INTERNET TARMOG‘IDA EKSTREMISTIK FAOLIYAT BILAN BOG‘LIQ JINOYATLARNI TERGOV QILISHDA RAQAMLI DALILLARDAN FOYDALANISH MUAMMOLARI

Muallif:IIV Akademiyasi Oliy ta’limdan keying ta’lim fakulteti doktoranti Hoshilov

Ulug‘bek Muhiddin o‘g‘li

Bugungi kunda ekstremistik g‘oyalarni tarqatish, tarafdorlarni jalb etish va jamoat tartibiga tahdid soluvchi materiallarni ommalashtirish asosan internet tarmog‘i, ijtimoiy tarmoqlar va messenjerlar orqali amalga oshirilmoqda. Shu sababli bu toifadagi jinoyatlarni tergov qilishda raqamli dalillar (elektron izlar) asosiy isbotlash vositalaridan biriga aylandi. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksiga ko‘ra, ish bo‘yicha haqiqatni aniqlashda foydalaniladigan har qanday faktik ma’lumotlar dalil sifatida e’tirof etiladi[1], biroq raqamli axborotning o‘ziga xos tabiati uning protsessual maqomi va ishonchliligini ta’minlashda bir qator muammolarni keltirib chiqaradi.

Birinchidan, raqamli dalillarning protsessual maqomi masalasi to‘liq hal etilmagan. Amaldagi qonunchilikda elektron ma’lumotlar alohida dalil turi sifatida mustahkamlanmagan, ular odatda hujjat yoki buyumli dalil sifatida rasmiylashtiriladi. Bu esa axborotning metama’lumotlari, yaratilgan vaqti, muallifligi va o‘zgartirilmaganligini tasdiqlashda amaliy qiyinchiliklar tug‘diradi. Ekstremizmga qarshi kurashish to‘g‘risidagi qonun ekstremistik materiallarning tarqatilishini taqiqlaydi[2], jinoiy javobgarlik esa Jinoyat

[1]O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi (1994 yil 22 sentyabr), 81-modda (Dalillar).

[2]O‘zbekiston Respublikasining «Ekstremizmga qarshi kurashish to‘g‘risida»gi Qonuni, 2018 yil 30 iyul, O‘RQ-489-son.

kodeksining tegishli moddalarida nazarda tutilgan[3], ammo bu normalarni qo‘llashda elektron dalilni to‘plash tartibi yetarlicha batafsil yoritilmagan.

Ikkinchidan, dalilning yaxlitligi va ishonchliligini ta’minlash muammosi mavjud. Raqamli axborot oson o‘zgartiriladi, o‘chiriladi yoki ko‘chiriladi; shu sababli uni aniqlash, to‘plash, nusxalash va saqlash jarayonida xesh-qiymat (hash) hisoblash, yozishdan himoyalangan holda nusxa olish hamda dalillar harakati zanjirini (chain of custody) yuritish zarur. Bu tamoyillar xalqaro standartda tavsiflangan[4] va sud-ekspertiza amaliyotida keng qo‘llaniladi[5]. Amaliyotda esa tergovchilar ko‘pincha skrinshot yoki oddiy kuzatuv bayonnomasi bilan cheklanadi, bu esa sudda dalilning qabul qilinmasligi xavfini oshiradi.

Uchinchidan, ekstremistik kontentning transchegaraviy xususiyati va ma’lumotlarga masofadan kirish muammosi dolzarb. Serverlar odatda xorijiy yurisdiksiyalarda joylashgan bo‘lib, xorijiy provayderlardan ma’lumot olish uchun huquqiy yordam ko‘rsatish tartibi uzoq vaqt talab qiladi. Bu esa dalillarning yo‘qolish xavfini kuchaytiradi. Xalqaro hamkorlikning huquqiy asoslari Kibermakon jinoyatlari to‘g‘risidagi Budapesht konvensiyasida[6] hamda ekstremizmga qarshi kurash bo‘yicha Shanxay konvensiyasida[7] ifodalangan bo‘lib, ularning mexanizmlaridan samarali foydalanish tergov amaliyotida muhim ahamiyat kasb etadi.

---

[3]O‘zbekiston Respublikasining Jinoyat kodeksi (1994 yil 22 sentyabr), 244-1 va 244-2-moddalar.

[4]ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

[5]Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. — Waltham: Academic Press, 2011.

[6]Convention on Cybercrime (Budapest, 23 November 2001), ETS No. 185, Council of Europe, 16-, 19- va 29-moddalar.

[7]Terrorizm, separatizm va ekstremizmga qarshi kurashish to‘g‘risidagi Shanxay konvensiyasi (Shanxay, 2001 yil 15 iyun).

To‘rtinchidan, shifrlash, anonimlashtirish vositalari (VPN, Tor, end-to-end shifrlangan messenjerlar), yo‘qolib ketuvchi xabarlar va soxta profillar shaxsni identifikatsiya qilish hamda ma’lumotlarni qo‘lga kiritishni murakkablashtiradi. Bunday sharoitda shaxsning aybdorligini isbotlash ko‘plab bilvosita raqamli izlar (IP-manzillar, qurilma identifikatorlari, geolokatsiya ma’lumotlari) majmuasini baholashni talab qiladi.

Beshinchidan, elektron qurilmalar va axborot tashuvchilar bilan bog‘liq tergov harakatlarini o‘tkazish tartibi muammoli bo‘lib qolmoqda. Smartfon, kompyuter, bulutli xotira va ijtimoiy tarmoq akkauntlarini ko‘zdan kechirish, tintuv o‘tkazish yoki olib qo‘yish chog‘ida ma’lumotlarning o‘zgarib ketishi, qurilma parol yoki biometrik himoya bilan bloklanishi hamda masofaviy o‘chirib yuborilishi xavfi mavjud. Shu bilan birga, bunday harakatlar shaxsning shaxsiy hayoti, yozishmalari va ma’lumotlarining daxlsizligi bilan bevosita bog‘liq bo‘lib, ular Konstitutsiya bilan kafolatlanadi[8]. Shu sababli tergov harakatlarining asosliligi, mutanosibligi va sud nazoratini ta’minlash zarur, aks holda to‘plangan dalil maqbulligini yo‘qotishi mumkin.

Oltinchidan, kompyuter-texnik ekspertizasi sohasida yagona uslubiy yondashuv va yetarli kadrlar salohiyati mavjud emas. Ekspert oldiga qo‘yiladigan savollar ko‘pincha umumiy xarakterga ega bo‘lib, ma’lumotni tiklash, fayl tizimini tahlil qilish, o‘chirilgan axborotni qayta tiklash va foydalanuvchi faoliyatini xronologik tiklash kabi chuqur masalalar yetarlicha aniqlashtirilmaydi[9]. Raqamli dalillarni tahlil qilish va sharhlash bo‘yicha xalqaro tavsiyalar ekspert xulosasining takrorlanuvchanligi va

[8]O‘zbekiston Respublikasi Konstitutsiyasi (2023 yil 30 aprel kuni umumxalq referendumida qabul qilingan yangi tahrir): shaxsiy hayot, yozishmalar va ma’lumotlar daxlsizligi kafolatlariga oid normalar.

[9]Carrier B. File System Forensic Analysis. — Boston: Addison-Wesley, 2005.

asoslanganligiga alohida e’tibor qaratadi[10]. Amaliyotda esa turli ekspertlar bir xil ma’lumotga nisbatan turlicha xulosa berishi, bu esa sudda ekspert xulosasining ishonchliligiga shubha tug‘dirishi mumkin.

Yettinchidan, tergovchilarning raqamli savodxonligi va moddiy-texnik ta’minot masalasi dolzarb. Ekstremistik faoliyat bilan bog‘liq ishlarda tergovchi nafaqat huquqiy bilimga, balki ijtimoiy tarmoqlar, messenjerlar, kriptovalyutalar va bulutli xizmatlarning ishlash tamoyillarini tushunishga ham muhtoj. Maxsus dasturiy-apparat vositalarining yetishmasligi, ularning yuqori narxi va doimiy yangilanib turishi zarurati qo‘shimcha qiyinchilik yaratadi. Natijada ko‘plab hollarda raqamli iz o‘z vaqtida qayd etilmaydi, tergov esa asosan guvohlar ko‘rsatmalari va bilvosita dalillarga tayanib qoladi.

Sakkizinchidan, axborot platformalari bilan hamkorlik masalasi alohida e’tiborni talab qiladi. Ijtimoiy tarmoq egalari foydalanuvchi ma’lumotlarini saqlash muddatlari, so‘rovlarni ko‘rib chiqish tartibi va ma’lumotlarni berish shartlari bo‘yicha turlicha siyosat yuritadi. Xalqaro hujjatlarda ma’lumotlarni tezkor saqlab qo‘yish (data preservation) mexanizmi nazarda tutilgan bo‘lib, uni milliy amaliyotga joriy etish dalillarning yo‘qolishini oldini olishga xizmat qiladi. Shu bilan birga, provayderlar bilan rasmiy aloqa kanallari yaratilmaguncha, tergov organlari uchun ma’lumotni olish jarayoni uzoq davom etaveradi.

To‘qqizinchidan, sun’iy intellekt yordamida yaratilgan soxta kontent (deepfake), tahrirlangan skrinshotlar va avtomatlashtirilgan akkauntlar (botlar) dalillarning haqiqiyligini tekshirishni yanada murakkablashtirmoqda. Bir tomondan, ekstremistik targ‘ibot materiallari soxta tarzda yaratilishi yoki tahrirlanishi, ikkinchi tomondan, aybsiz shaxsga nisbatan uydirma raqamli «dalil» tayyorlanishi mumkin. Shu sababli har bir raqamli dalil uchun uning

[10]ISO/IEC 27042:2015. Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. Geneva: ISO, 2015.

kelib chiqishi, yaratilish sharoiti va o‘zgartirilmaganligini tasdiqlovchi mustaqil texnik asoslar talab etiladi, sud esa bunday dalilni boshqa ish materiallari bilan birgalikda baholashi lozim.

Raqamli dalillarning maqbulligini baholash mezonlari ham amaliyotda yagona shaklga keltirilmagan. Sud dalilni baholashda uning mosligi (relevantligi), maqbulligi va ishonchliligini tekshiradi; raqamli axborot uchun bu mezonlar qo‘shimcha texnik ma’no kasb etadi. Masalan, dalil qanday qurilmadan olingani, qaysi dasturiy vosita bilan nusxalangani, jarayon kimlar ishtirokida va qanday hujjatlashtirilgani muhim ahamiyatga ega. Bu ma’lumotlar bayonnomada yetarlicha aks ettirilmasa, himoya tomoni dalilning yaxlitligiga shubha bildirishi, sud esa uni ishdan chiqarib tashlashi mumkin. Shu sababli ish yuritish hujjatlarida texnik parametrlarni batafsil qayd etish talab etiladi.

Ekstremizm bilan bog‘liq ishlarda yana bir o‘ziga xos muammo — kontentning ekstremistik xarakterini aniqlash va uni tarqatuvchi shaxsning qasdini isbotlashdir. Raqamli iz faktni tasdiqlaydi, ammo shaxsning maqsadi, material mazmuniga munosabati va uni tarqatishdagi ongli niyatini ochib bermasligi mumkin. Shu sababli raqamli dalillar diniy, lingvistik va psixologik ekspertizalar bilan birgalikda baholanishi, material ekstremistik deb topilishi esa sud qarori yoki vakolatli ekspert xulosasi bilan asoslanishi kerak. Aks holda oddiy foydalanuvchining beixtiyor qayta yuborgan xabari ham jinoiy ish asosiga aylanib qolishi xavfi mavjud.

Ushbu muammolarni bartaraf etishda ilg‘or xorijiy tajribani o‘rganish va milliy sharoitga moslashtirish foydali. Ko‘plab davlatlarda raqamli dalillar bilan ishlash bo‘yicha yagona yo‘riqnomalar, maxsus kiberjinoyatlar bo‘linmalari va ekspertlarni sertifikatlash tizimi joriy etilgan. O‘zbekiston uchun ham tergov organlari, prokuratura, sud-ekspertiza markazlari va axborot xavfsizligi sohasidagi mutaxassislarni o‘z ichiga oluvchi idoralararo hamkorlik

mexanizmini yo‘lga qo‘yish, shuningdek, tergovchilar uchun muntazam o‘quv kurslarini tashkil etish samarali natija berishi mumkin.

Shuningdek, shaxsga doir ma’lumotlarni himoya qilish talablari raqamli dalillar bilan ishlashda muhim cheklov bo‘lib xizmat qiladi. Qurilma yoki akkauntdan nusxa olinganda ishga aloqador bo‘lmagan uchinchi shaxslarning yozishmalari va ma’lumotlari ham qo‘lga kiritilishi mumkin. Bunday ma’lumotlarni saqlash, ulardan foydalanish va yo‘q qilish tartibi aniq belgilanmasa, shaxs huquqlari buzilishi xavfi paydo bo‘ladi. Shu sababli dalil sifatida faqat ish uchun zarur bo‘lgan ma’lumotlarni ajratib olish va qolgan axborotni himoyalangan tarzda saqlash tamoyili joriy etilishi maqsadga muvofiqdir.

Xulosa qilib aytganda, muammolarni hal etish uchun: raqamli dalillarning tushunchasi va to‘plash tartibini Jinoyat-protsessual kodeksida aniq belgilash; tergovchi, prokuror va sudyalar uchun raqamli kriminalistika bo‘yicha maxsus tayyorgarlikni yo‘lga qo‘yish; ekspert muassasalarining texnik bazasini kuchaytirish; ijtimoiy tarmoq va xorijiy provayderlar bilan hamkorlik mexanizmlarini takomillashtirish maqsadga muvofiqdir.