Mehriban Zeynalova

İNSAN ALVERİNƏ QARŞI MÜBARİZƏDƏ RƏQƏMSAL MONİTORİNQ ÜÇÜN

TƏLİMAT

BAKI - 2025

Elmi redaktor: f.ü.f.d., dosent **Mətləb Mahmudov**

Rəyçilər:

f.ü.f.d., **Zeynəddin Şabanov** - Əmək və sosial münasibətlər akademiyasının dosenti

f.ü.f.d., **Həbib Hüseynov** – AMEA Fəlsəfə və Sosilologiya İnstitutunun dosenti

Müəllif: MEHRİBAN ZEYNALOVA – fəlsəfə üzrə fəlsəfə doktoru, "Təmiz Dünya" Qadınlara Yardım ictiami Birliyinin sədri, İnsan alverinə qarşı mübarizə üzrə QHT Koalsiyasının sədri.

Metodiki vəsait. İnsan alverinə qarşı mübarizədə rəqəmsal monitorinq üçün Təlimat.). Bakı, "OPTİMİST"MMC-2025. 178 səh.

Bu vəsaitdə qarşıya qoyulan vəzifələr Azərbaycanın insan alverinə qarşı mübarizə sahəsində formalaşmış müsbət təcrübəsini qorumaqla yanaşı, rəqəmsal dövrün çağırışlarına çevik cavab verən yeni standartların tətbiqinə xidmət edir. Rəqəmsal aləmdə cinayətkar davranış formalarının artması fonunda bu təlimat həm praktik fəaliyyət aləti, həm də strateji sənədi kimi mühüm əhəmiyyət daşıyır.

Təqdim olunan bu təlimat ilk növbədə sosial işçilər, psixoloqlar, hüquq-mühafizə orqanlarının əməkdaşları, QHT nümayəndələri və jurnalistlər üçün nəzərdə tutulub.

ISBN 9 7 8 - 9 9 5 2 - 5 6 1 - 6 5 - 4

MÜNDƏRİCAT

1.Giriş

İlk növbədə qeyd etmək lazimdir ki, insan alveri müasir dövrdə qlobal miqyasda ən mürəkkəb və gizli istismar forması olaraq mühüm problemlərdən biridir. Rəqəmsal texnologiyaların sürətli inkişafı bu cinayət növünə yeni dinamika gətirmiş, onun ənənəvi formalarından fərqli olaraq onlayn mühitdə rekrutmentlik (burada işə düzəlmə adıyla qurbanların cəlb edilməsi), təhrif edilmiş fikirlərlə əqli manipulyasiya və istismar mexanizmlərinin inkişafına səbəb olmuşdur.

İnsan alveri qurbanlarının həyatı görünməz zəncirlər içində köləliyə çevrilmiş insan talelərinin hekayələridir.

Rəqəmsal dövr bu zəncirləri görünməz etməklə onları daha da təhlükəli hala gətirmişdir. Artıq qurbanların cəlb edilməsi küçələrdə deyil, monitorların arxasında — elanlarda, "iş təkliflərində", "xəyallar vəd edən" mesajlarda baş verir.

Azərbaycan son illərdə insan alveri ilə mübarizədə mühüm uğurlar əldə edib. Hüquqi baza formalaşıb, qurbanlar üçün profilaktik yönümlü xidmətlər yaradılıb, sosial reabilitasiya sistemi işləyir. Lakin yeni informasiya texnologiyaları günü gündən dünyanı dəyişdirməkdə davam edir. Texnologiyalar cinayətkar şəbəkələrə yeni alətlər, yeni üsullar, yeni maskalanmış sufətlər vasitəsiylə yeni yollar açır. Bu səbəbdən cəmiyyət bu dəyişikliklərə eyni dərəcədə ağıllı və çevik cavab verməyə hazır olmalıdır.

Təqdim olunan bu təlimat rəqəmsal insan alveri ilə mübarizədə Azərbaycan modelinin yeni mərhələsində cərəyan edən həmin çağırışlara ünvanlanan cavabın bir hissəsidir. Burada məqsəd yalnız onlayn cinayətləri izləməklə bitməyərək, hər hər toxunulan linklər, hər elan, hər mesaj arxasında gizlənmiş məkjrli niyyətləri vaxtında görmək, tanımaq və dayandırmaqdır.

İnsan alveri ilə mübarizə artıq təkcə hüquqi müstəvidə aparılan mübarizə deyil, həm də rəqəmsal məsuliyyət, etik şüur və texnoloji bacarıq məsələsidir. Bu sənədin hər səhifəsi, hər qaydası qurbanın səsini daha tez eşitmək, onun həyatını qorumaq və görünməz təhlükəni görünən etmək üçün yazılıb.

Rəqəmsal mühitdə aparılan monitorinq — erkən aşkarlama,

risk qiymətləndirmə və sübutların təhlükəsiz istiqamətlən-dirilməsi üçün əsas mexanizmə çevrilir. Bu, həm hüquq-mühafizə orqanlarının, həm də vətəndaş cəmiyyəti təşkilatlarının fəaliyyətində yeni mərhələnin başlanğıcıdır. Rəqəmsal Monitorinq Təlimatı məhz bu məqsədlə hazırlanaraq, insan alveri ilə mübarizədə dövlət–QHT əməkdaşlığını texnoloji səviyyədə sistemləşdirir, məlumatların etik, təhlükəsiz və hüquq müstəvisində idarə olunması üçün milli çərçivə təqdim edir.

Bu sənəd, Azərbaycanın insan alverinə qarşı mübarizə sahəsində formalaşmış müsbət təcrübəsini qorumaqla yanaşı, rəqəmsal dövrün çağırışlarına çevik cavab verən yeni standartların tətbiqinə xidmət edir. Rəqəmsal aləmdə cinayətkar davranış formalarının artması fonunda bu təlimat həm praktik fəaliyyət aləti, həm də strateji sənəd kimi mühüm əhəmiyyət daşıyır.

Qarşıda duran əsas vəzifə – insan alveri ilə mübarizəni yalnız hüquqi çərçivədə deyil, rəqəmsal etika və təhlükəsizlik mədəniyyəti səviyyəsində həyata keçirməkdir. Bu istiqamətdə hər bir mütəxəssis, qurum və vətəndaş birgə məsuliyyət daşıyır. Çünki, rəqəmsal monitorinq yalnız texnologiya deyil, insanın azadlığını qorumağın yeni dili, yeni etikasıdır.

İnsan alveri XXI əsrin ən sürətlə dəyişən transmilli cinayətlərindən biridir və o, rəqəmsallaşmanın inkişafı ilə yeni formalar almışdır. Əgər bir zamanlar istismar əsasən fiziki məkanlarda baş verirdisə, hazırda sosial media, onlayn elan saytları, sosial şəbəkələr vasitəsi ilə mesajlaşma tətbiqləri və hətta oyun platformaları alverçilərin potensial qurbanlara çıxışını asanlaşdırır. Bu səbəbdən insan alverinə qarşı mübarizə yalnız ənənəvi hüquqi və sosial yanaşmalarla məhdudlaşa bilməz, rəqəmsal mühitdə də aktiv monitorinq və aşkarlama mexanizmlərinin tətbiqni tələb edir.

BMT-nin Narkotiklər və Cinayətkarlıq üzrə İdarəsinin son hesabatında göstərilir ki, qurbanların 41%-i ilkin mərhələdə sosial media və onlayn elanlar vasitəsilə cəlb olunur[1]. Bu fakt rəqəmsal mühitdə monitorinqin və aşkarlamanın nə qədər vacib olduğunu bir daha sübut edir.

[1] UNODC. (2022). *Global report on trafficking in persons 2022*. United Nations Office on Drugs and Crime.

Rəqəmsal texnologiyalar insan alverçilərinin fəaliyyətini həm asanlaşdırır, həm də yeni aşkarlama imkanları yaradır. Avropa Təhlükəsizlik və Əməkdaşlıq Təşkilatının[2] araşdırmalarına görə, son illərdə qurbanların cəlb edilməsi əsasən Facebook, Instagram, Telegram və tanışlıq tətbiqləri üzərindən həyata keçirilir. Bu, ənənəvi hüquqi yanaşmaların yanında rəqəmsal mübarizə metodlarının da inkişaf etdirilməsini tələb edir.

Beynəlxalq Miqrasiya Təşkilatı[3] bildirir ki, rəqəmsal platformalarda aparılan monitorinq yalnız insan alveri qurbanlarını aşkarlamaq üçün deyil, həm də potensial riskləri qabaqlamaq üçün strateji vasitədir. Bu təlimat rəqəmsal müstəvidə insan alverinin risklərini izləmək, qurbanlar tərəfindən göndərilən mesajları daha tez aşkarlamaq və sosial media vasitəsilə cəlb etmə proseslərini anlamaq üçün hazırlanmışdır. Məqsəd — insan alveri cinayətini törədənlərin dəyişən metodlarını vaxtında tanımaq və zərərçəkənləri qorumaqdır. Buna görə də bu təlimat insan alverinə qarşı mübarizədə rəqəmsal izləmə, risklərin təsnifatı və təhlükəsiz ünsiyyət protokollarını sistemləşdirərək mütəxəssislərə praktik alət təqdim edir.

Təlimatın təqdim etdiyi metod və prosedurlar praktik olaraq rəqəmsal monitorinq işinin təxirə salınmadan tətbiqi üçün nəzərdə tutulmuşdur. Burada sosial media və elan saytlarında aşkarlama, şübhəli siqnalların qiymətləndirilməsi, qurbanlarla təhlükəsiz ünsiyyət protokolları və operativ yönləndirmə mexanizmləri sistemləşdirilmişdir. Təlimat, həm gündəlik monitorinqi həyata keçirən operatorlar, həm qərarverici şəxslər, həm də hüquq-mühafizə və sosial xidmət təşkilatları üçün zəruri sayılan alətlər və standart əməliyyat prosedurlarını (SOP) əhatə edir.

Təlimat, rəqəmsal mühitə yönəlik aşkarlama və ilkin müdaxilə prosedurlarını əhatə edir. Fiziki müdaxilə, məhkəmə ekspertizası və ya texniki kibertəhlükəsizlik forensika alətlərinin geniş tətbiqi metodlarını daxil etmir. Eyni zamanda, platforma əsaslı siyasət dəyişiklikləri (məsələn, sosial şəbəkə operatorları ilə hüquqi əməkdaş-

[2] OSCE. (2021). *Policy responses to technology-facilitated trafficking in human beings*. Organization for Security and Co-operation in Europe.

[3] IOM. (2022). *Counter-trafficking and technology: Emerging trends and challenges*. International Organization for Migration.

lıq) və milli qanunvericilikdəki dəyişikliklər bu təlimatın tətbiqinə təsir edə bilər.

Təqdim edilən sənəd, İnsan alverinə qarşı mübarizə üzrə beynəlxalq hüquq normaları ilə tənzimlənir: Palermo Protokolu və CEDAW kimi sənədlər dövlətlərin öhdəliklərini ortaya qoyur; milli kontekstdə isə cinayət məcəlləsi, əmək qanunvericiliyi və uşaq hüquqları ilə bağlı normativlər əsas rol oynayır. Rəqəmsal mühitdə aşkarlama və sübutların toplanması zamanı həm insan hüquqlarının qorunması, həm də sübut zəncirinin hüquqi etibarlılığı təmin edilməlidir.

Təlimatda rekrutment (cəlb etmə), means (məcburetmə üsulları), purpose (istismar məqsədi), sentiment analysis (emosional təhlil), reverse image search (şəkil əsasında axtarış) kimi geniş istifadə olunan anlayışlara aydınlıq gətirilir. Hər bir termin və anlayışın qısa və aydın formada tərifinin verilməsi təlimatın sonunda əlavələr hissəsində verilir ki, bu da operatorlar və mütəxəssislərin vahid anlayışlar sistemindən istifadə etmələrinə şərait yaradır.

Təlimat qeyd edilən monitorinq prosesi üç əsas mərhələdən ibarətdir:

(1) geniş-miqyaslı məlumat toplama (sadə açar söz və hashtag izləmələri),

(2) daraltma və filtrasiya (Böyl sorğuları, regex, pattern detection),

(3) əməli təsnifat və yönləndirmə (risk matrisasına əsasən yaşıl/sarı/qırmızı refleksiya qərarları). Bu metodologiya həm əl (fiziki olaraq) əməliyyatları, həm də süni intellekt dəstəkli alqoritmlərlə paralel işləmək üçün nəzərdə tutulub.

Monitorinq fəaliyyətində məxfiliyin təmin edilməsi əsas prioritetdir. Qurbanların şəxsi məlumatları yalnız lazım olan minimal səviyyədə toplanmalı və şifrələnmiş şəkildə saxlanılmalıdır. Həssas məlumatların paylaşılması üçün müvafiq razılıq və ya qanuni əsas tələb olunur. Operatorlar üçün məlumat əlçatanlığı, audit loqları və məlumatın məhdud saxlanma müddəti siyasətləri hazırlanmalıdır. (GDPR-tipli prinsiplərə istinadla)

Təlimatın tətbiqindən sonra gözlənilən əsas nəticələrə aşağıdakılar daxildir:

Aşkarlamanın sürətinin artırılması (ilk siqnaldan ilkin qiymətləndirməyə qədər vaxt),

qırmızı siqnalların sayına görə müdaxilə faizi,

yanlış pozitivlərin (false positives) azaldılması və hüquq-mühafizə orqanları ilə koordinasiyanın effektivliyi.

Bu göstəricilər monitorinq sisteminin davamlı qiymətləndirilməsi üçün əsas KPI-lər kimi istifadə olunmalıdır.

Rəqəmsal mühitdə insan alverinə qarşı mübarizə yalnız tək təşkilatın işi deyil. Təlimatla tanış olanlara təklif olunur ki, yerli QHT-lər, hüquq-mühafizə, media və platforma operatorları ilə əməkdaşlıq kanalları yaratsınlar, monitorinq nəticələrini paylaşsınlar və məxfi şəkildə qarşılıqlı məlumat mübadiləsi mexanizmlərini (MOU, data-sharing protocols) işə salsınlar. Bu yanaşma qurbanların müdafiəsini sürətləndirəcək və şəbəkə-əsaslı cavab mexanizmini gücləndirəcək.

Təqdim olunan bu təlimat ilk növbədə:

- **sosial işçilər** — qurbanların onlayn davranışlarını və siqnallarını düzgün oxumaq,
- **psixoloqlar** — rəqəmsal mühitdə travma əlamətlərini başa düşmək,
- **hüquq-mühafizə orqanlarının əməkdaşları** — sübut toplama və təcili müdaxilə mexanizmlərini gücləndirmək,
- **QHT nümayəndələri və jurnalistlər** üçün — aşkarlama və ictimai məlumatlandırma prosesini sistemləşdirmək məqsədilə nəzərdə tutulub.

İnsan alveri ilə mübarizədə rəqəmsal metodların tətbiqi bir sıra yenilikləri zəruri edir:

1. Açar söz və Böyl (məntiqi axtarış) izləmələri – sosial şəbəkələrdə riskli elanları və siqnalları aşkarlamaq üçün;
2. Emosional və daranış nümunəsinin analizi – kömək çağırışlarını avtomatik aşkarlamaq üçün süni intellekt dəstəyi;
3. Vizual identiklik əsasında axtarış və süni yaradılmış saxta görüntünün aşkarlaması – foto və video manipulyasiyalarının qarşısını almaq üçün;
4. Qurbanlarla etibarlı əlaqə yaratmaq üçün şifrəli ünsiyyət kanallarından (Signal, ProtonMail, Telegram Secret Chat) istifadə

edilməsi;

5. Siqnalları yaşıl-sarı-qırmızı kateqoriyalar üzrə təsnif edərək daha sürətli reaksiya vermək üçün Risk matrisalarının tətbiqi.

Beləliklə, bu təlimat yalnız nəzəri məlumat deyil, həm də praktik "iş aləti" rolunu oynayır. O, insan alverinə qarşı mübarizədə rəqəmsal transformasiyanın vacibliyini vurğulayır və ən son beynəlxalq təcrübələrə əsaslanır.

1.1. Təlimatın məqsədi

Təqdim edilən təlimatın əsas məqsədi insan alveri ilə mübarizədə rəqəmsal monitorinqin və aşkarlama metodlarının tətbiqini sistemləşdirmək, müvafiq peşəkar qruplara (sosial işçilər, psixoloqlar, hüquq-mühafizə orqanları, QHT nümayəndələri) praktiki alətlər təqdim etməkdir.

Müasir dövrdə insan alverçiləri qurbanların cəlb edilməsində sosial platformaları (Facebook, Instagram, TikTok), mesajlaşma tətbiqləri (Telegram, WhatsApp), onlayn elan saytları və tanışlıq tətbiqlərindən intensiv istifadə edirlər.

Təlimatın məqsədi üç istiqaməti əhatə edir:

1. Aşkarlama bacarıqlarını artırmaq – açar söz izləmələri, Böyl axtarışları, hashtag və geotag monitorinqi kimi metodları praktiki səviyyədə təqdim etmək;

2. Risklərin təsnifatı və reaksiya mexanizmini gücləndirmək – risk matrisalarından (yaşıl–sarı–qırmızı siqnallar) istifadə edərək operativ qərarverməni asanlaşdırmaq;

3. Təhlükəsizlik və etik prinsipləri qorumaq məqsədi ilə qurbanlarla ünsiyyətdə anonimlik, məxfilik, şifrəli ünsiyyət kanalları (Signal, ProtonMail, Telegram Secret Chat) barədə peşəkar davranış standartlarını formalaşdırmaq.

Beləliklə, təlimat yalnız nəzəri çərçivə deyil, həm də praktiki "iş kitabçası" rolunu oynayır. O, həm sahə mütəxəssislərinə, həm də yeni başlayanlara rəqəmsal mühitdə insan alverinin aşkarlanması və qarşısının alınması üçün lazım olan yeni yanaşmaları və alətləri təqdim edir.

1.2. İnsan alverinin rəqəmsal müstəvidə artan formaları

XXI əsrin ən təhlükəli transmilli cinayətlərindən biri olan insan alveri qlobal miqyasda yeni transformasiyalardan keçir. Əgər ənənəvi formalar (məcburi əmək, cinsi istismar və s.) uzun illər əsas təzahür kimi öyrənilirdisə, rəqəmsal texnologiyaların sürətli inkişafı bu fenomeni yeni ölçüyə dəyişib. İnternet, sosial platformalar, kriptovalyuta sistemləri və "darknet" kimi məkanlar insan alverçilərinə həm qurbanları cəlb etmək, həm də istismarı davam etdirmək üçün daha əlverişli imkanlar yaradıb.

BMT-nin 2022-ci il "İnsan alveri üzrə qlobal hesabatı"nda vurğulanır ki, pandemiya illərində onlayn mühit insan alveri hallarında əsas alətə çevrilib[4]. İnsan alverinin yeni üsulları, qadın və uşaqlar üçün xüsusilə təhlükələri artırır çünki onların sosial və iqtisadi asılılığı rəqəmsal müstəvidə manipulyasiya üçün imkanları asanlaşdırır.

Sosial media, iş elanları saytları və tanışlıq platformaları qurbanların ilkin cəlbi üçün əsas vasitəyə çevrilib. Araşdırmalar göstərir ki, insan alverçiləri "iş, təhsil, nikah" vədləri ilə qurbanları aldatmaq üçün Facebook, Instagram və TikTok kimi platformalardan geniş istifadə edirlər[5].

Texnologiya imkanları qurbanların məkan məhdudiyyətlərini aradan qaldırıb. İndi istismar yalnız fiziki deyil, həm də onlayn yayımlar vasitəsilə baş verir. "Kiber-seks alveri" adlanan bu forma xüsusilə Filippin, Hindistan, Latın Amerikası və Şərqi Avropa ölkələrində geniş yayılıb[6]. İnsan alveri cinayətkar qruplar üçün gəlirli "biznes" sahəsi kimi qalmaqdadır. Kriptovalyutaların istifadəsi isə pul axınlarını izləməyi çətinləşdirir. ABŞ Dövlət Departamentinin 2023-cü il üzrə İnsan alveri üzrə hesabatında qeyd edilir ki, "Bitcoin" və digər rəqəmsal valyutalar bu cinayətin maliyyələşməsində mühüm rol oynayır. Yeni texnologiyalarla insan alveri riskləri daha da dərinləşib. "Deepfake" texnologiyası qurbanların razılığı olmadan onların saxta intim videolarının hazırlanmasına və şantaj məq-

[4] United Nations Office on Drugs and Crime (UNODC). (2022). *Global Report on Trafficking in Persons.*

[5] Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA).*

[6] UNICEF. (2021). *Online Child Sexual Exploitation and Abuse: Policy Brief.*

sədilə istifadəsinə şərait yaradır. Bu, həm cəlb etməni, həm də istismarı gücləndirir. Anonimləşdirilmiş (inkoqnito) platformalar (məsələn, TOR) insan alverçiləri üçün "təhlükəsiz zona" rolunu oynayır. Burada uşaq istismarı materiallarının satışı, qanunsuz işçi bazarları və orqan alveri halları aşkarlanıb[7].

Rəqəmsallaşma insan alverinə qarşı mübarizəni həm mürəkkəbləşdirir, həm də onun aşkarlanması üçün yeni fürsətlər yaradır. Bir tərəfdən, rəqəmsal müstəvidə cinayətlər daha gizli və transsərhəd xarakter alır, digər tərəfdən, hüquq-mühafizə orqanları üçün yeni texnoloji alətlər – süni intellekt, "çox böyük həcmli" databaza analizləri, rəqəmsal siqnalların izlənilməsi kimi qabaqlayıcı tədbirlər üçün geniş imkanlar yaradır.

Azərbaycan kontekstində də bu çağırışlar getdikcə aktuallaşır. Ölkədə sosial şəbəkələrin kütləvi istifadəsi, qanuni və qeyri-qanuni miqrasiya prosesləri və iqtisadi həssas qrupların mövcudluğu rəqəmsal insan alveri qurbanına çevrilmə risklərini artırır. Bu səbəbdən milli strategiyalarda yalnız ənənəvi deyil, həm də rəqəmsal müstəvidə cərəyan edən təzahürlər nəzərə alınmalı, gənclər üçün profilaktika xarakterli rəqəmsal savadlılıq proqramları və hüquq-mühafizə strukturları üçün texnoloji resursların gücləndirilməsi təmin edilməlidir.

1.3. Sosial media və rəqəmsal platformalarda aşkarlamanın əhəmiyyəti

XXI əsrdə insan alveri yalnız ənənəvi cinayət forması kimi deyil, həm də rəqəmsal mühitin gətirdiyi yeni imkanlardan istifadə edən mürəkkəb transmilli şəbəkə kimi təzahür edir. İnternetin əlçatanlığı, sosial medianın gündəlik həyatın ayrılmaz hissəsinə çevrilməsi və rəqəmsal iqtisadiyyatın inkişafı insan alverçilərinə daha çevik, anonim və sərhədsiz fəaliyyət imkanı qazandırır.

Ənənəvi olaraq küçələrdə, sərhədyanı ərazilərdə və ya işəgötürmə proseslərində izlənilə bilən cinayətkarlar indi sosial media profillərinin arxasında gizlənir, onlayn elanlarla qurban axtarır və

[7] INTERPOL. (2021). *Human Trafficking and Technology Report*.

kriptovalyutalarla haqq-hesablarını icra edərək izlərini silirlər. Bu baxımdan, rəqəmsal mühit insan alverini həm daha görünməz, həm də daha sürətli yayılan cinayət növünə çevirib.

Məsələ təkcə qurbanların cəlb olunma üsullarının dəyişməsi ilə məhdudlaşmır. Rəqəmsal platformalar vasitəsilə qurbanlar üzərində nəzarət daha asan qurulur, təzyiq və şantaj mexanizmləri daha incə, lakin təsirli formalar alır. Bu səbəbdən, artıq insan alverinə qarşı mübarizə yalnız hüquqi və sosial sahədə deyil, həm də kibertəhlükəsizlik, rəqəmsal savadlılıq və texnologiya əsaslı aşkarlama sistemləri vasitəsilə aparılmalıdır.

UNODC qeyd edir ki, son illərdə qurbanların əhəmiyyətli hissəsi ilkin mərhələdə sosial media üzərindən cəlb olunur. Bu isə göstərir ki, rəqəmsal mühitdə vaxtında aşkarlama mexanizmlərinin işlənməsi həm qurbanların həyatını xilas etmək, həm də transmilli cinayətkar şəbəkələri ifşa etmək üçün strateji əhəmiyyət daşıyır.

Sosial medianın insan alverində rolu

Rəqəmsal texnologiyaların sürətli inkişafı insan alverinə qarşı mübarizədə yeni çağırışlar yaradıb. Əgər əvvəllər qurbanların cəlbi daha çox fiziki mühitdə baş verirdisə, bu gün sosial media platformaları və onlayn elanlar vasitəsilə həyata keçirilir. İnsan alverçiləri iş, təhsil, evlilik vədləri, yaxud saxta elanlarla qadınları, gəncləri və uşaqları manipulyasiya edərək hədəfə alır. Onların etimadını qazanmaq üçün müxtəlif psixoloji təsir vasitələrindən istifadə olunur, nəticədə qurbanlar könüllü şəkildə özlərini riskli situasiyalara atmış olurlar.

Eyni zamanda rəqəmsal mühit yalnız ilkin cəlb mərhələsi ilə məhdudlaşmır. Onlayn istismar, canlı yayımlar, "Kiber-seks alveri" və "cəlbetmə və manipulyasiya prosesi" halları getdikcə qlobal miqyasda artmaqdadır. Bu fenomen təkcə yetkinlərə deyil, uşaqlara qarşı da geniş istifadə olunur. Qurbanların intim görüntülərinin və ya şəxsi məlumatlarının ələ keçirilməsi insan alverçilərinə onların üzərində daha güclü nəzarət qurmaq, rəqəmsal şantaj yolu ilə davamlı istismar etmək imkanı verir.

Belə şəraitdə sosial media və rəqəmsal platformalarda insan

alverinin aşkarlanması strateji əhəmiyyət kəsb edir. İlk növbədə, erkən müdaxilə mexanizmləri vasitəsilə potensial qurbanların vaxtında aşkar olunması onların istismara düşmədən xilas edilməsini mümkün edir. Digər tərəfdən, rəqəmsal izlərin izlənməsi vasitəsilə cinayətkar qrupların fəaliyyət dairəsi, əlaqə şəbəkələri və maliyyə kanalları üzə çıxarılır. Bundan əlavə, onlayn mühitdə mövcud olan müraciət imkanları, "hesabat alətləri" və yardım xətləri qurbanların daha tez yardım almasına şərait yaradır.

Texnologiyanın imkanları bu prosesdə həm fürsət, həm də risk yaradır. Süni intellekt və böyük həcmli alətlər insan alverçilərinin davranış nümunələrini təhlil edərək şübhəli elan və profilləri avtomatik şəkildə müəyyən edə bilir[8]. Şəkil əsasında axtarış və deepfake aşkarlama texnologiyaları qurbanların razılığı olmadan yayılan və ya saxta materialların identifikasiyasını təmin edir. Blokçeyn (bloklar zənciri) texnologiyası və kriptovalyuta tranzaksiyalarının monitorinqi isə istismar şəbəkələrinin maliyyə mexanizmlərinin izlənməsi üçün mühüm alətə çevrilib[9].

Lakin bütün bu imkanlarla yanaşı, bir sıra risklər də mövcuddur. Ən başlıcası, məxfilik və şəxsi azadlıqlar məsələsidir. Sosial media monitorinqi zamanı qurbanların müdafiəsi ilə yanaşı, vətəndaşların hüquqlarının pozulması ehtimalı da diqqətlə nəzərə alınmalıdır[10]. Digər mühüm məsələ texnologiyanın sürətli transformasiyasıdır. İnsan alverçiləri yeni alət və metodlara asanlıqla uyğunlaşaraq aşkarlamadan yayınmağın yollarını tapırlar. Bundan başqa, sosial media platformalarının beynəlxalq xarakter daşıması problemin təkcə milli səviyyədə həllini mümkünsüz edir və çoxtərəfli beynəlxalq əməkdaşlığı zəruri edir.

Nəticə etibarilə, sosial media və rəqəmsal platformalarda insan alverinin aşkarlanması qlobal təhlükəsizlik və insan hüquqlarının müdafiəsi üçün kritik əhəmiyyətə malikdir. Bu, qurbanların həyatını xilas edir, cinayətkar şəbəkələrin ifşasına xidmət edir və dövlətlər, QHT-lər, texnoloji şirkətlər arasında çoxtərəfli əməkdaşlığın zəruriliyini ortaya qoyur.

---

[8] Microsoft & Thorn. (2020). *Project Artemis: AI against Online Grooming*.
[9] U.S. Department of State. (2023). *Trafficking in Persons Report*.
[10] Council of Europe. (2021). *Human Rights in the Digital Age*.

2. Əsas anlayışlar

2.1. İnsan alveri anlayışı və rəqəmsal çağırışlar

İnsan alveri XXI əsrin ən mürəkkəb və transmilli cinayətlərindən biri olaraq, həm klassik istismar formalarında, həm də müasir texnologiyaların təsiri altında yeni müstəvidə təzahür edir. BMT tərəfindən qəbul edilmiş Palermo Protokoluna görə insan alveri, şəxsin zor tətbiqi, hədə-qorxu, aldadılma və ya başqa formada məcburetmə ilə istismara cəlb olunması kimi müəyyənləşdirir[11]. İstismar məcburi əmək, cinsi istismar, orqan alveri və digər formalarda baş verə bilər. Ənənəvi olaraq insan alveri daha çox sosial-iqtisadi zəiflik üzərində qurulmuşdursa, bu gün rəqəmsal texnologiyalar cinayətin yeni ölçülərdə genişlənməsinə şərait yaradır.

Rəqəmsal platformaların kütləvi şəkildə yayılması insan alverçilərinə qurbanlara daha asan çıxış imkanı qazandırır. Sosial media üzərindən yayılan iş, təhsil və evlilik elanları, yaxud saxta reklamlar gəncləri və qadınları aldatmaq üçün ən çox istifadə olunan vasitələrdən biridir. İnsan alverçiləri rəqəmsal mühitdə yalnız cəlb etməni həyata keçirmir, eyni zamanda qurbanların intim görüntülərini və şəxsi məlumatlarını ələ keçirərək şantaj və nəzarət vasitəsi kimi istifadə edirlər. Europol və UNICEF-in məlumatına görə, xüsusilə uşaqlar "cəlbetmə və manipulyasiya prosesi" və "kiber-seks alveri" vasitəsilə rəqəmsal məkanın ən həssas hədəfinə çevrilir.

Bununla yanaşı, rəqəmsal çağırışlar insan alverinə qarşı mübarizənin özündə də yeni imkanlar və dilemlər yaradır. Süni intellekt və "böyük həcmli" texnologiyaları şübhəli davranış nümunələrinin analizi və qurbanların erkən aşkarlanması üçün əhəmiyyətli alətə çevrilib. "Şəkil əsasında axtarış" və deepfake aşkarlama texnologiyaları qurbanların razılığı olmadan yayılan saxta və ya zorla çəkilmiş materialların identifikasiyasını asanlaşdırır. Kriptovalyuta tranzaksiyalarının monitorinqi isə cinayətkar şəbəkələrin maliyyə resurslarının izlənməsinə imkan verir.

Lakin bu imkanlarla yanaşı, bir sıra risklər də mövcuddur. Rə-

[11] United Nations. (2000). *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (Palermo Protocol).*

qəmsal platformalarda monitorinqin gücləndirilməsi məxfilik və insan hüquqlarına dair suallar doğurur. Məxfiliklə təhlükəsizlik arasında balansın necə qorunacağı məsələsi beynəlxalq səviyyədə geniş müzakirə olunur . Digər tərəfdən, insan alverçilərinin texnologiyaya adaptasiya sürəti onların aşkarlama mexanizmlərindən yayınmasına şərait yaradır. Əlavə olaraq, sosial media və rəqəmsal platformaların transsərhəd xarakteri bu problemin təkcə milli qanunlarla deyil, həm də beynəlxalq əməkdaşlıq vasitəsilə həll olunmasını zəruri edir.

Nəticə etibarilə, insan alveri anlayışı bu gün yalnız sosial-iqtisadi zəifliklər kontekstində deyil, həm də rəqəmsal çağırışların doğurduğu risklər fonunda nəzərdən keçirilməlidir. Rəqəmsal mühit insan alverçilərinə həm daha geniş imkanlar yaradır, həm də hüquq-mühafizə orqanları və vətəndaş cəmiyyətinə yeni müdaxilə mexanizmləri təqdim edir. Bu səbəbdən mübarizə strategiyaları yalnız ənənəvi mexanizmlərlə məhdudlaşmamalı, həm texnologiyanın imkanları, həm də onun yaratdığı etik və hüquqi dilemmlər nəzərə alınmalıdır.

Azərbaycan da qlobal rəqəmsallaşma prosesindən kənarda qalmayıb. Ölkədə internet istifadəçilərinin sayı 10 milyondan çox əhalinin təqribən 82%-ni əhatə edir və əksər gənclər gündəlik həyatında sosial media platformalarından aktiv şəkildə yararlanır[12]. Bu, bir tərəfdən informasiya cəmiyyətinin inkişafı üçün müsbət haldır, digər tərəfdən isə insan alverçiləri üçün qurban cəlb etmə imkanlarını asanlaşdırır.

Son illərdə Daxili İşlər Nazirliyi[13] və Baş Prokurorluğun hesabatlarında da qeyd olunur ki, qurbanların bir hissəsi məhz sosial şəbəkələrdə yayılan "iş imkanları" və "xaricdə yüksək maaşlı təkliflər" vasitəsilə aldadılıb. Gənc qızlar və qadınlar isə daha çox "evlilik" və "model biznesi" elanları ilə manipulyasiyaya məruz qalırlar. Bu tendensiya həm regionlarda, həm də Bakıda müşahidə edilir və sosial-iqtisadi həssas qruplar daha çox risk altında qalır.

[12] World Bank. (2022). *Individuals using the Internet (% of population) – Azerbaijan*.

[13] Azərbaycan Respublikası Daxili İşlər Nazirliyi. (2023). *İnsan alverinə qarşı mübarizə üzrə illik hesabat.*

Azərbaycanın hüquqi çərçivəsi, Azərbaycan Respublikasının İnsan alverinə qarşı mübarizə haqqında Qanunu[14] və ardıcıl Milli Fəaliyyət Planları[15], ənənəvi insan alveri formalarının qarşısını almağa yönəlsə də, rəqəmsal mühitdə baş verən yeni halların aşkarlanması hələ də kompleks yanaşma tələb edir. Məsələn, kriptovalyutaların istifadəsi, deepfake texnologiyalarından doğan risklər və onlayn "cəlbetmə və manipulyasiya prosesi" hallarının qanunvericilikdə ayrıca mexanizmlərlə tənzimlənməsi zərurəti yaranır.

Digər mühüm məqam maarifləndirmədir. Tədqiqatlar göstərir ki, gənclərin və yeniyetmələrin böyük hissəsi onlayn təhlükələrlə bağlı məlumatlı olsa da, praktiki müdafiə vərdişlərinə malik deyil. Buna görə də rəqəmsal savadlılıq proqramlarının təhsil sisteminə inteqrasiya olunması, məktəblərdə və universitetlərdə xüsusi modulların tədrisi vacibdir. Bundan əlavə, QHT-lərin və media qurumlarının iştirakı ilə sosial maarifləndirmə kampaniyaları həyata keçirilməlidir.

Hüquq-mühafizə orqanlarının texnoloji imkanlarının artırılması da prioritet məsələdir. Rəqəmsal izlərin təhlili, onlayn elanların monitorinqi və sosial media platformaları ilə əməkdaşlıq üçün xüsusi texniki resurslar və kadr potensialı gücləndirilməlidir. Eyni zamanda beynəlxalq əməkdaşlıq, xüsusilə Avropa Şurası və BMT-nin müvafiq strukturları ilə birgə fəaliyyət, Azərbaycan üçün rəqəmsal müstəvidə insan alveri ilə mübarizədə mühüm əhəmiyyət kəsb edir.

Beləliklə, Azərbaycan kontekstində insan alveri ilə mübarizə yalnız hüquqi mexanizmlərlə məhdudlaşmamalı, həm də rəqəmsal çağırışlara cavab verən inteqrativ yanaşma tələb etməlidir. Bu, dövlət qurumlarının, QHT-lərin, texnologiya şirkətlərinin və cəmiyyətin birgə fəaliyyətini zəruri edir.

---

[14] Azərbaycan Respublikasının *İnsan alverinə qarşı mübarizə haqqında Qanunu* (2005).

[15] Azərbaycan Respublikasında *İnsan alverinə qarşı mübarizə üzrə Milli Fəaliyyət Planı 2020–2024*.

2.2. Monitorinq və izləmə: nədir, nə üçün vacibdir

Monitorinq və izləmə sosial elmlərdə, siyasət planlaşdırmasında və insan hüquqlarının müdafiəsində ən çox istifadə olunan anlayışlardan biridir. Monitorinq anlayışı latınca "monere" – yəni xəbərdar etmək, diqqətdə saxlamaq sözündən gəlir və əsasən hər hansı bir prosesin gedişatını sistemli şəkildə müşahidə etmək, məlumat toplamaq və qiymətləndirmək kimi izah olunur[16]. İzləmə isə monitorinqin tərkib hissəsi olmaqla yanaşı, daha çox davamlı və dövri nəzarəti, müəyyən göstəricilərin planlı şəkildə təhlilini əhatə edir.

Monitorinqin mahiyyəti yalnız məlumat toplamaqdan ibarət deyil, o, həm də qərarvermə üçün əsas yaradan, risklərin qarşısını alan və hesabatlılığı təmin edən mühüm mexanizmdir. Xüsusilə insan hüquqları, sosial xidmətlər, gender bərabərliyi və insan alverinə qarşı mübarizə kimi sahələrdə monitorinq prosesi həm dövlət orqanlarının, həm də vətəndaş cəmiyyətinin fəaliyyətində şəffaflığın təmin olunması üçün mühüm əhəmiyyət daşıyır.

Prosesin vacibliyi bir neçə istiqamətdə özünü göstərir. Əvvəla, monitorinq problemlərin erkən aşkarlanmasına imkan verir. Məsələn, insan alveri ilə mübarizədə sosial media platformalarının izlənməsi qurbanların istismara düşmədən öncə identifikasiyasına şərait yaradır. İkincisi, monitorinq əldə olunan məlumatlar əsasında siyasətlərin, proqramların və qanunvericiliyin effektivliyini ölçməyə imkan verir. BMT-nin Dayanıqlı İnkişaf Məqsədləri *(SDGs)* hesabatlarında da vurğulandığı kimi, davamlı inkişaf məqsədlərinin icrasında monitorinq olmadan nəticələr ölçülə bilməz və məsuliyyət zəifləyər. Üçüncüsü, monitorinq ictimaiyyətin maarifləndirilməsi və şəffaf hesabatlılıq baxımından əhəmiyyət daşıyır. Yığılan məlumatların açıqlanması və ictimaiyyətlə bölüşülməsi vətəndaşların iştirakçılığını artırır və dövlət-cəmiyyət etimadını gücləndirir.

İzləmə və monitorinq mexanizmlərinin gücləndirilməsi həm milli, həm də beynəlxalq səviyyədə vacib hesab olunur. Avropa Şurasının GRETA qrupu mexanizmi dövlətlərin insan alverinə qarşı mübarizə üzrə fəaliyyətini izləyərək, ölkələrə tövsiyələr verir və

[16] OECD. (2010). *Glossary of Key Terms in Evaluation and Results Based Management.*

beynəlxalq müqayisə imkanı yaradır. Bu, göstərir ki, monitorinq yalnız daxili idarəetmə üçün deyil, həm də beynəlxalq əməkdaşlıq və təcrübə mübadiləsi üçün mühüm alətdir.

Nəticə etibarilə, monitorinq və izləmə sadəcə texniki proses deyil, idarəetmənin, hüquqi sistemin və sosial müdafiənin əsas sütunlarından biridir. Onun vasitəsilə yalnız indiki vəziyyətin analizi deyil, həm də gələcək siyasətlərin formalaşdırılması mümkün olur. Bu səbəbdən, monitorinq mexanizmlərinin institusional gücləndirilməsi, rəqəmsal texnologiyaların tətbiqi və çoxşaxəli əməkdaşlığın artırılması müasir dövrün qaçılmaz tələbi hesab olunmalıdır.

Azərbaycan Respublikasında insan alverinə qarşı mübarizə və sosial sahələrdə monitorinq mexanizmləri son illərdə həm qanunvericilik, həm də institusional səviyyədə gücləndirilib. "İnsan alverinə qarşı mübarizə haqqında" Qanun və bu qanunun icrası üçün qəbul edilmiş Milli Fəaliyyət Planları monitorinq və izləmə mexanizmlərinin hüquqi əsaslarını formalaşdırır. Sonuncu 2020–2024-cü illər üçün Milli Fəaliyyət Planı dövlət qurumlarının, qeyri-hökumət təşkilatlarının və beynəlxalq tərəfdaşların fəaliyyətini koordinasiya etməklə yanaşı, hesabatlılıq mexanizmlərinin tətbiqini də nəzərdə tutur[17] .

Bu plan çərçivəsində Daxili İşlər Nazirliyinin İnsan Alverinə qarşı Mübarizə Baş İdarəsi illik hesabatlar dərc edir. Bu hesabatlarda qurbanların sayı, cinayət işlərinin dinamikası, sosial reabilitasiya tədbirləri və beynəlxalq əməkdaşlıq sahəsində əldə olunmuş nəticələr əks olunur. Hesabatlılıq mexanizmi yalnız dövlət orqanlarının deyil, həm də vətəndaş cəmiyyətinin fəaliyyətini nəzərə alır. QHT-lərin hesabatlarında isə sığınacaqlarda yerləşdirilən qadın və uşaqların sosial dəstəklə təmin olunması, psixoloji yardım, hüquqi məsləhət və təhsil proqramlarının monitorinqi aparılır.

Monitorinqin Azərbaycan kontekstində xüsusi əhəmiyyəti ondan ibarətdir ki, o, həm milli strategiyaların effektivliyini ölçməyə, həm də beynəlxalq öhdəliklərin yerinə yetirilməsinə dair şəffaf məlumat təqdim etməyə xidmət edir. Məsələn, Avropa Şurasının GRETA mexanizmi və ABŞ Dövlət Departamentinin hesabatlarında

[17] Azərbaycan Respublikası Nazirlər Kabineti. (2020). 2020–2024-cü illər üçün İnsan alverinə qarşı mübarizə üzrə Milli Fəaliyyət Planı.

Azərbaycanın fəaliyyəti təhlil edilir və milli monitorinq mexanizmlərinin təkmilləşdirilməsi üçün tövsiyyələr. Bu, göstərir ki, Azərbaycanın hesabatlılıq təcrübəsi qlobal miqyasda izlənilir və qiymətləndirilir.

Nəticə olaraq, Azərbaycan kontekstində monitorinq və izləmə yalnız qanuni tələblərin icrası deyil, həm də dövlət-vətəndaş cəmiyyəti beynəlxalq tərəfdaşlar arasında şəffaf əməkdaşlıq platformasıdır. Bu mexanizmlərin davamlı təkmilləşdirilməsi, rəqəmsal texnologiyaların inteqrasiyası və çoxsəviyyəli hesabatlılıq sistemi ölkənin insan hüquqları və sosial müdafiə sahəsində beynəlxalq standartlara yaxınlaşmasına xidmət edir.

2.3. Sadə açar söz axtarışı və Böyl axtarışın fərqi

İnformasiya bolluğu dövründə biliklərin idarə olunması və müvafiq məlumatın seçilməsi yalnız texnoloji deyil, həm də elmi-metodoloji məsələdir. Məlumat axtarışının ənənəvi üsullarından biri olan sadə açar söz axtarışı və daha inkişaf etmiş Böyl axtarışı bu baxımdan həm nəzəri, həm də tətbiqi sahədə geniş müzakirə olunmuşdur.

Rəqəmsal monitorinq və məlumat izləmə proseslərində axtarış metodlarının düzgün seçimi toplanan informasiyanın keyfiyyəti və aktuallığını birbaşa müəyyən edir. Bu kontekstdə sadə açar söz axtarışı ilə Böyl axtarışı arasındakı fərqləri anlamaq vacibdir.

Sadə açar söz axtarışı (simple keyword search) məhdud və əsasən "söz–mətn uyğunluğu"na əsaslanır. İstifadəçi konkret bir və ya bir neçə söz daxil etdikdə sistem həmin sözlərin olduğu materialları təqdim edir. Bu üsul sürətli nəticə versə də, çox vaxt ya həddən artıq çox, ya da kifayət qədər dəqiq olmayan nəticələr əldə olunur. Məsələn, "insan alveri" yazıldıqda bütün materiallarda bu ifadə keçən mətnlər çıxır, amma kontekstə görə fərqləndirmə aparılmır.

Sadə açar söz axtarışı mətnlərdə və verilənlər bazasında sözlərin düz uyğunluğunu tapmağa əsaslanır. İstifadəçi bir və ya bir neçə açar söz daxil etdikdə, sistem həmin sözləri daşıyan bütün mənbələri təqdim edir. Bu üsulun üstünlüyü onun sadəliyi və sürətidir. Lakin

bu yanaşma çox vaxt nəticələrin dəqiqliyini azaldır, çünki yalnız terminlərin mövcudluğuna əsaslanır, semantik əlaqələri nəzərə almır. Məsələn, "insan alveri" ifadəsi ilə sadə axtarış aparıldıqda həm bu mövzuya dair akademik məqalələr, həm də sadəcə "insan" və "alver" sözlərinin təsadüfi şəkildə işlədiyi mətnlər eyni nəticələr arasında görünə bilər[18].

Böyl axtarış isə daha mürəkkəb və analitik yanaşmadır. Burada "AND", "OR", "NOT", eləcə də sitat işarəsi (""), mötərizə və digər operatorlar vasitəsilə axtarış daha dəqiq çərçivəyə salınır. Məsələn, *"*insan alveri*" AND "*rəqəmsal cəlbetmə*"* yazıldıqda yalnız hər iki ifadənin birlikdə keçdiyi mənbələr təqdim olunur. Bu, tədqiqatçıya həm də ajiotajı (mövzuya aid olmayan nəticələri) azaltmaq imkanı verir və informasiya analitikasında daha etibarlı nəticələr əldə etməyə şərait yaradır.

Böyl axtarışı məntiqi operatorlardan (AND, OR, NOT) istifadə edərək nəticələri daha strukturlaşdırılmış və məqsədyönlü şəkildə süzgəcdən keçirir. Bu yanaşma informasiya əldə etmə nəzəriyyəsində klassik modellərdən biri hesab olunur[19]. Böyl üsulu vasitəsilə istifadəçi sorğunu semantik baxımdan daha məntiqli qurur: məsələn, *"*insan alveri AND rəqəmsal platformalar" sorğusu yalnız hər iki anlayışı eyni anda ehtiva edən mənbələri təqdim edir; *"*insan alveri OR məcburi əmək" sorğusu alternativ nəticələr verir; "insan alveri NOT tarix" isə lazımsız kontekstdə olan mənbələri istisna edir[20].

Elmi-tətbiqi baxımdan bu fərqlər mühüm nəticələr doğurur. Akademik tədqiqatlarda sadə açar söz axtarışı ilkin mənbələrin müəyyənləşdirilməsi üçün yararlı ola bilər, lakin dərin analitik araşdırma aparmaq üçün Böyl axtarışı daha funksionaldır. Böyük elmi bazalar (məsələn, *Scopus, Web of Science, ProQuest*) Böyl operatorları ilə yanaşı "truncation" (traffick → trafficking, trafficker), yaxınlıq operatorları (NEAR, ADJ) və "əvəzedici simvol" kimi əlavə alətlərdən istifadəni təşviq edir ki, nəticələr həm əhatəli, həm də dəqiq ol-

[18] Manning, C. D., Raghavan, P., & Schütze, H. (2008). *Introduction to Information Retrieval*. Cambridge University Press.

[19] Salton, G. (1989). Automatic Text Processing: The Transformation, Analysis, and Retrieval of Information by Computer. Addison-Wesley.

[20] Baeza-Yates, R., & Ribeiro-Neto, B. (2011). Modern Information Retrieval: The Concepts and Technology behind Search. Addison Wesley.

sun[21].

Tətbiqi sahədə isə bu fərqlər xüsusilə sosial media monitorinqi, insan alverinin rəqəmsal müstəvidə izlənməsi və kiber təhlükəsizlikdə aktualdır. Sadə açar söz axtarışı "iş elanları" və "təhsil imkanı" kimi nəticələri sürətlə toplamağa kömək edir. Lakin bu, çoxlu sayda əlaqəsiz məlumat gətirdiyindən, daha dərin təhlil üçün Böyl axtarışı tələb olunur. Məsələn, "iş elanları AND Dubay NOT könüllü" sorğusu yalnız xaricdəki iş elanlarını təqdim edir, amma könüllü iş elanlarını istisna edir. Belə strukturlaşdırma riskli kontentin erkən aşkarlanmasında və potensial qurbanların identifikasiyasında xüsusi rol oynayır .

Bu hissənin hazırlanması təsadüfi deyil. İnsan alveri, rəqəmsal zorakılıq və ya ictimai diskursların izlənməsi kimi sahələrdə sadəcə açar sözlərdən istifadə etmək risklidir – çünki nəticələr ya çox ümumi, ya da mövzunu əhatə etməyən ola bilər. Böyl yanaşması isə məlumatın strukturlaşdırılmış, sistemli və analitik süzgəcdən keçirilməsini təmin edir.

Nəticə etibarilə, sadə açar söz axtarışı ilə Böyl axtarış arasındakı əsas fərq onların dəqiqlik, semantik strukturlama və tətbiq sahələri ilə bağlıdır. Birinci üsul daha çox ilkin məlumat toplamaq üçün yararlıdır, ikinci isə həm elmi araşdırmalarda, həm də yüksək riskli sahələrdə (insan alveri, terrorizmlə mübarizə, kiber təhlükəsizlik) dəqiq nəticələrin əldə olunması üçün zəruridir. İnformasiyanın sürətlə artdığı rəqəmsal çağda Böyl axtarış strategiyalarının mənimsənilməsi yalnız akademik tədqiqatçılar üçün deyil, həm də sosial işçilər, hüquq-mühafizə orqanları və QHT-lər üçün strateji bacarıq hesab olunur.

Yekun olaraq bir daha qeyd edirik ki, müasir dövrdə insan alveri ənənəvi sərhədləri aşaraq qlobal miqyasda yeni formalar qazanmışdır. Əgər əvvəl bu cinayət daha çox fiziki məkanlarda gizli şəbəkələr vasitəsilə baş verirdisə, bu gün rəqəmsal mühit – sosial media platformaları, onlayn tanışlıq saytları və messencerlər – istismarçılar üçün əsas alətə çevrilmişdir. Onlayn "cəlbetmə" yalançı iş elanları, "cəlbetmə və manipulyasiya prosesi" və saxta

[21] Chowdhury, G. G. (2010). Introduction to Modern Information Retrieval. Facet Publishing.

profillər vasitəsilə qurbanların cəlb edilməsi rəqəmsal çağırışların miqyasını göstərir. Bu, həm də hüquq-mühafizə orqanlarının və sosial işçilərin müdaxilə metodlarını yenidən düşünməsini tələb edir.

Sadə açar söz axtarışı və Böyl axtarışın müqayisəsi

Meyar	Sadə açar söz axtarışı	Böyl axtarış
Tərif	Verilənlər bazasında və ya mətndə istifadəçinin daxil etdiyi sözlərin birbaşa uyğunluğunu tapır.	Məntiqi operatorlardan (AND, OR, NOT və s.) istifadə edərək sorğunu strukturlaşdırır və nəticələri süzgəcdən keçirir.
Metodologiya	Sözlərin və ifadələrin düz uyğunluğuna əsaslanır; semantik əlaqəni nəzərə almır.	Sorğunu məntiqi əlaqələrlə (qoşma, alternativ, istisna) qurur; daha strukturlaşdırılmış yanaşmadır.
Üstünlüklər	Sadə və sürətli; ilkin məlumat toplamaq üçün yararlıdır.	Dəqiq nəticələr verir; semantik baxımdan daha uyğun mənbələri seçir; elmi tədqiqat və risk monitorinqi üçün effektivdir.
Məhdudiyyətlər	Çoxlu sayda əlaqəsiz nəticə təqdim edə bilər; spesifik tədqiqat üçün yararsız ola bilər.	Daha mürəkkəbdir; istifadəçi operatorlardan düzgün istifadə etmədikdə nəticələr məhdudlaşa bilər.
Tətbiq sahələri	Gündəlik internet axtarışları; ümumi məlumat toplamaq.	Akademik tədqiqat, sosial media monitorinqi, insan alveri və kiber təhlükəsizlik üzrə xüsusi araşdırmalar.
Praktiki nümunə	“iş elanları” - həm real, həm də saxta elanlar birlikdə görünür.	“iş elanları AND Dubay NOT könüllü” - yalnız Dubayla bağlı elanlar çıxır, könüllü elanlar isə istisna olunur.

Bu kontekstdə monitorinq və izləmə xüsusi əhəmiyyət kəsb edir. Monitorinq təkcə məlumat toplamaq deyil, həm də riskləri əvvəlcədən aşkarlamaq, tendensiyaları izləmək və müdafiə mexanizm-

ləri qurmaq üçün vacibdir. Sosial şəbəkələrdə istifadə olunan terminlərin, şübhəli elanların və ya qurban hekayələrinin analizi praktik olaraq erkən xəbərdarlıq sistemi rolunu oynayır. Beləliklə, monitorinq həm profilaktika, həm də sübut toplama funksiyasını yerinə yetirir.

Bu sahədə istifadə olunan əsas vasitələrdən biri axtarış metodlarıdır. Sadə açar söz axtarışı ilkin mərhələdə tez məlumat tapmaq üçün əlverişli olsa da, çox zaman həddən artıq geniş və dəqiqlikdən uzaq nəticələr yaradır. Əksinə, Böyl axtarış "AND", "OR", "NOT" operatorları ilə kombinasiyalı şəkildə tətbiq olunaraq daha hədəfli və analitik nəticələr verir. Bu, insan alveri kimi mürəkkəb fenomenin izlənməsində " ajiotajı" azaldır və tədqiqatçıya dəqiq süzgəcdən keçirilmiş məlumat təqdim edir.

Ümumilikdə, insan alverinin rəqəmsal çağırışlarla birləşməsi, monitorinq və izləmə proseslərinin vacibliyini artırmış, həm də axtarış metodlarının sadədən mürəkkəbə keçməsini zəruri etmişdir. Bu yanaşma yalnız tədqiqatçılar üçün deyil, həm də sosial işçilər, hüquq müdafiəçiləri və dövlət qurumları üçün daha effektiv mübarizə aləti formalaşdırır.

3. İnternet platformaları üzrə izləmə

Rəqəmsal dövrdə insan alveri və zorakılıq halları ənənəvi mühitdən onlayn platformalara keçid edib. Sosial şəbəkələr, tanışlıq saytları və messencerlər artıq qurbanların cəlb edildiyi əsas yerlərə çevrilib. Məsələn, BMT-nin Narkotiklər və Cinayətkarlıq üzrə İdarəsinin hesabatına görə, insan alveri hallarında qurbanların 41%-i internet vasitəsilə rekrutmentə məruz qalıb. Bu fakt platforma izləməsinin vacibliyini açıq şəkildə göstərir.

İzləmə yalnız hüquq-mühafizə orqanları üçün deyil, həm də sosial işçilər və QHT-lər üçün mühüm əhəmiyyət daşıyır. Çünki bu proses şübhəli elanların, manipulyativ profillərin və ya riskli qrup davranışlarının erkən aşkar edilməsinə imkan verir. Məsələn, saxta iş elanlarının tez-tez Facebook və Telegram üzərindən paylanması qurbanların aldadılmasının ən yayğın üsullarından biridir.

Bundan əlavə, onlayn zorakılıq da ciddi sosial problemdir. Avropa Gender Bərabərliyi İnstitutunun[22] məlumatına əsasən, qadınların təxminən 23%-i kiberzorakılıqla üzləşib. Azərbaycanda isə rəqəmsal hüquqlarla bağlı tədqiqatlar məhdud olsa da, sosial mediada erkən nikah, qız uşaqlarına yönəlik təhqir və şantaj halları geniş müzakirə olunur. Bu, yerli səviyyədə də platforma izləməsinin aktuallığını artırır.

Platforma üzrə izləmə həm profilaktik tədbir, həm də sübut toplama vasitəsi kimi çıxış edir. Bu, qurbanların müdafiəsini gücləndirir, hüquqi proseslərdə dəlilləri möhkəmləndirir və ictimaiyyət üçün xəbərdarlıq funksiyası daşıyır. Sadə bir misal: "insan alveri" və "iş elanları" açar sözlərinin birlikdə izlənməsi riskli paylaşımları aşkarlamağa imkan yaradır, bu isə Böyl axtarış üsulunun praktiki gücünü göstərir.

Ümumilikdə, rəqəmsal çağırışların artdığı mühitdə platforma üzrə izləmə müasir mübarizə strategiyalarının ayrılmaz hissəsinə çevrilib. Bu yanaşma olmadan nə qlobal səviyyədə, nə də lokal mühitdə qurbanların vaxtında müdafiəsi mümkün deyil.

Platforma izləməsi sadəcə informasiya toplamaq deyil – bu,

[22] EIGE (2022). *Cyber violence against women and girls*.

erkən xəbərdarlıq və müdafiə vasitəsidir. Sosial işçi və hüquq mühafizə əməkdaşları üçün bu izləmə həm qurbanların qorunmasına, həm də cinayətkarların izlərinin vaxtında aşkarlanmasına imkan verir.

3.1. Facebook

2004-cü ildə ABŞ-da Mark Zukerberg tərəfindən Harvard Universitetində oxuyarkən yaradılıb. Layihəyə daha sonra Dastin Moskovitz, Eduardo Saverin, Kris Hyuges və Endryu MakCollum da qoşulublar. Platforma "The Facebook" adı ilə başlayıb, sonra "Facebook" adını alıb. Bugünkü gündə (2025) dünya üzrə təxminən 3,07 milyard aktiv aylıq istifadəçisi var. Facebook istifadəçiləri hər ay platformaya daxil olur. Gündəlik aktiv istifadəçi sayı da milyardlarla olaraq qiymətləndirilir.

2025-ci ilin iyun ayına olan məlumata görə Azərbaycanda təxminən 5,189,900 Facebook istifadəçisi vardır. Bu, ölkənin yetkin əhalisinin təxminən 85 %-ni təşkil edir. 2025-ci ildə Facebook istifadəçilərinin təxminən 55,1 %-i kişi, 44,9 %-i qadındır.

Facebook Azərbaycanda ən geniş istifadə olunan sosial şəbəkədir və təxminən əhalinin yarısını əhatə edir. Bu geniş yayılma imkanları ilə yanaşı ciddi risklər də yaradır. İnsan alverçiləri üçün belə böyük auditoriya həm qurban tapmaq, həm də onların etibarını qazanmaq baxımından əlverişli "meydan" rolunu oynayır. Ən çox rast gəlinən üsullardan biri saxta iş elanlarıdır. "Xaricdə yüksək maaşlı iş", "model axtarılır" və ya "təhsil üçün imkanlar" adı altında yayılan elanlardır.

Facebook-un daha bir təhlükəli tərəfi anonimlik və gizlənmə imkanıdır. Saxta profillərin çoxluğu alverçilərə real şəxsi məlumatlarını gizlədərək qurbanlarla münasibət qurmağa şərait yaradır. Azərbaycanda hüquq-mühafizə orqanlarının araşdırmalarında da dəfələrlə göstərilib ki, insan alveri işlərində sosial şəbəkələr əlverişli vasitə rolunu oynayır. Xüsusilə uşaqlar və yeniyetmələr bu baxımdan daha həssas qrup sayılır. 12–18 yaş arası qızlar Facebook üzərindən tanışlıq mesajları alır, ardınca oflayn görüşlərə çağırılır və bu proses çox vaxt "grooming" – yəni psixoloji manipulyasiya üsulu

ilə həyata keçirilir.

Problemi dərinləşdirən amillərdən biri də rəqəmsal savadlılığın zəif olmasıdır. Bir çox istifadəçi təhlükəsizlik parametrlərindən xəbərsiz olur, şəxsi məlumatlarını açıq paylaşır və bu, alverçilərin potensial hədəfi müəyyənləşdirməsini asanlaşdırır. Məsələn, "işsizəm" və ya "iş axtarıram" kimi açıq paylaşımlar qurban seçilmə riskini artırır. Beynəlxalq təcrübədə oxçar tendensiyalar da bu vəziyyəti təsdiqləyir. UNODC və ATƏT-in hesabatlarında göstərilir ki, dünyada insan alveri hallarında qurbanların 40 faizdən çoxu onlayn platformalar vasitəsilə cəlb olunur. Azərbaycan da bu qlobal mənzərədən kənarda deyil və region ölkələrində aparılan araşdırmalar sosial şəbəkələr üzərindən qurban cəlbinin ən sürətlə artan üsul olduğunu göstərir.

Bütün bunlar göstərir ki, Facebook Azərbaycanda yalnız ünsiyyət və informasiya mübadiləsi platforması deyil, həm də insan alveri baxımından yüksək risk daşıyan məkandır. Saxta elanlar, gizli profillər, uşaqların manipulyasiyaya açıq olması və rəqəmsal savadlılığın zəifliyi bu təhlükəni gücləndirir. Buna görə də Facebook-un izlənməsi və monitorinqi həm sosial işçilər, həm hüquq-mühafizə əməkdaşları, həm də ictimai təşkilatlar üçün vacibdir. Bu yanaşma qurbanların vaxtında müdafiəsi, risklərin erkən aşkarlanması və ictimaiyyətin maarifləndirilməsi baxımından mühüm əhəmiyyət kəsb edir.

3.1.1.Sadə açar sözlər

Sadə açar söz axtarışı Facebook-da ən çox istifadə olunan izləmə və məlumat toplama üsullarından biridir. Bu metodda istifadəçi konkret bir söz və ya ifadəni axtarış bölməsinə daxil edir və platforma həmin açar sözlərin olduğu bütün paylaşım, qrup, səhifə və ya profil məlumatlarını göstərir. Bu üsul xüsusilə ilkin mərhələdə geniş məlumat toplamaq və ümumi mənzərəni görmək üçün əlverişlidir.

Məsələn, əgər sosial işçi insan alveri risklərini izləmək istəyirsə, sadə açar söz olaraq *"iş elanları"*, *"xaricdə iş"*, *"model axtarılır"* kimi ifadələri yazmaqla Facebook-da açılan nəticələri görə bi-

lər. Bu nəticələr arasında həm real iş elanları, həm də şübhəli və potensial riskli təkliflər ola bilər. Sadə açar sözlərdən istifadə edərkən ən böyük üstünlük odur ki, axtarış çox sürətli və asandır, lakin eyni zamanda çox sayda nəticə gətirdiyinə görə, narahatlığa – yəni mövzuya aid olmayan, amma həmin sözləri daşıyan paylaşımlar da çıxır.

Praktiki misal kimi, *"*xaricdə iş*"* yazıldıqda yüzlərlə elan çıxır və onların arasında həm etibarlı şirkətlərin elanları, həm də insan alverçilərinin hazırladığı saxta təkliflər ola bilər. Sosial işçi və ya hüquq-mühafizə əməkdaşı sadə açar sözlə bu elanları ümumi şəkildə topladıqdan sonra onların məzmununu təhlil edir, şübhəli olanları ayırd edir. Digər misal olaraq *"pulsuz təhsil"* və ya "sponsor axtarılır" sözlərini yazmaq olar. Bu sözlər çox vaxt gəncləri və yeniyetmələri cəlb etmək üçün istifadə olunur və risk qruplarının hədəflənməsinə imkan yaradır.

Sadə açar söz axtarışı həmçinin ictimai tendensiyaları izləmək üçün də faydalıdır. Məsələn, "gömrükdə iş" və ya "Avropada iş" sözlərini yazmaqla istifadəçilərin hansı istiqamətlərə maraq göstərdiyi, hansı ölkələrin daha çox diqqət çəkdiyi barədə ümumi məlumat əldə etmək mümkündür. Bu, insan alverinə qarşı profilaktik tədbirlər üçün mühüm siqnaldır.

Ümumilikdə, sadə açar sözlər Facebook-da monitorinq üçün başlanğıc mərhələ rolunu oynayır. Onlar riskli məzmunu tez tapmağa imkan verir, amma nəticələrin dəqiq və məqsədli olması üçün sonrakı mərhələdə mütləq süzgəcdən keçirmə və əlavə təhlil aparmaq lazımdır

Numunə:

Addım	Görüləcək iş	Nümunələr / Qeydlər
1	Açar sözləri müəyyən et	*"*xaricdə iş", "model axtarılır", "asan qazanc", "pulsuz təhsil", "sponsor axtarılır"
2	Açar sözü Facebook axtarış bölməsinə daxil et	"Bütün" bölməsindən qruplar, səhifələr və postlara bax

3	Nəticələri süzgəcdən keçir	Şübhəli profilləri ayır: yalnız WhatsApp nömrəsi, real olmayan maaş vədləri, təkrar paylaşımlar
4	Sənədləşdir	Ekran görüntüsü çək, linki qeyd et, paylaşım tarixini və istifadəçi adını yaz
5	Təhlil və təsnifat apar	- Riskli elanlar - Maraqlı tendensiyalar - Adi paylaşımlar
6	Hesabat hazırla və paylaş	"Bu həftə 'xaricdə iş' üzrə 12 şübhəli elan aşkar olundu, əsas istiqamət: Türkiyə, Polşa"
7	Maarifləndirmədə istifadə et	"Şübhəli iş elanlarını necə tanımaq olar?" mövzusunda sosial paylaşım və ya təlim materialı hazırla

3.1.2.Böyl nümunələri

Facebook-da sadə açar sözlər ilkin izləmə üçün faydalı olsa da, çox zaman nəticələr çox geniş və qarışıq olur. Bu zaman Böyl axtarış üsulu köməyə gəlir. Böyl üsulu müəyyən operatorlardan (*AND, OR, NOT, " ", ()*) istifadə etməklə nəticələri daraldır və dəqiqləşdirir. Bu metod insan alveri, zorakılıq və ya digər sosial risklərlə bağlı monitorinq aparan sosial işçilər, hüquq-mühafizə əməkdaşları və tədqiqatçılar üçün daha məqsədli axtarış imkanı yaradır.

Məsələn, bir sosial işçi Facebook-da yalnız xaricdə iş elanları ilə bağlı şübhəli paylaşımları izləmək istəyirsə, sadəcə *"iş elanları"* yazdıqda yüzlərlə nəticə qarşısına çıxacaq. Amma Böyl operatoru ilə "iş elanları" AND "xaricdə" yazıldıqda yalnız hər iki ifadənin birlikdə olduğu paylaşımlar göstəriləcək. Bu, əlavə işi azaldır və diqqəti konkret riskə yönəldir.

Digər bir misal, insan alverçiləri çox vaxt modelləşdirmə adı ilə qızları aldadırlar. Sadəcə *"model"* sözünü yazmaq faydasız ola

bilər, çünki nəticələrdə real moda agentliklərinin paylaşımları da çıxacaq. Əgər sosial işçi "model" AND "iş" NOT "fotoqrafiya" yazarsa, şəkillə bağlı normal elanlar kənarda qalacaq, amma iş təklifləri önə çıxacaq. Bu isə potensial riskli elanları daha aydın görməyə imkan verir.

OR operatoru isə alternativ variantları birləşdirmək üçündür. Məsələn, "xaricdə iş" OR "otel işçisi" OR "hostess" yazıldıqda axtarış həm xaricdə iş elanlarını, həm də otel və hostes işlərini əhatə edir. Bu üsul insan alverçilərinin fərqli adlar altında yayımladığı elanları birləşdirmək üçün çox faydalıdır.

Dırnaq işarələri ("-") ifadənin tam şəkildə tapılması üçün vacibdir. Məsələn, *"xaricdə iş"* dırnaq içində yazıldıqda Facebook yalnız bu iki sözün ardıcıl olduğu nəticələri göstərəcək. Əgər dırnaqsız *xaricdə iş* yazılsa, nəticələrdə "xaricdə" və "iş" sözləri ayrı-ayrı hallarda da çıxa bilər.

Mötərizələr () isə mürəkkəb axtarışlarda kombinasiyaları idarə etmək üçün istifadə olunur. Məsələn, ("xaricdə iş" OR "hostess") AND "vizasız" yazıldıqda həm xaricdə iş, həm də hostes elanları tapılacaq, amma yalnız "vizasız" sözü ilə birlikdə olan nəticələr göstəriləcək. Bu, insan alverçilərinin "vizasız iş" adı altında cəlb etdiyi elanların seçilməsi üçün çox faydalıdır.

Nəticə etibarilə, Böyl üsulu sadə açar söz axtarışından fərqli olaraq sosial işçiyə daha az, amma daha dəqiq nəticələr təqdim edir. Bu, monitorinq işini yüngülləşdirir, vaxt itkisinin qarşısını alır və ən əsası, potensial riskli paylaşımların göz önünə çıxmasına şərait yaradır. Misallar göstərir ki, düzgün Böyl kombinasiyaları insan alveri və onlayn istismara qarşı mübarizədə effektiv alət ola bilər.

Nümunə:

Operator	Nümunə	Nəticə və izah
AND	"iş elanları" AND "xaricdə"	Hər iki sözün birlikdə olduğu paylaşımlar çıxır. Yalnız "iş elanları" və "xaricdə" bir yerdə olduqda nəticə göstərilir.
OR	"xaricdə iş" OR "hostess"	İstənilən birinin olduğu nəticələr çıxır. Hem

		“xaricdə iş”, həm də “hostess” sözləri olan elanları tapır.
NOT	"model" AND "iş" NOT "fotoqrafiya"	“Model” və “iş” sözləri birlikdə olan paylaşımları göstərir, amma içində “fotoqrafiya” olanları istisna edir.
“ ” (dırnaq)	"xaricdə iş"	İki söz ardıcıl şəkildə birlikdə axtarılır. “Xaricdə” və “iş” ayrı-ayrı düşən nəticələr çıxmır, yalnız tam ifadə tapılır.
( ) mötərizə	("xaricdə iş" OR "hostess") AND "vizasız"	Həm “xaricdə iş”, həm də “hostess” sözləri axtarılır, amma yalnız “vizasız” sözü ilə birlikdə olduqda nəticə göstərilir.

3.1.3.Riskli qruplar və səhifələrə dair göstəricilər

Facebook kimi sosial şəbəkələr insan alveri və onlayn istismarın əsas mühitlərindən biri kimi diqqət çəkir. Riskli qruplar və səhifələr çox vaxt açıq şəkildə fəaliyyət göstərir, amma onların məzmunu diqqətlə izlənməsə, tez gözə dəymir.

Facebook-da səhifələrin və qrupların riskli olub-olmadığını müəyyənləşdirmək üçün sosial işçilər bir neçə sadə, amma praktik siqnalı izləməlidirlər. Ən birincisi, elanların məzmununa diqqət etmək lazımdır. Əgər elanlarda “vizasız iş”, “sənəd tələb olunmur”, “həftədə minlərlə dollar qazanc” kimi qeyri-real vədlər varsa, bu, ciddi xəbərdarlıq əlamətidir. UNODC-nin 2023-cü il hesabatında da qeyd olunur ki, belə elanlar insan alverçilərinin ən çox istifadə etdiyi üsullardandır.

Digər mühüm siqnal səhifə və ya qrupun şəffaflıq səviyyəsidir. Əgər qrup qapalıdır, üzvlüyə yalnız dəvətlə daxil olmaq mümkündürsə və ya administratorların şəxsiyyəti bəlli deyilsə, bu, riskli

fəaliyyətə işarə edə bilər. Europol-un 2021-ci il IOCTA hesabatında vurğulanır ki, insan alveri ilə məşğul olan şəbəkələr çox vaxt belə qapalı onlayn mühitlərdən istifadə edirlər.

Şübhəli profillərin çoxluğu da siqnal sayılır. Real olmayan, yalnız cazibədar şəkillər yükləyən, amma şəxsi həyat və gündəlik fəaliyyətə dair paylaşım etməyən profillər, əslində, qurban cəlb etmək üçün yaradılmış ola bilər.

Elanların tez-tez təkrar olunması və əlaqə üçün yalnız şəxsi nömrələrin — WhatsApp və ya Telegram — göstərilməsi də təhlükənin əlamətidir. Əgər rəsmi şirkət ünvanı və ya sayt mövcud deyilsə, səhifə riskli sayılmalıdır. EIGE-nin 2022-ci il hesabatında da qadınların onlayn manipulyasiya ilə ən çox bu tip saxta elanlar vasitəsilə qarşılaşdığı vurğulanır.

Qrupların və səhifələrin riskli olub-olmadığını müəyyənləşdirmək üçün sosial işçilər bir neçə sadə siqnala diqqət yetirməlidir. Elanlarda həddən artıq cazibədar maaş vədləri, əlaqə vasitəsi kimi rəsmi şirkət ünvanı əvəzinə şəxsi nömrələrin göstərilməsi, paylaşımların sürətli təkrar olunması və qapalı üzvlük mexanizmi. Bu nümunələr göstərir ki, Facebook-un geniş auditoriyası ilə yanaşı, təhlükəli cəlbetmə məkanı da mövcuddur.

Ümumilikdə, riskli qruplar və səhifələr insan alverçilərinin qurban axtarışında mühüm rol oynayır. Onların göstəricilərini vaxtında tanımaq sosial işçilərə, hüquq-mühafizə əməkdaşlarına və vətəndaş cəmiyyəti təmsilçilərinə qurbanların müdafiəsində effektiv addımlar atmaq imkanı yaradır. Azərbaycanda sosial mediada müşahidə olunan nümunələr və beynəlxalq hesabatlardan gətirilən faktlar göstərir ki, bu təhlükə realdır və diqqətdən kənarda qalmamalıdır.

Yoxlama siyahısı: Facebook-da riskli qruplar və səhifələr

- Qeyri-real vədlər -“vizasız iş”, “sənəd tələb olunmur”, “həftədə 2000$ qazanc” kimi elan varmı?
- Şəffaflıq səviyyəsi- Qrup qapalıdır. Administratorların kimliyi bəlli deyil.
- Əlaqə vasitələri - əlaqə yalnız WhatsApp/Telegram nömrəsi ilədir, rəsmi sayt və ya e-mail yoxdur.
- Şübhəli profillər - profil şəkilləri çox cazibədardır, amma

şəxsi paylaşımlar yoxdur. Eyni şəkildən bir neçə profil yaradılıb.

➢ Paylaşımların xarakteri - elanlar tez-tez təkrar olunur. Həddindən artıq çox sayda "iş elanları", "sponsor axtarılır" postları var.

➢ Dil və üslub -paylaşımlarda dil səhvləri, avtomatik tərcümə izləri görünür.

➢ Məkan və uyğunluq -elan konkret ölkəni göstərir, amma viza/sənəd detalları qaranlıqdır.

➢ Təzyiq əlamətləri -"təcili qərar verin", "yalnız bu gün keçərlidir" tipli təzyiq mesajları var.

➢ Ödəniş tələbi -qrup və ya profil əvvəlcədən pul və ya şəxsi sənəd (pasport, şəhadətnamə) istəyir.

Əgər bu siyahıdakı siqnallardan bir neçəsi təsdiqlənirsə, səhifə və ya qrup riskli hesab edilməli, sənədləşdirilməli və aidiyyəti qurumlara bildirilməlidir.

Nümunə.

Siqnal	Təsvir	Risk kodu
Normal elan	Real şirkət, rəsmi əlaqə (sayt, e-mail), məntiqli maaş və şərtlər	🟢 Yaşıl (Normal)
Qeyri-real vədlər	"Vizasız iş", "sənəd tələb olunmur", "həftədə 2000$" kimi şişirdilmiş təkliflər	🟡 Sarı (Diqqət!)
Şəffaf olmayan struktur	Qrup qapalıdır, adminlər gizlidir, yalnız dəvətlə giriş mümkündür	🟡 Sarı (Diqqət!)
Əlaqə yalnız şəxsi kanallarla	Yalnız WhatsApp/Telegram nömrəsi verilib, rəsmi ünvan yoxdur	🔴 Qırmızı (Riskli)
Şübhəli profillər	Eyni şəkildən bir neçə profil, şəxsi paylaşım yoxdur, çox cazibədar şəkillər	🔴 Qırmızı (Riskli)
Tez-tez təkrar elanlar	Eyni məzmunlu iş elanlarının sıx paylaşılması	🟡 Sarı (Diqqət!)
Dil və üslub səhvləri	Avtomatik tərcümə izləri, ardıcıl yazı səhvləri	🟡 Sarı (Diqqət!)
Təcili qərar təzyiqi	"İndi qoşul!", "Bu gün son şansdır" tipli mesajlar	🔴 Qırmızı (Riskli)
Ödəniş və ya sənəd tələbi	Əvvəlcədən pul, pasport surəti, şəxsi məlumat istəyirlər	🔴 Qırmızı (Çox təhlükəli)

3.2. Telegram.

Telegram 2013-cü ildə rusiyalı qardaşlar Pavel və Nikolay Durov tərəfindən yaradılıb. Onlar əvvəllər Rusiyada məşhur VKontakte sosial şəbəkəsinin də təsisçiləri idilər. Telegramın arxasında Telegram Messenger LLP şirkəti dayanır. İlk vaxtlar şirkət Almaniyada qeydiyyatdan keçmişdi, daha sonra hüquqi ünvan dəyişdirildTelegram messencer sistemi rəsmi olaraq 14 avqust 2013 tarixində istifadəyə verilib. Qısa müddət ərzində gizlilik, sürət və müxtəlif funksionallığı (media paylaşımı, qruplar, kanallar və s.) sayəsində populyarlıq qazandı. 2025-ci ilədək Telegram-un dünyada aylıq aktiv istifadəçi sayı 1 milyarda çatıb. Platformanın istifadəçi bazasında cinsiyyət fərqi var: təxminən 56.9 % kişi, 43 % qadın istifadəçilər olduğu bildirilir. Yaş qruplarına görə ən böyük istifadəçi qrupu 25–34 yaş aralığında yerləşir, bu yaş qrupu ümumi istifadəçilərin ~30 %-ni təşkil edir.

Telegram sosial media kateqoriyasında Azərbaycanda geniş yayılıb və müxtəlif istiqamətlərdə istifadə olunur (ictimai kanallar, xəbərlər, qruplar, mesajlaşma). Lakin açıq mənbələr konkret istifadəçi sayı, demoqrafik göstəricilər və bölgələr üzrə paylanma barədə geniş statistik məlumat vermirlər. Azərbaycanda sosial media istifadəçilərinin sayı artmaqdadır. 2024-cü ilin əvvəlində ölkədə aktiv sosial media istifadəçisi sayı 6,10 milyon təşkil edirdi ki, bu da əhalinin böyük hissəsini əhatə edir. Telegram xüsusi halda siyasi, xəbər, ictimai forum və lokal elan kanalları kimi istifadə olunur və bəzən anonimlik təmin etməsi səbəbilə zərərli və radikal məzmunların yayıldığı platforma hesab edilir. Məsələn, "How Azerbaijan's Telegram Channels Fuel Intimidation" (Azərbaycanın Telegram kanalları necə qorxutmanı/qısnaməni gücləndirir) məqaləsində bildirilir ki, Telegram kanalları qismən senzura olunmaması və istifadəçi məxfiliyini qoruyan siyasəti səbəbilə dezinformasiya, hədə-qorxu və toksik məzmun üçün istifadə olunur.

3.2.1.Kanallar və qruplarda izləmə

Kanallar və qruplar rəqəmsal mühitdə informasiyanın ən sü-

rətlə yayıldığı platformalardan biridir. Onlar bəzən maarifləndirmə və ictimai müzakirələr üçün müsbət rol oynasa da, çox vaxt insan alveri, zorakılıq və saxta elanların yayılması üçün riskli mühitə çevrilir. Bu səbəbdən kanallarda və qruplarda izləmə texnologiyalarının tətbiqi müasir dövrdə xüsusi əhəmiyyət daşıyır. Akademik yanaşmalarda izləmə yalnız məlumat toplamaq prosesi kimi deyil, həm də məzmunun təhlili, davranış nümunələrinin müəyyənləşdirilməsi və risk siqnallarının vaxtında aşkarlanması kimi izah olunur. Burada əsas məqsəd cinayətkar şəbəkələrin erkən mərhələdə ifşa olunması və qurbanların qorunmasıdır.

Telegram qlobal miqyasda sürətlə yayılan və anonimlik səviyyəsi yüksək olan platformadır. Onun xüsusilə geniş qruplar və kanallar yaratmaq imkanı, şifrələmə və məxfilik üstünlükləri səbəbilə insan alveri, radikallaşma və saxta elanlar üçün istifadə olunması halları artmaqdadır. Bu mühitdə izləmə texnologiyaları qurbanların qorunması və risklərin aşkarlanması baxımından həyati əhəmiyyət daşıyır.

Telegram-un spesifik xüsusiyyəti ondan ibarətdir ki, qruplarda 200 minə qədər üzv ola bilir, kanallarda isə milyonlarla izləyici toplanır. Belə geniş auditoriya insan alverçilərinə "asan ov meydanı" yaradır. Məsələn, "vizasız iş", "model axtarılır" və ya "asan qazanc" tipli elanlar tez bir zamanda minlərlə istifadəçiyə çatır. Burada izləmə texnologiyası əsasən açar sözlərin və ifadələrin monitorinqinə əsaslanır. Riskli açar sözlər sistemli şəkildə izlənir və nəticələr təhlil olunur.

İzləmə prosesində bir neçə metod özünü doğruldur. İlk növbədə açar sözlərin monitorinqi mühüm yer tutur. "Vizasız iş", "asan qazanc" və ya "model axtarılır" kimi açar sözlər Facebook və Telegram qruplarında şübhəli elanları müəyyənləşdirmək üçün tez-tez istifadə olunur. Sadə açar sözlər geniş nəticə versə də, Böyl operatorlarının tətbiqi nəticələrin dəqiqləşdirilməsinə imkan verir. Digər bir istiqamət qruplarda davranış nümunələrinin izlənməsidir. Məsələn, eyni nömrənin və ya eyni tip elanların təkrar-təkrar paylaşılması risk siqnalı sayılır. Bu, ATƏT tərəfindən "nümunələrin tanınması" adlandırılan üsuldur və şübhəli davranışın aşkarlanmasına kömək edir. Şəbəkə analizi də vacibdir, çünki bir elan bir neçə qrup və

kanalda eyni vaxtda yayıldıqda, bu koordinasiyalı fəaliyyətin göstəricisi ola bilər.

Multimedia izləmə də önəmli texnologiyalardandır. Foto və videolar "şəkil əsasında axtarış" üsulu ilə yoxlanılır və əgər eyni şəkil onlarla qrupda elan kimi istifadə olunursa, bu, saxta profil və ya aldatma sxeminin mövcudluğunu göstərir. Son illərdə süni intellekt və maşın öyrənməsi metodları da izləmə texnologiyalarına əlavə olunub. Bu alətlər mətn, şəkil və hətta emojiləri analiz etməklə şübhəli məzmunu avtomatik aşkarlayır. Məsələn, Kanadada fəaliyyət göstərən Cybertip.ca platforması süni intellektdən istifadə edərək uşaq istismarına dair məzmunu real vaxtda filtrləyir və hüquq-mühafizə orqanlarına ötürür[23].

Şəbəkə analizi Telegram üçün xüsusilə önəmlidir. Bir kanal və ya qrupda yayılan elan çox vaxt eyni anda digər qruplarda da paylaşılır Məsələn, 2022-ci ildə Polşada Telegram-da "iş elanları" adı ilə fəaliyyət göstərən 50-dən çox qrup izləmə texnologiyası vasitəsilə aşkar edilib və bu qrupların insan alveri şəbəkələrinə bağlılığı sübut olunub. Azərbaycanda isə sosial işçilərin müşahidələri göstərib ki, bəzi Facebook qruplarında eyni telefon nömrəsi ilə təkrar paylaşılan elanlar mövcuddur və bunlar sonradan hüquq-mühafizə orqanları üçün sübut bazasına çevrilib. Bu faktlar izləmə texnologiyalarının praktik əhəmiyyətini bir daha ortaya qoyur.

Nəticə olaraq, kanallar və qruplarda izləmə texnologiyası yalnız texniki vasitə deyil, həm də sosial müdafiənin mühüm hissəsidir. Onun köməyi ilə riskli elanlar aşkarlanır, qurbanların qorunması güclənir və cinayətkar şəbəkələrin fəaliyyəti məhdudlaşdırılır. Akademik tədqiqatlar və beynəlxalq hesabatlar, o cümlədən UNODC-nin 2023-cü il Qlobal Hesabatı və Europol-un 2021-ci il IOCTA sənədi göstərir ki, izləmə texnologiyaları olmadan rəqəmsal mühitdə insan alveri və istismarla effektiv mübarizə mümkün deyil. Həm beynəlxalq təcrübələr, həm də yerli müşahidələr sübut edir ki, rəqəmsal çağırışların artdığı bir dövrdə bu texnologiyalar sosial işçilər, hüquq-mühafizə əməkdaşları və vətəndaş cəmiyyəti üçün zəruri alətə çevrilib.

[23] Cybertip.ca (Kanada, 2022). *Annual Report*.

Teleqramı izləmə texnikası

Telegram Azərbaycanda getdikcə daha geniş yayılan bir platformadır və onun həm açıq, həm də qapalı qrupları və kanalları sosial risklərin izlənməsi üçün mühüm mühit yaradır. Sosial işçilər üçün belə qruplarda və kanallarda monitorinq aparmaq həm potensial qurbanların müdafiəsi, həm də insan alveri və saxta elanların qarşısının alınması baxımından həyati əhəmiyyət daşıyır. Bu məqsədlə izləmə prosesi addım-addım planlaşdırılmalı və hər tapıntı sistemli şəkildə sənədləşdirilməlidir.

İlk mərhələdə hazırlıq işləri aparılmalıdır. Sosial işçi şəxsi hesabından istifadə etməməli, bunun əvəzinə ayrıca işçi hesabı və cihaz ayırmalıdır. Monitorinqin müddəti də öncədən müəyyənləşdirilməlidir: gündəlik qısa yoxlamalar təxminən 15–30 dəqiqə, həftəlik isə daha geniş analiz 1–2 saatlıq olmalıdır. Bundan əlavə, əvvəlcədən açar sözlərin siyahısı hazırlanmalıdır. Azərbaycan reallığında tez-tez rast gəlinən riskli ifadələr "xaricdə iş", "vizasız iş", "hotel işçisi", "hostess", "model axtarılır", "asan qazanc", "sponsor" və "pulsuz təhsil" kimi açar sözlərdir. Bütün tapıntıların qeyd olunacağı xüsusi cədvəl və ya təhlükəsiz fayl da işə başlamazdan əvvəl hazırlanmalıdır.

Axtarış mərhələsində sosial işçi seçilmiş açar sözləri Telegram-ın axtarış bölməsində yazaraq çıxan kanalları və qrupları nəzərdən keçirir. Tapılan nəticələrin adı, linki, üzv sayı və administrator barədə məlumat varsa, qeyd olunur. Bu mərhələdə ilk risk siqnallarını müəyyənləşdirmək vacibdir. Əgər paylaşımlarda "vizasız iş", "sənəd tələb olunmur", "çox yüksək maaş" kimi qeyri-real vədlər varsa, yalnız WhatsApp və ya Telegram nömrəsi göstərilirsə, qrup qapalı və yalnız dəvətlə açılırsa, eyni telefon nömrəsi təkrar paylaşılırsa və ya paylaşımlarda təcili qərar verməyə məcbur edən mesajlar görünürsə, həmin məzmun şübhəli sayılmalıdır.

Şübhəli məzmun aşkarlandıqda dərin yoxlama mərhələsi başlayır. İlk növbədə paylaşımların ekran görüntüləri götürülməli, link və paylaşım tarixi qeyd olunmalıdır. Əgər foto və ya video istifadə olunubsa, onun mənbəyini yoxlamaq üçün "reverse image search" üsulu tətbiq oluna bilər. Elanlarda göstərilən telefon nömrəsi də in-

ternetdə axtarış edilərək eyni nömrənin başqa qruplarda və ya şübhəli elanlarda istifadə olunub-olunmadığı müəyyənləşdirilməlidir. Bu məlumatların hamısı sənədləşdirildikdən sonra tapıntılar təsnif edilir: normal (yaşıl), diqqət tələb edən (sarı) və yüksək riskli (qırmızı).

Növbəti mərhələ hesabatın hazırlanmasıdır. Hər bir şübhəli hal üçün qısa hesabatda qrup və ya kanalın adı, linki, üzv sayı, paylaşım tarixi, ekran görüntüsü, əlaqə məlumatı və niyə şübhəli hesab edildiyi qeyd olunmalıdır. Əgər hadisə yüksək riskli təsnif edilirsə, o zaman dərhal eskalasiya proseduru işə salınmalıdır. Bu, hüquq-mühafizə orqanlarına məlumat vermək, təşkilatın hüquqşünası ilə məsləhətləşmək və ya təcili yardım mexanizmlərini işə salmaq ola bilər. Xüsusilə uşaqların və yeniyetmələrin təhlükədə olduğu hallar təcili reaksiya tələb edir.

İzləmə yalnız qurbanların müdafiəsi ilə məhdudlaşmır, həm də maarifləndirmə funksiyasını daşıyır. Sosial işçi əldə etdiyi nümunələrdən istifadə edərək ictimaiyyət üçün xəbərdarlıq mesajları hazırlaya bilər: məsələn, "saxta iş elanlarını necə tanımalı" və ya "sponsor təklifləri ilə manipulyasiya üsulları" barədə məlumatlandırıcı materiallar hazırlamaq mümkündür. Bu nümunələr real həyat hadisələrinə əsaslandığı üçün həm gənclər, həm də qadınlar üçün daha təsirli olur.

Texniki alətlər də işin bir hissəsidir. Ekran görüntülərinin vaxt və tarixlə saxlanılması, şəkillərin internetdə geri axtarışla yoxlanması, tapıntıların təhlükəsiz fayllarda saxlanılması və məlumatların məxfiliyinin qorunması əsas prinsiplərdəndir. Əlavə olaraq, əgər təşkilatın resursları imkan verirsə, açar söz izləməsini avtomatlaşdırmaq üçün sadə monitorinq botları və ya üçüncü tərəf proqramlarından da istifadə oluna bilər.

Bütün prosesdə etik prinsiplərə əməl etmək vacibdir. Qurbanların şəxsi məlumatları yalnız zəruri hallarda və hüquqi səlahiyyətli qurumlarla paylaşılmalı, heç vaxt ictimaiyyətə açıq şəkildə təqdim olunmamalıdır. Məxfilik və təhlükəsizlik prinsipləri pozulmadan aparılan izləmə həm hüquqi, həm də sosial baxımdan etibarlı nəticə verir.

Yekunda demək olar ki, Telegram qrupları və kanalları geniş

auditoriyaya çıxış imkanı verdiyi üçün həm faydalı, həm də riskli məkan ola bilər. Sosial işçilər üçün addım-addım izləmə planı bu risklərin vaxtında müəyyənləşdirilməsinə, sənədləşdirilməsinə və qurbanların müdafiəsinə xidmət edir. Azərbaycanın sosial reallığında bu alət dəsti hüquq-mühafizə orqanları, QHT-lər və ictimaiyyət arasında koordinasiyalı fəaliyyət üçün praktiki çərçivə rolunu oynaya bilər.

Telegram izləmə hesabatı şablonu
Təşkilat:_____

Hesabatı hazırlayan:_____

Tarix: ____ / ____ / _____

Kanal / Qrup məlumatı
Adı: _____
Link (URL): _____
Üzv sayı: _____
Administrator adı / linki (əgər görünürsə): _____

Şübhəli məzmunun təsviri
Axtarılan açar söz: _____
Paylaşımın tarixi: ____ / ____ / _____
Paylaşımın tipi: ☐ Mətn ☐ Şəkil ☐ Video ☐ Digər
Qısa məzmun təsviri:
Ekran görüntüsü əlavə edildi? ☐ Bəli ☐ Xeyr

Risk siqnalları (işarələyin)

- Qeyri-real vədlər (“vizasız iş”, “heç bir sənəd tələb olunmur”, “çox yüksək maaş”)
- Əlaqə yalnız WhatsApp/Telegram nömrəsi ilə verilib
- Qapalı və yalnız dəvətlə üzvlük
- Təkrar-təkrar eyni elan/nömrə paylaşılır
- Şübhəli profil (saxta şəkil, şəxsi məzmun yoxdur)
- Təcili qərar verməyə məcbur edən mesajlar

➢ Pul və ya sənəd tələbi (pasport, şəxsiyyət vəsiqəsi və s.)

Təsnifat

✓ ☐ Normal (əlavə risk yoxdur)

✓ ☐ Diqqət tələb edir (əlavə monitorinq lazımdır)

✓ ☐ Yüksək risk (dərhal eskalasiya olunmalıdır)

Tədbir və eskalasiya

Qısa qeydlər:

_____

Görülən tədbir:

✓ Monitorinq davam edir

✓ Hüquq-mühafizə orqanına göndərildi

✓ QHT-nin hüquqşünasına yönləndirildi

✓ Maarifləndirici material üçün nümunə kimi saxlanıldı

Əlavə qeydlər / müşahidələr

Bu şablon hər şübhəli kanal/qrup üzrə ayrı-ayrılıqda doldurulmalıdır. Ehtiyac olduqda sübut faylları (screenshot, link) əlavə edilməlidir.

3.2.2.Telefon nömrəsi və əlaqə patternləri

Telefon nömrələri və əlaqə patternləri rəqəmsal cəlb etmə (recruitment) və istismar sxemlərinin çox vaxt ilkin və ən açıq izidir. İnsan alveri və saxta iş elanlarında telefon nömrəsi bir "nexus" — yəni alverçinin qurbanla birbaşa əlaqə qurduğu əsas vasitədir; nömrənin tipi, paylaşıldığı tezlik, mesajlaşma kanalı və nömrənin necə təqdim olunması (şəxsi nömrə, korporativ nömrə, Click-to-Chat linki və s.) hamısı əhəmiyyətlidir. Bu nümunələrin sistemli təhlili "nümunələrin tanınması" (nümunə tanıma) vasitəsilə riskli şəbəkələrin identifikasiyasına yardım edir.

Əvvəlcə texniki və identifikasiya aspektlərinə qısa baxaq: telefon nömrələrinin forması və təqdim edilməsi platformadan-plat-

formaya fərqlənir, amma bir neçə ümumi kateqoriya vardır.

(1) Tam beynəlxalq formatda göstərilən nömrələr — məsələn, +994 50 123 45 67 (Azərbaycan), +90 532 123 45 67 (Türkiyə), +7 495 123 45 67 (Rusiya) — bunlar birbaşa əlaqə üçün real mobil/stasionar nömrələri göstərə bilər;

(2) yerli format (məsələn, 050 123 45 67) — region daxilində hədəfləmə üçün əlverişlidir;

(3) VOIP/virtual nömrələr (məsələn, +44 20 7xx xxxx kimi Qərb kodları ilə verilmiş, amma faktiki operator bilinməyən nömrələr) — saxtakarlıq və izinin gizlədilməsi üçün geniş istifadə olunur;

(4) qısa kodlar və ödəniş/USSD tərzi nömrələr — ödəniş tələb edən sistemlərdə görünə bilər;

(5)Click-to-Chat/WhatsApp linkləri (məsələn, https:// wa.me /994501234567) və Telegram istifadəçi adları (@username) — bu vasitələrlə alverçi qurbanı platformadan çıxarıb birbaşa mesajlaşma kanallarına yönləndirir.

Praktiki pattern nümunələri və onların risk analizini aşağıdakı kimi ümumiləşdirmək olar.

Misal 1 — təkrar nömrə nümunəsi: eyni telefon nömrəsi bir neçə kanal/qrup/posta təkrar-təkrar yapışdırılır. Məsələn, Facebook üzərində "xaricdə iş" qruplarında +90 532 555 66 77 nömrəsi müxtəlif elanlarda 12 dəfə görünürsə və eyni nömrəyə aid WhatsApp linki də paylaşılıbsa, bu, koordinasiyalı cəlb etmənin güclü göstəricisidir. Bu pattern həm yerli, həm də region xaricinə yönələn şəbəkələrdə istifadə olunur: nömrə bir dəfə yaradılır, sonra müxtəlif adı və örtük səhifələri vasitəsilə eyni nömrə ilə yüzlərlə potensial qurbana mesajlar göndərilir. Monitorinq zamanı ən sadə metrik — nömrənin paylaşıldığı unikal say (unique posts/channels) — təyin edilərək threshold (məsələn, 3+) keçərsə prioritetləşdirilməlidir.

Misal 2 — rotasiya və burner-nömrə nümunəsi: alverçilər tez-tez "burner" (müvəqqəti) nömrələrdən istifadə edir — bir neçə gün, həftə və ya ay üçün aktiv olan nömrələr. Məsələn, bir Telegram kanalı üç gün ərzində +971 50 888 99 00 nömrəsini göstərir, sonra başqa bir nömrəyə keçir. Bu pattern izlənildikdə, nömrələr arasında əlaqə qurmaq üçün reverse lookup, təqib edilmiş nömrələrin satın alındığı xidmətlərin müəyyən edilməsi və paylaşımların zamanla-

ması (post timestamp) analiz edilməlidir. Burner patterni daha çox riskli olduğuna görə, qısa yaşayış müddəti + yüksək paylaşımlı istifadə qırmızı bayraqdır.

Misal 3 — müxtəlif ölkə kodlu nömrələr nümunəsi: insan alveri şəbəkələri məkrli olaraq fərqli ölkə kodları istifadə edir ki, hədəf ölkənin qanunvericiliyindən yan keçsin və qurbanı xarici ölkəyə köçürən kimi göstərsin. Məsələn, Azərbaycan istifadəçisinin profili üzərində +48 (Polşa) və ya +90 (Türkiyə) kodlu nömrələr ardıcıl paylaşıla bilər. Bu halda yoxlanmalı: həmin nömrənin operatoru, klik-tarixi, paylaşılan işin ölkə adı ilə uyğunluğu — əks halda "vizasız iş" kimi reklamlar saxtalaşdırılır. Belə pattern həm də qurbanı fiziki olaraq xaricə göndərməyi nəzərdə tutan sxemlərdə çox rast gəlinir.

Misal 4 — əlaqənin yalnız şəxsi messencerə yönləndirilməsi: nümunə — "Müraciət üçün WhatsAppa yazın: +99450 1234567" və eyni postda rəsmi sayt və ya şirkət e-maili yoxdur. Bu patternın təhlükəsi ondan ibarətdir ki, şəxsi messencerə keçid platformanın moderasiya imkanlarını məhdudlaşdırır və şəxsi məlumatların (şəxsiyyət vəsiqəsi, pasport surəti) daha sürətlə toplanmasına şərait yaradır. Həmçinin, WhatsApp/Telegram chatları asanlıqla silinə və mesajlar arxivləşdirilə bilər; buna görə ilk aşamada screenshot + chat timestamp tutmaq, mesajın ID və URL (əgər mövcuddursa) saxlamaq vacibdir.

Misal 5 — Click-to-Call / Click-to-Chat link patterni: alverçilər tez-tez wa.me, tel: və ya Telegram t.me/username linklərini paylaşırlar. Məsələn,
https://wa.me/905321234567?text=I%20am%20interested və ya t.me/joinchat/AAAAAE... kimi. Bu linklər birbaşa əlaqə yaradır və sosial işçilərin dərhal həmin linkin tarixi, hansı postla bağlı olması, kanalda hansı auditoriya ilə paylaşıldığını sənədləşdirməsi lazımdır. Əgər linkin parametrlərində eyni sözdən (məsələn, ?text=job) çoxlu paylaşım varsa, bu şəbəkələşmiş kampaniyanın əlamətidir.

Texniki detektorlar üçün praktik göstəricilər (pragmatik qaydalar). Sosial işçi və monitorinq komandası üçün aşağıdakı meyarlar riskin ilkin skrininqində kömək edəcək:

• Nömrənin təkrarlanma count-u: bir nömrə 3 və daha çox

müstəqil post/kanalda paylaşılıbsa (və ya eyni kanal daxilində tez-tez təkrar olunubsa) prioritetləşdir.

• Nömrənin ölkə-kodunun qeyri-müəyyənliyi: hədəf ölkə ilə uyğun olmayan ölkə kodu və/və ya VOIP kodu şübhə elementi.

• Əlaqə kanalı təkcə messencerdirsə (WhatsApp/Signal/ Telegram DM) və rəsmi əlaqə yoxdursa ciddi siqnal.

• Nömrənin yaş-sürəti: yeni yaradılmış nömrə + yüksək paylaşımlı istifadə — müvəqqəti istifadə nümunəsi.

• Əlavə tələb (pul, sənəd, "sponsor ödənişi"): nömrəyə yazışdıqda öncədən ödəniş və ya sənəd tələb edilirsə qırmızı status.

Nömrə ilə bağlı media nümunəsi: eyni şəkil, eyni mətn şablonu, eyni nömrə birlikdə təkrar-təkrar koordinasiyalı kampaniya.

Bu meyarların tətbiqi praktikada belə görünür: sosial işçi xaricdə iş sözü ilə axtarış edir,, 7 kanal tapılır, hər kanalda eyni +90 532... nömrəsi görünür, eyni nömrəyə aid WhatsApp linkində "rezervasiya üçün 250$" tələb olunur , nəticə: burner/koordinasiyalı pattern + pul tələbi, dərhal hesabat və eskalasiya.

Texniki alətlər və metodlar. Patternləri aşkarlamaq üçün həm sadə, həm də daha mürəkkəb alətlər istifadə edilə bilər:

1. Manuel toplanma və Excel/Google Sheet: hər tapıntı üçün nömrə, kanal adı, post linki, vaxt göstəricisi qeyd olunur, pivot və COUNT funksiyaları ilə hansı nömrənin neçə dəfə paylaşıldığı təyin edilir. (Praktik və süətlidir.)

2. Nömrənin sahibini müəyyənləşdirmə / OSINT xidmətləri: bəzi onlayn alətlər nömrənin qeydiyyatı, operatoru və coğrafi göstəricisini təxmin etməyə kömək edir. VOIP nömrələrdə bu məlumat məhdud ola bilər, amma kömək edir.

3. Şəkil əsasında axtarış: nömrə ilə birlikdə paylaşılan şəkillərin təkrarlandığını aşkar etmək üçün.

4. Avtomatlaşdırılmış monitorinq botları / açar söz toplayıcıları: əgər təşkilatın texniki dəstəyi varsa, açar sözlərə əsaslanan Telegram botları və ya üçüncü tərəf xidmətlər vasitəsilə kanalları avtomatik skrində saxlamaq olar; botlar nömrə çıxarma (phone extraction) və təkrarlanma sayını çıxara bilər.

5. Süni intellekt və NER (Xüsusi adların tanınması): daha inkişaf etmiş yanaşma, postlardan telefon nömrələrini və əlaqə məlu-

matlarını avtomatik aşkarlayan və təsnif edən ML modelləri.

Etika və hüquqi məqamlar. Telefon nömrələrinin toplanması və saxlanması həssas məlumat hesab edilə bilər — buna görə:

• Məxfilik və qanunvericilik: şəxsi məlumatların toplanması və paylaşılması yerli qanunlara uyğun aparılmalıdır. Qurbanın razılığı olmadan şəxsi məlumatların yayılması qadağandır.

• Sübutların saxlanması: ekran görüntüləri şifrəli və məhdud girişli yaddaşda saxlanmalı, hüquq-mühafizə orqanlarına təqdim edərkən chain-of-custody (sübut zənciri) nəzərə alınmalıdır.

• Məişət təhlükəsizliyi: qurbanla əlaqə qurulanda onun təhlükəsizliyi prioritet olmalıdır — tək görüşə getmə, dərhal pul göndərmə və şəxsiyyət sənədi paylaşma kimi məsləhətlər verilməlidir.

Praktiki yoxlama və əməkdaşlıq tövsiyələri (step-by-step nümunə): bir sosial işçi tapıntını necə idarə etməlidir — qısa, konkret addımlar:

1. Aşkarlama: postun screenshotunu götür (tarix görünməlidir).
2. Köcür: post linkini və kanal/qrup adını qeyd et.
3. Çıxarmaq: post mətnindən nömrəni çıxar və beynəlxalq formata çevir (+994501234567).
4. Təkrar yoxlama: həmin nömrəni digər kanallarda/forumlarda axtar (platforma içi axtarış, Google, nömrənin sahibini müəyyənləşdirmə).
5. Nümunə analizi: nömrə neçə unikal postda görünür? hansı zaman intervallarında paylaşılıb? eyni mətn və şəkillərlə birlikdədir?
6. Təsnif et: uyğun kriteriyalar əsasında Yaşıl/Sarı/Qırmızı qərarı ver.
7. Eskalasiya: Qırmızı halda təşkilatın proseduruna uyğun DİN/hüquqşünas/sığınacaqla əlaqə.
8. Maarifləndir: nümunəni anonimləşdirərək maarifləndirmə materialına çevir.

Sonda bir neçə tez-tez rast gəlinən konkret nümunə-ssenari verək ki, praktik iş asanlaşsın:

A ssenarisi: Facebook qrupunda “xaricdə iş — 2000$/həftə”

postu; əlaqə +99450 1234567; eyni nömrə digər 4 qrupda da var.

Nümunə*:* təkrar nömrə + qeyri-real vəd → yüksək risk.

B ssenarisi: Telegram kanalında t.me/joinchat/AAA… link ilə birlikdə wa.me/905321234567 paylaşılıb; kanalda üzv sayı çoxdur, amma admin anonimdir.

Nümunə*:* Click-to-Chat + anonim admin → diqqət tələb edir, reverse image + nömrə lookup lazım.

C ssenarisi:: "Model axtarılır" elanında +7 495 111 22 33 (Rusiya) nömrəsi verilir; elan Azərbaycan publikasiyasında yayımlanır; WhatsApp-a yazmaq üçün çağırış var.

Nümunə*:* ölkə kodunun uyğun gəlməməsi + şəxsi messencerə yönləndirmə → riskli, qısa müddətdə araşdırılmalıdır.

D ssenarisi:: Eyni şəkil 12 kanalda paylaşılıb, lakin əlaqə olaraq hər dəfə fərqli VOIP nömrə () göstərilir.

Nümunə*:* şəkil paylaşımı + rotasiya edilmiş burner nömrələr → yüksək peşəkarlıq; hüquq-mühafizə ilə koordinasiya məsləhətdir.

3.2.3. Şübhəli elan nümunələri

Şübhəli elanlar müasir rəqəmsal mühitdə insan alveri, fırıldaqçılıq və istismar hallarının ən çox rast gəlinən formalarından biridir. Onlar adətən real iş təklifləri, təhsil və ya sponsorluq elanlarının arxasında gizlənərək qurbanların diqqətini cəlb edir və etimadını qazanmağa çalışır. Akademik tədqiqatlar göstərir ki, insan alverçiləri saxta elanlardan əsasən üç məqsəd üçün istifadə edirlər: ilkin əlaqə yaratmaq, etibar qurmaq və qurbanı offline mühitə çəkmək. Belə elanlar həm açıq sosial şəbəkə qruplarında, həm də qapalı messencer kanallarında rast gəlinir.

Tipik nümunələr arasında "xaricdə vizasız iş" elanları xüsusi yer tutur. Məsələn, "Türkiyədə otel işçisi tələb olunur, vizasız qəbul, aylıq maaş 2000 dollar, yalnız pasport kifayətdir" kimi elanlar bir çox gəncin və qadının diqqətini çəkə bilir. Reallıqda isə belə iş şərt-

ləri qeyri-mümkündür, çünki rəsmi iş vizası olmadan yüksək maaşlı işlər təklif edilmir. Europol-un 2021-ci il *IOCTA* hesabatında qeyd olunur ki, bu tip elanlar qurbanı qeyri-leqal əmək bazarına cəlb etmək və daha sonra borc əsarəti və ya istismara məruz qoymaq üçün istifadə olunur.

Başqa bir nümunə "model və ya hostes axtarılır" elanlarıdır. Burada tez-tez "yaş aralığı 18–25, xarici ölkədə iş, bütün xərclər qarşılanır" kimi cəlbedici şərtlər vurğulanır. Əslində isə bu elanlar qadınların cinsi istismara cəlb olunmasının klassik formalarından biridir. ATƏT-in araşdırmaları göstərir ki, belə elanlarda tez-tez saxta fotoşəkillər istifadə olunur və əlaqə yalnız WhatsApp nömrəsi ilə verilir. Bu, sosial işçilərin diqqət yetirməli olduğu açıq siqnallardan biridir.

Digər bir tez-tez rast gəlinən nümunə "asan qazanc" və ya "online iş" elanlarıdır. Burada elanlar qısa müddətdə yüksək qazanc vəd edir: "Gündəlik 300 dollar qazanmaq istəyirsən? Evdən çıxmadan sadəcə mesaj göndərməklə pul qazan!" Bu elanların arxasında çox vaxt "piramida sxemi" və ya insan alverçilərinin psixoloji manipulyasiyası dayanır. Qurban əvvəlcə "kiçik ödəniş" etməyə razı salınır, sonra isə davamlı olaraq yeni şərtlərlə qarşılaşır. EIGE-nin (2022) "Cyber violence against women and girls" hesabatında göstərilir ki, qadınların əhəmiyyətli bir hissəsi belə elanların qurbanına çevrilir, nəticədə həm maliyyə, həm də psixoloji itkilərlə üzləşirlər.

Azərbaycan reallığında da bu nümunələr geniş yayılıb. Facebook və Telegram kanallarında "Polşada iş", "BƏƏ-də otel işçisi", "Avropada qızlar üçün iş" kimi elanlara tez-tez rast gəlinir. Monitorinq zamanı müşahidə olunur ki, eyni telefon nömrəsi və ya eyni mətn müxtəlif qruplarda təkrar paylaşılır. Bu, saxta elan şəbəkələrinin fəaliyyətini göstərən tipik pattern-dir. Sosial işçilər üçün əsas göstəricilərdən biri də budur: təkrar istifadə olunan əlaqə məlumatı, qeyri-real vədlər və şəffaf olmayan şərtlər.

Beləliklə, şübhəli elanların mahiyyəti onların cazibədar görünməsinə baxmayaraq, faktiki olaraq qurbanların istismarına aparan aldatma mexanizmi olmasıdır. Onların vaxtında müəyyənləşdirilməsi yalnız fərdlərin təhlükəsizliyini deyil, həm də cəmiyyətin bütövlükdə istismardan qorunmasını təmin edir. Akademik mənbə-

lər və praktiki müşahidələr göstərir ki, şübhəli elanları tanımağın əsas üsulları qeyri-real şərtlərə, əlaqə patternlərinə və saxta vizual elementlərə diqqət yetirməkdir. Bu, sosial işçilər, hüquq-mühafizə əməkdaşları və QHT-lər üçün qurbanların müdafiəsində ən vacib başlanğıc nöqtələrdən biridir**.**

Nümunələr.

▪ "Tələbə vizası ilə xaricdə oxu və işlə" elanları. Məzmun: "Avropada təhsil + iş imkanı. Heç bir imtahan və sənəd tələb olunmur. Bütün xərclər ödənilir."

Təhlükə: Belə elanlar gəncləri aldadaraq qeyri-qanuni miqrasiya kanallarına yönəldir. UNODC hesabatında vurğulanır ki, tələbə vizası adı altında qurbanların təhsilə yox, qeyri-leqal işlərə və istismara məruz qaldığı çoxlu hallar qeydə alınıb.

▪ Evlilik vasitəsilə xaricdə həyat" elanları Məzmun: "Xaricdə yaşayan imkanlı şəxslə tanışlıq. Gənc xanımlara evlilik imkanı. Yaş məhdudiyyəti: 18–30."

Təhlükə: Bu elanların əksəriyyəti qurbanları "cəlbetmə və manipulyasiya prosesi" yolu ilə emosional asılılığa salaraq istismara gətirib çıxarır. ATƏT qeyd edir ki, belə elanlarda məqsəd qadınları əvvəlcə nikah və ya münasibət vədi ilə cəlb etmək, sonra isə məcburi əmək və ya cinsi istismara məruz qoymaqdır.

▪ "Au-pair" və ya "uşaq baxıcısı" elanları. Məzmun: "Avropada ailə yanına dayə tələb olunur. Heç bir təcrübə şərt deyil. Yüksək maaş. Vizaya ehtiyac yoxdur."

Təhlükə: Qurban ailə yanında işləmək adı ilə xaricə aparılır, lakin orada məcburi əmək, fiziki zorakılıq və sənəd müsadirəsi ilə üzləşir. Europol vurğulayır ki, xüsusilə gənc qızlar belə elanların hədəfinə çevrilir.

▪ "Sponsor və hədiyyə" elanları. Məzmun: "Xanımlara maddi

dəstək. Aylıq ödəniş 1000 dollar. Şərt: ünsiyyət və görüşlər."

Təhlükə: Bu tip elanlar tez-tez cinsi istismar məqsədilə qurulur. EIGE hesabatına görə, onlayn sponsorluq elanları qızları "sextortion" (seksual təzyiq və şantaj) riski ilə üz-üzə qoyur.

- "Könüllü iş və ya xeyriyyə layihəsi" elanları. Məzmun: "Afrikada könüllü iş. Təcrübə tələb olunmur, yalnız səyahət bileti almalısan."

Təhlükə: Qurban "humanitar iş" adı ilə istismar mühitinə salınır. Bəzi hallarda isə saxta QHT-lər vasitəsilə həm pul, həm də şəxsi məlumatlar toplanır.

- "Sosial media influencer" və ya "brend ambassador" elanları. Məzmun: "Gənc qızlar üçün beynəlxalq brend ambassador layihəsi. Foto çəkilişlər və səyahət təmin olunur."

Təhlükə: Bu elanların bir çoxu əslində "casting scam" formasında cinsi istismara aparır. ECPAT Internationalın araşdırmalarda göstərilib ki, onlayn "model axtarışı" elanlarının əhəmiyyətli hissəsi uşaq və yeniyetmələri istismara hədəfləyir.

- "Kripto / onlayn sərmayə" elanları. Məzmun: "Sadəcə 100 dollar yatır və həftədə 1000 dollar qazan. Ödənişlər birbaşa kartına köçürüləcək."

Təhlükə: Bu elanlarda maliyyə fırıldaqları ilə yanaşı, bəzən qurbanın şəxsiyyət sənədi və bank məlumatları da ələ keçirilir. UNODC xəbərdarlıq edir ki, rəqəmsal maliyyə alətləri son illərdə insan alveri şəbəkələrinin yeni cəlb üsullarına çevrilib.

Şübhəli elanların mahiyyəti dəyişsə də, onların ortaq xüsusiyyətləri var: qeyri-real şərtlər, şəffaf olmayan əlaqə vasitələri (yalnız WhatsApp/Telegram), saxta fotoşəkillər və qurbanı sürətli qərar verməyə məcbur edən mətnlər. Bu nümunələr həm beynəlxalq hesa-

batlarda, həm də Azərbaycan reallığında müşahidə olunan hallarda təsdiqini tapır.

3.3. Instagram

İnstagram müasir dövrdə dünyanın ən populyar sosial şəbəkələrindən biridir və həm şəxsi ünsiyyət, həm də biznes və ictimai fəaliyyətlər üçün geniş istifadə olunur.

Instagram 2010-cu ilin oktyabrında ABŞ-da Kevin Systrom və Mike Krieger tərəfindən yaradılıb. Əvvəlcə sadəcə foto paylaşmaq üçün mobil tətbiq kimi nəzərdə tutulmuşdu. 2025-ci ilə olan məlumata görə, Instagram-ın aylıq aktiv istifadəçi sayı 2,4 milyarddan çoxdur. Bu göstərici onu dünyanın ən böyük sosial media platformalarından biri edir. İstifadəçilərin böyük əksəriyyəti 18–34 yaş aralığında olan gənclərdir. Bu, Instagramı xüsusilə gənc auditoriyaya təsir edən bir platforma halına gətirir. Platforma 190-dan çox ölkədə əlçatandır və 30-dan çox dili dəstəkləyir. İnstagram həm də biznes üçün çox güclü alətə çevrilib: dünyada 200 milyondan çox biznes səhifəsi (business account) aktivdir. Başlanğıcda sadəcə foto paylaşımı ilə məhdudlaşsa da, sonrakı illərdə videolar, Stories (24 saatlıq paylaşımlar), IGTV (uzun video formatı), Reels (qısa videolar, TikTok-a rəqib) və birbaşa mesajlaşma funksiyaları əlavə olundu. Həmçinin, "Instagram Shop" funksiyası vasitəsilə istifadəçilər platforma üzərindən məhsul da ala bilirlər.

Azərbaycanda da Instagram ən populyar sosial media platformalarından biridir. 2024-cü ilin statistikasına görə, ölkədə təxminən 3,45 milyon aktiv istifadəçi var ki, bu da əhalinin təqribən 33%-ni təşkil edir. İstifadəçilərin çoxu 18–34 yaş aralığındadır və xüsusilə Bakı kimi iri şəhərlərdə daha geniş yayılıb. Azərbaycanda Instagram həm gənclər arasında ünsiyyət vasitəsi, həm də kiçik bizneslərin reklam və satış platforması kimi önə çıxır.

Instagram insan alverçiləri üçün çox əlverişli mühit ola bilər — niyə və necə olduğuna qısa, əsaslandırılmış və misallı izah təqdim edək.

Instagram vizual əsaslı, gənc auditoriyalı və sürətlə yayılan

məzmun platformasıdır; bu üç xüsusiyyət alverçilərin işini xeyli asanlaşdırır. İlk növbədə Instagram şəkillər, qısa videolar (Reels) və hekayələr vasitəsilə etibarlı və cəlbedici "şəxsiyyət"lər yaratmağa imkan verir. Saxta modellər, "iş təklif edən" profillər və ya "sponsorlar" həqiqi görünə bilir, bu isə qurbanın etibarını qısa müddətdə qazanmağa xidmət edir[24].

İkincisi, platforma şəxsi mesajlaşma (Direct Message) imkanları və "click-to-chat" davranışları ilə (bio-da linklər, story-də nömrə/WhatsApp linki) profildən birbaşa, platformadan kənar ünsiyyətə keçidi asanlaşdırır — bu da moderasiyanı və izlənməni çətinləşdirir. Polaris və oxşar təşkilatlar bu cür birbaşa mesajlaşmanın qurbanı izolyasiya edib manipulyasiya üçün ən çox istifadə olunan yol olduğunu vurğulayır[25].

Üçüncüsü, Instagram alqoritmləri istifadəçiyə "oxşar məzmun" göstərmək üçün qurulub; bir istifadəçi müəyyən tip məzmunla qarşılaşdıqda (məsələn, "model axtarışı" və ya "xaricdə iş" postları), ona oxşar paylaşımlar daha çox tövsiyə olunur — bu da hədəf seçilmiş şəxsin riskə məruz qalma sürətini artırır. Bundan əlavə, hashtag'lar, lokasiya etiketləri və influencer şəbəkələri vasitəsilə elanlar sürətlə geniş auditoriyaya yayılır. Europol/UNODC və digər tədqiqatlar göstərir ki, sosial media (o cümlədən Instagram) insan alverinin bütün mərhələlərində — cəlbetmə_ nəzarətə qədər — istifadə olunur.

Praktik nümunələr (real dünya sübutlarına əsasən):

• "Pimps" və təşkilatlı qruplar özlərini Instagram-da reklam edərək qurbanları "grooming"lə əldə ediblər; bəzi qlobal istintaqlarda bu hesabların hətta məhkum şəxslər tərəfindən idarə olunması aşkar edilib[26].

• Meta-nın daxili sənədləri və jurnalistik araşdırmalar platformada hər gün on minlərlə uşağın seksuallığa məruz qoyulduğunu göstərir — bu, Instagram-da uşaqların və yeniyetmələrin xüsusi risk

[24] https://www.theguardian.com/global-development/2024/mar/05/pimps-use-instagram-to-glorify-sexual-violence-and-abuse-investigation-finds

[25] https://polarisproject.org/human-trafficking-and-social-media

[26] https://www.theguardian.com/technology/2024/jan/18/instagram-facebook-child-sexual-harassment

altında olduğunu təsdiqləyir.

• Qlobal hesabatlar ümumi tendensiyanı təsdiqləyir: internet və sosial media insan alverçilərinin rekrutment üçün getdikcə ilk seçiminə çevrilib.

Niyə xüsusilə Instagram təhlükəlidir:

✓ Vizual inandırıcılıq (ideal profil təsvirləri, influencer estetikası).

✓ Birbaşa mesajlaşma ilə platformadan kənara çıxmaq (WhatsApp, Telegram və s.).

✓ Alqoritmik təkliflər və hashtag/lokasiya vasitəsilə sürətli yayılma.

✓ Gənc istifadəçi bazası (18–34), uşaqlar və yeniyetmələrə yüksək çıxış.

✓ Saxta reklam və "sponsored" postların, habelə burner hesabların rahat istifadəsi.

Instagram həm effektiv maarifləndirmə və qruplaşma kanalı ola bilər, həm də insan alverçilərinə yüksək effektivliklə qurban cəlb etməyə imkan verən alət. Beynəlxalq hesabatlar və jurnalistik araşdırmalar göstərir ki, platformanın strukturu (vizuallıq, DM, alqoritm tövsiyələri) istismar üçün əlverişli şərait yaradır və buna görə də hədəf qrupların qorunması üçün xüsusi monitorinq və təhsil tədbirləri vacibdir.

Hüquq-mühafizə orqanına göndəriləcək məktub--şablonu

Mövzu: Şübhəli Instagram elan(lar)ı barədə məlumat

Hörmətli [qurumun adı] nümayəndələri,

[Təşkilatınızın adı] tərəfindən aparılan onlayn monitorinq zamanı Instagram platformasında insan alveri və saxta iş təklifləri ilə bağlı şübhəli elan(lar) aşkarlanmışdır.

Əsas məlumatlar:

- Elanın linki: _____
- Səhifə / profil adı: _____
- Paylaşım tarixi: ____ / ____ / _____
- Əlaqə məlumatı: __ (telefon nömrəsi / WhatsApp / e-mail)
- Qısa məzmun təsviri:

_____

- Şübhəli siqnallar: (qeyri-real maaş vədi, vizasız iş, sənəd və ya pul tələbi, saxta foto və s.)

Əlavə olunub:

- Ekran görüntüləri (screenshot)
- Əlavə qeydlər (əgər varsa)

Xahiş edirik, bu məlumatların araşdırılması və müvafiq tədbirlərin görülməsi üçün tərəfimizlə əməkdaşlıq edəsiniz. Lazım gələrsə, əlavə sübutlar təqdim etməyə hazırıq.

Hörmətlə,

Ad,Soyad_____

_____

Vəzifə:_____

Təşkilatın adı_____

Əlaqə: _____

3.3.1. Hashtag izləmə

Hashtag izləmə texnologiyası müasir rəqəmsal mühitdə sosial medianın həm imkanlarını, həm də təhlükələrini anlamaq baxımından xüsusi əhəmiyyət daşıyır. Hashtag, yəni "#" işarəsi ilə başlayan açar söz və ya ifadə, ilk dəfə 2007-ci ildə Twitter-də tətbiq olunsa da, bu gün Instagram, Facebook, TikTok, Telegram kimi müxtəlif platformalarda geniş istifadə olunur. Onun əsas funksiyası paylaşımları mövzu üzrə qruplaşdırmaq və axtarışı asanlaşdırmaqdır. Lakin bu texnologiya təkcə istifadəçilərə məzmunu tapmaq üçün deyil, həm də sosial risklərin izlənməsi, insan alveri və saxta elanların aşkarlanması üçün mühüm alət rolunu oynayır.

Hashtag-ların izlənməsi sosial işçilərə və hüquq-mühafizə orqanlarına bir neçə üstünlük verir. Birincisi, sadə axtarış vasitəsilə konkret açar sözlərə əsaslanan paylaşımları görmək mümkündür. Məsələn, Azərbaycanda "#xaricdəiş", "#Polşadaİş", "#Türkiyədəo-

tel" kimi hashtag-lar altında tez-tez vizasız iş elanları yerləşdirilir. Bu elanların əksəriyyəti qeyri-real şərtlər təqdim edir və əlaqə vasitəsi kimi yalnız WhatsApp nömrəsini göstərir.

İkincisi, birdən çox hashtag-ın birlikdə istifadəsi daha dəqiq nəticələr verir. Məsələn, #job + #abroad və ya #visa + #easyprofit kombinasiyası sosial şəbəkələrdə potensial saxta elanların tez aşkarlanmasına imkan yaradır.

Üçüncüsü, avtomatlaşdırılmış izləmə sistemləri, API-lər və ya monitorinq alətləri vasitəsilə hashtag-ların real vaxtda analizi aparıla bilər. Belə texnologiyalar trend qrafiklərini çıxarmağa, ən çox paylaşılan məzmunu görməyə və aktiv istifadəçiləri müəyyənləşdirməyə imkan verir.

Kriminal şəbəkələr hashtag texnologiyasından manipulyasiya məqsədilə istifadə edirlər. Europol-un 2021-ci il hesabatında qeyd olunur ki, alverçilər tez-tez trend hashtag-ları dəyişdirilmiş formada işlədərək daha çox insana çatmağa çalışırlar. Bu, xüsusilə "kodlaşdırılmış hashtag"larda özünü göstərir. Məsələn, #newlife, #visaFree və #dreamjob kimi ifadələr zahirən adi görünür, amma əslində qurban cəlb etmə alətinə çevrilir. Eyni hal model və casting elanlarında da müşahidə olunur: #modelsearch və #castingcall altında saxta elanlar yerləşdirilərək gənc qızların foto və şəxsi məlumatları toplanır. Həmçinin, #easyprofit, #cryptoJob kimi hashtag-lar altında tez-tez piramida sxemləri və qeyri-real gəlir vədləri gizlədilir.

UNODC-nin 2023-cü il İnsan alveri üzrə Global hesabatında qeyd olunur ki, qurbanların təxminən 41%-i açar sözlər və hashtaglar vasitəsilə cəlb edilir. EIGE-nin 2022-ci il araşdırması göstərir ki, qadınlar və qızlar bu manipulyasiyaların əsas hədəfinə çevrilirlər. ATƏT isə 2021-ci ildəki siyasət sənədində xəbərdarlıq edir ki, hashtag-lar üzərindən aparılan "recruitment" üsulları getdikcə daha incə və daha az görünən formalar alır.

Azərbaycan kontekstində hashtag izləməsi xüsusilə önəmlidir. Çünki yerli sosial media məkanında işsizlik, xaricdə təhsil və sürətli qazanc kimi mövzular çox aktualdır. Bu isə insan alverçilərinin tez-tez "#xaricdəiş", "#Bakıjob", "#Polşadaotel" kimi etiketlərdən istifadə etməsinə şərait yaradır. Sosial işçilər bu hashtag-ların monitorinqini aparmaqla riskli elanları vaxtında müəyyən edə və sübut top-

laya bilərlər. Bu, həm qurbanların qorunması, həm də ictimaiyyətin maarifləndirilməsi üçün effektiv üsuldur.

Yekunda demək olar ki, hashtag izləmə texnologiyası sadəcə məzmun kəşfiyyatı üçün deyil, həm də sosial təhlükəsizliyin təmin edilməsi üçün strateji vasitədir. Onun gücü həm sadə axtarış, həm kombinə edilmiş filtrlər, həm də avtomatlaşdırılmış alətlərlə artırıla bilər. Sosial işçilər və hüquq-mühafizə orqanları hashtag-ları izləməklə istismar şəbəkələrinin fəaliyyətini daha erkən mərhələdə aşkar edə və qurbanların müdafiəsi üçün vaxtında tədbir görə bilərlər.

Sadə axtarış yolu ilə izləmə. Hashtagları birbaşa platformanın axtarış bölməsinə yazmaqla müvafiq paylaşımlar izlənə bilər. Məsələn:

- #xaricdəiş
- #modelaxtarılır
- #easyjob

Bu üsul sosial işçilər üçün ilkin və sürətli monitorinq imkanı yaradır.

Böyl və kombinə edilmiş izləmə. Tək hashtag ilə yanaşı, birdən çox hashtag-ın birlikdə istifadəsi daha dəqiq nəticə verir. Məsələn, Instagram-da #job + #abroad və ya #visa + #easyprofit kombinasiya edilərək saxta iş elanları daha tez müəyyən edilə bilər.

Avtomatlaşdırılmış izləmə (API və bot texnologiyaları). Platformaların açıq API-ləri və ya xüsusi izləmə alətləri (məsələn, Brandwatch, Hootsuite, Talkwalker) vasitəsilə hashtag-ların real vaxtda analizi mümkündür. Bu texnologiyalar trend qrafikləri, ən çox paylaşılan postlar və ən aktiv istifadəçiləri müəyyənləşdirə bilir.

Pattern tanıma və məzmun analizi. Bəzi hallarda hashtaglar konkret qrup və ya cinayətkar şəbəkələrin izini göstərir. Məsələn, insan alverçiləri tez-tez "kodlaşdırılmış hashtag"lardan istifadə edirlər: #newlife, #visaFree, #dreamjob. İlk baxışdan adi görünsə də, bu hashtag-lar qurban cəlb etmək üçün sistemli şəkildə istifadə olunur.

Risk və real nümunələr

İnsan alveri elanları: Azərbaycanda da tez-tez "#xaricdəiş", "#PolşadaİŞ", "#Türkiyədəotel" kimi hashtag-lar altında vizasız iş elanları paylaşılır. Monitorinq göstərir ki, bu paylaşımların əksəriyyətində əlaqə məlumatı yalnız WhatsApp nömrəsi ilə verilir.

Cinsi istismar və "model" elanları: Instagram və TikTok-da #modelsearch, #castingcall kimi hashtag-lar altında saxta elanlar yerləşdirilir. Bu tip elanların bir qismi qızların foto və şəxsi məlumatlarını toplamaq üçün nəzərdə tutulur[27].

Maliyyə fırıldaqları: #easyprofit, #cryptoJob və oxşar hashtag-lar altında tez-tez piramida sxemləri və qeyri-real gəlir vədləri gizlədilir.

3.3.2. Hashtag izləmə aləti (Checklist)

1. Hazırlıq mərhələsi

☐ İş üçün ayrıca sosial media hesabı yaradın (şəxsi hesabdan istifadə etməyin).

☐ Əvvəlcədən izlənəcək riskli hashtag-ların siyahısını hazırlayın (məsələn: #xaricdəiş, #visaFree, #easyprofit, #modelsearch, #dreamjob).

☐ Bütün tapıntıların qeyd ediləcəyi təhlükəsiz fayl və ya hesabat forması hazırlayın.

2. Axtarış və ilkin monitorinq

☐ Seçilmiş hashtag-ları sosial platformaların axtarış bölməsində yoxlayın.

☐ Ən çox paylaşılan postları və aktiv istifadəçiləri qeyd edin.

[27] OSCE (2021). *Policy responses to online exploitation.*

☐ Şübhəli məzmun aşkar olunarsa, ekran görüntüləri götürün.

3. Risk siqnallarını yoxlama

☐ Qeyri-real vədlər varmı? (“vizasız iş”, “çox yüksək maaş”, “asan qazanc”)

☐ Əlaqə yalnız WhatsApp/Telegram nömrəsi ilədir?

☐ Saxta və ya təkrar istifadə olunan fotoşəkillər görünürmü?

☐ Təcili müraciət çağırışı varmı? (“indi müraciət et”, “son şans”)

☐ Eyni məzmun bir neçə hashtag və ya səhifədə təkrar paylaşılıbmı?

4. Sənədləşdirmə

☐ Hər şübhəli paylaşımın linkini, tarixini və mətnini qeyd edin.

☐ Telefon nömrələri və ya digər əlaqə vasitələrini ayrıca çıxarın.

☐ Ekran görüntülərini arxivləşdirin.

5. Təsnifat

☐ Normal (risk siqnalları yoxdur)

☐ Diqqət tələb edir (əlavə monitorinq lazımdır)

☐ Yüksək risk (dərhal eskalasiya edilməlidir)

6. Tədbir və eskalasiya

☐ Yüksək riskli halları dərhal rəhbərliyə və hüquq-mühafizə orqanlarına yönləndirin.

☐ Təkrar paylaşılan və geniş yayılan riskli hashtag-lar barədə qısa xəbərdarlıq hesabatı hazırlayın.

☐ Maarifləndirici mesaj üçün nümunə saxlayın (məsələn, “saxta iş elanlarını tanımaq yolları”).

Bu checklist hər monitorinq seansı üçün tətbiq edilməlidir. Aşkar edilən hallar müntəzəm olaraq hesabatlaşdırılmalı və təhlükəsizlik prinsiplərinə uyğun şəkildə saxlanılmalıdır.

3.3.3. Bio və geotag izləmə

Bio və geotag izləmə rəqəmsal monitorinqdə xüsusi əhəmiyyət daşıyan üsullardan biridir və həm akademik, həm də praktik baxımdan sosial işçilər və hüquq-mühafizə orqanları üçün mühüm imkanlar açır. Bu metodlar insan alveri, saxta elanlar, riskli qruplar və potensial qurbanların müəyyənləşdirilməsində istifadə olunur.

İlk olaraq bio izləmə (profil təsviri analizi) haqqında danışaq. "Bio" sosial media hesablarında istifadəçinin özünü təqdim etdiyi qısa təsvir sahəsidir. Bu hissədə istifadəçilər adətən peşə, maraq dairəsi, əlaqə məlumatı və ya motivasiyaedici mesaj yerləşdirirlər. Lakin saxta profillərdə bio çox vaxt manipulyativ məzmun daşıyır. Məsələn, insan alverçiləri "model axtarışı", "xaricdə iş", "sponsor dəstəyi" kimi sözlərdən istifadə edərək bio hissəsini reklam lövhəsinə çevirirlər. Bəzi hallarda isə əlaqə nömrəsi və ya WhatsApp linki birbaşa bioya yerləşdirilir. UNODC-nin araşdırmalarına görə, sosial mediada insan alveri hallarında qurbanların 38%-i ilkin təmasa məhz belə profillər vasitəsilə cəlb olunur. Azərbaycanda da monitorinqlər göstərir ki, "#iş" və "#model" etiketi ilə paylaşılan bio-ların əhəmiyyətli qismi qeyri-real vədlərdən ibarətdir.

İkinci mühüm istiqamət geotag izləmədir. Geotag (coğrafi etiket) istifadəçinin paylaşımına əlavə olunan məkan məlumatıdır. Bu məlumat həm açıq, həm də gizli formada ola bilər. Açıq formada o zaman görünür ki, istifadəçi paylaşımına "Bakı", "İstanbul Hava Limanı", "Polşa – Varşava" kimi lokasiya əlavə edir. Gizli formada isə şəkil və ya video faylın "metadata" hissəsində saxlanılır və xüsusi texniki vasitələrlə çıxarıla bilər. Geotag izləməsi sosial risklərin aşkarlanmasında vacibdir, çünki bu məlumat vasitəsilə şübhəli elanların və ya qurbanların harada yerləşdiyi barədə ilkin ipucları əldə olunur. Europolun hesabatına əsasən, insan alveri ilə məşğul olan şəbəkələrin 22%-i potensial qurbanları məhz lokasiya əsaslı paylaşımlar vasitəsilə izləyir və manipulyasiya edir.

Praktik nümunələr göstərir ki, geotag izləməsi xüsusilə riskli elanların təhlilində faydalıdır. Məsələn, Telegram və Instagramda "xaricdə iş" elanları çox vaxt eyni şəhər və ya məkan etiketi ilə paylaşılır. Əgər bir neçə profil ardıcıl olaraq "Varşava" və ya "Dubay"

geotag-lı paylaşımlar edirsə, bu, həmin regionlarda fəaliyyət göstərən şəbəkə ilə bağlı ola bilər. Azərbaycan reallığında da "#Bakı" və "#Sumqayıt" etiketi altında şübhəli sponsorluq elanları müşahidə olunub. Bu, göstərir ki, bio və geotag izləməsi yalnız xaricdəki riskləri deyil, ölkədaxili manipulyasiyaları da aşkarlamağa imkan verir.

Akademik əsaslandırma baxımından qeyd etmək lazımdır ki, bio və geotag izləmə metodları "sosial media kəşfiyyatı" (SOCMINT) anlayışının əsas elementlərindəndir. ATƏT vurğulayır ki, bu üsullar erkən xəbərdarlıq sistemi kimi işlədilməli və hüquqi çərçivə ilə dəstəklənməlidir. EIGE isə bio və geotag analizini xüsusilə qadın və qızların rəqəmsal mühitdə qorunması üçün prioritet metodlardan biri hesab edir[28].

Yekun olaraq demək olar ki, bio və geotag izləmə texnologiyası sosial işçilərə iki vacib imkan verir: birincisi, qurbanların necə cəlb olunduğunu anlamaq (bio vasitəsilə manipulyativ təsvirlər); ikincisi, riskin hansı məkanlarda cəmləşdiyini müəyyənləşdirmək (geotag vasitəsilə lokasiya təhlili). Bu üsullar birlikdə tətbiq olunduqda daha dolğun təsəvvür yaradır və həm fərdi, həm də institusional səviyyədə insan alverinə qarşı mübarizədə güclü alət kimi çıxış edir.

Bio və Geotag yoxlama siyahısı

1. Bio (profil təsviri) yoxlaması

- Profil bio hissəsində "vizasız iş", "sponsor", "model axtarılır", "asan qazanc" kimi ifadələr varmı?
- Əlaqə vasitəsi (WhatsApp/Telegram nömrəsi, link) birbaşa bioya yerləşdirilibmi?
- Bio çox ümumi və şablon mətnlərdən ibarətdirmi ("New life", "Travel easy", "Work abroad")?
- Saxta etibar qazanmaq üçün "CEO", "agentlik", "internasional" kimi qondarma titullar istifadə olunubmu?
- Şəxsi məlumat yoxdur, amma intensiv reklam yönümlü təsvirlər verilibmi?

[28] EIGE (2022). *Cyber violence against women and girls*.

Geotag (məkan etiketi) yoxlaması

- Paylaşımlarda tez-tez eyni xarici məkanlar göstərilirmi (məsələn: “Varşava”, “Dubay”, “İstanbul”)
- Qısa müddətdə bir profilin bir neçə ölkədən geotag istifadə etməsi şübhəli görünürmü?
- Yerli kontekstdə riskli məkanlar (məsələn: “Bakı”, “Sumqayıt”) altında sponsorluqelanları paylaşılıbmı?
- Eyni məkan etiketi bir neçə şübhəli profil tərəfindən təkrar istifadə olunubmu?
- Metadata yoxlaması zamanı (foto/video fayllarda) gizli lokasiya məlumatı aşkar edilirmi?

Tədbirlər

- Şübhəli bio və ya geotag-ların ekran görüntülərini götürün.
- Linkləri və tarixləri ayrıca qeydə alın.
- Eyni məlumat bir neçə profildə təkrarlanırsa, ayrıca “pattern” faylı yaradın.
- Yüksək riskli halları rəhbərliyə və hüquq-mühafizə orqanına ötürün.

Bu checklist hər monitorinq seansı zamanı istifadə olunmalı, nəticələr ayrıca hesabat formasında saxlanılmalıdır.

Bio izləmə nümunələri

1. **Nümunə: “Xaricdə iş” elanlı bio**. *“Visa free work in Europe ✈️, WhatsApp: +99450xxxxxxx”*

Təhlil: Burada açıq risk siqnalı var — qeyri-real vəd (“vizasız iş”), birbaşa əlaqə vasitəsi (WhatsApp nömrəsi), şəxsi məlumat və şəffaflıq yoxdur. UNODC bu tip bio-ların insan alveri şəbəkələri üçün tipik olduğunu göstərir.

2. **Nümunə: “Model agentliyi” adı ilə bio**. *“International Model Agency 👗✨, girls 18–25 DM for casting”*

Təhlil: Heç bir hüquqi qeydiyyat və şəxsiyyət açıqlaması yoxdur. Yaş məhdudiyyəti xüsusi olaraq vurğulanıb (18–25), bu da qurban cəlbetmə strategiyasının göstəricisidir. ATƏT qeyd edir ki, belə bio-lar qızların cinsi istismara cəlbi üçün əsas kanallardan biridir.

3. **Nümunə: Sponsor bio-su**. “Gənc qızlarla tanışlıq üçün axtarış” 💎 💸, bütün xərclər ödənilir”

Təhlil: Bio açıq-aşkar manipulyativdir. “Xərclər qarşılanır” kimi ifadələr EIGE (2022)-nin təsnifatına görə “sponsorluq və sextortion riskləri” kateqoriyasına daxildir.

Geotag izləmə nümunələri

1. **Nümunə: Təkrar lokasiya etiketi**: *“*Asan iş, yüksək maaş” — geotag: *“Varşava, Polşa”*

Təhlil: Eyni tip elanlar bir neçə hesabda “Varşava” etiketi ilə yerləşdirilib. Europol (2021) bildirir ki, müəyyən regionlarda insan alveri şəbəkələri tez-tez lokasiya təkrarı ilə izlənilə bilir.

2. **Nümunə: Yerli kontekstdə geotag**.“Sponsor axtarılır, ciddi xanımlar yazsın” — geotag: *“Bakı, Azərbaycan”*

Təhlil: Burada lokasiya həm diqqəti cəlb etmək, həm də yerli auditoriyanı hədəfləmək üçün istifadə olunub. Azərbaycanın şəhər geotag-ları altında bu tip elanlar tez-tez aşkarlanır.

3. **Nümunə: Qısa müddətdə çoxsaylı ölkə geotagları**. bir həftə ərzində eyni profil “İstanbul”, “Minsk”, “Moskva” və “Dubay” geotag-ları ilə elan paylaşıb.

Təhlil: Normal istifadəçi bu qədər tez-tez ölkə dəyişə bilməz. Bu, ya saxta hesabdır, ya da şəbəkə tərəfindən idarə olunan bot profildir.

Bio izləmə zamanı əsas siqnallar — qeyri-real vədlər, əlaqə məlumatının birbaşa bioya yerləşdirilməsi, şablon mətnlər və yaş məhdudiyyəti vurğularıdır. Geotag izləmə isə təkrar istifadə olunan məkanlar, qısa müddətdə çoxsaylı ölkə etiketi və riskli yerli lokasiyalar vasitəsilə şübhəli məzmunu üzə çıxarır. Tədqiqatlar da göstərir ki, bio və geotag izləməsi sosial media üzərindən insan alveri və istismar nümunələrinin aşkarlanmasında əsas metodlardan biridir.

3.3.4. Vizual yoxlama

Vizual yoxlama (reverse image search) – şəkil faylının və ya onun linkinin internetdə axtarış motoruna yüklənməsi yolu ilə həmin şəkil və ya ona bənzər vizual materialların tapılması prosesidir. Ənənəvi mətn əsaslı axtarışdan fərqli olaraq burada giriş

məlumatı mətn deyil, birbaşa şəkil olur. Bu metodun əsasında rəng, forma, obyekt və məkan elementlərinin tanınması və verilənlər bazasında müqayisəsi dayanır[29].

Misal: Bir sosial şəbəkədə yayımlanan "iş elanı"nda yerləşdirilmiş şəkil Google Images vasitəsilə axtarıldıqda məlum olur ki, foto əslində başqa ölkədə yerləşən bir model agentliyinin saytından götürülüb. Bu fakt elanların saxta olduğunu sübut edir.

Reverse image search hüquqi və sosial iş sahələrində xüsusi əhəmiyyət daşıyır. Məsələn, jurnalistlər dezinformasiya ilə mübarizə aparmaq üçün yayımlanan fotoları yoxlayaraq ilkin mənbəni müəyyən edirlər[30] . Hüquq-mühafizə orqanları isə insan alveri ilə bağlı hallarda sosial şəbəkələrdə yayılan şəkillərin mənşəyini müəyyənləşdirməklə qurbanların identifikasiyasını həyata keçirə bilirlər. Yaradıcılıq sahəsində isə rəssam və fotoqraflar TinEye platforması vasitəsilə öz işlərinin icazəsiz istifadəsini aşkarlayaraq hüquqlarını müdafiə edirlər[31].

Misal: Fotoqraf bir müştərinin icazəsiz olaraq onun çəkdiyi şəkilləri kommersiya məqsədilə istifadə etdiyini müəyyən etmək istəyir. TinEye axtarışı nəticəsində fotoşəkil bir neçə onlayn mağazada tapılır. Bu məlumat hüquqi dəlil kimi istifadə olunur.

Metodun məhdudiyyətləri də mövcuddur. Keyfiyyəti zəif olan şəkillər sistem tərəfindən düzgün tanınmaya bilər, şəxsi fotoların kütləvi axtarışı məxfilik problemləri doğurur[32]. Bundan əlavə, deepfake və manipulyasiya edilmiş vizuallar klassik axtarış alqoritmlərindən yayınaraq əlavə texnologiyaların tətbiqini tələb edir.

Misal: Bir istifadəçi "məşhur şəxsin kompromat görüntüsü" kimi təqdim edilən fotoşəkli yoxladıqda nəticələrdə həmin şəkilin

[29] Torralba, A., Fergus, R., & Freeman, W. T. (2008). 80 million tiny images: A large dataset for nonparametric object and scene recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 30*(11), 1958–1970.

[30] Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society Research Institute.

[31] Cameron, S. (2018). *Intellectual property rights in the digital age*. Oxford University Press.

[32] Keegan, J. (2020). Privacy implications of reverse image search technologies. *Journal of Digital Ethics, 12*(3), 55–72.

montaj olunduğu və orijinalın illər əvvəl başqa kontekstdə çəkildiyi aşkarlanır. Bu, vizual yoxlamanın dezinformasiyaya qarşı gücünü göstərir.

Nəticə olaraq, vizual yoxlama rəqəmsal təhlükəsizlik, sosial iş və media savadlılığı sahələrində mühüm alət hesab olunur. O, həm qurbanların müdafiəsi, həm də ictimaiyyətin düzgün məlumatlandırılması üçün geniş imkanlar açır[33].

Vizual yoxlama – addım-addım

Mərhələ	Addım	Yoxlama bəndi
Hazırlıq	Şəkili seç	Şübhəli və ya yoxlanması lazım olan şəkil müəyyənləşdirildi?
	Keyfiyyət	Şəkilin yüksək keyfiyyətli versiyası əldə edildi?
	Fayl	Fayl cihazda saxlanıldı və ya link kopyalandı?
Platforma seçimi	Google Images	Geniş internet mənbələrində yoxlama aparmaq üçün seçildi?
	TinEye	Müəllif hüquqlarını qoruma və çoxsaylı sayt müqayisəsi üçün istifadə edildi?
	Yandex Images	Regional nəticələr və oxşar şəkillər üçün nəzərdən keçirildi?
	Bing Visual Search	Obyekt tanıma və kommersiya istifadəsi üçün istifadə olundu?
Axtarışın aparılması	Yükləmə	Şəkil platformaya yükləndi və ya link daxil edildi?
	Tarix	İlk yayımlanma tarixi yoxlanıldı?
	Kontekst	Şəkilin fərqli kontekstdə istifadəsi analiz edildi?
Analiz	Mənbə	Mənbənin etibarlılığı (rəsmi sayt, xəbər agentliyi) yoxlanıldı?
	Müqayisə	Şəkilin müxtəlif saytlardakı istifadəsi müqayisə edildi?

[33] Lewandowski, D. (2021). Search engines and image retrieval: A critical review. *Information Research, 26*(1).

	Forensik	Manipulyasiya ehtimalı olduqda əlavə analiz aparıldı?
Sənədləşdirmə	Ekran görüntüsü	Tapıntılar ekran görüntüsü ilə sənədləşdirildi?
	Linklər	Linklər qeyd edildi və arxivləşdirildi?
	Yazılı qeyd	Şəkilin ilk yayımlandığı tarix və sayt qeyd edildi?
Praktiki tətbiq	Sosial işçi	Qurbanın şəkli saxta elanlarda istifadə olunub-olunmadı yoxlanıldı?
	Hüquq-mühafizə	İstismar xarakterli foto və mənbələr izlənildi?
	Jurnalist	Xəbərlərdə istifadə olunan şəkillərin doğruluğu araşdırıldı?
Məxfilik və etika	Hüquqi əsas	Şəxsi fotolar yalnız hüquqi əsas və ya icazə ilə yoxlandı?
	Təhlükəsizlik	Qurbanların təhlükəsizliyi qorundu?
	Məxfilik	Nəticələr məhdud dairədə paylaşıldı və şəxsi məlumatlar qorundu?

3.4. Twitter (X)

Twitter 2006-cı ildə Jack Dorsey, Biz Stone və Evan Williams tərəfindən qurulub. İlk tvit 21 mart 2006-cı ildə Jack Dorsey tərəfindən yazılıb: *"just setting up my twttr"*. Başlanğıcda "twttr" adı ilə fəaliyyətə başlayan platforma qısa mesajlaşma xidməti kimi yaradılmışdı. 2007-ci ildən "Twitter" adını aldı və 140 simvolluq mesaj məhdudiyyəti ilə fərqləndi (2017-ci ildən bu limit 280 simvola qaldırıldı). 2023-cü ildə "Twitter" adı "X" ilə əvəzləndi. Musk-un planına görə X yalnız sosial şəbəkə deyil, həm də "super-app" – yəni ödəniş, xidmət sifarişi, media və kommunikasiya mərkəzi kimi fəaliyyət göstərəcək. Twitter (X) hazırda dünya üzrə 450 milyondan çox aktiv istifadəçiyə sahibdir[34]. Ən çox istifadəçilər ABŞ, Hindistan, Yaponiya və Braziliyada toplanıb. Platforma

[34] Statista. (2024). *Number of Twitter/X users worldwide*.

xüsusilə siyasət, media və ictimai debat üçün əsas kanallardan biridir. Ən aktiv istifadəçilər 18–29 yaş qrupu, 30–49 yaş qrupu isə xəbər və peşəkar əlaqələr üçün geniş istifadə edir. Araşdırmalara görə, Twitter-in istifadəçi profili gender baxımından nisbətən balanslı olsa da, kişilərin nisbəti bir qədər çoxdur[35].

Twitter Azərbaycanda 2010-cu illərdən etibarən populyarlıq qazanmağa başlayıb. Əvvəllər əsasən texnologiya həvəskarları və xarici dillərdə təhsil alan gənclər istifadə edirdilər. 2015-ci ildən sonra isə platforma sosial, siyasi və gender məsələlərinin müzakirə məkanı kimi inkişaf etdi. 2020-ci ildəki İkinci Qarabağ müharibəsi zamanı Twitter Azərbaycanda ən çox istifadə olunan sosial şəbəkələrdən birinə çevrildi.

Twitter (indiki adı ilə X) qlobal ictimai debat və sürətli məlumat mübadiləsi üçün əsas platformalardan biri olmaqla yanaşı, insan alverçilərinin də fəaliyyətlərini həyata keçirdikləri rəqəmsal məkana çevrilmişdir. Sosial media texnologiyalarının genişlənməsi insan alverinə qarşı mübarizə mexanizmlərini çətinləşdirir, çünki cinayətkarlar anonimlik, sürət və sərhədsiz ünsiyyət imkanlarından istifadə edərək həm qurban cəlbetmə, həm də istismar fəaliyyətlərini daha asan şəkildə qura bilirlər. Twitter bu mənada xüsusi risk daşıyır, çünki platforma mətn, şəkil, video və linkləri geniş auditoriyaya saniyələr içində çatdırmaq gücünə malikdir. Bu isə insan alverçilərinə həm rekrutment, həm də istismar şəbəkələrinin idarə olunması üçün yeni imkanlar açır.

İnsan alverçilərinin Twitter-dən istifadəsi əsasən üç istiqamətdə müşahidə olunur. Birincisi, rekrutment mərhələsidir. Burada qurbanların diqqətini cəlb etmək üçün saxta iş elanları, "model agentliyi" təklifləri, xaricdə yüksək qazanc vədləri paylaşılır. Bu elanlar tez-tez digər saytlardan götürülmüş şəkillərlə dəstəklənir və #job, #easycash, #modelling, #travel kimi beynəlxalq həştəqlər altında təqdim olunur. Beləliklə, sadə bir axtarışla gənclərin diqqətini çəkən elanlar Twitter üzərindən geniş yayıla bilir.

İnsan alverçiləri Twitter-dən bir neçə istiqamətdə istifadə

[35] Pew Research Center. (2021). *Twitter demographics and news consumption*.

edirlər. Birincisi, cəlbetmə məqsədilə saxta iş elanları, "model agentliyi" təklifləri və xaricdə yüksək gəlir vədləri yayılır. Belə elanlarda tez-tez başqa saytlardan götürülmüş şəkillər və hashtaglardan istifadə olunur. Məsələn, #job, #easycash, #travel kimi etiketlər altında yayılan elanlar əslində istismara aparan qapıdır. ABŞ-da aparılan tədqiqatlarda məlum olub ki, Twitter üzərindən "escort" elanları adı ilə əslində qadınların insan alverinə cəlbi həyata keçirilirdi[36]. Avropada isə Twitter bəzi hallarda uşaq istismar materiallarının yayılması üçün kanal rolunu oynayıb[37] .

İkincisi, insan alverçiləri şəxsi mesajlardan (DM) və anonim hesablarla əlaqə quraraq qurbanlarla güvən münasibəti yaradır, sonra isə onları WhatsApp və Telegram kimi daha qapalı platformalara yönləndirirlər. Nigeriyada 2022-ci ildə aşkarlanmış bir işdə Twitter vasitəsilə Dubaya "iş" təklifi alan gənc qadınların əslində cinsi istismara məruz qaldıqları sübuta yetirilmişdir[38]. Azərbaycanda isə Twitter əsas insan alveri platforması olmasa da, qlobal şəbəkələrlə bağlı elanların paylaşılması müşahidə olunur. Xüsusilə qadınlara "xaricdə iş" vədləri ilə ünvanlanan elanlar təhlükə yaradır. Yerli müşahidələr göstərir ki, kişi istifadəçilər daha çox "tez qazanc" elanlarına, qadınlar isə "model agentliyi" və "iş imkanları" elanlarına hədəflənirlər[39].

Üçüncü istiqamət isə istismar və qeyri-qanuni bazarlara çıxışdır. Twitter üzərindən qurbanların zorla çəkilmiş fotoları və videoları paylaşılaraq darknet platformalarına linklər təqdim edilir. Bəzi hallarda isə istismarçılar kriptovalyuta ödənişləri ilə bağlı elanlar verir, beləliklə, gizli maliyyə əməliyyatlarını gizlətməyə çalışırlar. Europol-un hesabatında qeyd olunur ki, Twitter və digər sosial şəbəkələr uşaq istismar materiallarının yayılmasında "kanal funksiyası" görür, bu da onların tamamilə qapalı platformalar qədər təhlükəli ola biləcəyini göstərir.

Twitter həmçinin vizual manipulyasiyalar üçün də istifadə

[36] Polaris Project. (2020). *Human Trafficking and Social Media*. Washington DC.
[37] Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA)*.
[38] UNODC. (2022). *Global Report on Trafficking in Persons*. United Nations.
[39] Azərbaycan Mətbuat Şurası. (2022). *Sosial şəbəkələrin Azərbaycanda istifadəsi: tendensiyalar və çağırışlar*.

olunur. Saxta elanlarda yerləşdirilən fotolar şəkil əsasında axtarışla yoxlanıldıqda məlum olur ki, onlar əslində başqa ölkələrin iş saytlarından və ya sosial media profillərindən götürülmüşdür. Bu texnologiyanın tətbiqi göstərir ki, insan alverçiləri ictimai etimadı qazanmaq üçün real görünən, lakin əslində oğurlanmış fotolardan geniş istifadə edirlər. Bu isə sosial işçilər və hüquq-mühafizə üçün mühüm xəbərdarlıqdır: hər hansı elan yoxlanmadan qəbul edilməməlidir.

Twitterdə insan alveri ilə bağlı əsas risklərdən biri anonimlikdir. Platformada saxta profillər açmaq nisbətən asandır və bu, istismarın aşkarlanmasını çətinləşdirir. Digər risk məlumatın sürətli yayılmasıdır; bir saxta elan qısa müddətdə yüzlərlə istifadəçiyə çata bilir. Bundan əlavə, həştəq manipulyasiyası xüsusi təhlükə daşıyır: "#iş", "#işaxtarıram", "#travel" kimi sadə axtarış terminləri istismarçılar tərəfindən istifadə olunur və qurban cəlbi daha effektiv hala gəlir. Qurbanların aldatma üsulları isə çox vaxt romantik münasibət və ya təhsil vədləri ilə başlayır, sonradan istismara çevrilir.

Gender aspektindən baxanda, Twitter-in həm gücləndirici, həm də riskli tərəfləri mövcuddur. Bir tərəfdən qadın fəallar, jurnalistlər və hüquq müdafiəçiləri Bu ikili reallıq Twitter-i həm güc mənbəyi, həm də təhlükəli məkana çevirir. Twitter həm qurbanların müdafiəsi, həm də istismar risklərinin artdığı bir məkan kimi görünür. Güclü tərəfi ondan ibarətdir ki, vətəndaş cəmiyyəti, QHT-lər və jurnalistlər bu platformadan ifşa kampaniyaları üçün də istifadə edə bilirlər. #MeToo hərəkatı kimi beynəlxalq nümunələr göstərir ki, qadınlar Twitter vasitəsilə öz səsini yüksəldə bilirlər[40]. Lakin eyni zamanda qurbanların açıq şəkildə hədəf alınması, nifrət nitqi və kiberzorakılıq təhlükələri də mövcuddur[41].

İnsan alveri ilə mübarizə çərçivəsində Twitter-in monitorinqi xüsusi əhəmiyyət daşıyır. Sosial işçilər və hüquq-mühafizə orqanları hashtag izləmə texnologiyalarından istifadə etməli, riskli elanların

[40]Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society Research Institute.

[41] Jane, E. A. (2020). Online abuse and gendered hate speech. *Feminist Media Studies, 20*(4), 512–528.

vizual yoxlamasını aparmalı və nəticələri sənədləşdirməlidirlər. Qurbanlara isə maarifləndirici təlimatlar verilməlidir: sosial şəbəkədə yayılan hər iş elanı etibarlı deyil, şəkil və mənbə mütləq yoxlanılmalıdır. Eyni zamanda Twitter şirkətinin öz "reportlama" və bağlama mexanizmləri daha effektiv işlədilməli, yerli QHT-lərlə əməkdaşlıq gücləndirilməlidir.

Nəticə olaraq, Twitter insan alverçiləri üçün tamamilə əsas meydan olmasa da, onların fəaliyyətlərinin ilkin mərhələlərində – yəni qurban cəlbi və manipulyasiya prosesində mühüm rol oynayır. Saxta iş elanları, sürətli yayılan hashtag kampaniyaları və şəxsi mesajlar ən çox istifadə olunan alətlərdir. Azərbaycan reallığında da bu risklər mövcuddur və xüsusilə gənclər, tələbələr və iş axtaran qadınlar üçün təhlükəlidir. Buna görə də Twitter yalnız ictimai debat və hüquq müdafiəsi üçün yox, həm də insan alverinə qarşı mübarizədə izlənilməsi vacib olan bir platforma kimi qəbul edilməlidir.

3.4.1. Real yardım çağırışları

Twitter (indiki adı ilə X) sosial medianın ən dinamik və açıq platformalarından biridir. Onun əsas xüsusiyyəti məlumatın saniyələr içində qlobal auditoriyaya çatdırılması və interaktiv reaksiyaların çox sürətli olmasıdır. Bu xüsusiyyət yalnız ictimai debat və siyasi müzakirələr üçün deyil, həm də insan hüquqları, gender bərabərliyi və zorakılıq hallarında real vaxt yardım çağırışlarının edilməsi üçün əhəmiyyətli imkan yaradır. Əslində Twitter bir növ "rəqəmsal siren sistemi" funksiyasını yerinə yetirir: qurbanlar və ya şahidlər təhlükə vəziyyətində qısa bir tvit vasitəsilə həm dost çevrəsini, həm də daha geniş ictimaiyyəti məlumatlandırmaq imkanı qazanırlar. Bu, digər qapalı sosial şəbəkələrdən (məsələn, WhatsApp və ya Facebook qruplarından) fərqli olaraq daha açıq və daha sürətli təsir yaradır[42]

Real vaxt yardım çağırışları bir neçə formada müşahidə olunur. Ən açıq forması "SOS" tipli mesajlardır. Bu tip

[42] Bruns, A., & Burgess, J. (2015). *Twitter and society*. Peter Lang.

paylaşımlarda istifadəçi birbaşa kömək tələb edir, çox vaxt məkan və ya vəziyyət barədə minimal məlumat verir. Məsələn, "Məni zorla evdə saxlayırlar, kömək edin! 📍 Yasamal rayonu" kimi bir tvit qurbanın təcili kömək istədiyini göstərir. Belə hallarda monitorinq aparan sosial işçi və ya hüquq-mühafizə əməkdaşı dərhal paylaşımı sənədləşdirməli, geolokasiya göstəricilərini yoxlamalı və təcili müdaxilə mexanizmini işə salmalıdır. ABŞ və Avropada aparılan araşdırmalar göstərir ki, məhz Twitter üzərindən edilən SOS çağırışları nəticəsində polis müdaxiləsi və qurbanın xilas olunması halları olub.

Daha dolayı formada edilən yardım çağırışları isə şifahi və ya şifrəli mesajlarla ifadə olunur. Qurbanlar bəzən açıq şəkildə kömək istəməkdən çəkinirlər, çünki istismarçı və ya zorakı şəxs onların sosial media hesablarını izləyə bilər. Belə hallarda onlar dolayı siqnallar göndərirlər: "Əgər bu həftə dostlarıma yazmasam, bilin ki, nəsə baş verib" və ya "Bugün çox qəribə bir vəziyyətdə qaldım, bura barədə danışa bilmirəm" kimi mesajlar qurbanın riskdə olduğunu göstərir. Monitorinq aparan şəxslər bu tip mesajlara xüsusi həssaslıqla yanaşmalı, profilin əvvəlki paylaşım tarixçəsini təhlil etməli və dəyişiklikləri müşahidə etməlidirlər.

Hashtag kampaniyaları real vaxt yardım çağırışlarının başqa bir formasıdır. Hashtag, yəni # işarəsi ilə başlayan açar sözlər, həm qurbanların, həm də dəstəkçilərin mesajlarını bir mövzu altında birləşdirir.

Geotag (lokasiya etiketi) isə real vaxt yardım çağırışlarında xüsusi əhəmiyyət daşıyır. Twitter istifadəçiləri tvit paylaşarkən yerləşdikləri məkanı əlavə edə bilirlər. Bu funksiya bəzi hallarda həyati dəyər kəsb edir. Məsələn, qurban "Məni məcburən buraya gətiriblər" kimi bir mesaj paylaşır və tvitin altında misal üçün, "Bakı Beynəlxalq Avtovağzal" geotagı görünür. Bu, qurbanın harada saxlanıldığını və ya haradan hərəkət etdiyini göstərən açıq ipucu rolunu oynayır. İnsan alveri və ya məişət zorakılığı hallarında bu cür məlumatlar qurbanın tez bir zamanda tapılması üçün mühüm göstəricidir.

Monitorinq aparan şəxslər üçün bir neçə əsas göstərici vardır. Əvvəla, mətnin tonu və emosional yüklənməsi diqqətlə təhlil

edilməlidir. SOS, “kömək edin”, “çıxış yolu yoxdur”, “məni saxlayırlar”, “qorxuram” kimi ifadələr yüksək risk siqnallarıdır.

İkincisi, lokasiya göstəriciləri diqqətə alınmalıdır. Tvitdə açıq məkan adı ola bilər, ya da əlavə edilmiş foto və video üzərindən geotag aşkar edilə bilər.

Üçüncüsü, hashtag istifadəsi mühüm əlamətdir; #SOS, #Help, #SaveMe, #qadınqətlləri kimi etiketlər real vaxt çağırışlarını qruplaşdırır.

Dördüncüsü, vaxt göstəricisi analiz olunmalıdır. Gecə saatlarında edilən təcili çağırışlar daha yüksək risk göstəricisi ola bilər.

Beşinci, profilin tarixi və davranış nümunələri qiymətləndirilməlidir. Yeni açılmış, az paylaşımlı və birdən-birə yardım çağırışı edən hesablar xüsusi diqqət tələb edir.

Real vaxt yardım çağırışlarının gender aspekti də mühümdür. Araşdırmalar göstərir ki, qadınlar Twitter vasitəsilə daha çox zorakılıq və ya istismar hallarını ifşa etmək üçün səs qaldırırlar. Bu, bir tərəfdən qadınların səsinin eşidilməsi və sosial dəstəyin mobilizasiyası üçün güclü vasitədir, digər tərəfdən isə onları kiberzorakılığa və təhdidlərə daha açıq hala gətirir.

Çağırışların hamısının həqiqi olmaması riski də mövcuddur. Sosial mediada bəzən saxta SOS mesajları yayıla bilər ki, bu da resursların boş yerə istifadəsinə səbəb olur. Ona görə də monitorinq aparan şəxslər hər paylaşımı dərhal real hesab etmədən, qısa müddətdə ilkin yoxlama aparmalı, lakin gecikmədən də reaksiya verməlidirlər. Burada balans mühümdür: hər mesaj potensial həyati siqnal kimi qəbul edilməli, eyni zamanda faktların yoxlanması prosesi paralel aparılmalıdır.

Nəticə etibarilə, Twitter real vaxt yardım çağırışları üçün müstəsna önəm daşıyan bir platformadır. Onun açıq xarakteri, sürətli yayılma gücü və geniş auditoriyaya çıxış imkanı həm qurbanlar, həm də sosial dəstək şəbəkələri üçün əvəzolunmazdır. Sosial işçilər və hüquq-mühafizə orqanları bu çağırışların monitorinqini sistemli şəkildə həyata keçirməli, hashtag izləmə, bio və geotag analizi, mətnin emosional yükünü qiymətləndirmə kimi metodlardan istifadə etməlidirlər. Hər bir çağırış potensial həyati xəbərdarlıqdır və onun vaxtında görülməsi bəzən bir insanın taleyini

dəyişə bilər. Bu səbəbdən Twitter yalnız ictimai debat və siyasi fikir mübadiləsi üçün deyil, həm də insan alveri və zorakılıqla mübarizədə "rəqəmsal xilasedici" funksiyası daşıyan bir vasitədir. İnsan alveri ilə mübarizə aparan QHT-lər potensial qurbanlar arasıdna məlumatlandırma təlimləri apararkən paltformanın imkanları barədə məlumat verməli, eləcə də qurbanların xilası üçün geniş istifadə etməsi məqsədəuyğundur.

Real vaxt yardım çağırışının monitorinq Forması

SOS siqnalının identifikasiyası

Yoxlama bəndi	Qeyd	✓ / ✗
Tvit açıq SOS mesajıdırmı? ("kömək edin", "SOS", "qorxuram")		
Dolayı mesaj varmı? ("Əgər mən yazmasam, nəsə olub")		
Mesajda emosional yüklənmə və təcili ton hiss olunurmu?		

Məkan və lokasiya təhlili

Yoxlama bəndi	Qeyd	✓ / ✗
Tvitdə açıq məkan adı çəkilibmi? ("Yasamal rayonu", "Avtovağzal")		
Geotag əlavə olunubmu (Twitter-in lokasiya funksiyası)?		
Paylaşılan şəkil/video üzərində məkan detalları görünürmü?		

Hashtag və şəbəkə analizi

Yoxlama bəndi	Qeyd	✓ / ✗
SOS və yardım həştəqləri varmı? (#SOS, #Help, #SaveMe, #qadınqətlləri)		
Yerli və regional həştəqlər izlənilibmi? (#uşaqhüquqları, #domesticviolence)		
İstifadəçi daha əvvəl bu tip həştəqlərlə paylaşımlar edibmi?		

Vaxt və kontekst

Yoxlama bəndi	Qeyd	✓ / ✗
Mesajın paylaşılma vaxtı qeyri-adi dövrə düşürmü (gecə, bayram vaxtı)?		
Son paylaşımlar arasında ziddiyyətli və ya təcili siqnallar varmı?		
Profil birdən-birə açılıb SOS çağırışı yayıb?		

İstifadəçi profilinin qiymətləndirilməsi

Yoxlama bəndi	Qeyd	✓ / ✗
Hesab real şəxs təsiri bağışlayırmı (foto, bio, keçmiş tvitlər)?		
Hesab yeni yaradılıb, yoxsa uzun müddətdir aktivdir?		
Əvvəlki paylaşımlarda risk siqnalları olubmu (zorakılıq, təhdid işarələri)?		

Təhlükənin qiymətləndirilməsi (Risk matrisi)

Risk Siqnalı	Aşağı	Orta	Yüksək
Açıq SOS mesajı			
Geotag və konkret məkan			
Təkrar kömək çağırışları			
Şifahi/dolayı mesaj			
Profilin yeni olması və qeyri-adi davranış			

Reaksiya və sənədləşdirmə

Yoxlama bəndi	Qeyd	✓ / ✗
Paylaşım ekran görüntüsü ilə sənədləşdirilibmi?		
Link və tvit ID qeydə alınıbmı?		
Hüquq-mühafizə və ya təcili yardım instansiyasına yönləndirilibmi?		
QHT və sosial işçi şəbəkəsinə xəbər verilibmi?		

Qısa qaydalar

- Hər SOS siqnalı potensial həyati xəbərdarlıq kimi qəbul olunmalıdır.
- Ən azı 2 sübut (məsələn, SOS mesaj + lokasiya) olduqda dərhal hüquq-mühafizəyə məlumat verilməlidir.
- Fakt yoxlanması aparılsa belə, gecikmə baş verməməlidir – çünki real vaxt çağırışı dəqiqələr içində həyati nəticə doğura bilər.

3.4.2. Böyl nümunələri

Twitter (X) platformasında Böyl axtarış üsullarının tətbiqi xüsusilə insan alveri, zorakılıq, real vaxt yardım çağırışları və saxta elanların izlənməsi baxımından mühüm əhəmiyyət daşıyır. Əgər sadəcə "iş" və ya "kömək" sözlərini axtarışa daxil etsək, minlərlə əlaqəsiz nəticə alınacaq. Halbuki Böyl operatorları ilə dəqiq kombinasiyalar qurmaq monitorinq aparan sosial işçi və hüquq-mühafizə əməkdaşı üçün real siqnalları aşkarlamağa imkan verir. Məsələn, "iş" AND "Dubai" OR "model" axtarışı Twitterdə qadınlara yönəldilən saxta iş elanlarını tapmaq üçün istifadə oluna bilər. Burada AND operatoru yalnız hər iki açar sözün olduğu paylaşımları çıxarır, OR operatoru isə alternativ terminləri də axtarışa daxil edir.

Böyl axtarış üsulları rəqəmsal monitorinq və məlumatların süzgəcdən keçirilməsi üçün ən geniş istifadə olunan metodlardan biridir. Onun mahiyyəti ondadır ki, sadəcə bir açar sözlə məhdudlaşmırıq, əksinə xüsusi operatorlardan (AND, OR, NOT, "“

dırnaq işarəsi, * ulduz simvolu və s.) istifadə edərək daha dəqiq və məqsədyönlü nəticələr əldə edirik. Bu metod sosial media izləməsi, insan alveri, zorakılıq halları, saxta elanların aşkarlanması və media analizlərində geniş tətbiq olunur[43]. Məsələn, sosial şəbəkələrdə insan alveri ilə bağlı monitorinq aparan bir mütəxəssis yalnız "iş" sözünü axtarışa daxil etsə, minlərlə əlaqəsiz nəticə qarşısına çıxacaq. Halbuki "iş" AND "xaric" AND "qadın" kimi bir Böyl kombinasiyası onu konkret riskli elanlara yaxınlaşdıracaq. Burada AND operatoru axtarış nəticələrini daraldır və yalnız hər üç açar sözün birlikdə istifadə olunduğu paylaşımları çıxarır.

OR operatoru nəticələri genişləndirmək üçün istifadə olunur. Tutaq ki, bir monitorinq aparan həm "escort", həm də "masaj" sözlərini izləmək istəyir, çünki istismarçılar çox vaxt bu terminlərdən paralel istifadə edirlər. Bu halda "escort" OR "masaj" yazmaq lazımdır. Nəticələrdə hər iki terminə aid paylaşımlar görünəcək və bu, qurbanların cəlb edildiyi müxtəlif elanları aşkarlamağa imkan verəcək. NOT operatoru isə əksinə, lazımsız nəticələri çıxarmağa xidmət edir. Məsələn, "iş" AND "model" NOT "rəsm" axtarışı zamanı yalnız model iş elanları qalacaq, amma incəsənətlə bağlı nəticələr istisna ediləcək. Bu, monitorinq aparan şəxsin vaxtını və resurslarını xeyli qənaət edir.

Twitter-də kiberzorakılıq və real vaxt SOS çağırışlarının izlənməsi üçün də Böyl üsulları əhəmiyyətlidir. Məsələn, "help" AND "trapped" OR "kidnapped" axtarışı zorla saxlanılma ilə bağlı yardım çağırışlarını tapmağa imkan verir. Hashtag-larla birlikdə bu üsul daha effektivdir: "#SOS" AND "məkan" OR "ünvan" yazıldıqda təcili kömək istəyən və məkan bildirən tvitlər üzə çıxır. Bu, xüsusilə insan alverinə məruz qalan və real vaxtda kömək istəyən qurbanların aşkarlanması üçün vacibdir.

Digər praktik nümunə "escort" OR "masaj" NOT "terapiya" kombinasiyasıdır. Bu üsul insan alverçilərinin Twitter-də gizli elanlar paylaşmaq üçün istifadə etdiyi terminləri izləməyə kömək edir. OR operatoru alternativ terminləri əhatə edir, NOT isə tibbi və ya əlaqəsiz nəticələri istisna edir. Beləliklə, monitorinq aparan şəxs

[43] Lewandowski, D. (2021). Search engines and Boolean logic: A review. *Information Research, 26*(1).

qurbanların cəlb edildiyi riskli elanları daha tez müəyyən edə bilir .

Twitterdə Böyl axtarışları yalnız riskli elanları deyil, həm də ictimai kampaniyaları izləmək üçün istifadə olunur. Məsələn, "#qadınqətlləri" OR "#femicide" yazıldıqda həm Azərbaycan, həm də beynəlxalq miqyasda femisid müzakirələrinə aid tvitlər görünür. Bu, qlobal trendlərlə yerli müzakirələrin müqayisəsi üçün əhəmiyyətli bir monitorinq üsuludur. Həmçinin "domestic violence" AND "help" AND "Baku" kombinasiyası Bakı şəhərində məişət zorakılığı ilə bağlı təcili yardım çağırışlarını aşkarlamağa imkan verir.

Böyl axtarış üsullarında dırnaq işarələri də mühüm rol oynayır. "Xaricdə iş" ifadəsini dırnaqla yazmaq nəticəsində sistem yalnız bu söz birləşməsinin eyni ardıcıllıqla olduğu mətnləri çıxarır. Əgər dırnaqsız yazılsa, sistem "xaricdə" və "iş" sözlərinin ayrı-ayrılıqda olduğu bütün nəticələri göstərəcək. Bu isə monitorinq zamanı əlavə məlumat kirliliyi yaradır. Ulduz *()* simvolu isə açar sözün müxtəlif sonluqlarını tapmaq üçün tətbiq edilir. Məsələn, "traf" yazdıqda həm "traffic", həm "trafficking", həm də "trafik" kimi nəticələr görünəcək. İnsan alveri mövzusunda izləmə aparan tədqiqatçı üçün bu operator olduqca faydalıdır, çünki cinayətkar şəbəkələr anlayışları müxtəlif dillərdə və variantlarda gizlətməyə çalışırlar[44] .

Real praktikada Böyl operatorlarının istifadəsinə aid bir neçə nümunə xüsusilə əhəmiyyətlidir. Məsələn, ABŞ-da Polaris Project göstərir ki, "job" AND "səyahət" AND "pulsuz viza" axtarışı insan alverçilərinin ən çox istifadə etdiyi saxta elanları aşkarlamaq üçün effektivdir. Avropada aparılan araşdırmalarda "escort" OR "erotik masaj" NOT "terapiya" kombinasiyası qurban cəlbi məqsədli elanları aşkarlamaqda istifadə olunub. Azərbaycanda isə "iş" AND "Dubai" OR "model" axtarışları potensial riskli elanların monitorinqi üçün istifadə oluna bilər, çünki çox vaxt qadınlar məhz "model agentliyi" və ya "xaricdə iş" adı altında aldatma yolu ilə istismara aparılırlar.

Bütün bunlar göstərir ki, Böyl axtarış üsulu sadəcə texniki bir

[44] Gillespie, T., & Duffy, B. (2012). *Search engines and the politics of relevance*. Yale University Press.

alət deyil, sosial işçilər, hüquq-mühafizə orqanları və tədqiqatçılar üçün strateji əhəmiyyət daşıyan bir monitorinq metodudur. O, məlumat çoxluğunu idarə etməyə, təhlükəli elanları ayırmağa və real riskləri vaxtında müəyyənləşdirməyə imkan verir. Nəticədə, həm qurbanların müdafiəsi, həm də insan alveri və zorakılıqla mübarizə prosesində vaxt və resurs qənaəti təmin olunur.

Twitter (X) üçün Böyl axtarış nümunələri

İstifadə sahəsi	Böyl nümunəsi	İstifadə məqsədi
Riskli iş elanları və insan alveri	"iş" AND "Dubai" OR "model"	Xaricdə “model agentliyi” və ya “iş” adı altında potensial aldatma elanlarını izləmək.
	"job" AND "travel" AND "free visa"	Saxta “iş + vizasız səyahət” təkliflərini aşkar etmək (Polaris Project, 2020).
	"escort" OR "masaj" NOT "terapiya"	Seksual istismar elanlarını müəyyənləşdirmək, tibbi nəticələri istisna etmək (Europol, 2020).
SOS və real vaxt yardım çağırışları	"help" AND "trapped" OR "kidnapped"	Qaçırılma və məcburi saxlanma ilə bağlı təcili SOS çağırışlarını tapmaq.
	"#SOS" AND "location" OR "address"	Lokasiya ilə birgə paylaşılan təcili yardım tvitlərini izləmək.
	"domestic violence" AND "help" AND "Baku"	Bakı şəhərində məişət zorakılığına dair təcili yardım çağırışlarını aşkarlamaq.
Kiberzorakılıq və nifrət nitqi	"qadın" AND ("sən sus" OR "öldürəcəyəm")	Qadınlara qarşı təhdid və zorakı dil nümunələrini izləmək.
	"#MeToo" OR "#qadınqətlləri"	Gender zorakılığına qarşı hərəkat və kampaniyaları izləmək.
Uşaq hüquqları və riskli məzmun	"child" AND "trafficking" OR "abuse"	Uşaqların istismarı və insan alveri ilə bağlı müzakirələri müəyyən etmək.
	"uşaq" AND	Uşaq əməyinə dair riskli

	"işlədir" NOT "təhsil"	elanları və ya şikayətləri izləmək.
Miqrasiya və potensial risklər	"refugee" AND "job" AND "Europe"	Qaçqın və miqrantların iş adı ilə aldatma risklərini izləmək.
	“miqrant" AND ("iş" OR "pul")	miqrant" AND ("iş" OR "pul")

Qısa qeyd:

- AND → hamısı birlikdə olmalıdır.
- OR → alternativ terminlər.
- NOT → istisna edilən sözlər.
- “ ” → tam ifadə axtarışı.

3.5. TikTok

TikTok 2016-cı ildə Çin şirkəti ByteDance tərəfindən “Douyin” adı ilə Çində istifadəyə buraxıldı. 2017-ci ildə beynəlxalq bazar üçün ayrıca versiya – “TikTok” yaradıldı və 2018-ci ildə ABŞ-ın məşhur “Musical.ly” tətbiqi ilə birləşdirilərək daha da geniş auditoriya qazandı. Bu addım qlobal populyarlığın başlanğıcı oldu. TikTok-un əsas yeniliyi 15–60 saniyəlik qısa videolar yaratmaq və onları musiqi, effektlər və filtrlərlə zənginləşdirmək imkanıdır. Platforma sürətlə inkişaf edərək 2021-ci ildə Facebook, YouTube və Instagram-dan sonra ən çox istifadə olunan sosial şəbəkələrdən birinə çevrildi[45].

TikTok-un qlobal əhatəsi olduqca genişdir. 2024-cü ilin məlumatlarına görə, dünyada təxminən 1,5 milyarddan çox aylıq aktiv istifadəçi var. Ən böyük bazarlar Asiya (Çin, Hindistanın qadağasından öncə böyük payı vardı, indi isə İndoneziya, Vyetnam, Filippin), ABŞ və Avropadır. TikTok xüsusilə Z nəsli (1995–2010-cu illərdə doğulanlar) və Alfa nəsli (2010 sonrası) arasında ən populyar platformadır. Bu gənc auditoriya platformanı həm əyləncə, həm də öyrənmə məkanı kimi istifadə edir.

TikTok-un istifadə imkanları çoxşaxəlidir. Əsas funksiyası

[45] Statista. (2023). *Number of monthly active TikTok users worldwide*.

qısa video paylaşımı olsa da, əlavə olaraq canlı yayımlar (live streaming), məhsul reklamı (TikTok Shop), sosial kampaniyalar və təhsil videoları da böyük rol oynayır. Platformanın alqoritmi istifadəçilərin maraqlarına uyğun "For You Page" (FYP) adlı fərdiləşdirilmiş lent təqdim edir ki, bu da kontentin sürətlə viral olmasına şərait yaradır. Bu sistem sayəsində kiçik istifadəçilər belə qısa müddətdə böyük auditoriyaya çata bilirlər.

Gender aspektindən baxanda, tədqiqatlar göstərir ki, TikTok istifadəçiləri arasında qadınların payı kişilərdən bir qədər çoxdur. ABŞ və Avropada qadın istifadəçilər 55–60%, kişilər isə 40–45% təşkil edir. Qadınlar platformadan əsasən özünüifadə, rəqs, moda, həyat tərzi və sosial mövzular üçün istifadə edirlər. Kişilər isə daha çox idman, oyun, texnologiya və yumor mövzulu kontent yaradırlar. Azərbaycanda da TikTok xüsusilə gənc qadınlar və qızlar arasında populyardır; eyni zamanda təhsil, psixologiya, ədəbiyyat və hətta hüquq sahəsində məlumat paylaşan qadın kontent yaradıcısı sayı artmaqdadır.

TikTok-un insan alveri və istismara təsiri

TikTok qlobal miqyasda ən sürətlə yayılan sosial şəbəkələrdən biri olmaqla yanaşı, insan alverçilərinin və istismar şəbəkələrinin də yeni "ov məkanı"na çevrilmişdir. Platformanın əsas üstünlüyü olan sürətli yayılma, geniş gənc auditoriya və vizual cəlbedicilik xüsusiyyətləri əslində cinayətkar qrupların da maraq dairəsinə düşür. Qısa videoların viral olması, alqoritmin istifadəçilərin maraqlarına uyğun məzmunu önə çıxarması və şəxsi mesajlaşma imkanları insan alverçilərinə həm qurban axtarma, həm də manipulyasiya üçün əlverişli zəmin yaradır[46] .

İnsan alverçiləri TikTok-dan əsasən üç istiqamətdə faydalanırlar. Birincisi, rekrutment, yəni qurban cəlbi mərhələsidir. Burada saxta iş elanları, model agentliyi və "asandır qazanc" tipli təkliflər qısa videolar vasitəsilə yayımlanır. Məsələn, cazibədar vizuallar və musiqi ilə müşayiət olunan "xaricdə iş imkanları"

[46] Montag, C., & Yang, H. (2021). Taming TikTok: The psychology of short-video social media. *Human Behavior and Emerging Technologies, 3*(5), 843–850.

elanları gəncləri, xüsusilə qızları aldatmaq üçün istifadə olunur. Polaris Projectin hesabatında göstərilir ki, gənc qızların TikTok üzərindən model və iş elanları ilə cəlb edilməsi halları artmaqdadır. Azərbaycanda da "Dubai", "Türkiyə" və "Avropa" sözləri ilə müşayiət olunan elanların TikTok-da reklam edildiyi müşahidə olunub və bu elanlar çox vaxt saxta profillərlə yayılır.

İkincisi, istismarçılar TikTok-un şəxsi mesajlaşma funksiyasından istifadə edərək qurbanlarla birbaşa əlaqə qururlar. İlk baxışdan sadə "follow" və "like" hərəkətləri ilə başlayan ünsiyyət sonradan "Direct Message" mərhələsinə keçir. Burada romantik münasibət, dostluq və ya iş vədləri ilə qurbanın etibarı qazanılır. Bu ünsiyyət qısa müddətdə qapalı platformalara – WhatsApp, Telegram və ya Snapchat-a yönləndirilir. Beləliklə, qurban artıq nəzarət altına düşür. Bəzi hallarda isə qurbanlardan "video challenge" adı ilə intim görüntülər istənilir və bu materiallar şantaj alətinə çevrilir. UNICEF-in hesabatında qeyd olunur ki, TikTok vasitəsilə uşaqların istismar məqsədli videolar yaratmağa təhrik edilməsi halları artmaqdadır.

Üçüncü istiqamət isə açıq və dolayı istismar kontentinin yayılmasıdır. TikTok-da bəzən "challenge" və ya "trend" adı ilə yayılan videolarda seksual xarakterli məzmun normalizə edilir. Bəzi şəbəkələr qurbanların videolarını gizli şəkildə çəkərək paylaşır və bu məzmun daha sonra başqa platformalara yönləndirilir. Europolun məlumatına görə, TikTok bəzi hallarda uşaq istismarı materiallarının ilk yayıldığı məkan olur və daha sonra darknet bazarlarına daşınır. Bu, platformanın təhlükəli tərəfidir: açıq görünən "əyləncə" formatı altında gizli istismar halları geniş yayılır.

TikTok-un insan alveri üçün cazibədar olması həm də onun auditoriyası ilə bağlıdır. Platformanın istifadəçilərinin əksəriyyəti 13–24 yaş arası gənclərdir və bu qrup ən həssas təbəqə sayılır. Gənclərin sosial statusu, işsizlik, asan qazanc arzusu və tanınmaq istəyi onları manipulyasiya üçün daha açıq edir. Azərbaycanda da gənclər, xüsusilə qızlar TikTok vasitəsilə həm özünüifadə, həm də gəlir qazanmaq arzusu ilə aktiv iştirak edirlər. İnsan alverçiləri isə bu istəkləri sui-istifadə edərək onları xaricdə iş, modelləşmə və ya "influencer dəstəyi" adı ilə aldatmağa çalışırlar.

Gender aspektindən baxanda, qadınlar və qızlar daha çox hədəf alınır. Onlar gözəllik, rəqs və həyat tərzi mövzularında kontent yaratdıqları üçün istismarçılar tərəfindən "potensial qurban" kimi görülürlər. Bununla yanaşı, oğlan uşaqları və gənc kişilər də müxtəlif yollarla cəlb edilə bilirlər – xüsusilə qeyri-qanuni işlərə, narkotik daşıma və ya zorakı qruplara qoşulma hallarında. UNICEF və UNODC-un hesabatları göstərir ki, TikTok üzərindən həm cinsi, həm də əmək istismarı üçün cəlbetmə halları qeydə alınıb.

TikTok-un təhlükələrindən biri də "hashtag manipulyasiyası"dır. İnsan alverçiləri qurban cəlbi üçün sadə və cazibədar həştəqlərdən istifadə edirlər: #iş, #easycash, #model, #visa və s. Bu həştəqlər altında yayılan videolar gənclərin diqqətini çəkir, amma əslində istismar məqsədli elanlara aparır. Azərbaycanda "iş axtarıram" tipli həştəqlərin altında bəzən saxta elanların yayılması müşahidə olunur və bu, insan alverçilərinin fəaliyyət dairəsini göstərir.

Bütün bunlar TikTok-un təkcə əyləncə platforması olmadığını, eyni zamanda istismar riskləri daşıdığını sübut edir. Bu risklərin qarşısını almaq üçün bir neçə istiqamətdə tədbirlər vacibdir. Əvvəla, sosial işçilər və hüquq-mühafizə orqanları TikTok üzərində hashtag izləmə və vizual yoxlama metodlarından istifadə etməlidirlər. Riskli elanlar şəkl əsasında axtarışla yoxlanmalı, qurbanların paylaşdıqları SOS tipli videolar diqqətlə izlənilməlidir.

İkincisi, valideynlər və təhsil müəssisələri gənclərə platformanın riskləri barədə maarifləndirici təlimlər keçməlidirlər.

Üçüncüsü, TikTok şirkətinin öz "reportlama" və məzmun filtrləmə mexanizmləri daha sərt şəkildə tətbiq edilməli, insan alveri və istismar kontenti dərhal bloklanmalıdır.

Nəticə olaraq, TikTok insan alverçiləri üçün həm qurban tapmaq, həm də istismar şəbəkələrini genişləndirmək baxımından effektiv bir platformadır. Onun vizual cazibədarlığı, gənc auditoriyası və viral alqoritmi cinayətkar qruplar üçün əlverişli mühit yaradır. Azərbaycan və qlobal miqyasda sosial işçilər, hüquq-mühafizə və QHT-lər bu platformanı diqqətlə izləməli, real vaxt monitorinq metodlarını tətbiq etməli və gənclər üçün təhlükəsizlik tədbirlərini gücləndirməlidirlər. TikTok-un gücü onun həm müsbət,

həm də mənfi təsirlərindədir və düzgün idarə olunmadıqda bu platforma insan alveri ilə mübarizədə ciddi risk faktoruna çevrilə bilər.

TikTok-da İnsan alveri risklərinin monitorinq aləti

Profil və davranış analizi

- Hesabın açılış tarixi – çox yeni yaradılıbsa, risk artmış sayılır.
- Profil fotosu və bio məlumatı real görünürmü, yoxsa saxta təəssürat yaradır?
- İzləyicilərin sayı və paylaşımların sayı arasında uyğunsuzluq varmı (məsələn, çox az video, amma minlərlə izləyici)?
- Əvvəlki videolarda iş, pul, xaricə getmək və ya romantik münasibət kimi mesajlar var?

Video və nəzmun təhlili

- Videolarda "asandır qazanc", "xaricdə iş", "model agentliyi" tipli elanlar varmı?
- Şəxsi və intim xarakterli məzmun paylaşmağa təşviq edilirmi?
- "Challenge" və ya trend adı altında riskli davranışlara çağırış var?
- Videolarda telefon nömrəsi, WhatsApp/Telegram linki paylaşılırmı?

Hashtag monitorinqi

- Riskli həştəqlər izlənilibmi? Məsələn: #iş, #easycash, #model, #visa, #fastmoney.
- Genderə yönəlmiş həştəqlər varmı? #qızlarüçüniş, #modellik, #gözəllikyarışması.
- Qurban çağırışları və dəstək həştəqləri izlənilibmi? #SOS, #SaveMe, #qadınqətlləri.

Şəxsi mesajlaşma riskləri

- Hesab tez-tez izləyicilərə "Direct Message (DM)" atırmı?
- Mesajlarda "iş təklifi", "görüş", "foto/video göndər" kimi tələblər varmı?

• Qurbanları başqa platformalara yönləndirməyə cəhd edilir? (WhatsApp, Telegram, Snapchat).

Lokasiya və vizual təhlil

• Videolarda lokasiya məlumatı (geotag, fon yazıları, tanınan məkan) görünürmü?

• İstismar riskli məkanlar (otel otaqları, tərk edilmiş yerlər) diqqət çəkirmi?

• Fotolar və videolar reverse image search ilə yoxlanılıb?

Risk qiymətləndirməsi

Risk siqnalı	Aşağı	Orta	Yüksək
Saxta görünən profil			
"Xaricdə iş" və "asandır qazanc" elanları			
Şəxsi mesajlarda iş və romantik dəvət			
Riskli hashtag istifadəsi			
SOS tipli yardım çağırışları			

Sənədləşdirmə və reaksiya

• Riskli kontent ekran görüntüsü və linklərlə sənədləşdirilib?

• Tapıntılar arxivləşdirilib və kodlaşdırılıb (tarix, profil ID, məzmun)?

• Məlumat hüquq-mühafizə və müvafiq QHT şəbəkəsinə ötürülüb?

• Qurbanın təhlükəsizliyi təmin etmək üçün anonimlik qorunub?

Qısa qaydalar

• Hər "iş" və ya "asandır qazanc" elanını potensial riskli elan kimi qiymətləndir.

• Hər SOS və ya dolayı yardım siqnalını həyati xəbərdarlıq hesab et.

• Monitorinq zamanı sürət, dəqiqlik və məxfilik prinsiplərinə əməl et.

3.5.1. Hashtag + geotag izləmə

Hashtag və geotag izləmə müasir sosial media monitorinqinin ən effektiv üsullarından biridir. Hashtag – yəni # işarəsi ilə yazılan açar sözlər – paylaşımları mövzu üzrə qruplaşdırır, geotag isə məkan məlumatı əlavə etməklə həmin paylaşımın harada edildiyini göstərir. İnsan alveri və istismar hallarının izlənməsində bu iki element birləşəndə həm məzmun, həm də məkan siqnalları eyni anda aşkarlana bilir. Bu isə sosial işçilər, hüquq-mühafizə orqanları və QHT-lər üçün real vaxtda riskləri izləməyə imkan verir[47] .

Hashtag izləməsi qurban cəlbi və ya istismar elanlarını aşkar etmək üçün xüsusilə faydalıdır. Məsələn, TikTok və Twitter-də #iş, #easycash, #modellik, #visa kimi həştəqlərlə yayılan videolar çox vaxt cazibədar görüntülərlə bəzədilir, lakin əslində insan alverinə aparan saxta təkliflər olur. Azərbaycanda "#işaxtarıram" etiketi altında yayılan bəzi elanların şəkl əsasında axtarış nəticəsində başqa ölkələrdəki saxta iş elanlarından köçürüldü aşkar edilib. Eyni zamanda qurbanların SOS tipli çağırışları da həştəqlər vasitəsilə izlənə bilər. Məsələn, #SOS, #SaveMe, #qadınqətlləri kimi etiklər altında paylaşılmış tvit və videolar çox vaxt təcili kömək siqnalıdır.

Geotag izləməsi isə məkan faktorunu nəzərə almağa imkan verir. TikTok və Twitter-də paylaşılan bəzi elan və videolarda istifadəçilər məkan əlavə edirlər. Bu, bəzən qurbanın saxlanıldığı və ya istismar edildiyi yeri aşkarlamaq üçün açar rolunu oynayır. Məsələn, bir qız TikTok-da "iş üçün gətirdilər" yazaraq video paylaşır və geotag "İstanbul hava limanı" göstərilir. Bu, potensial insan alveri hadisəsinin ilkin mərhələsini göstərən açıq ipucudur. Başqa bir nümunədə, Azərbaycanda gənclər arasında məşhurlaşan "#Dubai işləri" etiketi altında yayılan elanların bir neçəsində geotag məhz Dubayın müəyyən məkanlarını göstərib və bu elanların çoxu insan alveri riskləri ilə bağlı monitorinqlərdə qeyd olunub.

Hashtag və geotag birlikdə izlənəndə nəticələr daha dəqiq olur. Tutaq ki, monitorinqçi #iş AND #Dubai yazaraq həm məzmun, həm də məkan baxımından əlaqəli paylaşımları tapır. Bu, sadəcə

[47] Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA)*.

“iş” sözünü izləməkdən qat-qat effektlidir. Eyni şəkildə, #SOS həştəqi altında paylaşılan, geotag-ı “Bakı Avtovağzal” olan bir tvit qurbanın təcili yardım siqnalı göndərdiyini göstərir. ABŞ-da Polaris Projectin araşdırmaları göstərib ki, qurbanların 25%-dən çoxu yardım siqnallarını hashtag + geotag kombinasiyası ilə paylaşır.

Hashtag izləməsi həm də kodlaşdırılmış mesajların aşkarlanması üçün faydalıdır. İnsan alverçiləri bəzən açıq “iş” sözündən deyil, daha dolayı “#kolaypara”, “#easytravel”, “#newlife” kimi həştəqlərdən istifadə edirlər. Bu etiklər xüsusilə gənclərin diqqətini cəlb edir, amma əslində istismar risklərini gizlədir. Geotag isə həmin elanların haradan yayımlandığını göstərir və transsərhəd şəbəkələrin aşkarlanmasına kömək edir. Məsələn, Azərbaycanda Bakıda yayılan bir elanla Dubayda yayılan eyni məzmunlu elan eyni şəbəkəyə aid ola bilər – bunu hashtag və geotag izləmə birlikdə sübut edir.

Qurbanların real vaxt yardım çağırışları da çox vaxt hashtag və geotag vasitəsilə aşkar olunur. Bir qız TikTok-da “Məni buradan çıxarın” deyə yazır və #SOS həştəqi ilə birlikdə geotag “Gəncə” göstərir. Bu məlumat hüquq-mühafizə üçün dərhal müdaxilə siqnalıdır. 2020-ci ildə Avropada insan alverinə məruz qalan bir qız Twitter vasitəsilə #helpme həştəqi ilə paylaşım etmiş, lokasiya isə dəmir yolu stansiyası göstərmişdi və bu siqnal onun qurtarılmasına səbəb olmuşdu[48] .

Bütün bunlar göstərir ki, hashtag və geotag izləmə sadəcə texniki alət deyil, insan həyatını xilas edə biləcək strateji monitorinq metodudur. Sosial işçilər və hüquq-mühafizə əməkdaşları üçün əsas vəzifə yalnız populyar həştəqləri izləmək deyil, həm də riskli həştəqləri tanımaq və geotag məlumatlarını təhlil etməkdir. Bu üsul vasitəsilə saxta iş elanları, istismar şəbəkələrinin fəaliyyəti, SOS çağırışları və qurbanların hərəkət marşrutları barədə qiymətli məlumat toplamaq mümkündür.

[48] UNODC. (2022). *Global Report on Trafficking in Persons*. United Nations

Hashtag + Geotag izləmə təlimat cədvəli

Addım	Twitter (X) nümunəsi	TikTok nümunəsi
1. Riskli həştəqləri müəyyən et	#iş, #işaxtarıram, #easycash, #visa, #escort, #SOS, #Help, #SaveMe, #qadınqətlləri	#iş, #easycash, #modellik, #kolaypara, #visa, #SOS, #SaveMe, #qurtarın
2. Böyl kombinasiyalarından istifadə et	"iş" AND "Dubai", "#SOS" AND "location", "escort" OR "masaj" NOT "terapiya"	#iş AND Dubai, #modellik AND Bakı, #easycash AND Avropa
3. Geotag izləməsini yoxla	#SOS + geotag "Bakı Avtovağzal" → təcili risk siqnalı	#iş + geotag "Dubai" → xaricə aparılma riski
4. Vizual və məkan analizi apar	Tvitdə ünvan və ya şəkil fonunda məkan əlamətləri varmı?	Videoda otel otağı, avtovağzal və ya hava limanı görünürmü?
5. Şəxsi mesajlaşma riskini təhlil et	DM-lərdə "iş təklifi" və ya "foto göndər" tələbi	Videoda WhatsApp/Telegram linki varsa, yüksək risk
6. Sənədləşdirmə	Ekran görüntüsü + tvit linki + tarix	Video linki + istifadəçi adı + tarix
7. Praktiki nümunə	"Xaricdə model işi üçün qızlar tələb olunur" #iş #model + geotag İstanbul → insan alverinə cəlb siqnalı	"Yeni həyat səni gözləyir" #easycash + geotag Dubay → saxta elan riski
8. SOS çağırışı	"Məni saxlayırlar, kömək edin" #SOS + geotag Yasamal	Gənc qız video paylaşır: #SOS + geotag Gəncə → təcili yardım siqnalı

3.5.2. Video elan nümunələri

TikTok-un əsas xüsusiyyəti qısa videoların sürətlə viral olmasıdır. İnsan alverçiləri də bu xüsusiyyətdən istifadə edərək öz qurbanlarını cəlb etmək üçün cazibədar, musiqi ilə müşayiət olunan elanlar yerləşdirirlər. Bu elanlar çox vaxt iş, model agentliyi, vizasız səyahət, asan qazanc və ya "çöl ölkədə yeni həyat" tipli mesajlarla təqdim olunur. Monitorinq aparan şəxslər üçün əsas vəzifə bu elanların hansı elementlərdən ibarət olduğunu anlamaq və risk siqnallarını vaxtında aşkarlamaqdır.

Birinci siqnal – mətn və şüarların təhlili. İnsan alverçiləri qurbanları cəlb etmək üçün tez-tez "vizasız iş", "gözəl həyat", "tez pul qazan" kimi ifadələrdən istifadə edirlər. Bu cür videolarda sözlərin emosional və cazibədar tonla verilməsi diqqət çəkir. Məsələn, Azərbaycan reallığında "Türkiyədə model işi – 2000$ maaş, vizasız!" kimi elanlar qızların diqqətini çəkir. Halbuki, bu, tipik cəlb üsuludur və risk siqnalı sayılmalıdır.

İkinci siqnal – vizual elementlər. TikTok elanları çox vaxt gözqamaşdırıcı görüntülərlə müşayiət olunur. Bahalı maşınlar, lüks mənzillər, Dubay və ya Avropa şəhərlərinin fon görüntüləri tez-tez istifadə edilir. Bu vizuallar gənclərdə "yüksək həyat tərzinə çıxış" təsəvvürü yaradır, lakin əslində istismara aparır.

Üçüncü siqnal – musiqi və trend istifadəsi. İnsan alverçiləri elanlarını daha cazibədar göstərmək üçün TikTok-da populyar musiqilərdən və trend videolardan istifadə edirlər. Məsələn, bir "challenge" çərçivəsində "#newlife" və ya "#easycash" etiketi ilə yayılan videolar gəncləri aldatmaq üçün hazırlanır. Bu, xüsusilə yeniyetmələr üçün risklidir, çünki onlar viral olan hər şeyə daha çox inanırlar.

Dördüncü siqnal – hashtag və geotag. Elanların əksəriyyəti konkret həştəqlərlə yayılır. Riskli həştəqlərə misal: #iş, #kolaypara, #easycash, #visa, #model. Geotag isə elanların hansı məkandan yayımlandığını göstərir. Məsələn, "#iş" etiketi ilə yayılan bir video Dubay geotagı ilə müşayiət edilirsə, bu, ciddi istismar riskidir. Azərbaycanda "#işaxtarıram" həştəqi altında Bakıda yerləşdirilmiş, amma əslində Türkiyəyə yönəlik elanlar da qeydə alınıb.

Beşinci siqnal – əlaqə vasitələrinin paylaşılması. Əgər videonun sonunda WhatsApp, Telegram və ya telefon nömrəsi göstərilirsə, bu, çox yüksək risk əlamətidir. Çünki real iş elanları adətən sosial şəbəkələrdə şəxsi əlaqə vasitəsi ilə deyil, rəsmi sayt və ya agentlik üzərindən yayımlanır. İnsan alverçiləri isə qurbanı tez bir zamanda qapalı platformalara çəkməyə çalışırlar.

Altıncı siqnal – qurban çağırışları. Bəzən qurbanlar özləri də istismar videolarında dolayı siqnallar göndərirlər. Məsələn, bir qız rəqs videosu çəkib #SOS və ya #SaveMe etiketi əlavə edə bilər. Bu, adi izləyici üçün əyləncə kimi görünsə də, monitorinq aparan üçün təcili yardım siqnalıdır. 2022-ci ildə UNICEF-in hesabatında göstərilib ki, bəzi uşaqlar TikTok vasitəsilə dolayı SOS mesajları göndərərək istismardan qurtara biliblər.

Praktiki misallar:

- **Misal 1:** Video – "Xaricdə model işi, vizasız, yüksək maaş" yazısı, arxa planda Dubay görüntüləri, həştəqlər: #iş, #model, #easycash. Bu tip elan insan alverinə cəlb üsuludur.
- **Misal 2:** Video – "Məni buradan çıxarın" yazısı, #SOS həştəqi, geotag Gəncə. Bu, real vaxt yardım çağırışıdır.
- **Misal 3:** Video – Bahalı maşınlar, lüks otel otaqları, musiqi trendi ilə "Kolay para burda" yazısı. Həştəq: #kolaypara, geotag İstanbul. Bu, saxta elan və risk siqnalıdır.
- **Misal 4:** Video – Yeniyetmələr üçün "challenge": "Ən gözəl rəqsini göstər və pulsuz bilet qazan". Əlavədə Telegram linki var. Bu, gizli istismar məqsədli cəlb üsuludur.

TikTok-da video elanların aşkarlanması üçün monitorinq aparan şəxslər mətn, vizual, musiqi, hashtag və geotag elementlərini birlikdə analiz etməlidirlər. İnsan alverçiləri real elanlardan fərqli olaraq daha emosional, cazibədar və gizli manipulyativ üslubdan istifadə edirlər. Ən önəmlisi, hər hansı video elan rəsmi agentlik və ya etibarlı mənbə ilə dəstəklənmirsə, riskli elan kimi qiymətləndirilməlidir.

İnsan alverçilərinin istifadə etdiyi digər platformalar və fəaliyytə mexanizmi

Facebook / Facebook Marketplace

İstifadə üsulu: şəxsi qruplar, biznes səhifələri və Marketplace vasitəsilə "iş elanları", "ev işləri" və s. kimi saxta təkliflər paylaşılır; qapalı qruplara yönləndirmə.

Misal: "Xaricdə ev işləri — yollanma və yaşayış təmin olunur" postu + şəxsi mesajla təklif.

İndikatorlar: yeni yaradılmış hesablardan iş təklifləri; qapalı qruplarda tez-tez eyni tip elanlar; şəxsi mesajla kontakt verilən linklər.

Monitorinq tövsiyəsi: qrupları və Marketplace elanlarını Böyl ilə izləyin ("iş" AND "xaric" AND "qadın"), şəkilləri reverse image search ilə yoxlayın.

Instagram

İstifadə üsulu: cəlbedici foto/video + həştəqlər (#model, #casting) vasitəsilə rekrutment; DM ilə yönləndirmə; "link in bio" ilə xarici saytlara yönləndirilmə.

Misal: "Model axtarılır — sınaq üçün əlaqə DM" + lüks həyat fotoları.

İndikatorlar: #model/#casting həştəqləri ilə çoxsaylı eyni tip hesablar; bio-da şəxsi əlaqə nömrələri və ya Telegram linkləri.

Monitorinq tövsiyəsi: hashtag və bio izləmə; şübhəli profilləri reverse image yoxlayın.

Linkedin

İstifadə üsulu: rəsmi "iş elanları" örtüyü altında peşəkar cəlb etmə; saxta HR profilləri ilə inandırma; zərərli agentliklərin etibarlılıq təqlidi.

Misal: "Yüksək maaşlı xarici ofis işi — müsahibə üçün CV göndərin" (saxta şirkət profili).

İndikatorlar: yeni yaradılmış şirkət hesabları, qeyri-adi tezlikdə "iş təklifi" mesajları, rəsmi veb saytı olmayan employer-profil.

Monitorinq tövsiyəsi: şirkət və HR profillərinin doğruluğunu yoxlayın; URL, domen və iş ünvanı axtarışını aparın.

WhatsApp / Telegram (qapalı mesajlaşma)

İstifadə üsulu: ilkin əlaqə və sonra qapalı kanala (qrup/kanal) köçürmə; şəxsi təzyiq, şantaj, yönləndirmə.

Misal: "Müsahibə üçün Telegram qrupu" linki ilə DM göndərilməsi; sonra ödəniş və sənəd tələb olunur.

İndikatorlar: sosial platformada link paylaşımı; qruplara yönləndirmə; tələblər üçün öncədən ödəniş sorğuları.

Monitorinq tövsiyəsi: açıq platformalardakı linkləri və paylaşan hesabları sənədləşdirin; mümkün olduqda kanalın iç məzmununu izləyin (qanuni imkan daxilində).

TikTok

İstifadə üsulu: qısa cəlbedici videolarla saxta iş/model reklamı; challenge-larla diqqət cəlbi; video üzərindən kontakt paylaşımı.

Misal: "Dubayda model işi — ətraflı məlumat üçün DM" + geotag.

İndikatorlar: #model/#easycash həştəqləri, video sonlarında əlaqə məlumatı və ya link.

Monitorinq tövsiyəsi: hashtag + geotag kombinasiyasını izləyin; videoda görünən fon elementlərini və linkləri yoxlayın.

Twitter (X)

İstifadə üsulu: açıq elanlar, hashtag kampaniyaları, qısa linklərlə yönləndirmə; real vaxt SOS çağırışları da buradan gəlir.

Misal: "Job abroad! DM for details" + #job #visa.

İndikatorlar: yeni hesablardan eyni formalaşdırılmış postların təkrarlanması, bağlantılar və qısa URL-lər.

Monitorinq tövsiyəsi: Böyl axtarışlar, linklərin targetini açmadan arxivlə və reverse image yoxla.

Dating/apps (Tinder, Badoo, Bumble və s.)

İstifadə üsulu: romantik cəlb etmə (grooming) → sonra iş və ya səyahət təklifi; şəxsi görüşə dəvət etmə.

Misal: “Mən səyahət təşkilatçısıyam, sənin üçün iş tapa bilərəm; əlaqə üçün WhatsApp” (romantik başlanğıc).

İndikatorlar: sürətli şəxsi məlumat mübadiləsi, iş təklifinə tez keçid, əlaqə nömrəsinə keçid.

Monitorinq tövsiyəsi: hesabların çoxlu şikayətlərini, eyni şəklin müxtəlif profillərdə görünməsini izləyin.

YouTube / Shorts

İstifadə üsulu: uzun və ya qısa formalı reklam videoları, tutorial-tipli “işə necə getmək” və ya “model olmaq” videoları; description-da əlaqə.

Misal: “Model auditions in Istanbul — apply via Telegram” video description.

İndikatorlar: videonun description-ında şəxsi əlaqə, video altında spam şərhlər.

Monitorinq tövsiyəsi: video müəllifinin digər kanallarını və rəsmi əlaqə məlumatlarını yoxlayın.

Marketplaces və Classifieds (OLX, Craigslist və s.)

İstifadə üsulu: iş elanları, ev işləri, köməkçi kimi örtük; qısa mesajla əlaqə.

Misal: “Xaricdə ev işləri, yüksək maaş” elanları.

İndikatorlar: qeyri-adi tələblər (öncə ödəniş, sənəd və ya “agentlik haqqı”), eyni kontaktın müxtəlif elanlarda təkrarı.

Monitorinq tövsiyəsi: elan müəllifinin digər elanlarını və əlaqə tarixçəsini yoxlayın; şəkilləri reverse image.

Gaming platformaları və Virtual dünyalar (Discord, Roblox, Fortnite)

İstifadə üsulu: gənclərlə əlaqə qurmaq üçün oyun içi chat və Discord serverləri; “moderator”, “influencer” kimi rol alıb inandırma.

Misal: “Private server for models — apply” tipli Discord dəvətləri.

İndikatorlar: yaş doğrulaması olmayan hesablar, xüsusi serverə yönləndirmə, DM ilə təklif.

Monitorinq tövsiyəsi: oyun serverlərini və Discord linklərini izləyin, uşaqlar üçün təhlükəsizlik təlimatı verin.

Reddit və Forumlar

İstifadə üsulu: "job offers", "travel" və azsaylı subreddits vasitəsilə saxta elanlar; DM və ya xarici linklərlə yönləndirmə.

Misal: /r/forhire tipli subredditsdə saxta iş təklifləri. İndikatorlar: yeni hesabların job postları, linklərin xarici platformaya yönləndirməsi.

Monitorinq tövsiyəsi: subredditsdə moderator mesajlarını və post tarixçələrini yoxlayın.

Darknet / Tor bazarları

İstifadə üsulu: ekstremal halda istismar materiallarının satışı və sifarişi; bağlantıların əvvəlcə açıq platformalarda paylaşılması.

Misal: açıq platformada "exclusive offers" linki → darknet marketplace.

İndikatorlar: qısa URLlər, ödəniş kimi kriptovalyuta təklifləri, şifrəli kanallar.

Monitorinq tövsiyəsi: açıq platformada paylaşılmış linkləri təcrid edilmiş mühitdə analiz edin; hüquq-mühafizə ilə əlaqələndirin.

Ümumi indikatorlar — hər platformada axtarın

- "Asan qazanc", "vizasız", "model" kimi ifadələr.
- Hesabın yeni olması və ani fəaliyyət artımı.
- Şəxsi əlaqəyə (WhatsApp/Telegram/DM) yönləndirmə.
- Geotag ilə uyğunsuzluq (məsələn, Bakıda yerləşən profil Dubay geotagı göstərir).
- Eyni şəkil və ya mətnin çoxlu platformalarda təkrarlanması.
- Öncədən ödəniş və ya "agentlik haqqı" tələb edilməsi.
- Video/şəkildə təhdid, təzyiq və ya zorla yönləndirmə siqnalları.

Praktik tövsiyələr (monitorinq üçün)

1. Platformaya uyğun Böyl sorğuları hazırlayın (məs. Twitter/TikTok üçün hashtag+location; LinkedIn üçün "job" AND

“visa” NOT company_official).

2. Reverse image search (Google/TinEye) hər şübhəli vizual üçün tətbiq edin.

3. Tapılan hər riskli paylaşımı sənədləşdirin: screenshot, link, vaxt, profil ID.

4. Qapalı kanallara (Telegram/WhatsApp) yönləndirmə aşkar edilərsə, həmin keçidləri və profilləri hüquq-mühafizəyə ötürün.

5. Uşaqları və gəncləri hədəfləyən kampaniyalar üçün oyun və streaming platformalarını da daxil edin.

6. Məxfilik və etik qaydalara əməl edin — monitorinq edərkən qurbanın şəxsi təhlükəsizliyini prioritet tutun.

7. Platformalarla əməkdaşlıq olun: şübhəli hesabların report edilərək bloklanmasını tələb edin.

Platforma + tipik istifadə üsulu + risk indikatorları + monitorinq tövsiyyəsi cədvəli

Platforma	Tipik istifadə üsulu	Risk indikatorları	Monitorinq tövsiyəsi
Facebook / Marketplace / Qruplar	“Xaricdə iş”, ev işi, “mürəbbəlik”, agentlik elanları; qapalı qruplara yönləndirmə	Yeni yaradılmış hesablar tərəfindən eyni mətnin təkrarı; şəxsi DM-ə yönləndirmə; öncədən ödəniş tələb edən elanlar	Qrupları və Marketplace elanlarını Böyl ilə izləyin; şəkilləri TinEye/Google ilə yoxlayın; qapalı qrupları monitorinqə alın (mövcud ola bildikdə)
Instagram	Cəlbedici foto/video ilə “model/casting” elanları; bio-da “link in bio” → Telegram/WhatsApp	#model/#casting həştəqləri, bio-da şəxsi əlaqə və Telegram linki; çoxlu “sponsor” görüntüləri	Hashtag və bio izləmə; profillərin fotolarını reverse image ilə yoxlayın; “link in bio” URL-lərini arxivləşdirin
TikTok	Qısa viral videolarla “xaricdə iş”, “asandır qazanc”; challenge-lar; geotaglı elanlar	#easycash/#visa/#model həştəqləri + geotag; videonun sonunda WhatsApp/Telegram nömrəsi; lüks	Hashtag+geotag kombinasiyasını daimi izləyin; video fonunu (otel, hava limanı) analiz edin; şübhəli

		fon görüntüləri	videoları ekran görüntüsü ilə saxlayın
Twitter (X)	Qısa "job abroad" postları; hashtag kampaniyaları; qısa URL-lərlə yönləndirmə	Yeni hesablardan təkrarlanan postlar; qısa linklər (bit.ly) və DM yönləndirmələri	Böyl sorğularla hashtag-məkan axtarışları; qısa URL-ləri açmadan arxivlə və link targetini analiz et; SOS siqnallarına prioritet ver
LinkedIn	Saxta HR/şirkət profilləri üzərindən "rəsmi" iş təklifləri	Şirkətlərin yoxlanmamış domeni; profil məlumatı yoxdursa/şübhəlidirsə; CV göndərmə tələb olunur	Şirkət domeni və ofis ünvanını yoxla; iş elanı və employer profillərinin əlaqəsini araşdır; qeyri-adi "remote/visa" təkliflərinə şübhə ilə yanaş
WhatsApp / Telegram	Açıq platformada link paylaşılıb → qapalı qruplara/DM-lərə keçid (əsas kommunikasiya burada)	Açıq paylaşımda kanal/qrup linki, sonra ödəniş/sənəd tələbı; anonim adminlər	Açıq platformada paylaşılan linkləri sənədləşdir; qapalı kanalların sahibinin profilinə fokuslan; hüquq-mühafizəyə link və admin məlumatlarını ver
Dating apps (Tinder, Bumble, Badoo)	Romantik cəlbetmə → iş/səyahət təklifi; görüş üçün razılaşdırma	Sürətli şəxsi əlaqə tələbi; "mən işçi axtarıram" və ya "səyahət təşkil edirəm" kimi mesajlar	Hesab davranışını izləyin (tez biznesə keçid); eyni şəkil/foto birdən çox profildədirsə qeyd et; DM-lərdə iş söhbətlərinə diqqət
YouTube / Shorts	"Xaricdə necə iş tapmaq olar", "model müsabiqələri" videoları; description-da əlaqə	Description-da WhatsApp/Telegram linkləri; eyni video müxtəlif hesablar tərəfindən paylaşılır	Video müəllifinin digər kanallarını və rəsmi əlaqələrini yoxla; description linklərini arxivlə və analiz et

Classifieds (OLX, Craigslist, yerli elan saytları)	"Xaricdə ev işi", "ən yaxşı təklif" kimi klassik elanlar	Eyni kontaktın müxtəlif elanlarda təkrarı; öncədən ödəniş və ya agentlik haqqı tələb olunur	Kontaktların təkrarlanmasını və şəkillərin reverse image nəticələrini yoxla; əlaqə nömrələrini və e-poçtları sənədləşdir
Discord / Gaming (Roblox, Fortnite və s.)	Oyun içi chat və Discord serverləri vasitəsilə uşaqlarla əlaqə; "priv server" dəvətləri	Yaş doğrulamasının olmaması; server linkləri ilə qapalı dəvətlər; DM üzərindən "model" və ya "audition" dəvətləri	Uşaqlar üçün təhlükəsizlik təlimatı; oyun serverlərini və Discord dəvətlərini izləyin; şübhəli server linklərini hüquq-mühafizəyə ötürün
Reddit / Forumlar	/r/forhire və digər subredditsdə saxta iş elanları; xarici linklərlə yönləndirmə	Yeni hesabın "job" postları; linklərin xarici Telegram/WhatsApp-a çıxması	Subreddit moderatorlarının qeydlərinə baxın; post tarixçəsini və müəllif profilini yoxlayın; linkləri analiz et
Darknet / Tor bazarları	Aşkar istismar materiallarının və xidmətlərinin satışına yönəlmiş	Qısa URL-lərlə açıq platformadan yönləndirmələr; kripto ödəməsi tələb olunur	Açıq platformada paylaşılan qısa URL-ləri təhlükəsiz sandbox-da analiz et; hüquq-mühafizəyə məlumat verin

Qısa praktik qaydalar: hər platformada "xaricdə iş", "asandır qazanc", "model", "visa" kimi ifadələr və şəxsi əlaqəyə yönləndirmə əsas risk siqnallarıdır; eyni məzmunun çox platformada təkrarı şəbəkə əlamətidir; hər tapıntını ekran görüntüsü, link, vaxt və profil ID ilə sənədləşdirin; SOS/geotag siqnallarına prioritet verin; qurbanın anonimliyi və təhlükəsizliyini qoruyun.

Nəticə

İnsan alveri ilə mübarizədə sosial media və rəqəmsal platformalar xüsusi diqqət tələb edən məkanlardır, çünki cinayətkar şəbəkələr rekrutment, manipulyasiya və istismarı məhz bu kanallar vasitəsilə həyata keçirirlər. Ənənəvi olaraq Facebook, Instagram, Twitter (X), TikTok və LinkedIn açıq rekrutment elanlarının yayımlandığı, həmçinin qurbanlarla ilkin təmasın qurulduğu əsas meydanlardır. Facebook qruplarında və Marketplace-də "xaricdə iş" elanları, Instagram-da #model, #casting kimi həştəqlərlə yayılan paylaşımlar, TikTok-da qısa cazibədar videolar, LinkedIn-də saxta HR profilləri və Twitter-də "easy job abroad" tipli postlar insan alverçilərinin əsas vasitələrindəndir.

Daha qapalı ünsiyyət üçün isə WhatsApp və Telegram kanalları istifadə olunur. İnsan alverçiləri çox vaxt açıq platformada elan yerləşdirir, sonra isə qurbanı şəxsi mesencerə yönləndirərək manipulyasiya və nəzarəti artırırlar. Eyni metodikadan tanışlıq proqramlarında (Tinder, Badoo, Bumble) da istifadə edilir – romantik münasibət örtüyü altında iş və səyahət təklifi verilir. Bu, qurbanın etimadını qazanaraq onu xaricə aparmaq və ya şantaj yolu ilə istismara məcbur etmək üçün geniş yayılmış yanaşmadır.

Digər riskli məkanlar YouTube və Reddit forumlarıdır. YouTube-da "işə necə getmək", "model olmaq" adı ilə yerləşdirilən videoların description hissəsində WhatsApp və Telegram linkləri paylaşılır. Reddit və digər forumlarda isə saxta "for hire" elanları yerləşdirilir və DM vasitəsilə yönləndirmə aparılır. OLX, Craigslist kimi elan saytlarında "vizasız iş", "ev işləri" tipli qeyri-rəsmi elanlar da potensial risk daşıyır. Bu platformalarda eyni kontaktın müxtəlif elanlarda təkrarlandığı hallara rast gəlinir ki, bu da insan alveri şəbəkələrinin əlamətidir.

Son illər oyun platformaları (Roblox, Fortnite) və Discord serverləri də istismarçılar üçün yeni məkanlara çevrilib. Uşaqlarla oyun içi chat vasitəsilə tanışlıq qurulur, daha sonra onları ayrıca serverlərə dəvət edərək manipulyasiya edilir. Bu, xüsusilə azyaşlıların rəqəmsal təhlükəsizliyi baxımından ən kritik risklərdən biridir. Bəzi hallarda isə açıq platformalarda paylaşılan qısa URL-lər darknet ba-

zarlarına yönləndirilir və burada uşaq istismarı materialları və ya digər qanunsuz xidmətlər təqdim olunur.

Aşkarlama və xilas etmə baxımından bütün bu platformalarda bir neçə ortaq indikator nəzərə alınmalıdır: elanlarda "vizasız iş", "asan qazanc", "model agentliyi" kimi ifadələrin istifadəsi; hesabların çox yeni açılması və qeyri-normal aktivlik göstərməsi; WhatsApp və Telegram-a yönləndirmə; şəkillərin başqa mənbələrdən götürülməsi; SOS tipli həştəqlərin (#SOS, #SaveMe) geotag ilə birlikdə paylaşılması; videolarda otel otağı, avtovağzal, hava limanı kimi yerlərin görünməsi. Bu indikatorlar bir yerdə təhlil olunduqda risk siqnalları daha aydın görünür.

Qurtarma prosesində isə ən vacib məqam real vaxt monitorinqi və sürətli reaksiya mexanizmidir. SOS çağırışları dərhal hüquqmühafizə orqanlarına ötürülməli, tapıntılar ekran görüntüsü və linklərlə sənədləşdirilməli, qurbanın anonimliyi və təhlükəsizliyi qorunmalıdır. Hər bir platformada aparılan monitorinqdə yalnız açıq məlumatlar əsasında işləmək, qurbanların kimliyini ictimaiyyətə açıqlamamaq və etik prinsiplərə riayət etmək vacibdir.

Beləliklə, insan alverçiləri Facebook-dan TikTok-a, LinkedIndən Discord-a qədər geniş platforma spektrindən istifadə edirlər. Aşkarlama üçün hashtag, geotag və mətn analizi, reverse image search və Böyl axtarışları kimi üsullar tətbiq edilməli, xilas etmə isə operativ sənədləşdirmə, hüquqi əlaqələndirmə və qurbanın təhlükəsizliyi əsasında qurulmalıdır. Bu yanaşma həm qlobal, həm də Azərbaycan reallığında insan alverinə qarşı mübarizədə rəqəmsal mühitin izlənməsini zəruri və strateji alətə çevirir.

4. Açar sözlər və Böyl siyahısı

Açar sözlər və Böylün axtarış üsulları insan alveri ilə mübarizədə rəqəmsal monitorinqin əsas sütunlarından biridir. Sadə açar söz axtarışında “iş”, “vizasız”, “model” kimi sözlər yazmaq kifayət edir, amma bu çox geniş nəticələr verir. Böyl üsulu isə AND, OR, NOT, “” (tırnaq işarəsi) və () operatorlarından istifadə etməklə daha hədəfli nəticə əldə etməyə imkan yaradır. Bu üsul monitorinqdə həm açıq riskli elanların, həm də dolayı SOS çağırışlarının aşkarlanmasında mühüm rol oynayır.

Məsələn, təkcə “iş” sözünü izləsək, minlərlə nəticə çıxacaq. Amma "iş" AND "Dubai" sorğusu yalnız Dubayla bağlı iş elanlarını göstərəcək. Burada həm açar söz, həm də məkan faktoru birləşdirildiyi üçün risk siqnallarını daraltmaq olur. Eyni qayda ilə "iş" AND ("model" OR "qızlar") axtarışı insan alverçilərinin tipik elanlarını üzə çıxara bilər. Bu, xüsusilə sosial mediada tez-tez rast gəlinən “model agentliyi” örtüyü altında rekrutment hallarının aşkarlanması üçün faydalıdır.

SOS çağırışlarının izlənməsi üçün də Böyl axtarışları əlverişlidir. Məsələn, "#SOS" OR "#SaveMe" sorğusu bütün təcili yardım çağırışlarını çıxara bilər. Əgər buna məkan əlavə edilsə, məsələn, "#SOS" AND "Bakı" yazılsa, nəticələr yalnız Bakıda paylaşılmış çağırışları göstərəcək. Bu, real vaxt müdaxilə üçün kritik əhəmiyyət daşıyır.

Kiberzorakılıq və şantaj hallarında Böyl üsulları daha da dəyərli olur. Məsələn, "foto" AND ("şantaj" OR "nudes") sorğusu şantaj riskli paylaşımları üzə çıxara bilər. Azərbaycan reallığında “şəxsi şəkillər yayılıb” və ya “şantaj edirlər” tipli açıq yazışmalar belə sorğularla tapıla bilər. Bu hallarda monitorinqçi yalnız açıq mətnə baxmaqla kifayətlənməyib, paylaşımın kim tərəfindən edildiyini, hansı geotag ilə yayımlandığını və əlaqə nömrəsi olub-olmadığını da yoxlamalıdır.

Praktik nümunələr:

- "iş" AND "Türkiyə" NOT "təqaüd" → Türkiyədə iş elanlarını göstərir, amma təqaüd proqramlarını çıxarır.

- "model" OR "casting" AND "Bakı" → Bakıda yayılan model işləri və ya kastinq elanlarını tapır.
- ("#SOS" OR "#Help") AND "Gəncə" → Gəncədə paylaşılan SOS çağırışlarını üzə çıxarır.
- "kolay para" AND "WhatsApp" → saxta asan qazanc elanları + əlaqə nömrələri ilə bağlı paylaşımları aşkarlayır.

Polaris Projectin hesabatında göstərilir ki, insan alverçilərinin 70%-dən çoxu açıq platformalarda elan yerləşdirir və sonradan qurbanları WhatsApp və Telegram kimi qapalı platformalara yönləndirir. Buna görə Böyl üsulları açıq elanların aşkar edilməsində, qapalı şəbəkəyə keçiddən əvvəl riskləri görməkdə çox dəyərlidir.

Nəticə olaraq, açar söz və Böyl axtarışları monitorinqin ən mühüm alətlərindəndir. Sadə açar sözlər geniş məlumat verir, Böyl isə onu daraldaraq riskli nümunələri üzə çıxarır. Sosial mediada "iş", "model", "kolay para", "visa", "escort" kimi açar sözlər tipik risk siqnallarıdır. Böyl üsulu isə bunları məkan, zaman və kontekstə görə dəqiqləşdirməyə imkan yaradır. Beləliklə, həm riskli elanların, həm də qurbanların real vaxt yardım çağırışlarının vaxtında aşkar edilməsi mümkün olur və bu, insan həyatının xilas edilməsinə birbaşa təsir göstərir.

Böylün hazır sorğu nümunələri

Twitter (X) üçün

- "iş" AND "Dubai"
- ("#SOS" OR "#Help" OR "#SaveMe") AND ("Bakı" OR "Gəncə")
- "model" AND ("iş" OR "agentlik") AND NOT "təqaüd"
- "escort" OR "masaj" NOT "terapiya"
- "kolay para" AND "WhatsApp"

TikTok üçün

- #iş AND #Dubai
- #easycash OR #kolaypara AND #visa
- #SOS AND (Bakı OR Sumqayıt OR Gəncə)
- ("model" OR "casting") AND ("iş" OR "Bakı")

- "Yeni həyat" AND ("pulsuz bilet" OR "tez qazanc")

Instagram üçün

- #model OR #casting AND ("iş" OR "agentlik")
- ("iş" AND "vizasız") OR ("iş" AND "xaric")
- ("kolay para" OR "easycash") AND ("DM" OR "link in bio")
- "iş axtarıram" AND NOT "rəsmi agentlik"
- #SOS OR #SaveMe OR #qurtarın

LinkedIn üçün

- "job" AND ("visa sponsorship" OR "abroad")
- "HR" AND "Turkey" AND NOT "official company"
- "remote work" AND ("easy cash" OR "quick money")
- "model" OR "casting" AND "agency"
- "job offer" AND ("Telegram" OR "WhatsApp")

Facebook / Marketplace üçün

- ("iş" OR "job") AND ("xaric" OR "abroad") AND NOT "təqaüd"
- "model" AND ("iş" OR "agentlik")
- ("visa" OR "pulsuz bilet") AND ("iş" OR "xaric")
- ("kolay para" OR "easy money") AND ("əlavə qazanc")
- "iş axtarıram" AND ("Dubai" OR "İstanbul")

Digər nümunələr (ümumi)

- "iş" AND ("otel" OR "ev işi" OR "aşpaz") AND NOT "rəsmi agentlik"
- "şantaj" OR "nudes" OR "ifşa" AND "foto"
- ("uşaq" OR "yeniyetmə") AND ("iş" OR "casting")
- "travel" AND ("free visa" OR "work abroad")
- ("SOS" OR "Help") AND ("location" OR "geotag")

4.1. Kateqoriya üzrə sadə açar sözlər

1. İş elanları və saxta təkliflər
- iş
- iş axtarıram
- xaricdə iş
- vizasız iş
- ev işi
- model işi
- casting
- asan qazanc
- easycash
- kolay para
- pulsuz bilet
- yeni həyat

Misal:
TikTok-da “xaricdə iş” yazıldıqda çox vaxt Dubay və ya Türkiyə ilə bağlı riskli elanlar görünür.

SOS çağırışları və yardım siqnalları
- SOS
- Help
- SaveMe
- qurtarın
- kömək edin
- çıxarın məni
- dayandırın
- məni saxlayırlar
- itkin düşdü
- tapın məni

Misal:
Twitter-də “kömək edin” yazan və geotag əlavə edən paylaşımlar çox vaxt real vaxt siqnallarıdır.

Kiberzorakılıq və şantaj

- şantaj
- foto ifşa
- video yayıldı
- gizli çəkiliş
- nudes
- ifşa etdim
- təhdid
- zorla
- pul tələb edir
- məcbur edir

Misal:

Instagram şərhlərində "foto ifşa" yazılması çox vaxt şantaj və ya qurbanın təzyiq altında qalmasının göstəricisidir.

Uşaqlarla bağlı risklər

- uşaq işçisi
- yeniyetmə işçi
- uşaq baxıcısı
- babysitter
- child job
- teen model
- uşaq modellər
- tələbə iş
- qız uşağı
- oğlan uşağı

Misal:

Facebook-da "uşaq baxıcısı" elanları çox vaxt normal ola bilər, amma "xaricdə uşaq baxıcısı, vizasız" kimi elanlar riskli olur.

Səyahət və köçürülmə riskləri

- viza
- vizasız
- sərhəd
- bilet
- pulsuz yol

- turist iş
- travel work
- iş vizası
- deportasiya
- gedirəm xaricə

Misal:

LinkedIn-də “iş vizası ilə pulsuz gediş” tipli elanlar insan alverçilərinin istifadə etdiyi aldatma üsuludur.

Cinsi istismar və xidmət örtükləri

- escort
- masaj
- SPA qızları
- iş qadını
- nightlife
- bar işi
- klub işi
- gecə işi
- model xidmətləri
- təklif olunur qız

Misal:

Craigslist və ya OLX kimi saytlarda “masaj xidməti” elanlarının bəziləri əslində gizli istismar məqsədli olur.

Geotag və məkan açar sözləri

- Bakı avtovağzal
- Heydər Əliyev hava limanı
- Sumqayıt
- Gəncə
- Tbilisi
- İstanbul
- Ankara
- Dubay
- Moskva
- Avropa işləri

Misal:

TikTok-da “Dubay işləri” həştəqi + geotag Dubay → tipik insan alveri cəlb üsulu.

Kateqoriya	Açar sözlər	Praktiki misal
İş elanları və saxta təkliflər	iş, iş axtarıram, xaricdə iş, vizasız iş, ev işi, model işi, casting, asan qazanc, easycash, kolay para, pulsuz bilet, yeni həyat	TikTok-da “xaricdə iş” həştəqi ilə Dubayda yerləşdirilmiş elan → saxta iş təklifi və istismar riski
SOS çağırışları və yardım siqnalları	SOS, Help, SaveMe, qurtarın, kömək edin, çıxarın məni, dayandırın, məni saxlayırlar, itkin düşdü, tapın məni	Twitter-də “#SOS kömək edin” yazan tvit + geotag Bakı avtovağzal → real vaxt yardım siqnalı
Kiberzorakılıq və şantaj	şantaj, foto ifşa, video yayıldı, gizli çəkiliş, nudes, ifşa etdim, təhdid, zorla, pul tələb edir, məcbur edir	Instagram şərhində “şəkillərini ifşa edəcəyik” yazısı → qurbanın şantaj olunması əlaməti
Uşaqlarla bağlı risklər	uşaq işçisi, yeniyetmə işçi, uşaq baxıcısı, babysitter, child job, teen model, uşaq modellər, tələbə iş, qız uşağı, oğlan uşağı	Facebook-da “vizasız xaricdə uşaq baxıcısı” elanları → potensial insan alveri riski
Səyahət və köçürülmə riskləri	viza, vizasız, sərhəd, bilet, pulsuz yol, turist iş, travel work, iş vizası, deportasiya, gedirəm xaricə	LinkedIn-də “vizasız iş vizası ilə Avropaya gedin” elanları → şübhəli və qeyri-rəsmi təklif
Cinsi istismar və xidmət örtükləri	escort, masaj, SPA qızları, iş qadını, nightlife, bar işi, klub işi, gecə işi, model xidmətləri, təklif olunur qız	OLX-da “masaj qızları” elanları → gizli istismar məqsədli elan
Geotag və məkan açar sözləri	Bakı avtovağzal, Heydər Əliyev hava limanı, Sumqayıt, Gəncə, Tbilisi, İstanbul, Ankara, Dubay, Moskva, Avropa işləri	TikTok-da “#iş” həştəqi + geotag Dubay → Dubaya aparılma riski

4.2. Böyl axtarış nümunələri

Böyl nədir və niyə önəmlidir? Böylün axtarış – açar sözləri AND, OR, NOT, dırnaq "", mötərizə ( ) və bəzən ulduz * kimi operatorlarla birləşdirərək nəticələri daraltmaq (dəqiqləşdirmək) və ya genişləndirmək metodudur. Məqsəd: çox böyük məlumat axınında (Twitter, TikTok, Instagram, LinkedIn, Facebook, elan saytları və s.) risk siqnallarını daha tez və daha az səs-küylə tapmaq.

Əsas operatorların məntiqi (qısa):

- **AND** – hər iki söz mütləq olsun → nəticə **daralır**.
- **OR** – alternativ sözlərdən hər hansı biri kifayətdir → nəticə **genişlənir**.
- **NOT** – arzuolunmaz sözü çıxarır → **səsi azaldır**.
- **" " (dırnaq)** – tam ifadəni eyni ardıcıllıqla tapır → **yanlış pozitivləri azaldır**.
- **( )** – qruplaşdırma; uzun sorğuların məntiqini saxlayır.
- ***** – kök formasını genişləndirir (məs., **traf*** → traffic, trafficking, trafik).

“Xaricdə iş” və saxta təkliflər (rekrutment) – dəqiqləşdirilmiş nümunələr

Məntiq: “iş” sözü çox ümumidir; **məkan** + **mövzu** + bəzən **forma** (model/casting) əlavə edərək riskli elanlara yaxınlaşırıq.

- "iş" AND "Dubai"

İzah: “iş” + Dubayla əlaqəli paylaşımları gətirir. Saxta “vizasız iş” elanları tez görünür.

- "xaricdə iş" AND ("vizasız" OR "pulsuz bilet")

İzah: Xaricdə iş mövzusunu riskli sözlərlə (vizasız, pulsuz bilet) birləşdirir → istismar riski artır.

- ("model işi" OR "casting") AND ("Bakı" OR "İstanbul" OR "Dubai")

İzah: “Model agentliyi” örtüyü ilə edilən cəlbləri hədəf şəhərlər üzrə toplar.

- "iş" AND ("ev işi" OR "dayə" OR "babysitter") AND NOT "rəsmi agentlik"

İzah: Ev işləri sahəsində qeyri-rəsmi elanları seçir; rəsmi

agentlikləri çıxarır.

- "job" AND "free visa" AND ("Gulf" OR "UAE" OR "Dubai")

İzah: İngiliscə paylaşılmış Körfəz istiqamətli riskli elanları toplayır.

SOS və real vaxt yardım çağırışları – yüksək prioritet

Məntiq: SOS siqnalı bəzən açıq, bəzən dolayıdır. Hashtag + məkan kombinasiyası **operativ reaksiya** üçündür.

- ("#SOS" OR "#Help" OR "#SaveMe") AND ("Bakı" OR "Gəncə" OR "Sumqayıt")

İzah: Təcili çağırışları yalnız lokal məkanlarla qaytara bilər.

- ("kömək edin" OR "məni saxlayırlar" OR "çıxarın məni") AND ("metro" OR "avtovağzal" OR "hava limanı")

İzah: Dilimizdəki açıq SOS ifadələri + tez-tez rast gəlinən tranzit məkanlar.

- "help me" AND ("kidnapped" OR "trapped") AND ("location" OR "address")

İzah: İngiliscə SOS siqnalları; məkan göstəricisi varsa qırmızı bayraq.

Kiberzorakılıq, şantaj və ifşa – dolayı istismar indikatorları

Məntiq: Qurbanların təzyiq altında saxlanması və şantaj kanalları tez-tez açıq mətndə görünür.

- ("şantaj" OR "ifşa" OR "video yayıldı") AND ("foto" OR "nudes")

İzah: Şantajın tipik sözləri + material növü.

- "ifşa edəcəyəm" AND ("pul" OR "money" OR "ödə")

İzah: Maddi tələb ilə birləşən hədə.

- ("deepfake" OR "fake video") AND ("qız" OR "woman" OR "female")

İzah: Saxta video ilə hədəfə alma—qadınlara yönəlmiş zorakı təzyiq dinamika

Uşaqlarla (yeniyetmələrlə) bağlı risklər – prioritetləndirilmiş izlə

Məntiq: “uşaq/yeniyetmə + iş/casting” kombinasiyaları, eləcə də “grooming” izləri.

- ("uşaq" OR "yeniyetmə" OR "teen") AND ("iş" OR "model" OR "casting")

İzah: Yetkinlik yaşına çatmayanların “iş” mövzusu – yüksək risk.

- ("babysitter" OR "uşaq baxıcısı") AND ("vizasız" OR "pulsuz")

İzah: Uşaq baxıcılığı elanlarında qeyri-rəsmi yekunlar istismara açıqdır.

- ("Discord" OR "server") AND ("invite" OR "davet") AND ("model" OR "photo")

İzah: Uşaqların oyun/Discord kanalları üzərindən gizli dəvətlərlə cəlbi.

Cinsi istismar və “xidmət” örtükləri – terminoloji tələlər

Məntiq: “escort/masaj/nightlife” tipli sözlər bəzi platformalarda istismar örtüyüdür; tibbi/legitim məzmunu çıxarmaq lazımdır.

- ("escort" OR "masaj" OR "SPA qızları" OR "nightlife") AND ("iş" OR "iş təklifi") AND NOT ("fizioterapiya" OR "terapiya")

İzah: Əlaqəsiz tibbi nəticələri NOT ilə çıxarır, istismar niyyətli elanları saxlayır.

- ("klub işi" OR "bar işi" OR "gecə işi") AND ("qızlar" OR "women")

İzah: Gecə işləri adı altında riskli cəlb elanları.

Səyahət, viza və köçürülmə – marşrut siqnalları

Məntiq: “viza + iş”, “pulsuz bilet” və “tez köçürülmə” iddiaları tipik tələdir.

- ("visa" OR "vizasız") AND ("iş" OR "job") AND ("tez" OR "immediate")

İzah: Çevik, sənədsiz köçürmə vədləri → xüsusi risk.

- ("pulsuz bilet" OR "free ticket") AND ("iş" OR "model")

İzah: Süni cəlbetmə; qapalı mesencerə yönləndirməyə baxın.

Platforma-spesifik yazım nümunələri (praktik)

Məntiq: Hər platformanın axtarış imkanları fərqlidir; konsept eynidir, sintaksis dəyişə bilər.

Twitter (X):

✓ ("#SOS" OR "#Help") ("Bakı" OR "Gəncə") *(hashtag + məkan sözü)*

✓ "iş" "Dubai" *(tırnaqda tam ifadə və ya ardıcıl sözlər)*

TikTok:

✓ #iş #Dubai *(hashtag + hashtag)*

✓ #easycash #visa *(trend etikləri birlikdə izlənir)*

Instagram:

✓ #model OR #casting "iş" *(hashtag + söz)*

✓ "link in bio" ("job" OR "visa") *(bio üzərindən yönləndirmələr)*

LinkedIn:

✓ "job" ("visa sponsorship" OR "abroad") NOT "official site"

✓ "HR" "Turkey" NOT "verified company"

Facebook / Marketplace:

✓ ("iş" OR "job") ("xaric" OR "abroad") NOT "təqaüd"

✓ "ev işi" "vizasız"

Elan saytları (OLX və s.):

✓ ("model" OR "casting") ("iş" OR "job") ("İstanbul" OR "Dubai")

✓ ("babysitter" OR "uşaq baxıcısı") ("vizasız" OR "pulsuz bilet")

YouTube / Shorts (axtarış çubuğunda):

✓ "how to get job in Dubai" ("free visa" OR "ticket")

✓ "model audition" ("Telegram" OR "WhatsApp")

Geotag və məkan siqnallarını əlavə etmək

Məntiq: məkan sözü/etiketi sorğuya daxil olduqda **operativ** hadisələr önə çıxır.

✓ ("iş" OR "model") AND ("Dubay" OR "İstanbul" OR "Bakı avtovağzal")

✓ ("#SOS" OR "kömək edin") AND ("hava limanı" OR "railway" OR "bus station")

Ajiotajı azaltmaq üçün NOT və dırnaqlardan ağıllı istifadə

✓ "model işi" NOT "3D model" NOT "design" – "3D model" kimi əlaqəsiz nəticələri kəsir.

✓ "masaj işi" NOT "fizioterapiya" NOT "esthetic clinic" – tibbi/müalicə kontentini çıxarır.

✓ "iş vizası" NOT "məsləhət" NOT "məqalə" – məlumatlandırıcı yazıları kənara qoyur, elanlara fokuslanır.

Kateqoriya	Sadə açar sözlər	Böyl nümunələri
İş elanları	xaricdə iş, vizasız iş, sponsorlu iş, iş üçün gedirəm	("xaricdə iş" OR "vizasız iş" OR "sponsorlu iş") AND ("pulsuz yaşayış" OR "yol xərci mən tərəfdən")
İş elanları	agent haqqı, komissiya, placement fee, ön ödəniş	("agent haqqı" OR "komissiya" OR "placement fee" OR "ön ödəniş") AND ("iş" OR "vakansiya")
İş elanları	təcrübə tələb olunmur, çox asan iş, iş elanları	("təcrübə tələb olunmur" OR "çox asan iş") AND ("xaricdə iş" OR "iş elanları")
İş elanları	vizasız, sənədləşmə biz tərəfdən, sponsor	("vizasız" OR "sponsor" OR "sənədləşmə biz tərəfdən") AND ("iş" OR "xaricdə")
Manipulyasiya	etibar et mənə, sənə kömək edəcəm, yol xərci mən tərəfdən	("etibar et mənə" OR "sənə kömək edəcəm") AND ("iş" OR "gedirəm")
İstismar	escort, masaj salonu, model axtarılır,	("escort" OR "masaj salonu" OR "model

	xidmətçi	axtarılır") AND ("iş" OR "vakansiya" OR "qadın" OR "qız")
İstismar	məcburi əmək, borc var, borc qarşılığında işləmək	("borc" OR "avans" OR "placement fee") AND ("işləmək" OR "məcburi əmək" OR "geri qaytarmaq")
İstismar	pasportumu saxlayırlar, sənədlər işəgötürəndə qalır	("pasport" OR "sənəd") AND ("saxlayırlar" OR "tutublar" OR "vermirlər")
Yardım siqnalları	kömək et, çıxa bilmirəm, geri qayıda bilmirəm, məni buraxmırlar, satılıram	("kömək et" OR "çıxa bilmirəm" OR "geri qayıda bilmirəm" OR "məni buraxmırlar" OR "satılıram") AND ("iş" OR "xaricdə")
Uşaqların cəlbi	uşaq üçün iş, azyaşlı işçi, 15 yaşlı, azyaşlı model	("uşaq üçün iş" OR "azyaşlı işçi" OR "15 yaşlı" OR "azyaşlı model") AND ("iş" OR "model" OR "gənc qız")

Etik və əməli məqamlar. Axtarışlar yalnız açıq məlumatlar əsasında aparılmalıdır; qurbanın anonimliyi qorunmalı, potensial SOS siqnallarına dərhal prioritet reaksiya verilməlidir. Hər tapıntı sənədləşdirilməlidir: ekran görüntüsü, link, zaman damğası, profil ID. Şübhəli hallarda hüquq-mühafizə və müvafiq QHT şəbəkəsi ilə əlaqələndirmə aparılmalıdır.

4.3. İstifadə qaydaları (addım-addım)

1) Məqsudu və hüquqi çərçivəni dəqiqləşdir

• Missiyanız: “Riskli elanları və SOS siqnallarını aşkarlamaq, sənədləşdirmək, təhlükəsiz eskalasiya etmək.”

• Yalnız açıq məlumatlar ilə işləyin; gizli hesabları “qırmayın”, şəxsi məlumat toplamaqda minimum prinsipinə əməl

edin.

- QHT-lər və hüquq-mühafizə ilə əməkdaşlıq protokolu öncədən razılaşdırılsın.

2) Komanda və əməli rol bölgüsü qur

- Monitorinq (axtarış və ilkin analiz), Təsdiqləmə (forensik yoxlama), Sənədləşdirmə (sübutların toplanması), Eskalasiya (təcili yönləndirmə) rollarını ayırın.
- Növbəlilik və "ikinci baxış" (peer review) qaydasını tətbiq edin.

3) Kateqoriya və indikator siyahısı yaradın

- Kateqoriyalar: "İş elanları/saxta təkliflər", "SOS siqnalları", "Kiberzorakılıq/şantaj", "Uşaqlarla bağlı risklər", "Cinsi istismar örtükləri", "Səyahət/Viza riski", "Geotag-məkan".
- Hər kateqoriya üçün sadə açar sözlər + Böyl paketləri hazır saxlayın (aşağıdakı nümunələrdən istifadə edin).

4) Açar söz toxumu (seed) topla, sonra genişləndir

- Toxum: "iş, vizasız, model, casting, easycash, pulsuz bilet, SOS, kömək edin…"
- Genişləndir: sinonimlər, yazım variantları (kolay para/easycash), dillər (az/en/ru/tr), transliterasiya (Dubay/Dubai/دبي).

5) Böyl məntiqini praktik qaydaya çevir

- AND daraldır, OR genişləndirir, NOT səsi azaldır, " " tam ifadə, ( ) qruplaşdırma.
- Çərçivə: Mövzu + Məkan + Risk sözü + (istənməyənləri NOT-la çıxart).

6) Platforma üzrə sintaksisi düzgün tətbiq et (nümunələrlə)

- Twitter (X):

("iş" OR "xaricdə iş") AND ("Dubai" OR "İstanbul") ("#SOS" OR "#Help") AND ("Bakı" OR "Gəncə") "escort" OR "masaj" NOT "terapiya"

- TikTok (hashtag-a daha həssas):

#iş #Dubai , #easycash #visa , #SOS #Bakı ("model" OR "casting") AND "Bakı" (axtarış çubuğunda)

- Instagram:

#model OR #casting "iş" , ("kolay para" OR "easycash") AND ("DM" OR "link in bio")

- LinkedIn:

"job" AND ("visa sponsorship" OR "abroad") NOT "official site" "HR" "Turkey" NOT "verified company"

- Facebook/Marketplace:

("iş" OR "job") AND ("xaric" OR "abroad") NOT "təqaüd" "ev işi" "vizasız"

- Elan saytları (OLX və s.):

("model" OR "casting") ("İstanbul" OR "Dubai") ("iş" OR "job")

7) Hashtag + geotag izləməsini qoş

- Həştəq siyahıları: #iş, #model, #casting, #easycash, #visa, #SOS, #SaveMe, #qurtarın.
- Geotag/ məkan sözləri: "Bakı avtovağzal, Heydər Əliyev hava limanı, Gəncə, Sumqayıt, İstanbul, Dubay".
- Kombinasiya nümunəsi: #iş AND Dubay, #SOS AND Bakı.

8) Nəticələri triiyaj et (sürətli risk qiymətləndir)

- Yüksək risk (qırmızı): SOS + məkan; uşaqla bağlı istismar; şantaj/ifşa + pul tələbi; WhatsApp/Telegram nömrəsi.
- Orta risk (sarı): "vizasız iş", "pulsuz bilet", "asandır qazanc", lüks fonda iş vədi.
- Aşağı risk (yaşıl): ümumi "iş" paylaşımları, məlumatlandırıcı postlar.

9) Təsdiqləmə (verification) qaydası

- Reverse image search (Google/TinEye): elan şəkilləri başqa yerdən oğurlanıbsa — saxta siqnaldır.
- Link analizi: qısa URL (bit.ly və s.) hara aparır? "link in bio" → Telegram/WhatsApp?
- Mətn anomaliyası: eyni mətn müxtəlif profillərdə təkrarlanırsa — şəbəkə əlaməti.
- Profil tarixi: çox yeni hesab + yüksək aktivlik → diqqət.

10) Sənədləşdir və zəncirvari sübut yarat

- Ekran görüntüləri (UI + tarix/zaman zolağı görünsün), link, post ID/username, məzmun, geotag, həştəq siyahısı.
- Qısa xülasə yaz: "Nə görüldü? Niyə risklidir? Növbəti addım nədir?"

11) Eskalasiya və koordinasiya

- Yüksək risk halları dərhal hüquq-mühafizəyə və müvafiq QHT-yə yönləndir.
- Platformaya report göndər, post/hesabın dondurulmasını istə.
- Qurbanla birbaşa əlaqəyə girmə (dəstək xətti/protokol üzərindən hərəkət et**).**

12) Etik və məxfilik

- Qurbanın kimliyini ifşa etmə, paylaşımları yenidən yayma; yalnız zəruri məlumatları bölüş. Məlumatları məhdud çıxışla saxla; daxili paylaşımda "zəruri məlumat" prinsipi.

13) Tipik ssenarilər üçün mini-playbooklar (nümunə sorğu + reaksiya)

TikTok "Dubayda model işi" videosu:

Axtar: #model #iş #Dubai → Risk: lüks fon + əlaqə → Təsdiqlə: reverse image + bio link → Eskalasiya: sənədləşdir, hüquq-mühafizə/QHT.

Twitter #SOS + geotag:

Axtar: ("#SOS" OR "#Help") AND "Bakı" → Risk: yüksək → Təsdiqlə: profil tarixi, məkan → Eskalasiya: dərhal bildiriş, postu arxivlə.

LinkedIn "visa sponsorship" təklifi:

Axtar: "job" AND "visa sponsorship" NOT "official" → Risk: orta/yüksək → Təsdiqlə: domen, adres, HR profili → Eskalasiya: report + xəbərdarlıq.

14) Çoxdilli və yazım variantlarını unutma

- Dubay/Dubai/دبي; "kolay para/easycash"; "iş/işe/job/work".
- Lokal slang və qısa yazımlar: "visa spnsr", "free tkt", "mdl job".

15) Yalan pozitivləri azalt (NOT + dırnaq)

- "model işi" NOT "3D model" NOT "design"
- "masaj işi" NOT "fizioterapiya" NOT "clinic"
- "iş vizası" NOT "məqalə" NOT "məsləhət"

16) Əməli təhlükəsizlik (OpSec)

- Şəxsi hesabdan monitorinq etmə; əməli hesab istifadə et.

- Şübhəli linkləri izolyasiya olunmuş mühitdə aç; cihaz təhlükəsizliyini qoruyun.

17) Metriklər və keyfiyyət

- Göstəricilər: aşkarlanan case sayı, yalan pozitiv faizi, eskalasiyaya qədər orta vaxt, xilasetmə ilə nəticələnən hallar.
- Həftəlik baxış: hansı sorğular işləyir, hansılar səs-küy yaradır?

18) Davamlı təkmilləşdirmə

- Yeni trendlərə uyğun söz siyahısını yenilə (məs., yeni həştəqlər).
- Komanda daxilində mini-treninqlər və “case review” toplantıları keçir.

Tez tətbiq üçün hazır sorğu nümunələri (qısa xatırlatma)

- İş təklifi riskləri:"xaricdə iş" AND ("vizasız" OR "pulsuz bilet")

("model" OR "casting") AND ("Bakı" OR "İstanbul" OR "Dubai")

- SOS siqnalları:

("#SOS" OR "#Help" OR "#SaveMe") AND ("Bakı" OR "Gəncə")

("kömək edin" OR "məni saxlayırlar") AND ("avtovağzal" OR "hava limanı")

- Şantaj/ifşa:

("şantaj" OR "ifşa") AND ("foto" OR "video" OR "nudes") NOT "xəbər"

- Uşaqlarla risk:

("uşaq" OR "teen") AND ("model" OR "iş" OR "casting")

Monitorinq və eskalasiya cədvəli

Addım	Sorğu (Böyl / sadə)	Nəticə (qısa təsvir)	Risk səviyyəsi	Sübut (qeydlər)	Eskalasiya tarixi
1	"iş" AND "Dubai"	TikTok-da “vizasız iş” elanları Dubayla bağlı göründü	🟡 Orta	Video linki + ekran görüntüsü + profil adı	29/09/2025
2	("#SOS" OR "#Help") AND "Bakı"	Twitter-də SOS siqnalı + geotag Bakı avtovağzal	🔴 Yüksək	Tweet linki, screenshot, istifadəçi ID	29/09/2025 (dərhal)
3	("şantaj" OR "ifşa") AND ("foto" OR "video")	Instagram şərhində qurban “şəkillərimi ifşa edirlər” yazıb	🔴 Yüksək	Şərh screenshot + profil ID	28/09/2025
4	("uşaq" OR "teen") AND ("model" OR "iş")	Facebook-da “teen model işi” elanları tapıldı	🔴 Yüksək	Elan screenshot + link	28/09/2025
5	"escort" OR "masaj" NOT "terapiya"	OLX-da “masaj qızları” elanları → istismar şübhəsi	🟡 Orta	Ekran görüntüsü, əlaqə nömrəsi	27/09/2025
6	"visa" AND "free ticket"	LinkedIn-də “pulsuz vizalı iş” təklifləri → şübhəli	🟡 Orta	Post linki + screenshot	26/09/2025
7	#easycash #visa	TikTok-da trend video – “tez pul qazan” + geotag İstanbul	🟡 Orta	Video linki + fon analizi	26/09/2025
8	("kömək edin" OR "çıxarın məni") AND ("metro" OR "avtovağzal")	Twitter-də qız “məni saxlayırlar” yazıb → məkan avtovağzal	🔴 Yüksək	Post linki + screenshot	25/09/2025 (dərhal)

5. Risk qiymətləndirilməsi (matrisası)

Rəqəmsal insan alveri probleminin qiymətləndirilməsində risk matrisi xüsusi əhəmiyyət kəsb edir, çünki bu yanaşma həm qurbanların aşkarlanması, həm də potensial istismar hallarının proqnozlaşdırılması üçün sistemli çərçivə təqdim edir. Risk matrisi müxtəlif dəyişənlərin — texnoloji alətlər, sosial şəbəkə davranışları, qurbanın sosial-demoqrafik xüsusiyyətləri, cinayətkar şəbəkələrin fəaliyyət metodları — kəsişməsini təhlil etməyə imkan verir. Bu matrisi tətbiq etməklə tədqiqatçılar və praktiki mütəxəssislər müəyyən edə bilirlər ki, hansı faktorlar daha yüksək risk zonasında yerləşir, hansı hallarda isə monitorinq minimal təhlükə göstəricilərinə əsaslanmalıdır.

Akademik ədəbiyyatda risk matrisinin rəqəmsal insan alveri kontekstində istifadəsi "multifaktorial yanaşma" prinsipi ilə izah olunur. Burada əsasən üç səviyyə fərqləndirilir: fərdi səviyyə (qurbanın yaş, cins, iqtisadi vəziyyət, rəqəmsal savadlılıq kimi göstəriciləri), mühit səviyyəsi (ailə, icma, miqrasiya təcrübəsi, sosial təcrid) və texnoloji səviyyə (onlayn platformaların istifadəsi, kibertəhlükəsizlik boşluqları, sosial mediada iz buraxma). Bu yanaşma Bronfenbrennerin ekoloji sistem nəzəriyyəsi ilə də uzlaşır, çünki hər bir səviyyə digərini gücləndirə və ya zəiflədə bilər[49].

Risk matrisi eyni zamanda hüquq-mühafizə və sosial iş praktikasında prioritetləşdirmə funksiyasını daşıyır. Yüksək risk zonasında yerləşən hallar — məsələn, yetkinlik yaşına çatmayanların onlayn tanışlıq platformalarında təkrar-təkrar şübhəli şəxslərlə əlaqə yaratması və ya iqtisadi çətinliklər fonunda sosial mediada iş elanlarına həssaslıq — dərhal müdaxilə tələb edir. Orta risk zonasında isə izləmə, profilaktik maarifləndirmə və əlavə verifikasiya mexanizmləri təklif olunur. Aşağı risk zonasında isə əsasən monitorinq və maarifləndirmə yetərlidir. Bu metodologiya Bamberger və Donnelly tərəfindən təsvir edilən "risk-əsaslı idarəetmə modeli" ilə uyğun gəlir[50].

[49] Bronfenbrenner, U. (1979). *The Ecology of Human Development*. Harvard University Press.

[50] Bamberger, K. A., & Donnelly, D. (2019). *Risk Management and Regulatory*

Eyni zamanda, rəqəmsal insan alveri risk matrisinin hazırlanmasında etik və hüquqi çətinliklər də mövcuddur. Bir tərəfdən, potensial qurbanların profilini müəyyənləşdirmək proaktiv müdaxilə üçün zəruridir, digər tərəfdən isə bu, diskriminasiya və məxfilik hüquqlarının pozulması riski yarada bilər. Bu səbəbdən Avropa Şurasının İnsan Alverinə qarşı Mübarizə üzrə Ekspert Qrupu 2022-ci il hesabatında vurğulayır ki, risk matrisləri yalnız sübuta əsaslanan göstəricilərə söykənməli və fərdi məlumatların qorunması prinsipləri ilə uzlaşdırılmalıdır[51].

Nəticə etibarilə, rəqəmsal insan alveri probleminin risk matrisi həm nəzəri, həm də praktiki baxımdan kompleks bir alətdir. Onun üstünlüyü müxtəlif indikatorları vahid analitik çərçivədə birləşdirməsi, zəif siqnalları aşkarlaması və resursların daha səmərəli paylanmasına imkan yaratmasıdır. Lakin bu yanaşma yalnız dinamik, interdisiplinar və etik prinsiplərə söykənərək tətbiq edilərsə effektiv nəticə verə bilər. Buna görə də risk matrisi rəqəmsal insan alverinə qarşı mübarizədə əsaslı analitik vasitə kimi qəbul edilməli, sosial iş, hüquq-mühafizə və kibertəhlükəsizlik sahələrinin inteqrativ əməkdaşlığı ilə tətbiq olunmalıdır.

5.1. Yaşıl (aşağı risk) – sadəcə qeydiyyat

Risk matrisində "yaşıl zona" ən aşağı risk səviyyəsini ifadə edir. Bu mərhələdə əsas məqsəd hələ insan alverinə dair ciddi göstəricilər aşkar edilməmiş şəxslərin və ya fəaliyyətlərin sadəcə qeydiyyata alınması və monitorinq üçün saxlanılmasıdır. Yəni, sosial media platformasında, iş elan saytında və ya digər rəqəmsal məkanda müəyyən davranış nümunəsi müşahidə oluna bilər, lakin bu, insan alverinə dair konkret təhlükə siqnalı daşımır.

Yaşıl zonada qeydiyyat aşağıdakı məqsədlərə xidmət edir:

- İlkin məlumat bazası yaratmaq: Sistem bütün istifadəçi və fəaliyyətləri qeydiyyata alaraq gələcəkdə baş verə biləcək risk

Decision-Making in the Digital Age. Oxford University Press.

[51] GRETA. (2022). *Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings*. Strasbourg: Council of Europe.

eskalasiyasını izləmək üçün baza formalaşdırır. Bu, "erkən xəbərdarlıq mexanizmi" rolunu oynayır[52].

- Normativ davranış nümunələri ilə müqayisə: Sadəcə qeydiyyat edilən hallarda istifadəçi davranışları və ya elan məzmunları normal, geniş yayılmış fəaliyyətlərlə üst-üstə düşür. Məsələn, sosial şəbəkədə iş elanına baxmaq və ya onlayn təhsil platformasında qeydiyyatdan keçmək.
- Müdaxiləsiz monitorinq: Bu səviyyədə hüquq-mühafizə və sosial xidmət orqanlarının aktiv müdaxiləsi tələb olunmur. Əksinə, məqsəd potensial risk faktorlarının yalnız sistemdə saxlanılması və mütəmadi təhlilə cəlb edilməsidir[53].
- Etik prinsiplərin qorunması: Aşağı risk səviyyəsində qeydiyyat şəxsin məxfilik hüququnu pozmadan həyata keçirilməli, məlumatlar anonimləşdirilmiş şəkildə saxlanmalıdır. Avropa İttifaqının GDPR çərçivəsində də bu, "minimum məlumat toplama" prinsipi ilə tənzimlənir[54].

Praktiki nümunə kimi: sosial media platformasında "qonşu ölkədə mövsümi iş" elanına sadəcə baxan, lakin heç bir şəxsi məlumat paylaşmayan istifadəçi yaşıl zonada qeydiyyata düşə bilər. Bu, insan alverinə dair bilavasitə göstərici deyil, lakin gələcəkdə davranış intensivliyi və istiqaməti dəyişərsə (məsələn, təkrar-təkrar şübhəli elanlara cavab vermək), risk səviyyəsi sarı və ya qırmızı zonaya keçə bilər.

Beləliklə, yaşıl zonadakı sadəcə qeydiyyat, "təhlükə yoxdur" mənasına gəlmir, əksinə, önləyici monitorinqin ilkin mərhələsini təşkil edir. Bu yanaşma həm resursların səmərəli istifadəsinə, həm də qurbanların erkən mərhələdə müdafiəsinə xidmət edir.

[52] Kelly, L. (2017). *Ending the Abuse: Building a Future Without Violence*. Policy Press.

[53] Clawson, H. J., Dutch, N., Solomon, A., & Grace, L. G. (2009). *Human Trafficking into and within the United States: A Review of the Literature*. U.S. Department of Health and Human Services.

[54] GDPR (2016). *General Data Protection Regulation*. Official Journal of the European Union.

5.2. Sarı (orta risk) – əlavə izləmə

Risk matrisində sarı zona orta risk səviyyəsini göstərir və bu mərhələ artıq sadəcə qeydiyyatla kifayətlənməyin mümkün olmadığı situasiyaları əhatə edir. Burada müəyyən siqnallar mövcuddur ki, onlar insan alverinə dair bilavasitə sübut təşkil etməsə də, ehtiyatlı yanaşma və əlavə izləmə tələb edir. Əlavə izləmənin mahiyyəti şəxsin və ya qrupun davranış dinamikasını təhlil etmək, təkrarlanan fəaliyyətləri müşahidə etmək, verilən məlumatların dəqiqliyini yoxlamaq və riskli əlaqələri araşdırmaqdan ibarətdir. Bu mərhələdə həm sosial işçilərin, həm də hüquq-mühafizə orqanlarının aktiv monitorinq aparması zəruri hesab olunur.

Sarı zonada izləmə prosesi yalnız ilkin qeydiyyatla bitmir, əksinə daha dərin analiz tələb edir. Məsələn, istifadəçi qısa müddət ərzində bir neçə dəfə "yüksək maaşlı iş" elanlarına müraciət edirsə, bu, artıq sadəcə maraq yox, potensial həssaslıq göstəricisi ola bilər. Eyni zamanda, paylaşılan elanların və ya profillərin gerçəkliyinin yoxlanılması da vacibdir. Bu mərhələdə "fact-checking" metodları, həmçinin "reverse image search" texnologiyası tez-tez istifadə olunur, çünki eyni şəkillərin və ya mətnlərin müxtəlif saxta elanlarda təkrarlandığı müşahidə edilir.

Praktik müstəvidə sarı zonaya aid edilə biləcək nümunələr kifayət qədər çoxdur. Gənc bir qız sosial mediada dəfələrlə "Avropada təhsil və iş" elanlarına reaksiya verir, lakin hələ şəxsi məlumatlarını paylaşmayıb. Bu davranış yaşıl zonadan fərqli olaraq daha ciddi siqnaldır və izləmə tələb edir. Digər nümunədə bir şəxs birdən çox "qeyri-rəsmi iş" elanına müraciət edir, amma heç birində hüquqi müqavilə tələb etmir. Bu, onun potensial istismara açıq olduğunu göstərir. Başqa bir misalda isə istifadəçi birdən-birə çoxsaylı "səyahət bileti və iş paketi" təklifləri olan səhifələri izləməyə başlayır ki, bu da rekrutment göstəricisi hesab oluna bilər.

Sarı zona vacibdir, çünki bu mərhələ həm erkən müdaxilə imkanları yaradır, həm də resursların düzgün bölüşdürülməsinə xidmət edir. Yüksək risk zonası üçün resursları saxlamaq məqsədilə orta risk hallarında əsasən izləmə, maarifləndirmə və ilkin dəstək tədbirləri həyata keçirilir. Əlavə izləmə mexanizmləri həmçinin eskalasi-

yanın qarşısını almaq üçün "erkən xəbərdarlıq sistemi" rolunu oynayır. Belə hallarda sosial işçilər məlumatlandırıcı mesajlarla potensial qurbanı çəkindirməyə, hüquq-mühafizə orqanları isə texnoloji izləmə vasitələri ilə şəbəkələri müəyyən etməyə çalışa bilər.

Akademik ədəbiyyatda da vurğulandığı kimi, rəqəmsal insan alveri çox vaxt "gizli siqnallar" şəklində meydana çıxır və bu siqnallar vaxtında izlənilmədikdə cinayətkar şəbəkələrin fəaliyyəti genişlənir[55]. Bamberger və Donnelly risk əsaslı idarəetmə modelində qeyd edirlər ki, orta risk mərhələsində sistemli monitorinq və selektiv müdaxilələr resursların optimal istifadəsini təmin edir[56]. ATƏT-in tövsiyələrində isə xüsusi olaraq göstərilir ki, sarı zonada yalnız monitorinq kifayət etmir, eyni zamanda maarifləndirmə və xəbərdarlıq mesajları ilə profilaktik tədbirlər həyata keçirilməlidir.

Beləliklə, sarı zona insan alveri risk matrisinin mühüm elementlərindən biridir. Bu mərhələ nə tam təhlükəsizlik, nə də açıq təhlükə deməkdir; əksinə, diqqətli müşahidə və balanslaşdırılmış müdaxilə tələb edən halları əhatə edir. Misallar da göstərir ki, vaxtında əlavə izləmə aparılmasa, bu tip hallar asanlıqla qırmızı zonaya keçə bilər. Ona görə də sarı zona həm preventiv tədbirlərin, həm də erkən xəbərdarlıq sistemlərinin ən aktiv tətbiq olunduğu sahədir.

5.3. Qırmızı (yüksək risk) – təcili yönləndirmə

Qırmızı zona risk matrisində ən yüksək təhlükə səviyyəsini göstərir və bu mərhələdə artıq sadəcə qeydiyyat və ya əlavə izləmə ilə kifayətlənmək mümkün deyil, çünki qurbanın insan alverinə cəlb olunması və ya istismara məruz qalması ehtimalı çox yüksəkdir. Burada əsas prinsip "təcili yönləndirmə"dir – yəni, potensial qurban dərhal müvafiq müdafiə və dəstək strukturlarına istiqamətləndirilməli, hüquq-mühafizə orqanlarının iştirakı təmin edilməlidir. Bu yanaşma BMT-nin "Palermo Protokolu" (2000) və Avropa Şurasının "İnsan Alverinə qarşı Mübarizə Konvensiyası"nda (2005) təsbit

[55] Latonero, M. (2011). *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*. USC Annenberg Center on Communication Leadership & Policy.

[56] Bamberger, K. A., & Donnelly, D. (2019). *Risk Management and Regulatory Decision-Making in the Digital Age*. Oxford University Press.

olunmuş qoruma və müdafiə prinsiplərinə əsaslanır.

Yüksək risk vəziyyətləri bir sıra konkret misallarla izah oluna bilər. Məsələn, sosial media üzərindən yetkinlik yaşına çatmayan bir istifadəçiyə "pulsuz səyahət" və "iş imkanı" təklif edilir və ondan pasport məlumatlarının göndərilməsi tələb olunur. Digər nümunədə isə bir qadın qısa müddət ərzində şübhəli profillərlə dəfələrlə yazışır və onlardan "sərhədi problemsiz keçmək" vədi alır. Bəzi hallarda qurban artıq real həyatda görüşə razılıq verib və yeri barədə məlumat paylaşıb. Bu kimi situasiyalar artıq sadəcə risk siqnalı deyil, aktiv istismar niyyətini göstərir və dərhal müdaxilə tələb edir.

Təcili yönləndirmə mexanizmi bu mərhələdə əsas alətdir. Birincisi, hüquq-mühafizə orqanlarına dərhal xəbərdarlıq edilməli, fakt üzrə istintaq prosesi başlanmalıdır.

İkincisi, sosial xidmət orqanları və ya QHT-lər qurbanla ilkin əlaqə quraraq onu təhlükəsiz məkana yönləndirməlidir. Bu zaman "Milli İstiqamətləndirmə Mexanizmi" (NRM) çərçivəsində tətbiq olunan standart prosedurlar əsas götürülür: riskli şəxsin identifikasiyası, təhlükəsiz sığınacağa yerləşdirilməsi, tibbi və psixoloji dəstəyin təmin olunması.

Üçüncüsü, qurbanın məlumatlarının məxfiliyi və razılıq əsasında yönləndirmə prinsiplərinə ciddi əməl edilməlidir. Beynəlxalq Təşkilatların (BMqT, ATƏT) tövsiyələrinə görə, təcili yönləndirmə yalnız təhlükəsizliklə məhdudlaşmamalı, həm də uzunmüddətli reabilitasiya proqramlarına inteqrasiya ilə müşayiət olunmalıdır.

Akademik müzakirələrdə vurğulandığı kimi, yüksək risk zonasında zaman faktoru həyati əhəmiyyət daşıyır. Zimmerman və Kiss qeyd edirlər ki, insan alveri qurbanlarının müdafiəsində ilk 24 saat qurbanın təhlükəsizlik və inam hissini bərpa etmək baxımından həlledici rol oynayır[57]. Həmçinin GRETA hesabatında göstərilir ki, yüksək risk göstəriciləri müşahidə edilən şəxslərin gecikdirilmədən yönləndirilməsi həm onların istismardan xilas olunması, həm də cinayətkar şəbəkələrin ifşası üçün vacibdir.

Beləliklə, qırmızı zona risk matrisinin ən kritik hissəsidir və burada əsas məqsəd vaxt itirmədən qurbanı təhlükədən uzaqlaşdır-

[57] Zimmerman, C., & Kiss, L. (2017). Human trafficking and exploitation: A global health concern. *PLOS Medicine*, 14(11), e1002437

maq, müvafiq dövlət və qeyri-dövlət qurumlarını prosesə cəlb etməkdir. Misallardan da göründüyü kimi, bu mərhələdə hər hansı gecikmə qurbanın birbaşa istismara məruz qalması ilə nəticələnə bilər. Buna görə də təcili yönləndirmə yalnız bir prosedur deyil, həm də insan həyatını qorumaq üçün ən vacib müdafiə mexanizmidir.

5.4. Cədvəl + nümunə halları

Zona	Risk səviyyəsi	Tipik indikatorlar	Nümunə hallar	İstiqamətləndirmə mexanizmi
Yaşıl (aşağı risk)	Sadəcə qeydiyyat və monitorinq.	- Adi iş elanlarına baxmaq - Onlayn kurs və təhsil platformasında qeydiyyat - Şəxsi məlumat paylaşmamaq	Gənc istifadəçi “yay iş elanına” maraq göstərir, lakin heç bir şəxsi məlumat paylaşmır.	Yalnız qeydiyyat aparılır. Aktiv müdaxilə edilmir, məlumat anonimləşdirilir.
Sarı (orta risk)	Əlavə izləmə və faktların yoxlanması.	- Təkrar-təkrar “yüksək maaşlı iş” elanlarına müraciət - Şəxsi məlumat paylaşmağa meyillilik - Birdən-birə çoxlu şübhəli səhifə izləmək	Bir gənc qız dəfələrlə “Avropada iş və təhsil” elanlarına reaksiya verir. Başqa şəxs müxtəlif iş elanlarına yazılır, amma müqavilə istəmir.	Əlavə izləmə aparılır. Faktlar yoxlanılır, maarifləndirici mesaj göndərilir, ilkin profilaktik müdaxilə edilir.
Qırmızı (yüksək risk)	Təcili yönləndirmə.	- Pasport və ya şəxsiyyət məlumatı tələb edilməsi - Real görüş üçün	Yeniyetmədən “pulsuz səyahət” adı ilə pasport məlumatı	Dərhal hüquq-mühafizə və sosial xidmətə yönləndirmə. Təhlükəsiz

		razılıq - "Sərhədi problemsiz keçmək" vədi - Yetkinlik yaşına çatmayanlarla yazışma	istənilir. Bir qadın sosial mediada tanımadığı şəxslə real görüşə razılıq verir.	sığınacağa yerləşdirmə, tibbi və psixoloji yardım, istintaqın başlanması.

İzahlı ümunələr

• Yaşıl zona nümunəsi: 19 yaşlı bir gənc sosial mediada yay təcrübə proqramlarına baxır, amma heç bir məlumat paylaşmır. Bu hal aşağı risk daşıyır və sadəcə qeydiyyata alınır.

• Sarı zona nümunəsi: 22 yaşlı qadın bir ay ərzində dörd dəfə fərqli səhifələrdə "xaricdə ofisiant işi, vizasız qəbul" elanlarına yazılır. Şəxsi nömrəsini paylaşır, amma hələ görüş təyin etməyib. Bu hal orta riskdir, əlavə izləmə və xəbərdarlıq tələb edir.

• Qırmızı zona nümunəsi: 16 yaşlı qız "modellər üçün seçmələr" elanına yazılır və ondan pasportun surətini göndərməsi xahiş olunur. Elanı yerləşdirən şəxs real görüş üçün ünvan verir. Bu artıq yüksək riskdir və təcili hüquq-mühafizə orqanlarına və sosial xidmətlərə yönləndirmə tələb edir.

Rəqəmsal insan alveri ilə mübarizədə risk matrisi qurbanların aşkarlanması və müvafiq müdaxilə tədbirlərinin həyata keçirilməsi üçün sistemli yanaşma təqdim edir. Bu matrisi tətbiq etməklə mütəxəssislər müxtəlif davranış nümunələrini fərqli zonalara ayıraraq həm resursların səmərəli istifadəsini təmin edir, həm də potensial qurbanların təhlükədən qorunmasını mümkün edir. Yaşıl zonada əsas məqsəd sadəcə qeydiyyat aparmaq və ilkin monitorinqi təmin etməkdir. Burada hələ insan alverinə dair birbaşa göstəricilər müşahidə olunmur, lakin məlumatların saxlanılması gələcəkdə baş verə biləcək risk eskalasiyasını vaxtında müəyyənləşdirməyə imkan verir. Sarı zonada artıq əlavə izləmə tələb olunur, çünki davranış dinamikası potensial təhlükənin artdığını göstərir. Bu mərhələdə faktların yoxlanılması, maarifləndirici tədbirlər və profilaktik müdaxilələr həyata keçirilir ki, riskin qırmızı zonaya keçməsinin qarşısı alınsın. Qırmızı zona isə ən kritik mərhələdir və burada təcili yönləndirmə

vacibdir. Pasport məlumatlarının tələb edilməsi, real görüşlər üçün razılıqlar və yetkinlik yaşına çatmayanlarla əlaqələrin qurulması kimi hallar insan alverinə bilavasitə göstəricilərdir və dərhal hüquq-mühafizə orqanlarına, sosial xidmətlərə yönləndirmə aparılmalıdır. Beləliklə, risk matrisi sadəcə nəzəri yanaşma deyil, həm də praktik müdafiə və profilaktika alətidir. Onun tətbiqi ilə müvafiq strukturlar erkən xəbərdarlıq mexanizmlərini gücləndirir, yüksək risk hallarında isə qurbanların həyatını xilas edən operativ müdaxilələr həyata keçirirlər. Bu çərçivə həm milli, həm də beynəlxalq standartlara uyğun şəkildə insan alverinə qarşı effektiv mübarizənin əsas elementlərindən biri kimi qəbul edilməlidir.

6. Təhlükəsizlik və etik qaydalar

Rəqəmsal insan alveri ilə mübarizədə təhlükəsizlik və etik qaydalar yalnız qurbanların qorunması deyil, həm də məlumatların istifadəsi, monitorinq fəaliyyətlərinin aparılması və hüquqi çərçivələrin qorunması baxımından həlledici əhəmiyyət daşıyır. Bu sahədə beynəlxalq və regional səviyyədə qəbul edilmiş öhdəliklər, sənədlər və standartlar mövcuddur ki, onların hər biri insan hüquqlarının qorunması, qurbanların məxfiliyinin təmin edilməsi və etik prinsiplərə əsaslanan müdaxilə mexanizmlərinin formalaşdırılmasını zəruri edir.

Ən mühüm sənədlərdən biri BMT-nin Palermo Protokoludur. Bu sənəd insan alverinə qarşı beynəlxalq hüquqi çərçivənin əsasını qoyur və dövlətlərdən qurbanların müdafiəsi, istintaqın effektiv aparılması və profilaktik tədbirlərin həyata keçirilməsini tələb edir. Protokol həmçinin qurbanların hüquqlarının pozulmadan identifikasiyası və onların məcburi şəkildə kriminal məsuliyyətə cəlb edilməməsi prinsipini müəyyən edir.

Avropa Şurasının İnsan Alverinə qarşı Mübarizə Konvensiyası etik və təhlükəsizlik prinsiplərinə xüsusi vurğu edən digər mühüm sənəddir. Bu konvensiya qurbanların hüquqlarının qorunmasını dövlətlərin əsas öhdəliyi kimi təqdim edir, məxfilik prinsiplərini hüquqi öhdəlik səviyyəsinə qaldırır və "təhlükəsizlik öncəlikli yanaşma" prinsipini tətbiq edir. GRETA-nın hesabatında da qeyd olunur ki, etik yanaşmalar olmadan risk qiymətləndiriməsi kimi alətlərin istifadəsi qurbanlara zərər verə bilər, bu isə dövlətlərin beynəlxalq öhdəliklərinin pozulması ilə nəticələnir.

Avropa İttifaqının Ümumi məlumatların qorunması Qaydası rəqəmsal insan alveri kontekstində xüsusilə əhəmiyyətlidir. Monitorinq və risk matrisi fəaliyyətləri zamanı şəxsi məlumatların emalı, saxlanması və istifadəsi ciddi məhdudiyyətlərə tabedir. GDPR "minimum məlumat toplama" və "məxfilik üzrə dizayn" prinsiplərini təsbit edərək etik monitorinqin hüquqi əsasını qoyur.

ATƏT-in tövsiyələri isə rəqəmsal platformalarda insan alveri ilə mübarizə aparan dövlətlər və QHT-lər üçün etik çərçivə təqdim edir. Burada vurğulanır ki, hər bir monitorinq fəaliyyəti qurbanın

razılığı, təhlükəsizliyi və məxfilik hüququ nəzərə alınmaqla həyata keçirilməlidir.

Akademik müzakirələrdə də bu mövzunun əhəmiyyəti geniş vurğulanır. Latonero qeyd edir ki, rəqəmsal texnologiyalardan istifadə insan alverinə qarşı mübarizədə yeni imkanlar açsa da, bu, etik risklər də yaradır və qurbanların ikinci dəfə zərər görməməsi üçün ciddi qaydalar tələb olunur[58]. Zimmerman və Kiss isə qurbanların psixoloji və sosial reabilitasiyası baxımından məxfilik və təhlükəsizlik qaydalarının pozulmasının onların travmasının dərinləşməsinə gətirib çıxara biləcəyini göstərirlər.

Nəticə etibarilə, təhlükəsizlik və etik qaydalar rəqəmsal insan alveri ilə mübarizənin ayrılmaz hissəsidir. Onların əhəmiyyəti ikiqatdır- bir tərəfdən qurbanların hüquq və məxfiliyini qorumaqla onların bərpasına dəstək olur, digər tərəfdən isə dövlətlərin və təşkilatların beynəlxalq hüquqi öhdəliklərə uyğun fəaliyyət göstərməsini təmin edir. Bu qaydaların pozulması yalnız qurbanların deyil, həm də hüquqi və institusional çərçivələrin etibarlılığının itirilməsinə səbəb ola bilər.

6.1. Qurbanın anonimliyinin qorunması

Qurbanın anonimliyinin qorunması rəqəmsal insan alveri ilə mübarizədə ən həssas və vacib prinsiplərdən biridir. Anonimlik yalnız şəxsi məlumatların gizli saxlanması deyil, həm də qurbanın psixoloji təhlükəsizliyinin, sosial bərpasının və gələcək həyat imkanlarının qorunması deməkdir. Bir çox tədqiqat və ədəbiyyatda vurğulandığı kimi, məxfilik və anonimlik hüququ qurbanın ikincil travmadan qorunması və ədalət sisteminə inamının gücləndirilməsi baxımından əsas şərtlərdən biridir.

Anonimliyin qorunmaması ciddi sosial və hüquqi nəticələrə səbəb ola bilər. Məsələn, bəzi ölkələrdə insan alveri qurbanlarının kimliyi mətbuatda və ya sosial mediada yayımlandıqda onların ailə və icma tərəfindən damğalanması halları qeydə alınıb[59]. Digər

[58] Latonero, M. (2011). *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds.* USC Annenberg Center.

[59] Surtees, R. (2008). Traffickers and Trafficking in Southern and Eastern Europe:

hallarda, hüquq-mühafizə orqanlarının istintaq prosesində qurbanların şəxsi məlumatlarını yetərincə qorumağa bilməməsi onların yenidən istismara məruz qalmasına gətirib çıxarıb[60] (Brunovskis & Surtees, 2012). Belə situasiyalar yalnız qurbanın bərpasına mane olmur, həm də digər potensial qurbanların kömək üçün müraciət etməkdən çəkinməsinə səbəb olur.

Nəticə etibarilə, anonimliyin qorunması həm hüquqi, həm etik, həm də praktiki baxımdan insan alverinə qarşı mübarizədə həlledici rol oynayır. Anonimlik yalnız şəxsi məlumatların gizliliyi deyil, həm də qurbanın insan hüquqlarının və ləyaqətinin müdafiəsidir. Bu prinsipi pozmaq isə qurbanı ikinci dəfə zərər altında qoymaq, sosial damğalanma və travmanın dərinləşməsi ilə nəticələnə bilər. Buna görə də qurbanların anonimliyinin qorunması bütün milli və beynəlxalq mübarizə strategiyalarının mərkəzi elementi hesab edilməlidir.

Azərbaycanda insan alveri qurbanlarının anonimliyinin qorunması həm Cinayət Məcəlləsi, həm də "İnsan alverinə qarşı mübarizə haqqında" Qanun ilə təmin edilir. Azərbaycanda qeyd edilən qanunlarda əks edilən maddələrin mövcudluğu qurbanların ikinci dəfə zərər çəkməsinin (təkrar travmanın, damğalanma, sosial təcridin) qarşısını almaq, həmçinin onların hüquqi müdafiə orqanlarına müraciət etməkdə inamını gücləndirmək üçün həyati əhəmiyyət daşıyır. Əgər anonimlik qorunmazsa, qurban ictimai qınağa məruz qala, təhlükəsizliyi təhdid oluna bilər və nəticədə digər potensial qurbanlar da kömək üçün müraciət etməkdən çəkinə bilərlər.

6.2. Minimum məlumat prinsipi

Minimum məlumat prinsipi şəxsi məlumatların yalnız mütləq zəruri olduğu hallarda toplanması və emal edilməsini nəzərdə tutur. Bu prinsipin mahiyyəti ondan ibarətdir ki, insan alveri ilə

Considering the Other Side of Human Trafficking. European Journal of Criminology, 5(1), 39–68.

[60] Brunovskis, A., & Surtees, R. (2012). Leaving the past behind? When victims of trafficking decline assistance. Oslo: FAFO

mübarizədə və qurbanların identifikasiyası prosesində şəxslərin hüquq və azadlıqlarını qorumaq üçün yalnız məqsədəuyğun və kifayət qədər məlumat saxlanılmalıdır. Əlavə və ya artıq məlumatın toplanması həm məxfilik hüququnun pozulmasına, həm də qurbanın ikinci dəfə travmaya məruz qalmasına səbəb ola bilər. Bu prinsip Avropa İttifaqının Ümumi məlumatların qorunması Qaydası (GDPR, 2016, Maddə 5) ilə hüquqi öhdəlik kimi müəyyən edilib və burada açıq şəkildə vurğulanır ki, məlumatlar "məqsəd üçün adekvat, müvafiq və zəruri həddə" olmalıdır.

Bu yanaşmanın əhəmiyyəti həm hüquqi, həm də praktiki müstəvidə özünü göstərir. Bir tərəfdən, qurbanın anonimliyini qorumaqla onun damğalanmasının qarşısını alır və təhlükəsizlik risklərini azaldır. Digər tərəfdən, məlumatların həddindən artıq toplanması dövlət qurumları və QHT-lər üçün əlavə məsuliyyət yaradır və informasiyanın sızması halında qurbanların həyati təhlükə ilə üzləşməsinə səbəb ola bilər. Akademik müzakirələrdə də bu məsələ xüsusi vurğulanır. Latonero göstərir ki, rəqəmsal platformalarda insan alveri ilə mübarizə aparılarkən çoxsaylı məlumatların məqsədsiz toplanması qurbanların yenidən risk altına düşməsinə səbəb ola bilər[61]. Eyni zamanda, Brunovskis və Surtees qeyd edirlər ki, bəzi ölkələrdə yardım proqramları zamanı qurbanlardan artıq və həssas məlumat tələb olunması onların həmin xidmətlərdən imtina etməsinə gətirib çıxarır.

Praktiki misallara nəzər yetirsək, əgər insan alveri qurbanı sığınacağa yerləşdirilirsə, onun təhlükəsizliyini təmin etmək üçün yalnız əsas identifikasiya məlumatları (ad-soyad, yaş, vətəndaşlıq) tələb edilməli, şəxsi əlaqə ünvanı, ailə üzvlərinin kimliyi və digər həssas məlumatlar isə əlavə risk yaratmamaq üçün toplanmamalıdır. Digər nümunədə hüquq-mühafizə orqanları istintaq məqsədilə yalnız hadisə ilə bağlı bilavasitə sübut təşkil edən məlumatları saxlamalı, qurbanın şəxsi həyatına aid geniş detallar toplanmamalıdır.

Nəticə etibarilə, minimum məlumat prinsipi qurbanın hüquqlarının qorunması, onun inamının gücləndirilməsi və sosial

[61] Latonero, M. (2011). *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds.* USC Annenberg Center.

reabilitasiya prosesinə qoşulmasını asanlaşdırmaq üçün həyati əhəmiyyət kəsb edir. Bu prinsipin pozulması yalnız hüquqi məsuliyyət doğurmur, həm də qurbanların yenidən zərər çəkməsinə və kömək üçün müraciət etməməsinə səbəb ola bilər.

Azərbaycanda şəxsi məlumatların qorunması bir neçə əsas hüquqi sənədlə təmin edilir. Konstitusiyanın 32-ci maddəsi hər kəsin şəxsi və ailə həyatına hörmət hüququnu təsbit edir və qanunsuz yolla şəxsi məlumatların toplanmasını və yayılmasını qadağan edir. "Şəxsi məlumatlar haqqında" Qanun şəxsi məlumatların yalnız məqsədəuyğun, adekvat və zəruri həddə toplanmasını, həmçinin sahibinin razılığı olmadan üçüncü şəxslərə açıqlanmasının qadağan edilməsini nəzərdə tutur. "İnsan alverinə qarşı mübarizə haqqında" Qanun xüsusi olaraq qurbanların anonimlik və məxfilik hüququnu qoruyur, onların razılığı olmadan məlumatların istifadəsinə yol vermir. Cinayət Prosessual Məcəlləsi (maddə 123) isə istintaq və məhkəmə proseslərində zərərçəkmiş şəxslərin kimliyinin gizli saxlanmasını, qapalı iclasların keçirilməsini və təhlükəsizlik tədbirlərini təmin edir. Azərbaycan həm də Palermo Protokoluna və Avropa Şurasının İnsan Alverinə qarşı Mübarizə Konvensiyasına qoşulduğuna görə beynəlxalq öhdəlik daşıyır. Bu müddəalar qurbanların anonimliyini qorumaqla onların ikinci dəfə zərər çəkməsinin qarşısını alır və hüquqi sistemə inamı gücləndirir.

6.3. Şifrəli ünsiyyət kanalları

Şifrəli ünsiyyət kanalları müasir rəqəmsal mühitdə həm insan alveri qurbanlarının qorunması, həm də hüquq-mühafizə və sosial xidmət qurumlarının təhlükəsiz məlumat mübadiləsi aparması üçün əsas vasitələrdən biri hesab olunur. Şifrələmə (encryption) texnologiyası göndərilən məlumatın yalnız göndərici və alıcı tərəfindən oxuna bilməsini təmin edir və üçüncü şəxslərin, o cümlədən cinayətkar şəbəkələrin və ya icazəsiz dövlət qurumlarının həmin məlumatı əldə etməsini mümkünsüzləşdirir. Avropa Şurası və BMT-nin İnsan Hüquqları üzrə Ali Komissarlığı rəqəmsal hüquqlar çərçivəsində şifrələmənin ifadə azadlığı, şəxsi həyatın toxunul-

mazlığı və qurbanların təhlükəsizliyi üçün zəruri olduğunu xüsusi vurğulayır.

Şifrəli ünsiyyət kanallarının əsas əhəmiyyəti ondan ibarətdir ki, onlar həssas məlumatların – məsələn, insan alveri qurbanlarının identifikasiyası, yönləndirilməsi və hüquqi müdafiəsi ilə bağlı məlumatların – məxfiliyini qoruyur. Əgər bu məlumatlar qorunmazsa, qurban həm istismar şəbəkələrinin, həm də ictimai damğalanmanın hədəfinə çevrilə bilər. Məsələn, Zimmerman və Kiss qeyd edirlər ki, qurbanların tibbi və psixoloji yardımla bağlı məlumatlarının üçüncü şəxslərə açıqlanması onların reabilitasiya prosesinə ciddi zərbə vurur. Buna görə də şifrəli kanallardan istifadə sosial işin etik və hüquqi prinsiplərinin qorunması baxımından həyati əhəmiyyət daşıyır.

Praktik müstəvidə şifrəli ünsiyyət kanalları müxtəlif formalar alır. End-to-end şifrələmə texnologiyası (məsələn, WhatsApp, Signal və ya Telegram-ın gizli çatları) mesajların yalnız göndərici və alıcı tərəfindən oxuna bilməsini təmin edir. Bu, insan alveri qurbanları ilə ilkin əlaqə qurmaq və onların etimadını qazanmaq üçün çox vacibdir, çünki onlar başqa vasitələrlə izlənilə biləcəklərindən ehtiyat edirlər. Digər tərəfdən, hüquq-mühafizə və QHT əməkdaşları arasında qurbanların yönləndirilməsi və sığınacaqlara yerləşdirilməsi ilə bağlı məlumat mübadiləsi də şifrəli e-mail sistemləri (ProtonMail, Tutanota) və ya təhlükəsiz serverlər üzərindən aparılmalıdır.

Şifrələnmiş kanallardan istifadə etmədikdə real risklər yaranır. Məsələn, bəzi ölkələrdə hüquq-mühafizə orqanlarının zəif qorunan məlumat bazaları insan alveri şəbəkələri tərəfindən sındırılmış və qurbanların identik məlumatları əldə edilərək onların təkrar istismarı baş vermişdir. Digər hallarda isə, sosial xidmət qurumlarının adi e-mail üzərindən göndərdiyi yönləndirmə məlumatları üçüncü şəxslərin əlinə keçmiş və qurbanların təhlükəsizliyi pozulmuşdur.

Azərbaycan reallığında insan alveri ilə mübarizə aparan qurumlar, sosial işçilər və hüquq-mühafizə əməkdaşları üçün şifrəli ünsiyyət vasitələrinin seçimi həm texniki imkanlar, həm də sosial-mədəni faktorlarla bağlıdır. Burada əsas məqsəd qurbanların

təhlükəsizliyi, məxfilik hüququnun qorunması və operativ əlaqənin təmin edilməsidir.

Birinci növbədə mobil mesajlaşma tətbiqləri praktik baxımdan daha əlçatan hesab olunur. Azərbaycan əhalisinin böyük hissəsi mobil internetdən istifadə edir və bu, qurbanlarla ilkin əlaqənin qurulması üçün effektiv kanaldır. Signal tətbiqi beynəlxalq ekspertlər tərəfindən ən təhlükəsiz end-to-end şifrələnmiş platforma kimi tövsiyə olunur. Signal açıq mənbəli proqram olduğuna görə onun şifrələmə mexanizmləri şəffafdır və üçüncü tərəf müdaxiləsinə qarşı güclü müdafiə təmin edir. Lakin Azərbaycanda Signal hələ geniş yayılmayıb və istifadəsi daha çox maarifləndirmə tələb edir.

WhatsApp isə ölkədə ən çox istifadə olunan mesajlaşma platformasıdır və end-to-end şifrələmə tətbiq edir. Onun üstünlüyü geniş yayılması və insanların bu kanaldan rahat istifadə etməsidir. Amma eyni zamanda, WhatsApp Facebook/Meta şirkətinə məxsus olduğuna görə məlumatların meta-səviyyədə (məsələn, kim kimlə əlaqə saxlayır) toplanması mümkündür. Buna görə qurbanlarla həssas yazışmalarda ehtiyatlı yanaşmaq, şəxsi identifikasiya məlumatlarını mümkün qədər paylaşmamaq tövsiyə olunur.

Telegram Azərbaycanda populyar platformalardan biridir, lakin onun adi çatları tam şifrələnmir. Yalnız "Secret Chat" funksiyası end-to-end şifrələmə təmin edir. Qurbanların təhlükəsizliyi üçün Telegramdan istifadə olunarkən mütləq gizli çat funksiyasına üstünlük verilməlidir.

Elektron poçt mübadiləsində isə ən etibarlı seçimlərdən biri ProtonMail və ya Tutanota kimi şifrələnmiş e-mail xidmətləridir. Bu xidmətlər İsveçrə və Almaniya kimi sərt məlumat qoruma qanunları olan ölkələrdə yerləşir və Azərbaycan təşkilatları üçün beynəlxalq tərəfdaşlarla təhlükəsiz yazışma imkanı yaradır. Praktiki nümunə olaraq, qurbanın sığınacağa yönləndirilməsi barədə məlumatların dövlət qurumları və QHT-lər arasında paylaşılması ProtonMail üzərindən aparıla bilər.

Əlavə olaraq, Azərbaycanın dövlət strukturları üçün daxili server əsaslı şifrələnmiş rabitə sistemləri də vacibdir. Çünki beynəlxalq platformalara tam etibar etmək mümkün olmur və milli

təhlükəsizlik maraqları baxımından yerli infrastrukturda təhlükəsiz məlumat mübadiləsi kanalları qurulmalıdır. Bu istiqamətdə, "AzInTelecom"un dövlət bulud texnologiyaları və daxili şifrələnmiş e-mail sistemlərindən istifadə tövsiyə olunur.

Azərbaycan reallığında ən uyğun yanaşma gündəlik ünsiyyətdə WhatsApp və Telegram (yalnız gizli çat), qlobal partnyorlarla yazışmada ProtonMail/Tutanota, yüksək həssaslıq tələb edən hallarda isə Signal istifadəsi ola bilər. Bu yanaşma həm qurbanlarla daha rahat təmas qurmağa, həm də yüksək riskli məlumatları qorumağa imkan verir. Ən vacib məqam isə sosial işçilərin və hüquq-mühafizə əməkdaşlarının bu vasitələrin düzgün istifadəsi barədə xüsusi təlimlər keçməsi və məlumat təhlükəsizliyi mədəniyyətini inkişaf etdirməsidir.

Nəticə etibarilə, şifrəli ünsiyyət kanalları yalnız texnoloji seçim deyil, həm də etik və hüquqi öhdəlikdir. Onların istifadəsi insan alveri qurbanlarının təhlükəsizliyini, məxfilik hüququnu və bərpa prosesinə inamını təmin edir. Qlobal praktika da göstərir ki, şifrəli ünsiyyət olmadan nə hüquq-mühafizə, nə də sosial xidmət orqanlarının fəaliyyəti effektiv və etibarlı ola bilər. Buna görə də müasir mübarizə strategiyalarında şifrələmə texnologiyalarının tətbiqi vacib şərt kimi qəbul edilməlidir.

Nümunə.

Addım	**Tövsiyə olunan fəaliyyət**	**Alətlər / Metod**	**Qeydlər / Misallar**
1. Əsas prinsiplər	Yalnız zəruri məlumatı topla; qurbanın razılığını al; anonimliyi qoru	"Minimum məlumat prinsipi", məxfilik öhdəliyi	Razılıq olmadan ad, ünvan, foto paylaşma
2. Kanal seçimi	Həssas hallarda ən təhlükəsiz kanalı seç	Signal (üstünlük), WhatsApp (2FA + yox olan	Qurban ilkin olaraq WhatsApp istifadə edirsə, sonra Signal-a yönləndir

		mesajlar), Telegram Secret Chat	
3. İlk təmas	Sadə və etibarlı mesaj göndər	Travma-informasiyalı skript	"Adınızı yazmaq məcburi deyil. Təhlükəsiz ünsiyyət üçün sizi gizli kanala keçirə bilərik"
4. Əlavə izləmə	Davranış və məlumatı yoxla	Reverse image search, faktların təsdiqi	Eyni foto bir neçə elan saytında çıxırsa, risk artır
5. Yüksək risk əlaməti	Pasport tələb olunması, real görüş dəvəti, sərhəd keçid vədləri	Risk matrisində qırmızı zona	Yeniyetmədən şəxsiyyət vəsiqəsinin surəti istənilir
6. Təcili yönləndirmə	Hüquq-mühafizə və sığınacaqlara məlumat ötür	102, MİA İnsan alverinə qarşı mübarizə baş idarəsi, MİDİM mexanizmi	Qurbana: "Sizin təhlükəsizliyiniz önəmlidir, sizi dərhal təhlükəsiz məkana yönləndiririk"
7. Məlumatın qorunması	Sübutların təhlükəsiz saxlanması	Şifrəli fayl anbarı, xidməti cihaz	Fayl adı: "20250930_Signal_PasportTələbi"
8. İşi bağlama	Artıq məlumatları sil, yalnız statistik anonim qeyd saxla	Silinmə protokolu, GDPR uyğunluq	İstifadə olunmamış fotolar və ünvan məlumatları tam silinir

6.4. Sübutların saxlanması (screenshot, link, vaxt möhürü)

Sübutların düzgün saxlanması rəqəmsal insan alveri ilə mübarizədə həm hüquqi, həm də etik baxımdan əsas şərtlərdən biridir. Əldə olunan materialların (screenshot, link, vaxt möhürü və s.) bütövlüyünün qorunması qurbanın müdafiəsi, istintaqın effektivliyi və məhkəmə prosesində sübutların etibarlılığı üçün

həyati əhəmiyyət daşıyır. Akademik müzakirələrdə də vurğulandığı kimi, sübutların toplanması və saxlanmasında zəncirvari izləmə (chain of custody) prinsipi əsasdır – yəni hər bir materialın kim tərəfindən, hansı vaxtda və necə götürüldüyü dəqiq qeydə alınmalıdır[62] .

Ən çox istifadə edilən üsullardan biri screenshotların (ekran görüntülərinin) saxlanmasıdır. Bu zaman görüntünün orijinal formatda, dəyişiklik edilmədən, faylın yaradılma tarixi və cihaz məlumatları ilə birlikdə arxivləşdirilməsi vacibdir. Əgər mümkün olarsa, metaməlumatlar (metadata) da saxlanmalıdır. Bu, məhkəmə və hüquq-mühafizə orqanları qarşısında sübutun etibarlılığını artırır[63].

İkinci mühüm element linklərin və onlayn məzmunun arxivləşdirilməsidir. Çünki sosial media paylaşımları və elanlar tez silinə və ya dəyişdirilə bilər. Bu məqsədlə "veb səhifə şəkli" texnologiyaları və ya rəqəmsal sübut toplama proqramları istifadə olunur. Latonero qeyd edir ki, insan alveri ilə bağlı onlayn izlərin vaxtında saxlanmaması təhqiqatın davamlılığına ciddi zərər vurur[64].

Üçüncü vacib üsul vaxt göstəricisi (timestamp) tətbiqidir. Sübutların götürülmə tarixi və saatı dəqiq qeyd olunmalıdır ki, onların hadisə vaxtı ilə əlaqəsi sübut olunsun. Bu, xüsusilə hüquqi müstəvidə sübutun qəbul olunması üçün şərtdir. Müasir platformalar – məsələn, "Blokçeyn üzərindən vaxt qeydiyyatı" texnologiyaları – dəyişdirilməz vaxt möhürü təmin etmək üçün istifadə olunur[65].

Əlavə olaraq, sübutların saxlanmasında etik prinsiplər gözlənilməlidir. Qurbanın anonimliyi qorunmalı, onun şəxsiyyətini birbaşa açıqlayan elementlər (üz şəkli, ünvan və s.) yalnız hüquqi zərurət hallarında saxlanmalıdır. Brunovskis və Surtees göstərirlər ki, həssas məlumatların artıq saxlanması qurbanların təkrar zərər

[62] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.

[63] Sommer, P., & Brown, I. (2011). Reducing systemic cyber security risk. *OECD/IFP Project on Future Global Shocks*.

[64] Latonero, M. (2011). *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*. USC Annenberg Center.

[65] Lemieux, V. L. (2016). Trusting records: Is Blockchain technology the answer? *Records Management Journal*, 26(2), 110–139.

görməsinə səbəb ola bilər.

Nəticə olaraq, screenshot, link və vaxt möhürlərinin sistemli şəkildə saxlanması yalnız istintaqın gücləndirilməsi üçün deyil, həm də qurbanların hüquqlarının qorunması üçün zəruridir. Bu prosesin akademik və hüquqi çərçivəyə uyğun şəkildə aparılması Azərbaycan qanunvericiliyi və beynəlxalq standartlarla tam uzlaşır və rəqəmsal insan alveri ilə mübarizədə əsaslı alət rolunu oynayır.

7. İş axını / protokol

İş axını və ya protokol sosial iş, hüquq-mühafizə və insan alveri ilə mübarizə sahəsində fəaliyyətlərin ardıcıllığını və icra qaydalarını müəyyən edən normativ-etik çərçivədir. Bu anlayış konkret hadisə və ya proses zamanı kimlərin hansı addımı atmalı olduğunu, hansı məlumatların necə toplanıb emal ediləcəyini və hansı qurumların məsuliyyət daşıdığını aydın şəkildə göstərir. İş axını həm təşkilati nizam-intizamı, həm də hüquqi uyğunluğu təmin etmək məqsədi daşıyır.

Protokol adətən bir neçə əsas mərhələni əhatə edir: ilkin identifikasiya və siqnalın qeydi, risk qiymətləndirilməsi, məlumatların məxfi şəkildə toplanması, yönləndirmə və müdafiə mexanizmlərinin işə salınması, sübutların qorunması, habelə qurbanın uzunmüddətli sosial reabilitasiyası. Burada həm əməliyyat (kimin nə vaxt hansı addımı atacağı), həm də etik prinsiplər (anonimlik, minimum məlumat prinsipi, razılıq əsasında müdaxilə) əsas götürülür.

Azərbaycan kontekstində bu iş axını ilk növbədə "İnsan alverinə qarşı mübarizə haqqında" Qanunla tənzimlənir. Qanunun 14 və 15-ci maddələri qurbanların hüquqlarının qorunması və məxfilik öhdəliklərini müəyyən edir. Cinayət Prosessual Məcəlləsi iş axınında istintaq və məhkəmə mərhələlərində sübutların toplanması, qurban və şahidlərin təhlükəsizliyinin təmin olunması üçün hüquqi əsas verir (maddə 96, 97 və 123). "Şəxsi məlumatlar haqqında" Qanun isə məlumatların yalnız qanuni və məqsədyönlü şəkildə toplanmasını və minimum məlumat prinsipinə riayət olunmasını tələb edir.

Beynəlxalq çərçivədə iş axını və protokolların qurulması BMT-nin Palermo Protokolu (2000) ilə əlaqələndirilir; bu sənəd dövlətlərə insan alverinin qarşısını alma, qurbanları qoruma və cinayətkarları cəzalandırma istiqamətində 3P (prevention, protection, prosecution) yanaşmasını təqdim edir. Avropa Şurasının İnsan Alverinə qarşı Mübarizə Konvensiyası (2005) və onun həyata keçirilməsinə nəzarət edən GRETA mexanizmi də dövlətlərin qurban yönümlü iş axınlarını formalaşdırmasını tələb edir.

Həmçinin ATƏT rəqəmsal mühitdə insan alverinə qarşı fəaliyyətlərdə təhlükəsiz kommunikasiya və məlumat mübadiləsi protokollarını xüsusi tövsiyə edir.

Akademik ədəbiyyatda iş axını və protokolların əhəmiyyəti onların fragmentar müdaxilələrin qarşısını alması və koordinasiyanı gücləndirməsi ilə əsaslandırılır. Brunovskis və Surtees (2012) göstərirlər ki, düzgün işlənmiş protokollar olmadan qurbanların təkrar travmatizasiyası və hüquqi boşluqlardan sui-istifadə halları çoxalır. Casey isə sübutların saxlanmasında protokolun hüquqi qəbulolunma baxımından zəruri olduğunu vurğulayır.

Protokolun hazırlanması sadəcə yazılı sənəd yaratmaq deyil, həm də fəaliyyətlərin ardıcıllığını, məsul qurumların öhdəliklərini və etik-hüquqi prinsipləri aydın şəkildə müəyyənləşdirmək prosesidir. Akademik və praktiki yanaşmada protokol hazırlanması aşağıdakı əsas mərhələləri əhatə edir:

Birincisi, məqsəd və əhatə dairəsi müəyyən edilir. Protokol hansı vəziyyətlər üçün nəzərdə tutulur – məsələn, insan alveri qurbanının aşkarlanması, təcili yönləndirmə, sosial dəstək və ya sübutların toplanması – bunlar dəqiq qeyd olunmalıdır. Məqsədin aydın şəkildə yazılması həm əməliyyat əməkdaşları, həm də tərəfdaş qurumlar üçün çərçivə yaradır.

İkincisi, mövcud hüquqi və normativ baza nəzərə alınır. Azərbaycanda bu, "İnsan alverinə qarşı mübarizə haqqında" Qanun, "Şəxsi məlumatlar haqqında" Qanun, Cinayət Məcəlləsi (maddə 144-1), Cinayət Prosessual Məcəlləsi (maddə 96, 97, 123) və digər müvafiq normativ sənədləri əhatə edir. Beynəlxalq müstəvidə isə Palermo Protokolu, Avropa Şurasının Konvensiyası və GRETA tövsiyələri əsas götürülür.

Üçüncüsü, tərəflərin rolu və məsuliyyəti dəqiq bölüşdürülür. Protokolda kim ilkin identifikasiya aparır (sosial işçi, polis, səhiyyə işçisi), kim məlumatı toplayır, kim yönləndirir və kim sonrakı reabilitasiya ilə məşğul olur – bu ardıcıllıq aydın yazılmalıdır. Bu yanaşma həm də çoxsektorlu əməkdaşlıq modelini gücləndirir.

Dördüncüsü, əməliyyat addımları ardıcıllıqla təsvir edilir. Burada risk zonalarının təyini (yaşıl, sarı, qırmızı), qurbanla ilk təmas qaydaları, sübutların necə toplanıb saxlanacağı, hansı şifrəli

kanallardan istifadə olunacağı və hansı halda hüquq-mühafizə orqanlarına məlumat veriləcəyi konkretləşdirilir. Əməliyyat ardıcıllığı sadə və praktik olmalıdır ki, real şəraitdə sürətlə tətbiq edilə bilsin.

Beşincisi, etik və təhlükəsizlik prinsipləri sənədə daxil edilir. Burada minimum məlumat prinsipi, anonimlik və razılıq, travma-informasiyalı yanaşma, həmçinin qurban yönümlü müdaxilə əsas prinsiplər kimi qeyd olunur. Bu, qurbanların ikinci dəfə zərər görməsinin qarşısını almaq üçün vacibdir.

Altıncısı, monitorinq və yenilənmə mexanizmi əlavə olunur. Protokol statik sənəd olmamalı, texnoloji dəyişikliklərə, cinayətkar şəbəkələrin yeni metodlarına və qanunvericilikdəki yeniliklərə uyğun olaraq mütəmadi yenilənməlidir. Brunovskis və Surtees də qeyd edirlər ki, protokollar yalnız daim təkmilləşdirildikdə effektiv qalır.

Beləliklə, protokol hazırlanması hüquqi çərçivəyə söykənən, praktik ardıcıllığı olan, etik prinsiplərlə zəngin və çoxsektorlu əməkdaşlığa əsaslanan yazılı sənəd formalaşdırmaq deməkdir. Onun düzgün işlənməsi qurbanların müdafiəsini, sübutların etibarlılığını və dövlətin beynəlxalq öhdəliklərinin icrasını təmin edir.

7.1. Addım 1: Sadə izləmə, ilkin siqnallar

Sadə izləmə mərhələsi rəqəmsal insan alverinin aşkarlanması üzrə iş axınının ilk addımıdır və burada əsas məqsəd mümkün riskləri göstərən ilkin siqnalları qeydə almaqdır. Bu mərhələdə insan alverinə dair birbaşa sübutlar deyil, potensial təhlükəni işarə edən davranış nümunələri, elan məzmunları və ya onlayn fəaliyyətlər müşahidə olunur. Sadə izləmə, həm sosial işçilər, həm də hüquq-mühafizə əməkdaşları üçün "erkən xəbərdarlıq mexanizmi" rolunu oynayır. Casey qeyd edir ki, ilkin mərhələdə toplanan zəif siqnalların vaxtında təhlili gələcəkdə güclü sübutların formalaşmasına imkan yaradır.

İlkin siqnalların əhatə dairəsi genişdir və əsasən üç qrupda təsnif edilə bilər. Birincisi, onlayn elanlar və paylaşımlar: "xaricdə

yüksək maaşlı iş, təcrübə tələb olunmur", "tez pul qazanmaq imkanı", "pulsuz səyahət və qalmaq" kimi elanlar insan alveri riskinin ilkin göstəriciləri hesab olunur. Bu tip elanlar çox vaxt qeyri-rəsmi səhifələrdə və ya sosial şəbəkələrdə yayımlanır.

İkincisi, istifadəçi davranışları- müəyyən şəxsin dəfələrlə eyni tipli elanlara baxması və ya şübhəli profillərlə əlaqə yaratması əlavə diqqət tələb edən siqnallardır.

Üçüncüsü, profil və məzmun uyğunsuzluqları: yeni yaradılmış, az sayda izləyicisi olan profillərin intensiv şəkildə "iş və təhsil imkanı" elanları paylaşması və ya saxta fotolar istifadə etməsi risk göstəricisi ola bilər.

Praktik nümunələr bu mərhələni daha da aydınlaşdırır. Məsələn, sosial mediada bir istifadəçi qısa müddətdə beş müxtəlif "vizasız iş" elanına reaksiya verir, amma hələ şəxsi məlumat paylaşmayıb. Bu, sadə izləmə mərhələsində qeydiyyata alınmalı, lakin hələ təcili müdaxilə tələb etməyən siqnaldır. Digər nümunədə isə elan saytında "gənc qızlar üçün iş" başlığı ilə yayımlanmış elanlarda əlaqə məlumatının real işəgötürənlə uzlaşmaması müşahidə olunur. Bu da sadə izləmə mərhələsində qeydə alınaraq daha dərin təhlilə yönləndirilə bilər.

İlkin siqnalların toplanması yalnız passiv müşahidə deyil, həm də profilaktik tədbirlər üçün baza rolunu oynayır. ATƏT qeyd edir ki, texnologiya vasitəsilə insan alverinə qarşı mübarizədə sadə izləmə vasitələri qurbanların identifikasiyası və risklərin xəritələndirilməsi üçün ilk addımdır. Brunovskis və Surtees isə vurğulayırlar ki, qurbanların təhlükəsizliyini təmin etmək üçün zəif siqnallar belə diqqətdən yayınmamalıdır, çünki onlar çox vaxt istismara aparan yolun başlanğıcını göstərir.

Beləliklə, sadə izləmə mərhələsi insan alverinə qarşı mübarizədə fundamental başlanğıc nöqtəsidir. Bu addımın əhəmiyyəti ondadır ki, görünüşcə zərərsiz və təsadüfi görünən siqnallar vaxtında qeydə alındıqda həm qurbanların erkən müdafiəsinə, həm də cinayətkar şəbəkələrin aşkarlanmasına şərait yaradır.

7.2. Addım 2: Böyl axtarışı → filtrasiya

Böylün axtarışı rəqəmsal insan alverinin izlənməsi zamanı sadə açar sözlərin istifadəsindən daha dərin və sistemli bir mərhələdir. Bu üsulda məzmun müəyyən qaydalar üzrə filtrlənir və mətnlər, elanlar və ya sosial media paylaşımları arasında gizlənmiş nümunələrin üzə çıxarılması asanlaşır. Böyl məntiqi "AND", "OR", "NOT" və sitat işarələri ("…") kimi operatorlardan istifadə etməklə axtarış sorğularının dəqiqliyini artırır və nəticələri daraldaraq riskli məzmunun filtrasiya edilməsinə imkan verir.

Akademik müzakirələrdə də vurğulandığı kimi, rəqəmsal cinayətlərin aşkarlanmasında Böylün axtarış strategiyası həm süni intellekt alətləri, həm də insan monitorinqi üçün əsas vasitə rolunu oynayır. Bu yanaşma sadə siqnalların (Addım 1) daha dərin analizinə xidmət edir. Məsələn, "iş OR job AND 'no experience' AND abroad" sorğusu xaricdə təcrübəsiz gənclər üçün iş elanlarını birləşdirir və potensial risk daşıyan məzmunu daha dəqiq müəyyənləşdirir.

Praktik misallara baxaq. Sosial mediada "pulsuz viza" + "otel təmin olunur" kimi açar sözlər birlikdə axtarıldıqda insan alverçilərinin tez-tez istifadə etdiyi cəlbedici vədlər üzə çıxır. Digər tərəfdən, "free travel AND modeling OR hostess" sorğusu xüsusilə gənc qızlara yönələn riskli elanları filtrasiya edə bilər. Əksinə, "NOT internship" operatoru ilə həqiqi təcrübə proqramları riskli elanlardan ayrılır. Bu cür filtrasiya metodları ilkin siqnalların daha dəqiq dəyərləndirilməsinə imkan verir.

Filtrasiyanın əsas əhəmiyyəti ondadır ki, riskli məzmun dənizində məqsədyönlü şəkildə axtarış aparılır və insan resurslarının yüklənməsi azaldılır. Casey göstərir ki, sübut toplama prosesində məzmunun düzgün filtrasiya olunmaması həm hüquqi, həm də etik problemlər yarada bilər. Brunovskis və Surtees isə qeyd edirlər ki, həssas məlumatların artıq yığılması qurbanların etimadını azaldır. Buna görə Böylün axtarış sistemi yalnız məqsədli şəkildə tətbiq olunmalıdır.

Beləliklə, Böyl axtarışı sadə izləmədən sonrakı addım olaraq ilkin siqnalların dərinləşdirilmiş filtrasiya mərhələsini təşkil edir. Bu

metod həm qurbanların daha tez identifikasiyasına, həm də istismarçıların fəaliyyət nümunələrinin aşkarlanmasına xidmət edir və insan alverinə qarşı rəqəmsal mübarizədə elmi əsaslı yanaşmanın zəruri tərkib hissəsidir.

Nümunə

Kateqoriya	Axtarış sorğusu (Böyl formatında)	Praktik istifadə nümunəsi
Xaricdə iş elanları	"no experience" AND (abroad OR overseas) AND "free visa"	Təcrübəsiz gənclərə “pulsuz viza” ilə iş təklif edən riskli elanların aşkarlanması
Model agentlikləri və “hostess” elanları	(model OR hostess OR dancer) AND ("free travel" OR "paid accommodation")	“Səyahət və qalmaq pulsuz” şüarı ilə qadınların istismara cəlb edilməsi riskini filtrasiya etmək
Təhsil və təcrübə adı altında istismar	("scholarship" OR "internship") AND ("no tuition" AND "work opportunity")	Təhsil və təcrübə elanlarının arxasında gizlədilən işçi istismar hallarını müəyyənləşdirmək
Uşaqlar və yeniyetmələr üçün risk	("under 18" OR "teen") AND ("job offer" OR "modeling")	Yetkinlik yaşına çatmayanların “iş” və ya “model” elanları ilə cəlb olunmasını aşkarlamaq
Turizm və əyləncə sektoru	(massage OR spa OR escort) AND ("foreign women" OR "travel package")	Əyləncə və turizm adı ilə qadın alverinə dair siqnalların filtrasiyası
Ailə qulluqçusu / ev işləri	("domestic worker" OR "babysitter") AND ("no contract" OR "free ticket")	Miqrant qadınların qeyri-qanuni şərtlərlə işə cəlb olunması risklərini müəyyən etmək
Riskli açar sözlərin istisnası	("job offer" AND abroad) NOT ("Erasmus" OR "official internship")	Qanuni təhsil proqramlarını riskli elanlardan ayırmaq üçün filtrasiya aparmaq

Bu sorğular praktikada sosial şəbəkələrdə, elan saytlarında və

açıq mənbə monitorinq sistemlərində tətbiq edilə bilər. Onlar sadə izləmədən (Addım 1) gələn ilkin siqnalları dəqiqləşdirərək (Addım 2) riskli məzmunu daha aydın filtrasiya etməyə imkan verir.

7.3. Addım 3: Risk matrisinə görə təsnifat

Risk matrisinə görə təsnifat insan alveri ilə mübarizədə ilkin siqnallar və filtrasiya nəticəsində əldə olunan məlumatların risk dərəcəsinə uyğun olaraq qruplaşdırılmasıdır. Bu mərhələdə əsas məqsəd risklərin prioritetləşdirilməsi, müdaxilə ardıcıllığının müəyyənləşdirilməsi və resursların daha səmərəli istifadəsidir. Risk matrisinin tətbiqi sosial iş və hüquq-mühafizə təcrübəsində qəbul olunmuş "təhlükəsizlik tədbirləri" yanaşmaya uyğun şəkildə aparılır.

Risk matrisində adətən üç zona müəyyən edilir: yaşıl (aşağı risk), sarı (orta risk) və qırmızı (yüksək risk). Yaşıl zonaya daxil olan hallar ilkin müşahidə mərhələsində toplanan zəif siqnallardır. Burada qurbanın birbaşa təhlükə altında olması müşahidə edilmir, amma risk göstəriciləri mövcuddur. Məsələn, təcrübəsiz gənclər üçün elanlara maraq göstərilməsi və ya sosial mediada "pulsuz səyahət" kimi qeyri-real təkliflərə klikləmə bu qrupa aiddir. Bu zonada əsas tədbir monitorinq və profilaktik maarifləndirmədir.

Sarı zona orta risk qrupunu əhatə edir və burada artıq müəyyən davranış və ya məzmun potensial istismar niyyətini göstərir. Məsələn, real əlaqə qurulub, şəxsi məlumat (telefon nömrəsi, foto) paylaşılıb və ya "işə qəbul" prosesi barədə müzakirələr aparılıbsa, risk daha yüksək sayılır. Bu mərhələdə əlavə izləmə və təhlükəsizlik tədbirləri vacibdir, çünki potensial qurban istismara doğru cəlb edilməkdədir.

Qırmızı zona isə yüksək risk qrupunu təşkil edir və burada qurbanın birbaşa təhlükə altında olması ehtimalı yüksəkdir. Buraya pasport və digər sənəd tələbləri, real görüş və ya səyahət planlarının razılaşdırılması, yetkinlik yaşına çatmayanlarla yazışma halları daxildir. Bu zonada dərhal hüquq-mühafizə orqanlarına məlumat verilməsi və qurbanın təhlükəsizliyinin təmin olunması əsas prioritetdir.

Risk təsnifatı yalnız əməliyyat baxımından deyil, həm də etik və hüquqi baxımdan vacibdir. Brunovskis və Surtees qeyd edirlər ki, risk dərəcələrinin düzgün müəyyənləşdirilməsi qurbanların ikinci dəfə zərər görməsinin qarşısını alır və onların müdafiəsini daha effektiv edir. Bu yanaşma həmçinin dövlətlərin beynəlxalq öhdəlikləri ilə – xüsusilə Palermo Protokolu və Avropa Şurasının İnsan Alverinə qarşı Mübarizə Konvensiyası uzlaşır.

Beləliklə, risk matrisinə görə təsnifat prosesi sadə siqnallardan və filtrasiya nəticələrindən çıxış edərək qurban yönümlü müdaxilə ardıcıllığını təmin edir. Yaşıl zona maarifləndirmə və monitorinq, sarı zona əlavə izləmə və dəstək, qırmızı zona isə təcili müdaxilə və yönləndirmə tələb edir. Bu yanaşma sübutların daha sistemli toplanmasına, qurbanların təhlükəsizliyinin qorunmasına və insan alverinə qarşı koordinasiyalı mübarizəyə şərait yaradır.

7.4. Addım 4: Qırmızı siqnal olduqda yönləndirmə (hüquq-mühafizə, sığınacaq)

Qırmızı siqnallar müşahidə olunduqda – yəni insan alveri riskinin yüksək səviyyəyə çatdığı, qurbanın birbaşa istismar təhlükəsi ilə üzləşdiyi hallarda – ən vacib addım dərhal və düzgün yönləndirmədir. Bu mərhələ sadəcə məlumat ötürmək deyil, həm də qurbanın həyatını qorumaq, hüquqlarını təmin etmək və təkrar travmanın qarşısını almaq üçün multidissiplinar müdaxilə mexanizmini işə salmaqdır.

Yüksək risk əlamətləri adətən qurbanın pasport və ya digər şəxsiyyət sənədlərinin istənilməsi, real görüş və ya səyahət planlarının razılaşdırılması, yetkinlik yaşına çatmayan şəxslərlə yazışmaların aparılması və ya "işə qəbul" prosesində maliyyə ödənişlərinin tələb edilməsi ilə özünü göstərir. Bu kimi hallarda sosial işçi və ya monitorinq aparan mütəxəssis məlumatı dərhal hüquq-mühafizə orqanlarına ötürməlidir. Azərbaycanda bu, birbaşa 152 xidməti və ya Daxili İşlər Nazirliyinin İnsan Alverinə qarşı Mübarizə Baş İdarəsi vasitəsilə həyata keçirilir. Cinayət Prosessual Məcəlləsinin 123-cü maddəsi bu mərhələdə qurbanın

təhlükəsizliyini təmin etmək üçün xüsusi tədbirlərin görülməsini, məsələn, qapalı məhkəmə iclası və kimlik məlumatlarının gizlədilməsini nəzərdə tutur.

Eyni zamanda, yönləndirmə yalnız hüquq-mühafizə ilə məhdudlaşmır. Qurbanın dərhal təhlükəsiz məkana – sığınacağa yerləşdirilməsi vacibdir. Azərbaycan Respublikasının "İnsan alverinə qarşı mübarizə haqqında" Qanununun 14 və 15-ci maddələri dövlətin qurbanlara sosial dəstək, tibbi yardım və müvəqqəti sığınacaq təmin etmək öhdəliyini açıq şəkildə təsbit edir. Bu çərçivədə QHT-lər və dövlət qurumları arasında qurulmuş Milli İstiqamətləndirmə Mexanizmi qırmızı siqnal hallarında koordinasiyanı təmin edən əsas alət kimi çıxış edir.

Praktik misallara nəzər salsaq, əgər sosial mediada bir yeniyetməyə "sərhədi pulsuz keçirmək və model işində məşğulluq təmin etmək" təklifi verilibsə, bu, qırmızı siqnal sayılır. Belə halda sosial işçi həmin məlumatı hüquq-mühafizə orqanına ötürməli, eyni zamanda qurbanla etibarlı ünsiyyət quraraq onu QHT-nın sığınacağına istqiamətləndirir. Digər nümunədə, miqrant qadına "pulsuz bilet" vəd edilərək pasportunun əvvəlcədən göndərilməsi tələb olunursa, bu, yüksək riskin əlamətidir və dərhal cinayət təhqiqatına cəlb olunmalıdır.

Akademik tədqiqatlar göstərir ki, qırmızı siqnallar zamanı düzgün istiqamətləndirmə aparılmadıqda qurbanların ikinci dəfə zərər çəkmə riski çoxalır. Brunovskis və Surtees qeyd edirlər ki, kömək üçün müraciət edən qurbanların bir hissəsi məhz istqiamətləndirmə mexanizmlərinin qeyri-effektivliyi səbəbilə yardım prosesindən imtina edir. Zimmerman və Kiss isə qırmızı siqnal hallarında "təhlükəsizlik tədbirləri" yanaşmanın qurbanların travma sonrası bərpa prosesində həlledici olduğunu göstərirlər.

Beynəlxalq öhdəliklər də bu mərhələdə istqiamətləndirməni vacib tələb kimi müəyyən edir. Palermo Protokolu dövlətlərdən qurbanların dərhal müdafiə olunmasını, Avropa Şurasının Konvensiyası isə onların təhlükəsizliyinin və anonimliyinin təmin edilməsini tələb edir. ATƏT tövsiyələrində isə rəqəmsal mühitdə aşkarlanan qırmızı siqnallar zamanı hüquq-mühafizə və sosial dəstək xidmətləri arasında koordinasiyanın gecikmədən qurulması

vacib hesab edilir.

Nəticə olaraq, qırmızı siqnal hallarında yönləndirmə hüquq-mühafizə və sığınacaq xidmətlərinin sinxron fəaliyyətini tələb edən ən kritik mərhələdir. Bu, yalnız cinayətkarların cəzalandırılması deyil, həm də qurbanın həyatının və hüquqlarının qorunması baxımından əsaslı əhəmiyyət daşıyır. Düzgün işləyən protokol isə qurban yönümlü müdaxilənin beynəlxalq standartlara və milli qanunvericiliyə uyğunluğunu təmin edir.

8. Nəticə və tövsiyyələr

Rəqəmsal insan alveri ilə mübarizədə risklərin erkən identifikasiyası, məlumatların təhlükəsiz şəkildə toplanması və düzgün yönləndirmə mexanizmlərinin qurulması yalnız texniki deyil, həm də etik və hüquqi məsuliyyətdir. İstər sadə izləmə, istər Böyl axtarış, istərsə də risk matrisinə əsaslanan təsnifat mərhələləri göstərir ki, fragmentar müdaxilələr əksər hallarda qeyri-effektivdir və qurbanların ikinci dəfə zərər görməsi ilə nəticələnə bilər. Ona görə də, bu proseslərin ardıcıllıqla, protokollara uyğun şəkildə həyata keçirilməsi mühüm əhəmiyyət daşıyır.

Tövsiyə olunur ki, hər bir sosial işçi və hüquq-mühafizə əməkdaşı minimum məlumat prinsipinə ciddi riayət etsin, qurbanın anonimliyini qorusun və yalnız zəruri hallarda identifikasiyaedici məlumatı paylaşsın. Bu, həm Azərbaycan qanunvericiliyinin (Konstitusiya, "Şəxsi məlumatlar haqqında" Qanun, Cinayət Prosessual Məcəlləsi) tələblərinə, həm də beynəlxalq sənədlərdə (Palermo Protokolu, Avropa Şurası Konvensiyası) müəyyən olunmuş öhdəliklərə uyğundur.

Qırmızı siqnal hallarında yönləndirmə mexanizmləri sürətli və koordinasiyalı olmalıdır: hüquq-mühafizə orqanları ilə yanaşı sığınacaqlar, tibbi və psixoloji xidmətlər dərhal işə cəlb olunmalıdır. Bu yanaşma qurbanın təhlükəsizliyini və sosial reabilitasiyasını təmin edir, eyni zamanda dövlətin insan hüquqlarına hörmət prinsipinə sadiqliyini göstərir.

Akademik tədqiqatlar da göstərir ki, effektiv risk izləmə və yönləndirmə sistemləri qurbanların ədalətə çıxış imkanlarını artırır, travmanın dərinləşməsinin qarşısını alır və insan alveri ilə mübarizədə davamlı nəticələr verir. Bu baxımdan, həm milli, həm də beynəlxalq səviyyədə əməkdaşlığın gücləndirilməsi, şifrəli ünsiyyət texnologiyalarının tətbiqi və protokolların mütəmadi yenilənməsi tövsiyə olunur.

Nəticə etibarilə, rəqəmsal insan alveri ilə mübarizədə iş axınının hər bir addımı – izləmə, filtrasiya, risk təsnifatı və yönləndirmə – bir-birini tamamlayan elementlərdir. Bu addımların elmi əsaslara, etik prinsiplərə və hüquqi çərçivələrə söykənməsi

insan alveri qurbanlarının müdafiəsində ən mühüm zəmanət hesab olunmalıdır.

8.1. Təlimatın tətbiqi

Rəqəmsal insan alveri ilə mübarizə üzrə hazırlanmış təlimat yalnız nəzəri çərçivə deyil, həm də praktik fəaliyyətləri istiqamətləndirən əməli sənəddir. Onun tətbiqi, həm hüquq-mühafizə orqanlarının, həm də sosial xidmət qurumlarının koordinasiyalı işləməsini təmin etməklə qurban yönümlü müdaxilə mexanizmlərini gücləndirir.

Təlimatın tətbiqi ilk növbədə institusional səviyyədə həyata keçirilir. Dövlət orqanları (Daxili İşlər Nazirliyi, Əmək və Əhalinin Sosial Müdafiəsi Nazirliyi, Ailə, Qadın və Uşaq Problemləri üzrə Dövlət Komitəsi) və qeyri-hökumət təşkilatları protokolun müddəalarını gündəlik iş axınlarına daxil etməlidirlər. Burada hüquqi öhdəliklər – "İnsan alverinə qarşı mübarizə haqqında" Qanun, "Şəxsi məlumatlar haqqında" Qanun və Cinayət Prosessual Məcəllə (m.96, m.123) – tətbiqin hüquqi əsasını təşkil edir.

Əməliyyat səviyyəsində, təlimat sosial işçilərin və polis əməkdaşlarının konkret vəziyyətlərdə necə davranmalı olduqlarını göstərir: sadə izləmə ilə siqnalların qeydi, Böyl axtarış ilə riskli məzmunun filtrasiyası, risk matrisinə görə təsnifat və qırmızı siqnal hallarında yönləndirmə. Bu, protokolların vahid qaydada icrasına şərait yaradır və səhvlərin minimuma endirilməsinə xidmət edir.

Praktik tətbiq nümunələri göstərir ki, təlimat olmadan müxtəlif qurumlar arasında məlumat mübadiləsi pərakəndə olur və qurbanın müdafiəsi zəifləyir. Məsələn, ATƏT hesabatında qeyd edilir ki, risk matrisinə əsaslanan standart protokollar tətbiq edilən ölkələrdə qurbanların identifikasiyası və müdafiəsi daha sürətli və effektiv həyata keçirilir. Zimmerman və Kiss isə vurğulayırlar ki, təlimatın tətbiqi travma-informasiyalı yanaşmanı gücləndirərək qurbanların ikinci dəfə zərər görmə ehtimalını azaldır.

Monitorinq və qiymətləndirmə də təlimatın tətbiqinin ayrılmaz hissəsidir. Təlimata uyğun görülən tədbirlər mütəmadi qiymətləndirilməli, nəticələr əsasında yenilənmələr aparılmalıdır.

Brunovskis və Surtees göstərirlər ki, təlimatlar statik sənəd deyil, dəyişən cinayət mexanizmlərinə cavab verən dinamik alət olmalıdır.

Nəticə olaraq, təlimatın tətbiqi həm milli qanunvericiliyə, həm də beynəlxalq öhdəliklərə uyğun şəkildə vahid iş axını yaradır. Bu, qurbanların müdafiəsini gücləndirir, dövlət qurumları ilə QHT-lərin əməkdaşlığını möhkəmləndirir və rəqəmsal insan alverinə qarşı mübarizədə səmərəliliyi artırır.

8.2. Yerli və beynəlxalq əməkdaşlıq (polis, QHT, beynəlxalq şəbəkələr)

Rəqəmsal insan alveri ilə mübarizədə ən kritik amillərdən biri çoxsəviyyəli əməkdaşlıqdır. İnsan alveri transmilli xarakter daşıdığı üçün yalnız bir qurumun fəaliyyəti ilə effektiv nəticə əldə etmək mümkün deyil. Əməkdaşlıq həm milli səviyyədə dövlət strukturları və QHT-lər arasında, həm də beynəlxalq şəbəkələrlə inteqrasiya vasitəsilə həyata keçirilməlidir.

Yerli əməkdaşlıq. Azərbaycan kontekstində əsas məsul qurum Daxili İşlər Nazirliyinin İnsan Alverinə qarşı Mübarizə Baş İdarəsidir. Bu qurum cinayətkar şəbəkələrin aşkarlanması, istintaqın aparılması və qurbanların təhlükəsizliyinin təminində əsas rol oynayır. Lakin yalnız hüquq-mühafizə tədbirləri kifayət etmir; sosial dəstək, tibbi yardım və psixoloji reabilitasiya QHT-lərin iştirakı ilə həyata keçirilir. Məsələn, QHT-lər qurbanların sığınacaqlara yerləşdirilməsi, hüquqi məsləhət və sosial adaptasiya xidmətlərini təmin edir. Belə çoxsektorlu əməkdaşlıq həm qurban yönümlü yanaşmanı gücləndirir, həm də dövlətin beynəlxalq öhdəliklərinin icrasını asanlaşdırır.

Beynəlxalq əməkdaşlıq. İnsan alveri çox vaxt transsərhəd cinayət olduğuna görə, beynəlxalq şəbəkələrlə əməkdaşlıq zəruridir. Azərbaycan 2000-ci ildən Palermo Protokoluna, 2005-ci ildən Avropa Şurasının İnsan Alverinə qarşı Mübarizə Konvensiyasına qoşulmaqla bu əməkdaşlıq çərçivəsini rəsmiləşdirib. Bu sənədlərə uyğun olaraq məlumat mübadiləsi, təhqiqatların koordinasiyası və qurbanların repatriasiyası sahəsində digər dövlətlərin hüquq-mühafizə orqanları ilə əməkdaşlıq gücləndirilir. INTERPOL və

EUROPOL kimi beynəlxalq polis şəbəkələri cinayətkar qrupların izlənməsi və sübutların paylaşılmasında mühüm rol oynayır.

QHT-lər və beynəlxalq şəbəkələr. Beynəlxalq QHT-lər, məsələn, La Strada International və Beynəlxlaq Miqrasiya Təşkilatı qurbanların təhlükəsiz şəkildə repatriasiyası və reinteqrasiyasında dəstək göstərirlər. Praktik misal olaraq, Azərbaycandan insan alveri qurbanlarının başqa ölkələrə aparılması hallarının araşdırılmasında BMqT həm hüquqi, həm də logistik yardım göstərib. Bu əməkdaşlıq olmadan qurbanların sərhədlərarası mühafizəsi mümkün olmazdı.

Misal. Azərbaycan hüquq-mühafizə orqanları tərəfindən 2019-cu ildə aşkarlanan qadın alveri işi zamanı qurbanların bir qismi Türkiyəyə aparılmışdı. Bu zaman həm Türkiyə polisi, həm də IOM və yerli QHT-lərin iştirakı ilə qurbanların repatriasiyası təmin edildi. Hadisə göstərdi ki, yalnız polis əməliyyatları deyil, beynəlxalq koordinasiya və QHT-lərin sosial dəstək mexanizmləri olmadan qurban yönümlü nəticə əldə etmək mümkün deyil.

Akademik baxış. Zimmerman və Kiss qeyd edirlər ki, insan alveri ilə mübarizə yalnız cinayətkar şəbəkələrin ifşası ilə məhdudlaşmamalıdır; çoxsəviyyəli əməkdaşlıq qurbanların bərpasını və sosial reinteqrasiyasını əsas prioritetə çevirməlidir. ATƏT isə vurğulayır ki, rəqəmsal mühitdə insan alveri ilə mübarizə üçün dövlət orqanları, QHT-lər və texnoloji platformalar arasında yeni nəsil əməkdaşlıq mexanizmləri yaradılmalıdır.

Nəticə. Yerli və beynəlxalq əməkdaşlıq olmadan rəqəmsal insan alveri ilə mübarizə effektiv ola bilməz. Polis əməliyyatları hüquqi çərçivəni təmin edir, QHT-lər qurbanlara sosial dəstək göstərir, beynəlxalq şəbəkələr isə transmilli cinayətkar qruplara qarşı koordinasiyanı təmin edir. Bu üç istiqamətin inteqrasiyası həm qurbanların müdafiəsi, həm də cinayətkarların məsuliyyətə cəlb edilməsi üçün fundamental şərtdir.

8.3. Daimi yenilənmələrə zərurət (açar sözlər, yeni platformalar, yeni taktikalar)

Rəqəmsal insan alveri fenomeni statik deyil, daim dəyişən və cinayətkar qrupların texnoloji mühitə uyğunlaşması ilə inkişaf edən

bir sahədir. Buna görə də monitorinq mexanizmlərinin, açar sözlərin, platformaların və istifadə olunan metodların mütəmadi şəkildə yenilənməsi vacibdir. Əgər bu yenilənmələr aparılmazsa, qurbanların identifikasiyası çətinləşir, hüquq-mühafizə orqanlarının fəaliyyəti zəifləyir və mövcud protokollar effektivliyini itirir .

Açar sözlərin dinamikası. İnsan alverçiləri aşkarlanmaqdan yayınmaq üçün tez-tez açar sözlərini dəyişdirir, açıq-aşkar riskli ifadələrdən kodlaşdırılmış və neytral görsənən terminlərə keçir. Məsələn, əvvəllər "free visa", "escort job" və "massage service" kimi açıq terminlərdən istifadə olunurdusa, hazırda "sponsor dəstəyi", "xaricdə imkan", "sağlamlıq mərkəzi" kimi daha neytral ifadələr üstünlük təşkil edir. Latonero göstərir ki, bu dəyişikliklər monitorinq sistemlərini tez köhnəldir və aşkarlama effektivliyini zəiflədir. Ona görə də açar söz bazalarının aylıq və ya ən geci rüblük əsasda yenilənməsi vacibdir.

Yeni platformaların sürətli mənimsənilməsi. İnsan alverçiləri izləmədən yayınmaq üçün ənənəvi platformaları tez-tez dəyişdirir. 2010-cu illərdə daha çox "Craigslist" və açıq elan saytları üzərində fəaliyyət göstərirdilərsə, hazırda Telegram kanalları, TikTok videoları, Instagram Reels və hətta Discord kimi oyun platformaları vasitəsilə gizli əlaqələr qururlar. ATƏT bu tendensiyanı "platforma miqrasiyası" adlandırır və xəbərdarlıq edir ki, əgər hüquq-mühafizə orqanları və QHT-lər yeni platformaları izləmə planına daxil etməsə, cinayətkar şəbəkələr sürətlə üstünlük qazanacaq. Azərbaycanda da əgər əvvəllər bu cür hallar əsasən iş elan saytlarında rast gəlinən "xaricdə iş" elanların da olurdusa, indi bunun Instagram bio və WhatsApp status bölmələrində gizlədilmələri müşahidə olunur.

Yeni taktikaların yaranması. Cinayətkar şəbəkələr yalnız elanları dəyişmir, həm də metodlarını da yeniləyirlər:

Sosial media inflyönserləri vasitəsilə cəlbetmə. Cazibədar həyat tərzini nümayiş etdirən saxta profillər yaradılır və gənclər "iş və ya modeling imkanları" adı ilə aldadılır.

Onlayn oyunlar üzərindən aldatma. Yeniyetmələrlə oyun platformalarında tanışlıq qurulur, sonra "offline görüş" təklifləri verilir.

Kriptovalyuta ilə ödənişlər. Əvvəllər "Western Union" kimi vasitələrlə həyata keçirilən əməliyyatlar indi kriptovalyuta üzərindən aparılır, bu da izlənməni çətinləşdirir.

Bu yeni taktikalar hüquq-mühafizə və sosial işçilərin təlim proqramlarına daxil edilməlidir.

Yenilənmənin zəruriliyinə dair misal. Avropa ölkələrində aparılan tədqiqatlar göstərib ki, insan alveri ilə məşğul olan qruplar "job abroad" ifadəsini izləmədən yayınmaq üçün sadəcə emoji (✈️ 💼) ilə əvəz ediblər. Əgər monitorinq sistemi yalnız klassik açar sözlərə fokuslansaydı, bu elanların aşkarlanması mümkün olmayacaqdı. Eyni risk Azərbaycanda da mövcuddur: "otel işi" kimi ifadələr getdikcə "iaşə və xidmət sektorunda fürsət" və ya "səyahət paketi" terminləri ilə əvəz olunur.

Akademik baxış. Casey qeyd edir ki, rəqəmsal sübutların effektiv istifadəsi yalnız onların aktual saxlanması ilə mümkündür; köhnəlmiş metodologiya hüquqi nəticələrin də zəifləməsinə gətirib çıxarır. Zimmerman və Kiss isə göstərirlər ki, qurban yönümlü yanaşma yalnız real risklərə adaptasiya edildikdə effektiv olur. Bu da daimi yeniləmələri etik öhdəlik kimi müəyyənləşdirir.

Nəticə. Açar sözlər, platformalar və taktikalar daim dəyişdiyinə görə mübarizə mexanizmlərinin yenilənməsi sadəcə texniki ehtiyac deyil, həm də hüquqi və etik öhdəlikdir. Yalnız dinamik və adaptiv yanaşma qurbanların vaxtında müdafiəsini təmin edə, cinayətkar şəbəkələrin yeni üsullarına qarşı dayanıqlı sistem qura bilər. Beynəlxalq sənədlər – Palermo Protokolu (2000), Avropa Şurası Konvensiyası və ATƏT tövsiyyələri, adaptasiyanı dövlətlərin öhdəliyi kimi göstərir.

Rəqəmsal insan alveri ilə mübarizədə açar sözlərin, platformaların və cinayətkar taktikasının tez-tez dəyişməsi səbəbindən tətbiq edilən təlimatların və monitorinq alətlərinin daim yenilənməsi həyati əhəmiyyət kəsb edir. Bunun üçün praktik yanaşmalar aşağıdakı kimi tövsiyə olunur:

1. **Açar söz bazasının yenilənməsi.**

✓ Hər ay yeni terminlər, şifrəli ifadələr və emojilərlə

kodlaşdırılmış işarələr izlənilməli, monitorinq sistemlərinə əlavə edilməlidir.

✓ Məsələn, "job abroad" ifadəsinin ✈️💼 emojilərlə əvəz olunması halları avtomatik filtrlərə daxil edilməlidir.

2. **Yeni platformaların izlənməsi.**

✓ Ənənəvi elan saytları ilə yanaşı, TikTok, Telegram, Discord və WhatsApp status bölmələri kimi daha az nəzərə çarpan məkanlarda monitorinq aparılmalıdır.

✓ QHT və polis əməkdaşları üçün "platforma xəritəsi" hazırlanaraq hansı sosial media kanallarının mütəmadi izlənəcəyi dəqiqləşdirilməlidir.

3. **Taktikaların adaptiv izlənməsi.**

✓ Cinayətkar qrupların sosial media influencerləri, oyun platformaları və kriptovalyuta ilə ödənişlərdən istifadəsi halları ayrıca izləmə mexanizmlərinə daxil edilməlidir.

✓ Təlimlərdə bu yeni metodların nümunələri göstərilməli, real iş halları ilə təcrübə aparılmalıdır.

4. **Mütəmadi təlim və təcrübə mübadiləsi.**

✓ Sosial işçilər, polis əməkdaşları və QHT nümayəndələri üçün ən azı ildə bir dəfə təlimlər keçirilməli, yeni açar sözlər və platforma riskləri üzrə praktiki məşğələlər təşkil olunmalıdır.

✓ Beynəlxalq şəbəkələrlə (məsələn, ATƏT, BMqT, La Strada International) məlumat mübadiləsi aparılmalı, qlobal tendensiyalar yerli kontekstə uyğunlaşdırılmalıdır.

5. **Monitorinq və qiymətləndirmə mexanizmi.**

✓ Hər rüb tətbiq olunan açar sözlərin və platforma izləmələrinin effektivliyi qiymətləndirilməli, nəticələr əsasında siyahılar yenilənməlidir.

✓ Effektiv olmayan metodlar çıxarılmalı, yeni göstəricilər əlavə edilməlidir.

Nəticə: Daimi yeniləmələr yalnız texniki zərurət deyil, həm də qurban yönümlü yanaşmanın qorunması üçün etik və hüquqi öhdəlikdir. Əks halda, köhnəlmiş açar sözlər və izləmə metodları qurbanların vaxtında aşkarlanmasına mane olur və cinayətkar

şəbəkələrin üstünlük qazanmasına şərait yaradır[66].

Davamlı yeniləmələr üzrə tədbirlər

Tədbir	Müddət	Məsul qurum
Açar söz bazasının yenilənməsi (yeni terminlər, emojilər, kodlaşdırılmış ifadələr əlavə olunur)	Hər ay	DİN İnsan Alverinə Qarşı Mübarizə Baş İdarəsi, QHT-lər, Media monitorinq mərkəzləri
Yeni platformaların izləmə planına daxil edilməsi (TikTok, Telegram, Discord, WhatsApp status və s.)	Rüblük	Dövlət qurumları (DİN, RİNN), QHT şəbəkələri
Cinayətkarların yeni taktikalarının izlənməsi (influencer profilləri, oyun platformaları, kripto-ödənişlər)	Davamlı, hər rüb yenilənmə	Polis kiberkriminalistika şöbəsi, sosioloji tədqiqat institutları
Sosial işçilər və polis üçün praktiki təlimlərin keçirilməsi (yeni açar sözlər, platformalar, nümunə halları ilə)	İllik (ən azı 1 dəfə)	Əmək və Əhalinin Sosial Müdafiəsi Nazirliyi, QHT-lər, beynəlxalq təşkilatlar (OSCE, IOM)
Monitorinq və qiymətləndirmə (istifadə olunan açar sözlərin və metodların effektivliyinin yoxlanması)	Rüblük hesabatlarla	Dövlət qurumları, Milli İstqiamətləndirmə Mexanizmi üzrə Koordinasiya Şurası
Beynəlxalq təcrübə mübadiləsi və məlumat paylaşımı (ATƏT, La Strada, INTERPOL ilə)	İllik və ya ehtiyac yarandıqda	Xarici İşlər Nazirliyi, DİN, QHT koalisiyaları

[66] Latonero, M. (2011). Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds. USC Annenberg Center.

9.STANDARD ƏMƏLİYYAT PROTOKOLU (SOP)

Mövzu: Rəqəmsal insan alveri iddialarının identifikasiyası, məlum edilməsi və ilkin müdaxilə prosedura

Sənəd kodu: SOP-RA-001

Tərtib edən: _____ |
Təsdiq edən: _____

Yayımlanma tarixi: //_____ | Yenilənmə: illik / hər rüb (seçin)

Tətbiq dairəsi: [QHT/Sığınacaq/DİN və s.] — bütün əməkdaşlar, könüllülər və tərəfdaşlar.

1. Məqsəd

Bu SOP-un məqsədi rəqəmsal mənbələrdən (sosial media, elan saytları, mesajlaşma tətbiqləri, qapalı qruplar) aşkar edilən insan alveri şübhələri ilə bağlı vasvas proseduru (identifikasiya +qeydiyyat +ilkin müdaxilə + eskalasiya + sstiqamətləndirmə + sənədləşmə) təmin etməkdir. Məqsəd qurbanların təhlükəsizliyini prioritetləşdirərək hüquqi və psixososial yardımın operativ təmin edilməsidir.

1. Çərçivə və tətbiq sahəsi

- Bu SOP rəqəmsal mənbələrdə aşkarlanan şübhəli elan, mesaj və ya əlaqə üçün tətbiq olunur.
- Əməliyyat qismi: ilk 0–72 saat üzrə (əvvəlcə 0–2 saat — dərhal müdaxilə; 2–24 saat — ilkin yönləndirmə; 24–72 saat — ilkin sosial/psixoloji/hüquqi dəstək və daha dərin müdaxilə).

3. Anlayışlar

- Rəqəmsal insan alveri şübhəsi: Onlayn elan, DM, qrup paylaşımı və s. vasitəsilə qurban cəlbi, saxta iş təklifləri, vizasız iş və ya şantaj şübhəsi.
- Qurban: Şübhəli fəaliyyətdən təsirlənə bilən şəxs (potensial zərərçəkən).
- İlk müdaxilə: Qurbanın yerinə yetirilə biləcək ilkin təhlükəsizlik tədbirləri və informasiya toplama.

4. Rol və məsuliyyətlər (xülasə)

- İlk məsul şəxs (First Responder): [məsələn, Sosial işçi / Monitoring officer] — ilkin qiymətləndirmə, təhlükəsizlik tədbirlərinin tətbiqi.
- Məlumat və sübutları toplayan əlaqələndirici: [IT/Forensic / hüquq nümayəndəsi] — ekran görüntülərinin saxlanması, metadatanın qeydə alınması.
- Sığınacaq/RIS (Referral & Intake Specialist): — təhlükəsiz sığınacaq/yer təmin etmək, psixososial dəstək təşkil etmək.
- Hüquq-mühafizə əlaqələndiricisi: — polis/prokurorluqla əlaqə, hüquqi eskalasiya.
- Təhlükəsizlik və Məlumat Mühafizəsi məsulu (Data Protection Officer): — şəxsi məlumatların qorunması, məlumat paylaşım protokolları.

(Şəxslərin adlarını və əlaqə nömrələrini SOP-un sonundakı Əlavə-də daxil edin.)

5. Ümumi prinsiplər

1. Qurbanın təhlükəsizliyi birinci prioritetdir.

2. Minimum məlumat prinsipi: yalnız zəruri olan məlumat toplanmalı və paylaşılmalıdır.

3. Razılıq və məlumatlandırma: mümkün olduğu halda qurbanın razılığı alınmalıdır; lakin dərhal təhlükə olduqda hüquq-mühafizə ilə əməkdaşlıq üçün istisnalar tətbiq oluna bilər (yerli qanunlara əsasən).

4. Məxfilik və şifrələmə: bütün kommunikasiya və sənədlər şifrəli kanallarda saxlanmalıdır.

5. Sənədləşdirmə: bütün əməliyyat və qərarlar dəqiq şəkildə qeyd olunmalıdır.

6. Əməliyyat proseduru — addım-addım

A. Aşkar etmə və ilkin qiymətləndirmə (0–2 saat)

1. Aşkarlanma: Rəqəmsal monitorinq aləti, ictimai müraciət və ya əməkdaş bildirimi vasitəsilə şübhəli məzmun aşkarlandıqda:

➢ İlk məsul şəxsə məlumat verilir (ad, vaxt, platforma).

2. İlkin qiymətləndirmə: İlk məsul şəxs aşağıdakıları sürətlə qiymətləndirir və qeyd edir:

➢ Mənbə (URL/ekran görüntüsü / istifadəçi adı).

- Paylaşımın mətni və konteksi (açar sözlər, emojilər).
- Şübhəli şəxsin əlaqə məlumatı (əgər varsa).
- Potensial qurbanın yaşı (mümkünsə) və təhlükə səviyyəsi (yaşıl/sarı/qırmızı).

3. Təhlükəsizlik qərarı: əgər təcili təhlükə (qırmızı) aşkar olunubsa → dərhal eskalasiya (B-bənd). Əgər yoxsa → müşahidə qeydiyyatına alın və 24 saat ərzində daha dərin yoxlama apar.

Qeyd: İlkin qiymətləndirmə forması (Annex A) doldurulmalıdır.

B. Sübutların toplanması və qorunması (0–24 saat)

1. Ekran görüntüləri və metadata: Məlumat və sübutları toplayan əlaqələndirici orijinal postun/e-poçtun/mesajın ekran görüntüsünü alır və metadata (vaxt, URL, istifadəçi ID, post ID) qeydə alır.

2. Saxlama: Sübutlar şifrələnmiş daxili serverə və ya təşkilatın rəqəmsal dəlil lövhəsinə yüklənir; yalnız yetkiləndirilmiş şəxslərə giriş verilir.

3. Zəruri hallarda hüquqi tələb: Əgər platformadan əlavə məlumat tələb olunmalıdırsa, hüquq-mühafizə ilə koordinasiya və platforma ilə rəsmi məlumat sorğusu proseduru işə düşür.

C. İlkin təhlükəsizlik tədbirləri və əlaqə (0–24 saat)

1. Qurbanla əlaqə: Əgər təhlükəsiz şəkildə əlaqə saxlamaq mümkündürsə, ilk məsul şəxs qısa, travmayönümlü və təhlükəsiz ünsiyyət protokollarına uyğun şəkildə əlaqə qurur. Məqsəd: təhlükəsizlik vəziyyətini təsdiqləmək, təcili ehtiyac varsa təmin etmək, razılıq əsasında əlavə məlumat toplamaq.

2. Təhlükəsizlik tövsiyyələri: Qısa praktiki tövsiyələr verilir (məs: əlaqəni kəsmək, ekran görüntüləri saxlamaq, mövcud yer paylaşımını söndürmək).

3. Təcili təhlükə varsa: dərhal polis/sığınacaq/təcili xidmət çağırılır (əlaqə zənciri: Annex B).

Qeyd: Qurbanın razılığı olmadığı halda məlumat paylaşılması yalnız qəti təhlükə və ya qanuni tələb əsasında həyata keçirilə bilər.

D. İstiqamətləndirmə və dəstək (2–72 saat)

1. Sosial/psixoloji müdaxilə: Sığınacaq/RIS təcili dəstək (mülki müdafiə, tibbi yoxlama, psixoloji yardım) təmin edir. İlk 24–

72 saatda təhlükəsiz sığınacaq və ilkin tibbi/psixoloji qiymətləndirmə təşkil edilir.

2. Hüquqi dəstək: Hüquq-mühafizə əlaqələndiricisi qurban üçün hüquqi məsləhət və lazım gəldikdə rəsmi şikayət prosesini aktivləşdirir.

3. Uzunmüddətli plan: Reinteqrasiya, Fərdi Plan hazırlanır (sosial işçi + psixoloq + hüquqi nümayəndə).

E. Hesabat və təsdiq (24–72 saat və sonrası)

1. Əməliyyat hesabatı: İlk 72 saat ərzində Operativ Hesabat (Annex C) hazırlanır və məsul şəxslərə təqdim edilir.

2. Məlumat mübadiləsi: Yalnız razılıq əsasında və ya qanuni tələbə uyğun olaraq partnyorlara məlumat verilir. Hər paylaşma Data Protection Officer tərəfindən təsdiqlənir.

3. Monitorinq: Vəziyyətin davamlı monitorinqi və status yenilikləri 7, 14 və 30-cu günlərdə qeydə alınır.

7. Məlumatın qorunması və etik qaydalar

- Bütün şəxsi məlumatlar GDPR-tipli prinsiplərə uyğun saxlanmalıdır (əgər lokal qanunlar fərqlidirsə, lokal qanunvericiliyə uyğun).
- Məlumat paylaşımı yalnız ehtiyac əsasında və yazılı olaraq icazə ilə.
- Qeydiyyat sistemində hüquqi və etik məlumat (məsələn, mənbə etibarlılığı, razılıq qeydləri) saxlanmalıdır.

8. Təlim və bacarıqlar

- Bütün əməkdaşlar üçün təhlükəsiz ünsiyyət, rəqəmsal izləmə, dəlil qoruma və travma-məlumatlı yanaşma üzrə illik təlim proqramı olmalıdır.
- Xüsusi rol sahibləri (Dəlil Koordinatoru, İlk Məsul) əlavə texniki təlimlərdən keçməlidir (OSINT, digital forensics əsasları).

9. Koordinasiya və partnyorlarla əməkdaşlıq

- Əməkdaşlıq razılaşmaları (MOU) polis, sığınacaqlar, tibbi xidmətlər, beynəlxalq təşkilatlar (BMqT, ATƏT əlaqələri) və sosial media/platforma əlaqələndiriciləri ilə mövcud olmalıdır.
- Əlaqə siyahısı və eskalasiya xəritəsi (Annex B) hər zaman əlçatan olmalıdır.

10. Sənədləşmə və forma əlavələri (Annexlər)

Annex A — İlkin Aşkarlama / İstintaq Formu (qısa doldurulacaq):

- Tarix / Vaxt: _____
- Aşkar edən: _____ (ad, rol)
- Platforma/URL/İstifadəçi adı: _____
- Mətn / Screenshot qeyd: _____
- Potensial qurban identifikasiyası (ad / yaşı / əlaqə – əgər mövcuddursa): _____
- Təhlükə səviyyəsi: [Yaşıl / Sarı / Qırmızı]
- Təsdiqləyən şəxs: _____

Annex B — Eskalasiya və əlaqə siyahısı

- Polis (yerli) — telefon: _____
- Təcili yardım — telefon: _____
- Sığınacaq (yerli) — əlaqə: _____
- İT/sübut toplayan şəxs ya əlaqələndirici — əlaqə: _____
- Məlumatların mühafizəsi üzrə məsul şəxs — əlaqə: _____
- Beynəlxalq partnyor (IOM/OSCE) — əlaqə: _____

Annex C — İlk 72-saat Hesabatı (şablon)

- Hadisənin xülasəsi, görülən tədbirlər, növbəti addımlar, məsul şəxslər.

Annex D — Dəlil Qoruma Qaydası (qısa)

- Ekran görüntülərinin texniki tələbləri, fayl nömrələmə, şifrələmə qaydaları.

11. Nəzarət, qiymətləndirmə və yenilənmə

- SOP-un icrası üzrə aylıq/kvartal hesabatlar hazırlanır.
- Hər 12 ayda və ya böyük texnoloji dəyişiklikdən sonra SOP yenilənir.
- İcra göstəriciləri (KPI): İlk cavab müddəti, təhlükəsiz sığınacaq təmin olunma faizi, hüquqi eskalasiya sayı, məlumat paylaşımı halları.

12. Qanuni və etik məqamlar (xülasə)

- Hər bir addım yerli hüquqa uyğun həyata keçirilməlidir — uşaqlar, məcburi köç, və ya müəyyən qruplar üçün əlavə tədbirlər zəruri ola bilər.
- Qurbanın razılığı və məxfilik hüquqları prioritetdir; lakin vurğulanmalıdır: təcili təhlükə zamanı hüquq-mühafizə ilə

əməkdaşlıq vacib ola bilər.

13. Nümunə axın-sxemi (qısa təsvir)

1. Şübhəli paylaşım aşkarlanır + 2. İlk məsul şəxsə bildiriş + 3. İlkin qiymətləndirmə (0–2 saat) + 4a. Əgər təcilidirsə +dərhal eskalasiya + hüquq-mühafizə + sığınacaq; 4b. Əgər qeyri-təcili + sübut toplanması və müşahidə + 24 saatlıq yoxlama + 5. İstiqamətləndirmə və 72 saatlıq dəstək planı →+6. Hesabat və monitorinq.

Qısa nümunə (praktiki)

Senaryo: Instagramda "Avropada model işi, yaxşı qazanc, DM" şəklində elan aşkarlandı.

- İlk məsul şəxs: elan URL-ni və screenshotu götürür, təhlükə səviyyəsini SARİ yoxlayır.
- Sübut toplayan əlaqələndirici: metadata toplayır və şifrələnmiş serverə yükləyir.
- Sosial işçi: əgər şəxs özünü bildirərsə, təhlükəsizlik məsləhəti verir və sığınacaq seçimlərini müzakirə edir.
- Əgər 17 yaşlı uşaq şübhəsi varsa — dərhal polis və uşaq qorunması orqanı məlumatlandırılır.

Təklif olunan SOP — Cədvəl formatı

Addım / Bölmə	Məqsəd / Təsvir	Praktiki tətbiq / Addımlar	Məsul şəxs / Qurum	Vaxt çərçivəsi	Əlavə sənədlər / qeyd
Sənəd başlığı & meta	SOP-un identifikasiyası və tətbiqi dairəsi	Sənəd kodu, tərtib edən/təsdiq edən, yayım tarixi, tətbiq dairəsi	Təşkilat rəhbərliyi	Nəşr zamanı	SOP-RA-001, tətbiq dairəsi qeyd olunsun
1. Məqsəd	SOP-un məqsədinin qısa təsviri	Rəqəmsal mənbələrdə aşkarlanan insan alveri iddialarının operativ idarəsi	Rəhbərlik	Daimi	Məqsəd bloku sənəddə qeyd edilir
2. Çərçivə, tətbiq	SOP-un nəyi əhatə etdiyi	Hangi hallarda tətbiq olunur; ilkin 0–72 saat	Rəhbərlik, Operativ komanda	Əməliyyat başlanandа	Tətbiq dairəsi daxil edilsin

		əməliyyat mərhələsi			
3. Təriflər	Əsas terminlərin açıqlanması	“Rəqəmsal insan alveri”, “Qurban”, “İlkin müdaxilə” və s.	Rəhbərlik / Hüquq məsləhətçisi	Sənədin ilk versiyasında	Tərif lər bölməsi əlavə olunsun
4. Rol və məsuliyyətlər (xülasə)	Kimin nə iş gördüyünü göstərmək	İlk cavab verən (mütəxəssis), sübutları toplayan əlaqələndirici, RIS, Hüquq əlaqələndiricisi, DPO	Hər rol üçün ad/telefon	SOP qəbul edildikdə	Kontaktlar Annex B-də
5. Ümumi prinsiplər	Əməliyyat prinsipləri (məxfilik, minimum data və s.)	Məxfilik, razılıq, minimum məlumat, şifrələmə tələbləri	Bütün əməkdaşlar, DPO	Daimi	Etika qaydaları daxil edilsin
6.A Aşkar etmə, ilkin qiymətləndirmə	Şübhənin sürətli qiymətləndirilməsi	Aşkar edən + İlk cavab verən (mütəxəssis): URL/screen, kontekst, pot. qurban yaşı, risk səviyyəsi	İlk cavab verən (mütəxəssis) (sosial işçi/monitor)	0–2 saat	İlkin aşkarlama formu — Annex A
6.B **Sübutların** toplanması, qorunması	Sübutların hüquqi cəhətdən qorunması	Ekran görüntüləri, metadata, şifrələnmiş yükləmə, məhdud çıxış	Sübutları toplayan əlaqələndirici / IT	0–24 saat	Annex D — Dəlil qoruma qaydası
6.C İlkin tədbirləri, əlaqə	Qurbanla təhlükəsiz ilk əlaqə	Təhlükəsiz ünsiyyət protokolu, təhlükəsizlik tövsiyələri, razılıq alınması	First Responder / Sosial işçi	0–24 saat	Təhlükəsiz ünsiyyət protokolu (cədvəl)
6.D Yönləndirmə, dəstək	İlkin və davamlı yardımın təşkili	Sığınacaq, tibbi/psixoloji yardım, hüquqi	RIS / Sığınacaq / Hüquq	2–72 saat	Case Plan şablonu

		məsləhət, reintegration plan	əlaqələndiricisi		
6.E Hesabat, təsdiq	Əməliyyatın sənədləşməsi və məlumat mübadiləsi	72 saatlıq Operativ Hesabat, Data Protection təsdiqi ilə paylaşma	Operativ rəhbər / DPO	24–72 saat	Annex C — İlk 72-saat Hesabatı
7. Məlumatın qorunması	Şəxsi məlumatların təhlükəsizliyinin təminatı	GDPR-prinsipləri, şifrələmə, məxfi icazələr, log qeydləri	DPO / IT	Daimi	Məlumat qoruma siyasəti
8. Təlim və bacarıqlar	Personalın hazır olması	İlkin və illik təlimlər: təhlükəsiz ünsiyyət, məhkəmə ekspertizası, travma yönümlü xidmət	HR / Təlim koordinatoru	İlkin və illik	Təlim proqramı və sertifikatlar
9. Koor-dinasiya , partnyor-lar	Xarici tərəfdaşlarla əməkdaşlıq	MOU-lar: polis, sığınacaq, BMqT, ATƏT, platforma əlaqələri	Rəhbərlik / Əlaqə ofisi	SOP qüvvəyə mindikdə	Kontakt və MOU sənədləri
10. Annexlər , formasiyalar	Lazımi formaların siyahısı	Annex A (İlkin form), B (kontaktlar), C (72-saat hesabat), D (dəlil qaydası)	Operativ komanda	Hər hadisədə doldurulur	Annex sənədləri Excel/Word formatında
11. Nəzarət, qiymətləndir mə, yenilənmə	SOP icrasının monitorinqi	Aylıq/kvartal hesabatlar, KPI-lar, illik yeniləmə	Key Performance Officer / Rəhbərlik	Aylıq / İllik	KPI dashboard, yenilənmə qeydləri
12. Qanuni, etik məqamlar	Lokal qanunlara uyğunluq və xüsusi tədbirlər	Uşaq halda dərhal polislə əlaqə, məxfilik istisnaları,	Hüquq məsləhətçisi / DPO	Hadisə əsasında	Hüquqi göstərişlər sənədi

		razılıq qaydaları			
13. Axın-sxem (qısa)	Operativ axın: aşkarlama → qiymətləndirmə → eskalasiya → yönləndirmə → hesabat	Qısa addım-addım axın, eskalasiya nöqtələri və kontaktlar	Operativ rəhbər	Hər hadisə üçün	Axın-sxem PNG/PDF

Faydalı linklər və resurslar (OSCE, IOM, La Strada və s.)

Qurum	Link	Təklif olunan istifadə sahəsi
OSCE (Organization for Security and Co-operation in Europe)	OSCE Anti-Trafficking Portal	Milli yönləndirmə mexanizmi (NRM) üçün praktiki bələdçi, təlim materialları, hüquq-mühafizə orqanları və sosial işçilər üçün metodoloji sənədlər
IOM (International Organization for Migration)	IOM Counter-Trafficking	Miqrant qurbanların reabilitasiyası, reinteqrasiya proqramları, qlobal statistika və sahə hesabatları
La Strada International	La Strada International Network	Qurban dəstəyi, helpline təcrübələri, Avropa üzrə QHT şəbəkələrinin əməkdaşlıq mexanizmləri
UNODC (United Nations Office on Drugs and Crime)	UNODC Human Trafficking	Palermo Protokolu izahları, beynəlxalq qanunvericilik nümunələri, “Global Report on Trafficking in Persons” statistik hesabatları
GRETA (Council of Europe)	Council of Europe – GRETA	Avropa ölkələrinin hesabatlılıq mexanizmləri, qanunvericilik icrası üzrə monitorinq və tövsiyələr
Freedom Network USA	Freedom Network USA	Qurban yönümlü yanaşmalar, ABŞ-da sığınacaq və hüquqi yardım modelləri, təlim resursları
Polaris Project	Polaris Project	ABŞ milli hotline modeli,

		data əsaslı izləmə və risk indikatorları, qurban dəstəyi mexanizmləri
ECPAT International	ECPAT International	Uşaqların onlayn istismarının qarşısı, uşaq yönümlü təlim modulları, beynəlxalq kampaniyalar
INTERPOL	INTERPOL Human Trafficking	Sərhədlərarası əməkdaşlıq, əməliyyat resursları, beynəlxalq hüquq-mühafizə orqanlarının koordinasiyası
Europol	Europol Human Trafficking	Avropa İttifaqı çərçivəsində insan alveri cinayətlərinə dair əməliyyat hesabatları, kriminal şəbəkələrin xəritələndirilməsi
ICAT (Inter-Agency Coordination Group against Trafficking in Persons)	ICAT Platform	BMT agentliklərinin birgə sənədləri, siyasət tövsiyələri, qlobal koordinasiya mexanizmləri
UNICEF	UNICEF Child Protection	Uşaq alveri və istismarı üzrə resurslar, uşaq hüquqlarının müdafiəsinə dair metodik tövsiyələr
ILO (International Labour Organization)	ILO Forced Labour and Trafficking	Məcburi əmək və əmək istismarı üzrə hesabatlar, əmək hüquqlarının qorunmasına dair beynəlxalq standartlar
Walk Free Foundation	Global Slavery Index	Qlobal miqyasda insan alveri və müasir köləlik statistikasının izlənməsi
Regional: Azərbaycan Respublikası DİN – İnsan Alverinə qarşı Baş İdarə	Official MIA Page	Milli hotline, qurbanların identifikasiyası, dövlətin illik hesabatları

Regional: Ailə, Qadın və Uşaq Problemləri üzrə Dövlət Komitəsi	aqupdk.gov.az	Həssas qruplarla sosial müdafiə proqramları, qadın və uşaq hüquqlarının qorunması üzrə sənədlər
Regional: QHT Koalisiyası (Azərbaycan)	—	İctimai monitorinq hesabatları, yerli səviyyədə təlim materialları, sosial iş təcrübələrinin paylaşımı

10. Əlavələr

Rəqəmsal mühitdə insan alverinin qarşısının alınmasında açar sözlərin izlənməsi mühüm alətlərdən biridir. İnsan alverçiləri çox vaxt sosial media platformalarından, elan saytlarından və mesajlaşma proqramlarından istifadə edərək qurban axtarır. Bu səbəbdən, açar sözlərin sistemli şəkildə toplanması və təhlili metodik vəsaitdə xüsusi yer tutmalıdır.

İlk növbədə açar sözlər tematik kateqoriyalara ayrılmalıdır. Məsələn, iş təklifi ilə bağlı sözlər (“job offer”, “work abroad”, “seasonal work”), modelləşmə və əyləncə sahəsinə aid ifadələr (“model agency”, “casting”), miqrasiya və sənədləşməyə dair terminlər (“cheap visa”, “sponsor abroad”) və onlayn münasibətlərdə istifadə olunan riskli açar sözlər (“sugar daddy”, “romance chat”, “private photos”). Bu təsnifat izləmə işini asanlaşdırır və diqqəti riskli məzmunlara yönəldir.

İnsan alverçilərinin istifadə etdiyi açar sözlər çox vaxt şifrələnmiş və ya qeyri-rəsmi formada olur. Belə ki, emojilər (“✈️💃” – xaricdə rəqs işi), qısaltmalar (“PT” – private time), jarqon ifadələr və ya qarışıq dillərdə yazılışlar (“rabota devushek”, “iş qızlar üçün”) tez-tez rast gəlinir. Bu, izləmə prosesində yalnız açıq mətnlərlə kifayətlənməməyi, həmçinin kodlaşdırılmış işarələri nəzərə almağı tələb edir.

Platformalara görə də açar sözlərin istifadəsi fərqlidir. Məsələn, Facebook və Instagram-da #jobabroad və #modellife kimi hashtaglar və “DM for details” kimi qısa çağırışlar, Telegram və WhatsApp qruplarında “VIP club” və “private services” kimi örtülü adlar, TikTok-da isə qısa video təsvirlərində “opportunity abroad” kimi ifadələr daha çox istifadə olunur.

Açar sözlərin kombinasiyalarda izlənməsi də əhəmiyyətlidir. Tək bir söz çox zaman qeyri-dəqiq nəticə verir, lakin “job offer” + “free visa” və ya “model” + “Europe” + “quick money” kimi birləşmələr riskli məzmunu daha dəqiq aşkarlamağa kömək edir.

Açar sözlərin yanında onların risk səviyyəsi də qeyd olunmalıdır. Məsələn, “summer job” və “internship” kimi ifadələr aşağı risk, “quick money abroad” orta risk, “young girls for work”

isə yüksək risk siqnalı sayılmalıdır. Bu yanaşma sosial işçilərin və hüquq-mühafizə əməkdaşlarının prioritetləri düzgün müəyyən etməsinə yardım edir.

Sonda xüsusi olaraq vurğulanmalıdır ki, açar sözlər siyahısı daim yenilənməlidir. Sosial şəbəkələr dəyişdikcə, yeni platformalar yarandıqca (məsələn, Threads, OnlyFans və digərləri) monitorinq də mütəmadi test edilməlidir. Həmçinin, izləmə yalnız ingilis dilində deyil, regionda istifadə olunan dillərdə – Azərbaycan, rus və türk dillərində aparılmalıdır.

Metodik vəsaitdə açar sözlərdən başqa, əlavə edilə biləcək bəzi vacib məqamlar bunlardır:

Vizual elementlər: Təkcə mətn deyil, şəkillər, emojilər və simvollar da "açar söz" funksiyası daşıya bilər.

Geotag və məkan məlumatları: Sosial şəbəkə paylaşımlarında yerləşdirmə (location tag) çox vaxt qurban cəlbi üçün istifadə olunur.

Məxfi qruplar və darkweb: Rəqəmsal mühitdə yalnız açıq paylaşımlar deyil, qapalı forum və darknet platformaları da nəzərə alınmalıdır.

Trend izləmə: Yeni çıxan populyar hashtaglar, internet "slang" və gənclərin istifadə etdiyi qısaltmalar tezliklə alverçilərin də arsenalına daxil ola bilər.

Texnoloji yardım: Sadəcə əl ilə yox, avtomatlaşdırılmış "alert sistemi" qurmaq – yəni müəyyən açar sözlər göründükdə xəbərdarlıq siqnalı alınması.

Kontextual təhlil: Açar sözlər təkbaşına yox, istifadə edildiyi kontekstdə qiymətləndirilməlidir. Məsələn, "visa" sözü normal turizm səhifəsində risk daşımır, amma "free visa for young girls" konteksti yüksək risk yaradır.

11.Açar sözlər siyahısı (AZ/RU/EN)

Kateqoriya	AZ	RU	EN
İş təklifi və məşğulluq	iş təklifi, xaricdə iş, sezonlu iş, tez pul qazanmaq	работа за границей, работа для девушек, быстрые деньги, срочно работа	job abroad, work offer, seasonal work, quick money
Modelləşmə və əyləncə	model agentliyi, casting, rəqqasə işi, şou-biznes işi	модельное агентство, кастинг, работа танцовщицей, ночной клуб	model agency, casting call, dancer job, night club work
Migrasiya və sənədləşmə	vizasız iş, sponsor viza, ucuz viza, xaricdə təhsil + iş	дешевая виза, рабочая виза, спонсорская виза, оформление документов	cheap visa, free visa, sponsor visa, work permit
Onlayn münasibətlər və şantaj	sponsor kişi, şəkillərini paylaş, gizli görüş, sugar daddy	содержанка, личные фото, договоримся, папик	sugar daddy, private photos, romance chat, pay for pics
Seksual istismar və gizli xidmətlər	xüsusi xidmətlər, escort, VIP klub, massaj qızları	эскорт, девушки для работы, VIP услуги, ночные услуги	escort, private services, young girls for work, VIP club
Kodlaşdırılmış işarələr və emojilər	✈️💃 (xaricdə rəqs işi), 💵🔥 (tez pul),	✈️💃, 💵🔥, 🌍🛂, 📸😉, PT, GFE	✈️💃, 💵🔥, 🌍🛂, 📸😉, PT,

	🌎🛂 (xaricə getmək), 📸😉 (şəkil paylaş), PT, GFE		GFE, PSE

Siyahı mütəmadi yenilənməlidir, çünki alverçilər yeni şifrələr və emojilərdən istifadə etməyə başlayırlar. Hər açar söz kontekstə görə qiymətləndirilməlidir. Məsələn, “visa” sözü turizm mövzusunda normal ola bilər, amma “free visa for girls” risklidir. Region dillərində (azərbaycanca, rusca, türkcə) paralel izləmə aparmaq vacibdir.

12.Böyl formulları (praktiki istifadə üçün)

İş təklifi və məşğulluq

("job abroad" OR "work abroad" OR "seasonal work" OR "quick money")

OR ("iş təklifi" OR "xaricdə iş" OR "sezonlu iş" OR "tez pul qazanmaq")

OR ("работа за границей" OR "работа для девушек" OR "быстрые деньги" OR "срочно работа")

Modelləşdirmə və əyləncə

("model agency" OR "casting call" OR "dancer job" OR "night club work")

OR ("model agentliyi" OR "casting" OR "rəqqasə işi" OR "şou-biznes işi")

OR ("модельное агентство" OR "кастинг" OR "работа танцовщицей" OR "ночной клуб")

Migrasiya və sənədləşmə

("cheap visa" OR "free visa" OR "sponsor visa" OR "work permit")

OR ("vizasız iş" OR "sponsor viza" OR "ucuz viza" OR "xaricdə təhsil + iş")

OR ("дешевая виза" OR "рабочая виза" OR "спонсорская виза" OR "оформление документов")

Onlayn münasibətlər və şantaj (grooming / sextortion)

("sugar daddy" OR "private photos" OR "romance chat" OR "pay for pics")

OR ("sponsor kişi" OR "şəkillərini paylaş" OR "gizli görüş")

OR ("содержанка" OR "личные фото" OR "договоримся" OR "папик")

Seksual istismar və gizli xidmətlər

("escort" OR "private services" OR "young girls for work" OR "VIP club")

OR ("xüsusi xidmətlər" OR "massaj qızları" OR "VIP klub")

OR ("эскорт" OR "девушки для работы" OR "VIP услуги" OR "ночные услуги")

Kodlaşdırılmış işarələr və emojilər

Emojilər Böyl qaydaları ilə birbaşa işləməyə bilər, amma bəzi OSINT alətləri və sosial media axtarışları onları dəstəkləyir.

("✈️ 💃" OR "💵 🔥" OR "🌍 🛂" OR "📸 😉" OR "PT" OR "GFE" OR "PSE")

Praktiki istifadə qaydaları

Platformaya uyğunlaşdırma:

✓ Twitter/X → ("job abroad") lang:en

✓ Instagram → #jobabroad OR #modellife

✓ Telegram → qrup axtarışında yalnız sözləri OR ilə yazmaq daha effektlidir.

Kombinasiya: Yüksək riskli nəticə üçün sözləri AND ilə birləşdirmək:

("job offer" AND "free visa")

("model" AND "Europe" AND "quick money")

İstisna (NOT): Təhlükəsiz nəticələri ayırmaq üçün:

("visa" AND "work") NOT "tourism"

Təhlükəsiz ünsiyyət Protokolu – Cədvəl

Addım	Təhlükəsizlik tədbiri	Praktiki tətbiq	Məsul qurum/şəxs
1. Prinsiplərin müəyyənləşdirilməsi	Məxfilik, etibar, zərər verməmək, hüquqi uyğunluq prinsiplərinin yazılı təsbiti	Hər əməkdaş ilkin təlimdə bu prinsiplərlə tanış olur və imza ilə öhdəlik götürür	QHT rəhbərliyi, dövlət qurumlarının əlaqələndiriciləri
2. Əlaqə kanallarının seçilməsi	Təhlükəsiz ünsiyyət vasitələrinin	Üzbəüz görüş → təhlükəsiz məkan; Telefon/video →	Sosial işçi, psixoloq, hüquqi

	müəyyən edilməsi	şifrəli xətt; Yazılı → Signal, ProtonMail	nümayəndə
3. Identifikasiya və doğrulama	Qurban və əməkdaşın kimliyinin təsdiqi	"Giriş sualları" və ya kodlaşdırılmış ifadələr; razılaşdırılmış emoji/sözlə təhlükə siqnalı	Sosial işçi, hüquq-mühafizə əməkdaşı
4. Məlumat mübadiləsinin qorunması	Minimum məlumat prinsipi, şifrələmə və məxfilik səviyyələri	Yalnız zəruri məlumat toplanır; sənədlər şifrəli sistemdə saxlanılır; kağız daşıyıcılar kilidli yerdə qorunur	Sosial işçi, sığınacaq rəhbərliyi, IT təhlükəsizlik mütəxəssisi
5. Böhran vəziyyəti planı	Təhlükə yaranarsa dərhal eskalasiya	"SOS kodu" razılaşdırılır; ünsiyyət kəsilir və hüquq-mühafizə/sığınacaq/ təcili yardım işə cəlb olunur	Sosial işçi, polis, təcili yardım xidməti
6. Davamlı monitorinq və yenilənmə	Protokolun mütəmadi qiymətləndirilməsi və təkmilləşdirilməsi	Hər il yenilənmə; yeni texnologiyalar (AI, deepfake) nəzərə alınır; mütəmadi təlimlər keçirilir	Dövlət qurumları, QHT Koalisiyası, beynəlxalq tərəfdaşlar

Təhlükəsiz Ünsiyyət Protokolu aşağıdakı bölmələri əhatə etməlidir:

1. Giriş və məqsəd
2. Prinsiplər (məxfilik, hüquq, zərər verməmək)
3. Təhlükəsiz kanallar siyahısı
4. Identifikasiya və doğrulama prosedurları
5. Məlumatın qorunması və paylaşım qaydaları
6. Krizis vəziyyəti planı
7. Yenilənmə və monitorinq mexanizmləri

Böhran planı – Cədvəl

Addım	Təhlükəsizlik tədbiri	Praktiki tətbiq
1. Siqnal	Əvvəlcədən razılaşdırılmış kod/emoji ilə təhlükə barədə xəbərdarlıq	Qurban "SOS sözü" və ya xüsusi emoji istifadə edir
2. Dayandırma	Ünsiyyət dərhal kəsilir və əlavə sual verilmir	Telefon söhbəti bitirilir, yazışma dondurulur
3. Eskalasiya	Dərhal müvafiq qurumlara məlumat verilir	Polis (102), təcili yardım (112), sığınacaq əlaqələndiricisi işə cəlb olunur
4. Təhlükəsiz yönləndirmə	Qurban təhlükəsiz məkana çıxarılır	Sığınacaq, təhlükəsiz ev və ya gizli görüş nöqtəsi
5. Sənədləşdirmə	Hadisə qeydə alınır və hesabat hazırlanır	Tarix, vaxt, istifadə olunan siqnal, görülən tədbirlər qeyd edilir

Bu plan sosial işçilər, hüquq-mühafizə əməkdaşları və sığınacaq personalı üçün standart əməliyyat protokolu (SOP) rolunu oynayır.

3.YEKUN

İnsan alveri ilə mübarizədə rəqəmsal mühitin izlənməsi çağdaş dövrün qaçılmaz zərurətinə çevrilmişdir. Cinayətkar şəbəkələrin fəaliyyətində internet platformaları, sosial media və qapalı onlayn qruplar getdikcə daha geniş rol oynayır. İş elanları, saxta vizalar, modelləşmə təklifləri, onlayn münasibətlər və şantaj üsulları vasitəsilə qurban cəlbi yeni ölçülərə çıxarılır. Bu səbəbdən, insan alverinə qarşı mübarizədə açar sözlərin, emojilərin, kodlaşdırılmış işarələrin və onlayn platformalarda risk indikatorlarının izlənməsi xüsusi əhəmiyyət kəsb edir.

Hazırlanmış metodik vəsaitin əsas əhəmiyyəti ondan ibarətdir ki, o, yalnız nəzəri çərçivəni deyil, həm də praktiki tətbiq vasitələrini təqdim edir. Açar sözlər siyahısı, Böyl formulları, risk səviyyəsinə görə təsnifat və beynəlxalq resurslara istinadlar mütəxəssislərə rəqəmsal məkanın kompleks izlənməsində sistemli yanaşma imkanı yaradır. Bununla yanaşı, sənəd beynəlxalq təcrübəni (ATƏT, BMqT, La Strada, UNODC, GRETA və s.) yerli kontekstlə birləşdirərək universal və milli səviyyədə istifadə edilə biləcək çərçivə təqdim edir.

Metodik vəsaitin unikallığı bir neçə istiqamətdə özünü göstərir:

- Çoxsəviyyəli istifadə: sosial işçilər, hüquq-mühafizə orqanları və QHT-lər üçün eyni zamanda faydalı ola biləcək təlimat xarakteri;
- Praktiki yönümlülük: nəzəri anlayışların yanında əməli alətlərin təqdim olunması;
- Davamlılıq və yenilənmə prinsipi: rəqəmsal mühitin sürətli transformasiyasına uyğun olaraq açar sözlərin, platformaların və taktikanın mütəmadi yenilənməsinin zərurəti;
- Qlobal və lokal sintez: beynəlxalq standartların Azərbaycan reallığına uyğunlaşdırılması.

Siyasət tövsiyyələri

1. Milli strategiyaya inteqrasiya: İnsan alverinə qarşı 2025–2030-cu illər üzrə milli fəaliyyət planına rəqəmsal monitorinq bölməsi daxil edilməlidir.

2. İnstitusional gücləndirmə: Sosial işçilər, hüquq-mühafizə və QHT-lər üçün birgə rəqəmsal monitorinq mexanizmi yaradılmalıdır.

3. Təlim və resurslar: Açıq və kodlaşdırılmış açar sözlərin izlənməsi üzrə praktiki təlimatlar və tədris modulları hazırlanmalıdır.

4. Texnoloji əməkdaşlıq: Sosial media şirkətləri ilə MOU-lar bağlanaraq, riskli açar sözlərin avtomatik aşkar edilməsi üçün məlumat mübadiləsi təmin edilməlidir.

5. Daimi yenilənmə: Açar sözlər və risk indikatorları trendlərə uyğun hər rüb yenilənməli, beynəlxalq şəbəkələrlə (ATƏT, La Strada, GRETA) mütəmadi koordinasiya aparılmalıdır.

Nəticə etibarilə, bu metodik vəsait rəqəmsal mühitdə insan alveri ilə mübarizənin erkən xəbərdarlıq və risk identifikasiyası komponentini gücləndirir. Təqdim olunan yanaşmalar yalnız monitorinq mexanizmi deyil, həm də qurbanların vaxtında müdafiəsi üçün təhlükəsizlik çərçivəsi kimi nəzərdə tutulur.

Beləliklə, sənəd insan alveri ilə mübarizə üzrə milli və beynəlxalq siyasətlərdə rəqəmsal müstəvinin nəzərə alınmasının vacibliyini vurğulayan, praktik tətbiqi olan və gələcəkdə strateji planlaşdırma üçün baza yaradan unikal mənbədir.

ANLAYIŞLAR:

1. rekrutment (cəlb etmə)
2. means (məcburetmə üsulları)
3. purpose (istismar məqsədi)
4. sentiment analysis (emosional təhlil)
5. reverse image search (şəkil əsasında axtarış
6. Böyl (məntiqi axtarış)
7. Regex (Müntəzəm ifadə)– mətnlərdə müəyyən nümunələri (pattern) tapmaq, axtarmaq və ya dəyişdirmək üçün istifadə edilən formal dildir.

Sadə Regex nümunələri

Regex	İzah	Praktik nümunə
\d	Bir ədəd rəqəmi tapır	"Ev 25 nömrədir" → 2, 5
\d+	Bir və ya bir neçə ardıcıl rəqəmi tapır	"Ev 25 nömrədir" → 25
\w	Bir hərf və ya rəqəmi tapır (a–z, A–Z, 0–9, _)	"Salam_123" → S, a, l, …, 3
\w+	Bir və ya bir neçə hərf/rəqəm ardıcıllığını tapır	"Salam_123" → Salam_123
\s	Bir boşluq simvolunu tapır	"Salam Dünya" → (boşluq)
^abc	abc ilə başlayan sətrləri tapır	"abc kitab" → uyğun gəlir
abc$	abc ilə bitən sətrləri tapır	"kitab abc" → uyğun gəlir
.	İstənilən bir simvolu tapır (yeni sətrdən başqa)	"a1b" → a, 1, b

Daha mürəkkəb Regex nümunələri

Regex	İzah	Praktik nümunə
^[A-Z][a-z]+$	Böyük hərflə başlayan, ardınca kiçik hərflərdən ibarət söz	"Ali", "Nigar" uyğun gəlir, amma "ali" gəlmir
\b\d{4}\b	4 rəqəmdən ibarət söz (məsələn, il)	"1991-ci il" → 1991
`(+994	0)(50	51
`\b[A-Za-z0-9._%+-]+ @[A-Za-z0-9.-]+.[A-Z	a-z]{2,}\b`	E-poçt ünvanı
<([A-Za-z][A-Za-z0-9]*)\b[^>]*>(.*?)</\1>	HTML etiketlərini tapmaq (başlanğıc və bitiş uyğun olmalıdır)	Salam
(?=.*[A-Z])(?=.*[a-z])(?=.*\d)(?=.*[@$!%*?&]) [A-Za-z\d@$!%*?&]{8,}	Güclü şifrə (ən azı 8 simvol, böyük hərf, kiçik hərf, rəqəm və xüsusi işarə olmalıdır)	"Test123!" uyğun gəlir
`(\d{2})/(0[1-9]	1[0-2])/\d{4}`	Tarix (dd/mm/yyyy formatında)
Regex	İzah	Praktik nümunə
^[A-Z][a-z]+$	Böyük hərflə başlayan, ardınca kiçik hərflərdən ibarət söz	"Ali", "Nigar" uyğun gəlir, amma "ali" gəlmir
\b\d{4}\b	4 rəqəmdən ibarət söz (məsələn, il)	"1991-ci il" → 1991

–pattern detection- (nümunə aşkarlanması”)

–triage- (“təsnifat”, “seçim”)

–MOU (Anlaşma Memorandumu)

–data-sharing protocols (Məlumat mübadiləsi Protokolları)

–Cybersex trafficking” (Kiber-seks alveri)

–big data (çox böyük həcmli)

–UNODC (BMT-nin Narkotik və Cinayətkarlıq üzrə İdarəsi)

–grooming (cəlbetmə və manipulyasiya prosesi)

–reporting tools (Hesabat alətləri)

–Reverse image search (Şəkl əsasında axtarış)

–Blokçeyn – məlumatların paylanmış (distribütiv) və dəyişdirilməsi çətin olan ardıcıl bloklarda saxlandığı rəqəmsal texnologiyadır. (bloklar zənciri)

–simple keyword search (Sadə açar söz axtarışı)

–online recruitment (rəqəmsal cəlbetmə)

–irrelevant (mövzuya aid olmayan)

–Scopus, (Elsevier nəşriyyatına məxsus, dünyada ən böyük elmi bibliometrik baza və indeksasiya sistemidir)

–Web of Science” (Elmi İstinadlar Şəbəkəsi)

–ProQuest (ProQuest elektron məlumat bazası”dünyanın ən böyük rəqəmsal məlumat və akademik resurs bazalarından biridir.)

–traffick → trafficking, trafficker (insan alveri, insan alverçisi)

–wildcard (əvəzedici simvol)

–Böyl axtarış (Bul məntiqi – yalnız iki mümkün nəticəni (məsələn: doğru / yalnış, 1 / 0, var / yoxdur) ifadə edən məntiqi sistemdir.)

–Rekrutment (cəlbetmə)

–pattern recognition (Nümunələrin tanınması)

–Click-to-Chat linki (Çata keçid linki, məsələn WhatsApp-da https://wa.me/994501234567 → istifadəçi bu linkə klikləyir və dərhal yazışma pəncərəsi açılır.)

–burner patterni (müvəqqəti istifadə nümunəsi”)

–Sponsor fee (sponsor ödənişi)

–Timestamp (vaxt göstəricisi)

–Reverse phone lookup (nömrənin sahibini müəyyənləş-dirmə)

–keyword scrapers (Açar söz toplayıcıları) Named Entity Recognition (Xüsusi adların tanınması)

–Extract (Çıxarmaq)

–Cross-check (təkrar yoxlama)

–Sophistication (peşəkarlıq)

–Au-pair (xarici ölkədə ailə yanında qalaraq uşaqlara baxmaq və ya ev işlərinə kömək etmək müqabilində dil öyrənən və mədəni təcrübə qazanan gənc)

–Geotag (lokasiya etiketi)

–free visa (Pulsuz viza)

–erotic massage (Erotik masaj)

–challenge (Çağırış)

–end-to-end (əhatəli)

–chain of custody (zəncirvari izləmə)

–Craigslist ABŞ-da yaradılmış və hazırda bir çox ölkədə fəaliyyət göstərən məşhur onlayn elan platformasıdır.

–hospitality opportunity (iaşə və xidmət sektorunda fürsət)

–Travel package (Səyahət paketi- turizm şirkətlərinin təklif etdiyi, bir neçə xidmətin (aviabilet, otel, transfer, bələdçi, ekskursiyalar və s.) bir yerdə satıldığı paketdir.)

–quick money (asan qazanc)

–RIS (Reinteqrasiya və İnteqrasiya Sistemi)

–Data Protection Officer (DPO) (Məlumatların Mühafizəsi üzrə məsul şəxs)

–First Responder (ilkin qiymətləndirmə aparan mütəxəssis)

QEYDLƏR

Nəşriyyatın Baş direktoru:
Səməd Eyvazov

Texniki redaktor:
Mail Xəlilov

Kağız formatı:60x84 $_1$ /^{16}
Tiraj: 100 ədəd
Həcmi: 11 çap vərəqi

“OPTİMİST” MMC-də hazır diopozitivlərdən çap olunub