SUN'IY INTELLEKT YORDAMIDA SODIR ETILGAN JINOYATLARNING KRIMINOLOGIK VA HUQUQIY KLASSIFIKATSIYASIDAGI MUAMMOLAR

Muhammadjonova Gulasal Muzaffar qizi
Namangan davlat universiteti
Yuridik fakulteti 2-bosqich talabasi
muhammadjonovago07@gmail.com
https://doi.org/10.5281/zenodo.21439104

Annotatsiya. Mazkur maqolada sun'iy intellekt texnologiyalarining jadal rivojlanishi natijasida yuzaga kelayotgan kiberjinoyatlar va ularni huquqiy kvalifikatsiya qilish bilan bog'liq muammolar tahlil qilinadi. Sun'iy intellekt tizimlari jinoyat vositasi sifatida ishlatilishi, xususan deepfake, avtomatlashtirilgan phishing va botnet hujumlari kabi holatlar huquqiy jihatdan murakkablik tug'dirmoqda. Tadqiqotda amaldagi milliy qonunchilik normalari tahlil qilinib, ularning zamonaviy texnologik tahdidlarga mos kelish darajasi o'rganildi. Shuningdek, xalqaro tajriba asosida huquqiy yechimlar taklif etildi.

Kalit so'zlar. Sun'iy intellekt (SI), kiberjinoyat, huquqiy kvalifikatsiya, raqamli dalillar, deepfake, kiberxavfsizlik, jinoyat huquqi, huquqiy muammo.

So'nggi yillarda raqamli texnologiyalar va sun'iy intellekt tizimlarining jadal rivojlanishi jamiyat hayotining barcha sohalariga chuqur kirib bordi. Shu bilan birga, ushbu texnologiyalar kiberjinoyatchilikning yangi shakllarini yuzaga keltirmoqda. Sun'iy intellekt ishtirokidagi kiberjinoyatlar an'anaviy jinoyat huquqi normalari bilan to'liq qamrab olinmaganligi sababli ularni huquqiy jihatdan to'g'ri kvalifikatsiya qilish muammosi dolzarb bo'lib qolmoqda. Sun'iy intellekt (SI) texnologiyalarining jadal rivojlanishi zamonaviy jinoyatchilikning shakli, mazmuni va amalga oshirish usullarini tubdan o'zgartirmoqda. Bugungi kunda jinoyatlar faqat inson tomonidan emas, balki SI tizimlari yordamida, ular ishtirokida yoki qisman va to'liq avtomatlashtirilgan algoritmlar orqali ham sodir etilmoqda. Bu esa kriminologiya va jinoyat huquqi oldida yangi ilmiy va amaliy muammolarni keltirib chiqarmoqda. Xususan, jinoyat subyektini aniqlash, sababiy bog'lanishni belgilash hamda javobgarlikni taqsimlash masalalari an'anaviy huquqiy yondashuvlar doirasida to'liq hal etilmayapti.

Kriminologik nuqtayi nazardan SI yordamida sodir etiladigan jinoyatlarni uch asosiy guruhga ajratish mumkin. Birinchi guruhda SI vosita sifatida ishlatiladigan jinoyatlar bo'lib, bunda asosiy jinoyat subyekti inson hisoblanadi, SI esa faqat texnik vosita vazifasini bajaradi. Bunga deepfake texnologiyasi orqali shantaj qilish, fishing xabarlarini avtomatik generatsiya qilish yoki zararli kontent yaratishda SI dan foydalanish kiradi. Bunday holatlarda klassik jinoyat huquqi tamoyillari amal qiladi, biroq SI jinoyatning tezligi, ko'lami va anonimligini keskin oshiradi. Natijada jinoyatni aniqlash va isbotlash murakkablashadi. Shu sababli SI ishlatilgan holatlarni aniqlash bo'yicha maxsus raqamli ekspertiza va forensik metodlarni rivojlantirish zarur bo'ladi.

Ikkinchi guruh qisman avtomatlashtirilgan jinoyatlardan iborat bo'lib, bunda inson tomonidan berilgan topshiriq SI tizimlari tomonidan mustaqil ravishda yoki yarim avtomatik tarzda bajariladi. Masalan, bot-tarmoqlar orqali dezinformatsiya tarqatish, algoritmik savdo orqali bozorni manipulyatsiya qilish yoki ommaviy spam hujumlari shunday jinoyatlar sirasiga kiradi. Ushbu toifada asosiy muammo shundan iboratki, insonning niyati va SI tomonidan qabul qilingan qarorlar o'rtasidagi sababiy bog'lanish murakkablashadi. Natijada "tarqalgan javobgarlik" muammosi yuzaga keladi. Bunday holatlarda ishlab chiquvchi, foydalanuvchi va operator o'rtasidagi huquqiy mas'uliyatni aniq taqsimlash zarur bo'ladi hamda "nazorat darajasi" mezonini joriy etish muhim ahamiyat kasb etadi.

Uchinchi guruh to‘liq avtonom SI tizimlari orqali sodir etiladigan jinoyatlardir. Bunday holatda SI insonning bevosita nazoratisiz qaror qabul qiladi va harakatlarni amalga oshiradi. Avtonom dronlar tomonidan yetkazilgan zarar yoki o‘z-o‘zini o‘rganuvchi tizimlarning noqonuniy moliyaviy operatsiyalari bunga misol bo‘la oladi. Bu toifa eng murakkab huquqiy muammolarni keltirib chiqaradi, chunki an’anaviy jinoyat huquqi faqat insonni subyekt sifatida tan oladi. Shu sababli SI uchun cheklangan huquqiy rejim, majburiy algoritmik audit, “human-in-the-loop” prinsipi va xavfsizlik sertifikatsiyasi kabi yangi mexanizmlarni joriy etish zarur bo‘ladi.

Huquqiy klassifikatsiya nuqtayi nazaridan SI ishtirokidagi jinoyatlar uch asosiy yo‘nalishga bo‘linadi: an’anaviy jinoyatlar (SI vosita sifatida), kiberjinoyatlar va yangi shakllanayotgan algoritmik jinoyatlar. Eng katta muammo shundaki, SI huquqiy subyekt sifatida tan olinmaganligi sababli javobgarlik inson zanjiriga yuklanadi. Bu esa ishlab chiquvchi, operator, foydalanuvchi va platforma egasi o‘rtasida javobgarlikning tarqalib ketishiga olib keladi.

Isbotlash jarayonida ham bir qator murakkabliklar mavjud. Deepfake kontentni aniqlash har doim ham ishonchli emas, SI tizimlari “black box” tamoyili asosida ishlagani uchun qaror qabul qilish jarayoni tushunarsiz bo‘lib qoladi, raqamli dalillar esa oson o‘zgartirilishi yoki yo‘q qilinishi mumkin. Shu sababli AI-forensika laboratoriyalari, blokcheyn asosidagi dalillar tizimi va algoritmik audit majburiyatini joriy etish zarur hisoblanadi. SI yordamida sodir etilayotgan jinoyatlar zamonaviy jinoyat huquqi va kriminologiya uchun yangi bosqichni anglatadi. Bu jarayonda eng asosiy muammo texnologik taraqqiyot va huquqiy tartibga solish o‘rtasidagi nomutanosiblikdir. Mazkur muammoni hal etish uchun kompleks yondashuv zarur bo‘lib, u huquqiy islohotlar, texnologik nazorat mexanizmlari va ijtimoiy profilaktika choralarining uyg‘unlashuvini talab qiladi. Sun’iy intellekt yordamida sodir etilayotgan jinoyatlar kriminologiya va jinoyat huquqi nazariyasida tub o‘zgarishlarni talab qiladigan yangi fenomen sifatida baholanadi. Ushbu jinoyatlarning eng asosiy xususiyati shundaki, ular an’anaviy “inson — vosita — natija” zanjirini buzadi va uning o‘rniga “inson — algoritm — avtonom qaror — natija” modelini yuzaga keltiradi. Bu esa jinoyat tarkibini aniqlashda klassik yondashuvlarning yetarli emasligini ko‘rsatadi.

Eng muhim muammolardan biri jinoyat subyektining aniqlanishidir. An’anaviy huquq tizimida faqat jismoniy yoki yuridik shaxs jinoyat subyekti sifatida tan olinadi. Biroq SI tizimlari murakkab algoritmik qarorlar qabul qilishi, mustaqil o‘rganishi va hatto inson kiritmagan natijalarni ishlab chiqishi sababli, ularning huquqiy maqomi masalasi ochiq qolmoqda. Natijada javobgarlik inson zanjirining turli bo‘g‘inlariga — dasturchi, foydalanuvchi, operator yoki platforma egasiga tarqaladi, bu esa “diffuz javobgarlik” muammosini yuzaga keltiradi. Bundan tashqari, sababiy bog‘lanishni aniqlash masalasi ham murakkablashmoqda. Klassik jinoyat huquqida harakat va oqibat o‘rtasida bevosita va aniq bog‘liqlik talab qilinadi. SI tizimlarida esa qarorlar ko‘pincha ehtimollik asosida, ko‘p qatlamli neyrotarmoqlar orqali qabul qilinadi, bu esa “qaror qabul qilish jarayonining shaffof emasligi” (“black box” muammosi)ni keltirib chiqaradi. Natijada sud-tergov jarayonida jinoyatning aynan kimning harakati natijasida sodir bo‘lganini aniqlash qiyinlashadi. Shuningdek, SI yordamida sodir etiladigan jinoyatlarning tezligi va masshtabi ham an’anaviy jinoyatlardan tubdan farq qiladi. Birgina SI modeli yordamida minglab yoki millionlab maqsadlarga bir vaqtning o‘zida ta’sir ko‘rsatish mumkin. Bu esa jinoyatning individual xususiyatini yo‘qotib, uni ommaviy va avtomatlashtirilgan jarayonga aylantiradi. Ayniqsa, deepfake texnologiyalari va generativ modellar orqali axborot manipulyatsiyasi jamiyatda ishonch inqirozini kuchaytiradi.

Yana bir muhim jihat — jinoyatni isbotlash jarayonidagi qiyinchiliklar. Raqamli dalillar juda oson o‘zgartirilishi, yashirilishi yoki qayta yaratilishi mumkinligi sababli an’anaviy dalil standartlari yetarli samara bermay qolmoqda. SI tomonidan yaratilgan kontentni inson

yaratgan kontentdan farqlash ham tobora murakkablashib bormoqda. Bu esa sud amaliyotida ekspertiza xulosalariga bo‘lgan ehtiyojni keskin oshiradi. Shu bilan birga, SI jinoyatlarining huquqiy tartibga solinishi bo‘yicha xalqaro yondashuvlar ham bir xil emas. Ayrim davlatlar tavakkalchilikka asoslangan tartibga solish modelini qo‘llayotgan bo‘lsa, boshqalari umumiy kiberjinoyat qonunchiligi doirasida ushbu muammolarni hal etishga urinmoqda. Biroq har ikkala yondashuv ham SI texnologiyalarining tez rivojlanish sur’atiga to‘liq moslasha olmayapti.

Umuman olganda, SI jinoyatlari bo‘yicha asosiy muhokama markazi uchta yo‘nalishda jamlanadi: birinchidan, javobgarlik subyektining aniqlanishi; ikkinchidan, sababiy bog‘lanish va algoritmik qarorlar shaffofligi; uchinchidan, raqamli dalillarni isbotlashning yangi standartlarini ishlab chiqish zarurati. Ushbu muammolarni hal etish uchun faqat huquqiy yondashuv yetarli emas, balki texnologik, institutsional va kriminologik integratsiyalashgan tizim talab etiladi.

Shu nuqtayi nazardan, SI jinoyatlarini tartibga solish kelajakda “javobgarlikni taqsimlash huquqi” va “algoritmik shaffoflik prinsipi” kabi yangi huquqiy institutlarning shakllanishiga olib kelishi mumkin. Bu esa jinoyat huquqi rivojida yangi bosqichni anglatadi. Sun’iy intellekt yordamida sodir etilayotgan jinoyatlar murakkab va ko‘p qatlamli xususiyatga ega bo‘lgani uchun ularni samarali tartibga solish ham kompleks yondashuvni talab etadi. Biroq amaliy va nazariy jihatdan ushbu yechimlarni uchta asosiy yo‘nalishga jamlash mumkin: huquqiy-institutsional, texnologik va ijtimoiy-profilaktik yo‘nalishlar.

Birinchi yo‘nalish — huquqiy va institutsional islohotlar bilan bog‘liq. Ushbu yo‘nalishda SI ishtirokidagi jinoyatlar uchun alohida huquqiy asos yaratish zarur. Amaldagi jinoyat qonunchiligida SI alohida subyekt sifatida tan olinmaganligi sababli javobgarlik masalasi ko‘pincha umumiy normalar doirasida hal etiladi, bu esa huquqiy noaniqliklarni keltirib chiqaradi. Shu sababli “algoritmik jinoyatlar”, “SI vositasida sodir etilgan jinoyatlar” va “avtonom tizimlar bilan bog‘liq huquqbuzarliklar” kabi tushunchalarni aniq normativ darajada belgilash muhimdir. Bundan tashqari, javobgarlikni taqsimlashda ko‘p subyektli model joriy etilib, dasturchi, operator, platforma egasi va foydalanuvchi o‘rtasidagi mas’uliyat aniq chegaralanishi lozim. Shuningdek, SI tizimlarini nazorat qiluvchi maxsus institutsional organlar va ekspertiza markazlari tashkil etilishi ham ushbu yo‘nalishning muhim qismidir.

Ikkinchi yo‘nalish — texnologik xavfsizlik va nazorat tizimlarini rivojlantirishdir. SI bilan bog‘liq jinoyatlarning oldini olishda texnologik yechimlar hal qiluvchi ahamiyatga ega. Bunda algoritmik shaffoflikni ta’minlash, ya’ni SI tizimlarining qaror qabul qilish jarayonini audit qilish imkoniyatini yaratish zarur. “Black box” muammosini kamaytirish uchun majburiy algoritmik audit, log-fayllarni o‘zgarmas formatda saqlash va riskga asoslangan monitoring tizimlarini joriy etish kerak. Shuningdek, deepfake va generativ kontentlarni aniqlovchi avtomatlashtirilgan deteksiya tizimlarini rivojlantirish ham jinoyatlarning oldini olishda muhim rol o‘ynaydi. Raqamli dalillarni ishonchli saqlash uchun esa blokcheyn texnologiyalaridan foydalanish samarali yechim bo‘lishi mumkin.

Uchinchi yo‘nalish — ijtimoiy-profilaktik va ta’limiy choralar hisoblanadi. SI texnologiyalarining keng tarqalishi fonida aholining raqamli savodxonligi yetarli darajada bo‘lmasa, jinoyatchilik xavfi yanada ortadi. Shu sababli jamiyatda, ayniqsa yoshlar orasida SI xavflari, kiberfiribgarlik, deepfake va onlayn manipulyatsiyalarni aniqlash bo‘yicha bilimlarni oshirish zarur. Ta’lim tizimiga “sun’iy intellekt va huquq” yo‘nalishidagi maxsus kurslarni joriy etish, ommaviy axborot vositalari orqali profilaktik targ‘ibot olib borish ham muhim ahamiyatga ega. Bundan tashqari, fuqarolarning axborotga tanqidiy yondashuvini shakllantirish SI asosidagi jinoyatlarga qarshi eng samarali ijtimoiy himoya vositalaridan biri hisoblanadi.

Tadqiqot natijalari shuni ko‘rsatadiki, SI yordamida sodir etiladigan jinoyatlarda eng asosiy muammo jinoyat subyektini aniqlash, sababiy bog‘lanishni isbotlash va javobgarlikni adolatli taqsimlash bilan bog‘liqdir. Ayniqsa, qisman va to‘liq avtomatlashtirilgan tizimlarda inson va algoritm o‘rtasidagi mas’uliyat chegarasi tobora xiralashib bormoqda. Sun’iy intellekt yordamida sodir etiladigan jinoyatlar zamonaviy huquq tizimi uchun nafaqat xavf, balki yangi huquqiy paradigma shakllanishiga turtki beruvchi omil sifatida ham baholanadi. Shu nuqtayi nazardan, kelajak jinoyat huquqi “inson markazli” modeldan “inson–algoritm hamkorligi”ga asoslangan tizimga evolyutsiya qilish yo‘lida rivojlanishi ehtimoldan xoli emas.

Foydalanilgan adabiyotlar.

1. O‘zbekiston Respublikasi Jinoyat kodeksi (amaldagi tahrir). — https://lex.uz .
2. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni. — https://lex.uz .
3. O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni. — https://lex.uz .
4. Islomov Z.M. va boshqalar. Huquqshunoslik asoslari. Toshkent: TDYU nashriyoti, 2020.
5. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. Pearson Education, 2021.
6. European Commission. Artificial Intelligence Act (AI Act), 2024. — https://ec.europa.eu .
7. OECD. OECD Principles on Artificial Intelligence, 2023. — https://www.oecd.org .
8. UNODC. Cybercrime and Emerging Technologies Report, 2022. — https://www.unodc.org .
9. NIST. AI Risk Management Framework (AI RMF 1.0), 2023. — https://www.nist.gov .