Shaxsga doir ma’lumotlarni ochiq manbalardan yig‘ish: kiber kriminalistika va shaxs daxlsizligi huquqi o‘rtasidagi muvozanat

Butayev Asadbek Anvarjon o‘g‘li

Toshkent davlat yuridik universiteti

Annotatsiya. Maqolada ochiq manbalardan shaxsga doir ma’lumotlarni yig‘ish usuli (OSINT)ning kiber kriminalistikadagi o‘rni hamda uning shaxs daxlsizligi huquqi bilan o‘zaro munosabati huquqiy jihatdan tahlil qilinadi. Fotosuratlar metama’lumotlari misolida “ochiq” ma’lumotning huquqiy maqomi, shaxsga doir ma’lumotlarni qayta ishlash tamoyillari, OSINT natijalarining jinoyat protsessida dalil sifatidagi maqbulligi masalalari ko‘rib chiqiladi. O‘zbekiston qonunchiligi Yevropa Ittifoqining GDPR tajribasi bilan qiyoslanib, mavjud bo‘shliqlar aniqlanadi va qonunchilikni takomillashtirish bo‘yicha takliflar beriladi.

Kalit so‘zlar: OSINT, shaxsga doir ma’lumotlar, metama’lumotlar, EXIF, shaxs daxlsizligi, kiber kriminalistika, elektron dalil, GDPR.

Kirish

Raqamli texnologiyalarning jadal rivojlanishi natijasida har bir inson kundalik faoliyati davomida katta hajmdagi “raqamli iz”larni qoldirmoqda: ijtimoiy tarmoqlardagi profillar, joylashuv ma’lumotlari, fotosuratlar va ularga biriktirilgan metama’lumotlar shular jumlasidandir. Bunday ma’lumotlarning aksariyati texnik jihatdan ochiq manbalarda mavjud bo‘lib, ularni to‘plash va tahlil qilish usuli xalqaro amaliyotda OSINT (Open Source Intelligence, ochiq kodli razvedka ma’lumotlari) deb ataladi.

OSINT bir tomondan kiber kriminalistikada jinoyatlarni fosh etish, shaxslarni aniqlash va dalillar to‘plashning samarali vositasi bo‘lsa, ikkinchi tomondan

firibgarlik, ijtimoiy muhandislik va shaxsni ta’qib qilishda ham qo‘llanilmoqda. Jahon miqyosida Cybersecurity Ventures hisob-kitoblariga ko‘ra, “2025-yilda kiberjinoyatlarning iqtisodiy zarari taxminan 10,5 trillion AQSh dollarini tashkil etgan”[1]. FBI Internet Crime Complaint Center ma’lumotlariga ko‘ra, “2025-yilda faqat AQShda 1 milliondan ortiq shikoyat qayd etilib, zarar 20,877 milliard dollarga yetgan (2024-yilga nisbatan 26 foizga o‘sish)”[2]. Surfshark tadqiqotiga ko‘ra, “shu yili dunyo bo‘ylab 425,7 million akkaunt ma’lumotlari sizib chiqqan”[3]. O‘zbekistonda Ichki ishlar vazirligi ma’lumotlariga ko‘ra, 2021–2025-yillarda kiberjinoyatlar soni 11 baravarga oshib, 4 865 tadan 62 440 taga yetgan; fuqarolarga jami 3,73 trillion so‘m zarar yetkazilgan. 2024-yilda kiberjinoyatlar umumiy jinoyatchilikning 44,4 foizini (58 800 ta) tashkil etgan, ularning 98 foizi bank kartalari bilan bog‘liq firibgarlik va o‘g‘irliklardir.

Shu sababli muhim huquqiy muammo yuzaga keladi: ma’lumotning ochiq bo‘lishi uni erkin yig‘ish, saqlash va qayta ishlash mumkinligini anglatmaydi. Biroq OSINT faoliyatining, ayniqsa huquqni muhofaza qiluvchi organlar va kriminalistik ekspertlar tomonidan amalga oshirilishining huquqiy chegaralari, shuningdek, bunday yo‘l bilan olingan ma’lumotlarning dalil sifatidagi maqbulligi qonunchilikda aniq o‘z aksini topmagan. Maqolaning maqsadi ana shu muvozanatni ta’minlovchi huquqiy mexanizmlarni tahlil qilish va takliflar ishlab chiqishdir.

1. OSINT tushunchasi va uning huquqiy tabiati

OSINT ommaviy foydalanish mumkin bo‘lgan manbalar (ijtimoiy tarmoqlar, yangilik saytlari, ochiq reyestrlar, fotosuratlar, forumlar, ma’lumotlar bazalarining sizib chiqqan nusxalari kabi)dan axborot to‘plash, uni tahlil qilish va foydali xulosaga aylantirish jarayonidir. Shuni alohida ta’kidlash lozimki, OSINTning texnik jihatdan “ochiq” bo‘lishi uning huquqiy jihatdan “ruxsat etilgan” ekanini bildirmaydi. Tahlilda uchta mezonni farqlash maqsadga muvofiq:

manbaning qonuniyligi: ma’lumot qonuniy joylashtirilganmi, yoki sizib chiqqan,

noqonuniy olingan bazalardan keltirilganmi;

yig‘uvchi subyekt: huquqni muhofaza qiluvchi organ, kriminalistik ekspert, jurnalist, oddiy shaxs yoki jinoyatchi;

maqsad va hajm: bitta faktni tekshirish bilan shaxs haqida tizimli “dosye” (profil) shakllantirish o‘rtasida muhim huquqiy farq mavjud, chunki ayrim ochiq ma’lumotlarning agregatsiyasi (yig‘ib birlashtirilishi) o‘zi yangi xavf yaratadi.

2. Shaxsga doir ma’lumot va metama’lumotlarning huquqiy maqomi

“Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni shaxsga doir ma’lumotni muayyan jismoniy shaxsga taalluqli yoki uni identifikatsiya qilish imkonini beruvchi axborot sifatida belgilaydi. Shu ma’noda fotosurat metama’lumotlari (EXIF) e’tiborga loyiq. Ular odatda quyidagilarni o‘z ichiga oladi:

surat olingan sana va vaqt;

GPS koordinatalari (aniq joylashuv);

qurilma modeli, ba’zan seriya raqami va dasturiy ta’minot; tahrirlash tarixi.

Alohida olinganda bu ma’lumotlar shaxsni to‘g‘ridan-to‘g‘ri aniqlamasligi mumkin. Lekin ularning boshqa ochiq ma’lumotlar bilan (profil, do‘stlar ro‘yxati, boshqa suratlar) birlashtirilishi natijasida shaxsning yashash joyi, ish joyi, odatlari va harakatlanish jadvali aniqlanadi. Shu sababli metama’lumotlar, ayniqsa GPS koordinatalari, bilvosita identifikatsiya imkonini bergani uchun shaxsga doir ma’lumot sifatida baholanishi lozim, degan fikr asosli. Bu xulosa Yevropa Ittifoqi GDPR ning 4-moddasi 1-bandidaga mos keladi: unda shaxsga doir ma’lumot ta’rifida joylashuv ma’lumotlari va onlayn identifikatorlar alohida tilga olinadi.

Milliy qonunchilikda metama’lumotlar va qurilma identifikatorlari shaxsga doir ma’lumot tarkibida aniq nomlanmagan. Bu amaliyotda turlicha sharhlashga olib kelishi mumkin.

3. O‘zbekiston qonunchiligida himoya mexanizmlari

Tahlil qilinishi lozim bo‘lgan normativ-huquqiy hujjatlar quyidagicha:

Konstitutsiya: shaxsiy hayot daxlsizligi va shaxsga doir ma’lumotlarni himoya qilish huquqi kafolati.

“Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun: qayta ishlash tamoyillari (qonuniylik, maqsadga muvofiqlik, ma’lumotlar hajmining ortiqcha emasligi), subyektning roziligi, subyekt huquqlari, operator va mulkdorning majburiyatlari.

Kiberxavfsizlik, axborotlashtirish va axborot erkinligi sohasidagi qonunlar: axborotni himoya qilish tizimi va uni olish erkinligi o‘rtasidagi balans.

Javobgarlik normalari: Jinoyat kodeksi va Ma’muriy javobgarlik to‘g‘risidagi kodeksning shaxsiy hayot daxlsizligi va shaxsga doir ma’lumotlar qonunchiligini buzishga oid moddalari, shuningdek axborot texnologiyalari sohasidagi jinoyatlar bobi.

Mazkur normalar OSINT faoliyatini to‘g‘ridan-to‘g‘ri tartibga solmaydi. Natijada quyidagi masalalar ochiq qolmoqda: ochiq ijtimoiy tarmoqdagi profil ma’lumotlarini yig‘ishda subyekt roziligi talab etiladimi; huquqni muhofaza qiluvchi organlar OSINT yig‘ishda sud sanksiyasi yoki boshqa protsessual asosga muhtojmi, xususiy ekspertlar uchun cheklovlar qanday.

4. Xorijiy tajriba: GDPR va xalqaro hujjatlar

GDPR ochiq ma’lumotning ham “ochiq” bo‘lgani uchun erkin qayta ishlanishiga yo‘l qo‘ymaydi. Muhim jihatlari:

5- modda tamoyillari: qonuniylik, maqsad bilan cheklanganlik, ma’lumotlarni minimallashtirish, aniqlik, saqlash muddati va yaxlitlik;

6- modda: qayta ishlash uchun huquqiy asoslar, jumladan rozilik va “qonuniy manfaat” (1-band, f kichik band), bu asos subyektning huquq va erkinliklari bilan muvozanatda tekshiriladi;

profilash va avtomatlashtirilgan qaror qabul qilishga cheklovlar;

huquqni muhofaza qilish maqsadlarida qayta ishlash alohida tartibga solingan (Yevropa Ittifoqining Law Enforcement Directive hujjati).

Shuningdek, Yevropa Kengashining 108-Konvensiyasi (va uning yangilangan 108+ tahriri) shaxsga doir ma’lumotlarni himoya qilishning xalqaro standartini, Budapesht konvensiyasi (2001) esa kiberjinoyatlarga qarshi kurash va elektron dalillar bo‘yicha hamkorlik asoslarini belgilaydi.

Tahlil shuni ko‘rsatadiki, GDPR asosidagi tizimda OSINT yig‘uvchi ham shaxsga doir ma’lumotlar operatori deb hisoblanadi va qonuniy asos, maqsad hamda proporsionallik talablariga bo‘ysunadi. O‘zbekiston qonunchiligida esa bunday talab OSINT kontekstida aniqlashtirilmagan.

5. OSINT natijalarining jinoyat protsessida dalil sifatidagi maqbulligi

OSINT orqali olingan ma’lumot dalil sifatida qabul qilinishi uchun odatda quyidagi talablar bajarilishi kerak (jinoyat-protsessual qonunchilikdagi dalilning maqbulligi, ishonchliligi va yetarliligi mezonlari asosida:

Manba va olish tartibi hujjatlashtirilishi: qaysi manba, qachon, kim tomonidan, qaysi vosita bilan olingani.

Asl holatni saqlash: sahifa yoki faylning ekran nusxasi bilan cheklanmay, imkon qadar asl faylning o‘zi saqlanishi.

Yaxlitlikni tasdiqlash: fayl uchun xesh qiymat (masalan, SHA-256) hisoblanib, protokolga yozilishi.

Isbotlash zanjiri (chain of custody): faylni olgandan sudga taqdim etguncha bo‘lgan har bir qo‘ldan o‘tish qayd etilishi.

Ekspert xulosasi va takrorlanuvchanlik: boshqa mutaxassis xuddi shu usul bilan bir xil natijaga kelishi mumkin bo‘lishi.

Qonuniy olinganlik: shaxs daxlsizligini buzib olingan ma’lumot “nomaqbul dalil”

deb topilish xavfi bor.

Bu mezonlar OSINT uchun ishlab chiqilmaganligi, amaliyotda elektron dalillarga oid umumiy normalarga tayanishga to‘g‘ri kelishi, mavjud bo‘shliqlardan biridir.

6. Amaliy eksperiment: fotosurat metama’lumotlari

Metama’lumotlarning shaxsni identifikatsiya qilish imkoniyatini ko‘rsatish maqsadida qisqa eksperiment o‘tkazildi. **Etik talablarga muvofiq faqat muallifning o‘zi olgan va uning o‘ziga tegishli suratlardan foydalanildi; uchinchi shaxslarning ma’lumotlari tahlil qilinmadi.**

Usul. Smartfonda olingan fotosurat fayl ko‘rinishida [ExifTool yoki operatsion tizimning “Xossalar” oynasi] yordamida tekshirildi.

Natija. Aniqlangan ma’lumotlar surat egasining qayerda va qachon bo‘lganini, qaysi qurilmadan foydalanishini ko‘rsatdi, boshqa ochiq ma’lumotlar bilan birga esa yashash joyi yoki odatlarini taxmin qilish imkonini beradi.

Himoya choralari. Telefon kamerasi sozlamalarida geoteg (joylashuv yozuvi)ni o‘chirish, fayl yuborishdan oldin metama’lumotlarni tozalash (masalan, ExifTool yordamida), ijtimoiy tarmoqlar yuklashda metama’lumotlarni o‘zi o‘chirishini, lekin bu hamma platformada va fayl sifatida yuborilganda kafolatlanmasligini hisobga olish.

Xulosa. Eksperiment GPS koordinatalari va qurilma ma’lumotlari uchinchi shaxs tomonidan yig‘ilsa, shaxsga doir ma’lumotni qayta ishlash hisoblanishi, demak, qonuniy asos va maqsad talab qilinishini tasdiqlaydi.

1. Muammolar va qonunchilikni takomillashtirish bo‘yicha takliflar

Tahlil asosida quyidagi takliflar ilgari suriladi:

“Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunda metama’lumotlar, geolokatsiya ma’lumotlari va qurilma identifikatorlarining shaxsga doir ma’lumot tarkibiga kirishini aniq

belgilash.

Huquqni muhofaza qiluvchi organlar tomonidan OSINT usullaridan foydalanish asoslari, chegaralari va nazorat mexanizmini (maqsad, proporsionallik, saqlash muddati) normativ jihatdan tartibga solish.

Jinoyat-protsessual qonunchilikda ochiq manbalardan olingan raqamli ma’lumotlarni qayd etish va dalil sifatida taqdim etish tartibini (xesh, metama’lumotlarni saqlash, chain of custody) belgilash.

Ochiq ma’lumotlarni agregatsiya qilish orqali shaxsning batafsil profilini shakllantirish holatlari uchun javobgarlik yoki cheklov mexanizmini ko‘rib chiqish.

Fuqarolarning raqamli savodxonligini oshirish: metama’lumotlar va geoteg xavfi bo‘yicha axborot kampaniyalari.

OSINT kiber kriminalistikaning samarali vositasi bo‘lib, bir vaqtning o‘zida shaxs daxlsizligi huquqi uchun jiddiy xavf tug‘diradi. “Ochiq ma’lumot” tushunchasi “erkin foydalaniladigan ma’lumot” degani emas: metama’lumotlar kabi texnik ko‘rinishdagi ma’lumotlar ham agregatsiya natijasida shaxsni identifikatsiya qilish vositasiga aylanadi. O‘zbekiston qonunchiligida OSINT faoliyati, metama’lumotlarning maqomi va OSINT natijalarining dalil sifatidagi maqbulligi bo‘yicha aniq normalar yo‘qligi ushbu muvozanatni ta’minlashni qiyinlashtiradi. GDPR tajribasi va xalqaro standartlarni inobatga olgan holda yuqoridagi takliflarni amalga oshirish shaxs huquqlarini himoya qilish va kiberjinoyatlarga qarshi kurash samaradorligini oshirishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Konstitutsiyasi

2. “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni

3. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni

4. O‘zbekiston Respublikasi Jinoyat kodeksi va Jinoyat-protsessual kodeksi

5. Regulation (EU) 2016/679 (General Data Protection Regulation)

6. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) va 108+ Protokoli

7. Convention on Cybercrime (Budapest, 2001)

8. Koops B.-J., Hoepman J.-H., Leenes R. Open-source intelligence and privacy by design

9. Anorboyev A. Personal data law: personal data protection in the new era. 2026

10. Cybersecurity Ventures hisoboti - https://cybersecurityventures.com/

11. FBI Internet Crime Complaint Center (IC3), 2025-yil hisoboti - https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

12. Surfshark, 2025-yil ma'lumotlar sizib chiqishi bo'yicha tadqiqot https://surfshark.com/?coupon=onedeal&source=&aff_sub=737&offer_id=1528&utm_medium=42759&utm_source=Affiliates&affiliate_id=42759&utm_campaign=affiliate&transaction_id=10231dd7f1c2c7314b077bd1799dad&recurring_goal_id=1519&gad_source=1

13. O'zbekiston Respublikasi Ichki ishlar vazirligi ma'lumotlari - https://www.gazeta.uz/oz/2026/03/10/crime/