



Yevropa Ittifoqi tomonidan
moliyalashtiriladi



ZAMONAVIY
JURNALISTIKANI
RIVOJLANTIRISH
MARKAZI



LPRC
LEGAL POLICY
RESEARCH CENTRE

UDRMI
O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI

JURNALISTLAR, BLOGERLAR VA OAV UCHUN RAQAMLI HUQUQLAR

Ularni amalda qanday
tushunish, qo'llash?

JURNALISTLAR, BLOGERLAR VA OAV UCHUN RAQAMLI HUQUQLAR

Ularni amalda qanday
tushunish, qo'llash?

Toshkent
2026

Jurnalistlar, bloggerlar va OAV uchun raqamli huquqlar. Ularni amalda qanday tushunish, qo'llash. Toshkent, 2026 — 82 sahifa.

Ushbu qo'llanma Yevropa Ittifoqining moliyaviy ko'magida tayyorlandi. Uning mazmuni uchun to'liq mas'uliyat Zamonaviy jurnalistikani rivojlantirish markazi zimmasiga yuklatilgan bo'lib, unda bildirilgan fikrlar Yevropa Ittifoqining rasmiy nuqtai nazarini aks ettirmasligi mumkin.

Mualliflar jamoasi:

Artyom Goryaynov (Qirg'iziston)
Lola Mahmudova (O'zbekiston)
Madina Tursunova (O'zbekiston)
Olga Didenko (Qozog'iston)
Roman Reymer (Qozog'iston)

Muharrir:

Lola Islamova

Mundarija

Ushbu qo'llanmadan qanday foydalaniladi?	4
1-bo'lim. Raqamli huquqlar nima?	5
1.1. Raqamli huquqlar nazariyasiga kirish	5
1.2. Raqamli huquqlar sohasidagi xalqaro va mintaqaviy standartlar	11
1.3. O'zbekistonning raqamli huquqlar sohasidagi milliy qonunchiligi	17
2-bo'lim. Media va jurnalistlarning raqamli huquqlari	26
2.1. Raqamli muhitda kontent yaratish va tarqatish	26
2.2. Axborotdan foydalanish va akkreditatsiya	33
2.3. Raqamli muhitda kontent uchun javobgarlik	41
2.4. Mualliflik huquqlari va media	48
2.5. Raqamli muhitda jurnalistlar va media kasbiy faoliyatining axloqiy jihatlari	55
2.6. Onlayn media uchun siyosatlar	58
3-bo'lim. Raqamli muhitda jurnalistlar va tahririyatlar uchun tahdidlar	62
3.1. Asosiy tahdidlar	62
3.3. Tahririyatlar saytlari va mediaresurslarini himoya qilish choralari	72
Xulosa	78
Ilovalar	79

Ushbu qo'llanmadan qanday foydalaniladi?

Bu qo'llanma raqamli muhitda ishlaydigan jurnalistlar, tahririyatlar va ommaviy axborot vositalari uchun amaliy qo'llanma sifatida ishlab chiqilgan. Uning vazifasi nafaqat raqamli huquqlarning mohiyatini tushuntirish, balki ularni tahririyat qarorlarini qabul qilishda, ma'lumotlar bilan ishlashda va xavflarni boshqarishda qo'llashga yordam berishdir.

Material "tushunishdan amaliyotga" tamoyili asosida tuzilgan. Birinchi bo'lim raqamli huquqlar va ularni tartibga solishning huquqiy mantig'i haqida asosiy tasavvurni shakllantiradi. Ikkinchisi — bu tamoyillarni ommaviy axborot vositalarining kasbiy faoliyatiga olib kiradi: kontent yaratish va tarqatish, ma'lumotlarga kirish, auditoriya va platformalar bilan muloqot qilish. Uchinchi bo'lim raqamli muhitda jurnalistlar va tahririyatlar duch keladigan xavf-xatarlar va xavfsizlik choralariga qaratilgan.

Qo'llanmadan ikki rejimda foydalanish mumkin. Bir tomondan, mavzuni tizimli o'zlashtirish uchun izchil material sifatida. Boshqa tomondan, aniq vazifalarni hal qilish uchun ishchi qo'llanma sifatida: nashrlarni tayyorlash, huquqiy xavf-xatarlarni baholash, ma'lumotlarga kirishdagi cheklovlarga javob berish yoki raqamli platformalar bilan ishlash.

Qo'llanmaning ayrim elementlari — amaliy keyslar, tavsiyalar va chek-listlar kundalik tahririyat ishida qo'llash uchun mo'ljallangan. Ular aniq vaziyatni huquqiy doiralar bilan tezda bog'lash va asosli harakat strategiyasini tanlash imkonini beradi.

Raqamli muhit kontent va tahririyat qarorlari uchun yuqori mas'uliyatni taqozo etishini hisobga olish muhimdir. Shuning uchun qo'llanma materiallaridan universal javoblar sifatida emas, balki aniq kontekstni hisobga olgan holda professional tahlil va qaror qabul qilish uchun asos sifatida foydalanish lozim.

1-bo'lim

Raqamli huquqlar nima?

1.1. Raqamli huquqlar nazariyasiga kirish

Zamonaviy dunyo shiddatli raqamli transformatsiyani boshdan kechirmoqda. Raqamlashtirishning rivojlanishi inson hayotining deyarli barcha jabhalariga, jumladan, axborot olish, ta'lim olish, ishga joylashish, biznes yuritish va boshqalarga ta'sir qiladi. Aksariyat tovar va xizmatlarni ham davlat, ham biznes tomonidan taklif qilinadigan ixtisoslashtirilgan raqamli xizmatlardan foydalangan holda olish mumkin.

Bundan tashqari, internet foydalanuvchilari soni geometrik progressiya asosida ortib bormoqda. Xususan, 2025-yil oktabr oyida dunyoda internet foydalanuvchilari soni¹ 6,4 milliarddan oshdi. DataReportal² ma'lumotlariga ko'ra, O'zbekistonda internet foydalanuvchilari soni 32,7 million kishini yoki mamlakat umumiy aholisining 92,2 foizini tashkil etadi.

Yuqoridagilarni inobatga olgan holda, raqamli huquqlar fenomenini rivojlantirish orqali raqamli makonni tartibga solish asosiy masalaga aylanmoqda.

Raqamli inson huquqlari axborot inqilobining oqibati bo'lib, ularning rivojlanishini harakatlantiruvchi kuch sifatida namoyon bo'lmoqda.

Eng keng tarqalgan nazariy pozitsiyalardan biri "raqamli huquqlar" BMTning ko'plab xalqaro hujjatlarida, shuningdek, mintaqaviy darajadagi hujjatlarda aks ettirilgan "inson huquqlari" tushunchasining bevosita davomi hisoblanadi.

Shu bilan birga, biz zamonaviy ko'rinishda bilgan "inson huquqlari" tushunchasi Inson huquqlari umumjahon deklaratsiyasi (1948-yil), Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt (1966-yil), Iqtisodiy, ijtimoiy va madaniy huquqlar to'g'risidagi xalqaro pakt (1966-yil), shuningdek, ko'plab xalqaro va mintaqaviy hujjatlar prizmasi orqali katta yo'lni bosib o'tdi.

Shunday qilib, inson huquqlari konsepsiyasining zamonaviy ko'rinishdagi rivojlanish qirralarini umumiy tarzda belgilab olish lozim.

Shunday qilib, inson huquqlari millati, yashash joyi, jinsi, etnik mansubligi, terisining rangi, dini, tili yoki boshqa har qanday belgilaridan qat'i nazar, har bir insonning ajralmas huquqlari majmuidir.

¹ <https://www.statista.com/statistics/617136/digital-population-worldwide/?srsltid=AfmBOopuoljbxLwhRpgdDEslhkuTmSJ-jYKK6UPJ25PPsiw826z9BPwD>

² <https://datareportal.com/reports/digital-2025-uzbekistan>



Asosiy tamoyillar

- Universallik: ular hamma joyda va barcha uchun amal qiladi.
- Daxlsizlik: ularni tortib olish mumkin emas (qonunda nazarda tutilgan ayrim hollar, masalan, jinoyat uchun ozodlikni cheklash mustasno).
- Bo'linmaslik: fuqarolik, siyosiy, iqtisodiy va ijtimoiy huquqlar o'zaro bog'liqdir. Biri bo'lmagan joyda boshqalaridan to'laqonli foydalanib bo'lmaydi.

Inson huquqlari avlodlari

“Inson huquqlari avlodlari” konsepsiyasi 1979-yilda chex-fransuz huquqshunosi Karel Vashak³ tomonidan taklif etilgan. Muallif Buyuk fransuz inqilobining (1789-yil) “Ozodlik, tenglik, birodarlik”⁴ shioridan ilhomlangan. Har bir “avlod” ushbu shiordagi so'zlardan biriga mos keladi va huquqiy fikr taraqqiyotining tarixiy bosqichlarini aks ettiradi.



Birinchi avlod: Ozodlik (Fuqarolik va siyosiy huquqlar)

Ozodlik avlodining mohiyati insonni davlat zulmidan himoya qilish zarurati bilan bog'liq. Huquqlarning birinchi avlodi **“salbiy huquqlar”** atrofida jamlangan. Bu shuni anglatadiki, davlat aralashuvdan o'zini tiyishi (!) shart. Hokimiyatdan ma'lum sohalarda “hech narsa qilmaslik” (o'ldirmaslik, sudsiz qamamaslik, qiynoqqa solmaslik, qullikda saqlamaslik, senzura qilmaslik) talab qilinadi. Boshqacha aytganda, salbiy huquqlarni amalga oshirish uchun davlat ortiqcha kuch sarflashi yoki maxsus infratuzilma yaratishi shart emas.

Asosiy huquqlar:

- Yashash va jismoniy daxlsizlik huquqi
- Qiynoqlardan ozod bo'lish
- Qullikdan ozod bo'lish
- So'z, vijdon va din erkinligi
- Adolatli sudga bo'lgan huquq (habeas corpus)
- Saylov huquqlari (aktiv va passiv)
- Egalik huquqi

³ <https://bigenc.ru/c/vasak-karel-afd127>

⁴ <https://bigenc.ru/c/kontseptsia-pokolenii-prav-cheloveka-b16d88>



Ikkinchi avlod: Tenglik (Ijtimoiy-iqtisodiy huquqlar)

Tenglik avlodining mohiyati insonning munosib turmush darajasi va ijtimoiy ta'minotini ta'minlash atrofida rivojlanadi. Huquqlarning ikkinchi avlodi "pozitiv huquqlar" deb ataluvchi huquqlar atrofida jamlangan. Bu shuni anglatadiki, davlatdan insonni ijtimoiy qo'llab-quvvatlashning eng yuqori darajasini ta'minlash uchun infratuzilmani yaratish bo'yicha faol harakatlar (!) talab etiladi.

Asosiy huquqlar:

- Mehnat qilish va adolatli ish haqi olish huquqi
- Dam olish huquqi (me'yorlangan ish kuni)
- Ijtimoiy ta'minot (pensiya, nafaqa) olish huquqi
- Sog'liqni saqlash va tibbiy yordam olish huquqi
- Ta'lim olish huquqi



Uchinchi avlod: Birodarlik (Jamoaviy huquqlar / Birdamlik huquqlari)

Birodarlik avlodining mohiyati alohida bir insonga emas, balki butun guruhlar (xalqlar, millatlar) yoki butun insoniyatga tegishli bo'lgan huquqlar atrofida rivojlanadi, ya'ni bular jamoaviy deb ataladigan huquqlardir.

Asosiy huquqlar:

- Taraqqiyot huquqi
- Tinchlik va xavfsizlik huquqi
- Ekologik huquqlar, sog'lom va toza atrof-muhitga bo'lgan huquq
- Insoniyatning umumiy merosi huquqi

Karel Vashakning konsepsiyasi xalqaro tashkilotlar, jamoat harakatlari, ilmiy hamjamiyat vakillari, huquq himoyachilari va faollar tomonidan ancha iliq kutib olindi. Yaxshi qarshilanishdan tashqari, raqamli makonda, genom tadqiqotlarida va boshqa innovatsion sohalarda **inson huquqlarining to'rtinchi avlodini** asoslash hamda shakllantirishga urinishlar ham bo'ldi.

Bizni birinchi navbatda raqamli huquqlar fenomenining rivojlanishi qiziqtirganligi sababli, e'tiborimizni faqat unga qaratamiz.

Axborot inqilobi nafaqat mavjud ishlab chiqarish usullari va turmush tarzining kengayishi hamda tarqalishiga, balki an'anaviy sanoat-tijorat jamiyatining yangi "aqlli" jamiyat bilan global miqyosda almashinishiga ham olib keldi, buning natijasida inson huquqlarining to'rtinchi avlodi — raqamli inson huquqlari vujudga keldi.

Raqamli inson huquqlarining o'ziga xos xususiyatlaridan biri uning aniq obyektga egaligidir — bu maxsus raqamli shaklda taqdim etilgan axborot (ma'lumotlar).

Raqamli inson huquqlari raqamli texnologiyalar yordamida amalga oshiriladi (huquqlarning raqamli tatbiqi) va faqat "raqamli insonlar"ga (raqamli atributlarga ega bo'lgan shaxslarga) tegishlidir.

Raqamli inson huquqlari sohasidagi majburiyatlar davlatlar va xususiy subyektlarning ham ijobiy, ham salbiy majburiyatlarini o'z ichiga oladi. Shu tariqa, raqamli inson huquqlari huquqlarning yangi alohida avlodi⁵ (yoki tizimi) bilan mustahkamroq bog'lanadi.

Mantiqan aytganda, raqamli huquqlar — bu internet makonidagi inson huquqlaridir. Shunga qaramay, bunday mulohaza yuritish uchun tegishli huquqiy asos keltirilishi lozim.

Masalan, Inson huquqlari bo'yicha Kengash tomonidan qabul qilingan 'Internetda inson huquqlarini Internetda inson huquqlarini rag'batlantirish, himoya qilish va ta'minlash'⁶ Rezolyutsiyasi quyidagilarni tezis tarzida belgilaydi:

Internetda axborotga kirish butun dunyo bo'ylab arzon va inklyuziv ta'lim imkoniyatlarini kengaytiradi, shu tariqa ta'lim olish huquqini ilgari surishga xizmat qiluvchi muhim vosita hisoblanadi. Shu bilan birga, raqamli savodxonlikni ta'minlash va raqamli tafovutni qisqartirish zarurligi ta'kidlanadi, chunki bu omillar ta'lim olish huquqining amalga oshirilishiga bevosita ta'sir ko'rsatadi.



Internetda inson huquqlarini, xususan, so'z erkinligi huquqini amalga oshirish tobora katta qiziqish va ahamiyat kasb etayotgan masaladir.



Internetning global, ochiq va o'zaro moslashuvchan xususiyatini saqlab qolish uchun davlatlarning xavfsizlik muammolarini inson huquqlari sohasidagi xalqaro majburiyatlariga muvofiq hal qilishi juda muhimdir.



Internetdan foydalanishni ta'minlash va kengaytirishda keng qamrovli inson huquqlari yondashuvini qo'llash muhimligi



Onlayn muhitda shaxsiy hayot daxlsizligi o'z fikrlarini erkin ifodalash va u yoki bu qarashlarga to'sqinliksiz amal qilish huquqini hamda tinch yig'ilishlar va uyushmalar erkinligi huquqini amalga oshirish uchun muhim ahamiyatga ega;



barcha ayollar va qizlarning axborot-kommunikatsiya texnologiyalaridan foydalanish imkoniyatlarini kengaytirish orqali ularning huquq va imkoniyatlarini kengaytirish muhimligi;



Qonun insonning oflayn muhitda ega bo'lgan huquqlari onlayn muhitda ham himoya qilinishi kerakligini tasdiqlaydi.

Shunday qilib, Inson huquqlari bo'yicha kengash onlayn muhitda amalga oshirilishi mumkin bo'lgan inson huquqlari (ya'ni, raqamli huquqlar) himoya qilinishi kerakligini ta'kidlaydi.

E'tibor bering, bu yerda gap siyosiy (so'z va fikr erkinligi), iqtisodiy (ta'lim olish huquqi) hamda jamoaviy (Internetning global xarakteri) huquqlar haqida ketmoqda.

Bosh Assambleya tomonidan qabul qilingan rezolyutsiya: Raqamli texnologiyalar kontekstida⁷ inson huquqlarini rag'batlantirish va himoya qilish ilgari qabul qilingan rezolyutsiyani quyidagilar bilan to'ldiradi:

⁵ Gun Nan. 2024. "Aqlli jamiyatda inson huquqlarining to'rtinchi avlodi va asosiy konstitutsiyaviy huquqlarning o'zgarishi"

⁶ <https://www.refworld.org/ru/legal/resolution/unhrc/2016/ru/112398>

⁷ <https://docs.un.org/ru/a/res/78/213>



Barcha inson huquqlari universal, bo'linmas, o'zaro bog'liq, bir-biriga bog'liq va bir-birini to'ldiradi hamda odamlar Internetdan tashqarida ega bo'lgan huquqlar Internetda ham himoya qilinishi kerakligini tasdiqlaydi.



Raqamli texnologiyalardan tobora kengroq foydalanish inson huquqlarining keng ko'lamini amalga oshirishga ta'sir ko'rsatishini qayd etgan holda va raqamli texnologiyalar inson huquqlarini amalga oshirishga ko'maklashishi mumkinligini, biroq tegishli kafolatlarsiz ulardan inson huquqlarini himoya qilish va to'liq amalga oshirishga jiddiy tahdid solish uchun foydalanilishi mumkinligini tan olgan holda.

Shu tariqa, Birlashgan Millatlar Tashkiloti darajasida raqamli huquqlar, birinchidan, mavjudligi, ikkinchidan, inson huquqlarining bevosita davomi ekanligi, uchinchidan esa, universal, bo'linmas, o'zaro bog'liq, bir-biriga tobe va o'zaro to'ldiruvchi ekanligi tan olinadi.

Universallik, bo'linmaslik va huquqqa asoslangan yondashuvga qaramay, raqamli huquqlarni Internetga hamda turli raqamli texnologiyalar, platformalar va servislarga ulanish imkoniyatisiz tasavvur qilib bo'lmaydi.

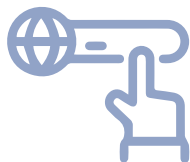
Shu munosabat bilan, Internetga kirish huquqi asosiy raqamli huquq hisoblanadi.

Insonning Internetga ulanishi davlatlar, texnologik kompaniyalar va boshqa uchinchi shaxslar tomonidan yuzaga keltiriladigan turli xavf-xatarlar, qiyinchiliklar va tahdidlar bilan bog'liq.

Masalan, raqamli tafovut, tarmoqda fikr bildirishni cheklash, Internetga kirishni bloklash, shaxsiy daxlsizlikning buzilishi va boshqa ko'plab holatlar shular jumlasidandir.

Bundan kelib chiqadiki, Internetdan foydalanish bilan bog'liq "qiyinchiliklar" o'z navbatida raqamli platformalardan va umuman Internetdan foydalanish holatlarida ko'proq qo'llaniladigan raqamli huquqlar ro'yxatini shakllantirish ko'rinishidagi "javob"ni yuzaga keltirdi.

Raqamli huquqlar ro'yxati



Internetdan foydalanish huquqi

Insonning so'z erkinligini amalga oshirish, ta'lim olish va zamonaviy ijtimoiy hamda iqtisodiy hayotda ishtirok etish uchun zarur bo'lgan global tarmoqqa ulanishning texnik va iqtisodiy imkoniyatlariga ega bo'lish huquqi.



Internetda so'z erkinligi

Insonning davlat chegaralaridan qat'i nazar, hokimiyat yoki korporatsiyalarning asossiz aralashuvisiz (senzurasiz) raqamli texnologiyalar va onlayn platformalar orqali har qanday turdagi axborot va g'oyalarni izlash, olish va tarqatish huquqi.



Tarmoq neytralligi

Internetning ishlash tamoyili, unga ko'ra internet-provayderlar tijorat yoki siyosiy maqsadlarda ma'lum kontent, ilovalar yoki saytlarni bloklamasdan, sekinlashtirmasdan va ularga ustuvorlik bermasdan, barcha uzatilayotgan ma'lumotlarni bir xil tarzda qayta ishlashlari kerak.



Unutilish huquqi

Shaxsga doir ma'lumotlar subyektiga muayyan asoslar mavjud bo'lgan taqdirda, unga taalluqli ma'lumotlarni ommaviy manbalardan olib tashlashni yoki ularning tarqatilishini to'xtatishni talab qilish imkonini beruvchi huquqiy mexanizm.



Kuzatuvdan himoya

Texnik vositalar orqali shaxsiy hayotga o'zboshimchalik bilan aralashishning oldini olishga qaratilgan shaxsiy hayot daxlsizligi huquqining o'ziga xos kafolati.



Ma'lumotlar maxfiyligi va himoyasi

Insonning raqamli muhitda o'zi haqidagi har qanday axborotni nazorat qilish (to'plash, saqlash, qayta ishlash) huquqi, shuningdek, ushbu axborotni uchinchi shaxslar (korporatsiyalar yoki davlat) tomonidan ruxsatsiz foydalanish, sizib chiqish va suiiste'mol qilishdan himoya qilishni kafolatlovchi huquqiy va texnik chora-tadbirlar majmui.



Shifrlash huquqi

Inson o'zining raqamli kommunikatsiyalari va saqlanayotgan ma'lumotlarining maxfiyligi, yaxlitligi va haqiqiylikini ta'minlash uchun kriptografik texnologiyalar va axborotni himoya qilish vositalaridan uchinchi shaxslarga (shu jumladan davlatga) deshifrlash kalitlarini taqdim etish majburiyatisiz to'sqinliksiz foydalanish huquqi.

1.2. Raqamli huquqlar sohasidagi xalqaro va mintaqaviy standartlar

Jamiyatning raqamli transformatsiyasi inson huquqlari klassik doktrinasini tubdan qayta talqin qilish, ya'ni BMTning oflayn va onlayn muhitlarda huquqlarni himoya qilishning bir xilligi to'g'risidagi asosiy tamoyili asosida ularni virtual makonga ko'chirish zaruratini keltirib chiqardi. 2026-yilga kelib, raqamli sohani tartibga solish endi mutlaqo milliy tanlov masalasi bo'lmay qoldi va BMTning universal paktlaridan tortib kiberxavfsizlik va ma'lumotlarni himoya qilish sohasidagi maxsus konvensiyalargacha bo'lgan xalqaro majburiyatlarning murakkab tuzilishiga bo'ysunadi. Ushbu me'yoriy asos ko'p darajali tizim sifatida ishlaydi, bu yerda global standartlar Yevropa Kengashi, Yevropa Ittifoqi, YEXHT, SHHT va MDHning mintaqaviy vositalari bilan to'ldiriladi va aniqlashtiriladi, bu esa shaxsning raqamli maqomining yagona huquqiy konturini shakllantiradi. Ushbu tizimda asosiy raqamli huquqlar kafolatlari, jumladan, Internetga universal kirish huquqi, algoritmik senzurasiz fikr bildirish erkinligi, katta ma'lumotlar iqtisodiyoti sharoitida shaxsiy hayot daxlsizligi markaziy o'rinni egallaydi. Xalqaro me'yorlar huquqlarning ruxsat etilgan cheklavlari masalalarida alohida ahamiyat kasb etib, davlat tomonidan tartibga solishning raqamli avtoritarizm vositalariga aylanishini oldini olish uchun qonuniylik va mutanosiblikning qat'iy **“uch tarkibli testi”**ni o'rnatmoqda. Shu bilan birga, standartlar evolyutsiyasi sun'iy intellekt etikasi, algoritmik kamsitish va transmilliy raqamli platformalarning mas'uliyati kabi to'rtinchi sanoat inqilobining yangi muammolarini qamrab olgan holda uzluksiz davom etmoqda. Shunday qilib, xalqaro-huquqiy poydevorni tahlil qilish global raqamlashtirish davrida ham davlat suvereniteti chegaralarini va inson hamda uning huquqlarini himoya qilish mexanizmlarini tushunish uchun zarur shart hisoblanadi.

Xalqaro standartlar

Global tartibga solishning asosi BMT Inson huquqlari bo'yicha kengashining (A/HRC/20/L.13, 2012-yil⁸⁾) rezolyutsiyasida mustahkamlangan huquqlarning tengligi tamoyilidir: “Insonning oflayn muhitda ega bo'lgan huquqlari onlayn muhitda ham himoya qilinishi kerak.”

Me'yoriy bazaning yadrosi Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt (FS'HXP⁹⁾) bo'lib, u quyidagi moddalarni o'z ichiga oladi:

19-modda (Fikrni ifoda etish, shuningdek, axborot olish erkinligi)

Axborotni “davlat chegaralaridan qat'i nazar” va “har qanday usulda” (jumladan, Internet orqali) tarqatish huquqini kafolatlaydi; bu haqda Inson huquqlari bo'yicha qo'mita o'zining 34-sonli Umumiy tartibdagi sharhida¹⁰ bevosita ko'rsatib o'tgan.

17-modda (Shaxsiy hayot daxlsizligi)

Shaxsiy hayotga o'zboshimchalik bilan aralashishdan himoya qiladi. BMTning Inson huquqlari bo'yicha qo'mitasi 16-sonli umumiy tartibdagi izohida¹¹ buni davlatlarning shaxsiy ma'lumotlarni kompyuterlar va ma'lumotlar banklarida to'plash va saqlashni qonuniy tartibga solish majburiyati sifatida talqin qiladi.

FS'HXP va Umumiy e'tirozlardan tashqari, Maxsus ma'ruzachilarning rolini alohida ta'kidlash lozim.

⁸ Internetda inson huquqlarini rag'batlantirish, himoya qilish va amalga oshirish

⁹ https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

¹⁰ <https://hrlibrary.umn.edu/russian/gencomm/Rhrcom34.html>

¹¹ <https://hrlibrary.umn.edu/russian/gencomm/Rhrcom16.html>

BMT maxsus ma'ruzachilari o'zlarining mavzuga oid ma'ruzalari orqali fikr erkinligi va uni erkin ifodalash huquqini himoya qilish va rag'batlantirish sohasidagi standartlarni ishlab chiqishda muhim rol o'ynaydilar.

Maxsus ma'ruzachilarning pozitsiyasi de-fakto "yumshoq huquq" bo'lib, mohiyatan alohida davlatlar tomonidan qo'llanilishi va implementatsiya qilinishi shart emasligiga qaramay. Shunga qaramay, Maxsus ma'ruzachilarning pozitsiyasi va ma'ruzalari alohida davlatlarning huquqiy tizimlari uchun huquqiy fikrning uslubi va yo'nalishini belgilaydi.

Asosiy ma'ruzalar

Fikr erkinligi va uni erkin ifodalash huquqini rag'batlantirish va himoya qilish bo'yicha maxsus ma'ruzachi Frank La Ryu ma'ruzasi, 2011-yil, A/HRC/17/27¹²

Ushbu ma'ruzada barcha shaxslarning Internet orqali har qanday turdagi axborot va g'oyalarni izlash, olish va tarqatish huquqi bilan bog'liq asosiy tendensiyalar va muammolar ko'rib chiqiladi. Maxsus ma'ruzachi Internetning o'ziga xos va o'zgaruvchan tabiatini ta'kidlaydi, bu esa shaxslarga nafaqat o'z fikr erkinligi va erkin so'zlash huquqini, balki boshqa bir qator inson huquqlarini ham amalga oshirish, shuningdek, umuman jamiyat rivojlanishiga hissa qo'shish imkonini beradi.

Ma'ruzada davlatlar tomonidan Internetdagi ma'lumotlarga nisbatan senzuraning kuchaytirishning ba'zi usullari tavsiflangan, xususan:

- kontentni ixtiyoriy ravishda bloklash yoki ixtiyoriy ravishda filtrlash;
- qonuniy fikr bildirishni jinoiy javobgarlikka tortish;
- javobgarlikni vositachilarga yuklash;
- foydalanuvchilarni Internetdan foydalanish imkoniyatidan mahrum qilish, shu jumladan intellektual mulk huquqlari to'g'risidagi qonunni buzish asosida;
- kiberhujumlar va shaxsiy hayot daxlsizligi hamda ma'lumotlarni himoya qilish huquqining yetarli darajada ta'minlanmaganligi.

Fikr erkinligi va uni erkin ifodalash huquqini rag'batlantirish va himoya qilish bo'yicha maxsus ma'ruzachi Devid Keyning ma'ruzasi, 2015-yil, A/HRC/29/32¹³

Ushbu ma'ruzada Maxsus ma'ruzachi raqamli xabarlarini uzatishda shifrlash vositalari va anonimlikdan foydalanish masalasini ko'rib chiqadi. Hisobotda shifrlash va anonimlik odamlarga raqamli asrda fikr erkinligi va ularni erkin ifodalash huquqlarini amalga oshirish imkonini beradi va shuning uchun ishonchli himoyadan foydalanishlari kerak, degan xulosaga kelingan.

Asosiy tezis: Ma'ruzachi shifrlash va anonimlikni erkin fikr bildirish uchun zarur bo'lgan **"maxfiylik hududi"** deb ta'rifladi. Uning ta'kidlashicha, "anonimlikni taqiqlash zo'ravonlik va qatag'on qurbonlariga sezilarli "sovutuvchi ta'sir" (chilling effect) ko'rsatadi," ularni tanib qolishdan qo'rqib jim turishga majbur qiladi.

Dezinformatsiya va fikrlar erkinligi hamda ularni erkin ifodalash Fikr va so'z erkinligi huquqini rag'batlantirish va himoya qilish bo'yicha maxsus ma'ruzachi Aydin Xanning 2021-yilgi ma'ruzasi, A/HRC/47/25¹⁴

Ushbu ma'ruzada Fikr erkinligi va uni erkin ifodalash huquqini rag'batlantirish va himoya qilish bo'yicha maxsus ma'ruzachi dezinformatsiya natijasida inson huquqlari, demokratik institutlar va rivojlanish jarayonlariga tahdidlarni ko'rib chiqadi.

Maxsus ma'ruzachi raqamli davrda noto'g'ri ma'lumotlar keltirib chiqaradigan qiyinchiliklar va muammolarni tan olgan holda, davlatlar va kompaniyalar tomonidan ko'rilgan choralar muammoli, nomuvofiq va inson huquqlari uchun zararli deb hisoblaydi.

Asosiy tezis: Xon "soxta yangiliklar"ga qarshi kurash to'g'risidagi qonunlarni tanqid qilib, noaniq iboralar davlatlarga senzura uchun "siyosiy erkinlik" berishini ta'kidladi. U standartni tasdiqladi: yolg'onga qarshi blokirovkalar bilan emas, balki ishonchli ma'lumotlar va raqamli savodxonlikni targ'ib qilish orqali kurashish kerak.

Shunday qilib, Maxsus ma'ruzachilar ishi tufayli xalqaro standartlar ayrim raqamli huquqlarni amalga oshirish va himoya qilish yondashuvini tartibga soluvchi o'ta muhim elementlar bilan to'ldirildi.

¹² <https://docs.un.org/ru/A/HRC/17/27>

¹³ <https://docs.un.org/ru/a/hrc/29/32>

¹⁴ <https://docs.un.org/ru/a/hrc/47/25>

Masalan, Frank La Ryu (A/HRC/17/27) ma'ruzasiga tayanib, xalqaro huquq internet-shatdaunlar (Internetga kirish huquqi) bo'yicha qat'iy pozitsiyani ishlab chiqdi.

Ya'ni, Internet yoki mobil aloqadan foydalanishni to'liq to'xtatish har qanday sharoitda (hatto favqulodda holat rejimida ham) nomutanosib chora hisoblanadi, chunki u favqulodda xizmatlar ishini falajlaydi va favqulodda holat predmetiga bevosita jalb qilinmagan aholiga nomutanosib zarar yetkazadi.

Keyinchalik, A/HRC/29/32 hisobotida Devid Key davlatlarga kriptografiya (maxfiylik va shifrlash huquqi) bo'yicha aniq talablarni belgilab berdi:

1. Davlatlar platformalardan "bekdorlar" (maxsus xizmatlar uchun zaifliklar) joriy etishni talab qilmasligi kerak.
2. Davlatlar shifrlash kalitlarini deponentlashni (ularni saqlash uchun uchinchi tomonga berishni) talab qilmasligi kerak.
3. Shifrlashni cheklashga butun xizmat uchun ommaviy ravishda emas, balki faqat individual asosda (sud qarori bilan muayyan qurilma uchun) yo'l qo'yiladi.

Nihoyat, Devid Key (A/HRC/38/35) o'z ma'ruzasida foydalanuvchi kontentini tartibga solish (Sun'iy intellekt va moderatsiya) bo'yicha quyidagi ma'ruzani taqdim etdi:

1. Kompaniyalar moderatsiya paytida "protsessual adolat"ni ta'minlashlari kerak. Bu shuni anglatadiki, agar algoritm (SI) foydalanuvchi postini o'chirib tashlasa, odam quyidagilarni olishi kerak:
 - 1.1. aniq sabab ko'rsatilgan xabarnoma;
 - 1.2. qarorga bot emas, balki haqiqiy xodim oldida e'tiroz bildirish imkoniyati.

Raqamli huquqlarni cheklash: "uch bosqichli test"

Raqamli huquqlar mutlaq emas va muayyan shartlar bajarilganda cheklanishi mumkin.

Masalan, FS'HXP 19-moddasining 3-bandiga ko'ra, cheklovlar faqat uchta shartga rioya qilinganda qonuniy hisoblanadi:

1. **Qonuniylik:** cheklov fuqaro o'z harakatlarining oqibatlarini oldindan ko'ra olishi uchun tushunarli, aniq va yetarli darajada aniq ifodalangan qonunda nazarda tutilishi kerak. (Qonunda ta'rif berilmagan "ijtimoiy adovatni qo'zg'atish" kabi noaniq iboralar ushbu tamoyilni buzadi).
2. **Qonuniy maqsad:** milliy xavfsizlik, tartib, sog'liq, axloq, boshqa shaxslarning huquqlarini himoya qilish.
3. **Zaruriyat va Mutanosiblik:** eng kam aralashuv tamoyiliga ko'ra, davlat tanlangan chora (masalan, bloklash) maqsadga erishishning eng kam qat'iy usuli ekanligini isbotlashi shart. Agar bitta fikrni o'chirish mumkin bo'lsa, butun saytni bloklash mumkin emas.

Isbotlash majburiyati foydalanuvchiga emas, davlatga yuklanadi.

Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt (1984) qoidalaridan cheklanishlar va istisnolarni sharhlashning Sirakuza tamoyillari (Sirakuza tamoyillari) muhim hujjat hisoblanadi.

FS'HXP ba'zi hollarda muayyan maqsadlar (masalan, jamoat tartibi) uchun ayrim inson huquqlarini (masalan, so'z yoki yig'ilishlar erkinligi) cheklashga ruxsat beradi. Biroq, davlatlar ko'pincha ushbu shartlarni suiiste'mol qiladilar.

Sirakuza tamoyillarining maqsadi "milliy xavfsizlik," "jamoat tartibi" va "zarurlik" atamalarining ma'nosini aniq huquqiy ta'riflashdan iborat bo'lib, ulardan qatag'on qilish uchun bahona sifatida foydalanish imkoniyatini istisno qiladi.

Sirakuza prinsiplari, shuningdek, Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt (matnda keyingi o'rinlarda — 'Sirakuza prinsiplari') qoidalaridan cheklovlar va chekinishlarni talqin qiladi va quyidagilarni belgilaydi:

- «Inson huquqlarini amalga oshirishdagi hech qanday cheklov Paktga zid bo'lmagan va cheklov joriy etilgan paytda amalda bo'lgan umumiy qo'llaniladigan milliy qonunga muvofiq joriy etilmaydi»¹⁵. (B.i.15 Sirakuza tamoyillari).
- Bundan tashqari, "Pakt bilan kafolatlangan huquqning cheklanishini asoslash majburiyati davlat zimmasida bo'ladi" (A.12. Sirakuza tamoyillari).



Sirakuza tamoyillari (1984) inson huquqlarining yo'l qo'yilishi mumkin bo'lgan cheklovlarini sharhlashning nufuzli manbai hisoblanadi. Ular milliy xavfsizlikka havola qilish hukumatni tanqiddan himoya qilish yoki huquqbuzarliklarni yashirish uchun qo'llanilmasligi va har qanday cheklovlar qat'iy zarur va tahdidga mutanosib bo'lishi kerakligini belgilaydi. Raqamli asrda bu tamoyillar ixtiyoriy blokirovka va yalpi kuzatuvga qarshi asosiy huquqiy dalil bo'lib xizmat qiladi».

Mintaqaviy standartlar

Ko'pgina me'yorlar deklarativ xususiyatga ega bo'lgan universal darajadan farqli o'laroq, inson huquqlarining mintaqaviy tizimlari majburiy huquqiy rejimlarni yaratadi. Jahonda raqamli tartibga solishning bir nechta «raqobatlashuvchi» tizimlari shakllangan.

Ushbu qo'llanmada biz Yevropa raqamli tartibga solish tizimiga e'tibor qaratamiz.

Yevropa tizimi Yevropa Kengashi va Yevropa Ittifoqini o'z ichiga oladi.

Yevropa hozirda raqamli huquqlarni kodifikatsiya qilishda global yetakchi bo'lib, Yevropa me'yorlari de-fakto global bo'lib borayotgan «Bryussel effekti»¹⁶ni shakllantirmoqda.

Normativ-huquqiy baza markazida Inson huquqlari bo'yicha Yevropa konvensiyasi (IHYK) turadi. Ushbu konvensiya Inson huquqlari bo'yicha Yevropa sudi tomonidan mohiyatan

¹⁵ Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt qoidalaridan cheklovlar va chekinishlarni talqin qilishning Sirakuza tamoyillari <http://adilet.zan.kz/rus/docs/O8500000001>

¹⁶ <https://sg-sofia.com.ua/kogda-rech-zahodit-o-rinkah-evropa-vovse-ne-ugosayushaya-sila#:~:text=%C2%AB%D0%91%D1%80%D1%8E%D1%81%D1%81%D0%B5%D0%BB%D1%8C%D1%81%D0%BA%D0%B8%D0%B9%20%D1%8D%D1%84%D0%B5%D0%BA%D1%82%C2%BB%20%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D0%BE%D0%BB%D0%B0%D0%B3%D0%B0%D0%B5%D1%82%2C%20%D1%87%D1%82%D0%BE,%D0%BD%D0%B5%D0%BC%D0%BD%D0%BE%D0%B3%D0%B8%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B8%20%D0%B7%D0%B0%D1%85%D0%BE%D1%82%D0%B5%D0%BB%D0%B8%20%D0%B1%D1%8B%20%D0%BE%D1%82%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D1%8C%D1%81%D1%8F.>

raqamli voqelikka moslashtirilgan 10-modda (fikrni ifoda etish erkinligi) va 8-moddani (shaxsiy hayot daxlsizligi) o'z ichiga oladi.

Misol

Cengiz and Others v. Turkey (2015-y.)¹⁷

Da'vogarlar, xususan, ularni YouTube'ga kirishdan butunlay mahrum qilgan chora ustidan shikoyat qilishdi. Inson huquqlari bo'yicha Yevropa sudi bitta video tufayli butun platformaga (bu holatda YouTube) kirishni bloklash Konvensiyani buzish deb hisoblaydigan standartni o'rnatdi, chunki bu fuqarolarni ulkan hajmdagi qonuniy ma'lumotlardan ("video kontent ensiklopediyasi") foydalanish imkoniyatidan mahrum qiladi.

Delfi AS v. Estoniya (2015-y.)¹⁸

Yevropa sudi o'z amaliyotida birinchi marta ommaviy axborot vositasining foydalanuvchilar tomonidan uning veb-saytiga joylashtirilgan kontent uchun javobgarligi masalasini ko'rib chiqdi. Yangiliklar portallari foydalanuvchilarning nafratni qo'zg'atuvchi sharhlari uchun, agar portal bundan tijoriy foyda ko'rsa, javobgarlikni belgiladi.

Mazkur kontekstda 2022 yilda qabul qilingan **Digital Services Act (DSA)**¹⁹ alohida e'tiborga loyiq. Agar 108+ Konvensiyasi va GDPR (quyida keltirilgan) ma'lumotlaringizni himoya qilsa, Digital Services Act qonuni platformalarning mazmuni va javobgarligini tartibga soladi.

Ushbu qonunni qabul qilishdan maqsad — kontent (onlayn-kontent) va foydalanuvchilar xavfsizligini nazorat qilish orqali xavfsiz raqamli muhit yaratish hamda texnologiya gigantlarining ta'sirini cheklashdir. Shuni ta'kidlash joizki, Digital Services Act ko'pincha **Digital Markets Act (2022-y.)**²⁰ bilan birgalikda tilga olinadi. Uni qabul qilishdan maqsad qonun "gatekeeperlar" deb ataydigan eng yirik texnologiya kompaniyalarining kuchini cheklashdir.

Ilgari Google yoki Apple ga qarshi antimonopoliya tekshiruvlari o'n yillab davom etardi; Digital Markets Act esa yondashuvni o'zgartirmoqda: endi qoidalar oldindan belgilangan va kompaniyalar ularga amal qilishga majbur, aks holda ulkan jarimalar xavfi mavjud.

N°	Digital Services Act	Digital Markets Act
1	Qoidabuzarliklarga munosabat bildirish qoidalarini belgilaydi.	Muayyan amaliyotlar zarar yetkazmasidan oldin taqiqlanadi.
2	"Aldamchi interfeyslar" (interfeys manipulyatsiyasi) va bolalarga mo'ljallangan reklamalarni taqiqlash.	"O'zini afzal ko'rish" (o'z xizmatlarini raqobatchilarnikidan ustun qo'yib targ'ib qilish) ni taqiqlash.
3	Shikoyatlarning shaffof mexanizmlarini joriy etish va bloklash sabablarini tushuntirish.	Messenjerlar va tizimlarning "interoperabelligi" (mosligi) ni ta'minlash.
4	Maxfiylikni himoya qilish. Din, salomatlik va jinsiy moyillik asosida targetingni taqiqlash	Iqtisodiy adolat. 'Gatekeeper'larga hamkorlarining ma'lumotlaridan ularga qarshi raqobat qilish maqsadida foydalanish taqiqlanadi
5	Soxta ma'lumotlarga qarshi kurashish va alohida foydalanuvchi akkauntning bloklanishiga e'tiroz bildirishning huquqiy tartibi.	Oldindan o'rnatilgan ilovalarni o'chirib tashlashingiz va turli manbalardan dasturiy ta'minotni yuklab olishingiz mumkin.

¹⁷ [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-159188%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159188%22]})

¹⁸ [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-155105%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-155105%22]})

¹⁹ https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

²⁰ <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>

6	Yevropa Ittifoqining har bir mamlakatidagi raqamli xizmatlar koordinatorlari + Yevrokomissiya (raqamli/teknologik gigantlar uchun).	Faqat Yevropa Komissiyasi (Bryusseldan bevosita nazorat).
7	Qoidabuzarliklar uchun jarima kompaniya yillik aylanmasining 6% gacha miqdorda belgilanadi	Qoidabuzarliklar uchun jarima kompaniya yillik aylanmasining 10% gacha miqdorda belgilanadi

Agar Digital Services Act va Digital Markets Act platformalarning mazmuni va mas'uliyatini tartibga solsa, 108+ Konvensiyasi, 95/46/EC Direktivasi va GDPR shaxsiy ma'lumotlarni himoya qiladi.

Shaxsiy ma'lumotlarni himoya qilish mavzusi bilan bog'liq xalqaro standartlar murakkab "evolyutsion" yo'lni bosib o'tmoqda va hozirgi vaqtda ma'lumotlar maxfiyligi tamoyillarining uchta "avlodi"ni ifodalaydi.

Ma'lumotlar maxfiyligi tamoyillarining birinchi "avlodi"ga Yevropa Kengashining Shaxsiy ma'lumotlarga avtomatlashtirilgan ishlov berishda jismoniy shaxslarni himoya qilish to'g'risidagi Konvensiyasi yoki 1981-yilda qabul qilingan [108²¹-Konvensiya](#) kiradi.

Ma'lumotlar maxfiyligi tamoyillarining ikkinchi "avlod"iga ko'proq Yevropa Ittifoqining "Shaxsiy ma'lumotlarga ishlov berishda jismoniy shaxslarni himoya qilish va bunday ma'lumotlarning erkin aylanishi to'g'risida"gi [95/46/EC²² sonli Direktivasini](#) kiritish mumkin.

Nihoyat, ma'lumotlar maxfiyligi standartlarining uchinchi "avlodi"ga 2016-yilda qabul qilingan [GDPR²³](#) hamda 108-sonli Konvensiya asosida 2018-yilda qabul qilingan 108+ Konvensiyasi kiradi.

Shuni ta'kidlash joizki, ma'lumotlar maxfiyligi tamoyillarining har bir "avlodi"da shartli ravishda (!) 10 tadan standartni ajratib ko'rsatish mumkin.

Standartlarning birinchi "avlodi"	
1	Ma'lumotlarni to'plash — cheklangan (me'yordan ortiq bo'lmagan), qonuniy (qonuniy maqsadlarda) va halol vositalar orqali amalga oshirilishi lozim.
2	Ma'lumotlar sifati — dolzarblik, aniqlik va yangilanganlik.
3	Yig'ish vaqti bo'yicha maqsadlarni belgilash.
4	Maqsad/huquqlar haqida xabarnoma.
5	Foydalanish — ko'rsatilgan yoki ular bilan mos keladigan maqsadlar doirasida cheklangan (jumladan, oshkor etish ham).
6	Oqilona ehtiyot choralari yordamida xavfsizlik.
7	Shaxsiy ma'lumotlardan foydalanish amaliyotiga nisbatan ochiqlik (nafaqat ma'lumotlar subyektlari uchun).
8	Kirish huquqi — shaxsning o'z ma'lumotlariga kirish bo'yicha individual huquqi.
9	Tuzatish — tuzatishga bo'lgan yakka tartibdagi huquq.
10	Hisobdorlik — identifikatsiya qilingan ma'lumotlar nazoratchisi.

²¹ <https://rm.coe.int/1680078c46>

²² <https://www.tgl.net.ru/files/infosafety/%D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%B0%2095-46.pdf>

²³ <https://gdpr-info.eu/>

Standartlarning ikkinchi “avlodi”	
1	Maqsadga erishish uchun zarur bo'lgan minimal ma'lumotlarni yig'ish (ma'lumotlarni minimallashtirish).
2	Maqsadga erishilgandan so'ng ma'lumotlarni yo'q qilish yoki egasizlantirish.
3	Muayyan toifadagi maxfiy ma'lumotlarni qo'shimcha himoyalash.
4	Ma'lumotlarni qayta ishlashning qonuniy asoslari belgilandi.
5	Ayrim sezgir ishlov berish tizimlariga qo'shimcha cheklovlar; “oldindan tekshirish” tartibi.
6	Avtomatlashtirilgan qaror qabul qilish cheklovlari (jumladan, qayta ishlash mantiqini bilish huquqi).
7	Qayta ishlashga jiddiy qonuniy sabablarga ko'ra e'tiroz bildirish.
8	Qabul qiluvchi davlatdan “muvofiq” yoki muqobil kafolatlar talab qiladigan ma'lumotlarning cheklangan eksporti.
9	Ma'lumotlarni himoya qiluvchi mustaqil organning mavjudligi.
10	Ma'lumotlarning maxfiyligini ta'minlash uchun sudga murojaat qilish.
Standartlarning uchinchi “avlodi”	
1	Reja va sukut bo'yicha ma'lumotlarni himoya qilish.
2	Namoyish etilgan hisobdorlik.
3	Ma'lumotlarni himoya qilish bo'yicha mustaqil organga ma'lumotlar buzilishi/sizib chiqishi haqida xabar berish.
4	Ishlov beruvchilarning (shaxsiy ma'lumotlarning) bevosita javobgarligi.
5	Rozilik olishning yanada qat'iy talablari.
6	Ishlov berishning barcha jabhalarida mutanosiblik talablari.
7	Qarorlar qabul qilish va ma'muriy jazo choralarini, shu jumladan jarimalarni qo'llash uchun ma'lumotlarni himoya qilish bo'yicha mustaqil organning mavjudligi.
8	Biometrik va genetik ma'lumotlarni himoya qilishga qo'yiladigan yuqori (qo'shimcha) talablar.
9	Ma'lumotlarni o'chirish bo'yicha kuchaytirilgan huquq, jumladan “unutish huquqi”.
10	Ma'lumotlarni himoya qilish bo'yicha mustaqil organ xalqaro shikoyatlarni ko'rib chiqishda hamkorlik qilishi shart.

1.3. O'zbekistonning raqamli huquqlar sohasidagi milliy qonunchiligi

O'zbekiston Respublikasi Konstitutsiyasi xalqaro huquqning umume'tirof etilgan normalari ustunligini tan oladi. Konstitutsiyaning 15-moddasida xalqaro huquq prinsiplari va normalari O'zbekiston huquq tizimining ajralmas qismi sifatida e'tirof etilib, inson huquq va erkinliklarini ta'minlash hamda ularni himoya qilish faqat davlatning ichki ishi doirasidan tashqariga chiqishi ko'rsatib o'tilgan. Xalqaro normalar va milliy qonunchilik bir-biriga zid bo'lgan taqdirda xalqaro shartnoma qoidalari qo'llaniladi. Konstitutsiyaviy tamoyillar so'z erkinligi, axborot olish, Internet va raqamli xizmatlardan foydalanish sohasidagi xalqaro standartlarning ustunligini tan olish uchun asos yaratadi.

Fikr bildirish erkinligi va axborot olish huquqi O'zbekiston Konstitutsiyasining 33-moddasida kafolatlangan bo'lib, unda shunday deyiladi: “Har kim fikrlash, so'z va e'tiqod erkinligi huquqiga ega. Har kim istalgan axborotni izlash, olish va tarqatish huquqiga ega,” shuningdek, davlatning axborotdan raqamli shaklda foydalanishni ta'minlash majburiyati: “Davlat Internet jahon axborot tarmog'idan foydalanishni ta'minlash uchun shart-sharoitlar yaratadi.”

Konstitutsiyaning 34-moddasida belgilangan axborot olish huquqlarining hajmi davlat organlari va tashkilotlari, fuqarolarning o'zini o'zi boshqarish organlari hamda ularning mansabdor shaxslari har kimga uning huquqlari va qonuniy manfaatlariga daxldor hujjatlar, qarorlar va boshqa materiallar bilan tanishish imkoniyatini ta'minlash majburiyatini nazarda tutadi.

Boshqa konstitutsiyaviy norma jamoatchilik nazorati shaklida axborotdan foydalanish huquqi uchun asosni belgilaydi: "Har kim qulay atrof-muhit, uning holati to'g'risida ishonchli axborot olish huquqiga ega. Davlat fuqarolarning ekologik huquqlarini ta'minlash va atrof-muhitga zararli ta'sir ko'rsatishning oldini olish maqsadida shaharsozlik faoliyati sohasida jamoatchilik nazoratini amalga oshirish uchun shart-sharoitlar yaratadi. Shaharsozlik hujjatlari loyihalari qonunda belgilangan tartibda jamoatchilik muhokamasidan o'tkaziladi.

Bundan tashqari, Konstitutsiyaning 31-moddasi xususiy hayot va shaxsga doir ma'lumotlarni himoya qilish huquqini belgilaydi:



Har bir inson xususiy hayot daxlsizligi, shaxsiy va oilaviy sir, o'z sha'ni va qadr-qimmatini himoya qilish huquqiga ega.

Har bir inson yozishmalar, telefon orqali so'zlashuvlar, pochta, elektron va boshqa xabarlar sir saqlanishi huquqiga ega. Ushbu huquqni cheklashga faqat qonunga muvofiq va sud qarori asosida yo'l qo'yiladi.

Har kim o'z shaxsiy ma'lumotlarini himoya qilish, shuningdek noto'g'ri ma'lumotlarni tuzatishni, o'zi to'g'risida qonunga xilof ravishda to'plangan yoki bundan buyon huquqiy asosga ega bo'lmagan ma'lumotlarni yo'q qilishni talab qilish huquqiga ega."

Ushbu qoidalar ma'lumotlarni himoya qilish va shaxsiy hayot bilan bog'liq mamlakat huquqiy bazasining eng muhim qismini tashkil etadi. Ushbu maqola axborotdan foydalanish huquqi va shaxsiy hayot hamda shaxsiy ma'lumotlarni himoya qilish zarurati o'rtasidagi muvozanatning muhimligini ta'kidlaydi.

Axborot erkinligi to'g'risidagi qonun hujjatlarining vazifalari axborot erkinligi prinsiplari va kafolatlariga rioya etilishini ta'minlashni; har kimning axborotni erkin va moneliksiz izlash, olish, o'rganish, tarqatish, undan foydalanish va uni saqlash huquqini amalga oshirishni; axborot muhofazasini hamda shaxs, jamiyat va davlatning axborot xavfsizligini ta'minlashni o'z ichiga oladi. Axborot olish huquqi davlat hokimiyati va boshqaruvi organlari hamda ular mansabdor shaxslarining qabul qilinayotgan qarorlar uchun mas'uliyatini oshirishni ta'minlashga qaratilgan. Har bir shaxs davlat organlarining tashkil etilishi va faoliyat ko'rsatishi hamda mazkur shaxsga yoki shaxslar guruhiga taalluqli hujjatlarni qabul qilish jarayonlari to'g'risidagi axborotdan foydalanish huquqiga ega. Biroq, amaldagi qonunchilik bazasi to'g'ridan to'g'ri axborot olish huquqini nazarda tutmaydi, balki axborotni izlash huquqini nazarda tutadi.

Axborot olish huquqi asosan "Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi O'zbekiston Respublikasi Qonuni, "Axborot olish kafolatlari va erkinligi to'g'risida"gi O'zbekiston Respublikasi Qonuni, "Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to'g'risida"gi O'zbekiston Respublikasi Qonuni, "Ommaviy axborot

vositalari to'g'risida"gi O'zbekiston Respublikasi Qonuni, "Rasmiy statistika to'g'risida"gi O'zbekiston Respublikasi Qonuni, "Korrupsiyaga qarshi kurashish to'g'risida"gi O'zbekiston Respublikasi Qonuni, "Huquqiy axborotni tarqatish va undan foydalanish to'g'risida"gi O'zbekiston Respublikasi Qonuni kabi birlamchi qonunchilik hujjatlari bilan ta'minlanadi.

Qonunchilik ham axborotga, ham hujjatlar yoki yozuvlarga kirishning umumiy huquqini nazarda tutadi. Huquqiy talablarning davlat hokimiyatining barcha tarmoqlariga qo'llanilishiga nisbatan qonun axborot egasiga qat'iy tartibda axborotga egalik qiluvchi, undan foydalanuvchi va uni tasarruf etuvchi hamda bunga bo'lgan huquqlari qonun hujjatlarida yoki axborot egasi tomonidan belgilangan huquqlar bilan cheklanmagan yuridik yoki jismoniy shaxs sifatida keng ta'rif beradi.

Shu bilan birga, qonunchilikda davlat nazorati ostidagi korxonalar, jamg'armalar, davlat funksiyalari berilgan tashkilotlarning o'z faoliyati to'g'risidagi axborotdan foydalanishini ta'minlash bo'yicha to'g'ridan-to'g'ri majburiyati mavjud emas. Vaholanki, xalqaro standartlar barcha davlat hokimiyati organlariga, shuningdek, davlat tomonidan moliyalashtiriladigan, davlat nazorati ostida bo'lgan yoki davlat funksiyalarini bajaruvchi xususiy tashkilotlarga taalluqli bo'lishi kerak bo'lgan axborotdan foydalanish foydasiga prezumpsiya o'rnatishni talab qiladi.

Konstitutsiyaning 33-moddasiga muvofiq "Axborotni izlash, olish va tarqatish huquqini cheklashga faqat qonunga muvofiq va faqat konstitutsiyaviy tuzumni, aholi sog'lig'ini, jamoat axloqini, boshqa shaxslarning huquq va erkinliklarini, jamoat xavfsizligini va jamoat tartibini himoya qilish, shuningdek davlat siri yoki qonun bilan qo'riqlanadigan boshqa sir oshkor etilishining oldini olish uchun zarur bo'lgan darajada yo'l qo'yiladi."

O'zbekiston Respublikasi "Davlat organlari faoliyatining ochiqligi to'g'risida"gi Qonunining 6-moddasiga muvofiq, davlat hokimiyati va boshqaruvi organlari faoliyati to'g'risidagi axborotga kirish cheklanadi, agar ushbu axborot qonunda belgilangan tartibda davlat siri yoki qonun bilan muhofaza qilinadigan boshqa sirlar toifasiga kiritilgan bo'lsa. Umumiy qoida sifatida davlat organlari, fuqarolarning o'zini o'zi boshqarish organlari, jamoat birlashmalari, korxonalar, muassasalar, tashkilotlar va mansabdor shaxslar davlat siri yoki qonun bilan muhofaza qilinadigan boshqa sirlarni o'z ichiga olgan axborotni taqdim etishga haqli emas.

Quyidagi ma'lumotlar cheklanishi mumkin emas:



Fuqarolarning huquq va erkinliklari, ularni amalga oshirish tartibi to'g'risidagi, shuningdek davlat hokimiyati va boshqaruvi organlari, fuqarolarning o'zini o'zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlarining huquqiy maqomini belgilovchi qonun hujjatlari;



Ekologik, meteorologik, demografik, sanitariya-epidemiologik, favqulodda vaziyatlar to'g'risidagi ma'lumotlar hamda aholi, aholi punktlari, ishlab chiqarish obyektlari va kommunikatsiyalarning xavfsizligini ta'minlash uchun zarur bo'lgan boshqa ma'lumotlar;



Axborot-kutubxona muassasalarining ochiq fondlarida, arxivlarda, idoraviy arxivlarda, O'zbekiston Respublikasi hududida faoliyat ko'rsatayotgan yuridik shaxslarning axborot tizimlarida mavjud bo'lgan axborot.

Qonunchilik davlat hokimiyati va boshqaruvi organlariga maxfiy ma'lumotlar ro'yxatini buyruqlar yoki ichki hujjatlar shaklida belgilashga ruxsat beradi, xalqaro standartlarga ko'ra esa har qanday cheklovlar qonunda nazarda tutilgan bo'lishi va uch komponentli testga mos kelishi kerak. Biroq, xalqaro standartlarga mos kelish uchun istisnalar konstitutsiyaviy majburiyatlarga mos kelishi va axborotdan foydalanish huquqi hajmini cheklamaslik uchun uch komponentli testni o'z ichiga olishi kerak. Axborotdan foydalanish to'g'risidagi qonunlarda axborotni oshkor qilish foydasiga istisnolardan foydalanish imkonini beruvchi jamoat manfaatlarining ustuvorligi to'g'risidagi qoidalar mavjud emas. Xalqaro maksimal oshkor qilish standartlariga javob berish uchun asosiy ijtimoiy ahamiyatga ega bo'lgan ma'lumotlar proaktiv yoki avtomatik ravishda e'lon qilinishi kerak.

1.3.1. Ommaviy axborot vositalari to'g'risidagi qonunchilik

O'zbekistonda ommaviy axborot vositalari (OAV) va jurnalistlar faoliyati quyidagi asosiy normativ-huquqiy hujjatlar bilan tartibga solinadi: O'zbekiston Respublikasi Konstitutsiyasi, O'zbekiston Respublikasining "Ommaviy axborot vositalari to'g'risida"gi, "Jurnalistlik faoliyatini himoya qilish to'g'risida"gi, "Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi, "Axborotlashtirish to'g'risida"gi, "Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to'g'risida"gi qonunlari, shuningdek, Vazirlar Mahkamasining "O'zbekiston Respublikasi hududida xorijiy davlatlar ommaviy axborot vositalari muxbirlarining kasbiy faoliyatini tartibga soluvchi asosiy qoidalarini tasdiqlash to'g'risida"gi qarori va OAVni davlat ro'yxatidan o'tkazish bo'yicha davlat xizmati ko'rsatishning ma'muriy reglamenti.

OAVning axborotni izlash, olish, tadqiq etish, tarqatish, foydalanish, saqlash erkinligi Konstitutsiyaning 81-moddasida tarqatilayotgan axborotning xolisligi va ishonchliligi uchun javobgarlik sharti bilan kafolatlanadi:



Ommaviy axborot vositalari erkindir va qonunga muvofiq faoliyat yuritadi. Davlat ommaviy axborot vositalari faoliyatining erkinligini, ularning axborotni izlash, olish, undan foydalanish va uni tarqatish huquqlarini amalga oshirishlarini kafolatlaydi. Ommaviy axborot vositalari o'zlari taqdim etayotgan axborotning ishonchliligi uchun javobgardirlar." Senzura taqiqlanadi va ommaviy axborot vositalari faoliyatiga to'sqinlik qilish yoki aralashish qonunga muvofiq javobgarlikka sabab bo'ladi.

O'zbekistonning ommaviy axborot vositalari to'g'risidagi qonunchiligi turli subyektlar, shu jumladan ommaviy axborot vositalari tomonidan axborot makonida yaratiladigan va tarqatiladigan ma'lumotlarning ishonchliligini ta'minlashga qaratilgan huquqiy asoslarni yaratadi.

Ommaviy axborot vositalari to'g'risidagi qonun quyidagi turdagi axborotlarni tarqatishni taqiqlaydi:

Axborot toifasi	Dezinformatsiya bilan bog'liqlik
Konstitutsiyaviy tuzumni zo'ravonlik bilan o'zgartirishga va separatizmga da'vat etish	Davlat yoki konstitutsiyaviy tuzumga putur yetkazishga qaratilgan nashrlarni to'g'ridan-to'g'ri taqiqlash, siyosiy dezinformatsiyaning bir shakli
Terrorizm va diniy ekstremizmni targ'ib qilish	Ko'pincha faktlarni buzib ko'rsatish orqali amalga oshiriladi.
Davlat sirini yoki boshqa maxfiy axborotni oshkor qilish	Agar u 'sensasiyaviy haqiqat' sifatida taqdim etilib, auditoriyani chalg'itsa, bu huquqbuzarlik hisoblanadi/ Agar biror ma'lumot chalg'ituvchi tarzda sensasiyaviy haqiqat" sifatida taqdim etilsa, bu qoidabuzarlik hisoblanadi.
Milliy, irqiy, etnik yoki diniy adovatni qo'zg'atuvchi axborot	Dezinformatsiya jamoatchilik fikrini manipulyatsiya qilish va nizolarni kuchaytirish uchun ishlatilishi mumkin
Surishtiruv, tergov yoki sud materiallarini e'lon qilishni taqiqlash	Surishtiruv va dastlabki tergov ma'lumotlarining maxfiyligini himoya qilish ochiq sud majlislarini yoritishga tatbiq etilmaydi.
Fuqarolarning sha'ni, qadr-qimmati yoki ishchanlik obro'siga putur yetkazuvchi ma'lumotlar	Shaxsning sha'nini yerga uradigan, oldindan bila turib yolg'on ma'lumotlar va faktlarni e'lon qilishni taqiqlash (diffamatsiya)

Bundan tashqari, ommaviy axborot vositalari jamoat tartibiga tahdid solgan yolg'on ma'lumotlarni e'lon qilganlik; taqiqlangan g'oyalarni targ'ib qilish maqsadida faktlarni manipulyatsiya qilganlik; fuqarolarning obro'si, huquqlari va shaxsiy hayotiga zarar yetkazgan faktlarni tekshirmasdan e'lon qilganlik uchun javobgarlikka tortilishi mumkin.

OAV bosh muharrir yoki jurnalist timsolida haqiqatga to'g'ri kelmaydigan materiallarni tarqatganlik uchun quyidagi hollarda javobgar bo'lmaydi, agar bu ma'lumotlar:



ma'lumotlar rasmiy xabarlar, normativ-huquqiy hujjatlar yoki rasmiy statistika hisoboti ma'lumotlaridan olingan yoxud axborot agentliklari yoki matbuot xizmatlari, shuningdek davlat hokimiyati va boshqaruvi organlarining rasmiy veb-saytlari orqali olingan bo'lsa;



oldindan yozib olinmasdan efirga uzatiladigan mualliflik chiqishlarida mavjud bo'lsa yoki chiqishlarning so'zma-so'z takrorlanishi (stenografik, audio-, videoyozuv) hisoblansa.

Ushbu normalar jurnalistlar va tahririyatlarni rasmiy yoki ishonchli manbalardan olingan ma'lumotlar uchun javobgarlikdan himoya qilish tamoyilini aks ettiruvchi javobgarlikni istisno etadi, bu esa o'z-o'zidan so'z erkinligi xalqaro standartlariga mos keladi. Biroq, javobgarlikdan ozod qilishning cheklangan hajmi OAV erkinligining haqiqiy kafolatlarini amalga oshirish nuqtai nazaridan savollar tug'diradi.

Ma'lumot ochiq, ammo norasmiy manbalardan (masalan, guvohlarning intervyulari, fuqarolik jurnalistikasi materiallari, xorijiy nashrlar) olingan hollarda, hatto e'lon qilingan paytda ma'lumotlarning ishonchliligiga shubha qilishga asos bo'lmasa ham, tahririyat javobgarlikka tortilishi mumkin. Bunday huquqiy noaniqlik tahririyatlarni, ayniqsa nozik mavzularda (korruptsiya, davlat xavfsizligi, saylovlar va boshqalar) o'z-o'zini senzura qilishga majbur qiladi.

Ommaviy axborot vositalari to'g'risidagi qonun har bir shaxsga ommaviy axborot vositalarida chiqish qilish, o'z fikri va e'tiqodini ochiq bayon etish huquqini beradi. Shu bilan birga, faktologik xabar va baholash mulohazasi o'rtasida aniq chegara yo'q, bu esa sanksiyalarni tanlab qo'llash uchun sharoit yaratadi. Fikrlar, hatto ular bahsli yoki yoqimsiz bo'lsa ham, "ishonchlilik"ka tekshirilmaydi va javobgarlikka asos bo'la olmaydi, chunki bu FS'HX'ning 19-moddasiga ziddir.

O'zbekiston Respublikasining "Jurnalistlar kasbiy faoliyatining kafolatlari to'g'risida"gi Qonunining 6-moddasida qo'shimcha qo'llab-quvvatlovchi mexanizmlar mavjud bo'lib, unda jurnalistlarning tayyorlanayotgan materiallarning ishonchliligini tekshirish va xolis axborot taqdim etish majburiyati belgilangan.

OAV va jurnalistlarga nisbatan asosiy cheklov choralari quyidagilarni o'z ichiga oladi:

Jurnalistning majburiyatlari	Tahririyatning majburiyatlari
Materiallarning ishonchliligini tekshirish va xolis axborot taqdim etish	Axborot manbalarini tekshirish, fakt-cheking.
Qonunchilik va xalqaro shartnomalarga rioya etish	Ommaviy axborot vositalari faoliyati va axborot tarqatish to'g'risidagi qonunchilikka rioya etish
Aybsizlik prezumpsiyasi	Ushbu tamoyil sudyalari, xalq maslahatchilari va jinoyat protsessi ishtirokchilari uchun majburiy bo'lib, shaxsning aybdorligiga oid barcha shubhalarni ayblanuvchining foydasiga talqin qilishni taqozo etadi. Jurnalistlar va fuqarolar fikrni shakllantirishda ushbu tamoyildan foydalanishga majbur emaslar. Ommaviy axborot vositalari materiallarini e'lon qilishda gumon qilinayotgan, ayblanayotgan yoki huquqbuzarlik sodir etganlikda sudlangan shaxsni farqlash zaruratidan iborat.
Kasbiy etikaga rioya qilish	Jurnalistlar hamjamiyati tomonidan o'zini o'zi tartibga solish tamoyili asosida ishlab chiqilishi va qo'llanilishi lozim bo'lgan ichki axloqiy qoidalarni belgilash.
Shaxsiy hayot haqidagi ma'lumotlardan shaxsiy maqsadlarda foydalanishni taqiqlash	Yetarli darajadagi ijtimoiy manfaatdorliksiz maxfiy bo'lgan shaxsiy hayot to'g'risidagi axborotni tarqatishni taqiqlash, bundan hamma foydalanishi mumkin bo'lgan manbalarda e'lon qilingan ma'lumotlar mustasno. Jamoatchilik nazorati va hisobdorligini amalga oshirish maqsadida davlat hokimiyati va boshqaruvi tizimida siyosiy lavozimlarni egallab turgan shaxslarga tatbiq etilmaydi.

Bunda, jurnalistlarning ishonchliligini tekshirish bo'yicha majburiyatlar kengaytirilgan formatda talqin qilinishi va shaxslarning fikrlari va mulohazalariga nisbatan qo'llanilishi mumkin. Qonunda "halol surishtiruv," "manbani jurnalistik tekshirish," "jamoat manfaati" tushunchalari mustahkamlanmagan, bu esa professional standartlarga rioya qilgan holda ham OAVni himoya qilishni qiyinlashtiradi. OAV va jurnalistlar to'g'ridan-to'g'ri dezinformatsiya uchun emas, balki uchinchi shaxslardan olingan ma'lumotlarni tekshirish imkoniyati yo'qligi uchun javobgar bo'lishi mumkin.

Qonunchilikda OAVning halollik prezumpsiyasi mavjud emas, bu esa OAV jurnalistlarini zaif ahvolga solib qo'yadi. Bahs-munozaralar yuzaga kelganda, OAV e'lon qilingan ma'lumotlarning to'g'riligini isbotlashga majbur bo'ladi. Bundan tashqari, jurnalistlar faoliyatining axloqiy masalalarini huquqiy tartibga solish ko'pincha ularni kamsitishga olib keladi. Davlat jurnalistlarning kasbiy majburiyatlarini belgilamasligi kerak. Faoliyatning axloqiy tamoyillari jurnalistlar hamjamiyati ixtiyoriga qoldirilishi lozim.

Ishonchli axborotni tarqatish bo'yicha talablar Internet tarmog'idagi axborot resurslariga tenglashtiriladigan, tahririy-nashriyot ishlovidan o'tgan, o'zgarmas shaklda tarqatish uchun

mo'ljallangan elektron shakldagi hujjatlar va ma'lumotlarni o'z ichiga olgan Internet OAVga nisbatan ham qo'llaniladi. Internet OAV o'z veb-saytida ro'yxatdan o'tkazilgan OAVni boshqa mediaresurslardan farqlash imkonini beruvchi davlat ro'yxatidan o'tkazilganligi to'g'risidagi guvohnomaning sanasi va raqamini joylashtirishi shart.

OAV to'g'risidagi qonunchilik, shuningdek, noto'g'ri ma'lumotlarni e'lon qilish bilan bog'liq nizolarni sudgacha hal qilishning muqobil usulini taqdim etadi. "Ommaviy axborot vositalari to'g'risida"gi Qonunning 34-moddasiga ko'ra, manfaatdor shaxslarga davlat aralashuvisiz ma'lumotlarni rad etish yoki ularga javob berish imkoniyati beriladi. E'lon qilish natijasida huquqlari va qonuniy manfaatlari buzilgan yuridik va jismoniy shaxslar mazkur ommaviy axborot vositasida raddiya yoki javob e'lon qilishga haqli. Raddiya yoki javob javobning paydo bo'lishiga sabab bo'lgan material joylashtirilgan sahifada maxsus rukn ostida e'lon qilinishi kerak. Teleko'rsatuvlar, radioeshittirishlar, videoeshittirishlar, kinoxronika dasturlari va ommaviy axborotni davriy tarqatishning boshqa elektron turlari tahririyati tomonidan olingan raddiya yoki javob kelib tushgan kundan e'tiboran bir oydan kechiktirmay o'sha dasturning o'zida yoxud ko'rsatuvlar turkumida efirga uzatiladi.

Agar raddiya yoki javobni uzatish hajmi va vaqti ommaviy axborot vositasi faoliyatiga zarar yetkazishi mumkin bo'lsa, u holda axborot manbasi yoki muallif bilan kelishilgan holda matnni asosli ravishda tuzatishga yo'l qo'yiladi. Ommaviy axborot vositasi raddiya, javobni e'lon qilishdan bosh tortgan yoki e'lon qilishning belgilangan muddatini buzgan taqdirda, yuridik yoki jismoniy shaxs da'vo arizasi bilan sudga murojaat qilishga haqli. Ushbu chora-tadbirlar dezinformatsiyaga mutanosib javob berish bo'yicha xalqaro yondashuvlarga mos keladi. Shunga qaramay, amaldagi mexanizm cheklangan va muayyan shaxslarga taalluqli bo'lmagan ijtimoiy ahamiyatga ega bo'lgan dezinformatsiyani rad etishni qamrab olmaydi.

Ommaviy axborot vositalarini soddalashtirilgan tartibda ro'yxatdan o'tkazish talablari media faoliyatining qonuniyligini nazorat qilish va Internet tarmog'ida ommaviy axborotning tarqatilishini nazorat qilish uchun huquqiy asos yaratadi.

Axborotlashtirish to'g'risidagi Qonunchilik

Umuman olganda, O'zbekistonning axborotlashtirish va axborot xavfsizligi sohasidagi qonunchiligi mamlakat axborot makonini himoya qilishga qaratilgan. Shunga qaramay, raqamli kontent moderatsiyasining shaffofligi va hisobdorligi bo'yicha xalqaro tamoyillarni aks ettiruvchi keng qamrovli tartibga solish mavjud emas. Internet tarmog'ida axborotni tarqatishni cheklashning mavjud tizimi ma'muriy organning axborotni monitoring qilish va baholash hamda axborotni o'chirish to'g'risida xabarnoma berish bo'yicha keng vakolatlarini nazarda tutadi.

"O'zbekiston Respublikasi qonunchiligi bilan tarqatilishi taqiqlangan axborotni o'z ichiga olgan Internet jahon axborot tarmog'idagi veb-saytlarga va (yoki) veb-sayt sahifalariga kirishni cheklash tartibi to'g'risida"gi nizom raqamli muhitda axborot tarqatishni cheklash tartibini nazarda tutadi. Foydalanishni cheklash tartib-taomili idoralararo tartib-taomil bo'lib, unda O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi huzuridagi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo'yicha inspeksiya (keyingi o'rinlarda "O'zkomnazorat" deb ataladi) ishtirok etadi.

Axborotning qonunga xilof xususiyatini baholashda O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonunining 12¹-moddasiga amal qilish zarur. O'zkomnazorat amaldagi qonunchilikka muvofiq noqonuniy deb topilgan, quyidagi maqsadlarda tarqatilayotgan axborotni aniqlash bo'yicha kompleks monitoring olib boradi:

- O'zbekiston Respublikasining mavjud konstitutsiyaviy tuzumini, hududiy yaxlitligini zo'rlik bilan o'zgartirishga da'vat etish;
- Ommaviy tartibsizliklarga, fuqarolarga nisbatan zo'ravonlikka, shuningdek, belgilangan tartibni buzgan holda o'tkaziladigan yig'ilishlar, mitinglar, ko'cha yurishlari va namoyishlarda ishtirok etishga da'vat etish, xuddi shuningdek, ushbu g'ayriqonuniy harakatlarni muvofiqlashtirish;
- jamoat tartibi yoki xavfsizligiga tahdid soluvchi bila turib yolg'on ma'lumotlarni tarqatish;
- Urush, zo'ravonlik va terrorizmni, shuningdek, diniy ekstremizm, separatizm va fundamentalizm g'oyalarini targ'ib qilish;
- davlat sirlarini yoki qonun bilan qo'riqlanadigan boshqa sirni tashkil etuvchi ma'lumotlarni oshkor etish;
- milliy, irqiy, etnik yoki diniy adovatni qo'zg'atuvchi, shuningdek fuqarolarning sha'ni va qadr-qimmatini yoki ishchanlik obro'sini to'kadigan, ularning shaxsiy hayotiga aralashishga imkon beruvchi axborotni tarqatish;
- axborotni tarqatish, shu jumladan jamiyatga, davlatga, davlat ramzlariga hurmatsizlik ko'rsatuvchi odobsiz shaklda ifodalangan axborotni tarqatish;
- giyohvandlik vositalari, psixotrop moddalar va prekursorlarni targ'ib qilish;
- Pornografiya, zo'ravonlik va shafqatsizlikka sig'inish, shuningdek o'z joniga qasd qilishga undashni targ'ib qilish;
- boshqa shaxslarga tegishli bo'lgan intellektual mulk obyektlaridan qonunga xilof ravishda foydalanish;
- fuqarolarni, shu jumladan voyaga yetmaganlarni o'z hayoti va (yoki) sog'lig'i yoxud boshqa shaxslarning hayoti va (yoki) sog'lig'i uchun xavf tug'diradigan qonunga xilof harakatlar sodir etishga undash yoki boshqacha tarzda jalb etishga qaratilgan axborotni tarqatish.

Monitoring natijalariga ko'ra, "O'zkomnazorat" veb-sayt yoki veb-sayt sahifasi egasiga 24 soat ichida noqonuniy kontentni olib tashlash to'g'risida talabnoma yuboradi. Internet OAV yoki veb-sayt egasi noqonuniy deb topilgan materialni olib tashlashga yoxud "O'zkomnazorat"ning xulosasi va Ekspert komissiyasining saytda qonun hujjatlarida taqiqlangan axborot mavjudligi to'g'risidagi qarori ustidan sud tartibida shikoyat qilishga haqli.

"O'zkomnazorat" tomonidan noqonuniy deb topilgan axborotni o'chirishni rad etish O'zbekiston Respublikasi hududida Internet tarmog'ining tegishli axborot resursiga foydalanuvchilarning kirishini to'xtatishga qaratilgan tashkiliy va dasturiy-texnik choralar majmui uchun asos bo'ladi. Internet tarmog'i axborot resurslaridan foydalanishni cheklash tartibi quyidagi tartibda amalga oshiriladi:



Taqiqlangan axborotni o'z ichiga olgan Internet tarmog'ining axborot resurslarini aniqlash.



Taqiqlangan axborotni o'z ichiga olgan Internet tarmog'ining axborot resursining identifikatsiya ma'lumotlarini Reestrda kiritish.



Internet tarmog'ining axborot resursiga kirishni cheklash.

Noqonuniy axborotni aniqlash bo'yicha yetarlicha keng vakolatlar ega bo'lishiga qaramay, "O'zkomnazorat" media va axborot resurslari sohasida huquqni qo'llash amaliyoti bo'yicha statistika va hisobotlarni e'lon qilmaydi. Kirish cheklangan veb-saytlar ro'yxati (Internet jahon axborot tarmog'ining axborot resurslari reyestri) cheklash sabablari va asoslari ko'rsatilgan holda faqat vakolatli davlat hokimiyati va boshqaruvi organlari, shuningdek, yuridik va jismoniy shaxslar tomonidan ularga tegishli bo'lgan Internet tarmog'idagi axborot resurslari to'g'risidagi so'rovlar asosida taqdim etilishi mumkin, bu esa xalqaro standartlarga ziddir.

Qonunchilikda nazarda tutilgan shikoyat qilish mexanizmlari O'zkomnazoratning axborotni noqonuniy deb topish bo'yicha harakatlari ustidan sudga shikoyat qilish uchun umumiy huquq beradi. Vaholanki, xalqaro standartlar Internet tarmog'idagi axborot resurslaridan foydalanishni cheklash ustidan shikoyat qilishning mustaqil sudgacha bo'lgan apellyatsiya mexanizmini yaratishni talab qiladi.

Xalqaro standartlar	O'zbekiston qonunchiligi	Izoh
Shaffoflik va hisobdorlik	Regulyator va raqamli platformalarga moderatsiya qoidalarini oshkor qilish va kontentni cheklash to'g'risidagi hisobotlarni e'lon qilish talablari mavjud emas.	Ijtimoiy tarmoqlar/platformalar uchun kontentni olib tashlash sabablarini tushuntirish majburiyati yo'q. O'zkomnazoratning kontentni cheklash to'g'risidagi hisobotlarni e'lon qilish majburiyati yo'q, Reyestrda foydalanish cheklangan.
Jarayonlar	Kontentni cheklash sud qarorisiz yakka tartibdagi ma'muriy qaror orqali amalga oshiriladi.	Kontentga kirishni cheklash bo'yicha qaror qabul qilishning muvozanatli mexanizmi mavjud emas
Shikoyat qilish huquqi	Veb-saytlarga kirishni cheklash ustidan faqat sud tartibida, agar axborotni o'chirish talabi bajarilgan bo'lsa, shikoyat qilinishi mumkin.	"O'zkomnazorat" monitoringi yoki Ekspert komissiyasi qarori asosida axborotni cheklash ustidan sudgacha shikoyat qilish choralari mavjud emas.
Fuqarolik jamiyatining ishtiroki	Mustaqil, nodavlat subyektni (OAV, ekspertlar, NNT) tashkil etish va uning faoliyat yuritishi nazarda tutilmagan.	Kontentni cheklash bo'yicha qarorlarni baholash va qabul qilishda fuqarolik jamiyatini jalb qilish mexanizmlari mavjud emas.

BMT Inson huquqlari qo'mitasining 34-umumiy sharhida belgilangan yondashuvga muvofiq, so'z erkinligi asosiy huquq bo'lib, u kommunikatsiyaning barcha shakllarini, jumladan, internet, jurnalistlar va blogerlar faoliyatini qamrab oladi. Har qanday cheklovlarga faqat qonuniylik, qonuniy maqsad va zaruriyat tamoyillariga qat'iy rioya qilinganda yo'l qo'yiladi.

Internet-OAV va axborotdan foydalanuvchilar zimmasiga axborotni doimiy monitoring va filtratsiya qilish majburiyatining yuklatilishi ularga senzura vazifasini yuklaydi. Bu orqali davlat so'z erkinligiga haddan tashqari aralashish xavfini yuzaga keltiradi va "sovutish effekti" deb ataluvchi holatga olib keladi, bunda foydalanuvchilar va jurnalistlar qonuniy, biroq bahsli bo'lishi mumkin bo'lgan kontentni e'lon qilishdan tiyila boshlaydi. Amaliyot shuni ko'rsatadiki, bunday majburiyatlar, ayniqsa, sanksiyalar xavfi mavjud sharoitda, ko'pincha kontentning, jumladan, qonuniy nashrlarning ham ortiqcha o'chirilishiga sabab bo'ladi. Shu munosabat bilan, monitoring va filtratsiyaga oid har qanday talablar faqat noqonuniy kontentning aniq belgilangan toifalariga nisbatan qo'llanilishi, shaffof tartib-taomillar va shikoyat qilishning samarali mexanizmlari bilan ta'minlanishi hamda OAV va blogerlarning erkin ijtimoiy muloqot ishtirokchisi sifatidagi fundamental rolini cheklamasligi lozim.

2-bo'lim

Media va jurnalistlarning raqamli huquqlari

2.1. Raqamli muhitda kontent yaratish va tarqatish

Internet global miqyosda tarqalgach, media muhit tubdan emas, balki sezilarli darajada o'zgarishi ayon bo'ldi. Mediakontent analog holatdan chiqib, raqamli ko'rinishga o'tadi; OAV tahririyatlari an'anaviy bo'lishdan to'xtab, konvergentga aylanadi. Auditoriya esa turli mavzudagi ulkan hajmdagi kontentdan foydalanish imkoniyatiga ega bo'ladi, uni istalgan vaqtda, turli qurilmalar orqali "iste'mol qilish", ya'ni ko'rish, tinglash va o'rganish mumkin bo'ladi. OAV oldida konvergent bo'lish, eng yaxshi mediakontent yaratish, uni tarqatishning boshqa kanallariga o'tish va auditoriya jalb qilinishini kuchaytirishdan o'zga chora qolmadi.

Raqamli muhit axborot yaratish va tarqatish jarayonini keskin tezlashtirganiga qaramay, nashr bir lahzada, ko'p kanalli va "jonli" (yangi ma'lumotlar kelib tushgani sayin yangilanib boradigan) bo'lishi mumkin. Shu bilan birga, fundamental huquq va kafolatlar o'zgarishsiz qoladi: fikr bildirish erkinligi hamda axborotni izlash, olish va tarqatish huquqi O'zbekiston Konstitutsiyasi bilan kafolatlangan, cheklovlarga esa faqat qonunda belgilangan asoslar va tartibda yo'l qo'yiladi. Endilikda bu kafolatlar nafaqat OAV uchun, balki barcha fuqarolar uchun raqamli muhitda tatbiq etilishi va huquqlar ta'minlanishi lozim.

Mediabiznes raqamli muhitga moslashgan ekan, kontent ham uning asosiy tamoyillariga javob berishi shart: klikka undovchanlik, muntazamlilik, vizuallashtirish, turli platformalarga moslashuvchanlik, monetizatsiya va auditoriyani jalb qilish. Bu tamoyillarga rioya qilish mediabiznesning daromadlilikini ta'minlaydi va mediakontent yaratuvchilar doirasi kengayishiga olib keladi. Biroq, bu jurnalistlar, blogerlar va mediakontent yaratuvchilar uchun huquqiy xatarlarni bir necha barobarga oshiradi. Quyida raqamli muhitdagi mediakontentning asosiy xususiyatlari, huquqiy xatarlar va ulardan qanday saqlanish haqida so'z yuritamiz.

2.1.1. Sarlavhaning bosilish ehtimoli (klikabel'ligi)"

Onlayn-mediya auditoriya e'tiborini jalb qilish uchun raqobat an'anaviy formatlarga qaraganda yuqoriroq bo'ladi. Sarlavha, yetakchi ma'lumot, video muqovasi, ijtimoiy tarmoqlar yoki messengerlardagi kartochka ko'pincha materialning ochilishiga ta'sir qiladi. Shuning uchun ko'pincha yangiliklar va nashrlarning yorqin, hayratlanarli sarlavhalarini ko'ramiz. Mediakontentni targ'ib qilishning yana bir muammosi — bu qidiruv tizimlaridagi so'rovlarga yo'naltirilganlikdir. Shundan kelib chiqib, quyidagi jadvalda keltirilgan bir nechta huquqiy xavflar yuzaga keladi.

Raqamli mediakontent tavsifi	Bu nimani anglatadi?	Nima uchun bu muammo hisoblanadi?	Mediakontent ishlab chiqaruvchilari uchun xavflarni qanday kamaytirish mumkin?
Klikbeyt (Clickbait)	Yorqin, ko'zga tashlanadigan sarlavha	Ko'pincha bunday sarlavha nashr matniga mos kelmasligi mumkin. Auditoriya va regulyatorda savollar tug'dirishi mumkin. Huquqiy (da'volar, shikoyatlar, arizalar) oqibatlariga va obro' yo'qotishlariga olib kelishi	Sarlavha nashr matniga to'liq mos bo'lishi kerak — uni mubolag'a qilmaslik yoki kamaytirmaslik lozim. Sarlavhani haqiqiy mazmun bilan solishtiring, dalilsiz qat'iy bayonotlar qilishdan saqlaning.
Qidiruv tizimlaridagi so'rovlarga yo'naltirish	Foydalanuvchi nashr yoki yangilik matniga "bosishi" uchun sarlavhani qidiruv so'rovlariga moslashtirish.	Bu holda matnlar sarlavhadan keskin farq qilishi mumkin, yolg'on ma'lumot tarqatishda ayblanish xavfi ortadi.	Qidiruv tizimlaridagi yetakchi so'rovlarga asosanib, sarlavhalarni postlarga moslashtirish g'oyasidan voz keching. Nashr matni va sarlavha bir-biriga aniq mos kelishi kerak. Nashrdagi barcha faktlar ishonchli bo'lishi yoki nashrning birlamchi manbasiga ega bo'lishi kerak.

2.1.2. Onlayn kontentning muntazamligi

Onlayn media uchun kontentni muntazam ravishda yangilab turish media bozorida omon qolish strategiyasining asosiy qismidir. Mediakontentni iste'mol qilish ijtimoiy tarmoqlar, messenjerlar va internet resurslari tomon siljiydi, yangiliklar, tahliliy va ko'ngilochar resurslar, saytlarni ko'rish chastotasi ortadi. Reklama beruvchilarning byudjetlari ham o'sha yerga yo'naltiriladi. Bu yopiq doira hosil qiladi: auditoriya ijtimoiy tarmoqlar, messenjerlar va saytlardagi kontentni qanchalik ko'p iste'mol qilsa, tahririyatlar auditoriya e'tiborini ushlab turish va algoritmik uzatishdan chetda qolmaslik uchun muntazam ravishda kontent ishlab chiqarishga shunchalik ko'p bog'liq bo'ladi. Onlayn platformalar (ijtimoiy tarmoqlar) va qidiruv tizimlari algoritmlari postlarning barqaror oqimini va "faollik signallari"ni — bosishlar, izohlar, ko'rish vaqti, foydalanuvchilarning qaytishini rag'batlantiradi. Natijada, tahririyat ko'zga tashlanib turish uchun tez-tez va ko'proq kontent chop etishga majbur bo'ladi, ko'zga tashlanib turish esa o'z navbatida reklama daromadlarini saqlab qolish va tijorat barqarorligini ta'minlash shartiga aylanadi.

Agar hamroh muammolar bo'lmaganida, bu sxemada hamma narsa a'lo darajada bo'lardi: ko'p miqdordagi kontentni doimiy ravishda yangilab turish talabi tekshirilmagan ma'lumotlar, noaniq iboralar, odamlarni noto'g'ri aniqlash, iqtiboslar va kontekstni buzib ko'rsatish xavfini oshiradi.

Shu bilan birga, raqamli muhitda har qanday xato an'anaviy ommaviy axborot vositalariga qaraganda tezroq kengayadi: material darhol chop etiladi, boshqa sahifalar va kanallar tomonidan nusxalanadi, skrinshot va "kesmalar," memlarga aylanadi, tuzatishlar va aniqliklar esa dastlabki xabarga qaraganda ancha yomonroq tarqaladi. Shu sababli, onlayn ommaviy axborot vositalari uchun yangilanishlarning muntazamligi bir vaqtning o'zida ham o'sish mexanizmi, ham yuqori huquqiy va obro' xavflari manbaiga aylanadi. Bunga qanday erishish mumkinligini tushunish uchun quyidagi jadvalga qarang.

Raqamli mediakontent tavsifi	Bu nimani anglatadi?	Nima uchun bu muammo hisoblanadi?	Mediakontent ishlab chiqaruvchilari uchun xavflarni qanday kamaytirish mumkin?
Yangilanishning muntazamligi	Yangiliklar dasturida, iqtiboslarning yuqori qismida ishtirok etish uchun kontentni tez-tez yangilab turish zarurati.	Faktlar va faktik ma'lumotlarni tekshirish sifati pasayadi. Xatolar repostlar orqali tez tarqaladi.	Minimal qayta tekshiruvsiz materialni nashr etmaslik — nima aniq ma'lum; qanday manba; ikkinchi manba bilan tasdiqlash mumkinmi; ikkinchi tomonning pozitsiyasi bormi (agar o'rinli bo'lsa). Markirovkadan foydalanish — "yangilangan," vaqt, aynan nima o'zgargan.
Katta hajmdagi kontent ishlab chiqarish	Bir kunda ko'p miqdorda material ishlab chiqarish zarurati.	Yuzaki tekshirish va noto'g'ri ma'lumotlarni e'lon qilish xavfi. Xato yoki noaniqlik bir vaqtning o'zida bir nechta platformalarga — veb-sayt, ijtimoiy tarmoqlar, messengerlardagi kanallarga tarqaladi.	Nashr etilayotgan kontentni tekshirishning turli algoritmlari mavjud — yangiliklar uchun (minimal), o'z tahririyat kontenti uchun (qat'iyroq) va foydalanuvchi kontenti uchun, jumladan ijtimoiy tarmoqlardagi kontent uchun (mualliflik huquqiga e'tibor qaratish).

2.1.3. Onlayn kontentni vizuallashtirish

Raqamli media kontent yuqori darajadagi vizualizatsiyani talab qiladi. Nega? Chunki raqamli muhitda foydalanuvchilar tasmani tez ko'rib chiqadilar va darhol e'tiborni tortadigan, ma'no yetkazadigan va qiziqishni ushlab turadigan vizual elementlarga yaxshiroq munosabat bildiradilar. Buning uchun fotosuratlar, infografikalar, skrinshotlar, qisqa videolar kerak bo'ladi. Bu yerda quyidagi jadvalda keltirilgan ikkita asosiy xavf mavjud.

Raqamli mediakontent tavsifi	Bu nimani anglatadi?	Nima uchun bu muammo hisoblanadi?	Mediakontent ishlab chiqaruvchilari uchun xavflarni qanday kamaytirish mumkin?
Muallif yoki mualliflik huquqi egasining ruxsatisiz boshqalarning suratlari, videolari, musiqasi, audiosi, matni, rasmlarini vizuallashtirish uchun foydalanish.	Mualliflik huquqini, O'zbekiston Respublikasining "Mualliflik huquqi va turdosh huquqlar to'g'risida"gi Qonuni talablarini buzish.	Ijtimoiy tarmoq platformalarida kontentni o'chirish, hisoblarni bloklash va cheklash xavfi. Mualliflar va mualliflik huquqi egalariga ehtimoliy kompensatsiya talablari. Ma'muriy yoki jinoiy javobgarlik.	Faqat o'z kontentingiz, suratlar to'plami yoki ijodkor roziligi bilan olingan materiallardan foydalaning. Bunday rozilikni olganingiz yoki rasm, video, matn va boshqa mualliflik huquqi bilan himoyalangan obyektlardan qonuniy foydalanganingiz haqidagi dalillarni saqlang.
Sun'iy intellekt yordamida vizuallashtirish uchun materiallarni qayta ishlash va yaratish.	Vizual, audio yoki video, rasmlarni yaratish yoki qayta ishlash uchun sun'iy intellektdan foydalanish.	"Begona" manbalardan foydalanish, asl materiallarga bo'lgan huquqlarni buzish, haqiqiy shaxslarning tasviri bilan bog'liq muammolar xavfi.	Boshqalarning foto, video va audiolarini yaratishda foydalanmaslik. O'z promptlarini yaratish. Zarur hollarda sun'iy intellekt yordamida yaratilgan kontentni belgilash.

2.1.4. Turli platformalarga moslashish

Auditoriya bitta kanalga — axborot sayti, muayyan ijtimoiy tarmoq yoki messenjerga “bog‘lanmagan.” Auditoriya bir manbadan ikkinchisiga “ko‘chib yuradi”. Bu degani, kontent hamma joyda mavjud bo‘lishi kerak.

Shuning uchun onlayn media deyarli har doim bir xil materialni bir vaqtning o‘zida bir nechta kanallarda tarqatadi: saytda, ijtimoiy tarmoqlarda, messenjerlarda, video platformalarda. Bu qamrovni oshiradi va auditoriyani saqlab qolishga yordam beradi, ammo shu bilan birga xavf tug‘diradi: bir xil ma’no turli formatlarga (qisqa video, kartochka, hikoya, post) “qayta qadoqlanadi,” kontekst muqarrar ravishda qisqaradi, platformalar talablari va auditoriya kutilmalari esa farq qiladi. Bu, shuningdek, quyidagi jadvalda ko‘rsatilgan ma’lum xavflarni keltirib chiqaradi

Raqamli mediakontent xususiyati	Bu nimani anglatadi?	Nima uchun bu muammo hisoblanadi?	Mediakontent ishlab chiqaruvchilari uchun xavflarni qanday kamaytirish mumkin?
Kontentni turli formatlarga moslashtirish	Ko‘pincha matnni qisqartirish, sarlavha.	Noto‘g‘ri ma’no, qat’iy fikrlar va faktlarni o‘zgartirish xavfi ortadi.	Asl nashrdagi faktlari, ma’nosi va mohiyatini o‘zgartirmang. To‘liq materialga havola qo‘shishni unutmang.
Onlayn platformalar va messenjerlarning turli qoidalari hamda algoritmlari	Har bir ijtimoiy tarmoq yoki messenjerning kontent, mualliflik huquqi bo‘yicha o‘z siyosati bor.	Onlayn platformalar siyosati buzilgan taqdirda, akkauntlar bloklanishi va kontent o‘chirib tashlanishi mumkin.	Kontent joylaydigan kanal va platformalarning barcha siyosatlarini tekshiring va ularga qat’iy rioya qiling.

2.1.5. Kontentni monetizatsiya qilish

Onlayn media monetizatsiyasi odatda reklama, homiylik materiallari, hamkorlikdagi maxsus loyihalar, obunalar va xayriyalar kombinatsiyasiga asoslanadi. Bu yerda asosiy yuridik yo‘nalish — reklama va tahririyat materialini farqlash. O‘zbekistonning “Reklama to‘g‘risida”gi qonunida reklamani taniqli bo‘lishi talabi mustahkamlangan; homiylik va “yashirin reklama”ga (xabarning reklama xususiyati tahririyat kontenti ostida niqoblanganda) yo‘l qo‘yilmasligi alohida tartibga solinadi.

Biroq, amalda haqiqat boshqacha: reklama beruvchilar mahalliy reklama va integratsiyalarning samaradorligiga qattiq ishonishadi va ko‘pincha jurnalist yoki blogerning materiali niqobi ostida reklama matnini yaratishni so‘rashadi. Bloggerlar ko‘pincha xayriya faoliyati niqobi ostida boshqa maqsadlar uchun pul yig‘adilar yoki reklama va integratsiyalardan olingan daromadlarini soliq solinadigan bazaga kiritmaydilar.

Quyidagi xavflarni yodda tutishni tavsiya qilamiz:

Raqamli mediakontent xususiyati	Bu nimani anglatadi?	Nima uchun bu muammo hisoblanadi?	Mediakontent ishlab chiqaruvchilari uchun xavflarni qanday kamaytirish mumkin?
Yashirin reklama	Reklama materiali aniq belgilanmagan holda tahririyat kontenti sifatida taqdim etiladi	Auditoriyani chalg'itadi, javobgarlik hamda obro'ni yo'qotish xavfini keltirib chiqaradi	Reklama va homiylikni doimo markirovka qilish kerak. Pullik kontentni markirovka qilish uchun ichki qoidalar va namunalarni qabul qilish
Bloggerlarning reklama daromadlarini yashirish	Reklama daromadlari qayd etilmaydi, soliqlar to'lanmaydi	Soliq va huquqiy oqibatlar xavfi; reklama beruvchilar bilan nizolar	Har qanday pullik joylashtirishlar uchun shartnomalar tuzish

2.1.6. Auditoriyani jalb qilish

Onlayn media uchun auditoriyani jalb qilish nima uchun shunchalik muhim? Fikrlar, munosabatlar, so'rovnomalar, jonli efirlar va foydalanuvchi kontenti reklama beruvchilarning tarqatilishi va qiziqishiga bevosita ta'sir qiladi. Bu barqaror o'sish va auditoriyaning reklama maydoniga bo'lgan qiziqishini oshiruvchi omil hisoblanadi,

Biroq, jalb qilish deyarli har doim xavflarni oshiradi: muhokamalar tezda haqorat va ta'qibga aylanadi, foydalanuvchilar shaxsiy ma'lumotlarni va tekshirilmagan ayblovlarni, haqoratlarni e'lon qiladilar. Bunday kontekstdagi xato yoki noto'g'ri ta'rif bir zumda kengayadi va ham obro'-e'tiborga, ham huquqiy yo'qotishlarga olib kelishi mumkin.

Ularni quyidagi jadvaldan ko'rib chiqing

Raqamli mediakontent xususiyati	Bu nimani anglatadi?	Nima uchun bu muammo hisoblanadi?	Mediakontent ishlab chiqaruvchilari uchun xavflarni qanday kamaytirish mumkin?
Materiallar ostida sharhlar va munozaralar.	Foydalanuvchilar faol fikr bildirishmoqda, mavzuga qiziqish ortmoqda.	Izohlarning anonimligi. Foydalanuvchilar nafratli nutq, yolg'on ma'lumotlar, haqoratlar, boshqalarning shaxsiy ma'lumotlarini tarqatishi, ma'lumotlarga putur yetkazishi mumkin.	Fikrlarni majburiy moderatsiya qilish. Foydalanuvchilar uchun qoidalar va javob choralari — aniq qoidabuzarliklarni kechiktirmasdan bartaraf etish. Nozik mavzular uchun — oldindan moderatsiya qilish va izohlarni cheklash.
Jonli efirlar va jonli formatlar.	Real vaqtda improvizatsiya qilish, savollarga javob berish.	Faktlarni, ma'lumotlarni tekshirishga vaqt yo'q. Fikrlar va baholar tanqidiy bo'lishi va uchinchi shaxslarning manfaatlariga tegishi mumkin.	Tayyor tezislar va ehtimoliy savollarga javoblar. Agar efir dastlabki ssenariy bo'yicha ketmasa, zaxira variant. Zarur bo'lsa, efirni kechiktirish va ma'lumotlarni tezda aniqlashtirish.
Foydalanuvchi kontenti (UGC)	O'quvchilar, voqea guvohlari va boshqalardan kelgan foto, video, audio va kichik matnlar.	Yolg'on ma'lumotlar, sahnalashtirishlar, uchinchi shaxslarning huquqlarini buzish, shaxsiy ma'lumotlarni tarqatish.	Bunday kontentni faqat minimal tekshiruvdan (qachon va qayerda suratga olingani, muallif kim ekanligi) va muallifning foydalanish uchun roziligini olgandan so'ng qabul qiling. Shaxsiy ma'lumotlarni o'chirib tashlang va zarur bo'lsa, tasvirni egasizlantiring (yuzlar, avtomobil raqamlari va hokazolar uchun blur)

2.1.7. Onlayn medianing professional standartlari

Media kontentni juda ko'p odamlar yaratadi: onlayn media tahririyatlari, media sohasidagi mutaxassislar (alohida media loyihalar — surishtiruvlar va boshqalar), bloggerlar va ijtimoiy tarmoq foydalanuvchilari, GR va PR mutaxassislari, reklama agentliklari, video ishlab chiqarish studiyalari, davlat organlari va xususiy kompaniyalar.

Ma'lumki, raqamli muhit har bir xatoning narxini oshirib yuboradi. Kontent bir zumda tarqaladi, nusxalanadi va qayta yuboriladi, memlar, skrinshotlar va qisqa parchalar shaklida “yashaydi,” auditoriya esa ko'pincha materialni sarlavha, muqova va birinchi xatboshi orqali idrok etadi. Shuning uchun onlayn media nafaqat “tahririyat ichidagi” standartlarga rioya qilishi, balki barcha formatlar — sayt, ijtimoiy tarmoqlar va messenjerlar uchun tushunarli qoidalarni ishlab chiqishi muhimdir.

Onlayn media uchun professional standartlar an'anaviy media uchun bir xil bo'lib qolmoqda. Bular — faktlarni bayon etishda aniqlik va haqqoniylik, muvozanat (nashrda barcha tomonlarni taqdim etish), fikrlarni baholovchi mulohazalardan ajratish, neytral pozitsiya, jurnalistikaning axloqiy tamoyillariga rioya qilish, ayniqsa bolalar, jinoyat qurbonlari va jamiyatning zaif guruhlariga nisbatan. Har bir standart amalda qanday ishlashini tushunish uchun quyidagi jadvalga qarang.

Onlayn media standarti	Professional standart tavsifi	Standart amalda qanday ishlashi kerak?
Faktlarni bayon qilishdagi aniqlik.	OAV (onlayn media) faqat tasdiqlanishi mumkin bo'lgan narsalarni nashr etadi; raqamlar, ismlar, sanalar va iqtiboslar nashr etishdan oldin tekshiriladi.	Nashr qilishdan oldin ismlar, sanalar, raqamlar va iqtiboslarni asl manba bilan solishtiramiz. Barcha tasdiqlovchi hujjatlarni saqlab qo'yamiz.
Faktlarni bayon qilishdagi ishonchlilik.	Faqat ishonchli manbalar va hujjatlarga tayanish zarur. E'lon qilishda faktlar va ishonchli ma'lumotlarni taxminlar, fikrlar va baholovchi mulohazalardan ajratish lozim.	Kamida ikkita mustaqil tasdiqlash yoki hujjat yoki izohlardan foydalanamiz. Agar ma'lumotlar yetarli bo'lmasa, matnda bu versiya yoki dastlabki ma'lumot ekanligini ko'rsatamiz.
Balans (nashrda barcha tomonlarning ifodalanishi).	Onlayn ommaviy axborot vositalari, ayniqsa, ma'lum bir shaxslarning huquqlari va obro'siga ta'sir qiladigan bo'lsa, barcha manfaatdor tomonlarning nuqtai nazarini taqdim etishga intiladi.	Asosiy tomonlardan izoh so'raymiz va so'rovlar yuboramiz. Agar e'lon qilish vaqtigacha javob olinmagan bo'lsa, biz buni albatta materialda ko'rsatamiz va pozitsiya kelib tushishi bilan nashrni yangilaymiz.
Fikrlarning bo'linishi va baholash mulohazalari.	Faktlar va baholar aralashtirilmaydi — faktik ma'lumotlar muallif yoki ekspertlarning talqinlaridan ajratilgan.	Matn yoki videoda “nima sodir bo'ldi” va “bu qanday baholanadi”ni ajratib ko'rsatamiz. Baholash ta'riflarini manbalar bilan mustahkamlaymiz yoki to'g'ridan-to'g'ri fikr yoki sharh sifatida belgilaymiz.
Betaraf pozitsiya	Onlayn-media tomonidan materialning uzatilishi to'g'ri va xolis bo'lishi lozim. Nashr tilida hissiy ayblovlar, stereotiplar va qoliplar bo'lmasligi kerak.	Aniq, huquqiy jihatdan puxta ta'riflardan foydalanamiz va isbotsiz qat'iy xulosalardan qochamiz. Nizoli mavzularda — hissiy sifatlashlarni olib tashlaymiz va faqat ishonchli faktlar va ma'lumotlarni qoldiramiz.
Jurnalistikaning axloqiy tamoyillariga rioya qilish	Onlayn media jamoatchilikni qiziqtirgan mavzularga ustuvorlik beradi. Bunda nafaqat qonunchilik talablariga, balki jurnalistikaning axloqiy tamoyillariga ham amal qilinadi.	Shokka tushiruvchi, kamsituvchi tafsilotlar, suratlar va videolarni joylashtirmaymiz. Biz shov-shuvga intilmaymiz, balki auditoriya uchun sifatli, ishonchli kontent taqdim etishni ta'minlaymiz.

Bolalar, jinoyat qurbonlari va zaif guruhlar nisbatan alohida ehtiyotkorlik choralarini ko'rish.	Bolalar va zaif guruhlar haqidagi materiallar shaxsiy hayot va xavfsizlikni yuqori darajada himoya qilishni talab etadi. Shaxsiy ma'lumotlar va fotosuratlarini tarqatish faqat aniq zarurat va qonuniy asoslarda ruxsat etiladi.	Ortiqcha identifikatsiya ma'lumotlarini (shaxslar, manzillar, raqamlar, shaxsni oson tanib olish mumkin bo'lgan tafsilotlar) olib tashlaymiz. Xavfsizlik xavflarini baholaymiz va zarur bo'lsa, materialni anonimlashtiramiz hamda surat va videolarda xiralashtirishdan foydalanamiz.
--	---	--

2.1.8. O'zbekiston huquqida internet nashrining maqomi

O'zbekistonning amaldagi qonunchiligida veb-sayt ommaviy axborot vositalarining mumkin bo'lgan shakli sifatida bevosita ko'rsatib o'tilgan²⁴. Onlayn nashr esa elektron shakldagi, tahririy-nashriy ishlovidan o'tgan va o'zgarmagan holda tarqatish uchun mo'ljallangan materiallarni o'z ichiga oluvchi axborot resursi hisoblanadi.

Agar veb-sayt OAV sifatida ro'yxatdan o'tkazilgan bo'lsa, bosh sahifada kamida quyidagilar ko'rsatilishi kerak: nomi, davlat ro'yxatidan o'tkazilganligi to'g'risidagi guvohnoma sanasi va raqami, ta'sischisi, bosh muharriri, tahririyat manzillari (pochta va elektron). Qonun bosma nashrning elektron versiyasi mavjud bo'lgan vaziyatni alohida tartibga soladi: u mustaqil OAV sifatida ro'yxatdan o'tmasdan, mazmuni bir xil bo'lgan (reklama va hajm bo'yicha bir qator shartlar bilan) va ro'yxatdan o'tkazuvchi organi xabardor qilgan holda tarqatilishi mumkin.

Raqamli mediakontent ishlab chiqaruvchilar uchun doimiy muammo — ularga OAV maqomi kerakmi yoki yo'qmi, degan savol. Quyida bunday qarorning ijobiy va salbiy tomonlari keltirilgan.



Internet nashrning OAV sifatida ro'yxatdan o'tishining afzalliklari

Tahririyatning rasmiy identifikatsiyasi hamda auditoriya va hamkorlar ishonchini oshirish.

Reklama beruvchilar va agentliklar uchun ro'yxatdan o'tgan OAV bilan ishlash osonroq: shartnoma tomoni, rekvizitlar, mas'ul shaxs sifatida bosh muharrir, yagona joylashtirish qoidalari tushunarliroq.

Akkreditatsiya va rasmiy kommunikatsiyalar amaliyotida tahririyat, muharrir va rasmiy maqomning mavjudligi yozishmalar va tashkiliy masalalarni (masalan, tahririyatdan so'rovlar, akkreditatsiya uchun arizalar berish) osonlashtiradi.



Internet nashrning OAV sifatida ro'yxatdan o'tishining kamchiliklari

To'liq shakllangan tahririyat tashkil etish zarurati

Nashrlar va tahririyat faoliyati ustidan yanada qat'iy monitoring olib borish

Kontentni e'lon qilish bo'yicha keng ko'lamli sanksiyalar (javobgarlik) mavjud: ma'muriy va fuqaroviy huquqiy javobgarlik. Jinoiy sanksiyalar esa tahririyatning mansabdor shaxslariga nisbatan qo'llanilishi mumkin.

2.1.9. Ijtimoiy tarmoqlar va messenjerlardagi onlayn media akkauntlari

Yuqorida biz raqamli mediakontentning asosiy xususiyatlaridan biri uning turli formatlar va tarqatish kanallariga moslashtirilishi ekanini muhokama qilgan edik. Shu sababli har

²⁴ O'zbekiston Respublikasining "Ommaviy axborot vositalari to'g'risida"gi Qonuni. Qonun matni bilan havola orqali tanishish mumkin: <https://www.lex.uz/acts/53112>

bir internet-nashr ijtimoiy tarmoqlar va messenjerlarda o'z akkauntlariga ega bo'ladi, ulardagi obunachilar soni esa ko'pincha saytdagi noyob tashrif buyuruvchilar sonidan ham ko'p bo'ladi. Rasmiy nuqtayi nazardan, internet-nashrning ijtimoiy tarmoqlardagi barcha akkauntlari ham OAV sifatida qaraladi. Shu bois qisqa post, sarlavha, videoga yozilgan izoh va hatto material muqovasi ham saytdagi nashr kabi baholanishi mumkin. Ijtimoiy tarmoqlar va messenjerlardagi akkauntlarda e'lon qilinadigan barcha materiallarga internet-nashr saytida joylashtirilgan mediakontent uchun mavjud bo'lgan xuddi shu xavf va javobgarliklar tatbiq etiladi.

Ehtimoliy muammola



Diffamatsiya (sha'n, qadr-qimmat va ishchanlik obro'siga putur yetkazuvchi noto'g'ri ma'lumotlarni tarqatish)

Post, sarlavha yoki videoga yozilgan izoh tuhmat yoki obro'ga putur yetkazuvchi ma'lumot tarqatish sifatida baholanishi mumkin. Ayniqsa subyektiv baholar, dalilsiz ayblovlar va hissiy ifodalar xavfni oshiradi.



Yolg'on axborot tarqatish

Manbani tekshirmasdan tezkor repost yoki material e'lon qilish ataylab yolg'on yoki ishonchsiz ma'lumotlarning tarqalishiga olib kelishi mumkin. Ayniqsa favqulodda vaziyatlar, texnogen va tabiiy ofatlar, pandemiyalar hamda hodisalar davrida bu juda xavfli hisoblanadi.



Shaxsiy ma'lumotlarni tarqatish

Rasmlar, videolar, yozishmalar skrinshotlari, telefon raqamlari, manzillar, STIR va boshqa identifikatorlarni qonuniy asoslarsiz e'lon qilish inson huquqlarini buzishi mumkin.



Hate speech (nafratga undovchi nutq) va tarqatilishi taqiqlangan kontent."

Izohlar, iqtiboslar va repostlarda nafrat so'zlari, zo'ravonlikka chaqiriqlar yoki boshqa taqiqlangan materiallar bo'lishi mumkin. Buning uchun ijtimoiy tarmoq ham, muayyan tahririyat yoki bloger ham javobgar hisoblanadi.



Mualliflik huquqlarining buzilishi

Boshqalarga tegishli foto, video, musiqa, infografika va memlardan "odatdagidek" foydalanish mumkin emas, hatto ular ochiq manbalarda topilgan bo'lsa ham. Bu da'volar, sud ishlari va huquqiy nizolar uchun asos yaratadi.

2.2. Axborotdan foydalanish va akkreditatsiya

Real voqea. Kichik shahardagi bir nechta maktablarda bolalarning zaharlanish holatlari yuz bermoqda va bu bo'yicha tekshiruv o'tkazilmoqda. Bolalar ovqatini yetkazib bergan ta'minotchini tanlash bir manbadan xarid qilish usuli orqali, ya'ni muqobilsiz tarzda amalga oshirilgan. Shartnoma, summa va majburiyatlarga oid hujjatlar maktab saytida mavjud emas. Ommaviy zaharlanishlardan so'ng shahar OAV tahririyati ta'lim boshqarmasi va maktabdan bolalar ovqatini yetkazib beruvchi ta'minotchiga oid hujjatlar hamda sanitariya-epidemiologiya xizmati tekshiruvi natijalarini so'raydi. Biroq ularga

hujjatlarni taqdim etish rad etiladi. Sabab sifatida tijorat siri va shaxsiy ma'lumotlarning mavjudligi ko'rsatiladi.

Yuqoridagi misol shuni ko'rsatadiki, qonunchilik talablari va jamoatchilik manfaati mavjudligiga qaramay, jurnalistlar va ommaviy axborot vositalari uchun davlat organlaridan ma'lumot so'rash, olish, uni auditoriyaga yetkazish va voqealar mohiyatini tushuntirish hali ham oson emas.

Axborot olish imkoniyatini davlatdan axborot ulashishni so'rash sifatida ko'rib chiqish mumkin emas, bu — so'z erkinligi elementi va jurnalistning professional qurolidir. U davlat chegaralaridan qat'i nazar, har qanday turdagi axborot va g'oyalarni izlash, olish va tarqatish huquqini o'z ichiga oladi. Amaliy ma'noda bu shuni anglatadiki, tahririyat va muallif davlat organlari va tashkilotlari ixtiyorida bo'lgan ma'lumotlar, hujjatlar va yozuvlarni so'rash hamda olish, shuningdek, bunday ma'lumotlarning ijtimoiy ahamiyatini asoslash huquqiga ega.

Shu bilan birga, mintaqaviy amaliyot shuni ko'rsatadiki, huquq rasman tan olinadi, ammo amalga oshirilishi qiyin: Global Right to Information Rating reytingida O'zbekiston 140 ta mamlakat orasida 129-o'rinni egalladi. To'g'ri, bu past ko'rsatkich. U ochiqlik, so'rovlarga javob berish muddatlariga rioya qilmaslik, javoblarning past sifati va deyarli ishlamaydigan shikoyat mexanizmlari bilan bog'liq doimiy muammolarni aks ettiradi.

2.2.1. Axborot va hujjatlarni qidirish uchun ochiq ma'lumotlar bazalari, reyestrlar va axborot tizimlariga kirish

Xalqaro huquqda axborotdan foydalanish erkinligining bir qismi sifatida qaraladi: huquq e'lon qilish bilan cheklanmaydi — u axborot olishdan boshlanadi.

1. **Davlat organlarining ma'lumotlaridan foydalanish.** Birinchi navbatda, ommaviy masalalarga oid materiallar, ma'lumotlar va hujjatlar: qarorlar, hisobotlar, reyestrlar, bayonnomalar, statistika, xaridlar, byudjetlar, tekshiruvlar natijalari mavjud bo'lishi kerak. Bu OAVning ijtimoiy ahamiyatga molik mavzular bo'yicha axborot olish huquqini ham, jamiyatning tekshirilgan hujjatlar asosida sifatli media kontent olish huquqini ham o'z ichiga oladi.
2. **O'zi haqidagi shaxsiy ma'lumotlardan foydalanish huquqi.** Har bir inson avtomatlashtirilgan bazalarda o'zi to'g'risida ma'lumotlar bor-yo'qligini, ular aynan qanday, kim tomonidan va qanday maqsadda to'planishi hamda saqlanishini bilish huquqiga ega. Jurnalist uchun bu kamida ikki vaziyatda muhim:
 - Tahririyat shaxsiy ma'lumotlarga ishlov berishning qonuniyligini tekshirganda (masalan, ma'lumotlar sizib chiqqanda);
 - Tahririyat jamoatchilik manfaatini shaxsiy hayotga aralashuvdan to'g'ri ajratishi kerak.
3. **Jamoatchilik manfaati — ma'lumotlarni oshkor qilishning asosiy omili sifatida.** So'rovlar o'z vaqtida, tushunarli tartibda ko'rib chiqilishi, ishlov berish uchun to'lov esa asossiz to'siqlar yaratmasligi kerak. Har qanday rad etish asoslantirilgan bo'lishi shart: davlat organi aynan nima uchun kirish cheklanganligini, qanday huquqiy asosga ko'ra va nima uchun cheklash zarurligini tushuntirishi lozim.

Albatta, ideal holatda axborot OAV, fuqarolik jamiyati va fuqarolarga birinchi talabda taqdim etilishini istaymiz. Ammo cheklovlar bor, bo'lgan va bo'ladi — bu real holat. Cheklovlar faqat qat'iy asoslangan hollarda maqbul bo'lishi mumkin. Bunga quyidagilar kiradi: xavfsizlik va mudofaa, xalqaro munosabatlar, jamoat xavfsizligi, jinoyatlarni tergov qilish, shaxsiy hayotni himoya qilish, tijorat manfaatlari, iqtisodiy va valyuta siyosati, adolat manfaatlari, atrof-muhitni muhofaza qilish, ichki muhokamalarning maxfiyligi.

Ammo **mavzuning o'zi** cheklovning qonuniyligini isbotlamaydi. Kasbiy faoliyatingizda axborotdan foydalanishni cheklashga bo'lgan har qanday urinishga nisbatan uchta savolni bering:

1. Qonunda to'g'ridan to'g'ri asos bormi?
2. Axborotning aynan shu qismi yopiq bo'lishi shartmi?
3. Hujjatni butunlay yopmasdan, qisman ochish (sezgir qismlarini olib tashlash) mumkinmi?

Jurnalistlar va bloggerlar uchun axborotning bir nechta yirik toifalarini (hujjatlar, ma'lumotlar) farqlash foydali bo'lib, ularga kirish butunlay yopilishi yoki vaqtincha cheklanishi mumkin.

Axborot toifalari



Davlat sirlari

Hujjatlarning eng murakkab va yopiq toifasi sanaladi, biroq bu yerda ham cheklovlarning vaqtinchalik ekani va qat'iy qonuniylikka asoslanishi tamoyili amal qiladi. Davlat sirlaridan faqat cheklangan doiradagi shaxslargina xabardor bo'lishi mumkin. Jurnalistlar bu doiraga kirmaydi.



Vaqtincha cheklanishi mumkin bo'lgan axborot

Bu eng keng va amaliyotda eng ko'p bahsli toifa. Cheklovlar aniq, proportsional va asoslangan bo'lishi kerak. Ammo amaliyotda vaqtinchalik cheklovlar ko'pincha doimiy cheklovga aylanadi. Ko'pincha hujjatning faqat zarur qismi emas, butun hujjat yopiladi.



Maxfiylashtirilmaydigan yoki cheklanmaydigan axborot

Bu ma'lumotlar qonunga ko'ra ochiq bo'lishi kerak, chunki ular davlat organlari faoliyatining shaffofligi va davlat mablag'larining sarflanishi (byudjetlar, xaridlar, qarorlar, hisobotlar, tekshiruvlar natijalari va ijtimoiy ahamiyatga molik masalalar bo'yicha statistika) bilan bevosita bog'liq.



Huquqiy sirlar (shaxsiy hayot, tijorat siri va boshqalar)

Ushbu rejimlar ijtimoiy ahamiyatga ega ma'lumotlarga bo'lgan huquqni bekor qilmaydi, lekin yanada sinchkov tahririyat tekshiruvini va shaxsiy hayotga aralashuvni kamaytirishni talab qiladi.

Markaziy Osiyoning barcha mamlakatlari kabi O'zbekiston ham davlat boshqaruvida raqamlashtirishni muvaffaqiyatli joriy etmoqda. Bu shuni anglatadiki, jamoatchilik nazorati endilikda davlat idoralariga so'rov yuborish bilan emas, balki ko'pincha ochiq raqamli manbalarni o'rganishdan boshlanadi. Bu faktche king sifatini tubdan o'zgartiradi: avvaliga asosiy faktlarni (me'yoriy-huquqiy baza, mahalliy hokimiyat qarorlari, xaridlar to'g'risidagi ma'lumotlar, statistika) tezda aniqlab olish, shundan so'ng zarur hujjatni

taqdim etishni talab qilib, aniq so'rovlar yuborish mumkin bo'ladi. Bunday yondashuv "mavhum va umumiy javob" olish xavfini kamaytiradi va so'rov yuboruvchining mavqeyini mustahkamlaydi. Chunki davlat idorasi tahririyatning hujjatlardan xabardorligini va "umuman olib" emas, balki aniq masala yuzasidan murojaat qilayotganini ko'radi.

Axborot olish uchun manbalar ro'yxati

Resurs nomi	Havola	Tavsif
Qonunchilikning me'yoriy bazasi Lex.UZ	https://lex.uz/en/	Amaldagi qonunlar, qonunosti hujjatlari va rasmiy matnlarni tez topish mumkin bo'lgan milliy qonunchilik bazasi LexUZ (LEX.UZ)
E-Qaror	https://cabinet-eqaror.gov.uz/ru/auth/login	Mahalliy davlat hokimiyati organlari tomonidan qabul qilinadigan qarorlarni ishlab chiqish, kelishish va ro'yxatdan o'tkazishning yagona elektron tizimi
Open Data Portal of the Republic of Uzbekistan	https://data.egov.uz/eng?utm_source=chatgpt.com	O'zbekiston davlat organlarining ochiq ma'lumotlar portali. Ma'lumotlarning ko'pligi, shu jumladan mashina o'qiy oladigan format.
Davlat xaridlari portali	https://xarid.uzex.uz/home	UzEx platformasidagi davlat xaridlari elektron tizimi (xarid.uzex.uz va tegishli xizmatlar) e'lonlar, xarid jarayonlari va asosiy ma'lumotlarni topish imkonini beradi.
Sud hujjatlari bazasi	https://publication.sud.uz/ — !/sign/view	O'zbekiston Respublikasi sudlari tomonidan chiqarilgan va qonuniy kuchga kirgan sud hujjatlari.
Milliy statistika portali	https://stat.uz/ru/47-ofitsialnaya-statistika	O'zbekiston iqtisodiyoti, aholisi va boshqa sohalar bo'yicha statistik ma'lumotlar.
O'zbekiston Respublikasi Prezidentining Virtual qabulxonasi	https://pm.gov.uz/ru/#/	Davlat rahbariga keng ko'lamli ichki va tashqi siyosat masalalari bo'yicha murojaatlar yuborish xizmati
O'zbekistondagi kompaniyalar reyestri	https://orginfo.uz/	Yuridik shaxslarning holati va faoliyati to'g'risidagi ma'lumotlar portali

2.2.2. Verifikatsiya va faktcheking

Ko'pincha jurnalistlar davlat organidan o'z so'roviga javob olingan bo'lsa, uni tasdiqlash yoki tekshirish shart emas deb o'ylashadi. Darhaqiqat, biror voqea yoki tadbir haqida xabar berganimizda, ko'pincha OAV tahririyatining so'roviga davlat organining javobini keltirish kifoya qiladi. Shunday qilib, muvozanatga erishiladi — nashrda manfaatdor tomonlarning barcha nuqtai nazarlari aks ettiriladi.

Ammo agar gap byudjet mablag'lari hisobidan amalga oshiriladigan tekshiruvlar, davlat xaridlari, loyihalar va hokazolar haqida ketsa, davlat organlarining javoblari va boshqa har qanday faktik ma'lumotlar **tekshirilishi, verifikatsiya qilinishi yoki faktcheking qilinishi lozim**.

O'zbekistonda yolg'on axborot tarqatish uchun ham ma'muriy, ham jinoiy javobgarlik belgilanganligini hisobga olsak, faktcheking jurnalistikaning asosiy tamoyiliga aylanadi. Quyidagi jadvalda ma'lumotlar, hujjatlar, jumladan, davlat organlaridan olingan ma'lumotlarni tekshirishning asosiy bosqichlari keltirilgan.

Hujjatlar, javoblar va ma'lumotlarni verifikatsiya qilish bo'yicha harakatlar (bosqichlar)

1-bosqich.

Tasdiqlash va kerakli hujjatni qayd etish

Bitta tekshirilishi mumkin bo'lgan faktni (summa, sana, yetkazib beruvchi, "bir manbadan olingan", tekshirish natijasi) shakllantiring va u qaysi hujjat yoki reyestr bilan tasdiqlanishini aniqlang.

Natija: Nimani tekshirish va nimani izlash kerakligi aniq



2-bosqich.

Birlamchi manba va hujjatni topish

Ko'pincha jurnalistlar mansabdor shaxsning/ amaldorning izohi yoki javobini yetarli deb hisoblaydilar. Ammo bu birlamchi manba emas. Hujjat bilan tasdiqlangan axborotni, ya'ni birlamchi manbani izlang.

Natija: Davlat xizmatchilarining fikri yoki mulohazasiga emas, balki hujjatga tayaniladi



3-bosqich.

Tasdiqlash uchun muqobil manbani izlash va o'rganish

Har bir faktni o'zaro bog'liq bo'lmagan uchta axborot manbasida tasdiqlash maqsadga muvofiqdir.

Natija: Yolg'on ma'lumot tarqatishda ayblanish xavfi kamayadi



4-bosqich.

Hujjatdagi faktik ma'lumotlarni tekshirish

Hujjat rekvizitlarini solishtiring: raqami, sanasi, organ/tashkilot nomi, predmeti, summasi, muddatlari, hujjatni imzolagan shaxsning F.I.Sh. va lavozimi.

Natija: Xatolar va "to'liq bo'lmagan" hujjatlar istisno qilinadi. Shikoyat va ayblovlar xavfi kamayadi.



2.2.3. Akkreditatsiya

Akkreditatsiya jurnalistlar uchun axborotga tezkorroq kirish vositasi sifatida hozir amaliyotda deyarli qo'llanilmaydi, davlat rahbari, vazirlar va boshqa yuqori martabali mansabdorlar ishtirokidagi tadbirlar uchun vaqtinchalik akkreditatsiya holatlari bundan mustasno. Bir tomondan, davlat organlari faoliyatiga raqamlashtirish va sun'iy intellekt joriy etilishi axborotga yanada tezkor kirishning yangi mexanizmlarini yaratishga imkon bermoqda — kollegial organlarning ochiq yig'ilishlarini videotranslyatsiya qilish, bayonnomalar va qabul qilingan qarorlar, hujjatlar bilan onlayn rejimda, davlat organlari va boshqa axborot egalari saytlarida foydalanish imkonini beradi.

O'zbekistonda akkreditatsiya qonunchilikda jurnalistning muayyan davlat organi yoki tashkilot faoliyatiga "muntazam kirish" usuli sifatida rasman mustahkamlangan. "Jurnalistning kasbiy faoliyatini himoya qilish to'g'risida"gi Qonunda²⁵ jurnalist davlat organi, jamoat birlashmasi yoki tashkilot huzurida akkreditatsiyadan o'tishi mumkinligi bevosita nazarda tutilgan. Akkreditatsiyadan o'tgan jurnalist esa quyidagi aniq huquqlarga ega bo'ladi:



Ochiq kollegial yig'ilishlar va ommaviy tadbirlar haqida oldindan axborot olish.



Akkreditatsiya qiluvchi organning binolariga u belgilagan tartib asosida kirish va ochiq yig'ilishlarda qatnashish.



Hujjatlar va materiallarni so'rash hamda olish.



Ommaviy tadbirlar yozuvlari bilan tanishish.



Material tayyorlashda nusxa olish va yozuvlardan foydalanish.

²⁵ Batafsil ma'lumotni quyidagi havola orqali olishingiz mumkin: <https://lex.uz/docs/2024>

Bundan tashqari, O'zbekiston Respublikasining "Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqqligi to'g'risida"gi Qonuni²⁶ ham amal qiladi. Unga ko'ra, ochiq kollegial yig'ilishlar oshkora o'tkazilishi kerak va davlat organi axborot foydalanuvchilarining ishtiroki uchun sharoit yaratishi shart. Biroq aniq tartib (kirish qoidalar, ro'yxatdan o'tish, kvotalar, xavfsizlik talablari) ushbu organning ichki hujjatlari bilan belgilanadi²⁷.

Aynan shu yerda amaliy muammo yuzaga keladi: qonun darajasida majburiyatlar belgilangan bo'lsa ham, akkreditatsiya har doim ham kafolatlangan kirishga aylanmaydi. Amaliyotda O'zbekistonda ochiq yig'ilishlarning videoyozuvi va onlayn yoritilishi tobora muhim ahamiyat kasb etmoqda. Rasmiy kommunikatsiyalarda Senat yalpi majlislari onlayn translatsiya qilinishi qayd etiladi, shuningdek parlament muhokamalarining onlayn translatsiyasi amaliyoti ham rivojlanmoqda.

OAV uchun bu muhim ish vositasi hisoblanadi, chunki ochiq yig'ilishlarning videotranslyatsiyalari jurnalistlarning vaqtini tejaydi, sitatlar va mansabdor shaxslar pozitsiyasining birlamchi manbasini beradi hamda keyinchalik aynan qaysi ma'lumotni hujjatlar bilan tasdiqlash zarurligini tushungan holda aniq hujjatlarni (kun tartibi, qaror loyihalari, bayonnoma, tekshiruv natijalari) so'rash imkonini yaratadi.

2.2.4. Axborot manbalarining himoyalaniishi va maxfiy saqlanishi

Jurnalist axborot manbalarining maxfiyligini saqlash — bu jurnalistikaning qonun darajasida, shuningdek Butunjahon jurnalistlar xartiyasida²⁸ mustahkamlangan asosiy professional tamoyillaridan biridir. U fikr bildirish erkinligi va jamiyatning axborot olish huquqi bilan bevosita bog'liq: maxfiylik kafolatlarisiz manbalar jamoat manfaatiga oid masalalar bo'yicha ma'lumot berishdan bosh tortishi mumkin.

O'zbekiston qonunchiligida manbalarni himoya qilish majburiyat va kafolat sifatida mustahkamlangan. O'zbekiston Respublikasining "Ommaviy axborot vositalari to'g'risida"gi Qonunida ommaviy axborot vositalari axborot, ma'lumot, fakt yoki dalilni taqdim etgan manbaning ismini, shuningdek taxallus bilan imzolangan muallifning ismini ularning yozma roziligisiz oshkor etishga haqli emasligi aniq belgilab qo'yilgan²⁹.

Bundan tashqari, OAV yozma roziliksiz manbaning (shuningdek, taxallusli muallifning) ismini oshkor qilishga haqli emas. O'zbekistonning "Jurnalistlik faoliyatini himoya qilish to'g'risida"gi³⁰ qonuni **jurnalist siri** tushunchasini kiritadi (ya'ni, maxfiy ma'lumot va ismini oshkor qilmaslik sharti bilan xabar qilingan ma'lumotlar), uni manbaning ruxsatisiz oshkor qilish va g'arazli maqsadlarda foydalanishni taqiqlaydi, shuningdek, jurnalistning

²⁶ O'zbekiston Respublikasining "Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqqligi to'g'risida"gi Qonuni. Qonunchilik palatasi tomonidan 2014-yil 11-martda qabul qilingan. Senat tomonidan 2014-yil 10-aprelda ma'qullangan: <https://lex.uz/mact/2381138>

²⁷ O'zbekiston Respublikasining "Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqqligi to'g'risida"gi Qonuni, 16-modda <https://lex.uz/mact/2381138>

²⁸ Xalqaro Jurnalistlar Federatsiyasining (XJF) Jurnalistlar etikasi bo'yicha global xartiyasi 2019-yil 12-iyunda Tunisda bo'lib o'tgan XJFning XXX Butunjahon Kongressida qabul qilingan. U "Bordo deklaratsiyasi" nomi bilan tanilgan Jurnalistlar xulq-atvori tamoyillari deklaratsiyasini (1954-yil) to'ldiradi. Xartiya matni quyidagi havola orqali mavjud: <https://lex.uz/mact/2381138>

²⁹ O'zbekiston Respublikasining "Ommaviy axborot vositalari to'g'risida"gi Qonuni, 10-modda. Qonun matni bilan quyidagi havola orqali tanishish mumkin: <https://www.lex.uz/acts/53112>

³⁰ O'zbekiston Respublikasining "Ommaviy axborot vositalari to'g'risida"gi Qonuni, 10-modda. Qonun matni bilan quyidagi havola orqali tanishish mumkin: <https://www.lex.uz/acts/53112>

kasbiy faoliyatiga aralashish va undan kasbiy majburiyatlarini bajarish chog'ida olingan ma'lumotlarni talab qilishni taqiqlaydi³¹.

Biroq qonunchilikdagi kafolatlarga qaramay, OAV tahririyatlari tobora ko'proq axborot manbasini oshkor qilish, uning ma'lumotlari va kontaktlarini taqdim etish talablari bilan to'qnash kelmoqda.

Sizga va axborot manbasiga barcha maxfiylik talablariga rioya qilishda yordam beradigan amaliy tavsiyalarni ulashmoqchimiz.



Maxfiylik shartini oldindan qayd eting. Buni manba bilan yozishmada belgilash va uni identifikatsiya qilish mumkin bo'lgan ma'lumotlarni minimallashtirish orqali amalga oshirish mumkin.



Agar "axborot manbasini oshkor qilish" talabi tushsa, bu haqda darhol muharrir va yuristga xabar bering.



Yodda tutingki, qonunchilikka ko'ra manbani himoya qilish jurnalistning huquqiy majburiyati va professional faoliyat kafolatlarining bir qismi hisoblanadi. Manbalaringizni birinchi talabdayoq oshkor qilmang va ularni aniqlanish, bosim yoki ta'qib xavfi ostida qoldirmang.

2.2.5. Messenjerlar va telegram-kanallar orqali rasmiy ma'lumotlarni olish

Davlat organlarining aloqalari tobora tezkor va to'liq raqamli formatga o'tmoqda. Matbuot xizmatlari ijtimoiy tarmoqlarda o'z akkauntlariga ega bo'lib, messenjerlardagi kanallar va chatlardan nafaqat jurnalistlar bilan tezkor aloqa qilish, balki favqulodda va inqirozli aloqalar uchun ham foydalanadilar. Matbuot xizmatlari darhol bayonotlar, raqamlar va tushuntirishlarni e'lon qilishi, shov-shuv va xatolarga tezda javob berishi, pozitsiyani to'g'ridan-to'g'ri auditoriyaga yetkazishi, fotosuratlar, videolar va hujjatlarni ilova qilishi mumkin. Bunday kommunikatsiyalar teskari aloqani ta'minlaydi.

Biroq, davlat organlari bilan telegram-kanallar orqali muloqot qilishda ikki darajani ajratish kerak — (1) tezkor muloqot — savollarga javob berish, qayta aloqa, avvalgi ma'lumotlarni aniqlashtirish yoki to'ldirish, fotosurat yoki video so'rash, lavozimlar va boshqa ma'lumotlarni tuzatish va (2) davlat organini, veb-saytga havolani albatta ko'rsatgan holda, nashrda ishonch bilan tayanish mumkin bo'lgan rasmiy ma'lumotni olish.

Ba'zi hollarda davlat organlari matbuot xizmatlari telegram-kanal rasmiy ma'lumot manbai emasligini darhol aniqlashtiradi. Bunday hollarda rasmiy manbalar orqali qo'shimcha ma'lumot so'rash va telegram-kanal orqali olingan faktlar yoki hujjatlarning ishonchligiga tayanmaslik xavfsizroqdir.

³¹ O'zbekiston Respublikasining "Ommaviy axborot vositalari to'g'risida"gi Qonuni, 7-modda. Qonun matni bilan quyidagi havola orqali tanishish mumkin: <https://www.lex.uz/acts/53112>

2.2.6. Muammolar yuzaga kelganda qanday harakat qilish kerak?

Axborot toifalari — “Xizmatda foydalanish uchun,” davlat sirlari va foydalanish cheklangan bo'lishi mumkin bo'lgan boshqa toifalar

O'zbekistonda ham, umuman Markaziy Osiyo mintaqasida ham OAV tahririyatlari, jumladan onlayn nashrlar amaliyoti bir xil tendensiyalarni ko'rsatmoqda — qonunchilikdagi kafolatlarga qaramay, axborotga kirish tobora ko'proq cheklanmoqda. Yopiqlik va maxfiylik madaniyati ochiqlik hamda shaffoflik madaniyatidan ustun kelmoqda. Davlat organlari ko'pincha inertsia bilan harakat qiladi: axborotni oshkor qilish va jamiyatga yetkazishdan ko'ra uni yopish osonroq. Davlat organlarining axborot resurslari hanuz yetarlicha informativ emas, muntazam yangilanmaydi, hujjatlar esa tanlab e'lon qilinadi. Axborot so'rayotgan jurnalist yoki OAV tahririyatidan “bu sizga nima uchun kerak” va “keyin nima qilmoqchisiz” kabi savollar berilishi, axborot olish maqsadi bilan qiziqilishi mumkin.

Amaliyotda OAV tahririyatlari va jurnalistlar axborotga kirish sohasida quyidagi huquqbuzarliklarga tez-tez duch keladilar. Ular quyidagi jadvalda keltirilgan.

Axborotdan foydalanish sohasidagi huquqbuzarlik	Qoidabuzarlik tavsifi va qanday harakat qilish kerak?
Javob berish muddatining buzilishi	Javob qonunda belgilangan muddatda berilmaydi yoki tushuntirishsiz kechikib yuboriladi. Ba'zan ariza beruvchiga so'rovning ro'yxatdan o'tkazilganligi haqida xabar berilmaydi va oraliq ma'lumot berilmaydi (kim ko'rib chiqadi, javob qachon tayyor bo'ladi). Tahririy yondashuv quyidagicha bo'lishi mumkin. Yuborish va ro'yxatdan o'tish sanasini qayd eting, dastlabki so'rovga havola va ko'rib chiqish holatini tasdiqlash so'rovi bilan qisqa eslatma yuboring. Agar muddat o'tib ketgan bo'lsa, kechikish sababi va javob berish sanasini ko'rsatish talabi bilan qayta so'rov yuboring. Zarurat tug'ilganda, darhol prokuratura organlariga shikoyat yuboring.
OAV tahririyati so'roviga to'liq bo'lmagan javob	Javobda umumiy ta'riflar keltiriladi, ammo aniq savollarga javob berilmaydi, so'ralgan hujjatlar yoki ma'lumotlar berilmaydi, javoblar uchun faqat qulay bandlar tanlanadi yoki ma'lumot taqdim etmasdan saytga yo'naltiriladi. Ko'pincha hujjat rekvizitlari (raqami, sanasi), ma'lumotlar manbalari va mas'ul mansabdor shaxs ko'rsatilmaydi. Tahririyat qanday ish tutishi kerak? Javobni so'rov bandlei bilan solishtiring va aynan nima berilmaganini ro'yxat orqali aniqlashtiring. Hujjatlarning nusxalari yoki ulardan ko'chirmalar, rekvizitlar va ma'lumotlar manbasini taqdim etishni so'rang. Agar ma'lumotlarning bir qismini oshkor qilish mumkin bo'lmasa, rad etishning huquqiy asosini so'rash va ma'lumotlarning qolgan qismini taqdim etish to'g'risida talabnoma yuborish mumkin.
So'ralayotgan axborot faqat xizmatda foydalanish uchun mo'ljallanganligini vaj qilib, ma'lumot berishni rad etish.	Xizmat doirasida foydalanish uchun mo'ljallangan axborotlar toifasiga kiritish tartibiga rioya qilinmayapti: juda ko'p hujjatlarga “XDFU” belgisi qo'yilmoqda, cheklov muddati hisobga olinmayapti, hujjat qisman cheklanishi o'rniga to'liqligicha yopib qo'yilmoqda. Bunday vaziyatda tahririyat yondashuvi quyidagicha bo'lishi lozim: agar hujjat to'liq yopilgan bo'lsa, uning aynan qaysi qismlari himoyaga olinganini va nima uchun qolgan qismini taqdim etish imkonini yo'qligini tushuntirishni talab qiling.
So'ralayotgan axborot sir, masalan, tijorat siri ekanligini sabab qilib ko'rsatib, uni taqdim etishdan bosh tortish	Tijorat siri ko'pincha xususiy tashkilotlar va davlat organlari tomonidan ma'lumotlarni oshkor qilishga qarshi dalil sifatida ishlatiladi. Har doim so'rovingiz ijtimoiy ahamiyatga ega ekanligini ta'kidlang (masalan, gap davlat mablag'larini sarflash yoki ijtimoiy sohalar uchun dasturlar, loyihalar haqida ketganda). Ijtimoiy ahamiyatga ega bo'lgan ma'lumotlarni oshkor qilish har doim ustuvor bo'lishi kerak.

Davlat organlari, xususiy kompaniyalar va tashkilotlar OAV tahririyatlari so'rovlariga javoban axborot taqdim etishda turli cheklovlarni qo'llashlariga qaramay, OAV tahririyatlariga huquqiy yordam ko'rsatish amaliy tajribasiga asoslangan bir nechta umumiy tavsiyalar mavjud:

- So'rovlarni imkon qadar aniq va ravshan shakllantirish maqsadga muvofiq. So'rov yoki kerakli hujjatlar qanchalik aniq ko'rsatilsa, kerakli ma'lumotni olish ehtimoli shunchalik yuqori bo'ladi.
- Faqat so'rovlarga tayanib qolmang. Muqobil axborot manbalari — ochiq ma'lumotlar, reyestrlar, ma'lumotlar bazalaridan faol foydalaning, axborot manbai sifatida esa bloglar va ijtimoiy tarmoqlardan foydalaning.
- Davlat idoralaridan izoh emas, aynan hujjatlarni so'rang. Izohlarni ekspertlar ham taqdim etishi mumkin. Bunday holda, siz talqin va subyektiv fikrlarga kamroq bog'liq bo'lasiz.

2.3. Raqamli muhitda kontent uchun javobgarlik

2.3.1. Noqonuniy (taqiqlangan) va nozik mazmundagi kontentga nimalar kiradi?

Markaziy Osiyo mamlakatlarida OAV tahririyatlari va kontent-meykerlar uchun mavzular ro'yxati mavjud bo'lib, ular ba'zi mamlakatlarda qonunchilik darajasida noqonuniy hisoblanadi (masalan, Qozog'iston), boshqa mamlakatlarda esa bu mavzulardagi nashrlar nomaqbul hisoblanadi, chunki ular nashr mualliflari, nodavlat notijorat tashkilotlari, OAV tahririyatlari va ularning mulkdorlari uchun jiddiy muammolarni keltirib chiqarishi mumkin.

O'zbekistonning xalqaro majburiyatlari quyidagi holatlar bilan bog'liq axborotlarga nisbatan eng qat'iy taqiqlov choralarini qo'llash zarurligini belgilaydi:

- ekstremizm va terrorizm targ'iboti hamda taqiqlangan tashkilotlar materiallari bilan bog'liq axborotlar (jumladan materiallar yoki ramzlarni, turli chaqiriqlarni tarqatishni taqiqlash);
- giyohvand moddalarni targ'ib qilish bilan bog'liq jinoyatlar;
- davlat sirlarini oshkor qilish va milliy xavfsizlik masalalari bilan bog'liq axborotlar;
- milliy, etnik yoki diniy adovatni qo'zg'atish (nafrat nutqi);
- bolalarni pornografiya va nomaqbul kontentdan himoya qilish bilan bog'liq masalalar;
- aniq jamoatchilik manfaati mavjud bo'lmagan hollarda shaxsiy hayot va shaxsiy ma'lumotlar bilan bog'liq axborotlar.

Biroq mavzularning katta qismi jurnalistlar va OAV uchun sezgir hisoblanadi, chunki tahririyat ushbu ro'yxatdagi masalalarni yoritgan taqdirda ehtimoliy yoki real huquqiy muammolar yuzaga kelishi mumkin. Shu bilan birga, bu mavzularda material e'lon qilish bo'yicha to'g'ridan-to'g'ri taqiq mavjud emas, ammo barcha OAV tahririyatlari, jurnalistlar va muharrirlar ushbu mavzularning sezgirligini yaxshi biladilar.

Jadvaldagi mavzular OAV uchun taqiqlangan yoki yopiq emas, lekin maksimal ehtiyotkorlikni, faktlarni qayta-qayta tekshirishni va ehtimoliy bosim yoki ta'qib xavfini baholashni talab qiladi.

Nashr mavzusi	Mavzu nimani qamrab oladi?
Taqiqlangan partiyalar faoliyati	Taqiqlangan tashkilotlar faoliyati, ularning bayonotlari, materiallari, ramzlari, shiorlari, atributikasi; ularning resurslariga havolalar; qo'llab-quvvatlash, ishtirok etish yoki moliyalashtirishga chaqiriqlar.
O'z joniga qasd qilishlar	O'z joniga qasd qilish yoki o'z joniga qasd qilishga urinish holatlari haqida sabablari va holatlari batafsil bayon etilgan xabarlar. Voyaga yetmaganlar orasida sodir bo'lgan holatlarning batafsil tavsifi; "ko'rsatma" beruvchi tafsilotlarni (usullar, joylar, harakatlar ketma-ketligi) o'z ichiga olishi mumkin bo'lgan nashrlar, bu esa Verter effektini keltirib chiqarishi mumkin.
Yuqori mansabdor shaxslarning shaxsiy hayoti	Oila va shaxsiy munosabatlar; sog'liq; yashash joyi va maishiy tafsilotlar; shaxsiy yozishmalar va fotosuratlar (oila a'zolarining o'zlari fotosuratlar va ma'lumotlarni ijtimoiy tarmoqlarga joylashtirgan hollar bundan mustasno); bolalar va yaqinlari haqidagi ma'lumotlar; ommaviy vazifa va vakolatlarni bajarish bilan bevosita bog'liq bo'lmagan ma'lumotlar.
Tarixiy voqealar	Tarixiy davrlar va voqealarga berilgan baholar hamda talqinlar; repressiyalar, mojarolar, chegaralar, identiklik mavzulari; bahsli xotira sanalari; jamoatchilik bahslarini keltirib chiqarishi mumkin bo'lgan tarixiy taqqoslashlar.
Millatlararo mojarolar	"Guruhlararo" hodisa va nizolar; millatlararo tus olgan maishiy mojarolar; etnik kelib chiqishi bo'yicha kamsitish; nafrat tili; etnik guruhlariga nisbatan ayblovlar.
Tashqi siyosat	Xalqaro munosabatlar va mansabdor shaxslar bayonotlari; diplomatik mojarolar; urushlar va inqirozlar bo'yicha pozitsiyalar; xalqaro kelishuvlar; tashriflar, muzokaralar, notalar; boshqa davlatlar va ularning yetakchilariga berilgan baholar.
Sanksiyalar	Sanksiya ro'yxatlari va cheklovlar (shaxslar, kompaniyalar, tarmoqlarga nisbatan); aktivlarni muzlatish, bitimlar, yetkazib berish va kirish taqiqlari; biznes uchun ikkilamchi oqibatlar.
Korrupsiya	Korrupsiyaga qarshi surishtiruvlar; mansabdor shaxslarga nisbatan ayblovlar; manfaatlar to'qnashuvi; davlat xaridlari va byudjet mablag'larini taqsimlash.
Ijtimoiy mojarolar	Tariflar, narxlar, kommunal xizmatlar, yer va uy-joy bilan bog'liq nizolar; aholi va hokimiyat hamda biznes o'rtasidagi nizolar; ommaviy shikoyatlar; rezonansli hodisalar.
Diskriminatsiya	Jins, yosh, nogironlik, kelib chiqish, til, din va boshqa belgilar bo'yicha teng bo'lmagan muomala va cheklovlar, shuningdek nafrat tili; inson qadr-qimmatini kamsitish; guruhlarni stereotiplashtirish.
Mitinglar va norozilik namoyishlari	Ommaviy yig'inlar, aksiyalar, piketlar; ularda ishtirok etishga chaqiriqlar; qatnashchilarning talablarini yoritish; qo'lga olishlar va ma'muriy choralar; ishtirokchilar va tashkilotchilarning foto va videolarini e'lon qilish.
Ish tashlashlar	Jamoaviy mehnat nizolari; ishni to'xtatish; xodimlarning talablari; ish beruvchi bilan muzokaralar; ishdan bo'shatish yoki bosim; xodimlar va kasaba uyushmasi faollarining shaxsiy ma'lumotlarini e'lon qilish.
LGBT hamjamiyati masalalari	Huquqlar, kamsitish va xavfsizlik haqidagi postlar; zo'ravonlik va tajovuz holatlari; tibbiy va inson huquqlari mavzulari; jinsiylik bilan bog'liq kontent.
Til masalalari	Tillar maqomi, til siyosati; ta'lim va xizmat ko'rsatish tili atrofidagi mojarolar; "falon tilda gapiring" degan talablar; til belgisi bo'yicha kamsitish; rezonansli bayonotlar va nizolar.
Din	Diniy tashkilotlar faoliyati; diniy marosimlar va ramzlar; diniy mojarolar; ekstremizmga ayblovlar; haqoratomuz deb hisoblanishi mumkin bo'lgan nozik nashrlar.
Gender masalalari	Teng huquq va imkoniyatlar; oiladagi/gender asosidagi zo'ravonlik; ayollarning siyosat va iqtisodiyotdagi ishtiroki; reproduktiv huquqlar; jins bo'yicha kamsitish; o'zaro kamsitishga duchor bo'lgan ayollar, qizlar va qizlarning zaif guruhlari.

Yana bir bor ta'kidlaymizki, yuqorida ko'rsatilgan mavzular OAV uchun taqiqlangan yoki yopiq emas, biroq ular maksimal ehtiyotkorlikni, faktlarni qayta-qayta tekshirishni hamda ehtimoliy bosim yoki ta'qib xavfini baholashni talab qiladi.

2.3.2. Diffamatsiya, tuhmat va haqorat uchun javobgarlik

Jismoniy va yuridik shaxslarning sha'ni, qadr-qimmati va obro'sini himoya qilish sud tartibida fuqarolik da'vosi orqali ham, tuhmat va haqorat qilingan taqdirda ma'muriy va jinoiy tartib-taomillar orqali ham amalga oshirilishi mumkin.

Qoidabuzarlik turi	Qo'llaniladigan tartib-qoidalar	Huquqiy oqibatlar
Sha'n, qadr-qimmat va ishchanlik obro'sini himoya qilish	O'zbekiston Respublikasi Fuqarolik kodeksining 100-moddasiga muvofiq sud tartibida da'vo taqdim etish orqali fuqarolik-huquqiy tartib ³²	Sha'n va qadr-qimmatga putur yetkazuvchi ma'lumotlarga raddiya e'lon qilish, ma'naviy zararni qoplash, ularni tarqatishni to'xtatish.
Tuhmat	O'zbekiston Ma'muriy javobgarlik to'g'risidagi kodeksining (MJTK) 40-moddasi ³³ bo'yicha ma'muriy ish. O'zbekiston Respublikasi Jinoyat kodeksining 139-moddasiga muvofiq ³⁴ tartib-taomil (shu jumladan, agar qilmish ma'muriy jazo qo'llanilganidan keyin sodir etilgan bo'lsa; ommaviy axborot vositalari, Internet orqali tarqatish alohida ko'rsatilgan)	Ma'muriy jarima 20–60 BHM. Jinoiy tartibda javobgarlik choralari. Jarima (shu jumladan BHMning 200 baravarigacha; OAV yoki Internet orqali e'lon qilinganda jarima 200–400 BHMni tashkil etadi), majburiy ishlar yoki axloq tuzatish ishlari, ozodlikni cheklash mumkin; kvalifikatsiya belgilari mavjud bo'lsa, yanada qattiqroq sanksiyalar qo'llanilishi mumkin (shu jumladan BHMning 300–500 baravarigacha jarima yoki 3 yilgacha ozodlikni cheklash).
Haqorat	MJTKning 41-moddasiga ³⁵ muvofiq ma'muriy tartib. Asoslar mavjud bo'lganda, O'zbekiston Respublikasi Jinoyat kodeksining 140-moddasiga muvofiq jinoiy-huquqiy taomillar qo'llanilishi mumkin (shu jumladan, ma'muriy jazo qo'llanilganidan keyin sodir etilgan bo'lsa; alohida hollarda ommaviy axborot vositalari yoki Internet orqali tarqatilganda) ³⁶ .	Ma'muriy jarima BHMning 20 baravaridan 40 baravarigacha bo'ladi. Jinoiy javobgarlik choralari: 200 BHMgacha jarima; OAV/Internet orqali e'lon qilinganda — 200–400 BHM), majburiy ishlar yoki axloq tuzatish ishlari; kvalifikatsiya belgilari mavjud bo'lsa, 400 dan 600 BHMgacha jarima yoki 1 yildan 2 yilgacha ozodlikni cheklash.

³² O'zbekiston Respublikasining Fuqarolik kodeksi, 100-modda. Kodeks matni quyidagi havola orqali mavjud: <https://lex.uz/docs/111181#159215>

³³ O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 40-moddasi. Kodeks matni quyidagi havola orqali mavjud: <https://www.lex.uz/acts/97661>

³⁴ O'zbekiston Respublikasi Jinoyat kodeksining 139-moddasi. Kodeks matni quyidagi havola orqali mavjud: <https://www.lex.uz/acts/111457>

³⁵ O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 41-moddasi. Kodeks matni quyidagi havola orqali mavjud: <https://www.lex.uz/acts/97661>

³⁶ O'zbekiston Respublikasi Jinoyat kodeksining 140-moddasi. Kodeks matni quyidagi havola orqali mavjud: <https://www.lex.uz/acts/111457>

2.3.3. Yolg'on axborot tarqatganlik uchun javobgarlik

Yolg'on axborot tarqatganlik uchun javobgarlik pandemiya davridagi feyklar to'loqiniga javob chorasini sifatida joriy etilgan bo'lib, ular asosan emlash, davolanish, pandemiya oqibatlari va boshqalarning xavf-xatarlari va oqibatlari bilan bog'liq edi. Pandemiya allaqachon tugagan, biroq yolg'on axborot tarqatganlik uchun javobgarlik hozirda jurnalist va blogerlarga nisbatan keng qo'llanilmoqda. Shu bilan birga, jurnalistlar va ommaviy axborot vositalariga nisbatan jinoiy javobgarlikning haddan tashqari keng asoslari va choralari sovuqlashtiruvchi ta'sir ko'rsatishi ma'lum — ya'ni jurnalistlar, ommaviy axborot vositalari tahririyatlari, blogerlar o'tkir mavzulardan qochishni boshlaydilar, iboralarni yumshatadilar, surishtiruvlar va tanqidiy materiallardan voz kechadilar, javobgarlikka tortilish xavfi tufayli maqolalarni tezroq o'chiradilar va muhokamalarni yopadilar; o'z-o'zini senzura qilish darajasi oshadi.

O'zbekistonda yolg'on axborotni tarqatganlik uchun ikki turdagi javobgarlik mavjud — ma'muriy va jinoiy. Quyidagi jadvalda biz qonunbuzarlik yuzaga kelishining huquqiy asoslari va yolg'on axborot tarqatilgan taqdirda qo'llanilishi mumkin bo'lgan javobgarlik choralarni ko'rsatdik o'tdik.

Javobgarlik turlari	Qachon qo'llanadi?	Javobgarlik choralari
Ma'muriy javobgarlik 	- OAVda yoki internetda shaxs sha'ni va qadr-qimmatini kamsituvchi yoki shaxsni obro'sizlantiruvchi yolg'on axborotni tarqatish³⁷. - OAVda yoki internetda jamoat tartibi yoki xavfsizligiga tahdid soluvchi yolg'on axborotni tarqatish³⁸.	Ma'muriy jarima BHMning 50 baravari yoki BHMning 50–100 baravari (moddaning qismiga qarab)
Jinoiy javobgarlik 	OAVda yoki internetda shaxs sha'ni va qadr-qimmatini kamsituvchi yoki shaxsni obro'sizlantiruvchi yolg'on axborotni tarqatish, agar bunday harakatlar uchun avval ma'muriy jazo qo'llanganidan keyin takror sodir etilgan bo'lsa ³⁹ .	150–200 BHMgacha jarima; 240–300 soatgacha majburiy jamoat ishlari; 2 yilgacha axloq tuzatish ishlari yoki 2–3 yilgacha ozodlikni cheklash.

2.3.4. Hate speech

Markaziy Osiyo mamlakatlarida, shu jumladan O'zbekistonda ham hate speech (nafratli nutq) mavzusi, eng avvalo, milliy, irqiy, etnik yoki diniy adovat qo'zg'atishning jinoiy-huquqiy taqiqlanishi bilan bog'liq. O'zbekistonda bunday taqiq Jinoyat kodeksining 156-moddasi⁴⁰ «Milliy, irqiy, etnik yoki diniy adovatni qo'zg'atish»da amalga oshirilgan.

³⁷ O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 202-moddasi. Kodeks matni havola orqali mavjud: <https://www.lex.uz/acts/97661>

³⁸ O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 202-moddasi. Kodeks matni havola orqali mavjud: <https://www.lex.uz/acts/97661>

³⁹ O'zbekiston Respublikasi Jinoyat kodeksining 244-moddasi. Kodeks matni quyidagi havola orqali mavjud: <https://www.lex.uz/acts/111457>

⁴⁰ O'zbekiston Respublikasi Jinoyat kodeksining 156-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: <https://www.lex.uz/acts/111457>

Modda ko'rsatilgan belgilar bo'yicha adovat qo'zg'atish va qadr-qimmatni kamsitishga qaratilgan qasddan qilingan harakatlarni, shuningdek, bunday adovatni targ'ib qiluvchi materiallarni tarqatish maqsadida tayyorlash, saqlash va tarqatishni qamrab oladi. Bu shuni anglatadiki, xavf zonasi nafaqat mualliflik matnida, balki boshqalarning materiallarini e'lon qilishda, sarlavhalar va illyustratsiyalarda, shuningdek, kontent tarqatuvchisi sifatida OAV tahririyatlari maydonchalarida auditoriyaning izohlarida paydo bo'ladi.

Alohida turdosh xavf — «urushni targ'ib qilish» (O'zbekiston Jinoyat kodeksining 150-moddasi⁴¹). Moddaning ta'sir doirasiga bir davlatning boshqasiga qarshi tajovuzini qo'zg'atish maqsadida g'oyalar yoki chaqiriqlar tarqatish kiradi; sanksiya 5 yildan 10 yilgacha ozodlikdan mahrum qilishni nazarda tutadi. Amaliy xulosa oddiy: nafrat tili yoki zo'ravonlikka da'vat qilish mumkin bo'lgan mavzularda imkon qadar betaraf taqdimot, umumlashtirish va stereotiplardan voz kechish, aniq iqtiboslar keltirish (haqoratli so'zlarni ko'paytirmasdan) va izohlarni tezda nazorat qilish kerak, shunda sizning resursingiz taqiqlangan materiallarni tarqatish kanaliga aylanmaydi.

2.3.5. Media akkauntlaridagi izohlar uchun javobgarlik

Endi OAV tahririyatlari va bloggerlarning foydalanuvchilar tomonidan qoldirilgan kontent uchun javobgarligi masalasiga batafsilroq to'xtalamiz. Izohlar muhokama qilinayotgan maqolaga aloqador bo'lmasligi ham mumkin, biroq izoh matnlarida noqonuniy kontent, haqorat, hate speech, begona shaxsiy ma'lumotlar, obro'ga putur yetkazuvchi ma'lumotlar yoki yolg'on axborot bo'lishi xavfi mavjud. Izohlar javobgarlikni izoh muallifi va OAV tahririyati yoki blogger o'rtasida taqsimlash nuqtai nazaridan ham muammoli bo'lishi mumkin.

Izoh mazmuni uchun javobgarlik izoh muallifining o'ziga yuklanadi, biroq OAV tahririyatlari va bloggerlar saytlar hamda bloglardan taqiqlangan axborotni joylashtirish uchun foydalanilishiga yo'l qo'ymasliklari shart. Bu "Axborotlashtirish to'g'risida"gi⁴² Qonunda bevosita mustahkamlangan. Shu sababli moderatsiyaning yo'qligi va murojaatlarni e'tiborsiz qoldirish tahririyatning o'zi uchun xavflarni oshiradi.

Muallif va OAV tahririyati o'rtasidagi javobgarlik chegarasi qayerda o'tadi? Quyidagi uch omildan hech bo'lmaganda bittasi mavjud bo'lsa, OAV tahririyatining muammoli izoh uchun javobgarlikka tortilish xavfi keskin oshadi:



Muammoli izohni ma'qullash (uni mahkamlash, alohida ajratish yoki "auditoriya pozitsiyasi" sifatida ko'rsatish).



Moderatsiyaning yo'qligi (mas'ul shaxs, qoidalar yoki o'chirish mexanizmi mavjud emas).



Izohlar bo'yicha murojaatlarni e'tiborsiz qoldirish (aniq qonunbuzarlikni o'chirmaslik, reaksiyani qayd etmaslik).

Muammoli izohlar uchun javobgarlikdan qochish maqsadida OAV tahririyati yoki blogger quyidagilarni ishlab chiqishi va joriy etishi mumkin:

⁴¹ O'zbekiston Respublikasi Jinoyat kodeksi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: <https://www.lex.uz/acts/111457>

⁴² "Axborotlashtirish to'g'risida"gi O'zbekiston Respublikasi Qonunining 12-moddasi. Qonun matni bilan quyidagi havola orqali tanishish mumkin: <https://lex.uz/acts/82956>

- foydalanuvchilar uchun izoh qoldirish qoidalari;
- premoderatsiya va moderatsiya bo'yicha ichki tartib.

Foydalanuvchilar uchun izoh qoldirish qoidalari — bu OAV tahririyati yoki blogerning ehtimoliy muammoli izohlar uchun javobgarlikni taqsimlash bo'yicha ommaviy siyosati (pozitsiyasi) hisoblanadi. Ushbu qoidalarga kiritilishi zarur bo'lgan minimal talablar quyidagilar:

- Izoh qoldirish qoidalari sayt va tahririyatning ijtimoiy tarmoqlar hamda messenjerlardagi barcha izohlariga tatbiq etiladi.
- Izoh qoldirgan foydalanuvchi qoidalar bilan roziligini tasdiqlaydi va mazmun uchun shaxsan javobgar bo'ladi.
- Izohlarda haqorat va qadr-qimmatni kamsitish, diskriminatsiya, adovat qo'zg'atish va zo'ravonlikka chaqiriqlar, ekstremizm, urush targ'iboti, pornografiya va narkotiklar, yolg'on axborot, shuningdek fishing, spam, tajovuzkor reklama, shaxsiy ma'lumotlar va shaxsiy yozishmalarni, skrinshotlarni e'lon qilish hamda haqoratli so'zlardan foydalanish taqiqlanadi.
- Tahririyat qoidalarini buzuvchi izohlarni o'chirish va foydalanuvchilarni bloklash huquqiga ega.
- Tahririyat qonunbuzarliklar haqidagi murojaatlarni ko'rib chiqadi va choralar ko'radi, jumladan izohlarni o'chirish va kirishni cheklash.

Izoh qoldirish qoidalaridan tashqari, OAV tahririyati izohlarni moderatsiya qilish bo'yicha ichki tartibni ham ishlab chiqishi va qabul qilishi mumkin. Ushbu hujjatga quyidagi qoidalar (minimal ro'yxat) kiritilishi lozim:

- Model belgilanadi — bu premoderatsiya bo'ladimi yoki postmoderatsiya? Yuqori xavfli mavzular uchun (adovat, zo'ravonlik, urush, feyklar, shaxsiy ma'lumotlar) kuchaytirilgan rejim o'rnatiladi (masalan, premoderatsiya yoki izohlarni cheklash).
- Muddatlar belgilanadi — yangi izohlar qanchalik tez tekshirilishi va tahririyat shikoyatlarga qanchalik tez javob berishi kerakligi (masalan, ish kuni davomida yoki yuqori xavfli mavzular uchun bir necha soat ichida).
- Taqiqlangan kontent va izoh qoldirish qoidalarini buzuvchi izohlar o'chirilishi (yoki yashirilishi), takroriy qoidabuzarlik qilgan foydalanuvchilar esa bloklanishi mustahkamlanadi. Qarorlar yagona mezonlar asosida qabul qilinadi.
- Bahsli yoki potensial xavfli holatlar uchun muammoli izohlarni qayd etish nazarda tutiladi. Bu izohga havola, sana va vaqtni saqlab qolish zarurligini anglatadi. Muammoli izohlarning skrinshotlari faqat ichki dosye uchun olinadi va tarqatilmaydi.
- Qaysi holatlar albatta muharrir yoki yuristga yuborilishi belgilanadi. Bular adovat qo'zg'atish, zo'ravonlikka chaqiriqlar, ekstremizm, shaxsiy ma'lumotlarni e'lon qilish, yolg'on axborot, narkotiklar targ'iboti va boshqa taqiqlangan kontent alomatlari mavjud bo'lgan izohlardir.
- Muammoli izohlarni “auditoriya pozitsiyasi” sifatida mahkamlash, iqtibos keltirish yoki qayta e'lon qilish taqiqlanadi. Tahririyat tomonidan izohni har qanday alohida ajratish javobgarlikning qo'shimcha omili sifatida baholanadi.

2.3.6. Kontent bo'yicha onlayn platformalar qoidalar/Onlayn-platformalarning kontent bo'yicha qoidalar

Onlayn platformalarning kontent qoidalar masalasiga alohida to'xtalib o'tamiz. Yuqorida biz O'zbekiston milliy qonunchiligiga muvofiq raqamli muhitda kontent uchun javobgarlik yuzaga kelishi mumkin bo'lgan muammoli vaziyatlarni tahlil qildik. Ammo onlayn platformalar ham o'z qoidalariga ko'ra ishlaydi. Bu alohida xavf, chunki kontent bloklanishi, tanbeh berilishi, monetizatsiya faolsizlantirilishi yoki hisob tugatilishi mumkin. Har bir onlayn platforma o'zining ommaviy va bajarilishi majburiy bo'lgan siyosatiga ega.

Onlayn-platformalar siyosati nuqtai nazaridan qanday kontent muammoli hisoblanadi?

- yuqorida aytib o'tilganidek, nafratli nutq (gumanizatsiyadan mahrum etish, kamsitish, diskriminatsiya yoki zo'ravonlikka da'vat qilish);
- xavfli kontent va zo'ravonlikka chaqiriqlar, ekstremistik va terroristik kontent;
- sezgir mavzulardagi dezinformatsiya (salomatlik, xavfsizlik, inqirozlar);
- bulling (tazyiq o'tkazish), ta'qib qilish yoki tahdidlar;
- shaxsiy daxlsizlikni buzadigan shaxsiy ma'lumotlar va postlar.

Onlayn platformalar siyosati:

Meta (Facebook, Instagram) Hateful Conduct

https://transparency.meta.com/policies/community-standards/hateful-conduct/?utm_source=chatgpt.com

YouTube Hate Speech Policy

https://support.google.com/youtube/answer/2801939?hl=en&utm_source=chatgpt.com

TikTok

<https://ads.tiktok.com/help/category?id=535nt8Z20sG4IW62MZPJvL>

Telegram

<https://telegram.org/moderation>

Tahririyat uchun amaliy xulosa shundan iboratki — tahririyat siyosatini ishlab chiqishda nafaqat O'zbekistonning amaldagi qonunchiligiga, balki onlayn-platformalarning aniq belgilangan taqiqlangan zonalariga ham tayanish kerak. Ayniqsa diskriminatsiya, zo'ravonlik, feyklar va shaxsiy ma'lumotlar bilan bog'liq mavzularda. Bahsli holatlarda xavflarni kamaytirish maqsadga muvofiq: jamoatchilik uchun muhim mavzularni chetlab o'tmagan holda, platformalarda muammo tug'dirmaydigan kontentni e'lon qilish xavfsizroq hisoblanadi.

2.4. Mualliflik huquqlari va media

Jurnalistlar va ommaviy axborot vositalari doimiy ravishda kontent yaratadi, shuningdek, boshqalarning kontenti: matnlar, fotosuratlar, videolar, musiqa, infografika, dizayn bilan ishlaydi. Jurnalistlar va tahririyatlar tomonidan yaratilayotgan mediamateriallarning aksariyati mualliflik huquqi obyekti hisoblanadi.

Mediakontentni mualliflik huquqi obyekti sifatida tan olishning asosiy mezonlari quyidagilarni o'z ichiga oladi:

- individual yoki jamoaviy ijodiy faoliyat;
- aniq va idrok etish mumkin bo'lgan shaklda ifodalanishi (matn, tasvir, audio/video, raqamli yozuv va hokazo).

O'zbekiston Respublikasining "Mualliflik huquqi va turdosh huquqlar to'g'risida"gi Qonuni (2006-yil 20-iyuldagi O'RQ-42-son) mualliflik huquqi "asar yaratilgan paytdan boshlab" vujudga kelishini va ro'yxatdan o'tkazish yoki boshqa rasmiyatchiliklarni talab qilmasligini belgilaydi..

Raqamli muhitda Internet tarmog'ida e'lon qilish "hammaning e'tiboriga yetkazish" bo'lib, unda foydalanuvchilar "o'zlari xohlagan joydan va istalgan vaqtda" kirishlari mumkin. Bu amal muallif yoki mualliflik huquqi egasining ekskluziv huquqlariga taalluqli (ya'ni ruxsat/litsenziya talab qiladi), shuningdek, ko'paytirish va tarqatishga ham taalluqlidir.

O'zbekiston mualliflik huquqlarini himoya qilishning xalqaro tizimiga kiritilgan. Mamlakat 2005-yil 19-apreldan boshlab Adabiy va badiiy asarlarni himoya qilish bo'yicha Bern konvensiyasida (Bern konvensiyasi), shuningdek, 2019-yil 17-iyuldan boshlab Butunjahon intellektual mulk tashkilotining "internet shartnomalari" deb ataladigan BIMTning mualliflik huquqi to'g'risidagi shartnomasi (WCT) va BIMTning ijrolar va fonogramma to'g'risidagi shartnomasi (WPPT) ishtirokchisi hisoblanadi.

Bern konvensiyasi ishtirokchi davlatlar mualliflari va asarlari uchun milliy himoya rejimi, mualliflik huquqlarining asar yaratilgan paytdan boshlab avtomatik himoyasi hamda kamida 50 yillik himoya muddatini belgilaydi. BIMT shartnomalari esa mualliflik huquqlarini raqamli muhitga moslashtiradi, jumladan texnik himoya choralarini (masalan, himoya yoki shifrlashni chetlab o'tish) va huquqlarni boshqarish haqidagi ma'lumotlarni (rights management information) himoya qilishni o'z ichiga oladi.

Qonunning 5-moddasiga muvofiq, "Mualliflik huquqi ilm-fan, adabiyot va san'at asarlariga, ularning maqsadi va qadr-qimmatidan, shuningdek ifoda etilish usulidan qat'i nazar, ijodiy faoliyat natijasi sifatida tatbiq etiladi". Mualliflik huquqi ham oshkor qilingan (e'lon qilingan, tarqatilgan, shu jumladan internetda joylashtirilgan), ham oshkor qilinmagan, obyektiv shaklda mavjud bo'lgan asarlarga nisbatan amal qiladi.

Mualliflik huquqi muallifning shaxsiy nomulkiy va mulkiy huquqlaridan iborat. Shaxsiy nomulkiy huquqlar begonalashtirilmaydi, mulkiy huquqlar esa muallif (hammualliflar) hayoti davomida va vafotidan keyin 70 yil davomida amal qiladi. Mulkiy huquqlar asardan istalgan formatda foydalanishning keng doirasini, jumladan asarni tarjima qilish va boshqa formatlarga moslashtirish huquqini ham o'z ichiga oladi.

Huquq turi	Toifa	Himoya hajmi	Huquqbuzarlik usullari
Shaxsiy nomulkiy	Mualliflik huquqi	Asar muallifi sifatida tan olinishi huquqi	Asardan muallif nomini ko'rsatmasdan nusxa ko'chirish va tarqatish yoki mualliflikni o'zlashtirish (plagiat)
	Muallif nomiga bo'lgan huquq	Asardan foydalanilganda muallif yoki uning taxallusi ko'rsatilishi shart	Asarni muallif roziligisiz yoki boshqa nom bilan e'lon qilish va tarqatish, ismni buzib ko'rsatish, taxallusni oshkor qilish
	Oshkor qilish huquqi	asarni har qanday shaklda e'lon qilish yoki e'lon qilishga ruxsat berish huquqi, shu jumladan asarni e'lon qilishdan voz kechish huquqi	Muallifning e'lon qilinmagan asari nusxalarini uning roziligisiz e'lon qilish.
	Muallif obro'sini himoya qilish huquqi	Asarni, shu jumladan uning nomini, muallif sha'ni va qadr-qimmatiga zarar yetkazishi mumkin bo'lgan har qanday buzilish yoki tajovuzdan himoya qilish huquqi	Asarning muallif roziligisiz buzib ko'rsatilishi va tahrir qilinishi
Mulkiy huquqlar	Ko'paytirish huquqi	Asarning raqamli yoki jismoniy nusxalarini yaratish	Muallif ruxsatisiz yaratish, nusxalash (qaroqchilik)
	Tarqatish huquqi	Asarning raqamli yoki jismoniy nusxalarini tarqatish va sotish, jumladan, ijaraga berish huquqi	Muallif ruxsatisiz sotish yoki ijaraga berish (kitob, musiqa yoki filmlarning noqonuniy savdosi)
	Ommaviy namoyish va ijro etish huquqi	Ommaviy ijro va ommaviy namoyish	Muallif ruxsatisiz asarni jamoat joylarida ko'rsatish yoki omma oldida ijro etish
	Qayta ishlash huquqi	Asl nusxa asosida yangi (hosila) asar yaratish	Muallifning ruxsatisiz asarni boshqa formatlarga qayta ishlash, xorijiy tillarga tarjima qilish, ssenariy, pyesa, sahna ko'rinishi, musiqiy asarlarning kaver-versiyalari, remikslarga moslashtirish
	Ommaga e'lon qilish/Ommaga yetkazish	Internetda raqamli nusxalarni tarqatish	Muallifning ruxsatisiz asarlarning raqamli nusxalarini raqamli muhitga yuklash va tarqatish

Muallifga (huquq egasiga) mualliflik haqini olish huquqi kafolatlanadi. Qonunchilik asarlarning aniq turlari va ulardan foydalanish usullari uchun mualliflik mukofotining minimal stavkalarini belgilaydi.

MUHIM MA'LUMOT

Intervyuga bo'lgan mualliflik huquqi, agar ular o'rtasidagi kelishuvda boshqacha nazarda tutilmagan bo'lsa, intervyu bergan shaxs va intervyu olgan shaxsga ham-muallif sifatida tegishli bo'ladi. Intervyudan foydalanish faqat intervyu bergan shaxsning roziligi bilan mumkin. Intervyuga mualliflik huquqlarini olish uchun intervyu bergan shaxs bilan mutlaq huquqlarni topshirish va mualliflik mukofotini to'lash shartlarini ko'rsatgan holda kelishuv tuzish zarur.

Mualliflik huquqlarini topshirishning asosiy usuli — mualliflik huquqi obyekti, foydalanish usullari va mualliflik mukofoti miqdori ko'rsatilgan mualliflik shartnomasini tuzishdir.

2.4.3. O'zgalar asarlaridan foydalanish qoidalar

Internet tarmog'i, ijtimoiy tarmoqlar, messenjerlar va veb-saytlarda kontentning keng tarqalishi mualliflik huquqi egalarining ruxsatisiz foydalanilishi mumkin bo'lgan o'zgalar kontentiga kirish imkonini beradi. Internetdagi materiallardan foydalanish erkin emas va mualliflar va (yoki) huquq egalarining rozilgisiz hamda haq to'lanmasdan hamma narsani takrorlash mumkin emas. Har bir matn yoki fotosurat, audio yoki video kontentning muallifi yoki mualliflik huquqi egasi bo'ladi. Saytlar va ijtimoiy tarmoqlardagi materiallardan foydalanish siyosatini diqqat bilan o'qib chiqish zarur. Ochiq akkauntida matn yoki fotosuratlarini e'lon qilish ularni hamma uchun va hamma joyda nashr etish mumkinligini anglatmaydi.

Yangiliklar mualliflik huquqi obyekti hisoblanmaydi. O'zbekiston Respublikasining "Mualliflik huquqi va turdosh huquqlar to'g'risida"gi qonunining 8-moddasiga ko'ra, "oddiy matbuot axboroti xususiyatiga ega bo'lgan kunning yangiliklari yoki joriy voqealar to'g'risidagi xabarlar" qonun bilan qo'riqlanadigan asarlarga kirmaydi.

Shunday qilib, faqat ijodiy faoliyat natijasini ifodalovchi materiallar (foto va videoreportajlar, tahliliy yoki obzor maqolalar, jurnalistik surishtiruvlar, intervyular) mualliflik huquqi himoyalangan asarlar hisoblanadi. Jurnalistlar mediakontent mualliflari, ommaviy axborot vositalari tahririyatlari esa davriy nashrda bosma shaklda yoki onlayn tarzda e'lon qilingan materiallarning huquq egalari hisoblanadi.

Umumiy qoidaga ko'ra, mutlaq mualliflik huquqlari boshqa jismoniy shaxslarga yoki kompaniyalarga tegishli bo'lgan asarlardan foydalanmoqchi bo'lgan shaxs mutlaq huquqlar egasining ruxsatini olishi shart ("Mualliflik huquqi va turdosh huquqlar to'g'risida"gi qonunning 19-moddasi). Ruxsatnoma mualliflik shartnomasi tuzish orqali yozma shaklda ifodalanishi (qonunning 38-moddasi) va mualliflik haqi to'lanishi lozim.

OAVda o'zgalar kontentidan erkin foydalanish misollari

OAV tahririyati mualliflik huquqi obyektlaridan huquq egasining alohida ruxsatisiz cheklangan hajmda foydalanishi mumkin, biroq quyidagi majburiy shartlarga rioya qilinishi kerak:

- **muallif va manbani ko'rsatish (va/yoki tegishli hollarda huquq egasini);**
- **maqsadga muvofiq hajmda foydalanish;**
- **foydalanish asardan odatiy foydalanishga zarar yetkazmasligi va muallifning qonuniy manfaatlarini buzmasligi kerak.**

Quyidagi hollarda:

- ilmiy, tadqiqot, polemik, tanqidiy va reklama bilan bog'liq bo'lmagan axborot maqsadlari uchun e'lon qilingan asarlardan parchalarni iqtibos keltirish;
- muallif yoki huquq egasining maxsus taqiqi bo'lmagan taqdirda, joriy siyosiy, iqtisodiy, ijtimoiy va diniy masalalar bo'yicha chop etilgan materiallarni qayta chop etish;
- omma oldida aytilgan siyosiy nutqlar, murojaatlar, ma'ruzalar va shunga o'xshash chiqishlarni axborot maqsadi bilan oqlangan hajmda qayta berish;
- joriy voqealarni yoritish jarayonida ko'rilgan yoki eshitilgan asarlardan axborot maqsadi bilan oqlangan hajmda foydalanish (konsert, galereya yoki foto ko'rgazmadan reportajlar).

Tahririyat uchun "qizil bayroqlar"

Agar quyidagi belgilaridan hech bo'lmaganda bittasi mavjud bo'lsa, erkin foydalanish qo'shimcha tekshiruvni va/yoki muallif yoki huquq egasining ruxsatini talab qiladi:



Reklama maqsadi yoki targ'ibot

Agar material reklama, mahalliy reklama, homiylik kontenti, PR nashrlari yoki sotuv/obunalarni rag'batlantirish uchun ishlatilsa.



Haddan tashqari katta hajmdagi o'zlashtirish

Matnning katta qismlarini nusxalash, to'liq fotoreportaj/to'liq video/to'liq audioyozuvni e'lon qilish "maqsadga muvofiq hajm"dan tashqariga chiqadi va mualliflik huquqining buzilishi xavfini tug'diradi.



To'g'ri atributsiyaning yo'qligi (manbani ko'rsatmaslik)

Muallif, manba ko'rsatilmagan, havola berilmagan yoki to'liq bo'lmagan ma'lumotlar ko'rsatilgan bo'lsa, hatto foydalanishning o'zi maqbul bo'lishi mumkin bo'lgan hollarda ham da'vo uchun asos bo'ladi.

Atributsiyaning oltin qoidasi: **Muallif + manba + sana + havola (mavjud bo'lsa). Muallif/huquq egasining maxsus taqiqi mavjudligi.** Agar birlamchi manba qayta chop etish/nashr etishni to'g'ridan to'g'ri taqiqlasa (saytda, material oxirida, foydalanish shartlarida), joriy maqolalarni qayta chop etish bandi bo'yicha erkin foydalanishga tayanish mumkin emas.

Cheklangan hajmda iqtibos keltirish o'rniga qayta ishlash. Tarjima qilish, moslashtirish, montaj qilish, musiqa qo'shish, "hosila" kontent yaratish, hatto asl material axborot maqsadlarida cheklangan miqdorda ishlatilgan bo'lsa ham, alohida ruxsat talab qilishi mumkin.

MUHIM!

© kopirayt belgisini qo'yish, o'zlashtirilgan manbani ko'rsatish (masalan, boshqa OAV yoki sayt) yoki unga havola berish, shuningdek mualliflik asaridan notijorat maqsadda foydalanish mualliflar yoki huquq egalarining noqonuniy foydalanish bo'yicha da'volaridan ozod qilmaydi.

2.4.4. Mualliflik huquqlarini himoya qilish usullari

Agar muallif yoki huquq egasi o'z mualliflik huquqlari buzilgan deb hisoblasa, ularni himoya qilish uchun huquqbuzarga noqonuniy foydalanishni to'xtatish talabi bilan murojaat qilishga haqli (imkon qadar yozma shaklda). Agar huquqbuzar talablarni bajarishdan bosh tortsa, muallif (huquq egasi) fuqarolik sudiga (agar tomonlardan biri jismoniy shaxs bo'lsa) yoki iqtisodiy sudga (agar ikkala tomon ham yuridik shaxs bo'lsa) quyidagi talablar bilan da'vo arizasi kiritishga haqli:

- huquqlarni tan olish;
- huquqbuzarlik sodir etilishidan oldingi holatni tiklash va huquqni buzuvchi yoki buzish xavfini tug'diruvchi harakatlarni to'xtatish;
- huquq egasi odatdagi fuqarolik muomalasi sharoitida, agar uning huquqi buzilmaganida olishi mumkin bo'lgan daromad miqdoridagi zararlarni qoplash. Agar huquqbuzar mualliflik yoki turdosh huquqlarni buzish natijasida daromad olgan bo'lsa, huquq egasi boshqa zararlarni bilan bir qatorda ushbu daromaddan kam bo'lmagan miqdorda boy berilgan foydani undirishni talab qilishga haqli;
- zararlarni qoplash o'rniga, buzilish xususiyati va huquqbuzarning aybi darajasidan kelib chiqib hamda ishbilarmonlik muomalasi odatlarini hisobga olgan holda, yigirmadan mingtagacha bazaviy hisoblash miqdori miqdorida kompensatsiya to'lashni talab qilish. Ushbu kompensatsiya zarar yetkazilgan- yetkazilmaganidan qat'i nazar to'lanadi.

Muallif (yoki huquq egasi) o'z huquqlari buzilgan taqdirda huquqbuzardan ma'naviy zarar uchun kompensatsiya talab qilishga haqli. Qonunchilikda mualliflik huquqlarini buzganlik uchun ma'muriy va jinoiy javobgarlik ham nazarda tutilgan.

Javobgarlik turlari	Qachon qo'llanadi	Javobgarlik choralari
MJtK 177¹-moddasi. Mualliflik huquqi va turdosh huquqlarni buzish	Asarlardan yoki turdosh huquqlar obyektlaridan qonunga xilof ravishda foydalanish, xuddi shuningdek asarlarning yoki turdosh huquqlar obyektlarining kontrafakt nusxalarini ko'paytirish, tarqatish, barchaning e'tiboriga yetkazish Mulkiy huquqlar yoxud asarlar yoki turdosh huquqlar obyektlari nusxalarida ularni tayyorlaganlar, ishlab chiqarilgan joylari, shuningdek mualliflik huquqi va turdosh huquqlar egalari to'g'risida yolg'on ma'lumotlar ko'rsatish Nomulkiy huquqlar	Birlamchi qoidabuzarlik Fuqarolar uchun — BHMning 1 baravaridan 5 baravarigacha miqdorda jarima Mansabdor shaxslar uchun — BHMning 5 baravaridan 10 baravarigacha miqdorda jarima. Yil davomida takroriy qoidabuzarlik Fuqarolar uchun — BHMning 5 baravaridan 10 baravarigacha miqdorda jarima Mansabdor shaxslar uchun — BHMning 10 baravaridan 20 baravarigacha miqdorda jarima. Kontrafakt mahsulotlar, materiallar va uskunalar musodara qilinadi.

149-modda. Mualliflik yoki ixtirochilik huquqlarini buzish	Intellectual mulk obyektlariga nisbatan mualliflik huquqini o'zlashtirish, hammualliflikka majburlash, xuddi shuningdek ushbu obyektlar to'g'risidagi ma'lumotlarni ular rasman ro'yxatdan o'tkazilgunga yoki e'lon qilingunga qadar muallifning roziligisiz oshkor qilish	BHMning 50 baravaridan 70 baravarigacha jarima Muayyan huquqdan 5 yilgacha mahrum qilish 360 soatgacha bo'lgan majburiy ishlar 2 yilgacha ozodlikni cheklash
Nomulkiy huquqlar		
149¹-modda. Mualliflik huquqi va turdosh huquqlarni buzish	Asarlardan yoki turdosh huquqlar obyektlaridan qonunga xilof ravishda foydalanish, shuningdek asarlarning yoki turdosh huquqlar obyektlarining kontrafakt nusxalarini takrorlash, tarqatish, barchaning e'tiboriga yetkazish, ularning tayyorlovchilari, tayyorlangan joyi, shuningdek mualliflik huquqi va turdosh huquqlar egalari to'g'risidagi yolg'on ma'lumotlar bilan nusxalar tayyorlash, agar bu ancha miqdorda zarar yetkazgan bo'lsa	50 dan 100 BHMgacha jarima 2 yilgacha axloq tuzatish ishlari 2 yilgacha ozodlikni cheklash 2 yilgacha ozodlikdan mahrum qilish
Mulkiy huquqlar		

2.4.5. Raqamli muhitda mualliflik huquqi obyektlaridan foydalanishni cheklash mexanizmlari

O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi qonuni boshqa shaxslarga tegishli bo'lgan intellektual mulk obyektlaridan foydalanishni taqiqlaydi. Veb-saytning va (yoki) veb-sayt sahifasining yoxud boshqa axborot resursining egalari, shu jumladan blogerlar o'z veb-saytlaridan va (yoki) veb-saytlarining sahifalaridan yoxud Internet jahon axborot tarmog'idagi boshqalarning mualliflik asarlaridan huquq egasining roziligisiz foydalanilishiga yo'l qo'ymasliklari shart.

O'zbekiston Respublikasi Vazirlar Mahkamasining 2018-yil 5-sentyabrdagi "Internet jahon axborot tarmog'ida axborot xavfsizligini ta'minlashni takomillashtirish chora-tadbirlari to'g'risida"gi 707-sonli qarori (707-sonli qaror) mualliflik huquqini buzadigan, tarqatilishi cheklangan onlayn kontentni olib tashlash mexanizmini nazarda tutadi. 707-sonli qaror bilan Raqamli texnologiyalar vazirligi huzuridagi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo'yicha "O'zkomnazorat" inspeksiyasiga veb-saytlar va ijtimoiy tarmoqlardagi ma'lumotlarni o'chirish to'g'risida ko'rsatmalar berish vakolati berildi.

Huquq egasi (muallif) "O'zkomnazorat"ga mualliflik huquqi obyektlaridan noqonuniy foydalanish holatlari to'g'risida ariza bilan murojaat qilishga haqli. "O'zkomnazorat" veb-sayt, veb-sayt sahifasi yoki axborot resursi egasiga noqonuniy materiallarni 24 soat ichida olib tashlash zarurligi to'g'risida xabarnoma yuboradi.

**Agar axborot ko'rsatilgan muddatda o'chirib tashlanmasa,
"O'zkomnazorat" quyidagi choralarni ko'rish huquqiga ega:**



Tegishli ijtimoiy tarmoq yoki messenger ma'muriyatiga to'g'ridan-to'g'ri murojaat qilib, ma'lumotni o'chirishni talab qilish.



Noqonuniy materiallar joylashtirilgan veb-sayt yoki veb-sayt sahifasiga kirishni cheklash.



Platforma ma'muriyatiga nisbatan taqiqlangan kontentni olib tashlash talabi bilan sudga da'vo arizasi bilan murojaat qilishingiz mumkin.

Raqamli muhitda mualliflik huquqlari buzilganligi to'g'risidagi ariza intellektual mulk sohasidagi nizolarni sudgacha ko'rib chiqish bo'yicha vakolatli organ — O'zbekiston Respublikasi Adliya vazirligining Intellektual mulk departamentiga yuborilishi mumkin.

2.4.6. Ijtimoiy tarmoqlar va raqamli platformalarda mualliflik huquqlarini himoya qilish mexanizmlari

Internetda huquqbuzarliklar ommaviy ravishda sodir bo'ladi va oflayn muhitdan farqli o'laroq, katta xarajatlarni talab qilmaydi. Eng ko'p uchraydigan qoidabuzarliklar — birovning mualliflik kontentini noqonuniy nusxalash va tarqatish, plagiat, asarlarni qayta ishlash va ulardan tijorat maqsadlarida foydalanishdir.

Aksariyat raqamli platformalar va ijtimoiy tarmoqlar mualliflik huquqi buzilishi haqida shikoyat qilish mexanizmini taqdim etadi. Mualliflik huquqi egalari kontent joylashtirilgan sayt yoki platforma egasiga da'vo yuborishi va mualliflik huquqi buzilishi haqida bildirishnoma yuborishi mumkin.

Shikoyat platforma tomonidan taqdim etilgan shakl orqali yuboriladi va quyidagi ma'lumotlarni ko'rsatishni talab qiladi:

- birovning mualliflik asarlari joylashtirilgan havolalar
- muallif yoki huquq egasining mualliflik huquqi obyektiga bo'lgan huquqlarini tasdiqlovchi hujjat (mualliflik shartnomasi, mualliflik huquqini ro'yxatdan o'tkazish to'g'risidagi guvohnoma)
- muallif va mualliflik huquqi egasining aloqa ma'lumotlari
- agar shikoyat huquq egasining vakili tomonidan taqdim etilayotgan bo'lsa, ishonchnoma.

Qidiruv tizimlarida matn yoki tasvir bo'yicha qidiruv, ijtimoiy tarmoqlar monitoringi, havolalar va eslatmalarni tekshirish yoki o'xshash mavzudagi saytlarni ko'rib chiqish mualliflik huquqi buzilishlarini aniqlash imkonini beradi.

Huquqbuzarliklarni aniqlashda yordam beradigan ayrim maxsus avtomatlashtirilgan vositalar mavjud:

Google Image Search

internetdagi tasvir nusxalarini qidirish imkonini beruvchi bepul vosita.

Copyscape

matnli materiallarda plagiatni aniqlash uchun xalqaro servis. Kengaytirilgan imkoniyatlarga ega bepul va pullik versiyalari mavjud.

Pixsy

tasvir bo'yicha qidiruv funksiyasiga ega fotosuratlar platformasi.

2.5. Raqamli muhitda jurnalistlar va media kasbiy faoliyatining axloqiy jihatlari

Raqamli muhit jurnalistik materiallarning ta'sirini kuchaytiradi. Internetdagi nashrlar bir zumda tarqaladi, cheklanmagan auditoriyaga taqdim etiladi va osongina nusxalanadi. Raqamli muhit algoritmlari nizolar, ta'qiblar va nozik kontentning tarqalishiga OAV tahririyati javob berishga ulgurmasdan tezroq sabab bo'lishi mumkin. Onlayn muhitda axloqiy qoidalar xavflarni kamaytirish va axborot manbalariga ishonchni saqlab qolishning amaliy vositasidir.

Jurnalistlarning kasbiy odob-axloq tamoyillari bir nechta asosiy jihatlarni o'z ichiga oladi:

Haqqoniylik va ishonchlilik:

Jurnalistlar haqqoniy va ishonchli ma'lumotlarni yetkazishga intilishlari lozim.



Mustaqillik:

Jurnalistlar siyosiy, iqtisodiy yoki boshqa manfaatlar ta'siridan mustaqil bo'lishlari kerak.



Adolatlilik va muvozanat:

Jurnalistlar axborotni adolatli va muvozanatli tarzda taqdim etishga intilishlari kerak.



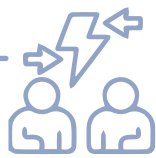
Maxfiylik va shaxsiylikni himoya qilish:

Jurnalistlar axborot manbalarining maxfiyligini va odamlarning shaxsiy hayotini hurmat qilishlari shart.



Manfaatlar to'qnashuvidan qochish:

Jurnalistlar manfaatlar to'qnashuviga olib kelishi mumkin bo'lgan holatlardan qochishlari kerak.



Jurnalistik etika jurnalistlardan halol, aniq va xolis bo'lishni talab qiladi.



Ijtimoiy tarmoqlar va shaxsiy fikr bildirish

Tamoyil: jurnalist ijtimoiy tarmoqlarda ham jurnalist bo'lib qoladi. Hatto shaxsiy akkaunt ham auditoriya tomonidan professional jurnalist va/yoki tahririyat pozitsiyasi sifatida qabul qilinishi mumkin.

O'zbekiston jurnalistlarining kasb etikasi kodeksida kasbning asosiy yo'nalishlari: halollik, xolislik, adolatlilik, fikrlar xilma-xilligi va inson huquqlarini hurmat qilish mustahkamlangan; shuningdek, axborotning aniqligini tekshirish va xatoni tezda tan olish, uzr so'rash va uni tuzatish majburiyati ta'kidlangan.



Amaliy tavsiyalar:

- **Fakt va bahoni ajrating.** Agar siz fikr bildirayotgan bo'lsangiz — uni fikr/kolonka/izoh sifatida belgilang, faktik qismni esa manbalar bilan tasdiqlang.
- **Nafrat tilidan qoching.** Ijtimoiy tarmoqlardagi sarkazm va hissiyotlar "klikbop" bo'lishi mumkin, ammo ular bosim o'tkazishi va auditoriyani ta'qibga undashi mumkin.
- **Manfaatlar to'qnashuvi shaffofligi.** Agar siz shaxsiy manfaat mavjud mavzu haqida yozayotgan bo'lsangiz (qarindoshlik, hamkorlik, loyiha ishtiroki) — buni to'g'ri ochiqdang.
- **Xato yoki noaniqliklarni tuzating.** Tuzatishlarni alohida izoh/post bilan, qaysi xato yoki noaniqlik bo'lganini ko'rsatgan holda kiriting.
- **Alohida guruhlarining manfaatlari va zaifligini hisobga oling.** Asosiy prinsip: "zarar yetkazma". Raqamli savodxonligi past odamlar (jumladan bolalar, keksalar, nogironligi bo'lgan shaxslar), shuningdek zaif holatdagi insonlar ko'pincha post, repost yoki ikkilamchi tarqatish oqibatlarini anglamaydilar.



Kiberbullingga yo'l qo'ymaslik va medianing raqamli muhit uchun javobgarligi

Kiberbulling ko'pincha jurnalistlarga, ayniqsa ayollarga tahdid, haqorat va doksing shaklida ta'sir ko'rsatadigan tizimli onlayn bezorilikdir. O'zbekiston va Markaziy Osiyoda bu muammo maxsus qonunchilikning yo'qligi tufayli yanada kuchaymoqda, ammo jurnalistika uni yoritish va unga qarshi kurashda asosiy rol o'ynaydi. Jurnalistlarning o'zlari qurbon bo'lishadi, bu esa o'z-o'zini senzura qilish va ruhiy bosimga olib keladi.

Kiberbulling haqoratlar, tahdidlar, shaxsiy ma'lumotlar va ijtimoiy tarmoqlarda soxta akkauntlarni tarqatishni o'z ichiga oladi va oflayn bullingdan 24 soat davom etishi bilan farq qiladi. UNESCO ma'lumotlariga ko'ra, jurnalistlar 73 foiz hollarda, shu jumladan gender zo'ravonligiga duch kelishadi.

O'zbekistondagi kiberbullingni yorituvchi jurnalistlar, ayniqsa jabrlanuvchilar, ko'pincha ayollar bilan ishlaganda, ikkilamchi jarohatlanishning oldini olish uchun gender sezgirligini hisobga olishlari muhim. Xavfsizlik mahalliy OAV qonunlarini hisobga olgan holda manbalarni anonimlashtirish, huquqiy himoya va texnik vositalarni o'z ichiga oladi. Bu choralar o'zi va jabrlanuvchilar uchun xavflarni kamaytirishga yordam beradi.



Amaliy tavsiyalar:

- **Moderatsiya va izohlar qoidalari**
Tushunarli qoidalarni e'lon qiling (tahdid, haqorat, doksing, nafratomuz nutqni taqiqlash), qoidabuzarliklarni kuzatib boring va qayd eting.
- **Ta'qibni kuchaytirmaslik**
Agar material qahramoni allaqachon hujumga uchragan bo'lsa, shaxsni aniqlashga yordam beradigan shaxsiy ma'lumotlarni e'lon qilishdan saqlaning.
- **Xodimlarni himoya qilish**
Kiberbulling holati uchun ichki siyosatni ishlab chiqish zarur: tahdidlarni baholash, dalillarni qayd etish, huquqni muhofaza qilish organlariga murojaat qilish.



Nozik kontent: o'z joniga qasd qilish, o'ziga jarohat yetkazish, og'ir zo'ravonlik, travmatik hodisalar

O'z joniga qasd qilish (suitsidlar)ni yoritish bo'yicha tadqiqotlar shuni ko'rsatadiki, ayrim yoritish usullari taqlid qilish xavfini oshirishi mumkin, aksincha inqirozni yengib o'tish haqidagi hikoyalar va to'g'ri materiallar profilaktikaga yordam beradi. Jahon sog'liqni saqlash tashkiloti jurnalistlarga suitsid mavzusini yoritishda "Do's and Don'ts" tavsiyalariga amal qilishni tavsiya qiladi.

Tavsiya etiladi:

- ehtiyotkor va neytral yozish, sensatsiya va klikbop usullardan qochish;
- voqeani "afsona-hikoya"ga aylantirmaslik va romantizatsiya qilmaslik;
- foydali ma'lumot berish: qayerga yordam uchun murojaat qilish, yaqinlar nima qilishi kerakligi;
- imkon qadar profilaktika va yordamga urg'u berish, jumladan yordam so'rash va inqirozni yengib o'tish haqidagi hikoyalarni yoritish.

Tavsiya etilmaydi:

- suitsid usuli, tafsilotlari, joyi haqida yozish;
- voqea joyidan foto/video, xayrlashuv xatlari yoki "oxirgi xabarlar"ni e'lon qilish;
- keskin sarlavhalar, stigmatizatsiya va drammatizatsiyadan foydalanish.

Ommaviy axborot vositalari uchun amaliy standart

Agar materialda o'z joniga qasd qilish yoki o'ziga jarohat yetkazish holatlari tilga olingan bo'lsa, maxfiy kontent haqida ogohlantirish va yordam xizmatlari (mahalliy rasmiy psixologik yordam xizmatlari, ishonch telefonlari) ma'lumotlarini qo'shish, shuningdek, qo'zg'atuvchi bo'lishi mumkin bo'lgan har qanday tafsilotlardan qochish.



2.6. Onlayn media uchun siyosatlar

Onlayn nashr tahririyati uchun huquqiy xatarlar ham raqamli media kontentni yaratish, ham ushbu media kontent tarqatiladigan kanallar bilan bog'liq. Ko'pincha media biznesning muvaffaqiyatli rivojlanishi uchun zarur bo'lgan barcha xavf-xatarlar va chora-tadbirlar yozma hujjatlarda — maxsus siyosatlarda aks ettiriladi, ularni faqat tahririyat ichida ishlab chiqish va yozma ravishda qabul qilish, e'lon qilish yoki foydalanish tavsiya etiladi.

Quyidagi jadvalda media-biznesning o'ziga xos xususiyatlaridan kelib chiqqan holda, onlayn nashr tahririyati uchun media-kontent yaratish va uni raqamli muhitda tarqatish bo'yicha siyosatlarning minimal ro'yxati (jami 5 ta siyosat) keltirilgan.



Tashqi siyosat (ommaviy hujjatlar, nashr veb-saytida e'lon qilinishi kerak)

1. Materiallardan foydalanish qoidalari
2. Shaxsiy ma'lumotlar siyosati
3. Foydalanuvchilar (obunachilar) uchun fikr bildirish qoidalari



Ichki siyosat (e'lon qilinmaydi, ammo tahririyat xodimlari uchun majburiy)

1. Tahririyat kontentini noqonuniy foydalanishdan himoya qilish siyosati
2. Tahririyatning ichki ish tartibi

Quyida O'zbekistonda onlayn nashrning ishlashi kontekstida har bir siyosatning qisqacha tavsifi va nima uchun bunday siyosatni ishlab chiqish va qabul qilish kerakligi keltirilgan.

2.6.1. Onlayn nashr materiallaridan (kontentdan) foydalanish qoidalari

Ushbu siyosatning maqsadi onlayn nashr tahririyati turli platformalar va kanallar orqali yaratilayotgan hamda tarqatilayotgan kontentning mualliflik huquqi egasi ekanligini ochiq e'lon qilishdir. Bu siyosat, shuningdek, mualliflik huquqi egasining (tahririyatning) ruxsatisiz, lekin muayyan shartlarga rioya qilgan holda o'z kontentidan foydalanish bo'yicha huquq egasining pozitsiyasini (ruxsatini) belgilaydi:

- Iqtibos keltirish holatlarida — onlayn nashr tahririyati tomonidan belgilangan iqtibos hajmiga rioya qilish (matnning 30% dan oshmasligi, birinchi xatboshi va hokazo), shuningdek, birlamchi manbaga gipermurojaat qilish va hokazo.
- Illyustratsiyalar, mualliflik fotosuratlaridan foydalanish holatlarida — fotosurat muallifi ko'rsatilishi shart bo'lgan holda e'lon qilinishi mumkin bo'lgan fotosuratlar yoki boshqa vizual materiallar soni va hokazo.
- Dayjestlar va sharhlarda foydalanilgan hollarda — onlayn nashr tahririyati tomonidan belgilangan iqtiboslar hajmiga rioya qilish (matnning 30% dan oshmasligi, birinchi xatboshi va hokazo), shuningdek, birlamchi manbaga gipermurojaat qilish va hokazo.

Shuningdek, ushbu siyosat UGC (foydalanuvchi kontenti; foydalanuvchilar tomonidan yaratilgan kontent) dan foydalanish tartib-qoidalarini, jumladan, foydalanuvchidan e'lon qilish uchun rozilik olish, foydalanuvchining yuborilgan materiallarga bo'lgan huquqlari uchun javobgarligi, uchinchi shaxslarning murojaati bo'yicha UGCni olib tashlash tartibini belgilaydi.

Siyosat internet, ijtimoiy tarmoqlar, messenjerlardan olingan materiallardan foydalanish bo'yicha asosiy tamoyillarni o'z ichiga oladi va huquqlarni tekshirmasdan "Internetdan olingan" matnli va audiovizual materiallardan foydalanishni taqiqlaydi.

2.6.2. Shaxsiy ma'lumotlar siyosati

Siyosatning maqsadi — sayt foydalanuvchilari, obunachilari va boshqalarning shaxsiy ma'lumotlarini qonuniy ravishda to'plash va ulardan foydalanish. Siyosat quyidagi ma'lumotlarni o'z ichiga olishi kerak:

Qanday ma'lumotlar to'planishi (ro'yxatdan o'tish, tarqatma xabarlar, sharhlar, arizalar, cookies/tahlil, mahsulot sotish, xayriya aksiyalarini o'tkazish davrida shaxsiy ma'lumotlarni to'plash va boshqalar);

Qayta ishlash maqsadlari, saqlash muddatlari, qabul qiluvchilar toifalari;

Murojaatlar uchun mas'ul shaxs/kanalning aloqa ma'lumotlari;

Ma'lumotlar subyektini himoya qilish choralari va huquqlari.

2.6.3. Fikr bildirish va moderatsiya qoidalari

Ushbu siyosatning maqsadi auditoriya uchun talablarni (red flags) oldindan belgilash va nashrning izohlari va sahifalarida taqiqlangan, tuhmat qiluvchi, yolg'on ma'lumotlarni tarqatganlik uchun javobgarlik xavfini kamaytirishdir.

Bunday siyosat quyidagi ma'lumotlarni o'z ichiga olishi lozim:

- Taqiqlangan (noqonuniy) va nozik kontent (nafrat tili/kamsitish, zo'ravonlikka chaqirish, ekstremistik materiallar, pornografiya, shaxsiy ma'lumotlarni oshkor qilish, tahdidlar, ta'qib qilish, ochiqdan-ochiq yolg'on ma'lumotlar, boshqa qonunbuzarliklar).

- Tahririyat izohlarni qanday nazorat qilishi (oldindan moderatsiya yoki moderatsiyadan keyin), bloklash, o'chirish, muhokamalarni cheklash qoidalari.
- Qoidabuzarliklar haqida xabar berish tartibi (qoidabuzarliklar haqida qanday xabar berish va bu yetarli asos deb hisoblanishi)
- Nashrning ijtimoiy tarmoqlar va messenjerlardagi sayti va akkauntlari uchun yagona qoidalar.

Nima uchun bunday siyosat onlayn nashrlar tahririyatlari uchun muhim? O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni veb-sayt va (yoki) veb-sahifa egalari (jumladan ijtimoiy tarmoqlar va messenjerlarda joylashtirilgan sahifalar) uchun resursdan taqiqlangan maqsadlarda foydalanishga yo'l qo'ymaslik va taqiqlangan axborotni o'chirish majburiyatini to'g'ridan-to'g'ri belgilaydi. Qoidabuzarlik holatlarida resursga kirishni cheklash imkoniyati mavjud⁴³.

2.6.4. Tahririy kontentni noqonuniy foydalanishdan himoya qilish siyosati

Bu ichki siyosat bo'lib, uni saytda e'lon qilish shart emas. Biroq tahririyatning barcha xodimlari ushbu siyosat qoidalarini bilishi va amalda qo'llashi kerak. Ushbu siyosatning maqsadi — tahririyat xodimlari tahririy kontentdan noqonuniy foydalanish holatlarini aniqlaganida qanday harakat qilish algoritmini belgilashdir. Boshqacha aytganda, tahririyat materiallari ruxsatsiz nusxalanib foydalanilganda xodimlar nima va qanday qilishini ko'rsatadi.

Bunday faktlar doimo ko'p — matnlar, fotosuratlar, audiovizual materiallardan boshqa ommaviy axborot vositalari, bloggerlar, pabliklar, telegram-kanallar tomonidan qisman yoki to'liq noqonuniy foydalanilishi mumkin. Agar materiallaringiz noqonuniy ishlatilsa, tomoshalar, noyob tashrif buyuruvchilar va shunga mos ravishda reklama daromadlarini yo'qotasiz.

Bunday siyosatda quyidagi minimal qoidalar bo'lishi kerak:

- Kontentingizdan noqonuniy foydalanish holatlarini aniqlash va kuzatish uchun qaysi servislar ishlatilishi (matn, foto, audio va video materiallar).
- Qoidabuzarliklarni qanday qayd etish kerakligi: havolalar, skrinshotlar, chop etilgan sana va vaqt, HTML yoki videoni saqlash, kontentdan noqonuniy foydalanayotgan shaxs haqidagi ma'lumotlarni saqlash.
- Sudgacha bo'lgan tartibda hal qilish choralari: ogohlantirish yuborish, o'chirish yoki foydalanishni qonuniylashtirish talabi.
- Agar sudgacha bo'lgan tartib natija bermasa, sud orqali himoya qilish bo'yicha harakatlar.

Ushbu siyosat qoidalari va barcha harakat algoritmlari tahririyatning barcha xodimlariga yaxshi ma'lum bo'lishi kerak.

⁴³ O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni.

2.6.5. Tahririyatning ichki ish tartibi

Ushbu siyosat tahririyatda ichki foydalanish uchun mo'ljallangan, nashr etish uchun emas. Mazkur siyosatning maqsadi — tahririyat kontentini tayyorlash va tarqatish bo'yicha standartlarni hamda kontent uchun javobgarlik xavfini imkon qadar kamaytirish maqsadida minimal huquqiy tartib-qoidalarni joriy etishdan iborat.

Bunday siyosat quyidagi qoidalarni o'z ichiga olishi mumkin:

- Tahririy kontent yaratish bosqichlari — yangiliklar, longridlar, audio va vizual kontent, auditoriyani jalb qilish aksiyalari.
- Nashr qilishdan oldingi majburiy tekshiruvlar (faktcheking, manbalar, diffamatsiya xavflari, shaxsiy ma'lumotlar, mualliflik huquqlari, reklama belgilanishi).
- Materiallarni o'zgartirish, yangilash va arxivlash tartibi.
- Rasmiy murojaatlar va so'rovlar bilan ishlash qoidalari (kim qabul qiladi, kim javob beradi, qanday qayd etiladi).
- Sayt va akkauntlarga kirishni boshqarish, parollar va ikki bosqichli autentifikatsiya talablari, jurnalistlar va boshqa tahririyat xodimlarining raqamli va jismoniy xavfsizligi bo'yicha boshqa choralar.

Sizga ushbu beshta siyosatni zamonaviy onlayn-media tahririyati faoliyatini ta'minlaydigan minimal hujjatlar to'plami sifatida ishlab chiqish, qabul qilish va joriy etishni tavsiya etamiz.

3-bo'lim

Raqamli muhitda jurnalistlar va tahririyatlar uchun tahdidlar

3.1. Asosiy tahdidlar

So'nggi o'n yillikda raqamli makon rivojlanishi bilan fuqarolik jamiyati uchun qanday tahdidlar ustuvor ekaniga doir qarashlarda tub burilish yuz bermoqda. Agar ilgari asosiy e'tibor jismoniy tahdidlarga qaratilgan bo'lsa, bugungi kunda kurashning oldingi chizig'i virtual tus olib, smartfonlarimiz, noutbuklarimiz va bulutli xotiramiz orqali o'tmoqda. Biz "oyina uy" davrida yashayapmiz: g'oyalarni tarqatish va tarafdorlarni jalb qilishga yordam beradigan raqamli shaffoflik hamda "hamma joyda mavjudlik" bizni ayni shu faoliyatimizga to'sqinlik qilmoqchi bo'lganlar oldida o'jiz qilib qo'yadi.

Jurnalistlar va tahririyat xodimlari uchun raqamli tahdidlar manzarasini anglash shunchaki "ma'lumot uchun" olinadigan narsa bo'lmay qoldi. Endi bu omon qolish, erkinlik va obro'ni saqlash masalasidir. "Mening yashiradigan hech narsam yo'q" yoki "menga qiziqish uchun juda kichik odamman" degan xayol — o'ta xavfli yanglishishdir. Zamonaviy ommaviy kuzatuv tizimlarida (DPI, yuzni tanish, katta hajmdagi ma'lumotlar tahlili) "ahamiyatsiz" nishonlarning o'zi yo'q; mo'ljalga har kim tushishi mumkin.

Onlayn tahdidlar va oflayn oqibatlar o'rtasidagi chegara yo'qolganini anglash o'ta muhimdir. Elektron pochtaning buzilishi shunchaki texnik nosozlik emas, balki keng doiradagi shaxslarga ta'sir qiladigan va uzoq davom etadigan oqibatlarga ega bo'lgan jiddiy xavfsizlik hodisasidir. Geolokatsiya metama'lumotlariga ega fotosurat yopiq uchrashuv ishtirokchilariga nisbatan jismoniy hujumga sabab bo'lishi mumkin. Kiberbulling va dezinformatsiya kompaniyalari esa odamlarning toliqishiga va tashkilotlar faoliyatining to'xtashiga olib keladigan haqiqiy ruhiy jarohatlar yetkazadi.

Ko'pgina tashkilotlar raqamli xavfsizlikni antivirus sotib olish kabi qabul qiladi: o'rnatdim — unutdim. Bu esa soxta xotirjamlik hissini uyg'otadi. Biroq haqiqiy himoya mexanizmi boshqacha quriladi. U tahdidlar manzarasini (kontekst, tashqi muhit), hujum vektorlarini (tahdidlar amalga oshirilishi mumkin bo'lgan yo'llarni) anglashni hamda o'z raqamli resurslari va ularning zaif tomonlarini aniq tasavvur qilishni talab etadi. Aynan shu bilimlar poydevorida tashkilotning barqaror xavfsizlik holati (security posture) shakllanadi. Bu shunday holatki, unda xavfsizlikni ta'minlash bir martalik harakat emas, balki uzluksiz jarayonga aylanadi.

Biroq zamonaviy raqamli dunyoda o'z raqamli aktivlarini himoya qilishning texnik vositalarini sozlashning o'zi kifoya qilmaydi. Hozirgi kunda xavfsizlikka nisbatan raqamli, jismoniy va psixosoztimoiy xavfsizlikni bir-biridan ajralmas deb biladigan xolistik (yaxlit) yondashuv tobora ommalashib bormoqda. Ular yagona ekotizimni hosil qiladi: bir sohadagi zaiflik boshqa sohalardagi himoyani ham muqarrar ravishda izdan chiqaradi.

Masalan:



Psixologik bosim

(tahdidlar, shantaj) xodimning hissiy toliqishiga olib keladi.



Hissiy toliqqan xodim

hushyorlikni yo'qotadi va fishing yoki ijtimoiy muhandislikning **(raqamli zaiflik)** osongina qurboniga aylanadi.



Raqamli resurslarning buzib kirilishi

nozik shaxsiy ma'lumotlarni (jinsiy orientatsiya, OIV maqomi va hokazo) fosh qiladi, bu esa manbalarning **jismoniy xavfsizligiga** bevosita tahdid tug'diradi.



Ma'lumotlarning sizib

chiqishi davlat tomonidan huquqiy sanksiyalar qo'llanilishiga, obro'ga putur yetishiga, auditoriya va reklama beruvchilarning ishonchi yo'qolishiga va natijada moliyaviy yetishmovchilikka hamda tashkilot faoliyatining yopilishiga olib keladi.

Shu sababli, ushbu to'plamda tahdidlar alohida emas, balki birgalikda ko'rib chiqiladi, bunda inson har qanday xavfsizlik tizimidagi asosiy aktiv va bir vaqtning o'zida hujumning asosiy vektori ekanligiga e'tibor qaratiladi.

Qulaylik uchun biz tahdidlarni ta'sir doirasiga ko'ra bir necha toifalarga ajratishimiz mumkin: texnik, jismoniy, huquqiy, ruhiy-ijtimoiy, iqtisodiy hamda insoniy va tashkiliy xarakterdagi tahdidlar. Bo'linish yetarlicha shartli, chunki aksariyat tahdidlar gibridd bo'lib, ularni turli toifalarga mansub tarkibiy qismlarga ajratish mumkin, masalan, "xorijiy agentlar" to'g'risidagi qonunlar bir vaqtning o'zida bir nechta toifaga bo'linadi: huquqiy — bu javobgarlik yuzaga keladigan shartlarni belgilaydigan qonun; iqtisodiy — tashkilotlarning moliyaviy barqarorligini xavf ostiga qo'yadi; ruhiy-ijtimoiy — xorijiy agent ta'rifi ostida qolganlarni kamsitadi; tashkiliy — tashkilotga qo'shimcha hisobotlar va belgilar shaklida qo'shimcha ma'muriy yuk yuklaydi; va texnik — talablarga rioya qilmaslik akkauntlar, saytlar va domenlarning bloklanishiga olib kelishi mumkin. Bunda tahdidni kim ko'rib chiqayotganiga qarab, ko'rib chiquvchiga yaqin bo'lgan toifa birinchi o'ringa chiqadi: huquqshunos uchun — huquqiy, moliyachi uchun — iqtisodiy, direktor uchun — operatsion, raqamli xavfsizlik bo'yicha mutaxassis uchun — texnik. Ushbu qo'llanmada biz tahdidlarning raqamli tarkibiy qismiga e'tibor qaratamiz va ularni aynan shu nuqtai nazardan baholaymiz.



1. Texnik tahdidlar —

raqamli infratuzilma, qurilmalar va ma'lumotlarning ishlashini buzish, ularni xavf ostiga qo'yish yoki ularga ruxsatsiz kirishga qaratilgan tahdidlar)

- **Ma'lumotlarni yig'ish va razvedka qilish (OSINT)** — to'g'ridan-to'g'ri tahdid emas, lekin ko'pincha maqsadli hujumning dastlabki bosqichi bo'lib, texnikadan tortib psixologik-ijtimoiygacha bo'lgan turli xil zaifliklarni aniqlash uchun ochiq ma'lumotlarni tahlil qilishni o'z ichiga oladi.
- **Zararli dasturlar** (josuslik dasturlari, shifrllovchi viruslar) bilan zararlanish eng keng tarqalgan kibertahdid bo'lib, u, masalan, ma'lumotlarni shifrlaydigan va to'lov talab qiladigan ommaviy viruslarni ham, qurilmani masofadan turib to'liq boshqarishni ta'minlaydigan murakkab josuslik dasturlari (masalan, Pegasus, Predator va boshqalar) yordamida maqsadli hujumlarni ham o'z ichiga oladi.

- **Raqamli akkauntlarni buzish** — elektron pochta, ijtimoiy tarmoqlar, messenjerlar va moliyaviy akkauntlarga ruxsatsiz kirish bilan bog'liq barcha holatlarni qamrab oladi. Asosan fishing, ijtimoiy muhandislik va sizib chiqqan parollar orqali amalga oshiriladi. Natija — aloqa kanallari va obro' ustidan nazoratni yo'qotish.
- **Veb-saytlarga hujumlar (DDoS, saytlarni buzish)** — tashkilotning ommaviy resurslariga qilingan to'g'ridan-to'g'ri hujumlar. DDoS hujumining maqsadi — resursni so'rovlar bilan ortiqcha yuklab, auditoriya uchun ishlamas holatga keltirish. Saytni buzishdan maqsad esa odatda kontentni almashtirish (deface), ma'lumotlarni o'g'irlash yoki zararli kod joylashtirishdir.
- **Himoyalanmagan tarmoqlarda ma'lumotlarni ushlab qolish** — jamoat joylarida (kafe, aeroportlar) o'zingiz nazorat qilmaydigan Wi-Fi nuqtasidan foydalanganda yuzaga keladigan dolzarb tahdiddir. Bunday holda tajovuzkor shifrlanmagan trafikni, jumladan, login va parollarni qo'lga kiritishi mumkin. Xuddi shu xavf shifrlashdan foydalanmaydigan (http protokoli) saytlarga kirganda ham mavjud bo'lib, bu haqda odatda brauzer va ba'zi antiviruslar ogohlantiradi.
- **Kompromat ma'lumotlarni** ataylab tarqatish — bu juda kam uchraydigan, biroq xavfli tahdid. Hujumchi qurilmaga kirish huquqini qo'lga kiritib, ma'lumotlarni o'g'irlash o'rniga, unga noqonuniy kontentni (ekstremistik materiallar, pornografiya va boshqalar) joylashtiradi. Maqsad — keyinchalik obro'sizlantirish yoki jinoiy ta'qib uchun asos yaratish.
- **Ta'minot zanjiriga hujumlar (Supply Chain Attacks) — bu tobora ommalashib borayotgan tahdid** bo'lib, unda sizga to'g'ridan-to'g'ri emas, balki ishonchli hamkoringizga (masalan, veb-saytingiz ishlab chiqaruvchisiga, dasturiy ta'minot ta'minotchisiga yoki kompyuter xizmatiga) hujum qilib, ularning tizimlari orqali infratuzilmangizga kirish mumkin.



2. Psixosotsial tahdidlar — bu faolning shaxsiyatiga, uning obro'siga, ruhiy holatiga va ijtimoiy aloqalariga nisbatan axloqni buzish va faoliyatini to'xtatish maqsadida qaratilgan tahdidlardir

- Muvofiqlashtirilgan onlayn tazyiq va dezinformatsiya kampaniyalari (Kiberbulling, trollar fabrikalari) — obro'ni to'kish maqsadida sharhlar, ijtimoiy tarmoqlar va boshqa manbalarda uyushtirilgan ommaviy hujumlar, haqorat, tahdid va yolg'on ma'lumotlarni, jumladan, dipfeyklar yordamida tarqatishdir.
- Doksing — raqamli tahdidni haqiqiy jismoniy xavfga aylantirish va faolni qo'rqitish maqsadida shaxsiy ma'lumotlarni (manzillar, telefon raqamlari, qarindoshlar ma'lumotlari) to'plash va ommaviy ravishda e'lon qilish.
- **Sekstorshn (sextortion), porno qasos va seks josuslik** — bu intim xarakterdagi materiallar (haqiqiy yoki sun'iy intellekt yordamida soxtalashtirilgan) orqali shantaj qilishga asoslangan tahdidlar bo'lib, ular ayniqsa konservativ jamiyatlarda faol ayollarga qarshi keng qo'llanadi.



3. Huquqiy va tartibga solish tahdidlari — qonunchilik, davlat institutlari va huquqiy tizimdan bosim, senzura va ta'qib vositasi sifatida foydalanadigan tahdidlar

- Repressiv qonunchilikni qo'llash ("feyklar," "tuhmat," "ekstremizm" to'g'risida) — internetda e'lonlar uchun ma'muriy va jinoiy ish qo'zg'atish uchun qonunlardagi noaniq ta'riflardan foydalanish tahdidi.
- "Xorijiy agentlar/vakillar" to'g'risidagi qonunlarning qo'llanilishi gibrid tahdid bo'lib, u o'z mohiyatiga ko'ra huquqiy hisoblanadi, ammo bevosita iqtisodiy, ruhiy-ijtimoiy va operatsion oqibatlariga ega.
- Davlat organlari talabiga ko'ra onlayn resurslarni bloklash yoki o'chirish — kontentni senzura qilish bo'yicha suddan tashqari yoki sud qarori tufayli saytni, ijtimoiy tarmoqdagi sahifani bloklash yoki kontentni o'chirish tahdidi.
- Platformalarning huquqiy mexanizmlarini suiiste'mol qilish (DMCA hujumlari) — mualliflik huquqi shikoyatlari, ijtimoiy tarmoqlardagi rasmiy kanallar orqali kontent, messenjerlar kabi platformalarning qonuniy vositalaridan noqonuniy maqsadlarda foydalanish (tovlamachilik, senzura).
- Davlat raqamli nazorati (SORM, DPI, yuzni tanib olish) — SORM, DPI, yuzni tanib olish tizimlari va biometriya kabi rasmiy-qonuniy vositalarni suiiste'mol qilishning bilvosita tahdidi, e'lon qilingan maqsadlardan (masalan, terrorizm yoki og'ir jinoyatlarga qarshi kurash) ancha tashqarida bo'lgan ommaviy va maqsadsiz ma'lumotlarni to'plash uchun raqamli profillarni yaratish.



4. Iqtisodiy tahdidlar — asosan gibrid tahdidlar bo'lib, ularning asosiy maqsadi yoki mexanizmi tashkilotning moliyaviy barqarorligiga bevosita ta'sir ko'rsatishdir

- **To'g'ridan-to'g'ri raqamli firibgarlik va mablag'larni o'g'irlash** — buzish yoki ijtimoiy muhandislik orqali moliyaviy hisoblarga ruxsatsiz kirish
- **Bank hisobvaraqlari va moliyaviy operatsiyalarni blokirovka qilish** — rasmiy huquqiy bahona bilan (masalan, da'voni ta'minlash bo'yicha iltimosnomani ta'minlash doirasida) boshlanishi mumkin bo'lgan harakat.
- Fandrayzing yoki kraudfandingga qarshi hujumlar to'g'ridan-to'g'ri firibgarlik, masalan, klon veb-saytlarni yaratish, xayriya mablag'larini qo'lga kiritish yoki bilvosita, sun'iy ravishda moliyalashtirishni qo'lga kiritadigan raqobatchi loyihalarni yaratish kabi ko'rinishlarga ega bo'lishi mumkin.
- **Ikkilamchi sanksiyalar yoki qo'shimcha zarar tahdidi** — bu xalqaro banklar, IT-kompaniyalar, donorlar va platformalar sanksiyalar rejimini buzishdan qo'rqib, sanksiyaga yaqin bo'lgan butun mintaqa bilan ishlashni butunlay to'xtatishi yoki cheklashi, bu esa bank operatsiyalari, hisob raqamlari bloklanishiga, xizmatlar cheklanishiga olib kelishi mumkin bo'lgan "muvofiglikdan tashqari" tahdid.



5. Inson omili va tashkiliy tahdidlar — ichki jarayonlardagi kamchiliklar, inson omili, shuningdek, qurilmalarning jismoniy xavfsizligi tufayli yuzaga keladigan tahdidlar

- **Xodimlarning tasodifiy xatolari va zaifliklari** — beparvolik, raqamli savodsizlik va toliqish kabi tahdidlarni birlashtiradi. Charchagan, o'qitilmagan yoki g'ayratsiz xodim — bu ko'plab texnik va ruhiy-ijtimoiy tahdidlar (masalan, fishing) amalga oshiriladigan zaiflikdir.
- **Ichkaridan qasddan qilingan dushmanlik harakatlari (insayderlar)** — xodim yoki ko'ngillilardan kelib chiqadigan tahdid bo'lib, ular ataylab ishni buzadi, ma'lumotlarni oshkor qiladi yoki uchinchi shaxslarga kirish huquqini beradi.
- **Qurilmalar va ma'lumot tashuvchilarning jismoniy yo'qolishi, o'g'irlanishi yoki musodara qilinishi** — bu texnika ustidan jismoniy nazoratni yo'qotadigan barcha ssenariylarni birlashtiradi (taksida unutib qoldirilgan, o'g'irlangan, tintuv paytida musodara qilingan). Shifrlashsiz bu ma'lumotlarning to'liq chiqib ketishiga, zaxira nusxalarsiz esa ma'lumotlarning butunlay yo'qolishiga tengdir.

Tashqi tahdidlarni shunchaki sanab o'tishdan himoya strategiyasini ishlab chiqishga o'tish o'zimizga berishimiz kerak bo'lgan savollarni yanada kengaytirishni talab qiladi. Bu nafaqat "Kim yoki nima tahdid solishi mumkin?" degan savol, balki "Biz aynan nimani himoya qilyapmiz?" va "Bizning zaif tomonlarimiz qayerda?" degan savollar hamdir. Ko'pincha bizning nazoratimizdan tashqarida bo'lgan faqat tashqi omillarga e'tibor qaratish o'rniga, tashkilotning ichki muhitiga e'tibor qaratish lozim. Har qanday strategiyaning asosida tashkilot uchun qaysi aktivlar muhim ekanligini aniq tushunish yotadi. Media sektori uchun bu, birinchi navbatda, oshkor etilishi odamlarga bevosita zarar yetkazishi mumkin bo'lgan axborot va ma'lumotlar; qonuniylik poydevori bo'lib xizmat qiladigan obro' va jamoatchilik ishonchi; farovonligi ish qobiliyatining sharti bo'lgan jamoa; va tashkilotga tashqi dunyo bilan o'zaro aloqa qilish imkoniyatini ta'minlaydigan aloqa kanallari. Tashqi tahdidlar o'zlariga mos zaifliklarni topib, ulardan foydalangandagina haqiqiy xavfga aylanadi. Har bir muvaffaqiyatli hujum tashqi omilning ichki himoyadagi bo'shliqlardan qanday foydalanganligi haqidagi hikoyadir.

Ushbu tahlil bizni xavfning rasmiy ta'rifiga olib keladi. Xavf — bu tahdidning o'zi ham, zaiflikning o'zi ham emas, balki muayyan tahdidning muayyan zaiflikdan muvaffaqiyatli foydalanishi va bu tashkilot aktivlariga ma'lum darajada zarar yetkazishi ehtimolidir.

Masalan, josuslik dasturiy ta'minotini joriy etish kabi texnik tahdidlar bevosita axborot aktivlariga qaratilgan. Biroq, ularning muvaffaqiyati deyarli har doim zaifliklar mavjudligi bilan bog'liq: zaif parol siyosati, ikki bosqichli autentifikatsiyaning yo'qligi yoki ko'pincha inson omilining zaifliklari, masalan, xabardorlikning yetishmasligi yoki charchash tufayli hushyorlikning pasayishi. Ma'lumotlar bazasi bo'lgan shifrlanmagan qattiq disk qurilma jismonan yo'qolganda yoki olib qo'yilganda oson o'ljaga aylanadi.

O'z navbatida, psixo-ijtimoiy hujumlar, jumladan, dezinformatsiya, doksing va dipfeyklardan foydalanish obro' va ishonchga putur yetkazishga qaratilgan. Ular xodimlarning ijtimoiy tarmoqlarda shaxsiy ma'lumotlarini haddan tashqari oshkor qilishi yoki tashkilotning soxta ma'lumotlarga qarshi kurashish uchun aniq kommunikatsiya strategiyasiga ega emasligi kabi zaifliklarda qulay zamin topmoqda. Hujum shaxsiy va ommaviy raqamli izlar o'rtasidagi chegaralar xiralashgan joyda muvaffaqiyatli bo'ladi.

Xuddi shunday, huquqiy va iqtisodiy bosim tashkiliy zaifliklarga qaratilganda ayniqsa samarali bo'ladi. "Xorijiy agentlar" to'g'risidagi qonunlar bir manbaga moliyaviy qaramlikni ekspluatatsiya qiladi, hisobvaraqlarning to'satdan blokirovka qilinishi esa tashkilotda diversifikatsiyalangan moliyaviy oqimlar va zaxira fondlarining yo'qligini ko'rsatadi. Tuhmat uchun qonuniy javobgarlikka tortish ko'pincha puxta ishlab chiqilgan tahririyat siyosati va faktlarni tekshirish tartib-qoidalarini mavjud bo'lmaganda mumkin bo'ladi.

Har qanday tashkilotning resurslari cheklanganligi sababli, barcha zaifliklarni bir vaqtning o'zida bartaraf etib bo'lmaydi. Xavf-xatarlarga ustuvorlik berish asosiy vazifaga aylanadi. Bu jarayon har bir tahdidni ikkita asosiy mezon bo'yicha baholash orqali amalga oshiriladi: uning amalga oshirish ehtimoli va muvaffaqiyat qozongan taqdirda ehtimoliy zarar. Ehtimollik tashkilotning maqsad sifatida jozibadorligi va uning zaif tomonlaridan foydalanish osonligiga bog'liq. Zarar zarbaga uchragan aktivning qiymati va uni tiklash qiymati bilan belgilanadi. Ikki bosqichli autentifikatsiya yo'qligi sababli maxfiy ma'lumotlarga ega ma'lumotlar bazasining buzilishi kabi yuqori ehtimollik va yuqori potensial zarar keltiruvchi xavflar zudlik bilan e'tibor qaratishni talab etadi. Shu bilan birga, ehtimoli past va kam zarar keltiradigan xatarlar vaqtincha kechiktirilishi mumkin.

Xavflar baholanib, ularga ustuvorlik berilgandan so'ng, tashkilot ularning har biri uchun to'rtta asosiy **boshqaruv strategiyasidan** birini tanlashi mumkin. Birinchidan, bu **qochish (Avoidance)** — yuqori xavf bilan bog'liq faoliyatni to'xtatishning strategik qaroridir. Masalan, tashkilot o'z missiyasi uchun mutlaqo zarur bo'lmasa, ma'lum turdagi nozik ma'lumotlarni to'plamaslikka qaror qilishi mumkin, bu esa ularning sizib chiqish xavfini butunlay bartaraf etadi. Ikkinchidan, **qabul qilish (Acceptance)** strategiyasi mavjud bo'lib, u past ustuvorlikka ega bo'lgan tavakkalchiliklarga nisbatan qo'llaniladi, bunda ularni kamaytirish qiymati potensial zarardan oshib ketadi. Uchinchidan, bu risklarni o'tkazish **(Transfer)** — riskning bir qismini uchinchi tomonga o'tkazishdir. Ma'lumotlarni saqlash uchun ishonchli bulutli provayderdan foydalanish klassik misol bo'lib, bu unga serverlarning jismoniy xavfsizligi va uskunalarining ishdan chiqishi bilan bog'liq xavflarni o'tkazadi. Nihoyat, bu xavfni kamaytirish **(Mitigation)** eng keng tarqalgan strategiya bo'lib, u ehtimollik yoki zararni kamaytirish uchun choralar ko'rishdan iborat. Masalan, shifrlashni joriy etish, xodimlar uchun treninglar o'tkazish yoki zaxira nusxalarini yaratish. Bu keyingi bo'limda ko'rib chiqiladigan asosiy strategiyadir.

3.2. Jurnalistlar va tahririyatlar uchun xavfsizlik choralari

O'z raqamli resurslaringiz xavfsizligini ta'minlash juda murakkab jarayon, ayniqsa alohida IT bo'limi yoki mutaxassis va resurslar bo'lmasa. Oldingi bo'limda sanab o'tilgan tahdidlarning to'liq bo'lmagan ro'yxati tushkunlikka tushirib, qo'lni tushirishga majbur qilishi mumkin, chunki hamma narsadan himoyalanih imkonsizdek tuyuladi. Shunga qaramay, bu yondashuv konstruktiv emas va ushbu bo'limda biz aksariyat tahririyatlar va alohida jurnalistlar uchun variantlarni tanlashga harakat qilamiz.

Avvalo, mutlaqo zarur bo'lgan minimal talablar mavjud — bu muammolarning 80 foizini hal qiladigan 20 foizlik sa'y-harakatdir:

- Raqamli resurslar inventarizatsiyasi — bu eng muhim raqamli resurslarning ro'yxatini tuzish jarayonidir. Odatda bunday ro'yxatga **barcha email-manzillar** (shaxsiy va ishchi), **ijtimoiy tarmoqlardagi akkauntlar (FB, IG,...)**, **messenjerlardagi akkauntlar (WhatsApp, Telegram, Signal,...)**, **bulutli saqlash xizmatlari (Google Drive, Dropbox, OneDrive,...)**, shuningdek eng muhim hujjatlar va ularning saqlanish joylari kiradi.

Bu bosqich alohida shaxslar yoki kichik tashkilotlar uchun kamdan-kam hollarda bir soatdan ko'proq vaqt oladi, biroq uning ahamiyatini ortiqcha baholash qiyin. Biz eslay olmaydigan raqamli resurslarni himoya qila olmaymiz, shuning uchun bu bosqich eng qimmatli raqamli aktivlarni ko'rish zonasiga kiritadi.

- **Parollar menejeri** — bu har bir sayt uchun o'ta murakkab parollarni yaratadigan va eslab qoladigan dastur. Siz faqat bitta asosiy parolni eslab qolishingiz kerak. Bu hisoblaringiz xavfsizligidagi eng katta bo'shliqni darhol yopadi. Jiddiy zaifliklardan biri bu juda zaif parollardan foydalanish yoki bir xil parolni bir nechta resurslar uchun qayta ishlatishdir. Parollar menejeri bilan bu muammolar hal qilinadi. Chunki barcha parollar parollar menejerida saqlanadi va ularni eslab qolishning hojati bo'lmaydi. Parollardan tashqari, parol menejerlarida turli xil maxfiy qaydlar, bank kartalari ma'lumotlari, shaxsiy ma'lumotlar va boshqa ma'lumotlarni saqlash mumkin. Muhim jihati shundaki, parollar menejeridagi parollaringiz shifrlangan holda saqlanadi va hatto ularning xizmati buzilsa ham, buzg'unchilar parollaringizga kira olmaydi. Faqat sinovdan o'tgan, ishonchli parol menejerlaridan foydalanish kerak, masalan, bepul versiyaga ega Bitwarden yoki 1Password. Hozirgi kunda ko'plab xizmatlar parolsiz kirishni joriy etmoqda, parol kalitlari yordamida, bu parollarga ideal muqobil bo'lib tuyulishi mumkin — murakkab kalit qurilmangizda saqlanadi, eslab qolishni talab qilmaydi va hech qayerga uzatilmaydi. Shu bilan birga, bu usul ham tahdidlardan himoyalalmagan. Shunday qilib, kalitga kirish PIN-kodni kiritish yoki biometrik aniqlash orqali amalga oshiriladi va agar kimdir sizning PIN-kodingizni bilib olsa yoki barmoq izi yoki FaceID'dan foydalanishga majbur qilsa, u sizning hisoblaringizga kirish huquqiga ega bo'ladi. Parolsiz sxemalardan farqli o'laroq, parollar menejeridan foydalanish turli tahdidlarda turli xil foydalanish variantlariga moslashtirilishi mumkin.
- **Ikki bosqichli autentifikatsiya (Two-factor authentication, 2FA)** hisoblaringiz uchun ikkinchi himoya chizig'idir. Agar parolingiz o'g'irlansa ham, telefoningizdagi kod, token, barmoq izi yoki FaceIDsiz firibgar hisobingizga kira olmaydi. **Bu buzib kirishga qarshi eng samarali chora.** Ko'pgina xizmatlarda u avtomatik ravishda yoqiladi (masalan, Google bildirishnomalari), ba'zilarida esa qo'lda yoqish kerak bo'ladi. Shunga qaramay, u nafaqat barcha xizmatlarda yoqilganligiga, balki to'g'ri sozlanganligiga ishonch hosil qilish kerak. Xususan, SMS orqali autentifikatsiya qilish xavfsiz emas va SMS xabarni ushlab orqali osongina buzib kirilishi mumkin, shuning uchun bu usul muqobil usullar mavjud bo'lgan joylarda o'chirilishi kerak. Shunday qilib, qulaylik va xavfsizlik nuqtai nazaridan "oltin o'rtalik" kirish uchun kodlarni mustaqil ravishda yaratuvchi autentifikator ilovasidan (Google Authenticator, Authy, Microsoft Authenticator, ...) foydalanishdir. Bundan tashqari, zaxira tiklash kodlari (backup codes) ishonchli va xavfsiz joyda saqlanishiga ishonch hosil qilish kerak, bu bir martalik kodlar telefon ishlamagan taqdirda ishlatiladi. Bu juda muhim qadam, aks holda hisobingizga kira olmay qolishingiz mumkin. Siz foydalanadigan messenjerlarda ham ikki bosqichli autentifikatsiya mavjudligini alohida tekshiring. Turli messenjerlarda u turlicha nomlanishi mumkin: WhatsApp — ikki bosqichli tekshiruv, Telegram — bulutli parol, Signal — ro'yxatdan o'tishni bloklash. Ushbu sozlamalar ro'yxatdan o'tish SMS xabarini ushlab qolish yoki SIM kartani almashtirish orqali messenjerni buzish imkoniyatining oldini oladi.
- **Zaxira nusxalarini yaratish (backup)** — mahalliy qurilmalarda saqlanadigan ma'lumotlarni apparat nosozliklari, zararli dasturiy ta'minot (xususan, shifrllovchi dasturlar) hujumlari va uskunaning jismonan yo'qolishi yoki olib qo'yilishi kabi tahdidlardan himoya qilishning o'ta muhim tarkibiy qismidir. Samarali zaxira nusxalashning asosiy tamoyili — bu jarayonni avtomatlashtirishdir. Foydalanuvchi tomonidan fayllarni

qo'lda nusxalashga asoslangan tizimlar inson omili tufayli ishonchliligi past bo'ladi. Avtomatlashtirilgan zaxira nusxalashni amalga oshirishning ikkita asosiy yondashuvi mavjud: tashqi tashuvchilardan foydalangan holda mahalliy zaxiralash hamda bulutli zaxiralash va sinxronlash. Mahalliy zaxira nusxalash uchun tashqi axborot tashuvchilar (qattiq disklar, SSD-to'plagichlar va hokazo) ishlatiladi. Bu jarayonni avtomatlashtirish uchun operatsion tizimning o'rnatilgan vositalaridan foydalanish mumkin. Microsoft Windows'da bu vazifani "Fayllar tarixi" (File History) vositasi bajaradi; u foydalanuvchi papkalaridagi fayllarni ko'rsatilgan tashqi diskka davriy nusxalashni sozlash imkonini beradi. Apple macOS'da esa shunga o'xshash funktsionallikni Time Machine tizimi taqdim etadi. U butun tizimning inkremental sur'atlarini yaratib, ham alohida fayllarni, ham butun operatsion tizimni ma'lum bir vaqtga qayta tiklashga imkon beradi. Bulutli zaxira nusxalash uchun Google Drive, Microsoft OneDrive, Dropbox kabi bulutli xizmatlardan foydalaniladi. Aksariyat zamonaviy bulutli xizmatlar avtomatik sinxronizatsiya tamoyili asosida ishlaydi: bunda mahalliy ilova o'rnatiladi, u mahalliy diskda maxsus papka yaratadi va shu papkaga joylashtirilgan har qanday fayl avtomatik ravishda bulutli xotiraga nusxalanadi hamda barcha ulangan qurilmalar o'rtasida sinxronlanadi. O'ta maxfiy ma'lumotlar bilan ishlaydigan tashkilotlarga boshdan-oyoq (end-to-end) shifrlashni taklif qiluvchi ixtisoslashtirilgan bulutli xizmatlarni ko'rib chiqish tavsiya etiladi. Bunday tizimlarda (masalan, Proton Drive, Sync.com, Tresorit, Mega.io) ma'lumotlar serverga yuborilishidan oldin foydalanuvchining qurilmasida shifrlanadi. Bu esa ma'lumotlardan hatto xizmat xodimlarining o'zi ham foydalana olmasligini ta'minlab, maksimal darajadagi maxfiylikni kafolatlaydi. Mobil qurilmalarda sinxronlash odatda ulangan akkauntlar (Google, iCloud) orqali amalga oshiriladi, biroq bulutli xizmatlar ilovalarining mobil versiyalaridan ham foydalanish mumkin. Eng yaxshisi, ikkala usulni "3-2-1" formulasi bo'yicha birga qo'llashdir: ma'lumotlarning 3 ta nusxasi bo'lib, ulardan ikkitasi turli jismoniy tashuvchilarda va bittasi bulutda saqlanadi. Bunday yondashuv nosozliklarga nisbatan eng yuqori darajadagi barqarorlikni ta'minlaydi va aksariyat inqirozli holatlarda ma'lumotlar saqlanishini kafolatlaydi. Bunda faqat ma'lumotlarning mavjudligi ta'minlanadi; zaxira nusxalarning himoyasi esa bulutli zaxiralashda akkauntning himoyalash, mahalliy saqlashda esa diskni to'liq shifrlash orqali amalga oshiriladi.

Oldinga siljish va xavfsizlik bo'yicha ijobiy o'zgarishlarni doimiy qilish uchun treninglar yoki xavfsizlik uchun zarur bo'lgan sozlamalarni o'rnatish kabi bir martalik aksiyalar kam. Kelajakda xavfsizlik tashkilotning butun faoliyatining ajralmas qismiga aylanganda, tizimli yondashuv muhim ahamiyat kasb etadi. Buning uchun korporativ xavfsizlikning Due Diligence va Due Care kabi ikki tushunchasini kiritish zarur. To'g'ridan-to'g'ri tarjimasi yo'q, ammo ularni quyidagicha ta'riflash mumkin:

- **Due Diligence** — bu "amal qilishdan oldin o'ylab ko'rish", ya'ni xavflarni baholash va harakatlarni rejalashtirishdir. Bu quyidagi savolga javob beradi: "Tahdidlarga tayyorlanish uchun qo'limizdan kelgan barcha choralarni ko'rdikmi?"
- **Due Care** — bu "har kuni harakat qilish majburiyati", ya'ni yaratilgan tizimni ishchi holatda saqlab turish bo'yicha kundalik sa'y-harakatlardir. Bu quyidagi savolga javob beradi: "Tahdidlarga tayyor turish uchun doimiy ravishda barcha zarur choralarni ko'ryapmizmi?"

Buning uchun har bir darajada rejalashtirish va ijro etish uchun qabul qilinishi kerak bo'lgan chora-tadbirlar joriy etiladi. Shunga ko'ra, har bir darajada minimal talablar va oldingi darajadagi talablar bajarilishi muhimdir.



1-daraja:

Intizom va bazaviy gigiyenani shakllantirish — alohida jurnalistlar va kichik jamoalar uchun mo'ljallangan bo'lib, uning maqsadi yakka tartibdagi xavfsizlik amaliyotlarini umumiy intizom va xavfsizlik madaniyatiga aylantirishdir.

Poydevorni rejalashtirish va tayyorlash (Due Diligence): Bu bosqichda operatsion xavfsizlik poydevori qo'yiladi. U yuqorida keltirilgan zaruriy minimumni, shuningdek, bir nechta asosiy qo'shimcha qadamlarni o'z ichiga oladi.

Iloji boricha faqat litsenziyalangan dasturiy ta'minotdan foydalanishga harakat qilish. Agar media tashkiloti qo'shimcha ravishda NNT sifatida ro'yxatdan o'tgan bo'lsa, u holda ro'yxatdan o'tgan NNT uchun ko'plab vendor'lar o'zlarining dasturiy mahsulotlarini bepul yoki katta chegirma bilan taqdim etadilar. Yirik ishlab chiqaruvchilarda NNTlar uchun maxsus dasturlar mavjud, masalan, notijorat tashkilotlar uchun Google va notijorat tashkilotlar uchun Microsoft, ular doirasida tijorat xizmatlaridan bepul foydalanish mumkin yoki Techsoup NNTlar uchun ko'plab mahsulotlarga, shu jumladan Windows litsenziyalariga maxsus narxlarda kirish nuqtasi hisoblanadi. Bundan tashqari, sotuvchilarga to'g'ridan-to'g'ri xat yozib, chegirma so'rashingiz mumkin.

Windows uchun — Bitlocker, Mac OS uchun — Filevault kabi to'liq diskli shifrlashni ta'minlash, tiklash kalitlarini ishonchli va xavfsiz joyda (masalan, parol menejerida) saqlash zarur.

Jamoa uchun dastlabki trening o'tkazish, unda nafaqat texnik jihatlar, balki fishingni aniqlash asoslari, ijtimoiy muhandislik va jismoniy xavfsizlik asoslari ham tushuntiriladi.

Nazoratni kuchaytirish va raqamli izni kamaytirish uchun ijtimoiy tarmoqlardagi shaxsiy va umumiy sahifalarda maxfiylikni baholash va sozlashni amalga oshirish.

Jamoa ichida norasmiy qoidalarni ishlab chiqish — masalan, “barcha ish yozishmalarini faqat Signalda olib boramiz” yoki “parollarni Google Docs'da saqlamaymiz.” Bu hali xavfsizlik siyosati emas, lekin unga birinchi qadamlardir.

Mamlakat qonunchiligidagi asosiy “qizil chiziqlar” (ekstremizm, tuhmat to'g'risidagi qonunlar va h.k.) hamda ularning tashkilot faoliyatiga ehtimoliy ta'siri yuzasidan yurist yoki ekspert ishtirokida dastlabki huquqiy yo'riqnoma o'tkazish.

Kundalik amaliyot (Due Care): Bu, birinchi navbatda, barcha qurilmalarda dasturiy ta'minot yangilanishlarini o'z vaqtida o'rnatishdir, chunki bu ma'lum zaifliklardan himoyalashning asosiy usulidir. Qurilmalarning jismoniy xavfsizligi amaliyoti — ish joyini tark etganda kompyuter ekranini bloklash odati ham shular jumlasidandir. Ommaviy Wi-Fi nuqtalari bilan ishlashda VPN dan foydalanish. Nihoyat, bu tanqidiy fikrlashni rivojlantirish uchun doimiy motivatsiya — o'zaro ta'sir muhitidir. Shuningdek, tahririyatlar faoliyati va so'z erkinligiga oid qonunchilikdagi o'zgarishlar haqidagi yangiliklarni doimiy ravishda kuzatib borish muhimdir.



2-daraja:

Rasmiylashtirilgan tashkiliy jarayonlarni joriy etish — xavfsizlik ustida tizimli ishlashga o'tishga tayyor bo'lgan jamoalar va tahririyatlar uchun mo'ljallangan.

Poydevorni rejalashtirish va tayyorlash (Due Diligence): Bu bosqichdagi asosiy qadam yagona Axborot xavfsizligi siyosatini ishlab chiqish va tasdiqlashdir. Ushbu hujjat parollarga, dasturiy ta'minotdan foydalanishga, ma'lumotlarni saqlashga, jismoniy xavfsizlikka qo'yiladigan talablarni rasmiylashtiradi va barcha keyingi harakatlar uchun asos bo'ladi. Eng kam imtiyozlar tamoyiliga asoslangan (xodimlarga faqat ish uchun mutlaqo zarur bo'lgan ma'lumotlardan foydalanish imkoniyatini berish) kirish huquqini boshqarish tartibi joriy etiladi. Bundan tashqari, foydalanilayotgan tashqi xizmatlarning asosiy xavfsizlik bahosi o'tkaziladi. Misol uchun, har bir xizmat uchun tekshiruv varaqasi tuzish mumkin: xavfsiz ikki bosqichli autentifikatsiya qo'llab-quvvatlanadimi, rollar bo'yicha kirish taqsimoti mavjudmi, zaxira nusxalari qanday yaratiladi va hokazo. Xuddi shu bosqichda barcha yangi xodimlar uchun xavfsizlik bo'yicha kirish yo'riqnomasi dasturi yaratiladi hamda stressni boshqarish, raqamli charchoq va asosiy psixologik o'z-o'ziga yordam berish bo'yicha treninglar o'tkaziladi. Bundan tashqari, tashkilot faoliyatining qonunchilikning barcha talablariga muvofiqligiga ishonch hosil qilish uchun yuridik va moliyaviy audit o'tkazish zarur.

Kundalik amaliyot (Due Care): Ushbu darajadagi operatsion faoliyat yanada tizimli bo'lishi kerak. Aslida, bu ishlab chiqilgan xavfsizlik siyosatini har kuni amalga oshirishdir. Zaxira nusxalarning ishlash qobiliyati muntazam ravishda tekshirilishi kerak, "3-2-1" zaxira nusxalash formulasiga tiklashda nol xato qo'shiladi va formula "3-2-1-0" bo'ladi. Shuningdek, asosiy xizmatlarga kirish huquqlari muntazam ravishda tekshirilishi kerak. Bu, ayniqsa, kadrlar qo'nimsizligi yoki xodimlarning lavozimlari o'zgarganda muhim ahamiyat kasb etadi. Tekshiruvning yo'qligi tashkilotdan ketgan xodimning tashkilot xizmatlaridan foydalanishiga yoki amaldagi xodimning xizmatlar yoki hujjatlardan ortiqcha foydalanishiga olib kelishi mumkin. Xuddi shu darajada ma'lumotlarni majburiy kriptografik o'chirishni o'z ichiga olgan eski texnikani foydalanishdan xavfsiz chiqarish tartibi ishlab chiqilishi kerak. Jamoa uchun vaqti-vaqti bilan qisqa treninglar o'tkazilishi va umumiy yig'ilishlarda dolzarb tahdidlar, jumladan huquqiy, psixosotsial va iqtisodiy tahdidlar muhokama qilinishi kerak.



3-daraja:

Strategik va faol himoyani yaratish — xavf darajasi yuqori bo'lgan muhitda ishlaydigan tashkilotlar uchun mo'ljallangan bo'lib, bunda tahdidlarni oldindan ko'ra bilish va inqiroz sharoitida harakatlarni rejalashtirish zarur bo'ladi.

Poydevorni rejalashtirish va tayyorlash (Due Diligence): Bu bosqichda tashkilot uchun strategik rejalashtirish asosiy bo'ladi. Xavflarni baholash asosiy poydevorga aylanmoqda, uning asosida hodisalarga javob berishning batafsil rejasi (Incident Response Plan) — turli xil hujumlar (buzib kirish, doksing, DDoS) uchun bosqichma-bosqich harakatlar ssenariysi ishlab chiqilishi lozim. Bu reja faoliyatning uzluksizligini ta'minlash rejasi (Business Continuity Plan) bilan to'ldiriladi, u halokatli ssenariylar amalga oshirilgan taqdirda tashkilot o'z missiyasini qanday davom ettirishini tavsiflaydi. Nafaqat ofis, balki asosiy xodimlarning yashash joylari uchun ham jismoniy tahdidlarga qarshi protokollar ishlab chiqilishi kerak.

Shuningdek, xavfsizlik uchun mas'ul shaxsning rasmiy roli belgilanishi, tashqi ekspertlar (huquqshunoslar, IT-mutaxassislar) bilan aloqalar o'rnatilishi va inqiroz holati uchun aloqa rejasi ishlab chiqilishi kerak. Iqtisodiy tahdidlarga qarshi kurashish uchun tashkilotning bir necha oy davomida ishlashini ta'minlash uchun zaxira jamg'armasini shakllantirish zarur.

Kundalik amaliyot (Due Care): Ushbu bosqichda tashkilot hodisalarga shunchaki munosabat bildirmasdan, balki oldindan ko'ra bilishi va tayyorgarlik ko'rishi lozim. Buning uchun tahdidlarni erta aniqlash uchun o'zining raqamli izi va axborot maydonini muntazam ravishda kuzatib borishi kerak. Turli xarakterdagi hodisalarga javob berish rejasini va faoliyatning uzluksizligini ta'minlash rejasini tekshirish hamda ishlab chiqish uchun ichki hujum simulyatsiyalari va o'quv trevogalari o'tkazilishi lozim. Barcha ishlab chiqilgan siyosat va rejalar har yili qayta ko'rib chiqilishi va yangi sharoitga moslashtirilishi kerak.

3.3. Tahririyatlar saytlari va mediaresurslarini himoya qilish choralari

Raqamli transformatsiya davrida tahririyatlar va jurnalistik tashkilotlarning saytlari hamda onlayn platformalari ularning vazifalari uchun muhim infratuzilmaga aylandi. Biroq, bu ularni o'sib borayotgan kiberhujumlar oldida zaif qilib qo'ydi. Ayniqsa, inson huquqlari tashkilotlari, mustaqil ommaviy axborot vositalari va faollar guruhlar ayniqsa zaif bo'lib, ular jinoyatchilar va haktivistlar, shuningdek, davlat subyektlari, shu jumladan xorijiy subyektlar uchun ham nishon bo'lishi mumkin.

Onlayn resurslarni, xususan, veb-saytlarni samarali himoya qilish tizimini yaratish uchun tashkilot qanday turdagi tahdidlarga duch kelishi mumkinligini tushunish zarur. Barcha hujumlarni shartli ravishda to'rtta asosiy toifaga bo'lish mumkin, ularning har biri oldini olish va javob berishga o'ziga xos yondashuvni talab qiladi.

Resursning komprometatsiyasi (buzib kirish)

Bu toifaga begona shaxslar saytingizning "ichki qismi"ga — uning boshqaruv tizimi, serveri yoki administrator hisoblariga ruxsatsiz kiradigan barcha hodisalar kiradi. Bunday kirishning oqibatlarini tajovuzkorning maqsadlariga qarab turlicha bo'lishi mumkin. Ba'zan bu ommaviy vandalizm (defeys) bo'lib, bosh sahifada begona xabar joylashtiriladi. Murakkabroq hollarda, bu ma'lumotni yashirincha o'zgartirishdir, ya'ni saytda sizning ishonchingizga putur yetkazish uchun raqamlar yoki faktlar sezdirmasdan o'zgartiriladi. Ko'pincha asosiy maqsad shaxsiy, moliyaviy va boshqa ma'lumotlarni o'g'irlashdir. Bundan tashqari, veb-saytingiz spam yuborish yoki tashrif buyuruvchilarning qurilmalarini zararlash uchun qurolga aylanishi mumkin. Shuningdek, buzib kirish natijasida saytdagi ma'lumotlar butunlay yo'q qilinishi mumkin.

Xizmat ko'rsatishni rad etish hujumi (DDoS hujumlari)

Bu toifa asosiy maqsadi saytingizni tashrif buyuruvchilar uchun mavjud bo'lmaydigan qilish, auditoriyangizning saytdan foydalanishiga deyarli imkon bermaydigan hujumlarni birlashtiradi. Qoida tariqasida, bu texnik hujum bo'lib, unda sizning resursingiz zararlangan qurilmalar tarmog'idan (botnet) foydasiz so'rovlarning katta oqimi bilan sun'iy ravishda qayta yuklanadi va u yuklamani boshqarish va foydalanuvchilar so'rovlariga javob berishni to'xtatadi. Ko'pincha bunday hujum qandaydir muhim voqealar, masalan, saylovlar, norozilik namoyishlari, auditoriyaga ma'lumot olish imkoniyatini bermaslik uchun qandaydir shov-shuvli materiallarni nashr etish paytida qo'llaniladi.

Huquqiy va ma'muriy bosim

Bu toifaga tashkilotingizning onlayn manbasi orqali unga bosim o'tkazish uchun qonunlar va rasmiy tartib-qoidalardan foydalanish kiradi. Bu hokimiyat yoki boshqa tuzilmalar sanksiyalar, mamlakatda resursni bloklash yoki domen nomini qaytarib olish tahdidi ostida muayyan materiallarni olib tashlashni talab qilganda, kontentni majburiy o'chirish (senzura) shaklida namoyon bo'lishi mumkin. Shuningdek, bu saytdagi nashrlar yoki sharhlar tashkilotga qarshi ish qo'zg'atish uchun asos bo'lgan hollarda qonuniy ta'qib orqali amalga oshirilishi mumkin.

Shaxsiyat va ishonchga qarshi hujumlar

Bu toifa sizning resursingizga emas, balki sizning nomingizga, brendingizga va auditoriyangiz ishonchiga qaratilgan tahdidlarni birlashtiradi. Bunday hujumlar tashrif buyuruvchilaringizni aldash uchun turli usullardan foydalanadi. Asosiy usullarga domen nomini o'g'irlash kiradi, bunda veb-manzilingiz nazorat qilinadi va tashrif buyuruvchilar soxta saytga yo'naltiriladi. Yana bir mashhur usul — sizni obro'sizlantirish yoki sizning nomingizdan xayriya yig'ish uchun siznikiga juda o'xshash manzillarda yoki sayt dizayni bilan bir xil bo'lgan klon saytlarni yaratishdir. Bunday hujumlardan maqsad — yillar davomida qurgan obro'yingizga putur yetkazishdir.

Avval ta'kidlanganidek, tahdidlarni tushunish xavfsizlik sari qo'yilgan birinchi qadamdir. Keyingi qadam — ularning oldini olish va oqibatlarini yumshatish uchun aniq chora-tadbirlarni joriy etish. Quyida to'rtta asosiy tahdid toifasiga muvofiq guruhlangan asosiy himoya strategiyalari keltirilgan.

Veb-resursni buzishga qarshi kurashish choralari

Ishonchli hosting provayderi — Hosting provayderini tanlash onlayn resursingizning xavfsizligi va barqarorligini belgilovchi asosiy qarordir. Baholashda texnik, huquqiy va operatsion omillar majmuasini ko'rib chiqib, uzluksiz ishlash narxi va vaqtdan tashqariga chiqish lozim. Texnik ishonchlilik zamonaviy infratuzilmaning mavjudligini, DDoS hujumlaridan majburiy himoyani, shuningdek, tezkor tiklash imkoniyatiga ega avtomatlashtirilgan kundalik zaxiralash tizimini o'z ichiga oladi. Huquqiy himoya ham muhim ahamiyatga ega: provayderning yurisdiksiyasi, uning maxfiylik siyosati va davlat organlarining so'rovlariga javoban mijozlar manfaatlarini himoya qilishga tayyorligini baholash zarur. Ideal provayder o'z faoliyatida shaffoflikni namoyish etishi va boshqa fuqarolik jamiyati tashkilotlarining fikr-mulohazalari bilan tasdiqlangan benuqson obro'ga ega bo'lishi kerak.

Operatsion ishonchlilik 24/7 texnik qo'llab-quvvatlash sifati va mavjudligi, shuningdek, saytni boshqarish uchun boshqaruv panelining qulayligi bilan belgilanadi. Biroq, tahririyatlar uchun axloqiy jihat ham juda muhim: provayder nafaqat xizmat ko'rsatishi, balki jurnalistlar va mustaqil tahririyatlar duch keladigan o'ziga xos xavf-xatarlarni ham tushunishi kerak. So'z erkinligi qadriyatlarini baham ko'radigan, fuqarolik jamiyatini faol qo'llab-quvvatlaydigan va inqirozli vaziyatlarda, jumladan, buzib kirishga urinishlarni tekshirishda qo'shimcha yordam ko'rsatishga tayyor bo'lgan kompaniyalarga ustunlik berilishi kerak. VirtualRoad.org (<https://www.qurium.org/>) yoki eQPress loyihasi doirasidagi eQualitie kabi WordPress veb-saytlari uchun xavfsiz xosting (<https://deflect.ca/solutions/hosting/>) taqdim etuvchi ixtisoslashtirilgan xizmatlar, shuningdek, Cloudflare kompaniyasining Project Galileo (<https://www.cloudflare.com/galileo/>) kabi qo'llab-quvvatlash dasturlari eng maqbul tanlovdir, chunki ular dastlab sektor duch keladigan

tahdidlarga qarshi kurashish uchun mo'ljallangan va o'z xizmatlarini fuqarolik jamiyati tashkilotlari hamda yuqori xavf darajasiga ega media tashkilotlariga bepul taqdim etadi.

Saytni boshqarishga xavfsiz kirishni ta'minlash — saytingizning administrativ paneliga, ya'ni kontent va sozlamalarni boshqarish tizimiga, shuningdek hosting paneliga kirish huquqlarini maksimal darajada himoya qilish zarur. Mustaqil ravishda amalga oshirilishi mumkin bo'lgan minimal choralar — murakkab va noyob parollardan foydalanish hamda ikki faktorli autentifikatsiyani (2FA) majburiy yoqishdir. Yaxshi hosting xizmatlarida bu odatda ro'yxatdan o'tish vaqtida standart tarzda sozlangan bo'ladi. WordPress, Drupal kabi kontentni boshqarish tizimlari (CMS) uchun uchinchi tomon modullaridan foydalanishga to'g'ri keladi. Texnik yordamni talab qilishi mumkin bo'lgan qo'shimcha himoya usullari faqat VPN orqali boshqaruv paneliga kirishni ta'minlash yoki standart kirish manzilini boshqasiga o'zgartirishdir. Bundan tashqari, parol bir necha marta noto'g'ri kiritilganda hisobni vaqtincha bloklashni sozlash mumkin.

Dasturiy ta'minotni o'z vaqtida yangilash — veb-resurslarning ko'plab buzilishlari yangilanmagan dasturiy ta'minot tufayli sodir bo'ladi, odatda bu kontentni boshqarish tizimi (CMS), qo'shimcha modullar (pluginlar) va sayt yozilgan platforma hisoblanadi. Ko'pincha veb-sayt ishlab chiquvchilar o'z vazifasiga “ qo'l uchida” yondashadilar va xavfsizlikka e'tibor bermaydilar, natijada mijoz yangilanmaydigan yoki zaif mavzular, pluginlar yoki “qo'lda yozilgan” tizimlar holatida butunlay zaif va qo'llab-quvvatlanmaydigan tizimga ega bo'ladi. WordPress, Drupal, Joomla kabi eng mashhur tizimlarda o'rnatilgan avtomatik yangilash tizimlari mavjud bo'lib, ular tizim komponentlarini avtomatik ravishda yangilaydi. Bu xavfsizlik nuqtai nazaridan yaxshi va to'g'ri, ammo shuni yodda tutish kerakki, ishlab chiquvchilar, komponentlar va boshqa omillarga qarab, keng ko'lamli yangilanishlar paytida veb-sayt qisman yoki butunlay ishlamay qolishi mumkin. Shuning uchun, avvalo, saytning zaxira nusxalari mavjudligiga e'tibor qaratish lozim, shunda avvalgi versiyani qayta tiklash va texnik qo'llab-quvvatlash yordamida yangilash imkoniyati bo'ladi.

Zaxira nusxalash — buzg'unchilik kabi noxush hodisalardan so'ng tizimni tez va to'liq tiklashning asosiy vositasidir. Hatto eng mukammal himoya ham yetarli bo'lmasligi mumkin, masalan, platforma dasturchilari hali bexabar bo'lgan zero-day (nolinchi kun zaifliklari) mavjud bo'lgan hollarda. Bunday zaifliklardan hatto to'liq yangilangan tizimlarda ham foydalanish mumkin. Bunday vaziyatda ziyonkor kod mavjudligini istisno qilish uchun eng yaxshi usul — tizimni zaxira nusxasidan tiklashdir. Agar buzg'unchilik qachon sodir bo'lgani aniq bo'lmasa, tizimni avvalroq yaratilgan nusxadan tiklashga to'g'ri kelishi mumkin. Xosting-provayderingiz muntazam ravishda zaxira nusxalarini yaratib, ularning turli versiyalarini saqlashiga ishonch hosil qiling. Agar tashkilotda texnik mutaxassis bo'lsa, zaxira nusxalarini yaratish va ularning versiyalarini saqlab borish uning vazifalariga kirishi lozim. Zaxira nusxalarini yaratish davriyligi resursning yangilanish tezligiga bog'liq. Odatda, o'zingizga savol berishingiz kerak: tiklash ishlari imkon qadar kam vaqt va kuch talab qilishi uchun nusxalar qanchalik tez-tez olinishi kerak?

Tashqi himoya xizmatlari — buzib kirish ehtimolini kamaytirish uchun, shu jumladan zero-day (nolinchi kun zaifliklaridan) foydalangan holda, WAF (Web Application Firewall) kabi qo'shimcha xizmatlar qo'llanilishi mumkin, bu himoya mexanizmi bo'lib, aksariyat buzib kirish urinishlarini veb-resursga yetib bormasdan turib to'xtatadi. Odatda, bunday funksiyani taqdim etuvchi xizmatlar bitta tugma bilan texnik tafsilotlarga e'tibor bermasdan asosiy to'plamni yoqish imkoniyatiga ega. Masalan, yuqorida tilga olingan Cloudflare kompaniyasining Project Galileo loyihasi asosiy sozlamalar to'plamini oddiy yoqish imkoniyatiga ega bo'lgan korporativ darajadagi WAFni o'z ichiga oladi. CMS uchun

WAF plaginlari ham mavjud, masalan, Wordpress uchun Wordfence va Joomla uchun Akeeba Admin Tools, ammo ular uchun funksionallikning katta qismi pullik.

DDoS hujumlariga qarshi choralar

Hozirgi vaqtda DDoS hujumlari kichik bir mamlakatning internet iste'moli bilan taqqoslanadigan ulkan miqdorlarga yetishi mumkin. Qayd etilgan eng muhim hujumlardan biri 2025-yilda sodir bo'lgan va 29,7 Tbit/s ni tashkil etgan. Bu bir soniyada saytdan taxminan 7000 ta filmni HD sifatda yuklab olish bilan barobar. Taxminlarga ko'ra, hujumda 1 milliondan ortiq zararlangan qurilmalar ishtirok etgan. Katta resurslarga ega bo'lmasdan turib, bunday hujumlarni, hatto kamroq kuchga ega bo'lganlarini ham yengish deyarli imkonsiz, shuning uchun eng samarali usul — zarbani o'z zimmasiga oladigan ixtisoslashgan vositachi xizmatlardan foydalanishdir. Yuqorida tilga olingan Cloudflare Project Galileo, VirtualRoad.org, eQualitie kabi tashkilotlar fuqarolik jamiyati uchun DDoS-hujumlardan himoyani taqdim etadi.

Huquqiy va ma'muriy tazyiqqa qarshi kurashish choralari

Ushbu turdagi tahdidlardan himoyalaniish asosan huquqiy va protsessual jihatdan, xususan, qonunchilikka rioya qilish, huquqshunoslar bilan maslahatlashish va malakali tahririyat siyosatining mavjudligi bilan bog'liq. Shu bilan birga, tayyorgarlik ishlarini olib borish va bunday tahdidlar amalga oshirilganda ishni davom ettirish imkonini beruvchi texnik jihatlar mavjud.

Birinchi navbatda, bu mamlakat ichidagi resurslarning mavjudligini minimallashtirishni o'z ichiga oladi, masalan, mamlakat ichidagi resursni joylashtirish va mamlakat zonasidagi domen nomi. Hosting provayderi yoki domen hududi administratoriga ma'muriy bosim o'tkazilganda, resursingiz o'chirilishi yoki olib tashlanishi, domen nomi esa olib qo'yilishi mumkin. Buning oldini olish uchun mamlakatdan tashqarida ishonchli hostingni ta'minlang va umumiy domen nomidan foydalaning (masalan, .org, .info, .ngo). Shuningdek, ko'zgu saytlarining (mirror sites) mavjudligini va Cloudflare yoki Akamai kabi kontent tarqatish tarmoqlaridan (CDN) foydalanishni ham hisobga oling. Va, albatta, zaxira nusxa olishni unutmang.

Shaxsiyat va ishonchga qarshi hujumlarga qarshi choralar

Ushbu toifadagi tahdidlarning aksariyati yomon nazorat qilinadi, shuning uchun ular odatda sizning nazoratingiz doirasidan tashqarida bo'ladi. Ammo avval aytib o'tilganidek, tahdidlar haqidagi bilim bizga ularga javob berish imkonini beradi, shuning uchun raqamli muhitni kuzatishni o'zingizga odat qiling, vaqti-vaqti bilan sizning nomingizga o'xshash saytlarni qidiring, bu ijtimoiy tarmoqlardagi sahifalarga ham tegishli. Soxta hisoblar haqidagi barcha xabarlarini tekshiring. Soxta klon saytlarni aniqlaganingizda, ularning xosting provayderi va domen registratoriga shikoyat bilan murojaat qiling, ijtimoiy tarmoqlar holatida rasmiy shikoyat kanallaridan foydalaning, shuningdek, barcha mavjud kanallar orqali auditoriyangizni ogohlantiring. O'z tomoningizdan saytingizning domen nomini himoya qilishingiz kerak. U qayerda va kimga ro'yxatdan o'tkazilganini hamda uning sozlamalariga qanday kirishni bilishingizga ishonch hosil qilishingiz kerak. Ko'pincha bu bilan veb-sayt ishlab chiquvchilari shug'ullanadilar, uni o'zlariga rasmiylashtiradilar va mavjud xavfsizlik imkoniyatlaridan (murakkab parol, ikki bosqichli autentifikatsiya, domenni ko'chirishni taqiqlash) foydalanmaydilar. Natijada, domen nomi bilan bog'liq muammolar yuzaga kelganda, masalan, domen o'g'irlanganda, tashkilot uni qaytarib olishi juda qiyin yoki imkonsiz bo'lishi mumkin. Shuningdek, veb-resursingizning haqiqiy

xavfsizlik sertifikatiga ega ekanligiga ishonch hosil qilish muhimdir. Bunday sertifikatning yo'qligi auditoriyaning saytingizga bo'lgan ishonchini pasaytirishi mumkin, chunki ulanish shifrlanmagan bo'ladi va trafik ushlab qolinishi yoki o'zgartirilishi mumkin, shuningdek, ba'zi antivirus dasturlari hozirda bunday saytlarga kirishni bloklaydi. Aksariyat ishonchli xostinglar bunday imkoniyatni sukut bo'yicha taqdim etadi. Agar bunday imkoniyat bo'lmasa, Let's Encrypt (letsencrypt.org) yordamida bepul sertifikat olish mumkin, bu esa ba'zi texnik ko'nikmalarni talab qiladi.

Hodisalarni tergov qilish va tahdidlarga javob qaytarish

Xavfsizlik hodisasi yuz berganda — bu saytning buzilishi, xodimga tahdidlar yoki muvofiqlashtirilgan hujum bo'ladimi — birinchi reaksiya deyarli har doim tartibsizlik va vahima, tizimsiz muvofiqlashtirilmagan harakatlar bo'lib, bu ko'pincha vaziyatning yomonlashishiga, tergov uchun izlarning yo'qolishiga va boshqa tegishli yo'qotishlarga olib keladi. Shuning uchun, har qanday hodisa yuz berganda, aniq, bosqichma-bosqich harakat rejasiga amal qilish kerak. Samarali javob nafaqat zararni kamaytiradi, balki kelajakda hodisa yoki uning oqibatlarini kamaytirish va tezroq tiklanish uchun saboq olishga yordam beradi.

Aniqlash, dastlabki chora-tadbirlar va hujjatlashtirish

Hodisa aniqlangandan keyingi dastlabki daqiqalar va soatlar juda muhimdir. Ushbu bosqichdagi asosiy vazifa — hodisada jabrlangan tashkilot va resurslar uchun mas'ul shaxslarni ogohlantirishdir. Birinchi navbatda, bu tashkilot direktori, IT mutaxassisi, agar u bo'lsa, tegishli yo'nalish rahbarlari (saytni buzib kirish holatlarida sayt yoki ijtimoiy tarmoqlar administratori, tahdidlar paytida HR mutaxassisi, ma'lumot sizib chiqqanda loyiha rahbari va boshqalar). Axborot sizib chiqishining oldini olish uchun zudlik bilan javob qaytarish guruhini tuzish va hodisa yuzasidan barcha muloqotlarni, masalan, Signal kabi himoyalangan kanallar orqali olib borish lozim. Sodir bo'layotgan barcha voqealarni: vaqti, alomatlari, ko'rilgan choralarni qayd etib, hodisa jurnalini yuritishni boshlash juda muhim. Bu hujjatlar keyingi tahlil uchun asos bo'lib xizmat qiladi. Hech qanday holatda hujum izlarini darhol yo'qotish mumkin emas; bu bilan muammoni hal qila olmaysiz, aksincha, muhim dalillarni yo'q qilasiz, xolos. Buning o'rniga skrinshotlar qilib, log fayllarining nusxalarini saqlab qo'yish kerak, chunki bu ma'lumotlar keyingi tekshiruv uchun muhim bo'lishi mumkin. Agar hodisadan zarar ko'rgan qurilma faol ishlatilayotgan bo'lsa (spam tarqatayotgan, unda qandaydir harakatlar sodir bo'layotgan bo'lsa), uni darhol tarmoqdan uzish kerak (tarmoq kabelini jismonan sug'urib olish yoki Wi-Fi'ni o'chirish lozim). Qurilmani butunlay o'chirish yaramaydi, chunki bu muhim izlarni yo'qotib yuborishi mumkin. Sayt buzilgan taqdirda, uni texnik xizmat ko'rsatish rejimiga o'tkazsa bo'ladi. Vaziyatni baholashda professional ko'mak beradigan Access Now (<https://www.accessnow.org/>) kabi ixtisoslashgan tashkilotlarning Digital Security Helpline (help@accessnow.org) xizmatiga tashqi ekspert yordami uchun zudlik bilan murojaat qilish zarur. Shuni yodda tutish kerakki, Access Now birinchi murojaatingizda maqomingizni tasdiqlash uchun sizni ishonchli hamkorlar orqali tekshirishi lozim va bu jarayon biroz vaqt talab qilishi mumkin. Shu sababli, hodisalarga oldindan tayyorgarlik ko'rgan ma'qul: hodisa yuz berganda zudlik bilan yordam olish uchun tashkilotning elektron pochtasidan Access Now'ga keyingi murojaatlar uchun tekshiruvdan o'tkazishni so'rab, oldindan xat yozib qo'ying. Digital Security Helpline ijtimoiy tarmoqlar va boshqa tashkilotlar bilan o'zaro aloqa kabi keng qamrovli masalalarga ixtisoslashgan. Veb-resurslarga qilingan hujumlar va dezinformatsiya kampaniyalarini tekshirish bo'yicha Qurium — The Media Foundation (<https://www.qurium.org/rapid-response/request/>) tashkilotiga ham murojaat qilish mumkin.

Zararni tahlil qilish va baholash

Keyinchalik, texnik mutaxassislar bilan birgalikda hujum yo'nalishini aniqlash uchun tahlil o'tkazish kerak: bu buzilgan parol, dasturiy ta'minotdagi zaiflik yoki fishing natijasi bo'lganmi. Hujumchi tizimga qanday qilib kirganini tushunish ushbu zaiflikni bartaraf etishning kalitidir. Zararni baholash hodisa tergovi bilan parallel ravishda amalga oshiriladi: ma'lumotlar o'g'irlanganmi yoki o'zgartirilganmi, resurs boshqalarga hujum qilish uchun ishlatilganmi va hodisa qanchalik keng tarqalishi (boshqa qurilmalarga yoki boshqa odamlarga ta'sir qilishi) mumkin.

Oqibatlarni bartaraf etish, tiklash va aloqa

Bu bosqichda bevosita oqibatlar bartaraf etiladi va normal ishlashga qaytiladi. Buzib kirilgan sayt uchun eng ishonchli usul uni zararli kodlardan "tozalashga" urinish emas, balki ataylab toza zaxira nusxasidan to'liq tiklashdir. Har qanday akkauntni buzish zudlik bilan buzilgan tizim bilan bog'liq barcha parollarni o'zgartirish va ikki bosqichli autentifikatsiyani yoqish bilan birga amalga oshirilishi kerak. Oshkor etilgan qurilmalar holatida, tizimni to'liq qayta o'rnatish yoki zavod sozlamalariga qaytarish to'g'ri bo'ladi. Ta'sirlangan tomonlar bilan muloqot qilish muhim qadamdir. Agar foydalanuvchilarning shaxsiy ma'lumotlari sizib chiqsa, ularni bu haqda xabardor qilish va kerakli ma'lumotlarni qanday taqdim etish bo'yicha huquqshunoslar bilan maslahatlashish lozim.

Hodisadan keyingi xulosalar

Vaziyat barqarorlashgandan so'ng, voqeani ichki tahlil qilish zarur. Ushbu tahlilning maqsadi aybdorlarni topish emas, balki jarayonlar va texnologiyalardagi zaif nuqtalarni aniqlashdir. Xulosalarga asoslanib, ichki xavfsizlik siyosatlarini yangilash, hodisalarga javob berish tartib-qoidalarini yaratish yoki yangilash, jamoa uchun qo'shimcha treninglar o'tkazish va yangi texnik himoya vositalarini joriy etish lozim. Bunday yondashuv har bir hodisani kelajakda tashkilotni yanada barqaror qiladigan saboqqa aylantiradi.

Huquqni muhofaza qilish organlariga murojaat qilish

Politsiyaga rasmiy ariza berish masalasi tahririyatlar uchun ancha murakkab va xavfli hisoblanadi. Bir tomondan, rasmiy bayonot hodisa faktini qayd etadi, bu esa o'g'irlangan ma'lumotlar yoki buzilgan resurs sizning nomingizdan noqonuniy faoliyat uchun ishlatilsa, huquqiy himoya vazifasini o'tashi mumkin. Boshqa tomondan, tergov doirasida huquq-tartibot idoralari sizning faoliyatingiz va hamkorlaringiz haqidagi maxfiy ma'lumotlarga qonuniy kirish imkoniyatiga ega bo'lib, barcha texnikangizni olib qo'yishi mumkin bo'lgan "qurbonni gumonlanuvchiga aylantirish"ning jiddiy xavfi mavjud.

Bu qaror faqat mamlakatdagi siyosiy vaziyatni, huquqiy tizimga bo'lgan ishonch darajasini va oshkor etilishi mumkin bo'lgan ma'lumotlarning nozikligini hisobga olgan holda xavflarni sinchkovlik bilan baholagandan so'ng qabul qilinishi kerak. Huquqni muhofaza qilish organlari bilan har qanday aloqadan oldin matbuot va so'z erkinligini himoya qilishga ixtisoslashgan ishonchli advokatdan maslahat olish qat'iy tavsiya etiladi.

Xulosa

Raqamli muhit notijorat tashkilotlar faoliyatining ajralmas qismiga aylandi. U muloqot, ma'lumotlarga kirish, loyihalarni amalga oshirish va auditoriya bilan muloqot qilish uchun yangi imkoniyatlar ochadi. Shu bilan birga, raqamlashtirish mas'uliyat, huquqiy savodxonlik va xavflarni boshqarishga bo'lgan talablarni kuchaytiradi.

Ushbu qo'llanmada ko'rsatilganidek, raqamli huquqlar mavhum kategoriya emas, balki tahririyatlarning kundalik ishiga bevosita ta'sir ko'rsatuvchi amaliy vositadir. Ma'lumotlarga kirish, shaxsiy ma'lumotlarni himoya qilish, kontentni e'lon qilish qoidalari, davlat organlari va onlayn platformalar bilan hamkorlik — bu masalalarning barchasi ongli va tizimli yondashuvni talab qiladi.

Shuni hisobga olish muhimki, huquqlarning rasmiy kafolatlari har doim ham ularni amalda avtomatik ravishda amalga oshirishni anglatmaydi. Tahririyatlar milliy qonunchilik, xalqaro standartlar va raqamli platformalar qoidalari bir vaqtning o'zida amal qiladigan muhitda ishlaydi. Bu tartibga solishning bir necha darajalarida mo'ljal olish va huquqiy hamda obro'-e'tibor oqibatlarini hisobga olgan holda puxta o'ylangan qarorlar qabul qilish qobiliyatini talab etadi.

Risklarni boshqarish alohida ahamiyat kasb etadi. Nozik ma'lumotlar bilan ishlash, kontent nashr etish, auditoriya va hamkorlar bilan muloqot qilish — bularning barchasi tashkilotning o'ziga ham, uning hamkorlariga ham ta'sir qilishi mumkin bo'lgan potensial tahdidlar bilan bog'liq. Bunday sharoitda ma'lumotlarni, axborot manbalarini himoya qilish va aloqa barqarorligini ta'minlashga qaratilgan ichki siyosat, tartib-qoidalar va amaliyotlarni ishlab chiqish muhim ahamiyatga ega.

Qo'llanma barcha mumkin bo'lgan vaziyatlarga universal javob berish maqsadini ko'zlamaydi. Uning vazifasi o'quvchida raqamli huquqlar mantiqini tushunish, asosiy xavf-xatarlarni ko'rsatish va muayyan sharoitlarda qaror qabul qilish vositalarini taklif etishdan iborat.

Shunday qilib, bugungi kunda tahririyatlarning raqamli muhitda samarali ishlashi huquqiy xabardorlik, amaliy ko'nikmalar hamda aloqa va xavfsizlikka strategik yondashuvni uyg'unlashtirmasdan mumkin emas. Aynan shu uyg'unlik nafaqat xavf-xatarlarni kamaytirish, balki raqamli vositalardan jamiyat manfaatlari yo'lida maksimal darajada samarali foydalanish imkonini beradi.

Begona kontentini nashr etishdan oldin tekshiruv ro'yxati (muharrir/jurnalist uchun)

1. Foydalanish turini aniqlang
 - ☐ Bu iqtibos/sharh/voqea haqidagi reportaj (cheklangan parcha) yoki aslida to'liq qayta nashr/qayta yuklashmi?
2. Begona kontentdan foydalanish uchun qonuniy asos mavjud:
 - ☐ Yozma ruxsat/litsenziya/shartnoma mavjud
 - ☐ Ochiq litsenziyali kontent (Creative Commons/stokda sotib olingan)
 - ☐ Kontent erkin foydalanish doirasiga kiradi (iqtibos keltirish, matbuot sharhi, joriy mavzularni yoritish, nutq, tadbir sharhi va boshqalar)
3. Mualliflik huquqi egasining taqiqi (ayniqsa, materiallarni qayta nashr etish uchun) tekshirildi:
 - ☐ Birlamchi manbada "qayta nashr etish taqiqlanadi" degan aniq belgi / nashr etishga taqiq / cheklovchi shartlar yo'q/aniq ko'rsatilmagan
 - ☐ Birlamchi manbada foydalanish uchun alohida ruxsat olish majburiyati ko'rsatilmagan
4. Foydalanish maqsadlari uchun zarur bo'lgan minimal hajm
 - ☐ Axborot berish/sharhlash maqsadlari uchun aynan kerakli miqdorda foydalanilgan
 - ☐ Nashr asl manbaning o'rnini bosmaydi va uning auditoriyasini o'ziga og'dirib olmaydi ("butun material allaqachon shu yerda" degan taassurot yo'q)
5. Atributsiya to'g'ri rasmiylashtirilgan
 - ☐ Muallif (va/yoki huquq egasi) + manba + sana + havola ko'rsatilgan
 - ☐ Tarjima uchun: "tahririyat tarjimasi" + asl nusxaga havola belgilangan
 - ☐ Foto/video uchun manba ko'rsatilgan (muallif/agentlik/stok/rasmiy akkaunt)
6. Qayta ishlashga tekshirish
 - ☐ Ruxsatsiz qayta ishlashga olib keladigan montaj/moslashtirish/tarjima/musiqqa qo'yish/ma'noni qisqartirish kabi amallar bajarilmagan
 - ☐ Suv belgilari/logotiplar/metama'lumotlar va huquqlarni boshqarishga doir boshqa ma'lumotlar o'chirilmagan
7. Nashr konteksti reklama emas
 - ☐ Bu reklama, nativ reklama yoki PR materialidir emas
8. Birlamchi manba haqidagi dalillar saqlangan
 - ☐ Havola, birlamchi manba skrini, litsenziya shartlari/ruxsatnoma, kirish sanasi saqlangan (ehtimoliy da'vo uchun)
9. Yakuniy test
 - ☐ Agar siz muallif bo'lganingizda, bu foydalanishni qonuniy va manbaga hurmat sifatida qabul qilarmidingiz?
 - ☐ Shubha tug'ilganda ruxsat so'rash yoki begona kontentdan foydalanmaslik kerak.

Ommaviy foydalanish uchun ochiq shaxsiy ma'lumotlarni qayta ishlash va e'lon qilish bo'yicha tahririyat reglamenti

1. Umumiy qoidalar

- 1.1. Mazkur Reglament jurnalistlar va tahririyat tomonidan shaxsiy ma'lumotlarni yig'ish, qayta ishlash va chop etish tartibini belgilaydi.
- 1.2. Reglamentning maqsadi:
 - shaxsiy ma'lumotlar to'g'risidagi qonunchilikka rioya etilishini ta'minlash
 - inson huquq va erkinliklarini himoya qilish
 - fikr bildirish erkinligi va shaxsiy hayot daxlsizligi huquqi o'rtasidagi muvozanatni ta'minlash
- 1.3. Reglament tahririyatning barcha xodimlariga tatbiq etiladi, jumladan:
 - shtatli jurnalistlar
 - muharrirlar
 - shtatdan tashqari mualliflar
 - SMM mutaxassislari

2. Normativ asos

- O'zbekiston Respublikasi shaxsiy ma'lumotlar to'g'risidagi qonunchiligi
- fikr bildirish erkinligi bo'yicha xalqaro standartlar
- ma'lumotlarni himoya qilish va maxfiylik tamoyillari

3. Asosiy tamoyillar

- Shaxsiy ma'lumotlarni qayta ishlashning har qanday shakli qonuniy asosga ega bo'lishi shart.
- Shaxsiy ma'lumotlar faqat jamoatchilik manfaatiga xizmat qiluvchi aniq jurnalistik maqsadlar uchun qo'llaniladi.
- Faqat zarur, dolzarb va nashr maqsadiga mutanosib ma'lumotlar e'lon qilinadi.
- Shaxsiy hayotga aralashuv darajasi jamoatchilik manfaatidan oshmasligi kerak.
- Tahririyat e'lon qilinayotgan ma'lumotlarning ishonchliligini tekshirishi shart

4. Shaxsiy ma'lumotlarni e'lon qilish asoslari

- 4.1. Shaxsiy ma'lumot subyekti tomonidan berilgan ixtiyoriy, ongli va aniq shakldagi (yozma) rozilik.
- 4.2. Shaxsiy ma'lumotlarni e'lon qilish jamoat xavfsizligini ta'minlash, huquqbuzarlik haqida xabar berish, aholini chalg'itishning oldini olish maqsadida ruxsat etiladi.
- 4.3. Shaxsiy ma'lumotlar subyektiga mutanosiblik va zararni minimallashtirish tamoyillariga rioya qilingan holda, rozilgisiz ishlov berishga yo'l qo'yiladi.

5. Ma'lumot subyektlari tasnifi

- 5.1. Ommaviy shaxslar — siyosatchilar, deputatlar, davlat xizmatchilari, yuqori boshqaruv lavozimlarini egallagan shaxslar hamda qaror qabul qilish va

sanksiyalar qo'llash vakolatiga ega boshqa shaxslar. Shaxsiy ma'lumotlarni, agar ular shaxsning ommaviy vazifalari bilan bog'liq bo'lsa, kengroq hajmda e'lon qilishga yo'l qo'yiladi.

- 5.2. Xususiy shaxslar — shaxsiy ma'lumotlari yuqori darajada himoya qilinadi; ularning ma'lumotlari faqat roziligi bilan e'lon qilinadi.
- 5.3. Voyaga yetmagan shaxslar — mutlaq maxfiylik huquqidan foydalanadilar. Voyaga yetmagan shaxsni identifikatsiya qilish mumkin bo'lgan shaxsga doir ma'lumotlar, yashash, o'qish joyi to'g'risidagi ma'lumotlar, fotosuratlar va videoyozuvlarni tarqatishga yo'l qo'yilmaydi. 14 yoshgacha bo'lgan voyaga yetmagan shaxslarning shaxsiy ma'lumotlarini e'lon qilishga faqat ikkala ota-ona, qonuniy vakillar, vasiylar va homiylarning roziligi bilan yo'l qo'yiladi. 14 yoshdan oshgan voyaga yetmaganlar ishtirokidagi sport musobaqalari, rasmiy marosimlar, olimpiadalar va festivallarni yoritish bundan mustasno.
- 5.4. Zaif toifalar (zo'ravonlik qurbonlari, nogironligi bo'lgan shaxslar, kam uchraydigan kasalliklarga chalingan shaxslar, og'ir hayotiy vaziyatga tushib qolgan shaxslar) — maxfiylikka bo'lgan mutlaq huquqdan foydalanadi. Zaif shaxsni identifikatsiya qilish mumkin bo'lgan shaxsiy ma'lumotlar, yashash joyi, o'qishi to'g'risidagi ma'lumotlar, fotosuratlar va videolarni tarqatishga yo'l qo'yilmaydi.

6. Shaxsiy ma'lumotlarni e'lon qilishni cheklash

6.1. Istisno asoslarsiz quyidagilarni e'lon qilish taqiqlanadi:

- yashash joyining aniq manzili
- aloqa ma'lumotlari (telefon, email)
- identifikatsiya hujjatlari
- bank ma'lumotlari
- tibbiy sirni tashkil etuvchi ma'lumotlar (medical confidentiality)
- shaxsiy va oilaviy hayotga oid ma'lumotlar

Shaxsiy ma'lumotlarni e'lon qilishda tahririyat shaxsni identifikatsiya qilish xavflarini va e'lon qilishning uzoq muddatli oqibatlarini baholashi shart.

7. Vizual materiallarni nashr etish

7.1. Vizual materiallarni nashr etishda tahririyat quyidagilarni bajarishi shart:

- matn, foto va videolarda shaxsni bevosita yoki bilvosita aniqlashga imkon beruvchi ma'lumotlar bor-yo'qligini tekshirish;
- shaxsiy ma'lumotlarni himoya qilish zarur bo'lganda yuzlarni xiralashtirish;
- metama'lumotlarni (geolokatsiyani) o'chirish;
- shaxsga doir ma'lumotlarning tarqalishiga to'sqinlik qiluvchi boshqa choralarni ko'rish.

8. Shaxsiy ma'lumotlarga ega materiallarni e'lon qilishdan oldin xavfni baholash

8.1. Nashrni e'lon qilishdan oldin tahririyat, jurnalist quyidagi mezonlar asosida baholashni amalga oshirishi shart:

- Shaxsiy ma'lumotlarni e'lon qilishda jamoatchilik manfaati bormi?
- Jamoatchilik manfaatiga zarar yetkazmagan holda shaxsiy ma'lumotlarsiz materialni e'lon qilish mumkinmi?

- Shaxsiy ma'lumotlar e'lon qilinganidan keyin zarar yetkazish ehtimoli bormi?
- Shaxsiy ma'lumotlar e'lon qilinganidan keyin javobgarlik va nizo kelib chiqish ehtimoli bormi?
- Shaxsiy ma'lumotlar qanday manbalardan olingan (Veb-saytlar, ijtimoiy tarmoqlar, rasmiy press-revizlar, deputatlikka nomzodlarning tarjimai holi, boshqa hujjatlar)
- Shaxsiy ma'lumotlarni e'lon qilish uchun rozilik olish zarurmi/mumkinmi.

9. Shaxsiy ma'lumotlar mavjud bo'lgan materiallarni nashr qilishdan oldin kelishish tartibi

- 9.1. Shaxsiy ma'lumotlarni o'z ichiga olgan materiallar muharrir tomonidan majburiy tekshiruvdan o'tkaziladi. Bahsli holatlarda huquqiy maslahat olish uchun yurist jalb qilinishi mumkin.
- 9.2. Tahririyat shaxsga javob qaytarish yoki shaxsiy ma'lumotlariga tuzatish kiritish huquqini taqdim etishi, shuningdek, shaxsiy ma'lumotlarni o'chirish bo'yicha so'rovlarni ko'rib chiqishi shart. Yakuniy qaror mas'ul muharrir zimmasida bo'ladi.

10. Yakuniy qoidalar

- 10.1. Reglament tahririyatning barcha shtatdagi va shtatdan tashqari xodimlari uchun majburiy hisoblanadi. Reglamentni buzish intizomiy javobgarlikka sabab bo'ladi.
- 10.2. Reglament qonunchilikdagi o'zgarishlar va raqamli texnologiyalarning rivojlanishini hisobga olgan holda muntazam ravishda qayta ko'rib chiqilishi lozim.
- 10.3. Tahririyatning barcha xodimlari Reglament bilan imzo qo'yib tanishtiriladi.



Yevropa Ittifoqi tomonidan
moliyalashtiriladi



ZAMONAVIY
JURNALISTIKANI
RIVOJLANTIRISH
MARKAZI



LPRC
LEGAL POLICY
RESEARCH CENTRE

UDRMI
O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI