Faculty of Law, Termez State University
uralov0106@gmail.com

Abstract. This scientific article provides an in-depth analysis of the jurisdiction of the International Criminal Court (ICC) and the legal mechanisms for the use of digital evidence in the era of modern technological transformations. The study examines the legal status of open-source intelligence (OSINT), satellite imagery, cryptographic communications, biometric data, and electronic traces within the metaverse environment under the framework of the Rome Statute. Additionally, the article addresses the challenges of maintaining procedural reliability in the context of emerging threats such as AI-generated content (deepfakes) and quantum technologies. Using international precedents, including the Al-Werfalli case, the paper explores issues related to the authentication and integrity of evidence. The study concludes with legislative proposals aimed at digitizing ICC operations, establishing specialized analytical structures, and implementing post-quantum security systems.

Keywords: *Rome Statute, International Criminal Court, electronic evidence, cyber jurisdiction, OSINT, AI security, Berkeley Protocol, metaverse analysis, quantum cryptography, procedural legality.*

XXI asrda qurolli mojarolar tabiati tubdan o'zgardi. Davlatlar o'rtasidagi klassik urushlar o'rnini ko'pincha davlat ichidagi assimetrik to'qnashuvlar, gibrid urushlar va kiberoperatsiyalar egallamoqda. Bunday sharoitda aybdorlikni isbotlash uchun an'anaviy dalillar – guvohlarning og'zaki ko'rsatmalari, jismoniy hujjatlar yoki moddiy ashyolar yetarli bo'lmay qolmoqda. Aksariyat hollarda jinoyatchilar o'z izlarini yashirishga intiladi, guvohlar

esa qo‘rquv, ko‘chirilish yoki o‘lim sababli sud oldida ko‘rsatma berish imkoniyatiga ega bo‘lmaydi. Shu bilan birga, raqamli texnologiyalar har bir fuqaroni potensial hujjatlashtiruvchiga aylantirdi. Ijtimoiy tarmoqlarga yuklangan videolar, sun’iy yo‘ldosh suratlari, shifrlangan xabar qaydlari va mobil telefon ma’lumotlari xalqaro jinoyatlarni tekshirishda misli ko‘rilmagan hajmda raqamli iz qoldirmoqda. 2023-yilda Ukraina hududidagi birgina BMT monitoring missiyasi o‘n minglab raqamli fayllarni qabul qilgani, ularning aksariyati smartfonlar yordamida oddiy fuqarolar tomonidan yozib olingani bu tendensiyaning yaqqol tasdig‘idir. Xalqaro Jinoyat Sudi (ICC yoki XJS) bog‘liq jiddiy muammolar. Mazkur maqolaning maqsadi – XJS yurisdiksiyasini raqamli asr kontekstida har tomonlama tahlil qilish, raqamli dalillar bilan ishlash jarayonida yuzaga kelayotgan nazariy va amaliy qiyinchiliklarni aniqlash, shuningdek, sud amaliyotini takomillashtirish bo‘yicha asoslangan tavsiyalarni ilgari surishdan iborat.

Xalqaro Jinoyat Sudi 1998-yilda qabul qilingan va 2002-yilda kuchga kirgan Rim statuti asosida tashkil etilgan. Sudning yurisdiksiyasi ushbu statut bilan aniq belgilangan bo‘lib, u shaxsiy, hududiy, vaqtinchalik va moddiy yurisdiksiya turlarini o‘z ichiga oladi. Shaxsiy yurisdiksiyaga ko‘ra, XJS faqat jismoniy shaxslarni javobgarlikka tortishi mumkin. Davlatlar yoki yuridik shaxslar sud yurisdiksiyasi ostiga kirmaydi. Bu qoida raqamli jinoyatlar kontekstida muhim ahamiyatga ega, chunki ko‘pincha kiberhujumlar ortida butun bir davlat apparati yoki xakerlik guruhlari turadi, biroq sud faqat aniq bajaruvchilarni yoki buyruq bergan rahbarlarni jinoiy javobgarlikka torta oladi. Hududiy yurisdiksiya jinoyat ishtirokchi-davlat hududida yoki uning fuqarosi tomonidan sodir etilgan bo‘lishini talab qiladi, biroq BMT Xavfsizlik Kengashi topshirig‘iga ko‘ra bu chegara kengayishi mumkin. Sudan (Darfur) yoki Liviya ishlari bunga misol bo‘la oladi. Raqamli dalillar nuqtai nazaridan, hudud mezoni qo‘shimcha qiyinchilik tug‘diradi: agar kiberhujum bir davlat hududidan turib amalga oshirilib, ta’siri boshqa davlatda yuz bersa, qaysi hudud sudning yurisdiksiyasini belgilaydi? Bunday hollarda, Rim statutining 30-moddasiga muvofiq, jinoyatning "oqibati yuz bergan joy" mezoni qo‘llanilishi mumkin, biroq bu masala hali ham munozarali. Vaqtinchalik yurisdiksiya faqat 2002-yil 1-iyuldan keyin sodir etilgan jinoyatlarni qamrab oladi. Bu shuni anglatadiki, undan oldingi davrda sodir bo‘lgan jinoyatlar (masalan, Yugoslaviya mojarolari) XJS tomonidan emas, balki maxsus ad hoc tribunallar tomonidan ko‘rilgan. Raqamli dalillar uchun esa vaqt cheklovi muhim ahamiyatga ega: 2002-yildan oldin yaratilgan raqamli yozuvlar kamdan-kam bo‘lib, aksariyat hollarda sud qarorida ularning isbotiy qiymati ko‘rib chiqilmaydi. Biroq, davom etayotgan jinoyatlarda (continuous crimes) vaqtinchalik yurisdiksiya masalasi yanada murakkablashadi. Moddiy yurisdiksiya to‘rtta asosiy jinoyat turini o‘z ichiga oladi: genotsid, insoniyatga qarshi jinoyatlar, urush jinoyatlari va agressiya jinoyati. Aynan mana shu to‘rtinchi tur – agressiya jinoyati – kiberoperatsiyalar kontekstida eng munozarali masalalardan biridir. Keng ko‘lamli kiberhujum natijasida fuqarolar orasida qurbonlar keltirish yoki muhim infratuzilmani izdan chiqarish insoniyatga qarshi jinoyat yoki urush jinoyati sifatida kvalifikatsiya qilinishi mumkin. Ammo mustaqil agressiya jinoyati sifatida baholanishi uchun davlat rahbariyatining buyrug‘i, bosqinchilik niyati va qurolli kuch ishlatish darajasidagi jiddiylik isbotlanishi shart. Masalan, 2010-yilda Stuxnet virusi orqali Eron yadro inshootlariga qilingan hujum ba’zi ekspertlar tomonidan "qurolli kuch ishlatish" sifatida talqin qilinsa-da, boshqalar uni oddiy diversiya yoki sanoat sabotaji sifatida ko‘radi. Hozirgi kunda Rim statutida kibermakonni bevosita tartibga soluvchi normalar yo‘qligi sababli, ko‘pchilik mutaxassislar raqamli agressiyani an’anaviy qurolli hujumlar bilan tenglashtirish uchun alohida qo‘shimcha protokollar zarurligini ta’kidlamoqda. Yana bir muhim tamoyil – komplementarlik (to‘ldiruvchanlik) prinsipi. XJS faqatgina milliy sud tizimi jinoyatchini jazolashni istamasa yoki bunga qodir bo‘lmasagina ishni o‘z yurisdiksiyasiga olishi mumkin. Raqamli dalillar kontekstida bu tamoyil murakkablashadi, chunki ko‘plab davlatlar o‘z hududidan tashqaridagi serverlarda saqlanayotgan raqamli ma’lumotlarga kirish imkoniyatiga ega emas. Misol uchun, agar jinoyatga oid muhim yozishmalar xorijiy kompaniyaga qarashli bulutli serverda saqlansa,

milliy tergov organlari bu ma'lumotlarni olish uchun o'zaro huquqiy yordam so'rovlariga majbur bo'ladi, bu esa jarayonni sekinlashtiradi. Natijada, milliy surishtiruv organlari raqamli izlarni yetarlicha to'play olmagani uchun "qodir emas" deb topilishi holatlari ko'paymoqda. Bu esa XJS va milliy organlar o'rtasida samarali raqamli ma'lumot almashinuvi mexanizmlarini yaratishni taqozo etadi. 2021-yilda XJS prokuraturasi ushbu muammoni yumshatish uchun "Texnologiya va huquqiy hamkorlik" dasturini ishga tushirdi, biroq uning natijalari hali cheklangan.

Raqamli dalillar nima o'zi ?

Raqamli dalillar deganda jinoyat sodir etilganligini tasdiqlovchi yoki rad etuvchi, elektron qurilmalarda saqlanadigan yoki uzatiladigan har qanday axborot tushuniladi. Xalqaro sud amaliyotida bunday dalillar shartli ravishda uchta katta guruhga bo'linadi.

Birinchi guruh – ochiq manbalardagi ma'lumotlar (OSINT). Bugungi kunda Telegram, X (sobiq Twitter), TikTok va Facebook kabi platformalar harbiy jinoyatchilarning o'zlari tomonidan yuklangan videolar bilan to'lib-toshgan. Jabrlanganlar va tasodifiy guvohlar tomonidan e'lon qilingan kontent jinoyat sodir etilgan joy va vaqtni aniqlashda bebaho manbadir. Biroq aynan shu turdagi dalillar eng ko'p shubhalarga sabab bo'ladi: akkauntlar soxta bo'lishi, videolar mazmuni kontekstdan uzib qo'yilishi yoki sun'iy intellekt yordamida o'zgartirilgan bo'lishi mumkin. 2019-yilda Myanma harbiylari rohinjlarni quvib chiqarish bo'yicha Facebook'da ko'plab nafrat uyg'otuvchi postlar yozgani fosh etilganda, kompaniya ancha keyin ularni o'chirgan. Bu postlar keyinchalik BMT Mustaqil Tekshiruv Missiyasi tomonidan genotsidga undash sifatida kvalifikatsiya qilindi va XJS prokurori bunga asoslangan holda dastlabki tekshiruv boshlagan. Shunday ekan, OSINT nafaqat jinoyatni isbotlash, balki ularning oldini olish kontekstida ham muhim ahamiyat kasb etadi.

Ikkinchi guruh – sun'iy yo'ldosh va geofazoviy ma'lumotlar. Yuqori aniqlikdagi tijorat sun'iy yo'ldoshlari (masalan, Maxar Technologies yoki Planet Labs) har kuni Yer yuzasining millionlab kvadrat kilometrini suratga oladi. Bu tasvirlar orqali qishloqlarning vayron etilishi, ommaviy qabrlar paydo bo'lishi yoki harbiy texnikaning siljishini aniq belgilash mumkin. XJS prokuraturasi bunday dalillardan, ayniqsa, BMT Xavfsizlik Kengashi tomonidan topshirilgan ishlarda muntazam foydalanmoqda. Darfurdagi harbiy jinoyatlar bo'yicha Ahmad Harun va Ali Kushayb ishida sun'iy yo'ldosh orqali olingan suratlar qishloqlarning yoqib yuborilgani va aholi ko'chirilganini ko'rsatgan. Geofazoviy dalillar nisbatan betaraf va ishonchli hisoblanadi, biroq ularni izohlashda maxsus bilim talab etiladi. Masalan, yong'in izlari tinch aholi uylarining ataylab yoqilganini yoki oddiy tabiiy yong'inni aks ettirishi mumkin, buni faqatgina ekspertiza hal qila oladi.

Uchinchi guruh – elektron aloqa ma'lumotlari. Harbiy qo'mondonlik zanjirini isbotlash uchun shifrlangan messenjerlar (Signal, WhatsApp) orqali amalga oshirilgan yozishmalar eng qimmatli dalillardan biridir. Ammo bunday ma'lumotlarni olish va ularni deshifrlash jiddiy texnik va huquqiy to'siqlarga ega. Birinchidan, shifrlangan xabarlarni ochish uchun ko'pincha xususiy kompaniyalar bilan hamkorlik qilish kerak bo'ladi, ular esa tijoriy yoki maxfiylik sabablari bilan ma'lumotni taqdim etishdan bosh tortishi mumkin. Masalan, 2020-yilda Fransiya hukumatining Telegram'dan terrorizmga aloqador shaxslarning xabarlarini ochib berishni so'ragani rad javobini olgan. Ikkinchidan, bunday dalillarning olinishi fuqarolarning shaxsiy hayot daxlsizligi huquqini buzish xavfini tug'diradi, bu esa sud tomonidan dalilni qabul qilmaslikka asos bo'la oladi. Shuning uchun prokuratura ko'pincha bunday dalillarni milliy qonunchilik doirasida olishga va ularni sudga taqdim etishda inson huquqlari standartlariga rioya qilishga intiladi. Sudda raqamli dalilning qabul qilinishi eng avvalo uning ishonchliligi va saqlanish zanjiri (chain of custody) bilan belgilanadi. Raqamli ma'lumotni dastlabki yig'ilgan paytdan to sud zaliga taqdim etilguniga qadar uning o'zgarmasligini kafolatlash

protsessual adolatning ajralmas qismidir. Zamonaviy texnologiyalar bu borada muhim yechimlarni taklif qilmoqda.

Xesh-kodlar (hash functions) har qanday raqamli faylning noyob raqamli barmoq izini yaratib, keyinchalik faylning bir bayti ham o‘zgarmaganligini tekshirish imkonini beradi. Masalan, agar bironta video sudga taqdim etilsa, uning xesh qiymati (MD5, SHA-256) oldindan hisoblab qo‘yiladi va ish davomida har qanday manipulyatsiya urinishi darhol oshkor bo‘ladi.

Blockchain texnologiyasi esa ma’lumotlarning o‘zgarmas daftarda saqlanishi orqali dalillar zanjirining buzilmasligini kafolatlaydi. Xalqaro nodavlat tashkilotlar, masalan, Hala Systems, Suriya va Ukrainadagi huquqbuzarliklarni hujjatlashtirish uchun maxsus blockchain platformalarini ishlamoqda. XJS ekspertlari tomonidan ushbu vositalardan foydalanish yo‘lga qo‘yilmoqda, biroq ularning majburiy standart sifatida belgilanmagani ba’zi ishlarda turlicha yondashuvlarga sabab bo‘lmoqda. Xalqaro darajada eng muhim hujjatlardan biri – Berkeley protokoli (2018). Bu protokol Birlashgan Millatlar Tashkilotining Inson huquqlari bo‘yicha Oliy komissari boshqarmasi va Kaliforniya universiteti huzuridagi Inson huquqlari markazi hamkorligida ishlab chiqilgan bo‘lib, ochiq manbalardagi raqamli ma’lumotlarni tekshirish va hujjatlashtirish bo‘yicha universal standartlarni belgilaydi. Protokol quyidagi asosiy tamoyillarni o‘z ichiga oladi: maqsadga muvofiqlik, xavfsizlik va himoya, ma’lumotlarni boshqarish, autentifikatsiya, tahlil va hisobot berish. Garchi XJS uchun qonuniy majburiy kuchga ega bo‘lmasa-da, sud amaliyotida ushbu protokolga havolalar ko‘payib bormoqda. Xususan, 2022-yilda XJS prokuraturasi o‘z xodimlari uchun Berkley protokoliga asoslangan ichki yo‘riqnomani qabul qildi. Shu bilan birga, nodavlat tashkilotlarning roli ham tobora ortmoqda. Bellingcat jurnalistik surishtiruv guruhi o‘zining raqamli tahlil metodologiyasi bilan bir qancha shov-shuvli ishlarni ochishga yordam berdi. Ular sun’iy yo‘ldosh tasvirlari, ijtimoiy tarmoq postlari va boshqa ochiq manbalarni sinxronlashtirish orqali jinoyat holatlarini aniqlashda XJS prokuraturasi uchun tayyor analitik materiallar taqdim etmoqda. Shuningdek, Syrian Archive kabi tashkilotlar mamlakatdagi harbiy jinoyatlarni raqamli arxivlashtirishga ixtisoslashgan. Biroq nodavlat tashkilotlarning mustaqilligi va ular tomonidan to‘plangan dalillarning sud tomonidan qay darajada ishonchli deb topilishi masalasi hali ham munozaraligicha qolmoqda. Chunki bu tashkilotlar davlatlarga qarashli emasligi sababli, ularning metodologiyasi har doim ham sud nazoratidan o‘tgan bo‘lavermaydi. Shuning uchun mutaxassislar bunday dalillarning sudda ishlatilishidan oldin mustaqil ekspertiza o‘tkazishni tavsiya etishadi. Raqamli dalillar hajmi va xilma-xilligi oshgani sari sud ularni qabul qilishda uchta jiddiy muammoga duch kelmoqda: autentifikatsiya, xususiy hayot daxlsizligi va isbotlash yuki standarti.

Muammo nimada o’zi ?

Birinchi va eng katta muammo – autentifikatsiya, ya’ni dalilning haqiqiy ekanligini aniqlash. Sun’iy intellektning rivojlanishi bilan manipulyatsiya imkoniyatlari keskin kengaydi. Deepfake texnologiyasi yordamida mavjud bo‘lmagan videolarni yaratish yoki mavjudlarini o‘zgartirish mumkin. Masalan, biror shaxsning yuz ifodasini almashtirish yoki ovozini klonlashtirish orqali soxta buyruq yoki tan olish videosini yasash mumkin. 2023-yilda Internetda tarqalgan Ukraina prezidenti V.Zelenskiyning soxta taslim bo‘lish haqidagi videosi bunga yaqqol misol bo‘ldi. Sud oldida turgan asosiy savol: raqamli dalilning soxta emasligini kim va qanday isbotlashi kerak? Amaldagi Rim statuti qoidalariga ko‘ra, dalil taqdim etuvchi taraf (odatda prokuror) uning ishonchliligini asoslashi shart. Bu esa prokurordan jiddiy texnik ekspertiza talab qiladi. XJS amaliyotida prokuratura ko‘pincha dalillarni ikki mustaqil manbadan tasdiqlash (cross-verification) strategiyasini qo‘llaydi. Ba’zi hollarda himoya tomoni dalilning soxta ekanligini isbotlash majburiyatini o‘z zimmasiga olishi kerak bo‘lmoqda, bu esa protsessual tenglik tamoyiliga soya soladi. Ikkinchi muammo – xususiy hayot daxlsizligi. Raqamli dalillar ko‘pincha jinoyatdan jabrlangan yoki uchinchi shaxslarning shaxsiy

ma'lumotlarini o'z ichiga oladi. Tibbiy yozuvlar, joylashuv ma'lumotlari yoki maxfiy xabarlar kabi sezgir axborotlardan sudda foydalanish inson huquqlari bo'yicha xalqaro standartlarga mos bo'lishi kerak. Inson huquqlari bo'yicha Yevropa sudi (ECtHR) va BMT Inson huquqlari qo'mitasining qarorlariga ko'ra, shaxsiy ma'lumotlarni yig'ish va saqlash qonuniylik, zaruriyat va mutanosiblik tamoyillariga javob berishi shart. XJS bu borada ikkita qarama-qarshi manfaatni muvozanatlashi lozim: bir tomondan haqiqatni aniqlash va jabrlanuvchilar uchun adolatni ta'minlash, ikkinchi tomondan shaxslarning shaxsiy hayot huquqini hurmat qilish. Masalan, shifrlangan messenjer orqali olingan yozishmalar jinoyatga aloqador bo'lmagan shaxslarning intim suhbatlarini oshkor qilishi mumkin. Bunday hollarda sud dalilni to'liq oshkor qilish o'rniga, uning faqat tegishli qismlarini qabul qilish yoki yopiq sud majlislarida ko'rib chiqish amaliyotidan foydalanadi. Shuningdek, ovozli va tasvirli materiallardan jabrlanuvchilarning yuzlarini yashirish yoki ovozini o'zgartirish kabi himoya choralari qo'llaniladi. Uchinchi muammo – isbotlash yuki standarti. Rim statutiga muvofiq, sud ayblovni asoslash uchun dalillarni "oqilona shubhadan xoli" darajada isbotlangan deb topishi kerak. Raqamli dalillar ko'p bo'laklardan iborat murakkab mozaikani tashkil etadi. Har bir alohida raqamli dalil zaif ko'rinishi mumkin, ammo ular birgalikda kuchli isbot kuchiga ega bo'lishi mumkin. XJS bu yondashuvni "butunlikdagi isbot" (proof by mosaic) deb ataydi. Sudyalar oldidagi savol shundaki, ular raqamli dalillarning umumiy og'irligini baholashda qanday matematik ehtimoliy yondashuvdan emas, balki yuridik ishonchdan kelib chiqishlari kerak. Bu borada aniq miqdoriy mezon yo'qligi amaliyotda turlicha qarorlarga olib kelmoqda. Masalan, Al-Mahdi ishida sud ayblanuvchining aybiga faqatgina videomateriallar va sun'iy yo'ldosh suratlari asosida ishonch hosil qilgan bo'lsa, boshqa ishlarda qo'shimcha guvohlik so'ralgan. Ushbu nomuvofiqlik sudning kelajakdagi ishlarida huquqiy aniqlikni ta'minlashga to'sqinlik qilishi mumkin.

Xalqaro pretsedentlar: Al-Werfalli ishi (Liviya). Ushbu ish XJS tarixida raqamli dalillar asosida hibsga olish orderi chiqarilgan birinchi yirik pretsedent hisoblanadi. 2017-yilda sud Liviya milliy armiyasi qo'mondoni Mahmud Mustafo Busayf Al-Werfallini urush jinoyatlarida ayblab, order berdi. Orderning asosiy dalili Facebook'da e'lon qilingan yettita video bo'lib, ularda harbiy kiyimdagi shaxslar tomonidan qurolsiz mahbuslarning otib tashlanishi aks etgan edi. Prokuratura ushbu videolarning autentikligini geolokatsiya, forma detallari, qotillar ovozlari va boshqa anonim manbalar bilan solishtirish orqali asoslab berdi. Ushbu ish raqamli ochiq manba dalillarining mustaqil isbot kuchiga ega bo'lishi mumkinligini ko'rsatdi, biroq shu bilan birga himoyaning dalillarni so'roq qilish imkoniyati cheklanganligi sababli protsessual adolat bo'yicha tanqidlarga ham uchradi. Al-Werfalli ayblangan videolarning asl manbalari hech qachon sudga taqdim etilmadi, faqat Facebook nusxalari ko'rsatildi. Al-Mahdi ishi (Mali). Bu ish raqamli dalillarning sud jarayonida qanday vizual platformalar orqali taqdim etilishining yorqin misolidir. Ahmad Al-Faqi Al-Mahdi 2012-yilda Timbuktudagi tarixiy diniy yodgorliklarni vayron qilganlikda ayblangan. Sud jarayonida prokuratura sun'iy yo'ldosh suratlari, vayronagarchilikdan oldingi va keyingi holatni aks ettiruvchi raqamli 3D modellar hamda mahalliy aholi tomonidan yozib olingan videolarni interaktiv raqamli platforma orqali taqdim etdi. Sud hay'ati ushbu platforma yordamida vayronagarchilikning ko'lamini yaxshiroq idrok etdi. Bu platforma sud amaliyotida yangi davrni boshlab berdi va ko'plab boshqa ishlarda, jumladan Al-Hassan sudida ham qo'llanildi. Ukraina va Falastin vaziyatlari. 2022-yildan beri davom etayotgan Ukrainadagi urush va 2023-yildan keyin kuchaygan Falastindagi mojaro XJS uchun raqamli dalillarning eng katta sinov maydoniga aylandi. Ukraina bo'yicha XJS prokuraturasi "Harmony" loyihasi doirasida yuz minglab raqamli fayllarni yig'ishni boshladi. Bu loyiha sun'iy intellekt yordamida ochiq manbalardagi mazmuniy kontentni avtomatik tarzda skanerlash, potensial jinoyat izlarini aniqlash va ularni tizimlashtirishga qaratilgan. Loyihada dron orqali olingan videolar, suhbat yozuvlari va ijtimoiy tarmoq postlari bir vaqtning o'zida tahlil qilinmoqda. Falastin bo'yicha esa, ko'plab hukumat va nodavlat tashkilotlar tomonidan taqdim etilgan sun'iy yo'ldosh suratlari va ijtimoiy media kontenti ommaviy qabrlarning

mavjudligini tasdiqlashda foydalanilmoqda. Hozircha bu dalillar sudning dastlabki bosqichlarida, asosan vaziyatni o‘rganish va order talab qilish uchun ishlatilmoqda, biroq kelajakdagi sud jarayonlari uchun eng asosiy dalillar bazasiga aylanishi kutilmoqda. Ayniqsa, XJS prokurori Karim Xonning 2024-yilda Ukraina bo‘yicha taqdim etgan ilk ayblov xulosalari to‘laligicha raqamli dalillarga asoslangani muhim burilish nuqtasi bo‘ldi.

Ushbu pretsedentlardan kelib chiqadigan asosiy xulosa shuki, XJS raqamli dalillarni qabul qilishga tayyor va ularga tayanib muhim protsessual harakatlarni amalga oshirmoqda. Shu bilan birga, sud hali ham ehtiyotkor yondashuvni saqlab, raqamli dalillarni boshqa turdagi dalillar bilan birga ko‘rib chiqishni afzal ko‘rmoqda.

Kelajak texnologiyalari va ularning XJS yurisdiksiyasiga ta’siri

Xalqaro Jinoyat Sudi o‘z tarixida bosma matbuotdan sun’iy yo‘ldoshgacha bo‘lgan texnologik siljishlarni boshdan kechirgan bo‘lsa-da, yaqin kelajakdagi uchta innovatsion yo‘nalish uning ish uslubi va yurisdiksiya chegaralarini tubdan qayta shakllantirishi mumkin. Bular – metaverse muhitida sodir etiladigan xatti-harakatlar, kvant kompyuterlarining shifrlash tizimlariga tahdidi hamda biometrik dalillarning keng qo‘llanilishi. Ushbu texnologiyalar nafaqat yangi jinoyat shakllarini yuzaga keltiradi, balki dalillar ishonchliligi, protsessual adolat va inson huquqlari bilan bog‘liq yangi savollarni ham ko‘taradi. Metaverse — foydalanuvchilar virtual identifikatorlar orqali o‘zaro aloqaga kirishadigan, iqtisodiy faoliyat yuritadigan va hatto mulkka egalik qiladigan doimiy immersiv raqamli muhitdir. Hozircha bu asosan o‘yin va ijtimoiy platformalar bilan chegaralangan bo‘lsa-da, Meta, Microsoft va boshqa texnologik gigantlar tomonidan yaratilayotgan infratuzilma uni kundalik hayotning davomiga aylantirishga intilmoqda. Xalqaro jinoyat huquqi nuqtai nazaridan, metaverseda sodir etilishi mumkin bo‘lgan harakatlar ikki asosiy toifaga bo‘linadi. Birinchisi — virtual muhitning o‘zida sodir etilib, real dunyoda bevosita jismoniy ta’sir ko‘rsatmaydigan, ammo jamoaviy ong va ijtimoiy munosabatlarga zarar yetkazadigan harakatlar. Masalan, virtual muhitda etnik guruhlarga qarshi nafrat uyg‘otuvchi yig‘inlar tashkil etish, ramziy genotsid sahnalarini jonlantirish yoki bolalar obrazidan foydalangan holda zo‘ravonlik simulyatsiyalarini yaratish. Ikkinchi toifa esa — metaversedagi faoliyat orqali real moddalar savdosini muvofiqlashtirish yoki harbiy operatsiyalarga oid maxfiy ma’lumotlarni almashish. XJS yurisdiksiyasi uchun asosiy muammo shundaki, Rim statuti asosan jismoniy jinoyatlarga qaratilgan bo‘lib, faqat virtual muhitda yuz bergan, moddiy oqibatlarga olib kelmagan harakatni genotsid, urush jinoyati yoki insoniyatga qarshi jinoyat sifatida kvalifikatsiya qilish qiyin. Biroq, agar metaversedagi nafrat uyg‘otuvchi kampaniyalar real dunyoda zo‘ravonliklarga bevosita sabab bo‘lsa, sud bunday kontentni jinoyat uchun tayyorgarlik yoki undash sifatida baholashi mumkin. Myanmadagi rohinjalarga qarshi Facebook’dagi tashviqot genotsid bilan bog‘langaniga o‘xshash, metaversedagi immersiv targ‘ibot yanada kuchliroq manipulyativ ta’sirga ega bo‘lishi ehtimoli yuqori. Dalillar nuqtai nazaridan, metaversedagi izlar o‘ziga xos xususiyatlarga ega. Avatarlar harakati, ovozli chat yozuvlari, virtual mulk operatsiyalari va hatto miya-to‘lqin interfeyslari orqali olingan biometrik ma’lumotlar jinoyat daliliga aylanishi mumkin. Biroq bu yerda "dalillar zanjiri" yanada murakkablashadi: virtual muhitni boshqaruvchi platforma kompaniyasi dalillarni o‘zgartirishi, yo‘qotishi yoki taqdim etishdan bosh tortishi mumkin. Bundan tashqari, avatar ortidagi shaxsning kimligini aniqlash ham qiyinchilik tug‘diradi. Shu sababli, metaversedan olingan dalillarni sudga taqdim etishda autentifikatsiyaning yangi, ko‘p bosqichli protokollari — jumladan, foydalanuvchining biometrik xatti-harakatlarini tahlil qilish, IP-manzillar, blokcheyn operatsiyalari va platforma ichidagi raqamli guvohliklarni bir-biri bilan kesishgan holda tekshirish talab etiladi. XJS kelajakda "virtual sud eksperti" lavozimini joriy etishi va metaverse provayderlari bilan hamkorlik qilish bo‘yicha xalqaro standartlarni ishlab chiqishi zarur.

Kvant kompyuterlari an'anaviy hisoblash mashinalaridan tubdan farq qiladigan kvant bitlari (qubit) asosida ishlaydi va ular hal qila olmaydigan matematik muammolarni soniyalarda yechishga qodir. Hozirgi kunda internet xavfsizligi, bank tizimlari va maxfiy aloqa kanallari uchun asos bo‘lgan RSA va elliptik egri chiziqli shifrlash algoritmlari aynan mana shunday matematik murakkabliklarga tayanadi. Kvant kompyuterlari amaliy bosqichga yetgach, ushbu shifrlash tizimlari bir necha daqiqada buzilishi mumkin. Xalqaro Jinoyat Sudi uchun bu ikki yoqlama tahdid yaratadi. Birinchidan, sud tomonidan saqlanayotgan raqamli dalillar — xususan, shifrlangan messenjer yozishmalari, bulutli serverlardagi maxfiy hujjatlar va himoyalangan ma'lumotlar omborlari — kvant hujumi orqali oshkor bo‘lishi yoki o‘zgartirilishi mumkin. Agar himoya tomoni yoki uchinchi bir kuch sudning raqamli arxiviga kirib, dalillarni manipulyatsiya qilsa, bu nafaqat alohida ishning qulashiga, balki umuman sudning ishonchliligiga jiddiy zarba beradi. Ikkinchi va ehtimol undan ham kattaroq tahdid — kvant kompyuterlari yordamida deepfake videolarni yaratish uchun ma'lum texnik bilim va vaqt kerak bo‘lsa, kvant quvvatiga ega sun'iy intellekt tizimlari bu jarayonni nihoyatda tez va sifatli bajarishi mumkin. Natijada, sud oldida haqiqiy va soxta dalilni farqlash bugungidan ham qiyinlashadi. Bu muammolarga qarshi choralar allaqachon ko‘rilmoqda. Post-kvant kriptografiyasi (PQC) deb ataluvchi yangi avlod shifrlash algoritmlari kvant hujumlariga chidamli bo‘lishi uchun loyihalashtirilmoqda. AQSh Milliy Standartlar va Texnologiyalar Instituti (NIST) 2024-yilda bir nechta PQC standartini tasdiqladi va yaqin yillarda ular keng qo‘llanilishi kutilmoqda. XJS o‘zining "Raqamli tahlil markazi" orqali ushbu standartlarga o‘tishi, dalillarni saqlashda kvantga chidamli shifrlashni joriy etishi va xodimlarini kvant tahdidi xabardorligi bo‘yicha o‘qitishi shart. Shuningdek, sudda dalillarning "kvantgacha bo‘lgan davr"da yig‘ilgani va ularning autentikligini tasdiqlovchi qo‘shimcha qatlam sifatida blokcheyn kabi texnologiyalardan foydalanish tavsiya etiladi. Biometrik texnologiyalar — yuzni tanish, ovoz izini aniqlash, barmoq izi, ko‘z qorachig‘i skanerlash va hatto yurish uslubi tahlili — so‘nggi yillarda nihoyatda takomillashdi. Ular jinoyatchilarni identifikatsiya qilish, qo‘mondonlik zanjirini isbotlash va jinoyat joyini qayta tiklashda qo‘llanilmoqda. Masalan, Ukrainadagi urushda yuzni tanish dasturlari orqali harbiy jinoyatchilarning shaxsini aniqlash, ovoz izi orqali esa sizdirilgan telefon suhbatlaridagi ishtirokchilarni tasdiqlash holatlari ko‘p uchramoqda.

Biroq biometrik dalillarning sud tomonidan qabul qilinishi bir qator jiddiy muammolarni keltirib chiqaradi. Birinchi muammo — aniqlik va tarafkashlik. Ko‘plab mustaqil tadqiqotlar shuni ko‘rsatganki, ayrim yuzni tanish tizimlari qora tanli va osiyolik shaxslarni aniqlashda yuqori xatolik ko‘rsatadi. Agar noto‘g‘ri identifikatsiya sababli begunoh shaxs XJS tomonidan ayblansa, bu sudning obro‘siga butunlay putur yetkazadi. Shuning uchun biometrik dalillar hech qachon yagona asosiy dalil sifatida qabul qilinmasligi, balki har doim boshqa mustaqil manbalar bilan tasdiqlanishi kerak.

Ikkinchi muammo — chuqur soxtalashtirish (deepfake) orqali biometrik ma'lumotlarni manipulyatsiya qilish. Sun'iy intellekt yordamida odamning yuz ifodasini, ovozini va hatto ko‘z qorachig‘ining yorug‘likka reaksiyasini soxtalashtirish mumkin. 2023-yilda bir tadqiqotchi sun'iy intellekt orqali yaratilgan ovoz yozuvi bilan bank autentifikatsiyasi tizimini aldab o‘tishga muvaffaq bo‘lgan edi. XJSda bunday dalillar bilan ishlashda, ularning olingan qurilmasining raqamli barmoq izi, metama'lumotlari va yaratilish vaqtidagi tarmoq izlari birgalikda tekshirilishi lozim.

Uchinchi va eng muhim muammo — shaxsiy daxlsizlik huquqi. Biometrik ma'lumotlar odamning eng sezgir shaxsiy ma'lumotlari sirasiga kiradi va ularni oshkor qilish yoki sudda namoyish etish qaytarib bo‘lmaydigan oqibatlarga olib kelishi mumkin. Yevropa Ittifoqi GDPR qoidalari va BMT Inson huquqlari qo‘mitasining qarorlariga binoan, biometrik ma'lumotlarni yig‘ish va qayta ishlash faqat qat'iy zarurat, mutanosiblik va qonuniy maqsad asosida amalga oshirilishi mumkin. XJS ham o‘z protsessual qoidalarida biometrik dalillarni yig‘ish va taqdim

etish uchun maxsus protokol ishlab chiqishi kerak. Mazkur protokolda jabrlanuvchilar va guvohlarning yuzlarini xiralashtirish, ovozini o‘zgartirish va ularning biometrik shaxsini oshkor qilmasdan dalil sifatida foydalanish imkoniyatlari aniq belgilanishi zarur. Metaverse, kvant kompyuterlari va biometrik texnologiyalar Xalqaro Jinoyat Sudi uchun yangi ufqlar ochish bilan birga, nazorat qilinmasa, sud protsessining asosiy tamoyillariga putur yetkazishi mumkin. Shu bois, texnologik innovatsiyalarga moslashish nafaqat texnik, balki chuqur huquqiy va axloqiy yondashuvni talab qiladi.

Xalqaro Jinoyat Sudi oldida turgan raqamli dalillar bilan bog‘liq chaqiriqlar nafaqat texnik, balki konseptual xarakterga ega. Yuqorida olib borilgan tahlillar shuni ko‘rsatmoqdaki, Rim statuti qabul qilingan paytda mavjud bo‘lmagan raqamli voqelik bugungi kunda sud yurisdiksiyasi, protsessual adolat va dalillar ishonchliligi masalalarini butunlay yangi kontekstga olib chiqmoqda. Ochiq manbalardagi ma’lumotlar, sun’iy yo‘ldosh suratlari, shifrlangan aloqa yozuvlari, biometrik identifikatorlar, metaversedagi izlar va sun’iy intellekt yordamida qayta ishlangan materiallar XJS amaliyotining ajralmas qismiga aylanib bormoqda. Biroq, sud ushbu imkoniyatlardan to‘liq foydalanish uchun bir qator jiddiy to‘siqlarni yengib o‘tishi zarur. Birinchi to‘siq — huquqiy asosning yetishmasligi. Rim statutida raqamli dalillar to‘g‘risida maxsus moddalar yo‘qligi sababli, har bir ishda turlicha yondashuvlar qo‘llanilmoqda. Ikkinchi to‘siq — texnologik imkoniyatlarning notekisligi. Prokuratura zamonaviy vositalarni qo‘llashga intilayotgan bir paytda, himoya tomoni ko‘pincha bir xil darajadagi texnik resurslardan mahrum. Uchinchi to‘siq — ishonchlilik va xavfsizlik muammolari. Deepfake, kvant tahdidi va biometrik manipulyatsiya imkoniyatlari dalillarning haqqoniyligiga bo‘lgan ishonchni zaiflashtirmoqda. Mazkur muammolarni hal etish va Xalqaro Jinoyat Sudining raqamli asrdagi samaradorligini ta’minlash uchun quyidagi takliflar ilgari suriladi:

Birinchidan, Rim statuti ishtirokchi-davlatlar assambleyasi tomonidan raqamli dalillar bo‘yicha alohida qo‘shimcha protokol qabul qilinishi zarur. Ushbu protokolda raqamli dalillarning ta’rifi, ularni to‘plash, saqlash va sudga taqdim etish standartlari, shuningdek dalillar zanjiri (chain of custody) bo‘yicha minimal talablar aniq belgilanishi kerak. Protokol Berkeley protokoli va Tallin qo‘llanmasi kabi mavjud xalqaro standartlarga asoslanishi, biroq majburiy yuridik kuchga ega bo‘lishi lozim.

Ikkinchidan, XJS qoshida doimiy faoliyat yurituvchi "Raqamli dalillar va texnologik tahlil markazi" tashkil etilishi taklif qilinadi. Mazkur markaz quyidagi funksiyalarni bajarishi kerak: prokuratura va himoya tomoni uchun mustaqil raqamli ekspertiza o‘tkazish; deepfake va boshqa manipulyatsiyalarni aniqlash bo‘yicha ilg‘or texnologiyalarni joriy etish; sudyalar, prokurorlar va advokatlar uchun raqamli savodxonlik bo‘yicha muntazam o‘quv dasturlarini amalga oshirish; hamda post-kvant kriptografiyasi kabi istiqbolli himoya vositalarini sinovdan o‘tkazish.

Uchinchidan, XJS ichki protsessual qoidalariga raqamli dalillarning autentifikatsiyasi bo‘yicha aniq mezonlar kiritilishi lozim. Xususan, har bir raqamli dalil kamida ikki mustaqil manba orqali tasdiqlanishi (cross-verification), xesh-kod bilan himoyalanishi va uning barcha metama’lumotlari sudga taqdim etilishi shart qilib belgilanishi kerak. Sun’iy intellekt yordamida olingan yoki qayta ishlangan dalillar uchun esa alohida ekspertiza talabi joriy etilishi zarur.

To‘rtinchidan, milliy yurisdiksiyalar bilan raqamli ma’lumot almashish mexanizmi takomillashtirilishi kerak. Buning uchun shifrlangan va standartlashtirilgan yagona raqamli platforma yaratilishi, u orqali milliy tergov organlari va XJS prokuraturasi o‘rtasida dalillar tezkor va xavfsiz almashinishi ta’minlanishi lozim. Platforma komplementarlik prinsipini mustahkamlashga xizmat qiladi va milliy organlarning transchegaraviy raqamli ma’lumotlarga kirish imkonini oshiradi.

Beshinchidan, biometrik va metaverse kabi yangi turdagi dalillar bilan ishlash bo‘yicha maxsus yo‘riqnomalar ishlab chiqilishi zarur. Ushbu yo‘riqnomalarda biometrik ma’lumotlarni yig‘ishda inson huquqlari standartlariga rioya qilish, jabrlanuvchilarning shaxsiy daxlsizligini himoya qilish (masalan, yuzni xiralashtirish, ovozni o‘zgartirish) va virtual muhitdan olingan dalillarni tekshirish tartibi batafsil yoritilishi kerak.

Oltinchidan, XJS o‘z qarorlarida raqamli dalillar bo‘yicha izchil pretsedent huquqini shakllantirishi lozim. Sud har bir raqamli dalilning qabul qilinishi yoki rad etilishi sabablarini batafsil asoslab borishi, kelajakdagi ishlar uchun bashorat qilinadigan huquqiy asos yaratishi kerak. Bu bilan protsessual aniqlik ta’minlanadi va taraflarning huquqlari kafolatlanadi.

Yettinchidan, sun’iy intellekt texnologiyalarining sud jarayonida qo‘llanilishiga oid axloqiy va huquqiy cheklovlar belgilanishi zarur. Avtomatlashtirilgan tahlil vositalarining xulosalari faqatgina inson ekspert tomonidan tasdiqlangandan so‘ng dalil sifatida qabul qilinishi mumkinligi haqida aniq qoida kiritilishi lozim.

Sakkizinchidan, kvant tahdidiga qarshi tayyorgarlik ko‘rish maqsadida XJS o‘zining barcha raqamli arxivlari va aloqa tizimlarini bosqichma-bosqich post-kvant kriptografiyasi standartlariga o‘tkazishi kerak. Bu jarayon kechiktirib bo‘lmaydigan ustuvor vazifa sifatida qaralishi lozim, chunki "hozir to‘plab, keyin ochish" (harvest now, decrypt later) hujumlari bugunoq amalga oshirilmoqda.

To‘qqizinchidan, jabrlanuvchilar va guvohlarning raqamli muhitda himoyasi kuchaytirilishi kerak. Raqamli dalillarni taqdim etishda ularning xavfsizligi, shaxsiy daxisizligi va ruhiy salomatligini himoya qilish bo‘yicha maxsus protokollar joriy etilishi, zarur hollarda yopiq sud majlislari yoki anonimlashtirilgan ko‘rsatmalar berish imkoniyatlari kengaytirilishi lozim.

O‘ninchidan, fuqarolik jamiyati va nodavlat tashkilotlar bilan hamkorlik standartlashtirilishi kerak. Bellingcat, Syrian Archive kabi tashkilotlar tomonidan taqdim etiladigan analitik materiallarning sud tomonidan qabul qilinishi tartibi aniq belgilanishi, ular mustaqil ekspertiza va metama’lumotlar tekshiruvidan o‘tkazilishi shart qilib qo‘yilishi lozim.

Umuman olganda, raqamli dalillar Xalqaro Jinoyat Sudi uchun ulkan imkoniyatlar yaratish bilan birga, mavjud huquqiy tizim va protsessual mexanizmlarni jiddiy sinovdan o‘tkazmoqda. Ushbu sinovdan muvaffaqiyatli o‘tish sudning nafaqat texnologik moslashuvchanligiga, balki adolat, tenglik va inson huquqlariga sodiqligini amalda namoyon etish qobiliyatiga bog‘liq. Yuqorida sanab o‘tilgan takliflar aynan shu muvozanatni ta’minlashga qaratilgan bo‘lib, ularning izchil amalga oshirilishi Xalqaro Jinoyat Sudining nufuzini mustahkamlashga va xalqaro jinoyatchilarning jazosiz qolishiga barham berishga xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. Rim statuti (1998). Xalqaro Jinoyat Sudi Nizomi, A/CONF.183/9.
2. Berkeley Protocol on Digital Open Source Investigations (2018). BMT Inson huquqlari bo‘yicha Oliy komissari boshqarmasi & UC Berkeley.
3. Croci, L. (2025). The International Criminal Court and Digital Evidence. i-lex, 18(1), 1-17.
4. McDermott, Y., Hausknecht, A. & Liefgreen, A. (2026). ICC judges’ perspectives on user-generated evidence. Oñati Socio-Legal Series.
6. Liulina, A. (2025). Evidentiary Digital Platforms: Al Mahdi and Al Hassan Cases. International Criminal Law Review, 25(5), 840-868.
7. Nilaei Sangari, Z. & Mohammadi, A. (2026). International Criminal Court and Digital Evidence. Journal of Criminal Law Research.
8. Gavrysh, K. (2025). Digital Evidence in the Practice of the ICC: Ukraine Proceedings.
9. ICC Office of the Prosecutor. (2024). Harmony Project Overview.

10. Lexology. (2026). The wrong type of legal spectacles: authenticity in litigation.
11. Bellingcat. (2023). Guide to Open Source Verification in Conflict Zones.
12. Human Rights Center, UC Berkeley. (2019). Digital Fingerprints: Using Open Source Data to Document Human Rights Abuses.
13. Yevropa sudining shaxsiy ma'lumotlar himoyasi bo'yicha ishlari: Big Brother Watch v. UK (2021), Szabó va Vissy v. Hungary (2016).
14. OTP, ICC. (2022). Policy on the Crime of Aggression.
15. Syrian Archive. (2020). Digital Evidence in International Criminal Proceedings: Challenges and Best Practices.
16. Khan, K. (2024). Statement of the Prosecutor to the Assembly of States Parties.