



RAQAMLI ERKINLIK, ZAMONAVIY TAHDIDLAR VA HUQUQIY CHORALAR

Mamanova Gulruh Ismatullayevna
TDYU huzuridagi M.Vosiqova nomidagi
Akademik litseyning bo'lim boshlig'i
gulruh151283@gmail.com

Annotatsiya:

Ushbu maqolada raqamli erkinlik tushunchasi, uning ijtimoiy va huquqiy jihatlarini, shuningdek, zamonaviy texnologiyalar bilan bog'liq tahdidlar tahlil qilinadi. Maqolada xalqaro tajribalar asosida ushbu muammolarni bartaraf etish bo'yicha samarali huquqiy choralar ko'rib chiqiladi. Xususan, kiberxavfsizlikni mustahkamlash, fuqarolarning shaxsiy ma'lumotlarini himoya qilish, internetda so'z va axborot erkinligini ta'minlash uchun qonunchilikni takomillashtirish masalalariga alohida e'tibor qaratiladi.

Maqolaning asosiy maqsadi – raqamli erkinlik va xavfsizlik o'rtasidagi muvozanatni saqlash, internetdan foydalanish madaniyatini rivojlantirish hamda raqamli muhitda inson huquqlarini himoya qilishning huquqiy asoslarini mustahkamlashga oid tavsiyalar ishlab chiqishdan iborat.

Kalit so'zlar: Raqamli erkinlik, internet huquqlari, axborot erkinligi, so'z erkinligi, kiberxavfsizlik, shaxsiy ma'lumotlarni himoya qilish, onlayn senzura, raqamli huquqlar, internetga teng huquqli kirish, zamonaviy tahdidlar, raqamli texnologiyalar, kiberjinoyatlar, huquqiy choralar.

Raqamli erkinlik tushunchasi

Raqamli erkinlik – insonning internet va raqamli texnologiyalar yordamida axborotga erkin kirishish, uni tarqatish, fikr bildirish, shaxsiy ma'lumotlarini himoya qilish hamda raqamli muhitdan erkin foydalanish huquqlarini o'z ichiga olgan tushunchadir. Bu erkinlik axborot texnologiyalarining rivojlanishi natijasida inson huquqlari tizimida muhim o'rin egallab, so'z va fikr erkinligining raqamli muhitdagi ifodasi sifatida namoyon bo'lmoqda.



Raqamli erkinlikning asosiy jihatlari quyidagilardan iborat:

- **Axborot erkinligi** – internet orqali har qanday axborotga erkin kirishish va undan foydalanish huquqi.
- **Soʻz erkinligi** – ijtimoiy tarmoqlar, bloglar va boshqa raqamli platformalar orqali oʻz fikrini erkin bildirish imkoniyati.
- **Shaxsiy maʼlumotlarni himoya qilish** – insonning raqamli makonda shaxsiy axborotlarini nazorat qilish va uni uchinchi shaxslardan himoya qilish huquqi.
- **Internetga teng huquqli kirish** – har bir insonning internet va raqamli texnologiyalardan foydalanish imkoniyatini taʼminlash.

Raqamli erkinlik demokratik jamiyatning ajralmas qismi boʻlib, fuqarolarning axborotga boʻlgan huquqini kafolatlash bilan birga, davlat va jamiyat oʻrtasidagi ochiqlik va shaffoflikni ham taʼminlaydi. Shu sababli, raqamli erkinlikni taʼminlash nafaqat texnologik, balki huquqiy va ijtimoiy masala hamdir.

Zamonaviy tahdidlar.

Raqamli texnologiyalar va internetning rivojlanishi insoniyatga mislsiz imkoniyatlar yaratdi. Biroq, bu jarayon bilan birga yangi xavf-xatarlar, yaʼni zamonaviy tahdidlar ham paydo boʻldi. Raqamli erkinlik va kiberxavfsizlik oʻrtasidagi muvozanatni saqlash, shaxsiy maʼlumotlarni himoya qilish, yolgʻon axborotga qarshi kurashish bugungi kunning eng dolzarb masalalaridan biri boʻlib qolmoqda. Quyida raqamli erkinlikka tahdid soluvchi asosiy zamonaviy xavf-xatarlar koʻrib chiqiladi.

Kiberjinoyatlar va kiberxavfsizlik muammolar.

Kiberjinoyatlar XXI asrda eng jiddiy xavflardan biriga aylandi. Xakerlar, kiberfiribgarlar va boshqa raqamli jinoyatchilar davlat muassasalari, xususiy kompaniyalar va jismoniy shaxslarga tahdid solmoqda.

Eng keng tarqalgan kiberjinoyatlar:

- **Maʼlumotlarni oʻgʻirlash** – maxfiy yoki shaxsiy maʼlumotlarni noqonuniy yoʻl bilan qoʻlga kiritish.
- **Kiberhujumlar** – davlat idoralari, kompaniyalar va xususiy shaxslarning serverlariga xakerlik hujumlari uyushtirish.
- **Fidokorona dasturlar (ransomware)** – zararli dasturlar orqali kompyuter tizimlarini bloklash va pul talab qilish.



- **Fishing (phishing)** – soxta veb-saytlar yoki elektron pochta orqali foydalanuvchilarni aldash va ularning shaxsiy ma'lumotlarini qo'lga kiritish.

Kiberjinoyatlar global miqyosda tez sur'atlar bilan o'sib bormoqda va ularga qarshi kurashish uchun samarali kiberxavfsizlik tizimlarini joriy etish zarur.

Onlayn senzura va internet erkinligining cheklanishi.

Ko'pgina mamlakatlarda internetga kirish nazorat qilinadi va ayrim veb-saytlar bloklanadi. Bu esa fuqarolarning axborot olish va so'z erkinligiga bo'lgan huquqlarini buzadi.

Onlayn senzura quyidagi ko'rinishlarda namoyon bo'ladi:

- **Ijtimoiy tarmoqlar va veb-saytlarning bloklanishi** – ayrim davlatlarda noqulay axborot tarqatadigan platformalar yopib qo'yiladi.
- **Fikrlarni cheklash va nazorat qilish** – hukumatlar yoki texnologik kompaniyalar ma'lum mavzularga oid fikrlarni yashirish yoki tahrirlash orqali jamoatchilik fikriga ta'sir o'tkazishi mumkin.
- **Sun'iy intellekt asosida tsenzura** – algoritmlar va AI vositalari orqali ayrim kontentlar yashirin ravishda bloklanishi yoki tarqatilishi cheklanishi mumkin.

Onlayn senzuraning kuchayishi raqamli erkinlik uchun jiddiy tahdiddir va bu borada xalqaro hamjamiyat erkin internetni saqlab qolish uchun harakat qilmoqda.

Shaxsiy ma'lumotlarning buzilishi va maxfiylik muammolari

Bugungi kunda ko'plab platformalar foydalanuvchilarning shaxsiy ma'lumotlarini yig'ib, ularni tijorat yoki kuzatuv maqsadida ishlatmoqda. Bu esa insonlarning shaxsiy hayoti daxlsizligiga tahdid solmoqda.

Shaxsiy ma'lumotlarni buzilishining asosiy xavflari:

- **Noto'g'ri ma'lumotlardan foydalanish** – texnologik kompaniyalar va davlat idoralari fuqarolarning shaxsiy ma'lumotlarini kuzatishi va tahlil qilishi mumkin.
- **Maxfiy axborotlarning tarqalishi** – foydalanuvchilarning ijtimoiy tarmoqlardagi ma'lumotlari, bank kartalari yoki shaxsiy yozishmalari tarqalib ketishi ehtimoli ortib bormoqda.
- **Deepfake va sun'iy intellekt asosidagi manipulyatsiya** – maxfiy ma'lumotlardan foydalanib, soxta videolar va tovush yozuvlari yaratish orqali odamlarni manipulyatsiya qilish.



Bu muammolarni hal qilish uchun shaxsiy ma'lumotlarni himoya qilish qonunchiligini mustahkamlash va foydalanuvchilarni raqamli xavfsizlik borasida xabardor qilish lozim.

Huquqiy choralar

Raqamli erkinlikni ta'minlash va zamonaviy tahdidlarga qarshi samarali kurashish uchun huquqiy choralar ishlab chiqilishi zarur. O'zbekiston Respublikasining Konstitutsiyasi 33-moddasida har kimning istalgan axborotni izlash, olish va tarqatish huquqi kafolatlangan bo'lib, davlat internetdan foydalanish uchun shart-sharoitlar yaratishi lozimligi belgilangan. Biroq bu huquq mutlaq emas – u qonuniy cheklolarga ega bo'lib, konstitutsiyaviy tuzumni, jamoat xavfsizligini, boshqa shaxslarning huquqlarini va davlat sirlarini himoya qilish maqsadida tartibga solinishi mumkin. Shu nuqtai nazardan, birinchidan, kiberjinoyatlarga qarshi qonunchilikni mustahkamlash muhimdir. Bugungi kunda kiberxavfsizlikni ta'minlash uchun kiberjinoyatlarga qarshi samarali qonunlar ishlab chiqilishi zarur. Xususan, shaxsiy ma'lumotlarni himoya qilish, kiberhujumlarni oldini olish va kiberjinoyatchilikni aniqlash bo'yicha qat'iy choralar belgilanishi lozim. Shuningdek, xalqaro hamkorlikni kengaytirish orqali transmilliy kiberjinoyatlarga qarshi kurashish ham dolzarb masalalardan biri hisoblanadi.

So'z erkinligini kafolatlash va onlayn senzuraning oldini olish.

Konstitutsiyaning 33-moddasiga muvofiq, har bir fuqaro axborotni izlash, olish va tarqatish huquqiga ega. Shu sababli, internet va raqamli muhitda so'z erkinligini himoya qilish uchun quyidagi choralar zarur:

Internet tsenzurasining qonuniy asoslarini belgilash – so'z erkinligiga noqonuniy cheklolvar qo'yilishining oldini olish va faqat konstitutsiyada belgilangan sabablarga ko'ra cheklash mexanizmlarini ishlab chiqish.

Ijtimoiy tarmoqlardagi fikr erkinligini qo'llab-quvvatlash – davlat tomonidan noxolis cheklolarning oldini olish va fuqaro fikrlarini erkin ifoda etishiga imkon yaratish.



Axborotga erkin kirish kafolatlarini mustahkamlash – hukumat, jamoatchilik va fuqarolik jamiyati tashkilotlari uchun ochiq axborot tizimlarini rivojlantirish. Kiberxavfsizlikni mustahkamlash va texnologik himoya tizimlarini joriy etish. Raqamli huquqlarni himoya qilish va kiberjinoyatlarga qarshi kurashish uchun texnologik infratuzilmani mustahkamlash lozim. Bunga quyidagilar kiradi:

Davlat va xususiy sektorda kiberxavfsizlik choralari kuchaytirish – muhim davlat tizimlari va bank infratuzilmalari uchun mustahkam himoya mexanizmlarini yaratish.

Fuqarolar uchun kiberxavfsizlik bo'yicha trening va o'quv dasturlarini ishlab chiqish – aholining internetdagi xatarlar haqida xabardorligini oshirish va ularni himoya qilish bo'yicha ko'nikmalar berish.

Davlat idoralari va xususiy sektor o'rtasida kiberxavfsizlik bo'yicha hamkorlikni yo'lga qo'yish – texnologik kompaniyalar, internet-provayderlar va huquqni muhofaza qilish organlari bilan hamkorlikni mustahkamlash.

Xulosa

Xulosa qilib aytganda, raqamli erkinlik inson huquqlarining ajralmas qismi bo'lib, O'zbekiston Respublikasi Konstitutsiyasining 33-moddasi bilan kafolatlangan. Biroq, kiberjinoyatlar, shaxsiy ma'lumotlarning noqonuniy yig'ilishi va yolg'on axborot tarqalishi kabi zamonaviy tahdidlar bu erkinlikka xavf solmoqda. Ularni oldini olish uchun kiberxavfsizlikni kuchaytirish, shaxsiy ma'lumotlarni himoya qilish, media savodxonlikni oshirish va so'z erkinligini qonuniy asoslarda tartibga solish zarur. Samarali huquqiy choralarning joriy etilishi raqamli muhitda xavfsizlik va erkinlik o'rtasidagi muvozanatni ta'minlab, fuqarolarning axborot olish va tarqatish huquqlarini himoya qiladi.

Foydalanilgan adabiyotlar ro'yxati:

1. O'zbekiston Respublikasi Konstitutsiyasi – Toshkent, 2023.
2. O'zbekiston Respublikasi "Axborot erkinligi to'g'risida"gi qonuni.
3. Xalqaro huquqiy hujjatlar: BMTning "Shaxsiy hayot daxlsizligi va axborot erkinligi" bo'yicha konvensiyalari.