Yevropa Ittifoqi tomonidan moliyalashtiriladi

ZAMONAVIY JURNALISTIKANI RIVOJLANTIRISH MARKAZI

LPRC LEGAL POLICY RESEARCH CENTRE

UDRMI O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI

YURISTLAR UCHUN RAQAMLI HUQUQLAR

Ularni qanday tushunish, qo‘llash va amaliyotda himoya qilish mumkin?

YURISTLAR UCHUN RAQAMLI HUQUQLAR

Ularni qanday tushunish, qo‘llash va amaliyotda himoya qilish mumkin?

Toshkent
2026

Yuristlar uchun raqamli huquqlar. Ularni qanday tushunish, qo‘llash va amaliyotda himoya qilish mumkin? Toshkent, 2026 — 95 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:
Lola Mahmudova (O‘zbekiston)
Madina Tursunova (O‘zbekiston)
Olga Didenko (Qozog‘iston)
Roman Reymer (Qozog‘iston)
Artyom Goryaynov (Qirg‘iziston)

Muharrir:
Lola Islamova

Mundarija

Ushbu qo‘llanmadan qanday foydalaniladi?

Zamonaviy jamiyat keng ko‘lamli raqamli transformatsiya jarayonini boshdan kechirmoqda. Raqamli texnologiyalar davlat boshqaruvi, iqtisodiyot va kundalik hayotning ajralmas qismiga aylandi. Bugungi kunda davlat xizmatlaridan foydalanish, biznes yuritish, ta’lim olish, kasbiy faoliyatni amalga oshirish hamda muloqot qilish tobora ko‘proq raqamli xizmatlar va axborot texnologiyalaridan foydalangan holda amalga oshirilmoqda.

Mazkur qo‘llanma davlat organlari, tijorat tashkilotlari, yuridik firmalar, nodavlat notijorat tashkilotlari hamda raqamli huquqlarga oid masalalar kundalik amaliyotning muhim qismiga aylanib borayotgan boshqa sohalarda faoliyat yuritayotgan yuristlar uchun amaliy qo‘llanma sifatida tayyorlandi.

An’anaviy darslikdan farqli o‘laroq, qo‘llanma raqamli huquqlarning butun nazariyasini batafsil bayon etishni maqsad qilmagan. Uning vazifasi asosiy masalalarni tezda tushunishga, ularning huquqiy tabiatini tushunishga va olingan bilimlarni kasbiy faoliyatda qo‘llashni o‘rganishga yordam berishdir.

Qo‘llanmaning tuzilishi “umumiylikdan xususiylikka” tamoyili asosida tuzilgan. Birinchi qismda raqamli huquqlar tushunchasi, ularning inson huquqlari tizimidagi o‘rni, xalqaro standartlar va O‘zbekiston Respublikasining milliy qonunchiligi ko‘rib chiqiladi. Ikkinchi qismda huquqshunoslar amaliyotda duch keladigan eng keng tarqalgan vaziyatlarga e’tibor qaratiladi: shaxsiy ma’lumotlarni himoya qilish, maxfiy ma’lumotlar, axborotdan foydalanish, raqamli kontent uchun javobgarlik, intellektual mulkni himoya qilish va ichki korporativ siyosatni ishlab chiqish. Uchinchi bo‘lim raqamli tahdidlar, axborot xavfsizligi va amaliy himoya choralariga bag‘ishlangan.

O‘quvchilar uchun qulaylik yaratish maqsadida ushbu qo‘llanmada axborotni taqdim etishning turli formatlaridan foydalanilgan:

- asosiy tushunchalarning mazmunini ochib beruvchi qisqacha nazariy izohlar;
- qonunchilikni amaliyotda qo‘llash bo‘yicha tavsiyalar;
- sud va huquqni qo‘llash amaliyotidan olingan misollar;
- xalqaro hujjatlar hamda normativ-huquqiy hujjatlarga havolalar;
- asosiy talablarning bajarilganligini tezkor tekshirish imkonini beruvchi chek-listlar;
- murakkab ma’lumotlarni osonroq anglashga yordam beruvchi sxemalar, jadvallar va qiyosiy materiallar.

Ushbu qo‘llanmani izchil ravishda boshidan oxirigacha o‘qish yoki undan ma’lumotnoma sifatida foydalanib, faqat muayyan kasbiy vazifani hal etish uchun zarur bo‘lgan bo‘limlarga murojaat qilish mumkin.

Shuni inobatga olish lozimki, raqamli texnologiyalar va ular bilan bog‘liq qonunchilik juda tez sur’atlarda rivojlanib bormoqda. Shu sababli mazkur qo‘llanmani amaliy faoliyat uchun tayanch manba sifatida qabul qilish hamda uni amaldagi normativ-huquqiy hujjatlar, sud amaliyoti va xalqaro hujjatlarni muntazam o‘rganish orqali to‘ldirib borish tavsiya etiladi.

Ushbu qo‘llanma yuristlarga raqamli huquqlar sohasidagi masalalarda yanada ishonchli yo‘l topishga, mijozlari va tashkilotlarining manfaatlarini samarali himoya qilishga hamda jamiyatning jadal raqamli transformatsiyasi sharoitida zamonaviy huquqiy yondashuvlarni amaliyotda qo‘llashga ko‘maklashishiga umid bildiramiz./ Umid qilamizki, ushbu qo‘llanma yuristlarga raqamli huquqlar masalalarida yanada ishonchli harakat qilish, mijozlar va tashkilotlar manfaatlarini samarali himoya qilish, shuningdek, jamiyatning tezkor raqamli transformatsiyasi sharoitida zamonaviy huquqiy yondashuvlarni qo‘llashda yordam beradi.

1-bo‘lim
Raqamli huquqlar nima?

1.1. Raqamli huquqlar nazariyasiga kirish

Zamonaviy dunyo jadal 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.

Dunyo bo‘ylab Internet foydalanuvchilari soni barqaror o‘sishda davom etmoqda. Shunday qilib, 2025-yil oktyabr oyida dunyo bo‘ylab internet foydalanuvchilari soni 6,4 milliarddan oshdi[1]. DataReportal ma’lumotlariga ko‘ra[2], O‘zbekistonda internetdan foydalanuvchilar soni 32,7 million kishini yoki mamlakat umumiy aholisining 92,2 foizini tashkil etadi.

Shu munosabat bilan raqamli huquqlar fenomenini rivojlantirish orqali raqamli makonni tartibga solish asosiy masalaga aylanmoqda.

Insonning raqamli huquqlari axborot inqilobining oqibati bo‘lib, ularning rivojlanishini harakatlantiruvchi kuch sifatida namoyon bo‘lmoqda.

Eng keng tarqalgan nazariy qarashlardan biri shundaki, “raqamli huquqlar” BMTning ko‘plab xalqaro hujjatlarida, shuningdek, mintaqaviy darajadagi hujjatlarda aks ettirilgan inson huquqlarining 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.

Raqamli huquqlarning mohiyatini tushunish uchun inson huquqlari evolyutsiyasini qisqacha ko‘rib chiqish zarur.

Inson huquqlari — har bir shaxsning millati, yashash joyi, jinsi, etnik kelib chiqishi, irqi, dini, tili yoki boshqa har qanday alomatlaridan qat’i nazar, ega bo‘lgan daxlsiz huquqlari majmuidir.

[1] https://www.statista.com/statistics/617136/digital-population-worldwide/?srsltid=AfmBOopuoIjbxLwhRpgdDEsIhkuTmSJ-jYKK6UPJ25PPsIw826z9BPwD

[2] https://datareportal.com/reports/digital-2025-uzbekistan

Asosiy tamoyillar

- Universallik: ular hamma joyda va hamma uchun amal qiladi.
- Ajralmasligi: ular o‘zboshimchalik bilan cheklanishi yoki olib qo‘yilishi mumkin emas, qonunda nazarda tutilgan hollar bundan mustasno.
- Bo‘linmaslik: fuqarolik, siyosiy, iqtisodiy va ijtimoiy huquqlar o‘zaro bog‘liq. Ulardan birisiz to‘laqonli foydalanib bo‘lmaydi.

Inson huquqlari avlodlari

Inson huquqlarini tasniflashning eng mashhur yondashuvlaridan biri 1979-yilda chex-fransuz huquqshunosi Karel Vashak tomonidan taklif etilgan inson huquqlari avlodlari konsepsiyasidir[3]. Muallif Buyuk fransuz inqilobining (1789-yil) “Ozodlik, tenglik, birodarlik” shioridan ilhomlangan[4]. Har bir “avlod” ushbu shiordagi so‘zlardan biriga mos keladi va huquqiy fikr taraqqiyotining tarixiy bosqichlarini aks ettiradi.

Birinchi avlod: Erkinlik (Fuqarolik va siyosiy huquqlar)

Ozodlik avlodining mohiyati insonni davlat zulmidan himoya qilish zarurati bilan bog‘liq. Huquqlarning birinchi avlodi “negativ huquqlar” atrofida jamlangan. Bu davlatning aralashuvdan o‘zini tiyishi (!) shartligini anglatadi. 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/kontseptsiia-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. Negativ huquqlardan farqli o‘laroq, pozitiv huquqlarni amalga oshirish davlatning tegishli huquqiy, tashkiliy va ijtimoiy mexanizmlarni yaratish, insonni ijtimoiy qo‘llab-quvvatlashning eng yuqori darajasini ta’minlash uchun infratuzilmani yaratish bo‘yicha faol harakatlarini nazarda tutadi.

Asosiy huquqlar:

- Mehnat qilish va adolatli mehnat haqi olish huquqi.
- Dam olish huquqi (mehnat vaqtining qonun bilan belgilangan davomiyligi).
- 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 shaxsga emas, balki butun guruhlarga (xalqlar, millatlar) yoki umuman insoniyatga tegishli bo‘lgan huquqlar atrofida shakllanadi. Shu sababli ushbu huquqlar jamoaviy huquqlar yoki birdamlik huquqlari deb yuritiladi.

Asosiy huquqlar:

- Rivojlanish huquqi.
- Tinchlik va xavfsizlik huquqi.
- Ekologik huquqlar, sog‘lom va toza atrof-muhitga bo‘lgan huquq.
- Insoniyatning umumiy merosidan foydalanish huquqi.

Karel Vashakning konsepsiyasi xalqaro tashkilotlar, jamoat harakatlari, ilmiy hamjamiyat vakillari, inson huquqlari himoyachilari va faollar tomonidan ko‘proq ijobiy qabul qilindi. Raqamli makonda, genom tadqiqotlari va boshqa innovatsion sohalarda inson huquqlarining to‘rtinchi avlodini asoslash va shakllantirishga qaratilgan sa’y-harakatlar amalga oshirildi.

Ushbu qo‘llanmaning predmeti raqamli huquqlar bo‘lganligi sababli, kelgusida aynan ularning rivojlanishi va mazmuniga e’tibor qaratiladi.

Axborot inqilobi nafaqat mavjud ishlab chiqarish usullari va turmush tarzining kengayishi va tarqalishiga, balki an’anaviy sanoat-tijorat jamiyatining yangi “aqlli” jamiyat bilan global almashinuviga olib keldi, natijada inson huquqlarining to‘rtinchi avlodi — raqamli inson huquqlari paydo bo‘ldi.

Raqamli huquqlarning o‘ziga xos xususiyati shundaki, ular raqamli shaklda mavjud bo‘lgan axborot va ma’lumotlar bilan bevosita bog‘liqdir.

Raqamli huquqlar raqamli texnologiyalar vositasida amalga oshiriladi hamda shaxsning raqamli muhit va raqamli xizmatlardan foydalanishi jarayonida vujudga keladi.

Insonning raqamli huquqlari sohasidagi majburiyatlar davlatlar va xususiy subyektlarning ham ijobiy (pozitiv), ham salbiy (negativ) majburiyatlarini o‘z ichiga oladi. Shu bois, insonning raqamli huquqlari inson huquqlarining alohida yangi avlodi (yoki mustaqil tizimi) sifatida e’tirof etilishi uchun yetarli asosga ega.[5]

Raqamli huquqlar — bu Internet makonidagi inson huquqlari.

Shunday bo‘lsa-da, bunday fikr yuritish uchun tegishli huquqiy asos yaratilishi kerak.

Masalan, Inson huquqlari kengashi tomonidan qabul qilingan «Internetda inson huquqlarini rag‘batlantirish, himoya qilish va amalga oshirish» Rezolyutsiyasida[6], jumladan, quyidagi qoidalar mustahkamlangan:

Internetdagi ma’lumotlardan foydalanish butun dunyo bo‘ylab qulay va inklyuziv ta’lim uchun keng imkoniyatlarni yaratadi, shu bilan ta’lim olish huquqini rag‘batlantirishning muhim vositasi bo‘lib, raqamli savodxonlikni ta’minlash va raqamli tafovutni bartaraf etish zarurligini ta’kidlaydi, chunki bu ta’lim olish huquqini amalga oshirishga ta’sir qiladi;

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.

BMTning Inson huquqlari bo‘yicha kengashi raqamli muhitda amalga oshiriladigan inson huquqlari oflayn rejimda amalga oshiriladigan huquqlar bilan bir xil himoyalanishi kerakligidan kelib chiqadi.

Keltirilgan qoidalardan ko‘rinib turibdiki, gap siyosiy huquqlar (so‘z va fikr ifodalash erkinligi), iqtisodiy (ta’lim olish huquqi) va jamoaviy (Internetning global xususiyati) huquqlar haqida bormoqda.

---

[5] Gun Nan. “Aqlli jamiyatda inson huquqlarining to‘rtinchi avlodi va asosiy konstitutsiyaviy huquqlarning transformatsiyasi”. 2024.

[6] https://www.refworld.org/ru/legal/resolution/unhrc/2016/ru/112398

Bosh Assambleya tomonidan qabul qilingan «Raqamli texnologiyalar kontekstida/ sharoitida inson huquqlarini rag‘batlantirish va himoya qilish» rezolyutsiyasi[7] avval qabul qilingan rezolyutsiya qoidalarini quyidagilar bilan to‘ldiradi:

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 oladi.

Shunday qilib, Birlashgan Millatlar Tashkiloti darajasida, birinchidan, raqamli huquqlarning mavjudligi, ikkinchidan, ular inson huquqlarining bevosita davomi ekanligi va, uchinchidan, universal, bo‘linmas, o‘zaro bog‘liq, o‘zaro qaram hamda bir-birini to‘ldiruvchi xususiyatga ega ekanligi e’tirof etiladi.

Raqamli huquqlarning universalligi, bo‘linmasligi va inson huquqlariga asoslangan yondashuvga qaramay, ularni Internetdan, shuningdek, turli raqamli texnologiyalar, platformalar va xizmatlardan foydalanish imkoniyatisiz tasavvur etib bo‘lmaydi.

Shu munosabat bilan Internetdan foydalanish huquqi asosiy raqamli huquqlardan biri hisoblanadi.

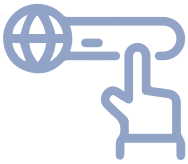
Insonning Internetdan foydalanishi davlatlar, texnologik kompaniyalar va boshqa uchinchi shaxslar faoliyati bilan bog‘liq turli muammolar, xavf-xatarlar va tahdidlarni yuzaga keltirishi mumkin.

Bunga, masalan, raqamli tafovut, Internetda fikr bildirish erkinligining cheklanishi, Internetga kirishning bloklanishi, shaxsiy hayot daxlsizligining buzilishi va boshqa ko‘plab holatlarni kiritish mumkin.

Shundan kelib chiqadiki, Internetdan foydalanish bilan bog‘liq «muammolar»ga javoban, asosan raqamli platformalardan va kengroq ma’noda Internetdan foydalanish jarayonida qo‘llaniladigan raqamli huquqlar majmui shakllandi.

[7] https://docs.un.org/ru/a/res/78/213

Raqamli huquqlar ro‘yxati

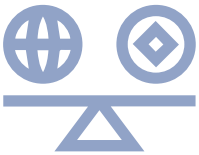


Internetdan foydalanish huquqi

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 fikr bildirish erkinligi

Insonning davlat chegaralaridan qat’i nazar hamda davlat organlari yoki korporatsiyalar tomonidan asossiz aralashuvsiz (senzurasiz) raqamli texnologiyalar va onlayn platformalar orqali har qanday turdagi axborot va g‘oyalarni izlash, olish va tarqatish huquqi.



Tarmoq neytralligi

Internetning ishlash tamoyili bo‘yicha, internet-provayderlar tijoriy yoki siyosiy maqsadlarda muayyan kontent, ilova yoki saytlarni bloklamasdan, sekinlatmasdan va ularga ustunlik bermasdan, barcha uzatilayotgan ma’lumotlarga bir xil yondashishi kerak.

Unutilish huquqi

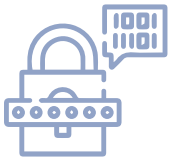
Shaxsga doir ma’lumotlar subyektiga muayyan asoslar mavjud bo‘lgan taqdirda, unga taalluqli ma’lumotlarni ommaviy manbalardan olib tashlashni yoki ularning tarqatilishini to‘xtatishni talab qilish imkonini beruvchi huquqiy mexanizm.

Kuzatuvdan himoya

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

Ma’lumotlarning maxfiyligi va ularni himoya qilish

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 haqiqiyligini 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 cheklovlari 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. Xalqaro huquqiy poydevorni tahlil qilish global raqamlashtirish davrida ham davlat suvereniteti chegaralarini va inson hamda uning huquqlarini himoya qilish mexanizmlarini tushunish uchun zarur shartdir.

Xalqaro standartlar

Global tartibga solishning poydevorini BMT Inson huquqlari bo'yicha kengashining 2012-yildagi A/HRC/20/L.13-sonli[8] rezolyutsiyasida mustahkamlangan huquqlar tengligi tamoyili tashkil etadi: "Inson oflayn muhitda ega bo'lgan huquqlar onlayn muhitda ham himoya qilinishi lozim".

Normativ-huquqiy bazaning asosini Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt (FSHXP[9]) tashkil etadi. Unda quyidagi moddalar nazarda tutilgan:

19-modda (Fikr bildirish va axborot olish erkinligi)	Axborotni «davlat chegaralaridan qat'i nazar» va "har qanday usulda" (shu jumladan, Internet orqali) tarqatish huquqini kafolatlaydi. Bu haqda Inson huquqlari bo'yicha qo'mita o'zining 34-sonli Umumiy tartibdagi izohida[10] 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 izohida[11] buni davlatlarning shaxsiy ma'lumotlarni kompyuterlar va ma'lumotlar banklarida to'plash va saqlashni qonuniy tartibga solish majburiyati sifatida talqin qiladi.

[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

FSHXP va Umumiy tartibdagi izohlardan tashqari, Maxsus ma’ruzachilarning rolini ham alohida ta’kidlash lozim.

BMTning Maxsus ma’ruzachilari o‘zlarining mavzuga oid ma’ruzalari orqali fikr erkinligi hamda fikrni erkin ifoda etish huquqini himoya qilish va rag‘batlantirish sohasidagi standartlarni rivojlantirishda muhim rol o‘ynaydi.

Maxsus ma’ruzachilarning pozitsiyasi de-fakto «yumshoq huquq» (soft law) xususiyatiga ega bo‘lib, alohida davlatlar uchun uni qo‘llash va milliy qonunchilikka implementatsiya qilish majburiy hisoblanmaydi. Shunga qaramay, Maxsus ma’ruzachilarning pozitsiyalari va ma’ruzalari alohida davlatlarning huquqiy tizimlarida huquqiy tafakkurning yo‘nalishi va rivojlanish tendensiyalarini belgilashga sezilarli ta’sir ko‘rsatadi.

Asosiy ma’ruzalar

Fikr erkinligi va uni erkin ifoda etish huquqini rag‘batlantirish va himoya qilish masalasi bo‘yicha Maxsus ma’ruzachi Frank La Rue ma’ruzasi, 2011-yil, A/HRC/17/27[12]

Mazkur ma’ruzada barcha shaxslarning Internet orqali har qanday axborot va g‘oyalarni izlash, olish hamda tarqatish huquqi bilan bog‘liq asosiy yo‘nalishlar va muammolar ko‘rib chiqilgan. Maxsus ma’ruzachi Internetning o‘ziga xos va o‘zgaruvchan tabiati shaxslarga nafaqat o‘z fikri va uni erkin ifoda etish huquqini, balki boshqa bir qator inson huquqlarini ham amalga oshirish, shuningdek, umuman jamiyat taraqqiyotiga hissa qo‘shish imkonini berishini alohida ta’kidlaydi.
Hisobotda davlatlar tomonidan internetdagi axborotga nisbatan senzuraning kuchaytirilishiga oid ayrim usullar bayon etilgan, xususan:

- kontentni o‘zboshimchalik bilan bloklash yoki filtrlash;
- qonuniy fikr bildirishni jinoyat deb hisoblash;
- javobgarlikni vositachilar zimmasiga yuklash;
- foydalanuvchilarni internetdan, jumladan, intellektual mulk huquqi to‘g‘risidagi qonunchilikni buzganlik asosida mahrum qilish;
- kiberhujumlar hamda shaxsiy hayot daxlsizligi va ma’lumotlar himoyasi huquqini yetarli darajada ta’minlamaslik.

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/29/32[13]

Ushbu ma’ruzada Maxsus ma’ruzachi raqamli xabarlarni uzatishda shifrlash va anonimlik vositalaridan 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 foydalanish 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 «sovuq ta’sir» (chilling effect) ko‘rsatadi,» ularni tanib qolishdan qo‘rqib jim turishga majbur qiladi.

Dezinformatsiya, fikr erkinligi va uni erkin ifoda etish Fikr erkinligi va uni erkin ifoda etish huquqini rag‘batlantirish va himoya qilish masalasi bo‘yicha Maxsus ma’ruzachi Ayreen Xan, 2021 yil, A/HRC/47/25[14]

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: Xan «soxta yangiliklar»ga qarshi kurash to‘g‘risidagi qonunlarni tanqid qilib, noaniq iboralar davlatlarga senzura uchun «siyosiy kart-blansh» 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.

[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

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.

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) haqidagi hisobotni taqdim etdi:

Kompaniyalar moderatsiya paytida “protsessual adolat”ni ta’minlashi kerak. Bu shuni anglatadiki, agar algoritm (SI) foydalanuvchining postini o‘chirsa, u quyidagilarni olishi lozim:

- aniq sababi ko‘rsatilgan bildirishnoma;

- qaror ustidan botga emas, balki haqiqiy xodimga e’tiroz bildirish imkoniyati.

Raqamli huquqlarni cheklash: «uch tarkibli test»

Raqamli huquqlar mutlaq emas va ma’lum shartlar asosida cheklanishi mumkin.

Masalan, FSHXP (Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt) 19-moddasining 3-bandiga ko‘ra, cheklovlar faqat uchta shartga rioya qilinganda qonuniy hisoblanadi:

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).

Qonuniy maqsad:

Milliy xavfsizlikni, tartibni, sog‘liqni, axloqni, boshqa shaxslarning huquqlarini himoya qilish.

Zarurat va mutanosiblik:

Eng kam aralashuv tamoyiliga ko‘ra, Davlat tanlangan chora (masalan, bloklash) maqsadga erishishning eng yengil usuli ekanligini isbotlashi shart. Agar bitta sharhni o‘chirish mumkin bo‘lsa, butun saytni bloklash mumkin emas.

Isbotlash majburiyati foydalanuvchining emas, davlatning zimmasiga yuklatiladi.

Fuqarolik va siyosiy huquqlar **to‘g‘risidagi xalqaro pakt (1984) qoidalariga oid cheklovlar va chekinishlarni sharhlash bo‘yicha Sirakuza tamoyillari (Sirakuza tamoyillari) muhim hujjat hisoblanadi**.

FSHXP ayrim hollarda muayyan maqsadlar (masalan, jamoat tartibini saqlash) yo‘lida ba’zi inson huquqlarini (masalan, so‘z yoki yig‘ilishlar erkinligini) cheklashga ruxsat beradi. Biroq davlatlar ko‘pincha bu kabi istisnolarni suiiste’mol qiladi.

Sirakuza tamoyillarining maqsadi — diktatorlik rejimlari ulardan repressiya uchun bahona sifatida foydalanishining oldini olish maqsadida “milliy xavfsizlik”, “jamoat tartibi” va “zarurat” atamalarining aniq huquqiy ta’rifini berishdir.

Sirakuza tamoyillari, shuningdek, Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt qoidalaridan cheklovlar va chekinishlarning talqini bo‘lib (matnda keyingi o‘rinlarda — “Sirakuza tamoyillari”), ularda quyidagilar belgilangan:

- «Inson huquqlarini amalga oshirishga doir hech bir cheklov Paktga zid kelmaydigan va cheklov joriy etilgan paytda amalda bo‘lgan umumiy qo‘llanuvchi milliy qonundan boshqacha tarzda kiritilmaydi»[15]. (Sirakuza tamoyillari, B.i.15).
- Bundan tashqari, «Pakt bilan kafolatlangan huquqning cheklanishini asoslash yuki davlat zimmasiga yuklatiladi». (Sirakuza tamoyillari, A.12).

> 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 kodifikatsiyalashda global yetakchi bo‘lib, «Bryussel effekti[16]» deb ataladigan holatni shakllantirmoqda, bunda Yevropa me’yorlari de-fakto global bo‘lib bormoqda.

---

[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%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

Me’yoriy-huquqiy bazaning markazida Inson huquqlari bo‘yicha Yevropa konvensiyasi (IHEK) joylashgan bo‘lib, u 10-modda (ifoda erkinligi) va 8-moddani (shaxsiy hayot) o‘z ichiga oladi, ular aslida Inson huquqlari bo‘yicha Yevropa sudi (IHEK) tomonidan raqamli voqelikka moslashtirilgan.

Misollar

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 Raqamli xizmatlar to‘g‘risidagi qonun (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 Raqamli bozorlar to‘g‘risidagi qonun (Digital Markets Act, 2022-y.)[20] bilan birga tilga olinadi. Ikkinchisini qabul qilishdan maqsad — qonunda “geytkiperlar” (gatekeepers — “darvozabonlar” yoki “kirish nazoratchilari”) deb ataluvchi yirik texnologiya kompaniyalarining qudratini 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.

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

[18] 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

№	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"ni taqiqlash (o‘z xizmatlarini raqobatchilardan ustun qo‘yish).
3	Shikoyatlarning shaffof mexanizmlarini joriy etish va bloklash sabablarini tushuntirish.	Messenjerlar va tizimlarning "interoperabelligi" (mosligi)ni ta’minlash.
4	Maxfiylikni himoya qilish. Din, salomatlik, orientatsiya 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 akkauntining bloklanishiga e’tiroz bildirishning huquqiy tartibi.	Oldindan o‘rnatilgan ilovalarni o‘chirib tashlashingiz va turli manbalardan dasturiy ta’minotni yuklab olishingiz mumkin.
6	Yevropa Ittifoqining har bir mamlakatidagi raqamli xizmatlar koordinatorlari + Yevrokomissiya (raqamli/texnologik 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 kontent hamda platformalarning javobgarligini tartibga solsa, 108+ Konvensiyasi, 95/46/EC-sonli Direktivasi va GDPR shaxsga doir ma’lumotlarni himoya qilishga qaratilgan.

Shaxsga doir ma’lumotlarni himoya qilish bilan bog‘liq xalqaro standartlar murakkab «evolyutsion» rivojlanish yo‘lini bosib o‘tgan bo‘lib, bugungi kunda ma’lumotlar maxfiyligi tamoyillarining uch «avlodi»ni tashkil etadi.

Ma’lumotlar maxfiyligi tamoyillarining birinchi «avlodi»ga 1981-yilda qabul qilingan Yevropa Kengashining Shaxsga doir ma’lumotlarni avtomatlashtirilgan tarzda qayta ishlashda jismoniy shaxslarni himoya qilish to‘g‘risidagi konvensiyasi, ya’ni 108-sonli[21] Konvensiya kiradi.

Ma’lumotlar maxfiyligi tamoyillarining ikkinchi «avlodi»ga, asosan, Shaxsga doir ma’lumotlarni qayta ishlashda jismoniy shaxslarni himoya qilish va bunday ma’lumotlarning erkin aylanishi to‘g‘risidagi 95/46/EC-sonli[22] Direktivasi kiradi.

Nihoyat, ma’lumotlar maxfiyligi standartlarining uchinchi «avlodi»ga 2016-yilda qabul qilingan GDPR[23], shuningdek, 108-sonli Konvensiya asosida 2018-yilda qabul qilingan 108+ Konvensiyasi kiradi.

[21] https://rm.coe.int/1680078c46

[22] https://www.tgl.net.ru/files/infosafety/директива95-46.pdf

[23] https://gdpr-info.eu/

Ma’lumotlar maxfiyligi tamoyillarining har bir «avlodi» doirasida shartli ravishda (!) o‘ntadan 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	Ko‘rsatilgan yoki mos keladigan maqsadlarda cheklangan (shu jumladan oshkor etilgan) foydalanish
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.
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. Raqamli huquqlar sohasidagi O‘zbekiston Respublikasining 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 axborot olish huquqiga jamoatchilik nazorati shaklida asos yaratadi: «Har kim qulay atrof-muhitga, uning holati to‘g‘risida haqqoniy axborotga ega bo‘lish huquqiga egadir. Davlat fuqarolarning ekologik huquqlarini ta’minlash va atrof-muhitga zararli ta’sirning oldini olish maqsadida shaharsozlik faoliyati sohasida jamoatchilik nazoratini amalga oshirish uchun sharoitlar yaratadi. Shaharsozlik hujjatlarining loyihalari qonunda belgilangan tartibda jamoatchilik muhokamasiga qo‘yiladi».

Maxfiylik va shaxsiy ma’lumotlarni himoya qilish

Konstitutsiyaning 31-moddasida shaxsiy hayot va shaxsga doir ma’lumotlarni himoya qilish huquqi belgilangan:

> Har bir inson shaxsiy hayotining daxlsizligi, shaxsiy va oilaviy siri, o‘z sha’ni va qadr-qimmati himoya qilinishi huquqiga ega.
>
> Shaxsning obro‘siga, qadr-qimmatiga yoki huquq subyektligiga ta’sir ko‘rsatishi mumkin bo‘lgan holatlarda uning roziligisiz ismini o‘zlashtirish, o‘zgartirish, qasddan buzib ko‘rsatish, undan raqamli makonda foydalanish bilan bog‘liq harakatlar nomulkiy huquqni buzish deb topiladi. Bu 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 noqonuniy yo‘l bilan 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.

O‘zbekiston Respublikasi Oliy sudining shaxsiy nomulkiy huquqlar va boshqa nomoddiy ne’matlarni himoya qilish to‘g‘risidagi da’volar bo‘yicha tushuntirishlariga ko‘ra, tegishli ma’lumotlarni tarqatish usulidan qat’i nazar (jumladan, bosma nashrlarda, radio, televideniye, veb-saytlar, veb-saytlar sahifalari, bloglar, ijtimoiy tarmoqlar profillari, messenjerlar va boshqa axborot-kommunikatsiya vositalarida), javobgarlar haqiqatga to‘g‘ri kelmaydigan, obro‘sizlantiruvchi ma’lumotlarning mualliflari, shuningdek, ularni tarqatgan shaxslar hisoblanadi.

Shaxsning roziligisiz tasvirni yozib olish yoki tarqatish, tasvirni buzish yoki uni kamsituvchi, obro‘sizlantiruvchi yoki chalg‘ituvchi kontekstda joylashtirish, tasvirdan tijorat maqsadlarida ruxsatsiz foydalanish, shaxsning asl qiyofasini buzishga olib keladigan tasvirga raqamli ishlov berish (shu jumladan dipfeyk, videomateriallarga kiritish, soxta “skrinshotlar” yaratish va h.k.), xabardor qilmasdan yoki cheklanmagan foydalanish huquqi bilan rozilik olmasdan internetda tarqatish tasvirga bo‘lgan huquqning buzilishi hisoblanadi.

Shaxsning tasvirga bo‘lgan huquqini himoya qilish harakatlarni qonunga xilof deb topish, raqamli makonda tasvirni olib tashlash yoki bloklash, vizual materialni olib tashlash, bloklash yoki undan foydalanishni texnik jihatdan cheklash majburiyatini yuklash (shu jumladan raqamli platformalar administratorlariga murojaat qilish orqali), tasvirdan kelgusida foydalanishni taqiqlash, moddiy zarar va ma’naviy ziyonni qoplash, huquq buzilishidan oldingi holatni tiklash orqali amalga oshiriladi.

Tasvirdan foydalanish salbiy kontekst bilan bog‘liq bo‘lgan hollarda (masalan, haqoratli nashrda, parodiyada, soxtalashtirilgan matn qo‘shilganda yoki buzib ko‘rsatilgan ma’lumotlar bilan foydalanilganda) nafaqat tasvirga bo‘lgan huquq, balki shaxsning sha’ni, qadr-qimmati, ishchanlik obro‘si hamda shaxsiy hayot daxlsizligi huquqi ham himoya qilinishi mumkin.

Shaxsning obro‘siga, qadr-qimmatiga yoki huquq subyektligiga ta’sir ko‘rsatishi mumkin bo‘lgan holatlarda uning roziligisiz ismini o‘zlashtirish, o‘zgartirish, qasddan buzib ko‘rsatish, undan raqamli makonda foydalanish bilan bog‘liq harakatlar nomulkiy huquqni buzish deb topiladi.

Axborot erkinligi to‘g‘risidagi qonunchilik

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; axborotning himoya qilinishini hamda shaxs, jamiyat va davlatning axborot xavfsizligini ta’minlashni o‘z ichiga oladi. Axborotdan foydalanish 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 O‘zbekiston Respublikasining “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasining “Axborot olish kafolatlari

va erkinligi to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasining “Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasining “Ommaviy axborot vositalari to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasining “Rasmiy statistika to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasining “Korrupsiyaga qarshi kurashish to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasining “Huquqiy axborotni tarqatish va undan foydalanish to‘g‘risida”gi 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 sirlar oshkor etilishining oldini olish uchun zarur bo‘lgan darajada yo‘l qo‘yiladi.”

“Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida”gi O‘zbekiston Respublikasi Qonunining 6-moddasida davlat hokimiyati va boshqaruvi organlarining faoliyati to‘g‘risidagi axborotdan foydalanish, agar mazkur axborot qonunda belgilangan tartibda davlat sirini yoki qonun bilan qo‘riqlanadigan boshqa sirni tashkil etuvchi ma’lumotlar jumlasiga kiritilgan bo‘lsa, cheklanishi belgilangan. Umumiy qoidaga ko‘ra, davlat organlari, fuqarolarning o‘zini o‘zi boshqarish organlari, jamoat birlashmalari, korxonalar, muassasalar, tashkilotlar va mansabdor shaxslar davlat sirini yoki qonun bilan qo‘riqlanadigan boshqa sirni 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;

O‘zbekiston Respublikasi hududida faoliyat ko‘rsatayotgan axborot-kutubxona muassasalari, arxivlar, idoraviy arxivlar, yuridik shaxslarning axborot tizimlaridagi ochiq fondlardagi mavjud ma’lumotlar.

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 istisnolar 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 rioya qilish uchun muhim ijtimoiy ahamiyatga ega bo‘lgan ma’lumotlar faol yoki avtomatik ravishda e’lon qilinishi kerak.

Axborotlashtirish 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 qoidalarni tasdiqlash haqida”gi qarori hamda OAVni davlat ro‘yxatidan o‘tkazish bo‘yicha davlat xizmatini ko‘rsatishning ma’muriy reglamenti.

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

> «Ommaviy axborot vositalari erkindir va qonunga muvofiq faoliyat ko‘rsatadi. Davlat ommaviy axborot vositalari faoliyatining erkinligini, ularning axborotni izlash, olish, undan foydalanish va uni tarqatish huquqini amalga oshirishini kafolatlaydi. Ommaviy axborot vositalari o‘zlari taqdim etadigan axborotning haqqoniyligi uchun javobgardir».

Senzuraga yo‘l qo‘ymaslik belgilangan, ommaviy axborot vositalari faoliyatiga to‘sqinlik qilish yoki aralashish esa qonunga muvofiq javobgarlikka sabab bo‘ladi.

O‘zbekistonning ommaviy axborot vositalari to‘g‘risidagi qonunchiligi axborot makonida turli subyektlar, jumladan, OAV tomonidan yaratiladigan va tarqatiladigan axborotning haqqoniyligini ta’minlashga qaratilgan huquqiy asoslarni yaratadi.

OAV to‘g‘risidagi Qonun quyidagi turdagi ma’lumotlarni tarqatishni taqiqlaydi:

Axborot toifasi	Dezinformatsiya bilan bog‘liqligi
Konstitutsiyaviy tuzumni zo‘rlik bilan o‘zgartirishga yoki separatizmga da’vat qiluvchi axborot	Davlat tuzumiga putur yetkazishga qaratilgan nashrlarni to‘g‘ridan-to‘g‘ri taqiqlash, siyosiy dezinformatsiya shakli
Terrorizm va diniy ekstremizmni targ‘ib qilish	Ko‘pincha faktlarni buzib ko‘rsatish orqali amalga oshiriladi — bu noto‘g‘ri ma’lumotning xavfli shakli hisoblanadi.
Davlat sirini yoki boshqa maxfiy axborotni oshkor qilish	"Shov-shuvli haqiqat" sifatida taqdim etilib, chalg‘itishga olib kelsa, bu qoidabuzarlik hisoblanadi.
Milliy, irqiy, etnik yoki diniy adovatni qo‘zg‘atuvchi axborot	Dezinformatsiya jamoatchilik fikrini manipulyatsiya qilish va mojarolarni avj oldirish uchun ishlatilishi mumkin./ Dezinformatsiya jamoatchilik fikrini manipulyatsiya qilish va nizolarni keskinlashtirish vositasi sifatida qo‘llanilishi mumkin.
Surishtiruv, tergov yoki sud materiallarini e’lon qilishni taqiqlash	Sud qaroridan oldin spekulyativ yoki soxta ma’lumotlarga qarshi kurashish
Fuqarolarning sha’ni va qadr-qimmati yoki ishchanlik obro‘siga putur yetkazuvchi axborot	Shaxsning sha’niga putur yetkazuvchi, bila turib yolg‘on ma’lumot va faktlarni e’lon qilishni taqiqlash./ Shaxsni obro‘sizlantiruvchi bila turib yolg‘on ma’lumotlar va faktlarni e’lon qilish taqiqlanadi.

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 faoliyatidagi cheklovlarning amaliy ahamiyati quyidagilar bilan belgilanadi:

- Ommaviy axborot vositalarining e’lon qilishdan oldin ma’lumotlarning ishonchliligini tekshirish va yolg‘on ma’lumotlar, feyklar, targ‘ibot va manipulyatsiyalarning tarqalishiga huquqiy to‘siq yaratish mas’uliyati va majburiyatlari orqali oldini olish funksiyasi.
- Shaxs manfaatlarini, jamoat tartibini va davlat xavfsizligini himoya qilish mexanizmlari orqali himoya qilish funksiyasi.
- Ommaviy axborot vositalari va jurnalistlar uchun tahririyat siyosati yo‘nalishlari va chegaralarini belgilash orqali axloqiy funksiya.

OAV bosh muharrir yoki jurnalist timsolida haqiqatga to‘g‘ri kelmaydigan materiallarni tarqatganlik uchun quyidagi hollarda javobgar bo‘lmaydi:

- rasmiy xabarlar, normativ-huquqiy hujjatlar yoki rasmiy statistik hisobot ma’lumotlaridan olingan yoxud axborot agentliklari yoki matbuot xizmatlari, shuningdek, davlat hokimiyati va boshqaruvi organlarining rasmiy veb-saytlari orqali olingan;
- oldindan yozib olinmasdan efirga uzatiladigan mualliflik nutqlarida mavjud bo‘lsa yoki nutqlarning so‘zma-so‘z takrorlanishi (stenografik, audio-, videoyozuv) bo‘lsa.

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 bo‘yicha xalqaro standartlarga mos keladi. Biroq, javobgarlikdan ozod qilishning cheklangan hajmi ommaviy axborot vositalari 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 (korrupsiya, 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.

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 axborotni taqdim etish	Axborot manbalarini tekshirish, fakt-cheking.
Qonunchilik va xalqaro shartnomalar talablariga rioya qilish	OAV faoliyati to‘g‘risidagi qonunchilikka rioya qilish
Aybsizlik prezumpsiyasi	Gumon qilinuvchi, ayblanuvchi, sudlanuvchi va hukm chiqarilgan shaxslar to‘g‘risidagi materiallarni e’lon qilishda aybsizlik prezumpsiyasi tamoyiliga rioya etish
Kasbiy odob-axloq qoidalariga rioya qilish	Ichki axloqiy qoidalarni belgilash
Shaxsiy hayot haqidagi ma’lumotlardan shaxsiy maqsadlarda foydalanishni taqiqlash	Maxfiy hisoblangan shaxsiy hayotga oid ma’lumotlarni tarqatishni taqiqlash, bundan ommaviy foydalanish mumkin bo‘lgan manbalarda e’lon qilingan ma’lumotlar mustasno

Shu bilan birga, jurnalistlarning ishonchliligini tekshirish bo‘yicha majburiyatlar kengaytirilgan formatda talqin qilinishi va shaxslarning fikrlari va mulohazalariga tatbiq etilishi mumkin. Qonunda «halol surishtiruv,» «manbani jurnalistik tekshirish» tushunchalari mustahkamlanmagan, bu esa professional standartlarga rioya qilgan holda ham OAVni himoya qilishni qiyinlashtiradi. OAV va jurnalistlar nafaqat to‘g‘ridan-to‘g‘ri dezinformatsiya uchun, balki uchinchi shaxslardan olingan ma’lumotlarni tekshirib bo‘lmagani uchun ham 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. Jurnalistlar hamjamiyati faoliyatining axloqiy tamoyillari o‘z-o‘zini tartibga solish mexanizmlari ixtiyoriga qoldirilishi lozim.

Ishonchli axborotni tarqatish bo‘yicha talablar Internet tarmog‘idagi o‘zgarmas shaklda tarqatish uchun mo‘ljallangan, tahririy-nashriyot ishlovidan o‘tgan elektron shakldagi hujjatlar va ma’lumotlarni o‘z ichiga olgan axborot resurslariga tenglashtiriladigan Internet OAVga nisbatan ham qo‘llaniladi. Internet OAV o‘z veb-saytida OAVni boshqa mediaresurslardan farqlash imkonini beruvchi davlat ro‘yxatidan o‘tkazilganligi to‘g‘risidagi guvohnomaning sanasi va raqamini joylashtirishi shart.

Ommaviy axborot vositalarida tarqatilgan baholovchi fikr yoki mulohaza o‘zining huquqlari va qonuniy manfaatlariga daxldor deb hisoblagan shaxs FK 100-moddasining oltinchi qismi va “Ommaviy axborot vositalari to‘g‘risida”gi Qonunning 34-moddasiga muvofiq, o‘ziga berilgan javob, sharh, luqma berish huquqidan foydalanib, mazkur ommaviy axborot vositasida tarqatilgan fikrlarning asossizligini isbotlash uchun ularga boshqacha baho berishni talab qilishga haqli.

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 matnga asosli tuzatish kiritishga 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 ommaviy axborot vositalari 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 (bundan buyon matnda “O‘zkomnazorat” deb yuritiladi), Axborot va ommaviy kommunikatsiyalar sohasidagi ekspert komissiyasi ishtirok etadi.

Internet tarmog‘idagi axborot resurslariga kirishni cheklash quyidagi tartibda amalga oshiriladi:

Internet tarmog‘ining taqiqlangan axborotlarni o‘z ichiga olgan axborot resurslarini **aniqlash**.

Taqiqlangan axborotni o‘z ichiga olgan Internet tarmog‘i axborot resursining identifikatsiya ma’lumotlarini Reyestrga **kiritish**.

Internet tarmog‘ining axborot resursiga kirishni **cheklash**.

Axborotning huquqqa xilof xususiyatini baholashda O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonunining 12^1-moddasiga amal qilish lozim. “O‘zkomnazorat” amaldagi qonun hujjatlariga muvofiq noqonuniy deb e’tirof etiladigan, quyidagi maqsadlarda tarqatiladigan axborotni aniqlash bo‘yicha kompleks monitoring olib boradi:

- O‘zbekiston Respublikasining mavjud konstitutsiyaviy tuzumini, hududiy yaxlitligini zo‘ravonlik yo‘li 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, shuningdek, ushbu g‘ayriqonuniy harakatlarni muvofiqlashtirish;
- jamoat tartibi yoki xavfsizligiga tahdid soluvchi bila turib yolg‘on ma’lumotlarni tarqatish;
- urush, zo‘ravonlik va terrorizm, shuningdek, diniy ekstremizm, separatizm va fundamentalizm g‘oyalarini targ‘ib qilish;
- davlat sirlarini yoki qonun bilan qo‘riqlanadigan boshqa sirni tashkil etuvchi ma’lumotlar oshkor etilganda;

- milliy, irqiy, etnik yoki diniy adovat qo‘zg‘atuvchi, shuningdek, fuqarolarning sha’ni va qadr-qimmati yoki ishchanlik obro‘siga putur yetkazuvchi, ularning shaxsiy hayotiga aralashishga yo‘l qo‘yuvchi ma’lumotlarni tarqatish;

- jamiyatga, davlatga, davlat ramzlariga hurmatsizlikni namoyish etuvchi axborotni, shu jumladan uyatsiz shaklda ifodalangan axborotni tarqatish;

- giyohvandlik vositalari, psixotrop moddalar va prekursorlarni targ‘ib qilish;

- pornografiyani targ‘ib qilish, zo‘ravonlik va shafqatsizlikka sig‘inish, shuningdek, o‘z joniga qasd qilishga undash;

- boshqa shaxslarga tegishli bo‘lgan intellektual mulk obyektlaridan noqonuniy foydalanish;

- fuqarolarni, shu jumladan voyaga yetmaganlarni ularning hayoti va (yoki) sog‘lig‘iga yoxud boshqa shaxslarning hayoti va (yoki) sog‘lig‘iga tahdid soluvchi g‘ayriqonuniy harakatlarni sodir etishga undashga yoki boshqacha tarzda jalb etishga qaratilgan axborotni tarqatish.

Taqiqlangan axborotni o‘z ichiga olgan Internet tarmog‘ining axborot resurslarini aniqlash maqsadida “O‘zkomnazorat” qonun hujjatlarida belgilangan tartibda Internet tarmog‘ining axborot resurslari monitoringini amalga oshiradi. Veb-saytdan yoki axborotdan foydalanishni cheklash “O‘zkomnazorat”ning monitoringi natijalariga ko‘ra yoki Axborot va ommaviy kommunikatsiyalar sohasidagi ekspert komissiyasining qarori asosida amalga oshiriladi.

“O‘zkomnazorat” veb-sayt yoki veb-sayt sahifasi egasiga 24 soat ichida noqonuniy kontentni olib tashlash to‘g‘risida bildirishnoma yuboradi. Veb-sayt egasi noqonuniy deb topilgan materialni olib tashlashga yoki “O‘zkomnazorat”ning xulosasi va Ekspert komissiyasining saytda qonun hujjatlari bilan taqiqlangan axborot mavjudligi to‘g‘risidagi qarori ustidan sud tartibida shikoyat qilishga haqli.

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:

- Internet tarmog‘idagi taqiqlangan axborotlarni o‘z ichiga olgan axborot resurslarini aniqlash;

- taqiqlangan axborotni o‘z ichiga olgan Internet tarmog‘i axborot resursining identifikatsiya ma’lumotlarini Reyestrga kiritish;

- Internet tarmog‘ining axborot resursiga kirishni cheklash.

Noqonuniy axborotni aniqlash bo‘yicha yetarlicha keng vakolatlarga 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‘ining axborot resurslari to‘g‘risidagi so‘rovlar asosida taqdim etiladi, bu esa xalqaro standartlarga ziddir.

Qonun hujjatlarida nazarda tutilgan shikoyat qilish mexanizmlari “O‘zkomnazorat”ning axborotni noqonuniy deb topish bo‘yicha harakatlari ustidan sudga shikoyat qilish uchun umumiy huquq beradi. Vaholanki, xalqaro standartlar axborot resurslaridan foydalanishni cheklash ustidan shikoyat qilishning sudgacha bo‘lgan mustaqil apellyatsiya mexanizmini yaratishga asoslangan.

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, Reyestrdan foydalanish cheklangan.
Tadbirlar/ Protseduralar	Kontentni cheklash sud qarorisiz yakka tartibdagi ma’muriy qaror orqali amalga oshiriladi.	Kontentga kirishni cheklash to‘g‘risidagi qarorlarni 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 shikoyat qilishning sudgacha bo‘lgan mexanizmlari 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.

2-bo‘lim
Yuristlar uchun raqamli huquqlar

2.1. Xodimlar, mijozlar va kontragentlarning shaxsga doir ma’lumotlarini himoya qilish

O‘zbekiston Respublikasida shaxsga doir ma’lumotlar, fuqarolarning shaxsiy hayoti va nomulkiy huquqlarini himoya qilish to‘g‘risidagi qonun hujjatlari amal qiladi. Shaxsga doir ma’lumotlarni qonunga xilof ravishda to‘plash va qayta ishlash, shaxsiy hayot to‘g‘risidagi ma’lumotlarni oshkor qilish uchun ma’muriy va jinoiy javobgarlik nazarda tutilgan.

O‘zbekiston Respublikasining 2019-yil 2-iyuldagi “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘RQ-547-sonli Qonuniga muvofiq, shaxsga doir ma’lumotlar — bu shaxsni identifikatsiya qilish imkonini beradigan har qanday axborot yoki ma’lumotlardir. Qonunda shaxsga doir ma’lumotlarning qat’iy va to‘liq ro‘yxati belgilanmagan. Unda nazarda tutilgan umumiy talablar shaxsning shaxsiy hayoti, kasbiy faoliyati va harakatlanishi bilan bog‘liq ma’lumotlarning keng doirasiga nisbatan tatbiq etiladi.

Ma’lumotlarning muayyan jismoniy shaxs yoki uning mol-mulki bilan bog‘liqligi, shuningdek, bunday ma’lumotlarning boshqa shaxs yoki tashkilot tomonidan shaxsiy ma’lumotlardan foydalanish va saqlash maqsadini hisobga olgan holda to‘planishi va foydalanilishi asosiy mezon hisoblanadi.

Shaxsga doir ma’lumotlar to‘g‘risidagi qonun ma’lumotlar bazalarida ishlov beriladigan shaxsga doir ma’lumotlarning to‘rt turini belgilaydi:

maxsus shaxsiy ma’lumotlar — irqiy yoki ijtimoiy kelib chiqishi, siyosiy, diniy yoki mafkuraviy e’tiqodlari, siyosiy partiyalar va kasaba uyushmalariga a’zoligi, shuningdek, jismoniy yoki ruhiy salomatligi, shaxsiy hayoti va sudlanganligi to‘g‘risidagi ma’lumotlar;

biometrik shaxsiy ma’lumotlar — subyektning anatomik va fiziologik xususiyatlarini tavsiflovchi shaxsiy ma’lumotlar;

genetik shaxsiy ma’lumotlar — subyektning irsiy yoki orttirilgan xususiyatlariga tegishli bo‘lgan shaxsiy ma’lumotlar bo‘lib, ular subyektning biologik namunasini tahlil qilish yoki ekvivalent ma’lumot olish imkonini beruvchi boshqa elementni tahlil qilish natijasi hisoblanadi;

hamma foydalanishi mumkin bo‘lgan shaxsiy ma’lumotlar — subyektning roziligi bilan erkin foydalanish mumkin bo‘lgan yoki maxfiylik talablariga mos kelmaydigan shaxsiy ma’lumotlar.

Shaxsga doir ma’lumotlarni qayta ishlashda mulkdor va (yoki) operator shaxsga doir ma’lumotlar xavfsizligiga tahdidlarni inobatga olgan holda ularni himoya qilish bo‘yicha tashkiliy va texnik choralarni joriy etishi shart.

Mulkdor (operator) xodimlarining shaxsga doir ma’lumotlari hamda mulkdor (operator) ning xodimi hisoblanmaydigan ma’lumotlar subyektlarining shaxsga doir ma’lumotlari alohida ma’lumotlar bazalarida ishlov berilishi kerak.

MUHIM!

Shaxsga doir ma’lumotlarga ishlov berish faqat ma’lumotlar subyektining xabardorligi va ixtiyoriy, aniq roziligi bilan yoki boshqa qonuniy asosda amalga oshirilishi mumkin.

Shaxsiy ma’lumotlarga ishlov berishning asosiy shartlari quyidagilardan iborat:

Shaxsga doir ma’lumotlar subyektining roziligi	Talabning huquqiy asosi	Izohlar
Shaxsga doir ma’lumotlarni qayta ishlashning qonuniy maqsadlari	Shaxsga doir ma’lumotlar to‘g‘risidagi Qonunning 19-moddasi: Shaxsga doir ma’lumotlarga ishlov berish maqsadlari mulkdorning va (yoki) operatorning faoliyatini tartibga soluvchi normativ-huquqiy hujjatlar, nizomlar, ta’sis hujjatlari yoki boshqa hujjatlar bilan belgilanadi hamda ushbu Qonunga muvofiq bo‘lishi kerak. Shaxsga doir ma'lumotlarga ishlov berishning maqsadlari ularni yig‘ish chog‘ida ilgari bildirilgan maqsadlarga, shuningdek mulkdorning va (yoki) operatorning huquq va majburiyatlariga muvofiq bo‘lishi kerak.	Shaxsga doir ma’lumotlarni qayta ishlash maqsadlari va usullarini mahalliy me’yoriy hujjatda tasdiqlash
Shaxsga doir ma’lumotlar toifalari	Shaxsga doir ma’lumotlar to‘g‘risidagi Qonunning 25-moddasi: Maxsus toifadagi shaxsga doir ma’lumotlarga Irqiy yoki ijtimoiy kelib chiqishga oid ma'lumotlar, siyosiy, diniy yoki dunyoqarashga oid e'tiqodlar, siyosiy partiyalar va kasaba uyushmalariga a'zolik to‘g‘risidagi ma'lumotlar, shuningdek jismoniy yoki ruhiy (psixik) salomatlikka taalluqli ma'lumotlar, shaxsiy hayot va sudlanganlik to‘g‘risidagi ma’lumotlar kiradi. Shaxsga doir ma’lumotlar to‘g‘risidagi Qonunning 26-moddasi: Biometrik ma’lumotlar — subyektning anatomik va fiziologik o‘ziga xos xususiyatlarini tavsiflovchi shaxsga doir ma’lumotlardir. Genetik ma’lumotlar — subyektning nasldan-naslga o‘tgan yoki orttirilgan xususiyatlariga taalluqli bo‘lgan, subyektning biologik qiyofasini tahlil qilish yoki muqobil axborot olish imkonini beradigan boshqa elementni tahlil qilish natijasi bo‘lgan shaxsga doirma’lumotlardir	**Qayta ishlash maqsadlari uchun zarur va yetarli bo‘lgan shaxsga doir ma’lumotlar tarkibini tasdiqlash.** Korxonada kirishni nazorat qilish va boshqarish tizimlarida (KNBT) biometrik ma’lumotlardan foydalanilganda subyektning roziligini olish Maxsus, biometrik va genetik ma’lumotlarni o‘z ichiga olgan shaxsiy ma’lumotlar bazalarini ro‘yxatdan o‘tkazish. Tahdidlar turini baholash hamda shaxsga doir ma’lumotlar bazalarini himoya qilish bo‘yicha tashkiliy va texnik choralarni joriy etish
Shaxsga doir ma’lumotlarni qayta ishlash muddatlari	Shaxsga doir ma’lumotlar to‘g‘risidagi Qonunning 10-moddasi: Shaxsga doir ma'lumotlarni saqlash muddati ularni yig‘ish va ularga ishlov berish maqsadiga erishish sanasi bilan belgilanadi. Shaxsga doir ma’lumotlar to‘g‘risidagi Qonunning 10-moddasi: Shaxsga doir ma'lumotlarga ishlov berish muddati subyektning o‘z shaxsga doir ma'lumotlariga ishlov berishga roziligi amal qiladigan muddatdan oshib ketmasligi kerak.	

Shaxsga doir ma'lumotlarga ishlov berishga rozilik berish va rozilikni chaqirib olish tartibi	Shaxsga doir ma'lumotlar to'g'risidagi Qonunning 21-moddasi: Shaxsga doir maxsus ma'lumotlarga ishlov berish uchun subyektning yozma shakldagi, shu jumladan elektron hujjat tarzidagi roziligi talab etiladi. Subyekt shaxsga doir ma'lumotlarga ishlov berish uchun berilgan rozilikni ushbu rozilik qanday shaklda berilgan bo'lsa, shunday shaklda yoxud yozma shaklda, shu jumladan elektron hujjat tarzida chaqirib oladi.	Shaxsiy ma'lumotlarni qayta ishlashga rozilik shaklini ishlab chiqish va tasdiqlash. Shaxsga doir ma'lumotlarni qayta ishlashga berilgan rozilikni chaqirib olish bo'yicha murojaatlarni ko'rib chiqish tartibi tasdiqlash.
Shaxsiy ma'lumotlarni yo'q qilish huquqi (unutilish huquqi)	Shaxsga doir ma'lumotlar to'g'risidagi Qonunning 17-moddasi: «Shaxsga doir ma'lumotlar mulkdor va (yoki) operator, shuningdek uchinchi shaxs tomonidan quyidagi hollarda yo'q qilinishi lozim: shaxsga doir ma'lumotlarga ishlov berish maqsadiga erishilganda; subyektning shaxsga doir ma'lumotlarga ishlov berish uchun berilgan roziligi chaqirib olinganda; shaxsga doir ma'lumotlarga ishlov berishning subyekt bergan rozilik bilan belgilangan muddati o'tganda; sudning qarori qonuniy kuchga kirganda»	Shaxsga doir ma'lumotlarni yo'q qilish tartibini tasdiqlash, Shaxsga doir ma'lumotlarni yo'q qilish dalolatnomalarini ishlab chiqish
Transchegaraviy uzatishga rozilik	Shaxsga doir ma'lumotlar to'g'risidagi Qonunning 15-moddasi: «Shaxsga doir ma'lumotlarning bir xilda himoya qilinishini ta'minlamaydigan chet davlatlar hududiga shaxsga doir ma'lumotlarni transchegaraviy uzatish quyidagi hollarda amalga oshirilishi mumkin: subyektning o'z shaxsga doir ma'lumotlarini transchegaraviy uzatish bo'yicha roziligi mavjud bo'lganda»	Shaxsiy ma'lumotlarni qayta ishlashga rozilik shakliga ma'lumotlarni uzatish va qayta ishlash maqsadlari, shaxslar, tashkilotlar, transchegaraviy uzatish yurisdiksiyasi ko'rsatilgan holda transchegaraviy uzatish holatlarini kiritish. Transchegaraviy uzatish yurisdiksiyasida shaxsiy ma'lumotlarni himoya qilish to'g'risidagi qonunchilik mavjudligini tekshirish. Shaxsiy ma'lumotlarni transchegaraviy uzatishda ularning himoyasini ta'minlash bo'yicha majburiyatlarni nazarda tutish.
Shaxsga doir ma'lumotlarni qayta ishlashda sun'iy intellekt texnologiyalaridan foydalanish	MJtKning 46²-moddasi[24]: «Sun'iy intellekt texnologiyalaridan foydalangan xolda shaxsga doir ma'lumotlarga qonunga xilof ravishda ishlov berish, ularni ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog'ida tarqatish, — ma'muriy huquqbuzarlikni sodir etish qurollarini musodara qilib, bazaviy hisoblash miqdorining ellik baravaridan yuz baravarigacha miqdorda jarima solishga sabab bo'ladi»	Shaxsga doir ma'lumotlarni sun'iy intellekt texnologiyalaridan foydalangan holda qayta ishlash usullarini cheklash. Qayta ishlashning qonuniy maqsadlari mavjud bo'lgan va ma'lumotlar subyekti huquqlarining buzilishi xavfi mavjud bo'lmagan hollarda, sun'iy intellektdan foydalanishga subyektning alohida roziligini nazarda tutish.
Shaxsga doir ma'lumotlarni qayta ishlash uchun mas'ul shaxsni tayinlash	3477-sonli buyruqning 6-bandiga muvofiq: «Shaxsiy ma'lumotlarga ishlov berish va ularni himoya qilish uchun mas'ul shaxsning asosiy vazifalari quyidagilardan iborat: • shaxsga doir ma'lumotlarga ishlov berishda ularning himoya qilinishini, yaxlitligini va but saqlanishini hamda maxfiyligiga rioya etilishini ta'minlash;	Shaxsga doir ma'lumotlarni qayta ishlash va himoya qilish uchun mas'ul shaxsni tayinlash. Shaxsiy ma'lumotlarga ishlov berish huquqiga ega bo'lgan shaxslarning lavozim yo'riqnomalari va doirasi tasdiqlansin.

[24] O'zbekiston Respublikasining 21.01.2026-yildagi «Sun'iy intellektni qo'llashda yuzaga keladigan munosabatlarni tartibga solish munosabati bilan O'zbekiston Respublikasining ayrim qonun hujjatlariga qo'shimcha va o'zgartirishlar kiritish to'g'risida»gi O'RQ-1115-sonli Qonuni https://lex.uz/ru/docs/8011377

- shaxsga doir ma'lumotlarga qonunga xilof ravishda ishlov berilishining oldini olish, qonunchilikda belgilangan talablar buzilganligi aniqlangan hollarda mulkdor va (yoki) operator bilan kelishgan holda shaxsga doir ma'lumotlarni bloklash (cheklash);
- mulkdor va (yoki) operatorning shaxsga doir ma'lumotlar bazasi xavfsizligini ta'minlash bo‘yicha axborot xavfsizligi siyosatini tashkil etish va muvofiqlashtirish;
- shaxsga doir ma'lumotlar bilan ishlovchi xodimlar uchun seminar-treninglar tashkil etish;

MUHIM!

Tegishli rozilikning yo‘qligi, ishlov berishning belgilangan maqsadlaridan chetga chiqish yoki qonuniylik va yetarlilik tamoyillariga rioya qilmaslik shaxsiy huquqlarning buzilishi deb tan olinadi va fuqarolik-huquqiy javobgarlikka sabab bo‘ladi.

Shaxsga doir ma’lumotlarga ishlov berish qonunga xilof deb topilganda, sud operator zimmasiga ma’lumotlarni to‘liq o‘chirish va ularning zaxira nusxalarini ham yo‘q qilish majburiyatini yuklashi mumkin.

SUD AMALIYOTI:

2025-yil 26-dekabrdagi
3-2203-2502/2951-sonli ma’muriy ish.

Qoidabuzarlik holatlari:

Banklardan birining bank xizmatlari markazi boshlig‘i o‘zi uchun maqsadli ko‘rsatkichlar (KPI) sifatida belgilangan aholi bandligi ko‘rsatkichlarini yaxshilash maqsadida fuqarolarning roziligisiz 68 nafar fuqaroning STIR/JSHSHIR ma’lumotlarini olgan va ulardan foydalangan.

Fuqarolarning shaxsga doir ma’lumotlari yangiish.mehnat.uz platformasiga kiritilib, ular o‘zini o‘zi band qilgan shaxslar sifatida rasmiylashtirilgan.

JSHSHIR — shaxsga doir ma’lumot hisoblanib, unga qonunga xilof ravishda ishlov berish shaxsga doir ma’lumotlar subyektining huquqlarini to‘g‘ridan-to‘g‘ri buzish hisoblanadi.

Sud qarorida «shaxsga doir ma’lumotlarga ishlov berish shaxsga doir ma’lumotlar subyektining roziligi bilan amalga oshirilishi» alohida ta’kidlangan.

Bank xodimi MJtKning 46-moddasi (“Shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilikni buzish”) bo‘yicha aybdor deb topilgan va unga nisbatan jarima miqdorini belgilashda MJtKning 33-moddasiga (“Yengilroq ma'muriy jazo chorasining qo‘llanilishi”) asoslanib, unga BHMning 7 baravari miqdorida jarima jazosi tayinlandi.

Shaxsga doir ma’lumotlarga ishlov berishning qonuniyligi ustidan davlat nazorati bir qator davlat organlari tomonidan amalga oshiriladi:

Nomi	Huquqiy asosi	Vakolatlari
O‘zbekiston Respublikasi Vazirlar Mahkamasi	«Shaxsga doir ma’lumotlar to‘g‘risida» gi Qonun	quyidagilarni belgilaydi: • xavfsizlikka tahdidlarga qarab shaxsga doir ma’lumotlarga ishlov berishda ularning himoyalanganlik darajalari; • shaxsga doir ma’lumotlarga ishlov berishda ularning himoyasini ta’minlashga doir talablar, ularning bajarilishi shaxsga doir ma’lumotlarning belgilangan himoya darajalarini ta’minlaydi; • biometrik va genetik ma’lumotlarning moddiy manbalariga va bunday ma’lumotlarni shaxsiy ma’lumotlar bazalaridan tashqarida saqlash texnologiyalariga qo‘yiladigan talablar
O‘zbekiston Respublikasi Ichki ishlar vazirligi huzuridagi Migratsiya va personallashtirish departamenti	O‘zbekiston Respublikasi Vazirlar Mahkamasining 08.02.2020 yildagi 71-son qarori Shaxsga doir ma’lumotlar bazalarining davlat reyestrini yuritish bo‘yicha davlat xizmatlarini ko‘rsatishning Ma’muriy reglamentini tasdiqlash to‘g‘risida	Jismoniy shaxsga shaxsiy identifikatsiya raqamini berish. O‘zbekiston Respublikasi fuqarosiga xorijga chiqish uchun biometrik pasport berish Shaxsga doir ma’lumotlar bazalarini shaxsga doir ma’lumotlar bazalarining davlat reyestriga kiritish
O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi huzuridagi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo‘yicha inspeksiya (“O’zkomnazorat”)	O‘zbekiston Respublikasi Vazirlar Mahkamasining 2021-yil 29-apreldagi 255-son qarori bilan tasdiqlangan “O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning maxsus shartlariga rioya etilishi ustidan davlat nazoratini amalga oshirish tartibi to‘g‘risida”gi Nizom	Shaxsga doir ma’lumotlarga ishlov berishning alohida shartlarini buzuvchi axborot resurslarini aniqlash Axborot resurslarini Shaxsga doir ma’lumotlar subyektlari huquqlarini buzuvchilar reyestriga (reyestrga) kiritish Reyestrga kiritilgan axborot resurslaridan foydalanishni cheklash

Xodimlarning shaxsga doir ma’lumotlarini qayta ishlash

Xodimlarning shaxsga doir ma’lumotlarini qayta ishlashning huquqiy asoslari va ular bilan ishlash qoidalari Mehnat kodeksi (bundan buyon matnda — MK) hamda 2019-yil 2-iyuldagi O‘RQ-547-son «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun bilan belgilanadi. MK shaxsga doir ma’lumotlarni qayta ishlash, saqlash va ulardan foydalanishning asosiy qoidalarini belgilaydi.

Xodimning shaxsga doir ma’lumotlari — xodim va uning oila a’zolari hayotidagi faktlar, voqealar va holatlar to‘g‘risidagi maxfiy axborotdir. Xodimlar ish beruvchiga shaxsiy ma’lumotlarni mehnat munosabatlari bilan bog‘liq holda taqdim etadilar.

Shaxsga doir ma’lumotlarga xodim to‘g‘risidagi quyidagi ma’lumotlar kiradi:

- F.I.O., tug‘ilgan sanasi va joyi;
- JSHSHIR (mavjud bo‘lsa);
- ta’lim/ ma’lumoti to‘g‘risidagi ma’lumotlar va hujjatlar;
- mehnat faoliyati boshlangan paytdan boshlab bajarilayotgan ish, shu jumladan harbiy xizmat to‘g‘risidagi ma’lumotlar;
- doimiy yoki vaqtincha yashash joyi bo‘yicha ro‘yxatga olingan manzil;
- pasport yoki ID-karta ma’lumotlari — seriyasi, raqami, kim tomonidan va qachon berilganligi;
- shaxsiy telefon raqami, elektron pochta manzili;
- zaxiradagi fuqarolar va harbiy xizmatga chaqirilishi lozim bo‘lgan shaxslar uchun harbiy majburiyatga munosabati, harbiy ro‘yxatga olish ma’lumotlari;
- Soliq to‘lovchining identifikatsiya raqami (mavjud bo‘lsa);
- shaxsiy jamg‘arib boriladigan pensiya hisobvarag‘i raqami (ShJBPH);
- majburiy tibbiy ko‘rik natijalari;
- xodim bilan mehnat shartnomasini bekor qilish asoslari;
- yaqin qarindoshlarining oilaviy holati, F.I.O. va tug‘ilgan sanasi;
- ish beruvchiga ma’lum bo‘lib qolgan xodim va uning oila a’zolari hayotiga oid faktlar, voqealar va holatlar haqidagi boshqa ma’lumotlar.

Xodimlarning shaxsga doir ma’lumotlarini qayta ishlashda Mehnat kodeksi ish beruvchiga quyidagi majburiyatlarni yuklaydi (MKning 176-moddasi):

- shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilik qoidalariga amal qilish;
- shaxsga doir ma’lumotlarni bevosita xodimning o‘zidan olish;
- shaxsga doir ma’lumotlarni uchinchi shaxslardan faqat xodimni yozma ravishda xabardor qilgan holda va uning roziligi bilan olish;/ uchinchi shaxslardan shaxsiy ma’lumotlarni faqat xodimning yozma xabari va uning roziligi bilan olish;
- xodimga shaxsga doir ma’lumotlarni olish maqsadlari, taxmin qilinayotgan manbalari va usullari, shuningdek ushbu ma’lumotlarning xususiyati haqida xabar berish;
- xodim shaxsga doir ma’lumotlarni olishga rozilik berishdan bosh tortgan taqdirda yuzaga kelishi mumkin bo‘lgan oqibatlar haqida uni xabardor qilish;
- xodimning shaxsga doir ma’lumotlari himoya qilinishini ta’minlash;
- xodimlarni shaxsga doir ma’lumotlarni qayta ishlash tartibi bilan imzo qo‘ydirgan holda tanishtirish;

- xodimlarning shaxsiy ma’lumotlarini himoya qilish choralarini ishlab chiqish;
- mehnat faoliyati jarayonida ma’lum bo‘lib qolgan shaxsga doir ma’lumotlarning oshkor etilishiga yo‘l qo‘ymaslik.

Xodimlarning shaxsga doir ma’lumotlarini qayta ishlashga oid asosiy qoidalar ish beruvchining ichki lokal hujjatlari bilan tartibga solinishi lozim. Xodimlarning shaxsga doir ma’lumotlari bazalarini ro‘yxatdan o‘tkazish talab etilmaydi.

Biometrik va genetik ma’lumotlarni qayta ishlash

«Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonunning 7-moddasiga muvofiq, O‘zbekiston Respublikasi Vazirlar Mahkamasi quyidagilarni belgilash vakolatiga ega:

- shaxsga doir ma’lumotlarni qayta ishlashda xavfsizlikka tahdidlardan kelib chiqqan holda ularning himoyalanganlik darajalarini;
- shaxsiy ma’lumotlarga ishlov berishda ularning himoyasini ta’minlash bo‘yicha talablar, ularga rioya etilishi shaxsiy ma’lumotlarning belgilangan himoya darajasini ta’minlaydi;
- biometrik va genetik ma’lumotlarning moddiy tashuvchilariga, shuningdek bunday ma’lumotlarni shaxsga doir ma’lumotlar bazalaridan tashqarida saqlash texnologiyalariga qo‘yiladigan talablarni.

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 5-oktyabrdagi “Shaxsga doir ma’lumotlarga ishlov berish sohasidagi ayrim normativ-huquqiy hujjatlarni tasdiqlash to‘g‘risida”gi 570-son qarori (keyingi o‘rinlarda — Qaror) bilan shaxsga doir ma’lumotlar operatorlariga himoya darajalari bilan bog‘liq qo‘shimcha talablar belgilandi va quyidagilar tasdiqlandi:

- Shaxsiy ma’lumotlarga ishlov berishda ularning himoyalanganlik darajalarini aniqlash tartibi to‘g‘risidagi nizom;
- Biometrik va genetik ma’lumotlarning moddiy manbalariga qo‘yiladigan talablar va bunday ma’lumotlarni shaxsiy ma’lumotlar bazalaridan tashqarida saqlash texnologiyalari to‘g‘risidagi nizom.

Xavflarni baholash talablariga rioya etish uchun bajarilishi majburiy bo‘lgan harakatlar:

- Tahdid turlari va ta’minlanadigan himoya darajalarini hisobga olgan holda shaxsiy ma’lumotlarni himoya qilish bo‘yicha tashkiliy va texnik choralarni joriy etish.
- Shaxsiy ma’lumotlarning moddiy tashuvchilarining, shuningdek onlayn yoki raqamli ma’lumotlar bazalarining ma’lumotlar bazasiga kirish va undan foydalanish bo‘yicha belgilangan himoya darajasini ta’minlash.
- Mulkdor va (yoki) operator rahbarining, shuningdek ma’lumotlar bazalarida qayta ishlanadigan shaxsga doir ma’lumotlarga kirish huquqiga ega bo‘lgan shaxslarning majburiyatlari hajmini, ularning xizmat (mehnat) majburiyatlarini bajarish uchun zarur bo‘lgan doirada, himoyalanganlik darajalari va tahdidlarni kamaytirish choralarini hisobga olgan holda belgilash.

- Axborotni himoya qilish vositalarining himoyalanganlik darajasi axborot xavfsizligi to‘g‘risidagi mahalliy qonunchilik talablariga muvofiqligini baholash tartibini tasdiqlash.

- Shaxsiy ma’lumotlarni qayta ishlash uchun mas’ul shaxsni tayinlash (Data Protection Officer).

Mulkdor yoki operator biometrik va genetik ma’lumotlarga ishlov berishda ularni himoya qilish va saqlash bo‘yicha tashkiliy va texnik choralarni ko‘radi. Har bir himoya darajasi shaxsga doir ma’lumotlarning mulkdori va (yoki) operatori tomonidan bajarilishi lozim bo‘lgan muayyan talablarni nazarda tutadi.

Himoya qilishning 1-darajasi

Qo‘llash shartlari (quyidagi shartlardan kamida bittasi bajarilsa, har bir himoya darajasi majburiy hisoblanadi):

1. ma'lumotlar bazalari uchun 1-turdagi tahdidlar mavjud bo‘lganda hamda ma'lumotlar bazalarida maxsus va (yoki) biometrik va (yoki) genetik ma'lumotlarga ishlov berilganda;

2. ma'lumotlar bazalari uchun 2-turdagi tahdidlar mavjud bo‘lganda hamda mulkdor va (yoki) operatorning xodimlari bo‘lmagan 50 000 dan ortiq subyektlarning maxsus ma'lumotlariga ishlov berilganda.

Himoya qilinganlik darajasini ta’minlash talablari:

- 2-himoya qilinganlik darajasi uchun belgilangan talablarning bajarilishi;

- mulkdorning va (yoki) operatorning ma’lumotlar bazalaridagi shaxsga doir ma’lumotlardan foydalanish vakolatlaridagi (avtorizatsiyadagi) o‘zgarishlarni elektron xavfsizlik jurnalida avtomatik tarzda qayd etib borish;

- ma’lumotlar bazalarida shaxsga doir ma’lumotlar xavfsizligini ta’minlashga mas’ul bo‘lgan tarkibiy bo‘linmani tuzish yoki bunday xavfsizlikni ta’minlash vazifalarini mavjud tarkibiy bo‘linmalardan birining zimmasiga yuklash.

Himoya qilishning 2-darajasi

Qo‘llash shartlari (quyidagi shartlardan kamida bittasi bajarilsa, har bir himoya darajasi majburiy hisoblanadi):

1. ma'lumotlar bazalari uchun 1-turdagi tahdidlar mavjud bo‘lganda hamda ma'lumotlar bazalarida hamma foydalanishi mumkin bo‘lgan ma'lumotlarga ishlov berilganda;

2. ma’lumotlar bazalari uchun 2-turdagi tahdidlar mavjud bo‘lganda va mulkdor va (yoki) operator xodimlarining maxsus ma’lumotlarini yoki mulkdor va (yoki) operatorning xodimlari bo‘lmagan 50 000 dan kam subyektlarning maxsus ma'lumotlariga ishlov berilganda;

3. ma'lumotlar bazalari uchun 2-turdagi tahdidlar mavjud bo‘lganda hamda ma'lumotlar bazalarida biometrik va (yoki) genetik ma'lumotlarga ishlov berilganda;

4. ma'lumotlar bazalari uchun 2-turdagi tahdidlar mavjud bo‘lganda hamda mulkdor va (yoki) operatorning xodimlari bo‘lmagan 50 000 dan ortiq subyektlarning hamma foydalanishi mumkin bo‘lgan ma'lumotlariga ishlov berilganda;

5. ma'lumotlar bazalari uchun 3-turdagi tahdidlar mavjud bo‘lganda hamda mulkdor va (yoki) operatorning xodimlari bo‘lmagan 50 000 dan ortiq subyektlarning maxsus ma'lumotlariga ishlov berilganda.

Himoya qilinganlik darajasini ta’minlash talablari:

- 3-himoya qilinganlik darajasi uchun belgilangan talablarning bajarilishi;
- xabarlarning elektron jurnaliga kirishni faqat mansabdor shaxslarga (xodimlarga) yoki mazkur jurnaldagi ma’lumotlar o‘z xizmat (mehnat) majburiyatlarini bajarish uchun zarur bo‘lgan vakolatli shaxsga taqdim etish.

Himoya qilishning 3-darajasi

Qo‘llash shartlari (quyidagi shartlardan kamida bittasi bajarilsa, har bir himoya darajasi majburiy hisoblanadi):

1. ma'lumotlar bazalari uchun 2-turdagi tahdidlar mavjud bo‘lganda hamda mulkdor va (yoki) operator xodimlarining hamma foydalanishi mumkin bo‘lgan ma'lumotlariga yoxud mulkdor va (yoki) operatorning xodimlari bo‘lmagan 50 000 dan kam bo‘lgan subyektlarning hamma foydalanishi mumkin bo‘lgan ma'lumotlariga ishlov berilganda;
2. ma'lumotlar bazalari uchun 3-turdagi tahdidlar mavjud bo‘lganda hamda mulkdor va (yoki) operator xodimlarining maxsus ma'lumotlariga yoki mulkdor va (yoki) operatorning xodimlari bo‘lmagan 50 000 dan kam bo‘lgan subyektlarning maxsus ma'lumotlariga ishlov berilganda;
3. ma'lumotlar bazalari uchun 3-turdagi tahdidlar mavjud bo‘lganda hamda biometrik va (yoki) genetik ma'lumotlarga ishlov berilganda.

Himoya qilinganlik darajasini ta’minlash talablari:

- 4-himoya qilinganlik darajasi uchun belgilangan talablarning bajarilishi;
- ma’lumotlar bazalarida shaxsiy ma’lumotlarning xavfsizligini ta’minlash uchun mas’ul mansabdor shaxs (xodim) tayinlanishi.

Himoya qilishning 4-darajasi

Qo‘llash shartlari (quyidagi shartlardan kamida bittasi bajarilsa, har bir himoya darajasi majburiy hisoblanadi):

1. ma'lumotlar bazalari uchun 3-turdagi tahdidlar mavjud bo‘lganda hamda ma'lumotlar bazasida hamma foydalanishi mumkin bo‘lgan ma'lumotlarga ishlov berilganda.

Himoya qilinganlik darajasini ta’minlash talablari:

- ma'lumotlar bazalari joylashgan binolarning xavfsizlik rejimini tashkil etish, ushbu binolarga kirish huquqiga ega bo‘lmagan shaxslarning nazoratsiz kirishi yoki ushbu binolarda qolishining oldini olish;
- shaxsga doir ma'lumotlar mavjud bo‘lgan moddiy jismlar xavfsizligini ta'minlash;

- ma'lumotlar bazalarida ishlov berilayotgan shaxsga doir ma'lumotlarga kirish, ularning xizmat (mehnat) vazifalarini bajarishi uchun zarur bo‘lgan shaxslar ro‘yxatini belgilaydigan hujjatni mulkdor va (yoki) operator rahbari tomonidan tasdiqlash;
- shaxsga doir ma'lumotlarni mavjud tahdidlardan himoya qilish, zarurat bo‘lganda axborot xavfsizligi sohasidagi qonunchilik talablariga muvofiqligini baholash tartibidan o‘tgan axborot xavfsizligi vositalaridan foydalanish.

2.2. Kompaniyada maxfiy ma’lumotlarni himoya qilish

Har bir tashkilotda oshkor qilinishi mumkin bo‘lmagan ma’lumotlar mavjud: mijozlar haqidagi ma’lumotlar, ichki hisobotlar, tijorat rejalari. Bunday ma’lumotlarni himoya qilish va yagona qoidalarni o‘rnatish uchun Maxfiy ma’lumotlar to‘g‘risidagi nizomni ishlab chiqish zarur. Ushbu hujjatda nima maxfiy axborot hisoblanishi, uni kim va qanday saqlashi kerakligi hamda bu qoidalarni buzganlik uchun qanday oqibatlar kelib chiqishi aniq ko‘rsatilishi muhimdir.

MUHIM!

Mazkur Nizom ma’lumotlar oshkor etilgan yoki axborot sizib chiqqan hollarda kompaniya manfaatlarini himoya qilish maqsadida xodimlar bilan NDA (maxfiylik to‘g‘risidagi kelishuv) tuzish uchun asos bo‘lib xizmat qiladi.

Maxfiylik to‘g‘risidagi nizomni ishlab chiqishda kompaniyaning haqiqiy biznes jarayonlariga amal qilish, maxfiy ma’lumotlar ro‘yxatini shakllantirish, kirish darajalarini belgilash zarur. Hujjat kompaniyaning o‘ziga xos xususiyatlarini, xodimlarning kirish darajasini, ma’lumotlar bilan ishlash shakllarini va xavf-xatarlarni hisobga olishi kerak.

Nizomning yuridik kuchga kirishi uchun kelishish, shu jumladan xodimlarning vakillik organi (mavjud bo‘lgan taqdirda) bilan kelishish tartib-taomilini amalga oshirish zarur.

Nizom kelishilgandan keyin ish beruvchi buyruq chiqarishga haqli bo‘lib, u bo‘yicha lokal hujjat amalga kiritiladi. Shu paytdan boshlab hujjat bajarilishi majburiy bo‘lib, maxfiy ma’lumotlarga kirish huquqiga ega bo‘lgan barcha xodimlar u bilan imzo qo‘ydirib tanishtirilishi kerak.

Nizom bo‘limi	Nimalarni kiritish lozim (bo‘lim mazmuni)	Misollar / izohlar
I. Umumiy qoidalar	Maxfiylik rejimining maqsadi va vazifalari. Huquqiy asoslar (normativ-huquqiy hujjatlar va ichki hujjatlar). Atamalar: «maxfiy axborot», «axborot tashuvchi», «foydalanish huquqi», «oshkor etish», «axborot sizib chiqishi», «insident». Amal qilish sohasi va shaxslar doirasi (xodimlar, stajyorlar, pudratchilar, maslahatchilar, kontragentlar vakillari). Tamoyillar: «bilish zarurati», foydalanish huquqini minimallashtirish, shaxsiy javobgarlik.	Ta’rifi: «Nizom maxfiy axborot bilan ishlashning yagona rejimini belgilaydi, rejimni buzganlik uchun javobgarlik va himoya choralarini belgilaydi.»
II. Maxfiy axborot tarkibi va tasnifi	Toifalar ro‘yxati (tijorat siri, shaxsiy ma’lumotlar, moliya, mijozlar/yetkazib beruvchilar, kod/texnik hujjatlar, hisobotlar, strategiyalar, shartnomalar, qoidalar, ma’lumotlar bazalari). Maxfiylik darajalari. Toifalarga/darajalarga kiritish mezonlari. Ro‘yxatni qayta ko‘rib chiqish tartibi.	Darajalarga misol: • «Xizmat doirasida foydalanish uchun»; • «Maxfiy»; • «O‘ta maxfiy».

III. Hisobga olish, saqlash va himoya qilishni tashkil etish	Saqlash joylari (serverlar, arxiv, bulut, ishchi stansiyalar, qog‘oz). Himoya choralari: tashkiliy / texnik / jismoniy. Amallar tartibi: belgilash, nusxa olish, skanerlash, fotosurat, jo‘natish, chop etish, yo‘q qilish, arxivlash. Jurnallar: berish/qaytarish, kirish jurnallari, tashuvchilar hisobi.	Texnik choralar: parollar, shifrlash, hodisalar jurnallari, antivirus, qurilmalarni nazorat qilish, zaxira nusxa olish.
IV. Xodimlarga ruxsat berish va foydalanish huquqini boshqarish	Foydalanishga ruxsat berish asosi (buyruq/ farmoyish, rahbarning talabnomasi, mas’ul shaxs bilan kelishish). «Faqat xizmat zarurati doirasida foydalanish» tamoyili. NDA/majburiyat: imzolash vaqti, amal qilish muddati, oqibatlari. Foydalanish darajalari (rollar matritsasi). Ishga qabul qilishda va davriy ravishda o‘qitish hamda yo‘riqnoma berish.	Ilova sifatida alohida foydalanish matritsasi tavsiya etiladi.
V. Uchinchi shaxslarga topshirish tartibi	Qachon va qanday asoslarda uzatishga ruxsat beriladi (shartnoma, topshiriq, NDA, minimallashtirish). Uzatish kanallari va ruxsatsiz uzatishga qo‘yilgan taqiqlar. Kontragentlarga qo‘yiladigan talablar: himoya choralari, subpudratchilarni cheklash, tugatgandan so‘ng qaytarish/yo‘q qilish. Kontragent vakillarining kirishini nazorat qilish (mehmon rejimi, hisobga olish).	Ruxsat etilmagan kanalsiz messenjerga” uzatishni taqiqlash to‘g‘risida alohida band (buyruq/reglament bo‘yicha istisnolar bilan).
VI.Axborotdan ommaviy muhitda foydalanish	Nashrlar, keyslar, taqdimotlar, ijtimoiy tarmoqlar, tadbirlar, intervyular. Ommaviy materiallarni kelishish tartibi (kim tasdiqlaydi). Mijozlar va xodimlarni ruxsatsiz oshkor qilish/ “deanonimizatsiya” qilish taqiqlanadi. Ofisda foto/ video olish qoidalari (agar mavjud bo‘lsa).	Foydali: «nashrdan oldin» nazorat ro‘yxati (kelishish uchun kimga yuborish kerak).
VII. Rejimga rioya etilishini nazorat qilish	Mas’ul bo‘linmalar (HR, IT, xavfsizlik/muvofiqlik, huquqshunoslar). Nazorat shakllari: rejali/rejadan tashqari tekshiruvlar, kirish huquqlari auditi, jurnallar auditi, tashuvchilarni tekshirish. Xizmat tekshiruvi: asoslari, muddatlari, rasmiylashtirilishi.	Rejali tekshiruvlar davriyligini ko‘rsating (masalan, har chorakda / yarim yilda bir marta).
VIII. Hodisalarga munosabat bildirish	Hodisani aniqlash. Xodimning darhol xabar berish majburiyati. Birlamchi choralar: kirishni bloklash, tashuvchini olib qo‘yish, izlarni qayd etish, tarqalishini cheklash. Tergov: komissiya, dalillar to‘plash, dalolatnoma, tuzatish choralari, o‘qitish. Kommunikatsiyalar: yagona ma’ruzachi, ruxsatsiz sharhlarni taqiqlash.	Quyidagi shablon tavsiya etiladi: “hodisa to‘g‘risida xabar” + “tekshiruv dalolatnomasi” shakli.
IX. Mas’uliyat	Intizomiy. Moddiy. Qonun bo‘yicha boshqa javobgarlik. Rasmiylashtirish tartibi: tushuntirish xati, dalolatnoma, buyruq, jazo.	Ta’rif: «Javobgarlik qonun hujjatlariga va ish beruvchining lokal hujjatlariga muvofiq yuzaga keladi.»
X. Yakuniy qoidalar	Nizomni tasdiqlash va kuchga kiritish. Xodimlarni imzo qo‘ydirgan holda tanishtirish. O‘zgartirishlar kiritish tartibi. Amal qilish muddati. Mas’ul shaxsning aloqa ma’lumotlari.	Qulay: “tanishish varaqasi” yoki “tanishish jurnali” ilovasi.
Ilovalar	Maxfiy ma’lumotlar ro‘yxati Xodimlar uchun maxfiy axborotni oshkor etmaslik majburiyati (NDA) shakli. Tashuvchilarni hisobga olish jurnali Hujjatlarni berish jurnali Tashuvchilar/hujjatlarni yo‘q qilish to‘g‘risidagi dalolatnoma namunasi. Xodimga eslatma Hodisa haqida xabar berish shakli	

Xodimlarni Maxfiylik to‘g‘risidagi nizom bilan tanishtirish tartibi

Nizom tasdiqlangandan so‘ng xodimlarni uning mazmuni bilan tanishtirish jarayonini to‘g‘ri tashkil etish muhimdir. Bu xodimlar maxfiy ma’lumotlarni himoya qilish bo‘yicha o‘z majburiyatlarini to‘liq anglab yetishlari va yuzaga kelishi mumkin bo‘lgan qoidabuzarliklar uchun javobgar bo‘lishlari uchun zarurdir.

Xodimlarni hujjat bilan tanishtirish uchun ish beruvchi quyidagi usullardan foydalanishi mumkin:

1. Mehnat shartnomasiga Maxfiylik to‘g‘risidagi nizom talablariga rioya etish majburiyati haqidagi bandni kiritish va hujjat rekvizitlarini ko‘rsatish.
2. Barcha xodimlar imzo qo‘yadigan Nizom bilan tanishganlik varaqasini rasmiylashtirish.
3. Maxfiylik to‘g‘risidagi nizom bilan tanishganlik jurnalini yuritish. Jurnalda quyidagi ustunlar nazarda tutiladi: F.I.O., lavozimi, lokal hujjat nomi, tanishgan sana va xodimning imzosi.
4. Har bir xodim uchun lokal hujjatlarning to‘liq ro‘yxati ko‘rsatilgan alohida tanishganlik varaqasini rasmiylashtirish. Xodim har bir lokal hujjat nomi qarshisiga o‘z imzosini qo‘yadi.

Ish beruvchi maxfiy axborot bilan ishlash bo‘yicha mas’ul bo‘lgan xodimlarni o‘qitishga haqli.

Maxfiylik to‘g‘risidagi nizomni joriy etish bo‘yicha chek-list

- ☐ Jarayonlar tavsiflangan: ma’lumotlar qayerda yaratilishi, ulardan kimlar foydalanishi va ular qayerga uzatilishi aniqlangan.
- ☐ Maxfiy axborot toifalari belgilangan va ularning ro‘yxati tasdiqlangan.
- ☐ Mas’ul shaxslar tayinlangan: IT / HR / yurist.
- ☐ Foydalanish huquqi darajalari hamda bunday huquqni berish va bekor qilish tartibi joriy etilgan.
- ☐ Minimal texnik himoya choralari yo‘lga qo‘yilgan: parollar, hodisalarni jurnallarda qayd etish, zaxira nusxalarini yaratish.
- ☐ Qog‘oz shaklidagi hujjatlar va axborot tashuvchilari bilan ishlash tartibi belgilangan.
- ☐ Axborotni uchinchi shaxslarga uzatish qoidalari mustahkamlangan (NDA shartnomasi, standart cheklovlar).
- ☐ Insidentlarga javob choralarini ko‘rish jarayoni joriy etilgan (xabar berish → lokalizatsiya qilish → tekshiruv o‘tkazish → tegishli choralarni ko‘rish).
- ☐ Xodimlarni imzo qo‘ydirgan holda hujjat bilan tanishtirish tashkil etilgan (tanishganlik jurnali / tanishganlik varaqasi).
- ☐ Tizimli o‘qitish tashkil etilgan (boshlang‘ich va har yili o‘tkaziladigan o‘qitish).

2.3. Yuristlarning kasbiy faoliyati uchun axborotdan foydalanish

Zamonaviy yuridik amaliyotni ishonchli axborotdan tezkor foydalanish imkoniyatisiz tasavvur etib bo‘lmaydi. Yuristlar har kuni normativ-huquqiy hujjatlar, sud amaliyoti, davlat reyestrlari, korporativ hujjatlar, ochiq ma’lumotlar hamda davlat hokimiyati organlarining raqamli xizmatlari bilan ishlaydi.

Bunda faqat zarur axborotni topishning o‘zi yetarli emas. Qaysi manbalar rasmiy hisoblanishini, qaysi ma’lumotlarga ishonish mumkinligini, foydalanish cheklangan axborot bilan ishlashda qonunchilikda qanday cheklovlar belgilanganini hamda axborotni taqdim etish rad etilgan taqdirda mijozning huquqlarini qanday himoya qilish lozimligini tushunish muhimdir.

Mazkur bo‘limda yuristning kasbiy faoliyatida axborotni izlash, tekshirish va undan qonuniy foydalanishning amaliy vositalari ko‘rib chiqiladi.

Axborotdan foydalanish huquqi, asosan, O‘zbekiston Respublikasining «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi Qonuni, «Axborot olish kafolatlari va erkinligi to‘g‘risida»gi Qonuni, «Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida»gi Qonuni, «Ommaviy axborot vositalari to‘g‘risida»gi Qonuni, «Rasmiy statistika to‘g‘risida»gi Qonuni, O‘zbekiston Respublikasining «Korrupsiyaga qarshi kurashish to‘g‘risida»gi Qonuni hamda «Huquqiy axborotni tarqatish va undan foydalanishni ta’minlash to‘g‘risida»gi 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, ijtimoiy axloqni, 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 doirada yo‘l qo‘yiladi.”

O‘zbekiston Respublikasining “Davlat organlari faoliyatining ochiqligi to‘g‘risida”gi Qonunining 6-moddasida davlat hokimiyati va boshqaruvi organlarining faoliyati to‘g‘risidagi axborotdan foydalanish, agar mazkur axborot qonunda belgilangan tartibda davlat sirini yoki qonun bilan qo‘riqlanadigan boshqa sirni tashkil etuvchi ma’lumotlar jumlasiga kiritilgan bo‘lsa, cheklanishi belgilangan. Umumiy qoidaga ko‘ra, davlat organlari, fuqarolarning o‘zini o‘zi boshqarish organlari, jamoat birlashmalari, korxonalar, muassasalar, tashkilotlar va mansabdor shaxslar davlat sirini yoki qonun bilan qo‘riqlanadigan boshqa sirni 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;

- O‘zbekiston Respublikasi hududida faoliyat ko‘rsatayotgan axborot-kutubxona muassasalari, arxivlar, idoraviy arxivlar, yuridik shaxslarning axborot tizimlaridagi ochiq fondlardagi mavjud ma’lumotlar.

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 istisnolar 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.

Axborot so‘rovi

O‘zbekiston Respublikasi qonunchiligi davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligini kafolatlaydi. Fuqarolar va yuridik shaxslar bevosita yoki o‘z vakillari orqali davlat hokimiyati va boshqaruvi organlarining faoliyati to‘g‘risida axborot olish uchun so‘rov bilan murojaat qilish huquqiga ega.

Davlat hokimiyati va boshqaruvi organlarining faoliyati to‘g‘risida axborot olishga doir so‘rov (bundan buyon matnda so‘rov deb yuritiladi) axborotdan foydalanuvchining davlat hokimiyati va boshqaruvi organlari faoliyati to‘g‘risida axborot taqdim etish haqida ushbu organlarga va (yoki) ularning mansabdor shaxslariga yo‘llanadigan og‘zaki yoki yozma shakldagi (shu jumladan elektron hujjat shaklidagi) talabidir. (O‘zbekiston Respublikasining «Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida»gi Qonuni 18-moddasi)

Axborot olish uchun so‘rov fuqarolar va yuridik shaxslarning murojaatlaridan tubdan farq qiladi.

Mezon	Fuqarolar/yuridik shaxslarning murojaati	Ma’lumot olish uchun so‘rov
Maqsad	Huquqlarni amalga oshirishga ko‘maklashish, buzilgan huquqlarni tiklash, qonuniy manfaatlarni himoya qilish, ishni yaxshilash bo‘yicha takliflar.	Davlat organi faoliyati to‘g‘risida aniq ma’lumotlar (hokimiyat va boshqaruv organlari faoliyati to‘g‘risida axborot) olish.
Mazmun	**Ariza** — yordam so‘rash. **Shikoyat** — huquqlarni tiklash talabi. **Taklif** — faoliyatni takomillashtirish bo‘yicha tavsiyalar.	Ma’lumot taqdim etish talabi. So‘rov og‘zaki/ yozma/elektron shaklda bo‘lishi mumkin.
Konstitutsiyaviy asos	Ariza, taklif va shikoyatlar bilan murojaat qilish huquqi.	Axborotni izlash, olish va tarqatish huquqi. Shuningdek, huquq va manfaatlarga daxldor hujjatlar bilan tanishish huquqi.
Huquqiy asos	O‘zbekiston Respublikasining «Jismoniy va yuridik shaxslarning murojaatlari to‘g‘risida»gi Qonuni (murojaat turlari, talablari, muddatlari).	O‘zbekiston Respublikasining “Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida”gi Qonuni (so‘rov tushunchasi, muddatlar). O‘zbekiston Respublikasining “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi Qonuni (so‘rov huquqi, shakllari va muddatlari). Davlat hokimiyati va boshqaruvi organlari faoliyati to‘g‘risidagi axborotni taqdim etish bo‘yicha so‘rovlarni qabul qilish, ro‘yxatdan o‘tkazish va ko‘rib chiqish tartibi to‘g‘risidagi Yo‘riqnoma (ro‘yxat raqami: 2769).
Kim murojaat qiladi	Jismoniy va yuridik shaxslar.	Har qanday axborot foydalanuvchisi (jismoniy yoki yuridik shaxs).
Til	Murojaatlar davlat tilida, shuningdek boshqa tillarda ham berilishi mumkin.	So‘rovlar davlat tilida, shuningdek boshqa tillarda ham berilishi mumkin.
Qayerga yuboriladi	Davlat organlari/davlat muassasalariga (va ba’zi hollarda qonun vakolatiga ko‘ra boshqa tashkilotlarga).	So‘rov masalalari bo‘yicha ma’lumot berish vakolatiga ega bo‘lgan hokimiyat organiga/ mansabdor shaxsga.
Ko‘rib chiqish muddati	Ariza/shikoyat — **15 kungacha.** Qo‘shimcha o‘rganish talab etilganda — **1 oygacha;** taklif **— 1 oygacha.**	Foydalanuvchi so‘rovi — ro‘yxatdan o‘tgan kundan boshlab **15 kungacha** OAV so‘rovi — **7 kungacha.**
Agar qabul qiluvchi vakolatli bo‘lmasa	Vakolatiga ko‘ra boshqa organga yuborish va murojaatchini xabardor qilish (qonunda belgilangan muddatlar doirasida).	Ro‘yxatdan o‘tkazilgan kundan e’tiboran **3 ish kuni** ichida vakolatli organga yuborish va foydalanuvchini xabardor qilish.
Ko‘rib chiqish natijalari	Murojaatning mohiyati bo‘yicha qaror va natijalar hamda ko‘rilgan choralar to‘g‘risida javob.	Ma’lumot taqdim etish; yoki asosli rad etish; yoki allaqachon e’lon qilingan manbalarga havola berish (rasmiy nashrlar/sayt). Rad etilgan taqdirda asoslantirilgan javob yuboriladi.
Identifikatsiya talablari	Murojaatning F.I.O./manzili (jismoniy shaxs uchun) yoki nomi/ manzili (yuridik shaxs uchun) va mohiyati ko‘rsatilishi shart.	So‘rovning F.I.O/manzili (jismoniy shaxs uchun) yoki nomi/manzili (yuridik shaxs uchun) va mohiyati ko‘rsatilishi shart.
Ma’nosi	Huquq va manfaatlarni harakat va qarorlar orqali himoya qilish.	Davlat va uning organlari faoliyati to‘g‘risidagi axborotdan foydalanish imkoniyatini ta’minlash.

Davlat hokimiyati va boshqaruvi organlari faoliyati to‘g‘risidagi axborotdan foydalanish mazkur axborot qonunda belgilangan tartibda davlat sirlarini yoki qonun bilan qo‘riqlanadigan boshqa sirni tashkil etuvchi ma’lumotlar toifasiga kiritilgan taqdirdagina cheklanishi mumkin.

Axborot olish uchun so‘rov yuborish algoritmi

1-bosqich.
Vakolatli davlat organini aniqlang

So‘ralgan ma’lumotlarga vakolati bo‘yicha ega bo‘lgan organni aniqlang. So‘rov unda ko‘rsatilgan masalalar bo‘yicha axborot taqdim etish vakolatiga ega bo‘lgan davlat organiga yoki mansabdor shaxsga yuborilishi lozim.

2-bosqich.
Organ vakolatlarini aniqlashtiring

Organning rasmiy veb-sayti va uning vazifa va funksiyalari to‘g‘risidagi nizomni tekshiring. Bu so‘rovni qayta yo‘naltirish va vaqtni yo‘qotish xavfini kamaytiradi.

3-bosqich.
So‘rovni to‘g‘ri tuzing

So‘rov — axborotdan foydalanuvchining organ faoliyati to‘g‘risidagi ma’lumotlarni taqdim etish haqidagi talabidir.

So‘rov og‘zaki, yozma yoki elektron hujjat shaklida bo‘lishi mumkin. Bir yoki bir nechta aniq savollarni shakllantiring.

Agar hujjatni so‘rayotgan bo‘lsangiz, agar ular ma’lum bo‘lsa, nomi va rekvizitlarini ko‘rsating.

4-bosqich.
So‘rovning majburiy ma’lumotlarini tekshiring

Jismoniy shaxs uchun F.I.O., yashash joyi haqidagi ma’lumotlarni va so‘rovning mohiyatini ko‘rsating.

Yuridik shaxs uchun to‘liq firma nomi, pochta manzili va so‘rovning mohiyatini ko‘rsating. Yozma so‘rov axborotdan foydalanuvchi tomonidan imzolanishi kerak.

Identifikatsiya uchun ma’lumotlarsiz so‘rov anonim hisoblanadi va ko‘rib chiqilmaydi.

5-bosqich.
Yo‘nalish kanalini tanlang

Qonun so‘rovning og‘zaki, yozma shakliga va elektron hujjatga to‘g‘ridan to‘g‘ri yo‘l qo‘yadi. Elektron murojaatlar amalda organning rasmiy veb-sayti, YIDXP (my.gov.uz) orqali rasmiy elektron pochtasi yoki.

6-bosqich.
So‘rov yuborilganini tasdiqlang

So‘rovdan nusxa oling.

Ro‘yxatdan o‘tish belgisini, kiruvchi raqamni yoki pochta kvitansiyasini saqlang.

7-bosqich.
Muddatlar va yozishmalarni nazorat qiling

Axborot so‘rovini ko‘rib chiqish muddati so‘rov ro‘yxatdan o‘tkazilgan kundan boshlab hisoblanadi.

Agar belgilangan muddat tugagunga qadar axborotga javob taqdim etilmasa, bu amaldagi qonunchilikning buzilishi hisoblanadi. Axborot berishni qonunga xilof ravishda rad etish ustidan fuqarolar va yuridik shaxslar prokuratura organlariga yoki ma’muriy sudga shikoyat qilishlari mumkin.

Huquqiy axborotdan foydalanish

Huquqiy axborotning asosiy manbasi O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlari milliy bazasi (**Lex.uz**) bo‘lib, unda amaldagi qonunchilik, shu jumladan qonunlar, prezident farmonlari va qarorlari, hukumat hujjatlari, mahalliy davlat hokimiyati organlarining qarorlari va boshqa normativ-huquqiy hujjatlar taqdim etilgan.

Qonun loyihalarining umumxalq muhokamasi **regulation.gov** portalida qonunlar, farmonlar, qarorlar, buyruqlar va davlat hokimiyati markaziy hamda mahalliy organlarining qarorlari loyihalari e’lon qilinadi.

O‘zbekiston Respublikasining “Huquqiy axborotni tarqatish to‘g‘risida”gi Qonuni (O‘RQ-461-son) har bir fuqaroning ishonchli, o‘z vaqtida va to‘liq huquqiy axborot olish huquqini mustahkamlaydi. Bunga qonunlar, qonunosti hujjatlari, xalqaro shartnomalar, shuningdek, mahalliy o‘zini o‘zi boshqarish organlarining hujjatlari to‘g‘risidagi ma’lumotlar kiradi.

Hujjat huquqiy axborotni taqdim etishda amal qilinishi lozim bo‘lgan asosiy tamoyillarni belgilaydi:

- Ochiqlik va hammaboplik.
- To‘liqlik va ishonchlilikni ta’minlash.
- Axborot to‘plash va tarqatishda shaxsiy hayotga aralashishga yo‘l qo‘yilmasligi.
- Fuqarolarning axborot olishdagi teng huquqliligi.

Davlat organlari rasmiy veb-saytlar va boshqa rasmiy manbalar orqali huquqiy axborotdan bepul foydalanish imkoniyatini ta’minlashi shart. Normativ-huquqiy hujjatlar matnlarining elektron nusxalari ularni qabul qilgan organlarning rasmiy veb-saytlarida belgilangan tartibda majburiy joylashtirilishi lozim. Shuningdek, qonun ularning aholini qonunchilikdagi o‘zgarishlar haqida xabardor qilish hamda fuqarolarga huquqiy masalalar yuzasidan

maslahat berish majburiyatini ham belgilaydi. Huquqiy axborotni tarqatish shakllari ommaviy axborot vositalarida rasmiy nashr etish, davlat axborot resurslariga joylashtirish va davlat muassasalarida bosma shaklda taqdim etishni o‘z ichiga oladi.

Har bir davlat organida axborot xizmati tashkil etilgan bo‘lib, uning vazifalariga davlat organi faoliyatini tartibga soluvchi huquqiy axborotni taqdim etish kiradi. Davlat organlari va tashkilotlari jismoniy hamda yuridik shaxslarning so‘roviga binoan o‘z faoliyatiga oid masalalar bo‘yicha normativ-huquqiy hujjatlarni qo‘llash tartibini tushuntirib beradi. Davlat organlari va tashkilotlari tomonidan tayyorlangan normativ-huquqiy hujjatlarni qo‘llash tartibi to‘g‘risidagi tushuntirishlar ushbu organlar va tashkilotlarning tarkibiy hamda hududiy bo‘linmalari uchun majburiy kuchga ega hisoblanadi.

Qonun hujjatlarini huquqiy targ‘ib qilish quyidagi usullar bilan amalga oshiriladi:

- Konferensiyalar, uchrashuvlar, seminarlar, davra suhbatlari va suhbatlar o‘tkazish;
- Ommaviy axborot vositalari, shu jumladan teleradioeshittirishlarni tashkil etish, bosma va elektron ommaviy axborot vositalarida maqolalar va axborot-huquqiy materiallarni joylashtirish orqali;
- Izohlar, broshyuralar, plakatlar, bukletlar va flayerlarni tarqatish;
- Ijtimoiy reklama (videoroliklar, infografikalar va boshqalar) va qonunchilikda taqiqlanmagan boshqa targ‘ibot turlari orqali amalga oshiriladi.

Jismoniy va yuridik shaxslar o‘z faoliyatiga taalluqli huquqiy axborotni taqdim etish to‘g‘risida davlat organlari va tashkilotlariga so‘rov bilan murojaat qilish huquqiga ega. Huquqiy axborot taqdim etish to‘g‘risidagi so‘rov u kelib tushgan kundan e’tiboran **o‘n besh kundan** ortiq bo‘lmagan muddatda ko‘rib chiqilishi lozim.

Huquqiy axborotni elektron shaklda taqdim etish bepul amalga oshiriladi. Huquqiy axborotni qog‘ozda taqdim etganlik uchun taraflarning kelishuviga binoan haq olinishi mumkin. Huquqiy axborot taqdim etish to‘g‘risidagi so‘rovni qanoatlantirishni rad etish asoslantirilgan bo‘lishi kerak. Fuqarolar, agar mansabdor shaxslarning noqonuniy harakatlari yoki harakatsizligi ularning huquqiy axborotdan foydalanish huquqini buzayotgan bo‘lsa, shikoyat qilish huquqiga egadirlar. Qonunda huquqiy axborot olishga to‘sqinlik qilganlik uchun javobgarlik ham belgilangan.

2.4. Raqamli muhitdagi kontent uchun javobgarlik

2.4.1. Qonunga xilof (taqiqlangan) va nozik kontentga nimalar kiradi?

Markaziy Osiyo mamlakatlarida OAV tahririyatlari va kontent yaratuvchilari uchun bir qator mavzular mavjud bo‘lib, ayrim mamlakatlarda ular qonunchilik darajasida qonunga xilof deb e’tirof etiladi (masalan, Qozog‘istonda). Boshqa mamlakatlarda esa bunday mavzularda materiallar e’lon qilish maqsadga muvofiq emas, chunki bu publikatsiya mualliflari, NNTlar, OAV tahririyatlari hamda ularning mulkdorlari uchun jiddiy muammolarni keltirib chiqarishi mumkin.

O‘zbekistonning xalqaro majburiyatlari axborot quyidagilar bilan bog‘liq bo‘lgan hollarda eng aniq taqiqlovchi choralarni ko‘rishni taqozo etadi:

- ekstremizm va terrorizmni targ‘ib qiluvchi va taqiqlangan tashkilotlarning materiallari (shu jumladan, materiallar yoki ramzlar, turli chaqiriqlar tarqatishni taqiqlash);
- giyohvand moddalarni targ‘ib qilish;
- davlat sirlarini oshkor qilish va milliy xavfsizlik masalalari bilan;
- milliy, etnik yoki diniy adovatni qo‘zg‘atish (hate speech -nafrat nutqi);
- bolalarni pornografiya va behayo kontentdan himoya qilish;
- agar aniq jamoat manfaati bo‘lmasa, shaxsiy hayot, shaxsiy ma’lumotlar bilan.

Biroq, mavzularning katta ro‘yxati jurnalistlar va ommaviy axborot vositalari uchun nozik bo‘lib, agar OAV tahririyati ushbu ro‘yxatdagi masalalarni yoritsa, yuzaga kelishi mumkin bo‘lgan mumkin bo‘lgan va haqiqiy huquqiy muammolar tufayli. Shu bilan birga, bu mavzularda biror narsani nashr etmaslik to‘g‘ridan-to‘g‘ri taqiqlanmagan, ammo barcha OAV tahririyatlari, jurnalistlar va muharrirlar bu mavzularning nozikligidan yaxshi xabardor.

Quyidagi jadvalda keltirilgan mavzular ommaviy axborot vositalari 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 nimalarni qamrab oladi?
Taqiqlangan partiyalar faoliyati	Taqiqlangan deb topilgan tashkilotlarning faoliyati haqida eslatma yoki tavsif; ularning bayonotlari va materiallari; ramzlari, shiorlari, atributlari; manbalariga havolalar; qo‘llab-quvvatlash, ishtirok etish yoki moliyalashtirishga chaqiriqlar.
O‘z joniga qasd qilishlar (Suitsidlar)	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 guruhlarga 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; jinsiy aloqaga oid kontent./ jinsiylik bilan bog‘liq kontent.
Til masalalari	Tillarning 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; ekstremizmda 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, yuqoridagi mavzular ommaviy axborot vositalari uchun taqiqlangan yoki yopiq emas, balki maksimal ehtiyotkorlikni, faktlarni qayta-qayta tekshirishni va ehtimoliy bosim yoki ta’qib xavfini baholashni talab qiladi.

Bunday hollarda yuridik yordam va himoyani ta’minlashning ikki usuli mavjud.

1. **Matnni e’lon qilishdan oldin dastlabki tahlil qilish**. Agar tahririyat “sezgir” mavzu bo‘yicha nashr qilishni rejalashtirayotgan bo‘lsa, yuridik yordam “oxirida” emas, balki materialni tayyorlash bosqichida — nashrdan oldin va saytda hamda ijtimoiy tarmoqlarda e’lon qilishdan oldin kiritilishi kerak. Amaliyotda bu quyidagicha ishlaydi: huquqshunos matn qoralamalarini, sarlavhalarni, rasmlar yoki videolarni, havolalar va asosiy iqtiboslarni oladi; iboralarni noqonuniy kontent belgilari bo‘yicha tekshiradi va ikkilamchi javobgarlik xavfini baholaydi (jumladan, fikrlar, repostlar, razm solish, teglar va imzolar). Natijalarga ko‘ra, huquqshunos qisqa xulosa beradi: qaysi qismlarni o‘zgartirish talab etiladi, qanday dalillar va tasdiqlar kerak (hujjatlar, so‘rovlarga javoblar, skrinshotlar, yozuvlar), qaysi shaxsiy ma’lumotlarni o‘chirish yoki egasizlantirish zarur va qaysi taqdim etish shakli xavfni kamaytiradi (neytral qayd etish, manbalar muvozanati, baholash da’volaridan fakt sifatida voz kechish).

2. **E’lon qilinganidan keyingi huquqiy munosabat**. Bunday holda, huquqshunos barcha holatlarni (havolalar, vaqt, skrinshotlar, platforma bildirishnomalari) qayd etadi, da’volarning huquqiy kvalifikatsiyasini aniqlaydi, tahririyatning pozitsiyasini tayyorlaydi va javobgarlikka tortish xavfini kamaytirish uchun huquqiy harakatlar strategiyasini tavsiya etadi.

2.4.2. 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[25] muvofiq sud tartibida da'vo taqdim etish orqali fuqarolik-huquqiy tartib	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[26] bo'yicha ma'muriy ish. O'zbekiston Respublikasi Jinoyat kodeksining 139-moddasiga muvofiq[27] 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 muvofiq ma'muriy tartib[28]. 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)[29].	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. yoki 1 yildan 2 yilgacha ozodlikni cheklash.

Yuridik yordam sha'n, qadr-qimmat va ishchanlik obro'sini himoya qilish to'g'risidagi fuqarolik-huquqiy da'volar bo'yicha yoki ma'muriy va jinoiy ishlar bo'yicha himoya qilish (dastlabki tergov va ishni sudda ko'rish bosqichida) bo'yicha sudda vakillik qilishdan iborat. Ushbu toifadagi ishlarda, qoida tariqasida, nashr matni yoki videoning sud ekspertizasi o'tkaziladi va isbotlashning boshqa usullaridan foydalaniladi. E'lon qilish natijasida jismoniy shaxslarga yetkazilgan ma'naviy zarar yoki yuridik shaxslarga yetkazilgan zararning mavjudligi maqbullik, aloqadorlik va ishonchlilik mezonlariga javob beradigan tegishli dalillar bilan tasdiqlanishi kerak.

[25] O'zbekiston Respublikasining Fuqarolik kodeksi, 100-modda. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://lex.uz/docs/111181#159215

[26] O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 40-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/97661

[27] O'zbekiston Respublikasi Jinoyat kodeksining 139-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/111457

[28] O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 41-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/97661

[29] O'zbekiston Respublikasi Jinoyat kodeksining 140-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/111457

2.4.3. Yolg‘on axborot tarqatganlik uchun javobgarlik

Yolg‘on ma’lumot tarqatganlik uchun javobgarlik pandemiya davridagi feyklar to‘lqiniga javob chorasi 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 asosan jurnalist va blogerlarga nisbatan keng qo‘llanilmoqda. Shu bilan birga, ma’lumki, kontent yaratuvchilarga nisbatan jinoiy javobgarlikning haddan tashqari keng asoslari va choralari sovituvchi ta’sirga ega — ya’ni jurnalistlar, OAV 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 ortadi. NNT vakillariga nisbatan ham shunday ta’sir bo‘lishi mumkin.

O‘zbekistonda yolg‘on ma’lumot tarqatganlik uchun javobgarlik ikki turda — ma’muriy va jinoiy javobgarlikda nazarda tutilgan. Quyidagi jadvalda biz qoidabuzarliklarning yuzaga kelishining huquqiy asoslari va yolg‘on ma’lumotlar tarqatilgan taqdirda qo‘llanilishi mumkin bo‘lgan javobgarlik choralarini ko‘rsatib o‘tdik.

Javobgarlik turlari	Qachon qo‘llanadi?	Javobgarlik choralari
Ma’muriy javobgarlik 	1. Shaxsning qadr-qimmatini kamsitishga yoki uni obro‘sizlantirishga olib keladigan yolg‘on axborotni, shu jumladan OAVda, internetda tarqatish[30]. 2. Jamoat tartibiga yoki xavfsizligiga tahdid soladigan yolg‘on axborotni, shu jumladan OAVda, internetda tarqatish[31]. BHMning 50 baravari yoki BHMning 50 baravaridan 100 baravarigacha miqdorda ma’muriy jarima (moddaning qismiga qarab).	Ma’muriy jarima BHMning 50 baravari yoki BHMning 50–100 baravari (moddaning qismiga qarab)
Jinoiy javobgarlik 	Shaxsning qadr-qimmatini kamsitishga yoki uni obro‘sizlantirishga olib keladigan yolg‘on axborotni tarqatish, shu jumladan ommaviy axborot vositalarida, internetda tarqatish, shunday harakatlar uchun ma’muriy jazo qo‘llanilganidan keyin sodir etilgan bo‘lsa[32]	150–200 BHMgacha jarima; 240–300 soatgacha majburiy ishlar yoki 2 yilgacha axloq tuzatish ishlari yoki 2–3 yilgacha ozodlikni cheklash;

Yolg‘on ma’lumot tarqatish to‘g‘risidagi ishlar bo‘yicha yuridik yordam, qoida tariqasida, muallif, bloger yoki tahririyatni ma’muriy va jinoiy javobgarlikka tortishda, barcha bosqichlarda himoya qilish va ularning manfaatlarini himoya qilishni o‘z ichiga oladi.

Ushbu toifadagi ishlarda e’lon qilingan ma’lumotlarning ishonchliligini isbotlovchi dalillar asosiy ahamiyatga ega. Sud yoki sudga qadar tekshiruv organi tomonidan nashr matni, sarlavhalar, sharhlar, videomateriallar va ularning fragmentlari (jumladan, imzolar, razm solish, montaj) ekspertizasi tayinlanadi, tarqatish konteksti, ma’lumotlar manbalari va axborotni tekshirishning halolligi tahlil qilinadi.

---

[30] O‘zbekiston Respublikasi Ma’muriy javobgarlik to‘g‘risidagi kodeksining 202-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/97661

[31] O‘zbekiston Respublikasi Ma’muriy javobgarlik to‘g‘risidagi kodeksining 202-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/97661

[32] O‘zbekiston Respublikasi Jinoyat kodeksining 244-moddasi. Kodeks matni quyidagi havola orqali mavjud: https://www.lex.uz/acts/111457

Bunday ishlar bo‘yicha himoya strategiyasi e’lon qilingan natijalarning baholanishini o‘z ichiga oladi (masalan, obro‘ga putur yetkazish, «obro‘sizlantirish,» jamoat tartibiga/xavfsizlikka tahdid). Bunday oqibatlar maqbullik, aloqadorlik va ishonchlilik mezonlariga javob beradigan tegishli dalillar bilan tasdiqlanishi kerak. E’lon qilish va kelib chiqqan oqibatlar o‘rtasidagi sababiy bog‘liqlik, shuningdek, qasd va takroriylikning mavjudligi yoki mavjud emasligi (jinoiy javobgarlik avval shunday harakatlar uchun ma’muriy javobgarlikka tortilganlik bilan bog‘liq bo‘lgan hollarda) alohida baholanadi.

2.4.4. “Nafrat tili” (Hate speech)

Markaziy Osiyo mamlakatlarida, shu jumladan O‘zbekistonda ham hate speech (nafrat tili) 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-moddasi “Milliy, irqiy, etnik yoki diniy adovatni qo‘zg‘atish”da[33] amalga oshirilgan.

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 rasmlarda, shuningdek, kontent tarqatuvchisi sifatida tashkilotning platformalaridagi auditoriya izohlarida ham yuzaga keladi.

Alohida turdosh xavf — “urushni targ‘ib qilish” (O‘zbekiston Jinoyat kodeksining 150-moddasi)[34]. Unga urushni targ‘ib qilish, ya'ni bir mamlakatni ikkinchi mamlakatga nisbatan qo‘zg‘atish uchun turli shakldagi qarashlar, g‘oyalar yoki chaqiriqlar tarqatish kiradi; м besh yildan o‘n yilgacha ozodlikdan mahrum qilishni nazarda tutadi. Bundan kelib chiqadigan amaliy xulosa oddiy: nafrat tili yoki zo‘ravonlikka chaqiriqlar uchrashi mumkin bo‘lgan mavzularda imkon qadar neytral yondashuv, umumlashtirish va stereotiplardan voz kechish, (haqoratli so‘zlarni tarqatmagan holda) ehtiyotkorlik bilan iqtibos keltirish hamda tashkilot sahifalari taqiqlangan materiallarni tarqatish kanaliga aylanib qolmasligi uchun sharhlarni tezkor moderatsiya qilish talab etiladi.

Ushbu toifadagi ishlarning murakkabligini hisobga olgan holda, yuridik yordam odatda advokatlar tomonidan ko‘rsatiladi va bunday yordam tashkilot, jurnalist, muharrir, ijtimoiy tarmoq foydalanuvchisi yoki blogerning jinoyat ishlari bo‘yicha huquq va manfaatlarini himoya qilish hamda ularga vakillik qilishni (tergovga qadar tekshiruv, dastlabki tergov bosqichlarida va sudda) o‘z ichiga oladi.

Bu toifadagi ishlarda qadr-qimmatni kamsitish, adovat qo‘zg‘atish, chaqiriqlar yoki targ‘ibot alomatlari mavjudligini baholash uchun matn, sarlavhalar, illustratsiyalar, videolar va sharhlarning sud ekspertizasi tayinlanadi. Bunda nashrning kontekstini, tahririyat tekshiruvining vijdonan o‘tkazilganini, adovat qo‘zg‘atish maqsadi bo‘lmaganini, shuningdek, taqiqlangan sharhlar va repostlar o‘z vaqtida moderatsiya qilinib, o‘chirilganini hujjatlar bilan tasdiqlash muhim. Chunki materiallarning tarqatilishi alohida javobgarlik sohasi sifatida baholanishi mumkin.

---

[33] O‘zbekiston Respublikasi Jinoyat kodeksining 156-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/111457

[34] O‘zbekiston Respublikasi Jinoyat kodeksining 150-moddasi. Kodeks matni bilan quyidagi havola orqali tanishish mumkin: https://www.lex.uz/acts/111457

2.4.5. Huquqiy sirlarni tarqatish

Javobgarlikka tortish uchun yana bir huquqiy asos OAV, ijtimoiy tarmoqlar va messenjerlarda huquqiy sirni tashkil etuvchi axborot yoki ma'lumotlarni tarqatish bo'lishi mumkin.

O'zbekiston qonunchiligida "sir" rejimlari, eng avvalo, shaxsiy hayot daxlsizligi va yozishmalar, telefon so'zlashuvlari, pochta, elektron va boshqa xabarlar sir saqlanishining konstitutsiyaviy kafolatlariga, shuningdek, shaxsga doir ma'lumotlarni himoya qilishga tayanadi; bu huquqlarni cheklashga faqat qonunda nazarda tutilgan hollarda va qoida tariqasida sud qarori asosida yo'l qo'yiladi[35]. Bundan tashqari, O'zbekiston Respublikasining «Axborot erkinligi prinsiplari va kafolatlari to'g'risida»gi Qonuni shaxsning roziligisiz uning shaxsiy hayotiga taalluqli ma'lumotlarni, shuningdek xabarlarni to'plash, saqlash, qayta ishlash, tarqatish va ulardan foydalanishni bevosita taqiqlaydi (qonunchilikda nazarda tutilgan hollar bundan mustasno)[36]. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi qonuni esa shaxsga doir ma'lumotlarga ishlov berish va ularni himoya qilish qoidalarini mustahkamlaydi[37].

O'zbekistonning amaldagi qonunchiligida shaxsiy hayot siridan tashqari yana qanday qonun bilan qo'riqlanadigan sirlar belgilanganligini bilish uchun quyidagi jadvalga qarang. Ular jumlasiga ayrim kasbiy sirlar ham kiradi va bunday ma'lumotlar muayyan toifadagi mutaxassislar (masalan, advokatlar, bank xodimlari, notariuslar va boshqalar) tomonidan oshkor etilmaydi. Mazkur ro'yxat to'liq emas va yuridik yordam ko'rsatish bo'yicha amaliy faoliyat jarayonida to'ldirilishi mumkin.

Huquqiy sirning nomi	Ma'lumotlar hajmini tartibga soluvchi qonun hujjati	Bu huquqiy sirga nimalar kiradi?
Tijorat siri 	O'zbekiston Respublikasining "Tijorat siri to'g'risida"gi Qonuni[38]	Uchinchi shaxslarga noma'lumligi sababli fan-texnika, texnologiya, ishlab chiqarish, moliya-iqtisodiyot sohalarida hamda boshqa sohalarda tijorat qimmatiga ega bo'lgan, qonuniy asosda erkin foydalanilmaydigan axborot bo'lib, ushbu axborot mulkdori uning maxfiyligini muhofaza qilish bo'yicha chora-tadbirlarni ko'radi; Qonun, shuningdek, ma'lumotlarni tijorat siriga kiritishning protsessual masalalarini hamda bunday ma'lumotlarni taqdim etish va himoya qilish tartibini belgilaydi.
Bank siri 	"Bank siri to'g'risida"gi Qonun[39]	Bank siri bank tomonidan muhofaza qilinadigan quyidagi ma'lumotlardan iboratdir: o`z mijozlarining (vakillarining) operatsiyalari, hisobvaraqlari va omonatlariga doir ma'lumotlar; • bank o`z mijoziga (vakiliga) bank xizmatlari ko`rsatishi munosabati bilan mazkur mijoz (vakil) to`g`risida olgan ma'lumotlar;

[35] O'zbekiston Respublikasi Konstitutsiyasining 31-moddasi. Hujjat matni bilan quyidagi havola orqali tanishish mumkin: https://lex.uz/docs/6445147#6445335

[36] "Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi O'zbekiston Respublikasi Qonunining 13-moddasi. Qonun matni bilan havola orqali tanishish mumkin: https://lex.uz/docs/52709

[37] O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni. Qonun matni bilan havola orqali tanishish mumkin: https://lex.uz/docs/4396428

[38] O'zbekiston Respublikasining "Tijorat siri to'g'risida"gi Qonuni. Hujjat matni quyidagi havola orqali mavjud: https://lex.uz/docs/2460799

[39] O'zbekiston Respublikasining "Bank siri to'g'risida"gi Qonuni. Hujjat matni quyidagi havola orqali mavjud: https://www.lex.uz/acts/41882

		• mijozning (vakilning) bank seyflari va binolarida saqlab turilgan mol-mulki, uning xususiyati va qiymati haqidagi ma'lumotlar; • mijoz (vakil) topshirig`iga binoan yoki uning foydasini ko`zlab amalga oshirilgan banklararo operatsiyalar va bitimlar to`g`risidagi ma'lumotlar; • bank sirini tashkil etuvchi ma'lumotlarning banklar o`rtasida muomalada bo`lishi natijasida ma'lum bo`lib qolgan, boshqa bankning mijoziga (vakiliga) doir ma'lumotlar; • jamg`arib boriladigan pensiya tizimining ishtirokchilari, pensiya badallarining miqdori va summalarining harakati, fuqarolarning shaxsiy jamg`arib boriladigan pensiya hisobvaraqlaridagi pensiya jamg`armalari to`g`risidagi ma'lumotlar.
Soliq siri	O'zbekiston Respublikasi Soliq kodeksi	Soliq sirini vakolatli organlar tomonidan olingan soliq to'lovchi to'g'risidagi ma'lumotlar tashkil etadi, O'zR Soliq kodeksining 29-moddasida ko'rsatilgan ayrim ma'lumotlar bundan mustasno[40].
Shifokor siri	O'zbekiston Respublikasining "Fuqarolar sog'lig'ini saqlash to'g'risida"gi Qonuni[41]	Tibbiy yordam so'rab murojaat qilganligi, fuqaroning sog'lig'i holati, uning kasalligi tashxisi to'g'risidagi ma'lumotlar hamda uni tekshirish va davolash chog'ida olingan boshqa ma'lumotlar.
Advokatlik siri	O'zbekiston Respublikasining "Advokatura to'g'risida"gi Qonuni[42], O'zbekiston Respublikasining "Advokatlik faoliyatining kafolatlari va advokatlarning ijtimoiy himoyasi to'g'risida"gi Qonuni[43]	Ishonch bildiruvchi (himoya ostidagi shaxs)ning advokat yordamiga murojaat qilganligi fakti, ishonch bildiruvchi (himoya ostidagi shaxs) yordam so'rab murojaat qilgan masalalar, advokatdan olingan maslahatlar, tavsiyalar va tushuntirishlarning mazmuni, shuningdek advokatning ishonch bildiruvchi (himoya ostidagi shaxs) bilan suhbatlari mazmuniga taalluqli barcha boshqa ma'lumotlar advokatlik sirining predmetini tashkil etadi.
Farzandlikka olish siri	O'zbekiston Respublikasi Oila kodeksi[44]	Farzandlikka olishni sir saqlash qonun bilan himoya qilinadi. Fuqarolik holati dalolatnomalarini qayd etish daftaridagi va boshqa hujjatlardagi farzandlikka oluvchilar farzandlikka olinganlarning ota-onasi emasligini bildiradigan mazmundagi yozuvlar bilan tanishtirish, bu yozuvlardan ko'chirmalar va boshqa ma'lumotlarni farzandlikka oluvchilarning roziligisiz, agar ular vafot etgan bo'lsa, vasiylik va homiylik organining roziligisiz berish taqiqlanadi. Farzandlikka oluvchining yoki vasiylik va homiylik organining erkiga hilof ravishda farzandlikka olish sirini oshkor qilgan shaxslar qonun bilan belgilangan javobgarlikka tortiladilar.

[40] O'zbekiston Respublikasi Soliq kodeksining 29-moddasi. Hujjat matni quyidagi havola orqali mavjud: https://buxgalter.uz/doc?id=610082_nalogovyy_kodeks_respubliki_uzbekistan_(utverjden_zakonom_ruz_ot_30_12_2019_g_n_zru-599)&prodid=1_vse_zakonodatelstvo_uzbekistana#%D1%81%D1%8229

[41] "Fuqarolar sog'lig'ini saqlash to'g'risida"gi O'zbekiston Respublikasi Qonunining 45-moddasi. Qonun matni bilan havola orqali tanishish mumkin: https://lex.uz/docs/41329?ONDATE=31.05.2024%2000#41781

[42] "Advokatura to'g'risida"gi O'zbekiston Respublikasi Qonunining 9-moddasi. Qonun matni bilan havola orqali tanishish mumkin: https://www.lex.uz/acts/58372

[43] O'zbekiston Respublikasining "Advokatlik faoliyatining kafolatlari va advokatlarning ijtimoiy himoyasi to'g'risida"gi Qonuni. Qonun matni bilan havola orqali tanishish mumkin: https://lex.uz/docs/1321

[44] O'zbekiston Respublikasi Oila kodeksining 153-moddasi. Kodeks matni quyidagi havola orqali mavjud: https://lex.uz/docs/104723#161584

Sudyalar maslahatlashuvining sir tutilishi 	O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi[45]	Sudya hukmni alohida xonada, sud esa maslahatxonada chiqaradi. Bunday paytda mazkur xonada faqat sudyaning o‘zi yoki ushbu ish bo‘yicha sud tarkibiga kirgan sudyalar hozir bo‘lishlari mumkin. Boshqa shaxslarning hozir bo‘lishlariga yo‘l qo‘yilmaydi.
Notarial harakatlarning sir saqlanishi 	O‘zbekiston Respublikasining “Notariat to‘g‘risida”gi Qonuni[46]	Notariusning, notarial harakatlarni amalga oshiruvchi boshqa mansabdor shaxslarning, shuningdek amalga oshirilayotgan notarial harakatlar to`g`risida o`z xizmat vazifalarini bajarishi munosabati bilan xabardor bo`lib qolgan shaxslarning o`zlariga ma’lum bo`lgan ma’lumotlarni oshkor qilishi, shu jumladan mehnat shartnomasi bekor qilinganidan keyin ham oshkor qilishi taqiqlanadi.

Huquqiy sirlarni saqlash tartib-taomillariga rioya qilish muhim, chunki xavf-xatarlar nafaqat bunday ma’lumotlarni tarqatishda, balki hujjatlarni qayta nashr etish, yozishmalardan iqtibos keltirish, moliyaviy va soliq ma’lumotlarini tegishli huquqiy asoslarsiz e’lon qilishda ham yuzaga keladi.

Bunday ishlar bo‘yicha yuridik yordam doirasi odatda materiallar va hujjatlarni e’lon qilish va oshkor qilishdan oldin huquqiy ekspertizadan o‘tkazish (huquqiy asos, rozilik, ma’lumotlarni minimallashtirish) hamda ma’muriy va jinoiy ishlar bo‘yicha tekshirish, dastlabki tergov bosqichida va sudda himoya qilishni o‘z ichiga oladi. Ushbu toifadagi ishlarda ko‘pincha sud ekspertizalari tayinlanadi va pozitsiyaning asosiy elementlari tegishli dalillarga asoslanadi: maqbullik, aloqadorlik, ishonchlilik, sabab-oqibat aloqasi va zarar yoki zararni hujjat bilan tasdiqlash.

2.4.6. Shaxsga doir ma’lumotlarni noqonuniy ravishda tarqatish

O‘zbekistonda shaxsga doir ma’lumotlarni noqonuniy tarqatish birinchi navbatda “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni bilan tartibga solinadi[47]. Shaxsga doir ma’lumotlarni tarqatish deganda, shaxsga doir ma'lumotlarni nomuayyan doiradagi shaxslarga oshkor etishga, shu jumladan shaxsga doir ma'lumotlarni ommaviy axborot vositalarida hammaga ma'lum qilishga, Internet jahon axborot tarmog‘iga joylashtirishga yoki shaxsga doir ma'lumotlardan biror-bir boshqa usul bilan foydalanish imkonini berishga qaratilgan harakatlar tushuniladi[48]. Bunda mulkdor/operator va shaxsga doir ma’lumotlarga kirish huquqini olgan har qanday shaxslar subyektning roziligisiz ularni oshkor qilmasligi va tarqatmasligi, bunday ma’lumotlarga ishlov beruvchi xodimlar esa ishonchli yoki o‘zlariga ma’lum bo‘lgan ma’lumotlarning oshkor etilishiga yo‘l qo‘ymasligi shart.

Shaxsiy ma’lumotlar bilan bog‘liq noqonuniy harakatlar uchun ham ma’muriy, ham jinoiy javobgarlik nazarda tutilgan. Ma’muriy javobgarlik shaxsga doir ma’lumotlarni qonunga xilof ravishda yig‘ish, tizimlashtirish, saqlash, o‘zgartirish, to‘ldirish, ulardan foydalanish,

[45] O‘zbekiston Respublikasi Jinoyat-protsessual kodeksining 456-moddasi. Kodeks matni quyidagi havola orqali mavjud: https://lex.uz/docs/111463#249950

[46] “Notariat to‘g‘risida”gi O‘zbekiston Respublikasi Qonunining 6-moddasi. Qonun matni bilan havola orqali tanishish mumkin: https://lex.uz/docs/57043#3992406

[47] O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. Qonun matni bilan havola orqali tanishish mumkin: https://lex.uz/docs/4396428#4397998

[48] 14-modda. O‘sha manba

ularni berish, tarqatish, uzatish, shu jumladan transchegaraviy uzatish uchun yuzaga keladi. Javobgarlik choralari — fuqarolarga BHMning 7 baravari, mansabdor shaxslarga esa BHMning 50 baravari miqdorida ma'muriy jarima[49].

Jinoiy javobgarlik ma'muriy jazo qo'llanilganidan keyin sodir etilgan xuddi shunday qilmishlar uchun kelib chiqadi va BHMning 100–150 baravarigacha miqdorda jarima solishga (yoki boshqa choralarga) sabab bo'ladi, kvalifikatsiya belgilari (guruh, takroriylik, g'arazli niyat, xizmat mavqeyidan foydalanish, og'ir oqibatlar) bo'lganda esa — ozodlikni cheklash yoki ozodlikdan mahrum qilishgacha bo'lgan og'irroq sanksiyalar qo'llaniladi[50].

Amaliy nuqtai nazardan shaxsiy ma'lumotlarni tarqatishning qonuniyligi bo'yicha asosiy masala deyarli har doim ishlov berish yoki e'lon qilishning huquqiy asosi va rozilikning isbotlanishiga borib taqaladi. Shaxsga doir ma'lumotlarni noqonuniy tarqatish bilan bog'liq ishlar bo'yicha yuridik yordam odatda quyidagilarni o'z ichiga oladi:

- shaxsga doir ma'lumotlar bilan bog'liq harakatlarning qonuniy asoslarini huquqiy baholash (rozilik olinganmi? Shaxsga doir ma'lumotlar qonuniy ravishda tarqatilganmi? Ularning tarqatilishi zarar yetkazilishiga olib kelganmi? Ushbu hodisalar o'rtasida sababiy bog'liqlik mavjudmi? va h.k.);
- ariza beruvchilar va davlat organlari bilan o'zaro hamkorlikni huquqiy jihatdan kuzatib borish (iltimosnomalar, tushuntirishlar va shikoyatlar taqdim etish);
- tekshiruv, dastlabki tergov va sud bosqichlarida ma'muriy hamda jinoyat ishlari bo'yicha himoya qilish.

Bunday nizolarda dalil-isbotlar hal qiluvchi rol o'ynaydi, xususan:

- ma'lumotni tarqatish fakti va usuli (skrinshotlar, loglar, havolalar, sana va vaqt);
- ma'lumotlar hajmi va ularning identifikatsiya qilinishi, rozilikning mavjudligi yoki yo'qligi hamda uning shakli;
- boshqa maqbul, aloqador va ishonchli dalillar.

2.4.7. Media akkauntlaridagi izohlar uchun javobgarlik

Endi foydalanuvchilarning nashrlar ostida qoldiradigan kontenti uchun javobgarlik masalasiga batafsilroq to'xtalib o'tamiz. Sharhlar muhokama qilinayotgan maqolaga aloqador bo'lmasligi mumkin, biroq ularning matnida qonunga zid kontent, haqorat, hate speech (nafrat tili), o'zgalarning shaxsiy ma'lumotlari, sha'n va qadr-qimmatga putur yetkazuvchi yoki yolg'on ma'lumotlar bo'lishi xavfi bor. Sharhlar, ularni qoldirgan muallif hamda nashri ostida fikr yozilgan akkaunt egasi o'rtasidagi javobgarlikni taqsimlash nuqtayi nazaridan muammoli bo'lishi mumkin.

[49] O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 462-moddasi. Kodeks matni bilan havola orqali tanishish mumkin: https://www.lex.uz/acts/97661

[50] O'zbekiston Respublikasi Jinoyat kodeksining 1412 -moddasi. Kodeks matni bilan havola orqali tanishish mumkin: https://www.lex.uz/acts/111457

Sharhning mazmuni uchun sharh muallifining o‘zi javobgar bo‘ladi, biroq raqamli axborot resurslari (saytlar, sahifalar, kanallar va ijtimoiy tarmoqlardagi akkauntlar) egalari va ma’murlari sayt va bloglardan taqiqlangan axborotni joylashtirish uchun foydalanishga yo‘l qo‘ymasliklari shart va bu “Axborotlashtirish to‘g‘risida”gi Qonunda to‘g‘ridan-to‘g‘ri mustahkamlab qo‘yilgan[51]. Shu sababli moderatsiyaning yo‘qligi va murojaatlarni e’tiborsiz qoldirish akkaunt egalari uchun xatarlarni oshiradi.

Sharh muallifi bilan ijtimoiy tarmoq yoki veb-saytdagi akkaunt egasi o‘rtasidagi javobgarlik chegarasi qayerdan o‘tadi? Muammoli sharh uchun javobgarlikka tortilish xavfi quyidagi uch omildan kamida bittasi mavjud bo‘lgan taqdirda keskin oshadi:

Muammoli izohni ma’qullash (uni mahkamlab, alohida belgilab qo‘yish, “auditoriya nuqtayi nazari” sifatida havola qilish).

Moderatsiyaning mavjud emasligi (mas’ul shaxsning yo‘qligi, qoidalarning yo‘qligi, o‘chirib tashlashning yo‘qligi).

Izohlardagi murojaatlarni e’tiborsiz qoldirish (yaqqol qoidabuzarlikni o‘chirmaslik, ko‘rilgan choralarni qayd etmaslik).

Muammoli izohlar uchun javobgarlikka tortilishning oldini olish maqsadida quyidagi choralarni ko‘rish mumkin:

- foydalanuvchilar uchun izoh qoldirish qoidalarini joriy etish;
- premoderatsiya va moderatsiyaning ichki tartibini ishlab chiqish.

Foydalanuvchilar uchun izoh qoldirish qoidalari — bu raqamli axborot resurslari egalari va ma’murlarining ehtimoliy muammoli izohlar uchun javobgarlikni taqsimlash masalasidagi ommaviy siyosati (pozitsiyasi) hisoblanadi. Mazkur qoidalarga kiritilishi lozim bo‘lgan majburiy minimal talablar quyidagilardan iborat:

- foydalanuvchilar uchun izoh qoldirish qoidalari veb-saytdagi, ijtimoiy tarmoqlardagi akkauntlarda va messenjerlardagi barcha izohlarga nisbatan qo‘llaniladi;
- izoh qoldirish orqali foydalanuvchi ushbu qoidalarga roziligini tasdiqlaydi va izoh mazmuni uchun shaxsan javobgar bo‘ladi;
- izohlarda haqorat va inson qadr-qimmatini kamsitish, kamsitish, adovatni qo‘zg‘atish va zo‘ravonlikka da’vatlar, ekstremizm, urushni targ‘ib qilish, pornografiya va giyohvandlik vositalarini targ‘ib qilish, yolg‘on axborot, shuningdek fishing, spam, majburan tiqishtiriladigan reklama, shaxsga doir ma’lumotlar va shaxsiy yozishmalarni, skrinshotlarni e’lon qilish hamda odobsiz so‘zlardan foydalanish taqiqlanadi;
- akkaunt egasi qoidalarni buzuvchi izohlarni o‘chirish va foydalanuvchilarni bloklash huquqiga ega;
- akkaunt egasi qoidabuzarliklar to‘g‘risidagi murojaatlarni ko‘rib chiqadi va izohlarni o‘chirish hamda ulardan foydalanishni cheklashni o‘z ichiga olgan tegishli choralarni ko‘radi.

[51] O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonunining 12-moddasi. Qonun matni bilan quyidagi havola orqali tanishish mumkin: https://lex.uz/acts/82956

Izoh qoldirish qoidalaridan tashqari, **izohlarni moderatsiya qilishning ichki tartibini** ishlab chiqish va qabul qilish tavsiya etiladi. Mazkur hujjatga quyidagi qoidalar kiritilishi lozim (minimal ro‘yxat):

- moderatsiya modeli belgilanadi — premoderatsiya yoki postmoderatsiya qo‘llaniladimi? Yuqori xavfli mavzular (adovat, zo‘ravonlik, urush, feyk axborot, shaxsga doir ma’lumotlar) uchun kuchaytirilgan tartib belgilanadi (masalan, premoderatsiya yoki izoh qoldirish imkoniyatini cheklash);
- muddatlar belgilanadi — yangi izohlar qanchalik tez tekshirilishi va tahririyat shikoyatlarga qanchalik tez munosabat bildirishi lozimligi aniqlanadi (masalan, ish kuni davomida yoki yuqori xavfli mavzular bo‘yicha bir necha soat ichida);
- taqiqlangan kontentni o‘z ichiga olgan va Izoh qoldirish qoidalarini buzuvchi izohlar o‘chirilishi (yoki yashirilishi), takroriy qoidabuzarlik sodir etgan foydalanuvchilar esa bloklanishi belgilab qo‘yiladi. Qarorlar yagona mezonlar asosida qabul qilinadi;
- bahsli yoki ehtimoliy xavf tug‘diruvchi holatlar uchun muammoli izohlarni qayd etish tartibi nazarda tutiladi. Bu izohga havola, sana va vaqtni saqlash zarurligini anglatadi. Muammoli izohlarning skrinshotlari faqat ichki dosye uchun olinadi va tarqatilmaydi;
- qaysi holatlar majburiy ravishda muharrir yoki yuristga yuborilishi belgilanadi. Bular adovatni qo‘zg‘atish alomatlari, zo‘ravonlikka da’vatlar, ekstremizm, shaxsga doir ma’lumotlarni e’lon qilish, yolg‘on axborot, giyohvandlik vositalarini targ‘ib qilish va boshqa taqiqlangan kontent mavjud bo‘lgan izohlardir;
- muammoli izohlarni «auditoriya pozitsiyasi» sifatida mahkamlab qo‘yish, ulardan iqtibos keltirish yoki ularni qayta e’lon qilish taqiqlanadi. Tahririyat tomonidan izohni har qanday tarzda alohida ajratib ko‘rsatish javobgarlik xavfini oshiruvchi qo‘shimcha omil sifatida baholanadi.

Izohlar uchun javobgarlik masalalari bo‘yicha yuridik yordam, odatda, pablik egalari va ma’murlarining fuqarolik-huquqiy nizolarda, shu jumladan sha’n, qadr-qimmat va ishchanlik obro‘sini himoya qilish bilan bog‘liq nizolarda huquq va manfaatlarini himoya qilish hamda ularga vakillik qilishni o‘z ichiga oladi. Agar bildirilgan da’volar izohlardagi qonunga xilof kontent, haqorat, tuhmat yoki yolg‘on axborotni tarqatish bilan bog‘liq bo‘lsa, yuridik yordam ma’muriy yoki jinoyat ishlari bo‘yicha himoyani ham qamrab oladi.

Bunday ishlarda izohga havola, sana va vaqt, akkaunt ma’lumotlari (agar mavjud bo‘lsa), kelib tushgan shikoyatlar hamda moderatsiya doirasida ko‘rilgan choralar (yashirish, o‘chirish yoki bloklash) dalil sifatida qayd etiladi. Zarur hollarda izoh matni va publikatsiya konteksti yuzasidan ekspertiza o‘tkaziladi.

2.4.8. Onlayn platformalarning kontentga oid qoidalari

Onlayn platformalarning kontent qoidalari 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. Tahririyat uchun bu alohida xavf, chunki kontent bloklanishi, ogohlantirish berilishi, monetizatsiya to‘xtatilishi 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 qayd etilganidek, hate speech yoki nafrat tili (insoniylikdan mahrum etuvchi ifodalar, kamsitish, diskriminatsiya yoki zo‘ravonlikka da’vatlar);
- xavfli kontent va zo‘ravonlikka da’vatlar, ekstremistik va terroristik kontent;
- nozik mavzulardagi dezinformatsiya (sog‘liq, xavfsizlik, inqirozlar);
- ta’qib, tegajog‘lik yoki tahdidlar;
- shaxsga doir ma’lumotlar va shaxsiy hayot daxlsizligini buzuvchi publikatsiyalar.

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=535nt8Z20sG4lW62MZPJvL

Telegram
https://telegram.org/moderation

Amaliy xulosa — o‘z siyosatingizda nafaqat O‘zbekistonning amaldagi qonunchiligiga, balki onlayn platformalar tomonidan aniq belgilangan taqiqlangan kontent doiralariga, ayniqsa kamsitish, zo‘ravonlik, soxta ma’lumotlar va shaxsiy ma’lumotlar masalalariga oid mavzularga ham e’tibor qarating. Bahsli holatlarda xavflarni kamaytirish, muammolarga sabab bo‘lmaydigan, biroq ayni paytda ijtimoiy ahamiyatga ega mavzularni chetlab o‘tmaydigan kontentni e’lon qilish xavfsizroq hisoblanadi.

2.4.9. Raqamli muhitda kontent nazorati qanday amalga oshiriladi?

Yuristlar uchun raqamli muhitdagi kontent ustidan nazorat nafaqat O‘zbekistonda, balki Markaziy Osiyoning boshqa mamlakatlarida qanday amalga oshirilishini bilish foydali bo‘ladi. Bunday nazorat (1) onlayn platformalarning o‘zi, (2) auditoriya va (3) davlat organlari/vakolatli tuzilmalar tomonidan amalga oshiriladi.

E’tibor bering, ushbu nazorat kanallari parallel ravishda amal qiladi. Bu ayni bir post yoki izoh bir vaqtning o‘zida platforma qoidalarini buzishi, muayyan shaxsning huquqlariga daxl qilishi va milliy qonunchilikda belgilangan cheklovlar doirasiga tushishi mumkinligini anglatadi.

Birinchidan, onlayn platformalar taqiqlangan kontentni (nafrat tili, zo‘ravonlikka chaqiriqlar, pornografiya, noqonuniy savdo va h.k.) aniqlash uchun avtomatik filtrlar va moderatsiya orqali o‘z standart va tartib-taomillarini qo‘llaydi. Buning oqibatlari ko‘pincha kontentni o‘chirish, qamrovni cheklash, ogohlantirishlar (“strayklar”), vaqtinchalik blokirovka qilish

va monetizatsiyani o‘chirib qo‘yishdan iborat bo‘ladi. Tahririyatlar va mualliflar uchun bu platforma qoidalari bo‘yicha xatarlarni oldindan baholash, o‘z harakatlarining halolligini isbotlovchi dalillarni (manbalar, faktcheking) saqlash va platforma qarorlari ustidan shikoyat qilish tartib-taomillaridan foydalanish zarurligini anglatadi.

Ikkinchidan, auditoriya onlayn platformalar ma’muriyatiga ham, davlat organlari, politsiya, prokuraturaga ham shikoyat yuborishi mumkin. Amalda shikoyatlar oqimi o‘z-o‘zidan bir bosim vositasiga aylanadi. Shu bois, huquqiy jihatdan to‘g‘ri yondashuv — izoh qoldirishning tushunarli qoidalariga, murojaatlarni qabul qilish kanaliga ega bo‘lish va bildirilgan munosabatni (aynan nima, qachon va qanday asosda o‘chirilgani yoki yashirilganini) qayd etib borishdir.

Uchinchidan, davlat organlari yoki vakolatli tashkilotlar ijtimoiy tarmoqlar va saytlardagi ommaviy kontentni milliy qonunchilik bilan taqiqlangan materiallar mavjudligi yuzasidan monitoring qilishi va o‘z vakolatlari doirasida javob choralarini (jumladan, kontentni o‘chirishni talab qilish, kirishni cheklash, protsessual tekshiruvlar o‘tkazish) ko‘rishi mumkin.

Raqamli muhitda kontentni nazorat qilish va monitoring yuritishning bunday uch bosqichli tizimi tahririyat yoki muallif uchun huquqiy xatar bir yo‘la uchta manbadan: (1) platformaning harakatlari, siyosati va qarorlaridan, (2) auditoriya shikoyatlaridan hamda (3) vakolatli davlat organlarining harakatlari va qarorlaridan kelib chiqishini anglatadi. Shu sababli yurist uchun materialni bir vaqtning o‘zida ham platforma qoidalari, ham xususiy da’volar xatarlari (diffamatsiya, shaxsga doir ma’lumotlar, haqorat, mualliflik huquqi), ham O‘zbekiston Respublikasi milliy qonunchiligidagi cheklovlar nuqtayi nazaridan baholash muhimdir.

2.5. Raqamli muhitda mualliflik huquqlarini himoya qilish

Internet foydalanuvchilari, jurnalistlar va media vakillari muntazam ravishda kontent yaratadi, shuningdek boshqa shaxslarga tegishli kontent — matnlar, fotosuratlar, videolar, musiqa, infografika va dizayn materiallari bilan ishlaydi. Jurnalistlar va tahririyatlar tomonidan yaratiladigan mediamateriallarning aksariyati mualliflik huquqi obyekti hisoblanadi.

Mediakontentni mualliflik huquqi obyekti deb e’tirof etishning asosiy mezonlari quyidagilardan iborat:

- yakka tartibdagi yoki birgalikdagi ijodiy faoliyat natijasi bo‘lishi;
- idrok etish mumkin bo‘lgan muayyan shaklda ifodalangan bo‘lishi (matn, tasvir, audio/video, raqamli yozuv va h.k.).

O‘zbekiston Respublikasining “Mualliflik huquqi va turdosh huquqlar to‘g‘risida”gi Qonuni (O‘RQ-42, 20.07.2006-y.) mualliflik huquqi “yaratish fakti tufayli” yuzaga kelishini va ro‘yxatdan o‘tkazish yoki boshqa rasmiyatchiliklarni talab qilmasligini belgilaydi.

Raqamli muhitda asarni Internet tarmog‘ida e’lon qilish «barchaning e’tiboriga yetkazish», ya’ni foydalanuvchilar asardan «o‘z tanloviga ko‘ra istalgan joyda va istalgan vaqtda» foydalana olishi mumkin bo‘lgan tarzda taqdim etish hisoblanadi. Mazkur harakat asarni takrorlash va tarqatish bilan bir qatorda muallif yoki huquq egasining mutlaq huquqlari jumlasiga kiradi (ya’ni ruxsat yoki litsenziya olishni talab etadi).

O‘zbekiston mualliflik huquqlarini himoya qilishning xalqaro tizimiga qo‘shilgan. Mamlakat 2005-yil 19-apreldan boshlab Adabiy va badiiy asarlarni muhofaza qilish to‘g‘risidagi Bern konvensiyasining (Bern konvensiyasi), shuningdek 2019-yil 17-iyuldan boshlab Butunjahon intellektual mulk tashkilotining «internet shartnomalari» deb ataluvchi hujjatlari — BIMTning Mualliflik huquqi bo‘yicha shartnomasi (WCT) va BIMTning Ijrolar va fonogrammalar bo‘yicha shartnomasi (WPPT) ishtirokchisi hisoblanadi.

Bern konvensiyasi ishtirokchi davlatlar mualliflari va asarlariga nisbatan milliy muhofaza rejimi prinsipini, asar yaratilganligi fakti asosida mualliflik huquqlarining avtomatik muhofaza qilinishini hamda mualliflik huquqlarini muhofaza qilishning kamida 50 yillik muddatini belgilaydi. BIMT shartnomalari mualliflik huquqlarini himoya qilishni raqamli muhitga moslashtiradi, jumladan texnik himoya choralarini (masalan, himoya yoki shifrlash vositalarini chetlab o‘tishdan himoya qilish) hamda huquqlarni boshqarish to‘g‘risidagi axborotni (rights management information) himoya qilishni nazarda tutadi.

Qonunning 5-moddasiga muvofiq, «Mualliflik huquqi ijodiy faoliyat natijasi bo‘lmish fan, adabiyot va san’at asarlariga, ularning maqsadi va qadr-qimmati, shuningdek ifodalanish usulidan qat’i nazar, tatbiq etiladi». Mualliflik huquqi biron-bir obyektiv shaklda bo‘lgan oshkor qilingan asarlarga ham (nashr etilgan, biror-bir usulda, shu jumladan Internet tarmog‘ida tarqatilgan), oshkor qilinmagan asarlarga ham tatbiq etiladi.

Mualliflik huquqi muallifning shaxsiy nomulkiy va mulkiy huquqlaridan iborat. Shaxsiy nomulkiy huquqlar begonalashtirilmaydi, mulkiy huquqlar esa muallifning (hammualliflarning) butun hayoti davomida va muallif (hammualliflar) vafot etganidan keyin 70 yil mobaynida amal qiladi. Mulkiy huquqlar asardan har qanday shaklda foydalanish bilan bog‘liq keng doiradagi huquqlarni, shu jumladan asarni tarjima qilish va uni boshqa shakllarga qayta ishlash huquqlarini o‘z ichiga oladi.

Huquqlar turi	Toifa	Himoya hajmi	Buzilish usullari
Shaxsiy nomulkiy huquqlar	Mualliflik huquqi	Asar muallifi sifatida e’tirof etilmoq	Asardan muallif nomini ko‘rsatmasdan nusxa ko‘chirish va tarqatish yoki mualliflikni o‘zlashtirish (plagiat)
	Muallif nomiga bo‘lgan huquq	Asardan foydalanilganda muallifning ismi yoki uning taxallusi ko‘rsatilishi shart	Asarni muallifning roziligisiz yoki boshqa shaxs nomi ostida yoxud muallif nomini buzib ko‘rsatgan holda nashr etish va tarqatish, muallifning taxallusini oshkor qilish
	Mualliflik huquqida e’lon qilish huquqi	Asarni har qanday shaklda ommaga e’lon qilish yoki e’lon qilishga ruxsat berish huquqi, shu jumladan asarni ommaga e’lon qilishdan voz kechish (asarni qaytarib olish) huquqi.	Muallifning e’lon qilinmagan asari nusxalarini uning roziligisiz chop etish
	Muallif obro‘sini himoya qilish huquqi	Asarni, shu jumladan uning nomini muallifning sha’ni va qadr-qimmatiga putur yetkazishi mumkin bo‘lgan har qanday buzib ko‘rsatishdan yoki boshqa har qanday tajovuzdan himoya qilish huquqi	Asarni muallifning roziligisiz buzib ko‘rsatish va tahrir qilish

Mulkiy huquqlar	Ko‘paytirish huquqi	Asarning raqamli yoki jismoniy nusxalarini (nusxalarini) yaratish	Muallif ruxsatisiz asarni yaratish va nusxa ko‘chirish (qaroqchilik)
	Tarqatish huquqi	Asarning raqamli yoki jismoniy nusxalarini tarqatish va sotish, shu jumladan ijaraga berish huquqi	Muallif ruxsatisiz sotish, ijaraga berish (kitoblar, musiqa yoki filmlarning noqonuniy savdosi)
	Ommaviy namoyish va ijro etish huquqi	Ommaviy ijro va omma oldida namoyish qilish	Muallif ruxsatisiz jamoat joylarida asarni namoyish qilish yoki ommaviy ijro etish
	Qayta ishlash huquqi	Asl nusxa asosida yangi (hosilaviy) asarlar yaratish	Muallif ruxsatisiz asarni boshqa formatlarga qayta ishlash, chet tillariga tarjima qilish, ssenariy, pyesa, sahna ko‘rinishiga moslashtirish, musiqiy kaver va remikslar yaratish
	Omma e’tiboriga etkazish	Raqamli nusxalarni Internetda tarqatish	Asarning raqamli nusxalarini muallifning ruxsatisiz raqamli muhitga yuklash va tarqatish

Muallifga (huquq egasiga) mualliflik haqini olish huquqi kafolatlanadi. Qonunchilikda asarlarning muayyan turlari va ulardan foydalanish usullari uchun mualliflik haqining eng kam stavkalari belgilanadi.

2.5.1. Boshqa shaxslarga tegishli asarlardan foydalanish qoidalari

Internet tarmog‘i, ijtimoiy tarmoqlar, messenjerlar va veb-saytlarda kontentning keng tarqalishi boshqa shaxslarga tegishli kontentdan foydalanish imkonini beradi va bunday kontent huquq egalarining ruxsatisiz ishlatilishi mumkin. Biroq Internetdagi materiallardan erkin foydalanish mumkin emas hamda mualliflar va (yoki) huquq egalarining roziligisiz va mualliflik haqini to‘lamasdan barcha materiallarni takrorlashga yo‘l qo‘yilmaydi. Har bir matn yoki fotosurat, audio yoxud videokontentning o‘z muallifi yoki huquq egasi mavjud. Veb-saytlar va ijtimoiy tarmoqlardagi materiallardan foydalanish siyosatini diqqat bilan o‘rganish zarur. Matn yoki fotosuratning ochiq akkauntda e’lon qilinganligi uni barcha shaxslar tomonidan va istalgan joyda qayta e’lon qilish 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 tusidagi kundalik yangiliklarga doir va joriy voqealar haqidagi xabarlar” qonun bilan muhofaza qilinadigan asarlar jumlasiga kirmaydi.

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

Ijrochilarga, fonogramma ishlab chiqaruvchilarga va efir yoki kabel orqali ko‘rsatuv yoxud eshittirish beruvchi tashkilotlarga beriladigan turdosh huquqlar ham Internetda muhofaza qilinadi. Masalan, fonogrammalar, musiqa asarlarining yozuvlari, konsertlar va jonli ijrolarning translyatsiyalari hamda yozuvlari.

Umumiy qoidaga ko‘ra, mutlaq mualliflik huquqlari boshqa jismoniy shaxslar yoki kompaniyalarga tegishli bo‘lgan asarlardan foydalanishni istagan shaxs mutlaq huquqlar egasining ruxsatini olishi shart («Mualliflik huquqi va turdosh huquqlar to‘g‘risida»gi Qonunning 19-moddasi). Ruxsat mualliflik shartnomasini tuzish orqali yozma shaklda ifodalanishi (Qonunning 38-moddasi) va mualliflik haqi to‘lanishi lozim.

MUHIM!

© mualliflik huquqini muhofaza qilish belgisini ko‘rsatish, o‘zlashtirilgan material manbasini (masalan, boshqa OAV yoki veb-saytni) qayd etish yoxud unga havola berish, shuningdek mualliflik asaridan notijorat maqsadlarda foydalanish mualliflar yoki huquq egalarining asardan noqonuniy foydalanish bilan bog‘liq da’volaridan ozod etmaydi.

2.5.2. Mualliflik huquqini himoya qilish usullari

Agar muallif yoki huquq egasi o‘zining mualliflik huquqlari buzilgan deb hisoblasa, ularni himoya qilish uchun huquqbuzarga (yaxshisi, yozma ravishda) noqonuniy foydalanishni to‘xtatish talabi bilan murojaat qilishga haqli. Agar huquqbuzar talablarni bajarishdan bosh tortsa, muallif (huquq egasi) fuqarolik (agar taraflardan biri jismoniy shaxs bo‘lsa) yoki iqtisodiy ishlar bo‘yicha (agar ikkala taraf ham yuridik shaxs bo‘lsa) sudiga quyidagi da’vo bilan murojaat qilishga haqli:

- huquqlarni tan olish;
- huquq buzilishidan oldin mavjud bo‘lgan holatni tiklash va huquqni buzuvchi yoki uni buzish xavfini tug‘diruvchi harakatlarni to‘xtatish;
- huquq egasining huquqi buzilmaganida, huquq egasi fuqarolik muomalasining odatdagi sharoitlarida olishi mumkin bo‘lgan olinmagan daromadlar miqdorida zararni qoplash. Agar huquqbuzar mualliflik huquqi yoki turdosh huquqlarni buzish oqibatida daromad olgan bo‘lsa, huquq egalari boshqa zararlar bilan bir qatorda boy berilgan foydaning o‘rnini ushbu daromadlardan kam bo‘lmagan miqdorda qoplashni talab qilishga haqli;
- zarar yetkazilganligidan qat’i nazar, ish muomalasi odatlarini hisobga olgan holda huquqbuzarlikning xususiyati va huquqbuzarning aybdorlik darajasidan kelib chiqqan holda to‘lanadigan zararni qoplash o‘rniga bazaviy hisoblash miqdorining yigirma baravaridan ming baravarigacha miqdorda kompensatsiya to‘lash.

Muallif (yoki huquq egasi) o‘z huquqlari buzilgan taqdirda, huquqbuzardan ma’naviy zararni qoplashni talab qilishga haqli. Qonunchilikda mualliflik huquqlarini buzganlik uchun ma’muriy va jinoiy javobgarlik belgilangan.

Javobgarlik turlari	Qachon qo‘llanadi	Javobgarlik choralari
MJtK 177[1]-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	Intellektual 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 **Nomulkiy huquqlar**	BHMning 50 baravaridan 70 baravarigacha jarima Muayyan huquqdan 5 yilgacha mahrum qilish 360 soatgacha bo‘lgan majburiy ishlar 2 yilgacha ozodlikni cheklash
149[1]-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 **Mulkiy huquqlar**	50 dan 100 BHMgacha jarima 2 yilgacha axloq tuzatish ishlari 2 yilgacha ozodlikni cheklash 2 yilgacha ozodlikdan mahrum qilish

2.5.3. 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 messenjer 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 qilishi 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.

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 shaklda yuboriladi va quyidagi ma’lumotlarni ko‘rsatishni talab etadi:

- boshqa mualliflik asarlari joylashtirilgan havolalar;
- muallif yoki huquq egasining mualliflik huquqi obyekti bo‘yicha 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;

Qoidabuzarlikni aniqlashda yordam beruvchi ayrim maxsus avtomatik vositalar:

Google Image Search	Copyscape	Pixsy
internetdagi tasvir nusxalarini qidirish imkonini beruvchi bepul vosita;	matn materiallarida plagiatni aniqlash uchun xalqaro xizmat. Kengaytirilgan imkoniyatlarga ega bepul va pullik versiyalar mavjud;	tasvir bo‘yicha qidirish funksiyasiga ega fotosuratlar bilan ishlash platformasi.

2.6. Kompaniyalar uchun muhim hujjatlar va siyosatlar

Maxfiy materiallardan foydalanish siyosati kompaniyaning ichki hujjati bo‘lib, u erkin tarqatish uchun mo‘ljallanmagan ma’lumotlar bilan ishlashning tushunarli qoidalarini belgilaydi. Bunday siyosat kompaniya, mijozlar, hamkorlar va xodimlarning manfaatlarini himoya qiladi, shuningdek, ma’lumotlar sizib chiqishi, suiiste’molchiliklar va nizolar xavfini kamaytiradi. Raqamli huquqlar nuqtai nazaridan, maxfiylikni himoya qilish haddan tashqari nazoratga aylanib qolmasligi va shaxsiy hayot, so‘z erkinligi hamda nizoli vaziyatlarni ko‘rib chiqishning adolatli tartibini buzmasligi muhimdir.

Siyosatda nimalar maxfiy deb hisoblanishi va ma’lumotlarning qanday toifalari mavjudligi aniq tushuntirilishi kerak. Odatda quyidagilar ajratib ko‘rsatiladi:

- shaxsiy ma’lumotlar (mijozlar, xodimlar, nomzodlar);
- tijorat siri va ichki strategik ma’lumotlar;
- texnik ma’lumotlar (dastlabki kod, tizim arxitekturasi, modellar, algoritmlar);
- shartnoma bo‘yicha taqdim etilgan hamkorlar va pudratchilarning materiallari;
- ichki foydalanish uchun cheklangan xizmat hujjatlari.

Amaliy jihatdan axborotni foydalanish darajalari bo‘yicha tasniflashni joriy etish (masalan: ochiq, ichki foydalanish uchun, maxfiy, qat’iy cheklangan) va har bir daraja bo‘yicha misollar keltirish muhimdir. Bu o‘zboshimchalik bilan qaror qabul qilish holatlarini kamaytiradi va xodimlarga kundalik ish faoliyatida qanday harakat qilish lozimligini tushunishga yordam beradi. Raqamli huquqlar nuqtai nazaridan korporativ va shaxsiy ma’lumotlarni aniq ajratish muhim: himoya choralari ish materiallarining xavfsizligini ta’minlashga qaratilishi hamda xodimning shaxsiy ma’lumotlaridan nazoratsiz foydalanishga aylanib qolmasligi kerak.

Siyosat bir vaqtning o‘zida xavfsizlikni mustahkamlaydigan va inson huquqlarini himoya qiladigan asosiy tamoyillarga asoslanishi lozim:

- **foydalanishni minimallashtirish:** axborotdan faqat xizmat vazifalarini bajarish uchun ushbu axborot zarur bo‘lgan shaxslar foydalanish huquqiga ega bo‘lishi lozim;
- **shaffoflik:** xodimlar axborotdan foydalanish, uni saqlash va nazorat qilish qoidalari haqida oldindan xabardor qilinishi lozim;
- **mutanosiblik:** xavfsizlik va monitoring choralari real xavflarga mos bo‘lishi va haddan tashqari bo‘lmasligi lozim;
- **hisobdorlik:** qarorlar qabul qilish, axborotdan foydalanish va nazorat uchun kim javobgar ekanligi (mas’ul shaxslar va bo‘linmalar) aniq belgilanishi lozim;

- **adolatli tartib-taomil:** huquqbuzarlik sodir etilganligi haqida shubha mavjud bo‘lganda, kompaniya holatlarni tekshirish va ko‘rib chiqishning tushunarli tartibiga rioya qilishi hamda o‘zboshimchalik bilan qarorlar qabul qilinishiga yo‘l qo‘ymasligi shart.

Zamonaviy xavflar ommaviy sun’iy intellekt xizmatlari va chat-botlardan foydalanish bilan bog‘liq.

Siyosatda quyidagilar alohida belgilanishi lozim:

- ruxsatsiz va xavflarni baholamasdan ommaviy sun’iy intellekt vositalariga maxfiy ma’lumotlar va shaxsiy ma’lumotlarni kiritishni taqiqlash;
- faqat kompaniya maxfiylik va ma’lumotlarni himoya qilish bo‘yicha shartnomaviy kafolatlarga ega bo‘lgan xizmatlardan foydalanish;
- so‘rovlar va misollarni tayyorlashda axborotni egasizlantirish zarurati.

Ijtimoiy tarmoqlarda izoh qoldirish siyosati- bu kompaniya (yoki tashkilot)ning sahifa ma’murlari va moderatorlar foydalanuvchilarning izohlariga qanday munosabat bildirishi, qanday materiallarga yo‘l qo‘yilishi va qaysi materiallar cheklanishi mumkinligini belgilovchi ichki qoidalaridir. Bunday siyosat raqamli huquqlar nuqtai nazaridan ayniqsa muhimdir, chunki u fikr bildirish erkinligi, axborotdan foydalanish, shaxsga doir ma’lumotlarni himoya qilish hamda moderatsiyaning adolatli tartib-taomiliga daxldor.

Siyosat nima uchun kerakligini aniq ko‘rsatishi kerak. Odatda maqsadlar quyidagilarni o‘z ichiga oladi:

- xavfsiz va o‘zaro hurmatga asoslangan muloqotni ta’minlash;
- nafrat tili va zo‘ravonlikning oldini olish;
- foydalanuvchilarni ta’qib va diskriminatsiyadan himoya qilish;
- qonunchilik va platformalar qoidalariga rioya etish;
- tanqid va jamoatchilik muhokamasi uchun imkoniyatni saqlab qolish.

Moderatsiya nomaqbul fikrlarni bostirish yoki tashkilot faoliyatiga nisbatan bildirilgan tanqidni o‘chirish uchun qo‘llanilmasligi lozimligini alohida ta’kidlash muhim.

Siyosat quyidagi axloqiy standartlarni belgilashi lozim:

- inson qadr-qimmatini kamsituvchi ifodalar, «shok-kontent», stigmatizatsiya orqali hissiyotlarga bosim o‘tkazishga yo‘l qo‘yilmaydi;
- yordam oluvchilarning foto va videolaridan faqat ularning roziligi mavjud bo‘lganda hamda e’lon qilish oqibatlari tushunilgan holda foydalaniladi;
- nogironlik, zo‘ravonlik, kambag‘allik va boshqa ta’sirchan masalalarni yoritishda to‘g‘ri va ehtiyotkor yondashuv qo‘llaniladi;
- auditoriyaning turli tillariga hurmat bilan munosabatda bo‘lish va diskriminatsiyaga yo‘l qo‘ymaydigan ifodalardan foydalanish lozim.

Onlayn yoki ijtimoiy tarmoqlarda xayriya aksiyalarini o‘tkazish siyosati

Onlayn xayriya — bu Internet va ijtimoiy tarmoqlar orqali pul mablag‘lari yoki boshqa resurslarni yig‘ishdir. Bunday kampaniyalar tashkilotga bo‘lgan ishonchni oshiradi, biroq ular noto‘g‘ri tashkil etilganda firibgarlik, donorlar va yordam oluvchilarning huquqlari buzilishi, shuningdek shaxsga doir ma’lumotlarning sizib chiqishi bilan bog‘liq xavflarni yuzaga keltiradi. Siyosat barcha ishtirokchilarning huquqlariga hurmat bilan munosabatda bo‘lish, shaffoflik va xavfsizlikni ta’minlash uchun zarur.

Siyosatda quyidagilar belgilanishi lozim:

- qanday formatlar qo‘llab-quvvatlanishi (xayriya mablag‘lari, kraudfanding, buyumlar yig‘ish, xizmatlar ko‘rsatish uchun resurslar yig‘ish, volontyorlik);
- qanday platformalardan foydalanilishi (rasmiy veb-sayt, ijtimoiy tarmoqlar, to‘lov servislar);
- kampaniyani kim boshlashi mumkinligi (faqat tashkilot yoki vakolatli shaxslar).

Tavsiya etiladigan tamoyillar:

- shaffoflik: aniq maqsad, muddatlar, zarur mablag‘/ehtiyoj, sarflash usuli;
- hisobdorlik: kampaniya yakunlari bo‘yicha hisobot berish, to‘lovlar va xarajatlarni tasdiqlash;
- xavfsizlik: to‘lovlarni himoya qilish, fishing va to‘lov rekvizitlarini almashtirishning oldini olish;
- ma’lumotlarni minimallashtirish: faqat haqiqatda zarur bo‘lgan shaxsga doir ma’lumotlarni yig‘ish;
- qadr-qimmatni hurmat qilish: yordam oluvchilarni kamsitmasdan va shov-shuvsiz axloqiy muloqot qilish.

Kampaniya boshlanishidan oldin quyidagi ma’lumotlarni e’lon qilish tavsiya etiladi:

- tashkilotchi va mas’ul shaxslar;
- mablag‘ yig‘ish maqsadi va yordam ko‘rsatish mezonlari;
- kampaniya muddatlari va uni to‘xtatish mexanizmi (agar belgilangan summa yig‘ilgan bo‘lsa);
- rasmiy to‘lov rekvizitlari/to‘lov tizimiga havolalar;
- hisobot berish tartibi (hisobot qachon va qayerda e’lon qilinishi);
- savollar va shikoyatlar uchun aloqa ma’lumotlari.

Bu suiiste’molliklar xavfini kamaytiradi va auditoriyaning ishonchini oshiradi.

Siyosatda quyidagi himoya choralari mustahkamlab qo‘yilishi lozim:

- faqat rasmiy to‘lov kanallaridan foydalanish;
- agar alohida tartibda nazarda tutilmagan va nazorat qilinmasa, «xodimlarning shaxsiy bank kartalari» rekvizitlarini e’lon qilishni taqiqlash;

- e’lonlar joylashtiriladigan akkauntlarda ikki faktorli autentifikatsiyadan foydalanish;
- to‘lov rekvizitlarini almashtirishga urinish holatlariga munosabat bildirish qoidalarini belgilash;
- obunachilarni keng tarqalgan firibgarlik sxemalari (soxta akkauntlar, o‘xshash havolalar) haqida ogohlantirish.

Donorlar va yordam oluvchilarning shaxsiy ma’lumotlari

Raqamli huquqlar nuqtai nazaridan asosiy yo‘nalish — ma’lumotlar va inson qadr-qimmatini himoya qilish:

- donorlar qanday ma’lumotlar (masalan, ism, tasdiqlash uchun aloqa) va nima uchun to‘planishini tushunishlari kerak;
- donorlar ro‘yxatini faqat rozilik bilan e’lon qilish mumkin (“anonim” opsiyasi mavjud bo‘lishi kerak);
- yordam oluvchilarning (ayniqsa bolalar va zaif guruhlarning) ma’lumotlarini zarurat bo‘lmasa va qonuniy asoslar/rozilik bo‘lmasa oshkor qilish mumkin emas;
- inson uchun xavf tug‘diradigan hujjatlar, tashxislar, manzillar, aniq geolokatsiya va boshqa ma’lumotlarni e’lon qilish taqiqlanadi.

Sezgir holatlar bilan ishlashda ma’lumotlarni shaxssizlantirish usulidan foydalanish maqsadga muvofiq: umumiy tavsiflardan foydalanish, shaxslarning yuzlarini yashirish, shuningdek shaxsni bevosita yoki bilvosita identifikatsiya qilish imkonini beruvchi tafsilotlarni chiqarib tashlash.

Onlayn xayriya kampaniyasining yakuniy hisobotida yig‘ilgan mablag‘lar summasi (yoki ko‘rsatilgan yordam hajmi), asosiy xarajatlar va shaxsga doir ma’lumotlarni himoya qilish talablariga rioya etilgan holda tasdiqlovchi hujjatlar to‘g‘risidagi ma’lumotlar, erishilgan natijaning tavsifi (ortiqcha identifikatsiyaga yo‘l qo‘ymasdan, kimga va qanday yordam ko‘rsatilgani), shuningdek mablag‘lar qoldig‘idan foydalanish bo‘yicha oldindan belgilangan qoida — mablag‘larni keyingi davrga o‘tkazish, qaytarish yoki ulardan boshqa maqsadli yo‘nalishda foydalanish tartibi aks ettirilishi lozim.

3-bo‘lim
Raqamli muhitda yuristlar va advokatlar uchun tahdidlar

3.1. Asosiy tahdidlar

So‘nggi o‘n yillikda raqamli makonning rivojlanishi tufayli fuqarolik jamiyatiga qanday tahdidlar ustunlik qilishi borasida tub o‘zgarishlar yuz bermoqda. Ilgari asosiy e’tibor jismoniy tahdidlarga qaratilgan bo‘lsa, bugungi kunda front chizig‘i virtual bo‘lib, smartfonlarimiz, noutbuklarimiz va bulutli xotiralarimiz orqali o‘tmoqda. Biz “shisha uy” davrida yashayapmiz, bu davrda g‘oyalarni tarqatish va tarafdorlarni jalb qilishga yordam beradigan raqamli shaffoflik va “hamma joyda” bo‘lish bizni bu faoliyatga to‘sqinlik qilmoqchi bo‘lganlar oldida zaif qilib qo‘yadi.

Yuristlar va advokatlar uchun raqamli tahdidlar manzarasini tushunish endilikda shunchaki «ma’lumot uchun» zarur bo‘lgan masala emas. Bugun bu advokatlik sirini, obro‘-e’tiborni va mijozlarning erkinligini saqlab qolish masalasidir. «Mening yashiradigan narsam yo‘q» yoki «men bilan qiziqishlari uchun juda kichik shaxsman» degan tasavvur — o‘ta xavfli yanglish fikrdir. Zamonaviy ommaviy kuzatuv tizimlarida (DPI, yuzni tanib olish, katta ma’lumotlar tahlili) «ahamiyatsiz» nishonlar mavjud emas — har kim kuzatuv obyektiga aylanishi mumkin.

Onlayn tahdidlar bilan oflayn oqibatlar o‘rtasidagi chegaralar yo‘qolganini tushunish juda muhim. Elektron pochtani buzish shunchaki texnik nosozlik emas, balki keng doiradagi shaxslarga ta’sir ko‘rsatadigan uzoq muddatli oqibatlarga ega bo‘lgan muhim xavfsizlik hodisasidir, geolokatsiya metama’lumotlari bilan fotosurat yopiq uchrashuv ishtirokchilariga jismoniy hujumga olib kelishi mumkin, kiberbulling va dezinformatsiya kampaniyalari esa tashkilotlarning charchashi va faoliyatini to‘xtatishiga olib keladigan haqiqiy psixologik jarohatlarni keltirib chiqaradi.

Ko‘plab tashkilotlar raqamli xavfsizlikni antivirus sotib olishdek qabul qilishadi: o‘rnatib qo‘yib, unutib yuborishadi, bunda soxta xavfsizlik hissi paydo bo‘ladi. Biroq haqiqiy himoya mexanizmi boshqacha tuzilgan. U tahdidlar manzarasini (kontekst, tashqi muhit) tushunishni, **hujum vektorlarini** (tahdidlar amalga oshirilishi mumkin bo‘lgan yo‘llarni) bilishni va o‘zining raqamli resurslari hamda ularning zaif tomonlarini aniq tasavvur qilishni talab etadi. Aynan shu bilimlar asosida tashkilotning barqaror **xavfsizlik profili** (security posture) shakllanadi — bu shunday holatki, bunda xavfsizlikni ta’minlash bir martalik harakat emas, balki uzluksiz jarayonga aylanadi.

Biroq, zamonaviy raqamli dunyoda raqamli aktivlarni himoya qilishning texnik komponentlarini sozlashning o‘zi yetarli emas. Hozirgi kunda xavfsizlikka xolistik (yaxlit) yondashuv tobora ommalashib bormoqda, bu esa raqamli, jismoniy va ruhiy-ijtimoiy xavfsizlikning ajralmasligidan kelib chiqadi. Ular yagona ekotizimni tashkil etadi, bu yerda bir sohadagi zaiflik muqarrar ravishda boshqalardagi himoyani buzadi.

Masalan:

Psixologik bosim

(do‘q-po‘pisa, shantaj) xodimning hissiy charchashiga olib keladi

Charchagan xodim

hushyorligini yo‘qotadi va fishing yoki ijtimoiy muhandislikning (raqamli zaiflik) osongina qurboniga aylanadi.

Raqamli resurslarni buzish

orqali nozik shaxsiy ma’lumotlar (jinsiy oriyentatsiya, OIV holati, ...) oshkor etiladi, bu esa benefitsiarlarning jismoniy xavfsizligiga to‘g‘ridan-to‘g‘ri tahdid soladi.

Ma’lumotlarning sizib

chiqishi davlatning huquqiy sanksiyalariga, obro‘siga putur yetishiga, donorlarning ishonchsizligiga 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 gibrid 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; 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, shifrlovchi 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** — ruxsatsiz kirishning barcha turlarini (pochta, ijtimoiy tarmoqlar, messenjerlar, moliyaviy akkauntlarga) birlashtiradi. Bu asosan fishing, ijtimoiy muhandislik usullari va parollarning sizib chiqishi tufayli sodir bo‘ladi. Natija — aloqa kanallari va obro‘ ustidan nazoratni yo‘qotish.

- **Veb-saytlarga hujumlar (DDoS, saytlarni buzish)** — tashkilotning ommaviy resurslariga to‘g‘ridan-to‘g‘ri hujumlar DDoS-hujumlarning maqsadi — zararlangan qurilmalardan so‘rovlar bilan qayta yuklash orqali resursni auditoriya uchun mavjud bo‘lmaydigan qilish. Buzib kirishning maqsadi odatda defes (kontentni almashtirish), ma’lumotlarni o‘g‘irlash yoki zararli kodni joylashtirishdir.

- **Himoyalanmagan tarmoqlarda ma’lumotlarning ushlab qolinishi** — 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 “tashlab qo‘yish” —** 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 zanjiri hujumlari (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. Psixoijtimoiy tahdidlar —

yuristning shaxsiyati, obro‘-e’tibori, psixologik holati va ijtimoiy aloqalariga qaratilgan, uni ruhiy tushkunlikka tushirish va faoliyatini to‘xtatishga majbur qilishni ko‘zlovchi tahdidlar.

- **Muvofiqlashtirilgan onlayn ta’qib va dezinformatsiya kampaniyalari (kiberbulling, troll fabrikalari)** — izohlar, ijtimoiy tarmoqlar va boshqa manbalarda amalga oshiriladigan keng ko‘lamli hujumlar, haqorat, tahdid va yolg‘on axborotni, shu jumladan dipfeyklar yordamida yaratilgan materiallarni tarqatish. Bunday hujumlar, odatda, shaxsning obro‘-e’tiboriga putur yetkazish maqsadida uyushtiriladi.

- **Doksing —** raqamli tahdidni real jismoniy xavfga aylantirish hamda yurist yoki uning mijozlarini qo‘rqitish maqsadida shaxsga doir ma’lumotlarni (manzil, telefon raqamlari, qarindoshlar haqidagi ma’lumotlar) to‘plash va ommaga oshkor qilish.

- **Sekstorshn, pornografik qasos, sekspionaj** (seks josuslik**)** — bu intim xarakterdagi materiallar (haqiqiy yoki sun’iy intellekt yordamida soxtalashtirilgan) orqali shantaj qilish. Bunday tahdid advokatlarning o‘ziga qarshi ham, ularning mijozlarini obro‘sizlantirish maqsadida ham qo‘llaniladi.

3. Huquqiy va tartibga soluvchi tahdidlar —

qonunchilik, davlat institutlari va huquqiy tizimdan bosim o‘tkazish, senzura va ta’qib vositasi sifatida foydalanish bilan bog‘liq tahdidlar.

- **Repressiv qonunchilikni («feyklar», «tuhmat», «ekstremizm» to‘g‘risida) qo‘llash** — qonunlardagi noaniq va keng talqin qilinishi mumkin bo‘lgan formulirovkalardan Internetdagi publikatsiyalar uchun ma’muriy yoki jinoyat ishlarini qo‘zg‘atish maqsadida foydalanish tahdidi.
- **«Xorijiy agentlar/vakillar» to‘g‘risidagi qonunlarni qo‘llash** — mohiyatan huquqiy bo‘lgan, biroq bevosita iqtisodiy, ruhiy-ijtimoiy va operatsion oqibatlarga olib keluvchi gibrid tahdid.
- **Davlat organlari talabi asosida onlayn resurslarni bloklash yoki o‘chirish** — kontentni senzura qilishga qaratilgan suddan tashqari yoki sud qarori natijasida veb-sayt, ijtimoiy tarmoqdagi sahifani bloklash yoxud kontentni o‘chirish tahdidi.
- **Platformalarning huquqiy mexanizmlarini suiiste’mol qilish (DMCA hujumlari)** — platformalarning qonuniy vositalaridan, masalan, mualliflik huquqi buzilganligi yuzasidan shikoyat qilish yoki ijtimoiy tarmoqlar va messenjerlardagi rasmiy kanallar orqali kontent ustidan shikoyat yuborish mexanizmlaridan noqonuniy maqsadlarda (tovlamachilik, senzura) foydalanish.
- **Davlat raqamli nazorati** — TQTT, 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 qilishdan iborat.

- **To‘g‘ridan-to‘g‘ri raqamli firibgarlik va mablag‘larni o‘g‘irlash** — buzish yoki ijtimoiy muhandislik orqali moliyaviy akkauntlarga 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 hujumlar** — klon saytlarni yaratish, xayriya mablag‘larini o‘zlashtirish kabi to‘g‘ridan-to‘g‘ri firibgarlik, shuningdek, mablag‘larni qo‘lga kiritadigan raqobatchi loyihalarni (GONGO) sun’iy ravishda yaratish kabi bilvosita 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 tomonidan cheklanishiga olib kelishi mumkin bo‘lgan “muvofiqlikdan tashqari” tahdid.

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

- **Xodimlarning beixtiyor 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 olib qo‘yilishi** — siz texnika ustidan jismoniy nazoratni yo‘qotadigan (taksida unutib qoldirilgan, o‘g‘irlangan, tintuv paytida musodara qilingan) barcha ssenariylarni birlashtiradi. 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. Fuqarolik 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 chuqur feyklardan 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-qoidalari 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 oshish 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 uskunalarning 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. Yuristlar va advokatlar xavfsizligini ta’minlash 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 himoyalanish imkonsizdek tuyuladi. Shunga qaramay, bu yondashuv konstruktiv emas va ushbu bo‘limda biz ko‘pchilik tashkilotlar va alohida faollar 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 himoyalanmagan. 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 ushlash 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, shifrlovchi 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 funksionallikni 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 akkauntni 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 tarjima yo‘q, lekin quyidagicha aniqlash 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 asosiy gigiyenani shakllantirish — alohida faoliyat yurituvchi advokatlar va kichik jamoalar uchun mo‘ljallangan bo‘lib, uning maqsadi yakka tartibdagi amaliyotlarni umumiy intizom va xavfsizlik madaniyatiga aylantirishdir.

Rejalashtirish va asos yaratish (Due Diligence): ushbu bosqichda operatsion xavfsizlikning poydevori yaratiladi. U yuqorida keltirilgan zarur minimal choralarni, shuningdek bir nechta muhim qo‘shimcha qadamlarni o‘z ichiga oladi.

Imkon qadar faqat litsenziyalangan dasturiy ta’minotdan foydalanishga harakat qilish lozim. Advokatlik amaliyoti uchun standart tijorat mahsulotlari mavjud: Microsoft 365 Business va Google Workspace Business korporativ elektron pochta, bulutli saqlash tizimi va ofis ilovalarini o‘z ichiga olgan barcha zarur vositalar to‘plamini taqdim etadi. NNT tarkibida faoliyat yurituvchi yoki inson huquqlarini himoya qilish bilan shug‘ullanuvchi advokatlar uchun imtiyozli dasturlar, xususan TechSoup orqali, shuningdek Microsoft va Google’ning notijorat tashkilotlar uchun dasturlari mavjud bo‘lishi mumkin.

Diskni to‘liq shifrlashni (full-disk encryption) ta’minlash zarur: Windows uchun — BitLocker, macOS uchun — FileVault. Tiklash kalitlari (recovery keys) ishonchli va xavfsiz joyda (masalan, parollar menejerida) saqlanishi lozim.

Jamoa uchun dastlabki trening o‘tkazish zarur. Unda nafaqat texnik jihatlar, balki fishing va ijtimoiy muhandislikni aniqlash asoslari, shuningdek jismoniy xavfsizlikning asosiy qoidalari ham tushuntirilishi lozim.

Nazoratni kuchaytirish va raqamli izni kamaytirish maqsadida ijtimoiy tarmoqlardagi shaxsiy va umumiy sahifalarning maxfiylik sozlamalarini baholash va tegishli tarzda sozlash zarur.

Jamoa ichida norasmiy qoidalarni ishlab chiqish lozim. Masalan: «barcha ish yozishmalarini faqat Signal orqali olib boramiz» yoki «parollarni Google Docs’da saqlamaymiz». Bu hali xavfsizlik siyosati emas, biroq uni shakllantirish yo‘lidagi dastlabki qadamlardir.

Kundalik amaliyot (Due Care): Bu, birinchi navbatda, barcha qurilmalarda dasturiy ta’minot yangilanishlarini o‘z vaqtida o‘rnatishni anglatadi, chunki bu ma’lum zaifliklardan himoyalanishning asosiy usullaridan biridir. Shuningdek, qurilmalarning jismoniy xavfsizligini ta’minlash amaliyoti — ish joyidan ketayotganda kompyuter ekranini bloklash odatini shakllantirish ham muhimdir. Ommaviy Wi-Fi tarmoqlaridan foydalanishda VPN’dan foydalanish tavsiya etiladi. Bundan tashqari, jamoada tanqidiy fikrlashni muntazam rivojlantirishga rag‘batlantiruvchi o‘zaro hamkorlik muhitini shakllantirish muhim ahamiyatga ega. Shuningdek, advokatlik tuzilmalari faoliyati va advokatlik siriga taalluqli qonunchilikdagi o‘zgarishlar haqidagi yangiliklarni muntazam kuzatib borish zarur.

2-daraja:
Rasmiylashtirilgan tashkiliy jarayonlarni joriy etish — xavfsizlikni ta’minlash bo‘yicha tizimli ishlashga o‘tishga tayyor bo‘lgan advokatlik byurolari, advokatlar hay’atlari va yuridik firmalar uchun mo‘ljallangan.

Rejalashtirish va asos yaratish (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 proaktiv himoya tizimini yaratish — yuqori xavf darajasiga ega muhitda faoliyat yurituvchi tashkilotlar uchun mo‘ljallangan bo‘lib, bunday sharoitda tahdidlarni oldindan ko‘ra bilish va inqiroz holatlarida amalga oshiriladigan harakatlarni rejalashtirish zarur.

Rejalashtirish va asos yaratish (Due Diligence): ushbu bosqichda tashkilot uchun strategik rejalashtirish asosiy ahamiyat kasb etadi. Xavflarni baholash asosiy poydevorga aylanadi va uning asosida hodisalarga javob berishning batafsil rejasi (Incident Response Plan) ishlab chiqilishi lozim. Ushbu reja turli xil hujumlar (akkaunt yoki tizimni buzib kirish, doksing, DDoS-hujumlar) yuz berganda amalga oshiriladigan harakatlarning bosqichma-bosqich ssenariysini belgilaydi. Mazkur reja faoliyatning uzluksizligini ta’minlash rejasi

(Business Continuity Plan) bilan to‘ldiriladi. Unda halokatli ssenariylar ro‘y bergan taqdirda tashkilot o‘z missiyasi va faoliyatini qanday davom ettirishi bayon etiladi. Jismoniy tahdidlar yuzaga kelgan holatlar uchun nafaqat ofisga, balki asosiy xodimlarning yashash joylariga nisbatan ham xavfsizlik protokollari ishlab chiqilishi lozim. Shuningdek, xavfsizlik uchun mas’ul shaxsning rasmiy roli belgilanishi, tashqi ekspertlar (yuristlar, IT-mutaxassislar) bilan aloqa o‘rnatilishi hamda inqiroz holatlari uchun kommunikatsiya rejasi ishlab chiqilishi zarur. Iqtisodiy tahdidlarga qarshi turish maqsadida tashkilot faoliyatini bir necha oy davomida ta’minlash imkonini beruvchi zaxira jamg‘armasini shakllantirish zarur.

Kundalik amaliyot (Due Care): ushbu bosqichda tashkilot hodisalarga shunchaki javob berish bilan cheklanmasligi, balki tahdidlarni oldindan aniqlashi va ularga tayyorlanishi lozim. Buning uchun tahdidlarni erta aniqlash maqsadida tashkilotning raqamli izi va axborot maydoni muntazam monitoring qilinishi zarur. Turli xususiyatdagi hodisalarga javob berish rejasi hamda faoliyatning uzluksizligini ta’minlash rejasini tekshirish va amalda sinab ko‘rish uchun hujumlarning ichki simulyatsiyalari va o‘quv mashqlari muntazam ravishda o‘tkazilishi lozim. Barcha ishlab chiqilgan siyosatlar va rejalar har yili qayta ko‘rib chiqilishi hamda yangi sharoit va o‘zgarib borayotgan tahdidlar muhitiga moslashtirilishi zarur.

3.3. Advokatlik tuzilmalarining veb-saytlari va onlayn resurslarini himoya qilish choralari

Raqamli transformatsiya davrida advokatlik tuzilmalarining veb-saytlari va onlayn platformalari ularning ommaviy ishtiroki va mijozlar bilan muloqotining muhim qismiga aylandi. Bu ularni kiberhujumlar oldida zaif qilib qo‘yadi. Ayniqsa, shov-shuvli ishlar bilan shug‘ullanuvchi advokatlar, inson huquqlari himoyachilari va faollar yoki muxolifat manfaatlarini himoya qiluvchi huquqshunoslar zaif bo‘lib, ular ham jinoyatchilar, ham davlat subyektlari uchun nishon bo‘lishi mumkin.

Onlayn resurslarni, xususan, veb-saytlarni himoya qilishning samarali 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 kompрometatsiya qilinishi (buzib kirish)

Ushbu toifaga begona shaxslar veb-saytingizning «ichki qismi» — uning boshqaruv tizimi, serveri yoki administrator akkauntlariga ruxsatsiz kirish huquqini qo‘lga kiritadigan barcha hodisalar kiradi. Bunday buzib kirishning oqibatlari tajovuzkorning maqsadlariga qarab turlicha bo‘lishi mumkin. Ba’zan bu ommaviy vandalizm (deface) shaklida namoyon bo‘ladi, bunda veb-saytning bosh sahifasiga begona xabar joylashtiriladi. Murakkabroq holatlarda axborot yashirin tarzda almashtiriladi — tashkilotga bo‘lgan ishonchni pasaytirish maqsadida saytdagi raqamlar yoki faktlar sezdirmasdan o‘zgartiriladi. Ko‘pincha asosiy maqsad shaxsga doir, moliyaviy va boshqa ma’lumotlarni o‘g‘irlashdan iborat bo‘ladi. Bundan tashqari, veb-saytingiz spam tarqatish yoki tashrif buyuruvchilarning qurilmalariga zararli dasturlarni yuqtirish uchun foydalaniladigan vositaga aylantirilishi mumkin. Buzib kirish natijasida veb-saytdagi axborotning to‘liq yo‘q qilinishi ham mumkin.

Xizmat ko‘rsatishni rad etishga qaratilgan hujum (DDoS-hujumlar)

Ushbu toifa asosiy maqsadi veb-saytingizni tashrif buyuruvchilar uchun ishlamaydigan holatga keltirish, ya’ni auditoriyaning resursdan foydalanish imkoniyatini amalda cheklashdan iborat bo‘lgan hujumlarni birlashtiradi. Odatda, bu texnik hujum bo‘lib, unda resurs zararlangan qurilmalar tarmog‘idan (botnet) yuboriladigan juda katta hajmdagi foydasiz so‘rovlar oqimi bilan sun’iy ravishda ortiqcha yuklanadi. Natijada veb-sayt bunday yuklamani qayta ishlay olmay qoladi va foydalanuvchilarning so‘rovlariga javob berishni to‘xtatadi. Bunday hujumlar ko‘pincha saylovlar, norozilik namoyishlari yoki jamoatchilikda katta rezonans uyg‘otgan materiallarning e’lon qilinishi kabi muhim voqealar vaqtida auditoriyaning axborot olish imkoniyatini cheklash maqsadida amalga oshiriladi.

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 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 nazorati qo‘lga olinadi 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-resursning kompрometatsiya qilinishiga (buzib kirilishiga) qarshi choralar

Ishonchli hosting-provayder. Hosting-provayderni tanlash onlayn resursingizning xavfsizligi va barqarorligini belgilovchi asosiy qarorlardan biridir. Provayderni baholashda faqat xizmat narxi va uzluksiz ishlash vaqtiga e’tibor qaratish bilan cheklanmasdan, texnik, huquqiy va operatsion omillar majmuini hisobga olish lozim. Texnik ishonchlilik zamonaviy infratuzilmaning mavjudligi, DDoS-hujumlardan majburiy himoya, shuningdek tezkor tiklash imkoniyatiga ega avtomatlashtirilgan kundalik zaxira nusxalash tizimini o‘z ichiga oladi. Huquqiy himoyalanganlik ham kam ahamiyatga ega emas: provayderning yurisdiksiyasi, maxfiylik siyosati va davlat organlarining so‘rovlariga javob berishda mijozlar manfaatlarini himoya qilishga tayyorligini baholash zarur. Maqbul provayder o‘z faoliyatida shaffoflikni namoyon etishi va mijozlar hamda boshqa tashkilotlarning fikr-mulohazalari bilan tasdiqlangan yuqori obro‘-e’tiborga ega bo‘lishi lozim.

Advokatlik tuzilmalari uchun faoliyat yuritilayotgan mamlakatdan tashqaridagi yurisdiksiyada joylashgan, qat'iy maxfiylik siyosatiga ega va ikki faktorli autentifikatsiyani (2FA) qo'llab-quvvatlovchi tijorat xosting-provayderlari maqbul tanlov bo'lishi mumkin. Inson huquqlarini himoya qilish bilan shug'ullanuvchi yoki faollar va fuqarolik jamiyati vakillarining manfaatlarini ifodalovchi advokatlar uchun ixtisoslashtirilgan himoyalangan xosting servislaridan foydalanish imkoniyati mavjud bo'lishi mumkin. Jumladan, VirtualRoad.org (https://www.qurium.org/) va eQualitie (https://deflect.ca/) Deflect xavf guruhidagi tashkilotlarni himoya qilishga qaratilgan xizmatlarni taqdim etadi. Cloudflare'ning Project Galileo (https://www.cloudflare.com/galileo/) loyihasi esa DDoS-hujumlardan bepul himoyani taqdim etadi. Azure (Microsoft) dan foydalanish ham mumkin, biroq uni to'g'ri sozlash uchun texnik mutaxassis talab etiladi.

Sayt boshqaruviga xavfsiz kirishni ta'minlash. Veb-saytingizning ma'muriy panelidan (kontent va sozlamalarni boshqarish uchun), shuningdek xosting boshqaruv panelidan foydalanish huquqlarini imkon qadar yuqori darajada himoya qilish zarur. Mustaqil ravishda amalga oshirish mumkin bo'lgan eng oddiy chora — murakkab, noyob parollardan foydalanish va ikki bosqichli autentifikatsiyani (2FA) majburiy tarzda yoqishdir. Ishonchli xosting-provayderlarda ushbu funksiya, odatda, ro'yxatdan o'tish vaqtidayoq standart sozlama sifatida yoqilgan bo'lishi mumkin. WordPress, Drupal kabi kontentni boshqarish tizimlarida (CMS) esa ikki faktorli autentifikatsiyani ta'minlash uchun uchinchi tomon modullari yoki plaginlaridan foydalanish talab etilishi mumkin. Texnik yordamni talab qilishi mumkin bo'lgan qo'shimcha himoya usullariga ma'muriy paneldan faqat VPN orqali foydalanishni ta'minlash yoki standart kirish manzilini boshqa manzilga o'zgartirish kiradi. Bundan tashqari, parol bir necha marta noto'g'ri kiritilganda foydalanuvchi akkauntini vaqtincha bloklash mexanizmini sozlash mumkin.

Dasturiy ta'minotni o'z vaqtida yangilash. Veb-resurslarga buzib kirish holatlarining katta qismi yangilanmagan dasturiy ta'minot bilan bog'liq. Odatda, bu kontentni boshqarish tizimi (CMS), qo'shimcha modullar (plaginlar) va veb-sayt yaratilgan dasturiy platformaga taalluqlidir. Ko'pincha veb-sayt ishlab chiquvchilari o'z vazifalariga yetarlicha mas'uliyat bilan yondashmaydi va xavfsizlik masalalariga zarur e'tibor qaratmaydi. Natijada mijoz yangilanmaydigan yoki zaif mavzular va plaginlarga ega veb-saytni, «qo'lda yozilgan» tizimlar holatida esa jiddiy zaifliklarga ega va texnik jihatdan qo'llab-quvvatlanmaydigan tizimni olishi mumkin. 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 — hodisalardan, jumladan veb-resursga buzib kirish holatlaridan keyin tizimni tez va to'liq tiklashning asosiy vositasidir. Hatto eng yaxshi himoya ham yetarli bo'lmasligi mumkin, masalan, platforma ishlab chiquvchilari hali bexabar bo'lgan zero-day (nolinchi kun zaifliklari) mavjud bo'lgan hollarda. Bunday zaifliklardan hatto to'liq yangilangan tizimlarda ham foydalanish mumkin. Bunday holda, zararli kodning mavjudligini istisno qilish uchun eng yaxshi tiklash usuli zaxira nusxasidan tiklash bo'ladi. Agar buzib kirilgan vaqt aniq bo'lmasa, tizimni avvalroq yaratilgan nusxadan tiklashga to'g'ri kelishi mumkin. Hosting — provayderingiz muntazam ravishda nusxalashini va ularning versiyalarini saqlab turishini tekshiring. 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-hujumlarga 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 himoyalanish 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 xabarlarni 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 tekshirish va tahdidlarga javob berish

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

Raqamli xavfsizlik bo‘yicha mutaxassislarga kechiktirmasdan tashqi ekspert yordami uchun murojaat qilish zarur. Inson huquqlarini himoya qilish bilan shug‘ullanuvchi yoki faollar va fuqarolik jamiyati vakillarini ifodalovchi advokatlar uchun Access Now Digital Security Helpline (help@accessnow.org, https://www.accessnow.org/) yordamidan foydalanish mumkin — bu tashkilot xavf ostidagi guruhlarni qo‘llab-quvvatlash va platformalar bilan hamkorlik qilishga ixtisoslashgan. Tijorat asosida faoliyat yurituvchi advokatlik amaliyotlari esa hodisa yuz bergan taqdirda tezkor yordam ko‘rsatishi mumkin bo‘lgan professional IT-hamkor yoki MSSP (Managed Security Service Provider) Boshqariladigan xavfsizlik xizmati provayderi bilan oldindan shartnoma tuzib qo‘yishlari tavsiya etiladi.

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. Zararkunanda tizimga qanday qilib kirganini tushunish ushbu zaiflikni bartaraf etishning kalitidir. Shu bilan birga, zarar baholanadi: 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 advokatlar uchun ham munozarali hisoblanadi. Bir tomondan, rasmiy ariza voqea sodir bo‘lganligini tasdiqlaydi, bu esa o‘g‘irlangan ma’lumotlar yoki buzilgan resurs sizning nomingizdan noqonuniy faoliyat uchun ishlatilsa, huquqiy himoyaga xizmat qilishi mumkin. Boshqa tomondan, tergov doirasida huquqni muhofaza qiluvchi organlar sizning faoliyatingiz, mijozlaringiz va himoya strategiyangiz haqidagi maxfiy ma’lumotlarga qonuniy ravishda kirish imkoniga ega bo‘lib, barcha texnik vositalaringizni olib qo‘yishi mumkin bo‘lgan “jabrlanuvchini gumonlanuvchiga aylantirish” xavfi ham mavjud. Bu qaror faqat xavflarni sinchkovlik bilan baholash, mamlakatdagi siyosiy vaziyatni, huquqiy tizimga ishonch darajasini va oshkor etilishi mumkin bo‘lgan ma’lumotlarning sezgirligini hisobga olgan holda qabul qilinishi kerak. Huquqni muhofaza qiluvchi organlar bilan har qanday aloqa qilishdan oldin ishonchli hamkasbingiz yoki Advokatlar palatasining advokatidan maslahat olish — oltin qoidadir.

Xulosa

Raqamli muhit huquqshunoslar va advokatlar 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 xatarlarni boshqarishga bo‘lgan talablarni kuchaytiradi.

Ushbu qo‘llanmada ko‘rsatilganidek, raqamli huquqlar mavhum kategoriya emas, balki advokatning kundalik ishiga bevosita ta’sir ko‘rsatadigan amaliy vositadir. Kirish imkoniyati Mijozlarning shaxsiy ma’lumotlarini himoya qilish, raqamli muhitda advokatlik sirini saqlash, davlat organlari va onlayn platformalar bilan hamkorlik qilish — 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. Advokatlar bir vaqtning o‘zida milliy qonunchilik, advokaturaning kasbiy standartlari va raqamli platformalar qoidalari amal qiladigan muhitda faoliyat yuritadilar. 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. Mijozlar haqidagi nozik ma’lumotlar bilan ishlash, ishlarni yuritish, ishonchli vakillar va hamkorlar bilan o‘zaro aloqa o‘rnatish — bularning barchasi amaliyotning o‘ziga ham, uning ishonchli vakillariga ham ta’sir qilishi mumkin bo‘lgan potentsial tahdidlar bilan bog‘liq. Bunday sharoitda ma’lumotlarni himoya qilish, advokatlik sirini saqlash va aloqalarning 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 aniq sharoitlarda qaror qabul qilish vositalarini taklif etishdan iborat.

Bugungi kunda advokatning 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.

Ilovalar

1-ilova

O‘zbekiston Respublikasining shaxsga doir ma’lumotlar to‘g‘risidagi qonunchiligining asosiy talablarini bajarish bo‘yicha nazorat ro‘yxati

Manba: https://www.itts.uz/

	Talab	Korxonada talab qanday amalga oshirilgan? Oddiyroq — Bor/Yo‘q yoki +/- Yaxshiroq — mas’ul shaxslar ismlari, buyruq raqamlari, hujjat nomlari va boshqalarni ko‘rsatish	Manba normativ-huquqiy hujjat	URL, NHH bandiga havola
1	Korxonada shaxsga doir ma’lumotlarni qayta ishlash uchun huquqiy asoslar belgilanganmi? Qanday asoslar? (yozma rozilik, shartnoma ijrosi, NHH talablari)		O‘zbekiston Respublikasining « Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 18-modda	https://lex.uz/docs/4396428#4398418
2	Shaxsiy ma’lumotlarni qayta ishlashga rozilikning namunaviy shakllari ishlab chiqilganmi?			
3	Shartnomalarning namunaviy shakllariga shaxsga doir ma’lumotlarni qayta ishlash to‘g‘risidagi bandlar kiritilganmi?			
4	Subyekt bilan tuzilgan shartnoma muddati tugaganidan keyin shaxsiy ma’lumotlar qayta ishlanadimi? Ha bo‘lsa, qanday asosda?			
5	Shaxsiy ma’lumotlarni qayta ishlashga rozilik shakli qonunchilik talablariga javob beradimi, unga barcha majburiy maydonlar kiritilganmi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘i, 11-band	https://lex.uz/docs/6663967#6664336

6	Barcha tegishli shaxsiy ma’lumotlar bazalari davlat reyestrida ro‘yxatdan o‘tkazilganmi?		O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 31-modda	https://lex.uz/docs/4396428#4398788
7	Shaxsiy ma’lumotlarni qayta ishlashga subyektning roziligi qanday qayd etiladi? Rozilik berilgan sana/vaqt/qurilma identifikatori/IP-manzil saqlanadimi?		O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni, 21-modda	https://lex.uz/docs/4396428#4398514
8	Rozilik berilgan shaklda uni qaytarib olish imkoniyati mavjudmi? Rozilikni qaytarib olishni elektron hujjat shaklida yuborish imkoniyati bormi?			
9	Vafot etgan subyektlarning shaxsiy ma’lumotlari qayta ishlanadimi? Bunday qayta ishlashga kim rozilik bergan? (hayotligida berilgan rozilik, qonuniy merosxo‘rlar roziligi)			
10	Subyektlarning so‘rovlari bo‘yicha shaxsiy ma’lumotlarga ishlov berish to‘g‘risidagi ma’lumotlarni qaysi bo‘linma taqdim etadi?		O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 22-modda	https://lex.uz/docs/4396428#4398536
11	Shaxsga doir ma’lumotlar subyektining murojaati asosida shaxsga doir ma’lumotlarni bloklash va yo‘q qilish tartibi belgilanganmi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘ining 30.13-bandi	https://lex.uz/docs/6663967#6664487
12	Shaxsga doir ma’lumotlarga bir-biriga mos kelmaydigan maqsadlarda ishlov berilayotgan bo‘lsa, ma’lumotlar bazalari ajratilganmi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘ining 5-bandi	https://lex.uz/docs/6663967#6664304
13	Subyekt uning shaxsiy ma’lumotlari shaxsiy ma’lumotlar bazasiga kiritilgani to‘g‘risida qanday xabardor qilinadi?		O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 23-modda	https://lex.uz/docs/4396428#4398628
14	Subyektning shaxsiy ma’lumotlari uchinchi shaxslarga berilganda u qanday xabardor qilinadi?			

15	Uchinchi shaxslar ro‘yxati shakllantirilganmi? Uni kim va qanday qilib dolzarblashtiradi?		
16	Korxonada shaxsiy ma’lumotlarga to‘liq avtomatlashtirilgan ishlov berish, masalan, skoring amalga oshiriladimi?	O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 24-modda	https://lex.uz/docs/4396428#4398652
17	Subyektning shaxsiy ma’lumotlarini to‘liq avtomatlashtirilgan holda qayta ishlashga roziligini qanday olish mumkin? Bunday qayta ishlashning huquqiy asosi qanday?		
18	Maxsus shaxsiy ma’lumotlar (sog‘lig‘i, oila tarkibi, millati haqidagi ma’lumotlar) qayta ishlanadimi?* *Maxsus shaxsiy ma’lumotlarga ishlov berish taqiqlanadi, cheklangan holatlar bundan mustasno.	O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 25-modda	https://lex.uz/docs/4396428#4398682
19	Korxonada biometrik shaxsiy ma’lumotlar (fotosuratlar, barmoq izlari va boshqalar) qayta ishlanadimi?	O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni, 26-modda	https://lex.uz/docs/4396428#4398727
20	Bunday ishlov berishning huquqiy asoslari qanday? Subyekt/xodim bunday ishlov berishga rozilik berganmi?		
21	Korxonada biometrik KNBT mavjudmi? Uning ma’lumotlar bazasi shaxsiy ma’lumotlar bazalari davlat reestrida ro‘yxatdan o‘tkazilganmi? KNBT bazasiga kiritilgan barcha shaxslarning yozma roziligi olinganmi?		
22	Biometrik/genetik ma’lumotlarni o‘z ichiga olgan moddiy manbalarni hisobga olish qanday amalga oshiriladi?	5.10.2022-yildagi 570-son VMQga 2-ilovaning 5-bandi	https://lex.uz/ru/docs/6225462#6227477
23	Biometrik ma’lumotlarni shifrlash va kriptografik himoyalash talabi qanday amalga oshirilgan?	5.10.2022-yildagi 570-son VMQga 2-ilovaning 4-bandi	https://lex.uz/ru/docs/6225462#6227475

24	Biometrik ma’lumotlar tashuvchilarga grif qo‘yilganmi? Tashuvchilarning jismoniy xavfsizligini ta’minlash uchun qanday aniq majburiy choralar qo‘llaniladi? Biometrik ma’lumotlarga kirish huquqiga ega bo‘lgan qurilmalarning IP va MAC manzillari qayd etiladimi?		05.10.2022-yildagi 570-son VMQga 2-ilovaning 2-bobi.	https://lex.uz/ru/docs/6225462#6227469
25	O‘zbekiston fuqarolarining shaxsga doir ma’lumotlariga (ShDMa) qayerda va qanday ishlov beriladi? Ishlov beriladigan uskunalar jismonan qayerda joylashgan?		O‘zbekiston Respublikasining “ Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni, 271-modda	https://lex.uz/docs/4396428#5271076
26	Shaxsiy ma’lumotlarning boshqa davlatlarga uzatiladimi? (transchegaraviy uzatish) Qaysi mamlakatlar hududiga?		O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 15-modda	https://lex.uz/docs/4396428#4398348
27	Korxona vazifalarini bajarish uchun zarur va yetarli bo‘lgan shaxsiy ma’lumotlarning tasdiqlangan tarkibi?		O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 31-modda	https://lex.uz/docs/4396428#4398788
28	Shaxsiy ma’lumotlarni qayta ishlash va himoya qilish bilan bog‘liq ishlar uchun mas’ul bo‘lgan tarkibiy bo‘linma yoki mansabdor shaxs belgilanganmi?			
29	Shaxsga doir ma’lumotlarga ishlov berish muddatlari belgilanganmi (har bir toifa, har bir baza bo‘yicha)? Bu muddatlar qanday?		O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 10 va 19-moddalar	https://lex.uz/docs/4396428#4398106
30	Korxonada shaxsiy ma’lumotlar bilan tarixiy, statistik, sotsiologik yoki ilmiy tadqiqotlar o‘tkaziladimi? Bunda ushbu shaxsiy ma’lumotlar majburiy ravishda shaxssizlashtiriladimi?		O‘zbekiston Respublikasining «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonuni, 16-modda	https://lex.uz/docs/4396428#4398378
31	Shaxsiy ma’lumotlar yo‘q qilinadimi? Kim, qanday? Buni qaysi hujjat tartibga soladi?		O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 17-modda	https://lex.uz/docs/4396428#4398388

32	Har bir shaxsiy ma’lumotlar bazasi uchun dolzarb bo‘lgan tahdid turlari aniqlanganmi? Har bir bazaga himoya darajalari belgilanganmi?		5.10.2022-yildagi 570-son VMQning 2-bandi	https://lex.uz/uz/docs/6225462#6227189
33	Shaxsiy ma’lumotlar bazalarining har biri uchun ularga berilgan himoya darajasi asosida axborot xavfsizligi talablari bajarilayaptimi? Muayyan bazaga qanday aniq choralar qo‘llaniladi?		O‘zbekiston Respublikasi VM2022-yil 5-oktyabrdagi 570-son qarori, 10-bob	https://lex.uz/uz/docs/6225462#6227279
34	Shaxsiy ma’lumotlar himoyasini ta’minlash uchun mas’ul bo‘linma bevosita korxona rahbariga bo‘ysunadimi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3477-son buyrug‘I, 3-band	https://lex.uz/docs/6663969#6668986
35	Shaxsiy ma’lumotlar bazasi vaqti-vaqti bilan tekshirib turiladimi? Ro‘yxatga olish ma’lumotlarining dolzarbligi oxirgi marta qachon tekshirilgan?		Adliya vazirligining 2023-yil 15-noyabrdagi 3477-sonli buyrug‘I, 8-band	https://lex.uz/docs/6663969#6669029
36	Korxonaning shaxsga doir ma’lumotlar bazalari bilan ishlash huquqiga ega bo‘lgan xodimlari ro‘yxati shakllantirilganmi?			
37	Shaxsiy ma’lumotlar bilan ishlovchilar (jurnalistlar, IT, kadrlar, huquqshunoslar) uchun seminarlar yoki treninglar o‘tkaziladimi?			
38	Ruxsatsiz kirish natijasida yo‘q qilingan yoki shikastlangan shaxsiy ma’lumotlarni tiklash imkoniyati ta’minlanganmi?			
39	Agar shaxsiy ma’lumotlarga ishlov berish oferta asosida amalga oshirilayotgan bo‘lsa, unda ishlov berishning aniq maqsadlari ko‘rsatilganmi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘I, 9-band	https://lex.uz/docs/6663967#6664327
40	Korxonada videokuzatuv amalga oshiriladimi? Nima maqsadda? Qanday shaxsiy ma’lumotlar qayta ishlanadi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘I, 12-band	https://lex.uz/docs/6663967#6664354
41	Shaxsiy ma’lumotlarni qayta ishlash va himoya qilish bo‘yicha mulkdor/operator siyosatini belgilovchi ichki hujjatlar tasdiqlanganmi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘I, 30.12-bandi	https://lex.uz/docs/6663967#6664485

42	Kadrlar ishini yuritishda xodimning shaxsiy ma’lumotlarini himoya qilish bo‘yicha O‘zbekiston Respublikasining yangi Mehnat kodeksi talablari inobatga olinadimi? Kadrlar xizmati xodimlari shaxsiy ma’lumotlar sohasida minimal malakaga egami?		6-§. O‘zbekiston Respublikasi Mehnat kodeksining xodimning shaxsiy ma’lumotlarini himoya qilish	https://lex.uz/ru/docs/6257291#6262031
43	Agar xodimning shaxsiy ma’lumotlari uchinchi shaxslardan olinayotgan bo‘lsa (sudlanganlik, dispanserlarda hisobda turish), xodim bu haqda oldindan yozma ravishda xabardor qilinadimi va undan yozma rozilik olinganmi?		O‘zbekiston Respublikasi Mehnat kodeksi, 176-modda	https://lex.uz/ru/docs/6257291#6262106
44	Xodim ish beruvchida saqlanayotgan barcha shaxsiy ma’lumotlaridan to‘liq foydalana oladimi? Ulardan nusxa ko‘chirishi mumkinmi?		O‘zbekiston Respublikasi Mehnat kodeksi, 179-modda	https://lex.uz/ru/docs/6257291#6262129
45	*Rozilik shakllari va takliflarda «dark patterns» mavjud emas: - ishlov berishga rozilik belgisi va bayroqchalar shaxsiy ma’lumotlar avtomatik tarzda kiritilmagan bo‘lsa; - shartlarga rozilik tugmasi faqat subyekt taklif etilayotgan shartnoma (oferta) ning barcha sahifalarini to‘liq ko‘rib chiqqandan so‘ng bosilishi mumkin; - belgilar qo‘yish va shartlar bilan tasdiqlash tugmasini bosish fakti sana, vaqt, IP-manzil va mijoz identifikatorini ko‘rsatgan holda qayd etilishi shart * talablar faqat tijorat banklariga taalluqli		O‘zR MBning 2018-yil 2-iyuldagi 3030-sonli Qarori, 28-bandi	https://lex.uz/docs/3804290#3805017
46	Axborot xavfsizligini boshqarish tizimiga (AXBT) shaxsiy ma’lumotlarni himoya qilish joriy etilganmi?		Adliya vazirligining 2023-yil 15-noyabrdagi 3478-sonli buyrug‘ining 31-bandi A.5.34 ISO/IEC 27001:2022 A.18.1.4 O‘z DSt ISO/IEC 27001:2020	https://lex.uz/docs/6663967#6664488 https://stt2.unicon.uz/#/post/772

2-ilova

Shaxsiy ma’lumotlarga ishlov berish tartib-taomillarining universal nazorat ro‘yxati

A. Shaxsiy ma’lumotlarni qayta ishlash jarayonlari va shaxsiy ma’lumotlar bazalari reestri
   - Shaxsiy ma’lumotlarni qayta ishlash jarayonlari reestri tuzildi (maqsadlar, asoslar, subyektlar toifalari, ma’lumotlar tarkibi, qabul qiluvchilar, saqlash muddatlari).
   - Shaxsiy ma’lumotlar bazalari reestri tuzildi.
   - Shaxsiy ma’lumotlar bazalari ro‘yxatga olindi.
   - Har bir jarayonning egasi tayinlandi.
   - Tahdidlar baholandi va baholash dalolatnomasi tuzildi
   - Shaxsiy ma’lumotlarni qayta ishlash siyosati tasdiqlandi

B. Shaxsiy ma’lumotlarni yig‘ish va xabardor qilish tartibi
   - Har bir yig‘ish kanali uchun maqsadlar va asoslar belgilangan.
   - Bazaga kiritilganda subyektga xabar berish matni tayyorlandi.
   - Shakllar/skriptlar (sayt, so‘rovnomalar, shartnomalar, HR shakllari) sozlangan.
   - Ortiqcha maydonlar chiqarib tashlandi (“har ehtimolga qarshi” asos hisoblanmaydi).

C. Rozilik berish tartibi
   - Rozilik olinganlik faktini tasdiqlash imkonini beradigan shaklda qayd etiladi.
   - Maxsus ma’lumotlar uchun — yozma rozilik (shu jumladan elektron hujjat).
   - Rozilik isboti (log, imzolangan hujjat, yozuvli chek-boks) saqlanadi.
   - Fikr-mulohaza o‘sha shaklda yoki yozma ravishda (shu jumladan elektron shaklda) qabul qilinadi.

D. Kirish va ichki foydalanish tartibi
   - Kirish matritsasi (role-based) kiritildi.
   - Foydalanish huquqi talabnoma bo‘yicha va zaruriyat prinsipiga ko‘ra beriladi.
   - Kirish va operatsiyalar jurnallari yuritiladi.
   - Nusxalash, tushirish, olinadigan tashuvchilar tartibga solingan.
   - Olinadigan tashuvchilarni saqlash joylari reglamentlangan.

E. Ma’lumotlarni o‘zgartirish tartibi va sifati
   - Tasdiqlovchi hujjatlar bo‘yicha ma’lumotlarni tuzatish/aniqlashtirish uchun kanal mavjud.
   - Agar tuzatish imkoni bo‘lmasa, yo‘q qilish ko‘zda tutilgan.
   - Muhim ma’lumotlarni (aloqalar, hujjatlar) yangilash muddatlari belgilandi.

F. Shaxsiy ma’lumotlar subyektlarining so‘rovlari bilan ishlash tartibi
   - Shaxsiy ma’lumotlar subyektiga ularning ma’lumotlariga ishlov berish to‘g‘risida taqdim etiladigan axborot tarkibi tavsiflangan.
   - Ariza beruvchini identifikatsiya qilish yolga qo‘yilgan.
   - Hujjatlarni to‘xtatib turish/yo‘q qilish uchun elektron shaklda yuborish imkoniyati ta’minlangan.

- Shaxsiy ma’lumotlar so‘rovlariga javob berishning ichki muddatlari va shablonlari belgilangan.

G. Uchinchi shaxslarga berish tartibi
   - Berishga faqat asos mavjud bo‘lgandagina yo‘l qo‘yiladi (shu jumladan rozilik/shartnoma/qonun).
   - Himoya va maxfiylik majburiyatlari bilan shartnoma tuzilgan.
   - Subyekt, agar istisno bo‘lmasa, uchinchi shaxsga berilganligi to‘g‘risida 3 kun ichida xabardor qilinadi.
   - Uchinchi shaxslar va beriladigan shaxsiy ma’lumotlar toifalari reyestri yuritiladi.

H. Tarqatish (e’lon qilish) tartibi
   - E’lon qilingan maqsadlardan tashqari har qanday tarqatish faqat subyektning roziligi bilan amalga oshiriladi. ([LEX.UZ][1])
   - Sayt, ijtimoiy tarmoqlar, keyslar, foto/video, sharhlar uchun alohida qoidalar.
   - Ma’lumotlarning “ommaviyligi” va kirish asoslarini tekshirish.

I. Transchegaraviy uzatish tartibi
   - Mamlakat aniqlanadi va “yetarlicha himoya” baholanadi (qonunchilikning mavjudligi, maxfiylik to‘g‘risidagi shartnoma, ichki siyosat, texnik himoya choralari)
   - “Noadekvat” mamlakatlar uchun asos (masalan, rozilik) qayd etiladi.
   - Transchegaraviy o‘tkazmalar reyestri yuritiladi (tizim, provayder, sana, asos).
   - Transchegaraviy o‘tkazish to‘g‘risida regulyatorni xabardor qilish tartibi

J. Mahalliylashtirish va ro‘yxatdan o‘tkazish (O‘zR fuqarolari ma’lumotlari uchun)
   - O‘zbekiston Respublikasida texnik vositalarda yig‘ish/tizimlash/saqlash ta’minlangan.
   - Ma’lumotlar bazasi davlat reyestrida ro‘yxatga olingan.
   - Bulutli xizmatlar, zaxiralash va tashqi xizmatlarni boshqarish.

K. Saqlash, o‘chirish va yo‘q qilish tartibi
   - Qayta ishlash maqsadlariga ko‘ra saqlash muddatlari belgilangan.
   - Yo‘q qilish asoslari: maqsadga erishilgan, rozilik qaytarib olingan, qayta ishlash muddati tugagan, sud qarori.
   - Yo‘q qilish dalolatnoma bilan rasmiylashtiriladi.
   - Nusxalar va zaxiralarning reglament bo‘yicha o‘chirilishi tekshiriladi.

L. Insidentlarga (ma’lumotlarning sizib chiqishi/buzilishlarga) javob qaytarish tartibi
   - Hodisalar toifalari va javob berish guruhi aniqlandi.
   - Qayta ishlash shartlari buzilganligi to‘g‘risida ma’lumot mavjud bo‘lgan taqdirda, qayta ishlashni to‘xtatib turish yoki yo‘q qilish nazarda tutilgan.
   - Ta’minlangan: lokalizatsiya, hodisalarni tekshirish, sabablarini bartaraf etish, hujjatlashtirish.
   - Bildirishnoma shablonlari va aloqa protokoli kiritildi.

https://lex.uz/docs/4396428 «Shaxsga doir ma’lumotlar to‘g‘risida»gi O‘RQ-547-sonli Qonuni, 02.07.2019

3-ilova

Shaxsiy ma’lumotlarga ishlov berish va ularni himoya qilish siyosatining tuzilmasi

1. Umumiy qoidalar
   1.1. Siyosatning maqsadi.
   1.2. Qo‘llanish sohasi (xodimlar, nomzodlar, mijozlar, kontragentlar, kontragentlar vakillari).
   1.3. Atamalar va ta’riflar (subyekt, operator/mulkdor, uchinchi shaxs, Shaxsiy ma’lumotlar bazasi, tarqatish, transchegaraviy uzatish).
   1.4. Ishlov berish tamoyillari.

2. Rollar va mas’uliyat
   2.1. Mulkdor va (yoki) operator.
   2.2. Shaxsiy ma’lumotlar bo‘yicha mas’ul bo‘linma/mansabdor shaxs (vazifasi va funksiyalari).
   2.3. Foydalanuvchilar va jarayonlar egalarining vakolatlari.

3. Qayta ishlashning huquqiy asoslari va maqsadlari
   3.1. Qayta ishlash shartlari (asoslari) (rozilik, shartnoma, qonun, qonuniy manfaatlar, ijtimoiy ahamiyatga ega maqsadlar, egasizlantirilganda o‘tkaziladigan tadqiqotlar, hamma foydalanishi mumkin bo‘lgan manbalar).
   3.2. Ichki hujjatlarda ishlov berish maqsadlarini belgilash va ularning yig‘ishda ilgari e’lon qilingan maqsadlarga muvofiqligi.

4. Ma’lumotlar toifalari va subyektlar
   4.1. Subyektlarning toifalari.
   4.2. Ma’lumotlar toifalari (oddiy, maxsus; mavjud bo‘lsa — biometrik/genetik).
   4.3. Ma’lumotlar tarkibini minimallashtirish (zarurligi va yetarliligi).

5. Ishlov berishning hayotiy davri
   5.1. Yig‘ish, tizimlashtirish, saqlash.
   5.2. Foydalanish.
   5.3. Kompaniya ichida taqdim etish va foydalanish.
   5.4. Uchinchi shaxslarga berish.
   5.5. Tarqatish (nashr, sayt, OAV).
   5.6. Transchegaraviy uzatish.
   5.7. Egasizlantirish (agar qo‘llanilsa).
   5.8. Yo‘q qilish (olib tashlash).

6. Rozilik va roziliklarni boshqarish
   6.1. Rozilik shakli va uning olinganligini isbotlash.
   6.2. Maxsus ma’lumotlarga uchun rozilik (yozma shaklda, shu jumladan elektron hujjat shaklida).
   6.3. Rozilikni qaytarib olish va uni qayd etish.

7. Subyektlarning huquqlari va ularni amalga oshirish tartibi
    7.1. Qayta ishlash haqida ma’lumot olish huquqi va taqdim etiladigan ma’lumot tarkibi.
    7.2. Ma’lumotlarning sifati/qonuniyligi/zaruriyati bilan bog‘liq muammolar yuzaga kelganda, ularni qayta ishlashni vaqtincha to‘xtatib turishni talab qilish huquqi.
    7.3. So‘rovlarni yuborish kanallari va ichki ko‘rib chiqish muddatlari (ichki SLA).
    7.4. Ariza beruvchini identifikasiya qilish.
8. Subyektlarni xabardor qilish
    8.1. Ma’lumotlarni bazaga kiritishda xabardor qilish (maqsadlar va huquqlar).
    8.2. Ma’lumotlarni uchinchi shaxsga uzatishda xabardor qilish (3 kun, istisnolar).
9. Maxfiylik va ochiq ma’lumotlar
    9.1. Maxfiylik rejimi.
    9.2. Hamma foydalanishi mumkin bo‘lgan shaxsiy ma’lumotlar va ular bilan ishlash qoidalari.
10. Bazalarni mahalliylashtirish va ro‘yxatdan o‘tkazish
    10.1. O‘zbekiston Respublikasi fuqarolari ma’lumotlarini AT/Internetdan foydalangan holda qayta ishlash shartlari (mahalliylashtirish + davlat reyestrida ro‘yxatdan o‘tkazish).
    10.2. Bazalarni ro‘yxatga olish va ro‘yxatga olish uchun ma’lumotlar o‘zgarganligi to‘g‘risida xabardor qilish.
11. Himoya choralari
    11.1. Huquqiy, tashkiliy va texnik choralar.
    11.2. Foydalanishni boshqarish, hisob qaydnomalari, jurnallar, tashuvchilar, xonalar.
    11.3. Pudratchilar va uchinchi shaxslar nazorati.
12. Amaliy ma’noda o‘chirish, yo‘q qilish va “unutilish huquqi”
    12.1. Yo‘q qilish/o‘chirish asoslari asoslari (maqsadga erishilganligi, rozilikni qaytarib olish, muddatning tugashi, sud qarori).
    12.2. Cheklash/to‘xtatish talablarini qayta ishlash.
    12.3. Yo‘q qilishni hujjatlashtirish (dalolatnomalar, loglar).
13. Hodisalar va sizib chiqishlarga munosabat bildirish
    13.1. Ma’lumotlarni qayta ishlash shartlari buzilganligi haqida ma’lumot mavjud bo‘lganda, ularni qayta ishlashni to‘xtatish yoki yo‘q qilish majburiyati.
    13.2. Tekshirish, lokalizatsiya, tuzatish va hisobot berish tartibi.
14. Transchegaraviy uzatish
    14.1. “Muvofiq himoya” mezonlari.
    14.2. “Nomuvofiq” mamlakatlarga o‘tkazish va ruxsat etilgan asoslar (shu jumladan rozilik).
    14.3. Transchegaraviy uzatishlar reyestri va oqimlar nazorati.
15. Yakuniy qoidalar
    15.1. Xodimlarni o‘qitish va javobgarlik.
    15.2. Siyosatni audit qilish va qayta ko‘rib chiqish.
    15.3. Mas’ul shaxs kontaktlari.

ZAMONAVIY
JURNALISTIKANI
RIVOJLANTIRISH
MARKAZI