ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БАС ПРОКУРАТУРАСЫНЫҢ
ЖАНЫНДАҒЫ ҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫ АКАДЕМИЯСЫ

ЖОҒАРЫ ОҚУ ОРНЫНАН КЕЙІНГІ БІЛІМ БЕРУ ИНСТИТУТЫ

АМАНОВА ҰЛЗИРА ҒАНИҚЫЗЫ

«Кибергрумминг» қылмыстарын тергеп-тексерудің теориялық және практикалық проблемалары

7М12301 «Құқық қорғау қызметі» (бейінді бағыт) білім беру бағдарламасы бойынша ұлттық қауіпсіздік және әскери іс магистрі дәрежесін алуға жоба

Ғылыми жетекші:
арнайы заң пәндері
кафедрасының меңгерушісі
А.А. Ешназаров**,**
заң ғылымдарының кандидаты,
аға әділет кеңесшісі
_____

Қосшы қ., 2025 ж.

ТҮЙІНДЕМЕ

Зерттеу жобасы кибергрумингке қарсы күрестің құқықтық және практикалық мәселелерін кешенді талдауға арналған. Онда кибергруминг ұғымының мәні, құрылымдық белгілері, қылмыстық-құқықтық және криминологиялық аспектілері қарастырылды.Ұлттық заңнамадағы арнайы құрамның болмауы, цифрлық дәлелдемелерді жинау мен бағалаудың ерекшеліктері, кәмелетке толмаған жәбірленушілермен жұмыстың психологиялық-процессуалдық қырлары талданды. Зерттеу нәтижесінде қылмыстық заңнамаға жаңа құрам енгізу, цифрлық дәлелдемелерді рәсімдеу тәртібін нақтылау, балаларға қатысты тергеу әрекеттерін бейімдеу бойынша ұсыныстар әзірленді. Сонымен қатар, Қазақстанның Будапешт және Ланзароте конвенцияларына қосылуы негізделді.

РЕЗЮМЕ

Диссертационный проект посвящена комплексному анализу правовых и практических проблем противодействия кибергрумингу. Рассмотрены сущность понятия кибергруминга, его структурные признаки, уголовно-правовые и криминологические аспекты. Проанализированы трудности квалификации в рамках национального законодательства, отсутствие специального состава в Уголовном кодексе, особенности сбора и оценки цифровых доказательств, а также психологические и процессуальные особенности работы с несовершеннолетними потерпевшими. По результатам исследования обоснованы предложения по введению нового состава преступления в уголовное законодательство, уточнению порядка оформления цифровых доказательств, адаптации следственных действий в отношении детей. Также обоснована необходимость присоединения Казахстана к Будапештской и Ланзаротской конвенциям.

SUMMARY

This dissertation project a comprehensive analysis of the legal and practical issues in combating cyber grooming. It examines the concept of cyber grooming, its structural elements, as well as its criminal-legal and criminological aspects. The study analyzes the challenges of qualification within national legislation, the absence of a specific offense in the Criminal Code, the peculiarities of collecting and evaluating digital evidence, and the psychological and procedural specifics of working with minor victims. Based on the research results, proposals have been substantiated for introducing a new criminal offense into legislation, clarifying procedures for handling digital evidence, and adapting investigative actions involving children. The necessity for Kazakhstan to join the Budapest and Lanzarote Conventions has also been justified.

МАЗМҰНЫ

НОРМАТИВТІК СІЛТЕМЕЛЕР

Осы жобада мынандай стандарттарға сілтемелер пайдаланылған:

1. Қазақстан Республикасының Конституциясы - 1995 жылғы 30 тамызда республикалық референдумда қабылданған.
2. Қазақстан Республикасының Қылмыстық кодексі - 2014 жылғы 3 шілдедегі № 226-V ҚРЗ.
3. Қазақстан Республикасының Қылмыстық-процестуалдық кодексі - 2014 жылғы 4 шілдедегі № 231-V ҚРЗ.
4. Қазақстан Республикасының "Баланың құқықтары туралы" заңы - 2002 жылғы 8 тамыздағы № 345.
5. Қазақстан Республикасының "Ақпараттандыру туралы" заңы - 2015 жылғы 24 қарашадағы № 418-V ҚРЗ.
6. Қазақстан Республикасының "Жеке деректер және оларды қорғау туралы" заңы - 2013 жылғы 21 мамырдағы № 94-V.
7. Қазақстан Республикасының "Халықаралық шарттар туралы" заңы - 2005 жылғы 30 мамырдағы № 54-III.
8. Еуропа Кеңесінің Будапешт конвенциясы (Киберқылмыс туралы конвенция) - 2001 жылғы 23 қараша.
9. Еуропа Кеңесінің Ланзароте конвенциясы (Балаларды жыныстық қанаудан және жыныстық зорлықтан қорғау туралы конвенция) - 2007 жылғы 25 қазан.
10. Біріккен Ұлттар Ұйымының Баланың құқықтары туралы конвенциясы - 1989 жылғы 20 қараша (Қазақстан Республикасы 1994 жылы ратификациялады).
11. БҰҰ-ның Киберқылмысқа қарсы конвенциясының жобасы - 2024 жылғы БҰҰ Бас Ассамблеясы қабылдаған (жоба жағдайында қолданылады).
12. ҚР Ішкі істер министрлігінің «Киберқылмысқа қарсы күрес тұжырымдамасы» - 2022-2025 жылдарға арналған (ведомстволық құжат).

АНЫҚТАМАЛАР

Осы жобада сәйкесінше анықтамалары бар келесі терминдер қолданылған:

1. Кибергруминг - кәмелетке толмаған тұлғамен интернет немесе өзге де электрондық коммуникация құралдары арқылы жыныстық мақсатта байланыс орнату, оның сеніміне кіру, манипуляция жасау және жыныстық сипаттағы әрекеттерге итермелеу процесі.

2. Кәмелетке толмаған - он сегіз жасқа толмаған тұлға (ҚР Азаматтық кодексі, 17-бап).

3. Сандық (электрондық) дәлелдеме - қылмыстық істі тергеу мен сотта қарау барысында маңызы бар және электрондық (сандық) форматта сақталған, арнайы техникалық құралдармен алынған ақпарат (хат-хабарлар, файлдар, логтар, IP-адрестер, метадеректер және т.б.).

4. Жыныстық ниет - тұлғаның басқа адамға қатысты жыныстық сипаттағы әрекеттер жасауға бағытталған ішкі мотиві немесе мақсаты.

5. Виртуалды орта (цифрлық орта) - ақпараттық-коммуникациялық технологияларды қолдану арқылы әрекет ететін және пайдаланушылардың интернетте өзара байланысуына мүмкіндік беретін кеңістік.

6. Латентті қылмыс - ресми тіркелмеген немесе жәбірленушінің, куәгерлердің, қоғамның хабарламауына байланысты жасырын күйде қалған қылмыстық әрекет.

7. Психолингвистикалық сараптама - мәтіндер мен сөйлесулердің мазмұнын, құрылымын және астарын саралау арқылы қылмыстық ниетті, агрессия немесе манипуляция элементтерін анықтайтын сараптамалық зерттеу түрі.

8. Будапешт конвенциясы - Еуропа Кеңесінің 2001 жылғы Киберқылмыс туралы конвенциясы, мемлекеттер арасындағы киберқылмыстармен күрес бойынша құқықтық көмек көрсету мен дәлелдемелермен алмасу тәртібін белгілейді.

9. Ланзароте конвенциясы - Еуропа Кеңесінің 2007 жылғы балаларды жыныстық қанаудан және жыныстық зорлық-зомбылықтан қорғау туралы конвенциясы.

10. Анонимизация - интернет пайдаланушысының шынайы жеке басын, орналасқан орнын немесе құрылғысын жасыруға бағытталған техникалық шаралар (VPN, TOR, жалған аккаунттар және т.б.).

БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР

ҚР - Қазақстан Республикасы
ҚК - Қазақстан Республикасының Қылмыстық кодексі
ҚПК - Қазақстан Республикасының Қылмыстық-процестуалдық кодексі
БҰҰ - Біріккен Ұлттар Ұйымы
ЕО - Еуропалық Одақ
ЮНИСЕФ - Біріккен Ұлттар Ұйымының Балалар қоры (UNICEF - United Nations Children’s Fund)
ІІМ - Қазақстан Республикасының Ішкі істер министрлігі
VPN - Виртуалды жеке желі (Virtual Private Network)
IP - Интернет-протокол (Internet Protocol)
AI - Жасанды интеллект (Artificial Intelligence)
TOR - The Onion Router - интернеттегі анонимділікті қамтамасыз ететін жүйе
FBI - Америка Құрама Штаттарының Федералдық тергеу бюросы (Federal Bureau of Investigation)
FTK - Forensic Toolkit - сандық дәлелдемелерді талдауға арналған криминалистикалық бағдарлама
CEOP - Child Exploitation and Online Protection Centre (Ұлыбританиядағы балаларды онлайн қанаудан қорғау орталығы)
HTTPS - Қорғалған гипермәтіндік тасымалдау протоколы (HyperText Transfer Protocol Secure)
ENCASE - Сандық криминалистикада қолданылатын сараптамалық бағдарлама
URL - Бүкіләлемдік желідегі ресурс адресі (Uniform Resource Locator)

КІРІСПЕ

Жүргізілетін зерттеудің өзектілігі. Қазақстан Республикасының Президенті Қасым-Жомарт Кемелұлы Тоқаев киберқылмыспен күрес және ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне ерекше назар аударады. Ол өз баяндамаларында және құқық қорғау органдарына берген тапсырмаларында киберқауіптерге қарсы күресті күшейтудің маңыздылығын бірнеше рет атап өткен. 2024 жылғы 22 қаңтарда Ішкі істер министрлігінің кеңейтілген алқа отырысында Президент қылмысқа қарсы күрестің негізгі міндеттерінің бірі ретінде киберқылмыстарға, оның ішінде интернет-алаяқтық пен кәмелетке толмағандарға қатысты қылмыстарға қарсы әрекеттерді күшейту қажет екенін мәлімдеді. Мемлекет басшысының тапсырмасына сәйкес Қазақстанда Ішкі істер министрлігі жанынан Киберқылмысқа қарсы күрес департаменті құрылды. Бұл құрылымның негізгі міндеттері - киберқылмыстарды анықтау, тергеу және олармен күрес стратегияларын әзірлеу болып табылады.

Қазіргі заманғы цифрлық технологиялардың дамуы киберқылмыстардың жаңа түрлерін тудырып, олардың қоғамға тигізетін қауіпін арттыруда. Осыған байланысты Қазақстан Республикасы құқық қорғау органдарының алдында киберқылмысқа қарсы күресті жетілдіру, оның ішінде балаларды интернет арқылы азғыру және алдау әрекеттерінен қорғау мәселесі тұр. Президенттің тапсырмасына сәйкес ақпараттық қауіпсіздікті қамтамасыз ету және киберқылмыстардың алдын алу бойынша кешенді шаралар қабылдануда. Бұл шаралар халықаралық ынтымақтастықты кеңейту, интернет-платформалармен серіктестік орнату және цифрлық қауіпсіздік жүйелерін жетілдіруді қамтиды.

Сонымен қатар, Қасым-Жомарт Тоқаев киберқылмысқа қарсы халықаралық деңгейде күрес жүргізу қажеттілігін де атап өткен. Ол Шанхай ынтымақтастық ұйымына мүше мемлекеттердің саммитінде ақпараттық қауіпсіздікті қамтамасыз ету үшін киберқылмыспен күрес шараларын күшейту қажеттігін айтты. Президенттің айтуынша, киберқылмыстар тек бір мемлекеттің аясында шешіле алмайды, сондықтан бұл мәселені халықаралық деңгейде үйлестірілген іс-қимылдар арқылы шешу қажет.

2023 жылдың қазан айында Президент "Мемлекеттік техникалық қызмет" АҚ-на сапармен барып, елдің ақпараттық қауіпсіздігін қамтамасыз ету шараларымен танысты. Оған мемлекеттік органдар мен стратегиялық маңызды нысандарға 2023 жылдың алғашқы тоғыз айында 163 миллионнан астам кибершабуыл жасалғаны туралы мәлімет берілді. Президент бұл салада ұлттық қауіпсіздікке төнетін қатерлерге ерекше назар аударып, ақпараттық инфрақұрылымды қорғау шараларын күшейту қажеттігін атап өтті.

Қазіргі уақытта ақпараттық-коммуникациялық технологиялардың жедел дамуы киберқылмыстардың жаңа түрлерінің пайда болуына ықпал етуде. Солардың бірі - *кибергруминг*, яғни интернетті пайдаланушылардың, көбінесе кәмелетке толмағандардың, сеніміне кіру және оларды жыныстық сипаттағы әрекеттерге итермелеу мақсатында жасалатын қылмыстық әрекеттер. Кибергрумингтің қауіптілігі оның жасырын сипатында, қылмыскерлердің техникалық құралдарды пайдалана отырып өздерінің заңсыз әрекеттерін жүзеге

асыруында және құқық қорғау органдары үшін мұндай қылмыстарды анықтау мен тергеудің күрделілігінде жатыр. Осыған байланысты кибергрумингке қарсы күрестің теориялық және практикалық мәселелерін зерттеу өзекті болып отыр.

Шешілетін практикалық міндеттің қазіргі уақыттағы жағдайы. Қазіргі таңда кибергруминг мәселесі құқық қорғау органдарының, заңгерлердің, криминологтардың және IT-мамандардың назарында тұр. Дегенмен, қылмыстың бұл түрін тергеу мен дәлелдеу әдістемесі әлі де жетілдіруді қажет етеді. Қазақстан Республикасында және әлемнің басқа да елдерінде кибергрумингке қатысты қылмыстық істердің саны артып келе жатқанын ескерсек, *оның құқықтық реттелуін жетілдіру, тергеу әдістерін жаңғырту және халықаралық ынтымақтастықты дамыту өзекті міндет болып табылады.*

Зерттеу мақсаты. Кибергруминг қылмыстарының теориялық және құқықтық негіздерін зерделеу, оларды тергеу мен дәлелдеу әдістерін жетілдіру бойынша ғылыми негізделген ұсыныстар әзірлеу.

Осы мақсатқа жету үшін келесі міндеттер қойылады:

1) Кибергрумингті дербес қылмыстық-құқықтық категория ретінде ғылыми негіздеу, оны Қазақстан Республикасының Қылмыстық кодексіне жеке құрам ретінде енгізу қажеттілігін дәлелдеу;

2) Сандық дәлелдемелерді жинау, сақтау және рәсімдеудің процессуалдық тәртібін жетілдіру, ҚР Қылмыстық процестік кодексінде қосымша норма-«Сандық дәлелдемелерді рәсімдеу тәртібі» толықтыру қажеттігін дәлелдеу;

3) Тергеу және сот практикасы шеңберінде кәмелетке толмаған жәбірленушілермен жұмыс істеудің стандартталған, бейімделген алгоритмін әзірлеу және енгізу жолдарын ұсыну;

4) Кибергрумингке қарсы халықаралық ынтымақтастықты күшейту, Қазақстанның шет елдердің конвенцияларына қосылуының маңыздылығын айқындау.

Зерттеу объектісі: кибергрумингке байланысты қылмыстық әрекеттер және олармен күресі әдістері.

Зерттеу тақырыбы: кибергрумингке қарсы күрестің құқықтық негіздері, тергеу әдістері мен сот тәжірибесі.

Зерттеуді жүргізудің әдістері мен әдіснамалық негіздері: жалпығылыми және арнайы әдістер қолданылды, атап айтқанда:

- Жалпығылыми әдістер: талдау, синтез, индукция, дедукция, тарихи-құқықтық әдіс;
- Арнайы әдістер: салыстырмалы-құқықтық талдау, криминологиялық әдістер, эмпирикалық мәліметтерді зерттеу, құқық қолдану тәжірибесін зерделеу.

Зерттеудің әдіснамалық негізін құқықтық позитивизм, жүйелілік, кешенділік және салыстырмалы құқықтық талдау принциптері құрайды.

Ғылыми жаңалықтың негіздемесі кибергрумингті құқықтық тұрғыдан талдау және оның тергеу әдістерін жетілдіру бойынша кешенді көзқарасты ұсынуында жатыр. Атап айтқанда:

1) Кибергрумингтің ұғымы мен белгілеріне нақты анықтама беріледі;

2) Қазақстан Республикасының және шетелдік мемлекеттердің заңнамаларындағы кибергрумингке қарсы күрестің ерекшеліктері зерттеледі;

3) Тергеудің және дәлелдемелерді жинаудың жаңа әдістері ұсынылады;

4) Құқық қорғау органдары мен интернет-платформалар арасындағы ынтымақтастықты нығайту жолдары қарастырылады.

Практикалық ұсынымдар:

1) Кибергрумингті қылмыстық-құқықтық категория ретінде дербес тану қажет және ҚР Қылмыстық кодексіне 124-1-бап енгізу.

2) Сандық дәлелдемелермен жұмыс істеу тәртібін ҚР ҚПК-де нақтылау, оның ішінде заңнаманы толықтыру - «Сандық дәлелдемелерді рәсімдеу тәртібі» бекіту қажет.

3) Тергеу және сот тәжірибесінде кәмелетке толмаған жәбірленушімен жұмыс істеудің стандартталған, бейімделген алгоритмін ұсыну [Қосымша 1]

4) Қазақстанның халықаралық құқықтық актілерге қосылуы - трансшекаралық ынтымақтастықтың тиімді құралы ретінде заңды негізге алынуы тиіс (Ланзароте конвенциясы).

Апробация және нәтижелерін енгізу: Зерттеудің негізгі нәтижелері ғылыми мақалалар түрінде жарияланып, конференцияларда баяндалды. Сонымен қатар, алынған тұжырымдар құқық қорғау органдарының тәжірибесінде қолдану үшін ұсынылады.

Бұл зерттеу кибергрумингпен күрестің теориялық және практикалық негіздерін жетілдіруге ықпал етеді, сонымен қатар құқық қорғау органдарының, заңгерлердің және IT-мамандардың кибергруминг қылмыстарын тергеу әдістерін жақсартуға бағытталған нақты ұсыныстар әзірлеуге мүмкіндік береді.

1. Кибергрумингтің теориялық-құқықтық негіздері

1.1 Кибергрумингтің ұғымы, мәні және көрініс формалары

Қазіргі заманғы ақпараттық-коммуникациялық технологиялардың қарқынды дамуы қоғам өмірінің барлық салаларына елеулі өзгерістер енгізіп қана қоймай, жаңа қауіп-қатерлердің пайда болуына да ықпал етуде. Соның ішінде кәмелетке толмағандарға қатысты жасалатын интернет-қылмыстардың жаңа түрлері құқық қорғау органдары үшін өзекті мәселеге айналуда. Кибергруминг - ақпараттық-коммуникациялық технологиялар арқылы жүзеге асырылатын, кәмелетке толмағандардың сеніміне кіру және оларды жыныстық сипаттағы әрекеттерге итермелеуге бағытталған қылмыстық әрекет болып табылады [1].

Кибергрумингтің құқықтық анықтамасы әртүрлі елдердің заңнамаларында әркелкі сипатталған. Қазақстан Республикасының қылмыстық заңнамасында «кибергруминг» термині арнайы бекітілмеген, алайда оның қылмыстық-құқықтық мазмұны бірнеше баптар аясында қарастырылады. Атап айтқанда, ҚР Қылмыстық кодексінің 124-бабында (кәмелетке толмаған адамды азғындық жолға түсіру), 122-бабында (он алты жасқа толмаған адаммен жыныстық қатынас немесе сексуалдық сипаттағы өзге де әрекеттер жасау) және 273-бабында (ақпараттық-коммуникациялық желілерді қылмыстық мақсатта пайдалану) белгілі бір дәрежеде кибергрумингке қатысты құқықтық нормалар қамтылған [2].

Халықаралық тәжірибеде кибергруминг қылмысы БҰҰ, Еуропа Кеңесі және басқа да халықаралық ұйымдардың құжаттарында кеңінен қарастырылған. Мысалы, Еуропа Кеңесінің 2001 жылғы Будапешт киберқылмыс жөніндегі конвенциясы мен 2007 жылғы Ланцарот Конвенциясы (Балаларды сексуалдық қанаудан және зорлық-зомбылықтан қорғау туралы Конвенция) кибергрумингті тануды және оған қарсы тиімді күрес шараларын қабылдауды қарастырады. Сонымен қатар, Ұлыбритания, АҚШ, Германия және Франция секілді елдерде кибергруминг үшін арнайы қылмыстық жауапкершілік көзделген.

Кибергруминг - әлеуметтік қауіпті құбылыс, өйткені ол интернет желісін пайдалану арқылы жасөспірімдерді алдау, манипуляциялау және олардың психологиялық әлсіздігін қылмыстық мақсатта пайдалану арқылы жүзеге асырылады. Бұл қылмыстың ерекшелігі қылмыскердің құрбанымен физикалық байланысқа түспей-ақ, оны интернет арқылы басқаруға ұмтылуында [3].

Кибергруминг процесінде қылмыскер бірнеше негізгі кезеңдерді жүзеге асырады:

1. Алғашқы байланыс орнату - кибергруминг жасаушы тұлға интернет арқылы кәмелетке толмаған баламен байланысқа шығады. Әдетте, әлеуметтік желілер, мессенджерлер, форумдар, ойын платформалары қолданылады.

2. Сенімге кіру және эмоциялық байланыс орнату - қылмыскер жәбірленушімен эмоционалды байланыс орнатып, өзін сенімді тұлға ретінде көрсетеді.

3. Құрбанның оқшауланuын күшейту - қылмыскер құрбанды ата-анасынан, достарынан немесе қоршаған ортасынан алшақтатуға тырысады.

4. Құрбанды манипуляциялау және қорқыту - жәбірленушіні белгілі бір әрекеттер жасауға көндіру, көбінесе сексуалдық сипаттағы материалдарды жіберуге мәжбүрлеу немесе кездесуге шақыру.

5. Қылмыстық әрекетті жүзеге асыру - бұл кезеңде кибергруминг жасаушы өз мақсатына жетуге тырысады, яғни жәбірленушіні физикалық немесе виртуалды сексуалдық қанауға ұшыратады.

Бұл қылмыс баланың психологиялық, әлеуметтік және құқықтық қауіпсіздігіне тікелей зиян тигізеді. Көптеген жағдайларда кибергрумингтің құрбандары ұзақ мерзімді психологиялық жарақат алады, ал кейбір жағдайларда бұл суицидке дейін әкелуі мүмкін.

Кибергруминг әртүрлі нысандарда көрініс табуы мүмкін(кесте 1). Талдау негізінде төмендегідей негізгі түрлерін бөліп көрсетуге болады:

Кесте 1 - Кибергрумингтің негізгі түрлері мен сипаттамалары

Кибергруминг түрі	Сипаттамасы
Жалған тұлға арқылы байланыс жасау *(Fake Identity Grooming)*	Қылмыскер жалған профиль жасап, өзін жасөспірім, атақты тұлға немесе сенімді адам ретінде көрсетеді. Бұл әдіс арқылы ол құрбанмен байланыс орнатып, сенімге кіреді.
Ұзақ мерзімді психологиялық манипуляция *(Long-Term Grooming)*	Қылмыскер айлар, тіпті жылдар бойы құрбанын психологиялық тұрғыда өңдеп, оны тәуелділікке түсіреді. Мұндай әдіс құрбанды толық бақылауға алуға бағытталған.
Күш қолдану немесе қорқыту арқылы бақылау *(Threat-Based Grooming)*	Қылмыскер жәбірленушіні шантаж жасау, бопсалау арқылы қорқытады. Жәбірленуші сексуалдық сипаттағы материалдарды таратамын деген қоқан-лоққының астында қылмыскердің талаптарын орындауға мәжбүр болады.
Ойын платформалары арқылы кибергруминг *(Gaming Grooming)*	Қазіргі таңда көптеген жасөспірімдер онлайн ойындарды белсенді пайдаланады. Қылмыскерлер осы платформаларды пайдаланып, балалармен байланыс орнатып, оларды сексуалдық сипаттағы әрекеттер жасауға итермелейді.
Финанс арқылы алдау *(Financial Grooming)*	Қылмыскер жәбірленушіге қаржылай көмек көрсету немесе сыйлықтар беру арқылы сенімге кіреді. Бұл сенім кейіннен жәбірленушіні қылмыстық мақсатта пайдалануға мүмкіндік береді.

Жоғарыда көрсетілгендей, кибергруминг заманауи қылмыстық-құқықтық жүйеде аса өзекті мәселе болып табылады. Ол балалардың қауіпсіздігіне елеулі қауіп төндіреді, сондықтан бұл қылмысты тергеу мен оған қарсы күресті күшейту - құқық қорғау органдарының басым бағыттарының бірі болуы тиіс.

Қазіргі таңда Қазақстан Республикасының қылмыстық заңнамасында кибергрумингті жеке құрам ретінде қарастыру қажеттілігі туындап отыр. Сонымен қатар, құқық қорғау органдарының ақпараттық-коммуникациялық технологияларды пайдалана отырып, тергеу әдістерін жетілдіруі, халықаралық ұйымдармен ынтымақтастықты кеңейтуі және интернет-платформалармен серіктестікті нығайтуы қажет.

Кибергрумингтің ерте алдын алу шараларын жүзеге асыру, ата-аналар мен білім беру мекемелерінің ақпараттық қауіпсіздік деңгейін арттыру, сонымен қатар заңнаманы жетілдіру - осы қылмыстың таралуына қарсы күрестің негізгі бағыттары болып табылады.

Кибергрумингтің көрініс формалары әртүрлі болуы мүмкін, олардың ішінде:

- Жыныстық сипаттағы контентпен алмасу (секстинг);
- Видеоқоңырау арқылы интимді әрекеттер жасауға көндіру;
- Жеке фотосуреттерді немесе ақпаратты пайдаланып бопсалау (сексуалдық шантаж);
- Кәмелетке толмағанды нақты кездесуге шақырып, зорлық-зомбылық әрекеттер жасау.

Зерттеулер көрсеткендей, кибергрумингке ұшырайтын балалардың көпшілігі жас ерекшелігіне байланысты интернеттегі қатерлерді бағалай алмайды. Еуропалық Одақтың баланың құқықтарын қорғау агенттігінің (FRA) 2020 жылғы баяндамасында 9-16 жас аралығындағы балалардың шамамен 29%-ы бейтаныс адамдардан жыныстық сипаттағы хабарламалар алғаны анықталған [4]. Қазақстандағы жағдай да алаңдатарлық: ҚР ІІМ деректері бойынша, жыл сайын кәмелетке толмағандарға қатысты онлайн-қылмыстар саны артуда, бұл киберкеңістіктегі қауіпсіздік жүйесінің әлсіздігін көрсетеді.

Кибергрумингтің қауіптілігі - оның латенттілігі мен дәлелдеу қиындықтарында. Көп жағдайда жәбірленуші бұл әрекеттердің қылмыстық сипатын түсінбейді немесе ұялу, кінәлі сезіну, қорқу салдарынан бұл туралы ешкімге айтпайды. Сонымен қатар, қылмыскерлер өздерінің анонимдігін сақтау үшін VPN, шифрланған чаттар, фейк аккаунттар пайдаланады, бұл тергеу процесін күрделендіреді [3].

Кибергруминг әрекеттерін құқықтық тұрғыдан бағалау да әр елде әртүрлі. Қазақстан Республикасының Қылмыстық кодексінде бұл әрекеттер жеке құрам ретінде нақты сипатталмағанымен, олар ҚК-нің 122-бабы (он алты жасқа толмаған адаммен жыныстық қатынас), 123-бабы (жыныстық сипаттағы күш қолданбай жасалған әрекеттер), 124-бабы (кәмелетке толмағанды азғыру) шеңберінде сараланuы мүмкін [2]. Дегенмен, бұл баптар көбінесе нақты іс-әрекет жасалғаннан кейін ғана қолданылып жатады. Ал кибергруминг алдын алу мақсатында да қылмыстық-құқықтық жауапкершілік шараларын қажет етеді.

Осыған байланысты халықаралық тәжірибе маңызды. Мәселен, Германияның ҚК-нің 176-бабының 4-тармағы интернеттегі азғыру әрекеттерін жеке құрам ретінде қарастырады [5]. Сол сияқты, Австралия, АҚШ, Канада

елдерінде де балалармен онлайн байланыс орнату арқылы жыныстық мақсат көздеген кез келген әрекет заңмен қудаланады. Бұл тәжірибені Қазақстанның қылмыстық заңнамасына бейімдеу қажеттігі туындайды.

Кибергруминг феноменінің күрделілігі - бұл қылмыстың алдын алудағы профилактикалық, құқықтық және ақпараттық әрекеттердің өзара тығыз байланысында жатыр. Себебі, кибергруминг тек заңдық категория ретінде емес, сонымен қатар әлеуметтік-психологиялық, технологиялық және мәдени құбылыс ретінде де көрініс табады. Сондықтан да бұл мәселе бойынша кешенді және көпдеңгейлі зерттеу қажет.

Халықаралық сарапшылардың пікірінше, кибергруминг - бұл баланың санасына ұзақ мерзімді әсер ету арқылы жүзеге асырылатын қылмыстық тактика. 2021 жылы Еуропа Кеңесінің Балаларға қатысты жыныстық қылмыстарды алдын алу комитеті (Lanzarote Committee) жариялаған баяндамасында көрсетілгендей, интернеттегі жыныстық сипаттағы азғыру әрекеттері физикалық зорлық-зомбылықтың алдында жиі кездесетін кезең болып табылады. Яғни, кибергруминг — бұл қылмыскердің нақты әрекетке дейінгі дайындық алаңы, құрбандарды «психологиялық бақылауға алу» тәсілі ретінде қызмет етеді.

Сандық ортадағы кибергрумингті жүзеге асыратын субъектілердің әрекеттері күрделі манипулятивті тәсілдерге негізделеді. Көп жағдайда олар өздерін құрбандарымен қатарлас жас ретінде таныстырып, жалған профайлдар мен аватарлар арқылы сенім орнатады. Олар балалардың сеніміне кіру үшін эмоционалды қолдау көрсетіп, ата-анасынан немесе мектептен алшақ болуға итермелейді, бұл жәбірленушіні оқшауландыру механизмі ретінде қарастырылады.

Кибергруминг құрбандарының психологиялық портреті зерттеушілердің назарында. 2020 жылы Американың «Thorn» үкіметтік емес ұйымы жүргізген зерттеуде 13-17 жас аралығындағы жастардың 40%-ы интернетте бейтаныс адаммен жыныстық сипаттағы диалог жүргізгенін, ал 17%-ы фотосурет жіберуге мәжбүр болғанын хабарлаған [6]. Бұл зерттеу көрсеткендей, кибергрумингке бейім балалардың басым бөлігі - интернеттегі эмоциялық қолдауға мұқтаж, өзін-өзі бағалауы төмен және отбасында немесе мектепте жеткілікті назар ала алмайтын тұлғалар.

Кибергрумингтің қауіпті формаларының бірі - сексуалдық шартты байланыс (coercive cyber grooming), мұнда қылмыскер баланы қорқыту немесе бопсалау арқылы әрекетке итермелейді. Бұл жағдайда құрбан алғашында өз еркімен байланыс орнатқандай көрінгенімен, кейін қылмыскер оны интимді фотосуреттерімен немесе хабарламаларымен шантаж жасап, «сандық тұтқынға» айналдырады. Бұл жағдайлар көп жағдайда балада ұялу, кінәлі сезім, күйзеліс және суицидтік ойларға дейін апаратын теріс психологиялық салдарларға алып келеді.

Қазақстандық жағдайға келетін болсақ, соңғы жылдары Ішкі істер министрлігі мен Бас прокуратура жанындағы Құқық қорғау органдары академиясы бірлесіп жүргізген аналитикалық есептерде, әсіресе пандемия

кезеңінен кейін онлайн-қылмыстар, оның ішінде кәмелетке толмағандарға бағытталған кибергруминтің айтарлықтай өскені анықталған. Балалардың интернетте өткізетін уақыты артқан сайын олар киберкеңістіктегі қауіп-қатерлерге жиі тап болады. Алайда бұл қылмыстардың көпшілігі латентті күйде қалады, өйткені ата-аналар да, балалар да бұл әрекеттердің құқық бұзушылық екенін нақты түсінбеуі мүмкін.

БҰҰ-ның Балалар қорының (немесе ЮНИСЕФ) 2019 жылғы баяндамасында балалардың сандық құқықтарын қорғау және оларды онлайн-зорлықтан сақтау үшін мемлекеттерге үш негізгі бағыт ұсынылған:

1. Заңнамалық базаны халықаралық стандарттарға сәйкестендіру;

2. Сандық білім мен интернет-гигиена бойынша мектеп бағдарламаларын енгізу;

3. Балаларға арналған қауіпсіз онлайн-платформалар құру [7].

Қазақстанда бұл ұсыныстардың кейбірі іске асырылуда, алайда кибергрумингті нақты құқықтық құрам ретінде тану мәселесі өзекті күйде қалып отыр. ҚР ҚК-нің қазіргі редакциясында «кибергруминг» термині нақты көрсетілмегендіктен, құқық қорғау органдары бұл әрекеттерді жанама құрамдар арқылы саралайды. Бұл болса, тергеу мен дәлелдеу барысында құқықтық дәлсіздіктерге және сот практикасының бірізді еместігіне әкеліп соғады.

Кибергрумингке қарсы тиімді күрес жүргізу үшін тек құқықтық шаралар ғана емес, сонымен қатар институционалдық және мәдени өзгерістер қажет. Мұнда медиа-грамоталықты арттыру, балалар мен ата-аналарға арналған ақпараттық-түсіндіру жұмыстары маңызды рөл атқарады. Мысалы, Германия мен Финляндияда мектеп бағдарламасына арнайы «интернеттегі қауіпсіздік» модульдері енгізілген, ал Ұлыбританияда балаларға арналған «CEOP» атты онлайн-портал арқылы күмәнді әрекеттер туралы тікелей хабарлауға мүмкіндік берілген.

Сонымен қатар, кибергрумингпен күресте жеке деректердің қорғалуы мәселесі де ерекше мәнге ие. ҚР «Дербес деректер және оларды қорғау туралы» заңында балалардың деректерін өңдеуге қатысты нақты шектеулер енгізу қажеттілігі пісіп жетілді. Бұл - киберқылмыскерлердің әлеуметтік инженерия әдістерін шектеуге бағытталған маңызды қадам болар еді [8].

Жоғарыда келтірілген талдау кибергрумингтің тек қылмыстық әрекет қана емес, сонымен қатар балалардың өмірі мен денсаулығына, жалпы қоғамның моральдық және құқықтық қауіпсіздігіне төнетін күрделі қатер екенін айқын көрсетеді. Бұл құбылысқа қарсы тұру үшін ұлттық заңнама мен халықаралық стандарттар арасындағы үйлесімділік, құқық қорғау тәжірибесінің жетілдірілуі және сандық қауіпсіздіктің мәдениетін қалыптастыру қажет.

Кибергрумингтің күрделілігі оның тек жеке бір әрекет емес, тұтас *әлеуметтік психологиялық процесс* екенін көрсетеді. Ол кезең-кезеңмен дамып, баланың эмоционалды және мінез-құлықтық саласына ықпал етеді. Сондықтан да бұл құбылысты тек құқықтық категориямен шектемей, оны жүйелі әлеуметтік проблема ретінде қарау қажет.

Кибергрумингтің бірнеше нақты түрлері мен тәсілдері қазіргі зерттеулерде нақты жіктелген. Мысалы, 2022 жылы Америка Құрама Штаттарының Федералдық Тергеу Бюросының (ағылш.FBI) жариялаған сараптамалық баяндамада кибергруминг келесі негізгі формаларда көрініс табатыны көрсетілген:

1. Эмоционалды байланысқа негізделген груминг - баламен терең достық немесе романтикалық қарым-қатынас орнату арқылы сенімге кіру. Мұнда қылмыскер өз әрекетін агрессиясыз, керісінше қолдау мен махаббат көрсету арқылы жүзеге асырады.

2. Материалдық немесе әлеуметтік уәделер арқылы алдау - құрбанға ақша, сыйлық немесе мансаптық көмек (мысалы, модель болу, атақты болу) ұсыну арқылы байланыс орнату.

3. Қорқыту және шантаж түріндегі груминг - бала туралы ақпарат немесе интимдік фотосуреттер арқылы манипуляция жасау. Мұндай жағдайларда бала өзін кінәлі сезініп, ересектерге немесе құқық қорғау органдарына жүгінуге қорқады.

4. "Груминг-көпір" (grooming as a bridge) - киберқылмыскер бірнеше платформа арқылы (мысалы, ойындар, TikTok, Instagram) жүйелі түрде байланыс орнатып, балаға біртіндеп әсер етеді. Бұл тәсіл қазіргі балалардың цифрлық өмір салтын ескере отырып кең таралуда [9].

Қазақстанда да бұл үрдістер байқалуда. ҚР Бас прокуратурасының 2023 жылғы мәліметінше, балаларға қатысты онлайн-қылмыстардың ішінде кибергрумингке байланысты шағымдар саны 2020 жылмен салыстырғанда 2,4 есеге өскен [10]. Бұл тек тіркелген және ресми мәліметтер. Латентті қылмыстарды ескерсек, нақты көрсеткіш бұдан бірнеше есе жоғары болуы ықтимал.

Бүгінгі күні кибергрумингтің кең таралуының негізгі себептері мыналар болып табылады:

- Цифрлық сауаттың жеткіліксіздігі. Көптеген балалар киберқатерлердің не екенін білмейді, ал ата-аналар балаларының онлайн әрекеттерін бақылауға қабілетсіз немесе құлықсыз.
- Құқықтық олқылықтар. Қазақстанда кибергруминг нақты құқық бұзушылық ретінде танылмаған, нәтижесінде құқық қорғау органдары тек салдарымен күресуге мәжбүр болады.
- Анонимділік мүмкіндіктері. VPN, TOR, жалған аккаунттар арқылы қылмыскерлер заңнан оңай жасырына алады.
- Медиа-контенттің еркін таралуы. Pornhub, Reddit, Telegram секілді платформаларда жасыру мүмкіндігі жоғары, бұл жыныстық сипаттағы контенттің балаларға қолжетімділігін арттырады.

Еуропалық зерттеушілердің пікірінше, кибергрумингке қарсы күресте құқық қорғау саласынан бөлек IT-сектордың жауапкершілігі де маңызды. 2022 жылы Еурокомиссия Google, Meta (Facebook, Instagram), TikTok және Snapchat сияқты ірі платформалармен жаңа келісім қабылдап, балаларды қорғауға

бағытталған қосымша алгоритмдерді енгізуге міндеттеді. Бұл - жасанды интеллект арқылы киберқатерлерді ерте анықтау (proactive AI screening), автоматты хабарландырулар жүйесі және шектеу сүзгілерін пайдалану.

Қазақстанда да мұндай тетіктерді заңнамалық және техникалық деңгейде енгізу қажеттігі туындап отыр. Бұл үшін ең алдымен Қазақстан Республикасының Қылмыстық кодексіне «кибергруминг» түсінігін енгізіп, оны жекелеген құрам ретінде қарастыру орынды болар еді. Сонымен қатар, Интернет-провайдерлер мен әлеуметтік желілерге баланың құқықтарын қорғау жөніндегі талаптарды енгізу - өзекті реформа бағыттарының бірі.

1.2 Кибергрумингке қарсы күрестің құқықтық негіздері: халықаралық және ұлттық аспектілер

Кибергруминг - бұл кәмелетке толмағандарды интернет арқылы жыныстық сипаттағы әрекеттерге тарту мақсатында жасалатын қылмыстық әрекеттердің жиынтығы. Бұл құбылыспен күресу үшін халықаралық және ұлттық деңгейде құқықтық негіздер қалыптасқан.

1. Будапешт конвенциясы (2001 ж.)

Еуропа Кеңесінің Будапешт конвенциясы - киберқылмыстармен күресуге бағытталған алғашқы халықаралық келісім. Ол ұлттық заңнамаларды үйлестіру, тергеу әдістерін жетілдіру және мемлекеттер арасындағы ынтымақтастықты нығайту мақсатында қабылданды. Конвенцияның 9-бабы балалардың жыныстық сипаттағы материалдарын таратуға қарсы бағытталған.

2. Ланзароте конвенциясы (2007 ж.)

Еуропа Кеңесінің Ланзароте конвенциясы кәмелетке толмағандарды жыныстық қанаудан қорғауға бағытталған. Конвенцияның 23-бабында кибергрумингті жеке қылмыс ретінде қарастыру қажеттілігі көрсетілген.

3. БҰҰ-ның Киберқылмысқа қарсы конвенциясы (2024 ж.)

2024 жылы БҰҰ Бас Ассамблеясы киберқылмыстармен күресу және электрондық дәлелдемелермен алмасуды жеңілдету мақсатында жаңа конвенция қабылдады. Бұл құжат мемлекеттер арасындағы ынтымақтастықты арттыруға бағытталған.

Қазақстанда кибергруминг нақты қылмыс ретінде заңда көрсетілмегенімен, бірқатар баптар арқылы бұл әрекеттерге қарсы шаралар қабылдануда:

- ҚР ҚК 122-бабы - он алты жасқа толмаған адаммен жыныстық қатынас.
- ҚР ҚК 123-бабы - жыныстық сипаттағы күш қолданбай жасалған әрекеттер.
- ҚР ҚК 124-бабы - кәмелетке толмағанды азғыру.

Алайда, бұл баптар көбінесе нақты әрекет жасалғаннан кейін ғана қолданылады, ал кибергрумингтің алдын алу үшін арнайы құқықтық нормалар қажет.

Сонымен қатар, Қазақстанда киберқылмыстармен күресу үшін "Қазақстанның киберқалқаны" атты концепция қабылданған. Бұл құжат ақпараттық қауіпсіздікті қамтамасыз ету және киберқылмыстардың алдын алу мақсатында әзірленген.

Кибергрумингпен тиімді күресу үшін Қазақстан халықаралық тәжірибені ескере отырып, ұлттық заңнамасын жетілдіруі қажет. Бұл үшін кибергрумингті жеке қылмыс ретінде тану, құқық қорғау органдарының мүмкіндіктерін арттыру және халықаралық ынтымақтастықты нығайту маңызды.

Кибергрумингке қарсы күрестің құқықтық негіздерін дамыту - бұл тек жазалау функциясы емес, сонымен қатар балалардың цифрлық құқықтарын қорғауға бағытталған құқықтық мәдениетті қалыптастыру үдерісі. Бұл бағытта халықаралық құқықтық стандарттарды ұлттық заңнамаға үйлестіру - маңызды әрі өзекті мәселе.

Көптеген дамыған елдерде кибергруминг қылмысы нақты құқықтық құрам ретінде бекітілген. Мысалы:

- Германия ҚК 176-бабының 4-тармағында кәмелетке толмағанмен жыныстық сипаттағы байланысты интернет арқылы орнатуға талпыну жеке қылмыс ретінде қарастырылады.
- Австралия ҚК 474.26 және 474.27-баптарында ересек адамның кәмелетке толмағанмен онлайн байланыс орнатуының өзі-ақ қылмыстық жауапкершілікке әкеледі.
- АҚШ-та федералды деңгейде «Protect Act» (2003) және «Adam Walsh Child Protection Act» (2006) заңдары арқылы кибергруминг нақты құқықбұзушылық ретінде қатаң реттеледі.

Қазақстанда бұл тәжірибе әлі толық деңгейде енгізілмеген. ҚР Қылмыстық кодексінде кибергруминг термині пайдаланылмайды, ал заңнамалық нормалар көбінесе нақты сексуалдық әрекет жасалғаннан кейін ғана іске қосылады. Бұл — алдын алу тетіктерінің әлсіздігін көрсететін заңнамалық олқылық.

Қазақстанның құқық қорғау тәжірибесінде көбінесе ҚК 124-бабы (кәмелетке толмағанды азғыру) пайдаланылады. Алайда, бұл баптың өзі физикалық байланыс орнату ниеті болған жағдайда ғана жұмыс істейді. Ал кибергруминг - көбіне виртуалды кеңістікте жүзеге асатын, физикалық жанасусыз, бірақ психологиялық әсері күшті әрекет. Демек, заңнамалық база бұл әрекеттердің шынайы табиғатын ескермейді [11].

Кибергрумингті тану үшін құқық қорғау саласында объективті және субъективті белгілерді нақтылау қажет:

- Объективтік белгілер: интернеттегі хат-хабарлар, фото немесе видео сұрау, кездесуге шақыру, виртуалды әрекеттерге итермелеу.
- Субъективтік белгілер: жыныстық қатынасқа тарту ниеті, манипуляциялық мақсат.

Бұл элементтер қазіргі қылмыстық заңнамада жүйеленбеген, сондықтан тергеушілер мен прокурорларға іс жүргізу барысында бірізділік жетіспейді.

Нәтижесінде құқық қолдану практикасы тұрақсыз, кейде бұл әрекеттер құқық бұзушылық ретінде тіркелмей қалуы да мүмкін.

Салыстырмалы құқықтық талдау көрсеткендей, көптеген мемлекеттер кибергрумингке қарсы арнайы заңдар қабылдауға көшуде. Мәселен, Ұлыбританияда «Sexual Communication with a Child» бабы 2015 жылдан бастап Criminal Justice and Courts Act құрамында енгізілген [12]. Бұл бап интернет арқылы жыныстық тақырыпта байланыс орнатқан тұлғаны нақты жауапкершілікке тартуға мүмкіндік береді. Тіпті физикалық кездесудің болмауы да жауапкершіліктен босатпайды.

Бұған қоса, кибергрумингпен күрес тек қылмыстық құқық шеңберінде емес, әкімшілік, азаматтық және білім беру жүйелері арқылы да жүзеге асуы тиіс. Мысалы, АҚШ пен Нидерландыда мектептерде балалардың интернет қауіпсіздігі туралы арнайы модульдер енгізілген. Мұндай білім беру бағдарламалары балалардың құқықтық санасын арттырып, оларды қауіп-қатерден қорғай алады.

Қазақстанда бұл бағыт енді қалыптасу үстінде. 2022 жылдан бастап «Цифрлық гигиена» тақырыбы кейбір мектеп пәндерінде қарастырыла бастады, алайда ол кибергруминг секілді күрделі құбылысты тануға жеткіліксіз.

Кибергрумингке қарсы күресте халықаралық ынтымақтастық та аса маңызды. Себебі, интернет - трансшекаралық кеңістік. Бір елде жасалған киберқылмыс екінші елде салдар тудыруы мүмкін. Осы себепті мемлекеттер экстрадиция, электронды дәлелдерді беру және трансұлттық тергеулер бойынша келісімдерге келуі тиіс.

Будапешт конвенциясы мен БҰҰ-ның жаңа Киберқылмысқа қарсы конвенциясы осы ынтымақтастықты нығайтуға бағытталған. Қазақстан Будапешт конвенциясына әлі қосылған жоқ. Бұл - құқықтық интеграция үшін маңызды қадамдардың бірі болуы тиіс.

Бұдан бөлек, кибергрумингпен күресте ақпараттық-коммуникациялық технологияларды қолданудың құқықтық негіздерін жетілдіру қажет. Бұл ретте:

- Электрондық дәлелдемелерді заңдастыру;
- Әлеуметтік желілермен меморандумдар жасау;
- Автоматтандырылған іздеу жүйелерін енгізу (AI көмегімен жәбірленушіні қорғау).

2023 жылы Еурокомиссия жасанды интеллект негізінде жұмыс істейтін «Child Safety AI» жобасын іске қосты. Бұл жүйе интернет кеңістігінде кибергруминг белгілерін автоматты түрде анықтап, қауіп туралы ата-аналар мен платформаларға хабарлайды. Осындай құралдар Қазақстан үшін де аса өзекті болар еді.

Кибергрумингке қарсы күрестің құқықтық тетіктері тек жаза қолданумен шектелмей, кешенді және көпдеңгейлі механизмдерден тұруы тиіс. Бұл тетіктердің тиімділігі мемлекет ішіндегі заңнамалық нормалар мен халықаралық стандарттардың өзара байланысына тікелей тәуелді. Өкінішке орай, қазіргі Қазақстан заңнамасында кибергруминг нақты қылмыстық құрам ретінде

қарастырылмаған. Бұл жағдай құқық қолдану практикасында бірқатар қиындықтарды тудырып, балалардың интернеттегі құқықтарының осалдығын арттырып отыр.

Қазақстан Республикасы Қылмыстық кодексінің 122, 123 және 124-баптары, әрине, жыныстық сипаттағы әрекеттерді реттейді, бірақ олардың мазмұны кибергрумингтің ерекшеліктерін - оның виртуалды, кезеңдік және манипулятивтік сипатын толық қамти алмайды. Қылмыскер жәбірленушімен ұзақ уақыт бойы интернет арқылы байланыс орнатып, сеніміне кіріп, нақты әрекетке бармаса да, моральдық, психологиялық және ақпараттық зиян келтіреді. Бірақ осы аралық кезеңде ол құқықтық тұрғыда жазасыз қалуы мүмкін. Бұл - заңнаманың алдын алу рөлін әлсірететін фактор.

Көптеген елдердің тәжірибесі көрсеткендей, кибергрумингтің алдын алу үшін оны нақты қылмыс ретінде тану ғана емес, оған қатысты процессуалдық дәлелдер жинау тетіктері де жетілдірілуі тиіс. Мысалы, Нидерланды мен Германияда интернеттегі хат-хабар алмасу, чат жазбалары, видео немесе фото арқылы жүргізілген әңгімелер, тіпті жыныстық сипаттағы әңгіме қозғалғаны туралы фактінің өзі сотта дәлел ретінде мойындалады. Ал Қазақстанда мұндай цифрлық дәлелдерді заңдастыру, сақтау және қолдану процесі құқықтық реттеудің айқын болмауына байланысты қиындық тудырады [13].

Сонымен қатар, елімізде кибергруминг фактілері көп жағдайда баланың немесе оның ата-анасының арызынан кейін ғана тергеледі. Бұл - әрекетке реактивті тәсіл, ал кибергруминг сияқты алдын алуға болатын қауіптерге проактивті тәсіл қажет. Яғни, заңнама тек болған әрекетке емес, болуы мүмкін әрекеттерге де құқықтық тосқауыл қоюға бағытталуы тиіс. Мәселен, Ұлыбританияда 18 жастан асқан адам егер 16 жасқа толмаған баламен бірнеше рет жыныстық тақырыпта хат-хабар алмасса, жыныстық мақсатта байланыс орнатқаны үшін жауапқа тартылуы мүмкін. Бұл үлгі алдын алудың нақты мысалы ретінде тиімді.

Қазақстанда кибергрумингпен күресетін құқық қорғау органдарының әрекеттері көбінесе көп сатылы келісімдер мен сараптамаларға тіреліп қалады. Цифрлық платформалармен (Meta, Telegram, TikTok) жұмыс істеу барысында құқық қорғау органдары халықаралық процедураларға тәуелді болады. Алайда көптеген жағдайда бұл платформалар Қазақстан құқық қорғау органдарына деректерді беруден бас тартады немесе ұзаққа созылатын бюрократиялық процестер арқылы жедел тергеуге кедергі келтіреді [14].

Сондықтан Қазақстан үшін мынадай реформалар өзекті:

1. ҚК-ге кибергруминг ұғымын енгізу. Бұл жаңа қылмыстық құрамның заңи анықтамасын жасап, оны нақты объективтік және субъективтік белгілермен бекіту қажет.

2. Қылмыстық іс жүргізу кодексіне өзгерістер енгізу. Цифрлық дәлелдемелерді жинау, сақтау және сараптау бойынша процедуралар жетілдірілуі тиіс.

3. Тергеушілер мен прокурорлар үшін арнайы нұсқаулықтар мен методикалар енгізу. Бұл әрекет киберқылмыстармен жұмыс істейтін мамандардың кәсіби деңгейін көтеруге сеп болады.

4. Мектептер мен колледждерде цифрлық құқықтар және қауіпсіздік бойынша міндетті пән енгізу. Бұл балалардың құқықтық санасын арттырып, қауіптің алдын алуға көмектеседі.

5. Халықаралық құқықтық ынтымақтастықты нығайту. Қазақстан Будапешт конвенциясына қосылу арқылы шетелдік интернет-платформалармен ресми әрі құқықтық байланыс орната алар еді.

Бұдан бөлек, Қазақстанда кибергрумингті құқықтық тұрғыда бағалаудағы моральдық және мәдени ерекшеліктер де назардан тыс қалмауы тиіс. Қоғамда сексуалдық тақырыптарға қатысты жабық көзқарас кибергрумингке ұшыраған балалардың көмекке жүгінуін қиындатады. Сондықтан бұл мәселені құқықтық ғана емес, әлеуметтік және педагогикалық деңгейде де шешу қажет. Жәбірленушілерге сенімді орталар (жасөспірімдерге арналған шұғыл желі, құпия психолог қызметі, мектеп инспекторлары) арқылы қолдау көрсету - құқықтық қорғаныстың тиімділігін арттырады.

Қазіргі таңда құқық қорғау қызметкерлерінің дайындығы мен техникалық мүмкіндіктері де шектеулі. Сандық іздермен жұмыс істейтін мамандар аз, ал барларының жүктемесі көп. Көп жағдайда тергеушілер өз бетімен интернеттегі іздерді талдауға, виртуалды серверлермен жұмыс істеуге мәжбүр болады. Бұл — тергеу сапасына әсер ететін фактор. Сондықтан кибертергеу бөлімдерін жеке құрылым ретінде дамытып, IT мамандар мен құқық қорғаушыларды бірлесе оқытатын жүйе енгізу қажет [15].

1.3 Кибергруминг қылмыскерлері мен құрбандарының криминологиялық сипаттамасы

Кибергрумингті кешенді түрде түсіну үшін тек құқықтық немесе технологиялық тұрғыдан қарау жеткіліксіз. Бұл құбылыстың шынайы табиғатын ашу үшін оған қатысушылардың - яғни, қылмыскер мен жәбірленушінің - криминологиялық портретін, әлеуметтік бейнесін, психологиялық мотивациясын және әрекет моделін зерделеу қажет. Бұл тәсіл қылмысты дер кезінде анықтау, алдын алу және тиімді тергеу үшін аса маңызды [16].

Кибергруминг қылмыскерінің криминологиялық портреті

Зерттеулер мен құқық қорғау практикасы кибергрумингпен айналысатын тұлғалардың нақты типологиялық белгілерін анықтап отыр. Бұл қылмыскерлер көбінесе дәстүрлі зорлық-зомбылық қылмыскерлерінен ерекшеленеді - олар интернеттегі анонимділікті пайдаланатын, психологиялық манипуляцияға бейім, көбінесе сырт көзге "қалыпты" адам ретінде көрінетін тұлғалар.

2020 жылы Еуропол жүргізген аналитикалық баяндамасында кибергрумингке қатысқан қылмыскерлердің келесі ортақ сипаттары анықталған:

- Жасы: 25-тен 55 жасқа дейінгі ер адамдар басым (шамамен 88%);

- Әлеуметтік статусы: Көпшілігі тұрақты жұмысы бар, кейбіреуі отбасылы;
- Психологиялық ерекшеліктері: Эмпатияның төмендігі, нарциссизм, сексуалдық фрустрация, билікке құмарлық, педофильдік бейімділік;
- Техникалық сауаттылығы: Жоғары немесе орташа деңгейде - VPN, Tor, анонимді шолғыштарды пайдаланады, фейк аккаунттар ашады;
- Қылмыстық ниет: Нақты сексуалдық қатынас орнату, фото-видео материал жинау, жәбірленушіні бақылау немесе бопсалау [17].

Олардың негізгі тактикалық ерекшеліктері - бұл сенімге кіру, эмоционалды тәуелділік қалыптастыру, жалған уәделер мен манипуляция. Жыныстық зорлық-зомбылық жасаушы "дәстүрлі" қылмыскерлерге қарағанда, кибергрумерлер ұзақ мерзімді стратегиялық байланыс орната отырып, "цифрлық жәбірлеуші" рөлін атқарады.

Кейбір жағдайларда қылмыскерлер жасөспірімдердің өз бейнесіне еліктеп, олардың тілін, қызығушылығын және мәдени кодтарын үйреніп, арнайы бейнеге енеді. Мұндай "маскаланған" әрекеттер - кибергрумингтің ең қауіпті аспектілерінің бірі.

Кибергруминг құрбандарының криминологиялық бейнесі

Қылмыстың екінші жағы - жәбірленуші, яғни кәмелетке толмаған тұлға. Көп жағдайда бұл балалар мен жасөспірімдер 10-17 жас аралығында болады. Олар интернетке жиі кіретін, цифрлық әлемде көп уақыт өткізетін, өзіндік жеке шекарасы мен қорғану стратегиясы қалыптаспаған тұлғалар.

Зерттеулер құрбандардың ортақ сипаттарын төмендегідей сипаттайды:

- Жасы: ең жиі кездесетін жас тобы - 11-14 жас;
- Жынысы: қыз балалар басым (шамамен 70-75%), бірақ ер балалардың да саны артып келеді;
- Отбасылық факторлар: ата-ана назарының жетіспеуі, толық емес отбасы, отбасылық жанжал;
- Психологиялық ерекшеліктері: өзін-өзі бағалаудың төмендігі, қабылдауға деген мұқтаждық, эмоционалды жалғыздық;
- Цифрлық мінез-құлық: әлеуметтік желілерде белсенділік, белгісіз адамдармен оңай байланыс орнату, виртуалды таныстықтарға сену.

2022 жылы жүргізілген ЮНИСЕФ зерттеуіне сәйкес, Қазақстандағы жасөспірімдердің шамамен 47%-ы интернет арқылы бұрын таныс емес адамдармен сөйлескен, ал 23%-ы оларға жеке ақпаратын берген. Бұл - балалардың интернеттегі қауіпсіздік туралы білімі аз екенін көрсетеді. Сол себепті кибергруминг қылмыскерлеріне құрбан табу қиындық тудырмайды [18].

Кибергруминг құрбандары көбінесе қылмыстық оқиғаны жасырғысы келеді, бұл - қылмыстың латенттілігін арттыратын негізгі фактор. Балалар көп жағдайда өздерін кінәлі сезінеді, ұялады, не болатынын түсінбейді немесе қылмыскер тарапынан қорқытылады. Бұл латенттілік құқық қорғау

органдарының жұмысын қиындатып, қылмыскердің жазасыз қалу қаупін арттырады.

Қылмыскер мен құрбанының өзара әрекет механизмі

Кибергруминг - бұл тек біржақты емес, екі тараптың (қылмыскер мен жәбірленушінің) ұзақ өзара әрекеті арқылы дамитын процесс. Бұл өзара әрекет әдетте келесі сатылардан тұрады:

1. Танысу және байланыс орнату - қылмыскер өз құрбанын чаттарда, әлеуметтік желілерде немесе онлайн ойындарда табады.
2. Сенім орнату - балаға қызығушылық білдіру, эмоционалдық қолдау көрсету арқылы оны ата-анасынан немесе жақын ортасынан алыстату.
3. Манипуляция кезеңі - жасырын жыныстық мазмұндағы диалогтар, фото немесе видео сұрату.
4. Эксплуатация - бала жыныстық әрекетке итермеленіп, қылмыстық материал өндіруге немесе бопсалауға тартылады.

Бұл процесте қылмыскер психологиялық әсер ету әдістерін, мысалы: эмоционалды шантаж, «құпияны бірге сақтау» тактикасы, кінә тағу, қысым көрсету сияқты тәсілдерді шебер қолданады.

Криминологиялық қауіп факторлары мен алдын алу мүмкіндіктері

Кибергрумингтің басты қауіпі - оның айқын шекараларының болмауында. Бұл қылмыс физикалық қатынассыз да жасалуы мүмкін. Сондықтан құқық қорғау органдары мен қоғам оған тек сексуалдық зорлық-зомбылық ретінде емес, интернеттегі балаларға қарсы манипулятивті әрекет ретінде қарауы керек.

Алдын алу үшін келесі кешенді шаралар маңызды:

- Қылмыскерлердің психологиялық типологиясын ескере отырып, профилактикалық мониторинг жүйелерін енгізу;
- Балалардың цифрлық қауіпсіздігі туралы білімін арттыру, психологиялық сауаттылықты дамыту;
- Ата-аналарға арналған ақпараттық науқандар өткізу;
- Жәбірленушілерге арналған құпия көмек платформаларын құру.

Сондай-ақ, кибергрумингке байланысты рецидивизм деңгейі де жоғары. Көптеген халықаралық дереккөздер мұндай қылмыскерлердің қайтадан құрбан іздеуге бейім болатынын көрсетеді. Сондықтан оларды анықтап, мәжбүрлі емдеу, тіркеу және қоғамдық бақылау жүйесін енгізу қажет.

Кибергруминг - бұл тек сексуалдық мазмұндағы онлайн әрекет қана емес, ол әлеуметтік девиацияның жаңа түрі, қоғамдағы моральдық құндылықтар мен цифрлық мәдениеттің дағдарысын көрсететін құбылыс. Бұл қылмыстың ерекшелігі - оның классикалық қылмыстармен салыстырғанда жасырын, кезеңдік және психологиялық тұрғыдан күрделі сипатында. Сондықтан кибергрумингпен айналысатын тұлғалар мен олардың құрбандарының терең криминологиялық бейнесі - алдын алу және тергеу стратегияларын әзірлеудің негізі болып табылады.

Қылмыскерлердің психологиялық портретін тереңірек талдай отырып, олардың әрекет ету механизмдері көбінесе педофильдік бейімділіктен немесе

жеке тұлғалық бұзылыстардан туындайтынын байқауға болады. Психиатрия және криминология саласындағы зерттеулерге сүйенсек, мұндай қылмыскерлердің едәуір бөлігі - қоғамда өзін шеттетілген сезінетін, эмоциялық тұрақсыз, бірақ интеллектуалды қабілеті жоғары адамдар. Олар нақты өмірде баламен қарым-қатынас орната алмағандықтан, интернет кеңістігін "қауіпсіз алаң" ретінде пайдаланады [19].

Психологтар кибергрумерлерді бірнеше типке бөледі:

- "Қамқоршы" типі - өзін баланың қорғаушысы, "жалғыз досы" ретінде көрсетіп, эмоционалды байланыс орнатады;
- "Қарапайым құрдас" бейнесіндегі қылмыскер - өзін құрбанмен жасты етіп көрсетіп, ортақ қызығушылықтар арқылы достық құрады;
- "Агрессор" типі - алғашында жылы сөйлесіп, кейіннен қорқытып, қысым көрсетіп, бопсалау тактикасына көшеді;
- "Коллекционер" типі - балалардан интимді фотосуреттер жинаумен айналысады және оларды желілерде таратады немесе сатады.

Бұл типологиялар кибергрумингке қарсы күресте тергеушілер мен профилактика жүргізушілер үшін пайдалы. Өйткені әр тип өзіне тән тактикалар мен дәлелдемелер қалдырады. Мысалы, «қамқоршы» типі хат алмасуларда сенімге кіру фразаларын жиі қолданады, ал «агрессор» типі - бопсалау тілін пайдаланып, ашық қауіп төндіру белгілерін көрсетеді.

Құрбандарға келетін болсақ, олардың мінез-құлқы көбінесе отбасы, мектеп, құрдастар ортасы мен интернет кеңістігі арқылы қалыптасады. Көптеген жағдайларда кибергрумингке ұшыраған балалар психоэмоционалды тұрғыда осал, өмірлік тәжірибесі аз, интернеттегі қауіптерді толық бағалай алмайтын тұлғалар. Бұл жағдайды 2021 жылы жүргізілген Ресей, Қазақстан және Қырғызстан бойынша ЮНИСЕФ-тің зерттеуі де дәлелдеген - қатысқан балалардың 37%-ы интернеттегі жағымсыз қарым-қатынасқа ұшырағанын, ал 14%-ы жыныстық сипаттағы хабарламалар алғанын мойындаған [20].

Қылмыскер мен құрбан арасындағы қарым-қатынас әрдайым ассиметриялық, яғни бір жақ психологиялық басымдылыққа ие. Мұны тергеу барысында ескеру - өте маңызды. Көп жағдайда қылмыскер құрбанды әлеуметтік қолдаудан айырылған тұлға ретінде таңдайды: достары жоқ, ата-анамен сенімді байланыс орнамаған, мектепте буллингке ұшыраған. Осы тұрғыдан алғанда, кибергруминг - бұл тек құқықтық мәселе ғана емес, әлеуметтік психологияның да салдары [21].

Кибергрумингке ықпал ететін тағы бір фактор - интернет платформаларының еркіндігі. Әлеуметтік желілер мен мессенджерлерде фейк аккаунт ашу оңай, пайдаланушыларды бақылау шектеулі, ал модерация көбіне автоматты алгоритмдер арқылы ғана жүргізіледі. Мысалы, TikTok немесе Instagram сияқты платформаларда балалардың өздері жеке парақшалар ашып, өздерін танымал етуге тырысады. Осы мақсатпен олар ашық фотосуреттер, өмірлік мәліметтер, эмоциялық посттар жариялайды - бұл ақпараттың бәрі киберқылмыскерлер үшін өте құнды.

Цифрлық кеңістіктегі баланың мінез-құлқын бақылау мен реттеу - ата-аналардың ғана емес, бүкіл қоғамның міндеті. Бірақ бүгінде бұл реттеу тым әлсіз. Ата-аналардың едәуір бөлігі цифрлық технологияларды баланың тыныштығы үшін пайдаланады, бірақ оның қандай сайттарға кіріп жатқанын, кіммен сөйлесіп жүргенін білмейді. Осыдан келіп, құқық қорғау органдары үшін ең қиын мәселе туындайды - қылмыстың дер кезінде анықталмауы. Нәтижесінде кибергруминг көбінесе тек жәбірленуші тарапынан келіп түскен шағымнан кейін ғана тергеледі, ал кейбір жағдайларда мүлде тіркелмей қалады.

Криминологиялық тәжірибеде кибергрумингке қатысушы қылмыскерлердің белгілі бір бөлігі бірнеше құрбанға бір уақытта немесе жүйелі түрде әсер етеді. Яғни олар әлеуметтік желілерде параллель түрде 5-10 балаға жазып, олардың ішінен "осал" құрбандарды таңдайды. Бұл олардың әрекетінде алдын ала дайындық, іздену және жоспарлау элементтері бар екенін көрсетеді. Осындай факторлар қылмыстың ерекше қауіптілігі мен жүйелілігін дәлелдейді [22].

Кибергруминг - бұл қазіргі заманның ең күрделі және қауіпті қылмыстық-әлеуметтік құбылыстарының бірі ретінде зерттелді. 1-бөлім аясында жүргізілген теориялық, құқықтық және криминологиялық талдаулар бұл құбылыстың тек жыныстық сипаттағы қылмыс қана емес, сонымен қатар цифрлық кеңістікте балалардың қауіпсіздігіне төнген жүйелі қатер екенін айқын көрсетті.

Біріншіден, кибергруминг ұғымына нақты анықтама беріліп, оның құрылымдық белгілері, көрініс формалары мен психологиялық табиғаты қарастырылды. Бұл әрекет кезеңдік сипатқа ие болып, жәбірленушімен сенімді қатынас орнатудан бастап, манипуляция мен бопсалауға дейінгі бірнеше сатыдан өтетіндігі айқындалды. Сонымен қатар, оның виртуалды түрде жүзеге асатыны - дәлелдеуді, алдын алуды қиындататын басты ерекшеліктердің бірі.

Екіншіден, кибергрумингке қарсы күрестің құқықтық негіздеріне терең талдау жүргізілді. Халықаралық тәжірибеде бұл әрекет дербес қылмыс ретінде қарастырылып, Будапешт және Ланзароте конвенциялары аясында реттелген. Германия, Ұлыбритания, АҚШ сияқты елдер кибергрумингті арнайы қылмыстық құрам ретінде танып, тиімді құқықтық және техникалық шешімдер қабылдауда. Ал Қазақстанда кибергруминг әлі күнге дейін Қылмыстық кодекстің нақты бір бабымен қарастырылмаған, бұл құқық қолдану тәжірибесінде елеулі құқықтық вакуум туғызуда. Осыған байланысты кибергрумингті ҚК-де нақты қылмыс ретінде заңдастыру қажеттілігі дәлелденді.

Үшіншіден, кибергрумингке қатысушылардың - яғни, қылмыскер мен жәбірленушінің - криминологиялық сипаттамасы берілді. Қылмыскерлер көбінесе техникалық сауатты, жасырын әрекет ететін, манипуляция мен сенімге кіру тактикаларын пайдаланатын тұлғалар екені анықталды. Ал құрбандар - көбінесе психологиялық осал, әлеуметтік қолдаудан айырылған немесе интернеттегі назарға мұқтаж балалар. Бұл қылмыстардың латенттілігі жоғары екенін және оларды анықтау мен тергеудің күрделілігін көрсетті [19].

Жалпы алғанда, 1-бөлім аясында кибергрумингті қылмыстық құқық, халықаралық құқық және криминология тұрғысынан кешенді талдау оның табиғатын, ерекшеліктерін және құқықтық реттеудегі кемшіліктерді нақтылауға мүмкіндік берді. Бұл бөлімде жасалған қорытындылар 2 және 3-тарауларда кибергрумингпен күресудің нақты тергеу әдістемесі мен құқық қорғау жүйесін жетілдіру бағытындағы ұсыныстарды әзірлеудің ғылыми негізі болып табылады.

2. Кибергрумингке байланысты қылмыстарды тергеу әдістемесі

2.1 Кибергруминг бойынша қылмыстық істерді қозғаудың ерекшеліктері

Кибергрумингке байланысты қылмыстық істерді қозғау - қылмыстық процестің ең күрделі, әрі жауапты кезеңдерінің бірі болып табылады. Бұл әрекет көбінесе жасырын, жасанды виртуалды ортада жүзеге асатындықтан, оның құқықтық табиғатын анықтау, дәлел жинау және процессуалдық шешім қабылдау құқық қорғау органдары үшін бірқатар әдістемелік, құқықтық және психологиялық қиындықтар тудырады. Кибергруминг бойынша қылмыстық іс қозғаудың күрделілігі ең алдымен оның латенттілігіне, құқықтық

классификациясының нақты болмауына және дәлелдемелердің спецификасына байланысты [23].

Біріншіден, кибергруминг фактілері көп жағдайда жәбірленушінің арызы негізінде ғана ашылады, бұл оның анықталуын кешеуілдетеді. Кәмелетке толмағандар көбіне психологиялық қысым, ұялу немесе қылмыскердің қорқытуына байланысты құқық қорғау органдарына жүгінбейді. Қазақстан Республикасының қылмыстық-процессуалдық кодексінің 179-бабына сәйкес, қылмыстық іс дәлелді арыз, хабар немесе өзге де ақпарат негізінде қозғалуы мүмкін. Алайда кибергруминг жағдайында мұндай ақпарат көбіне ата-аналар тарапынан түседі, бұл тергеудің басталуын субъективті факторларға тәуелді етеді. Яғни, іс қозғау фактісі көбіне баланың психологиялық жағдайына, отбасының құқықтық сауаттылығына және мектеп немесе әлеуметтік қызметтердің белсенділігіне байланысты болады.

Екіншіден, қылмыстық істі қозғау кезінде негізгі проблемалардың бірі - қылмыстың құқықтық сараланууы. Қазіргі қолданыстағы ҚР Қылмыстық кодексінде кибергруминг ұғымы нақты қылмыстық құрам ретінде көрсетілмеген. Тергеушілер мұндай әрекеттерді ҚК-нің 122-бабы (он алты жасқа толмағанмен жыныстық қатынас), 123-бабы (жыныстық сипаттағы күш қолданбай жасалған әрекеттер) немесе 124-бабы (кәмелетке толмағанды азғыру) аясында саралауға тырысады. Алайда бұл баптар нақты физикалық әрекетті талап етеді, ал кибергруминг - көп жағдайда виртуалды байланыс деңгейінде шектеліп, нақты сексуалдық актіге ұласпауы мүмкін. Нәтижесінде, қылмыстық істі қозғау барысында дәлелдеу шегінің (стандартының) жетіспеушілігі немесе іс-әрекеттің құқықтық белгісіздігіне байланысты қылмыстық іс тіркелмей қалуы мүмкін [2].

Үшіншіден, кибергрумингке байланысты істі қозғау үшін сандық дәлелдерге сүйену қажет, ал оларды жинау мен сараптау процесі де өзіндік ерекшеліктерге ие. Қылмыскер мен жәбірленуші арасындағы хат алмасу, фотосуреттер, скриншоттар, аудиохабарламалар, IP-адрестер және әлеуметтік желідегі логтар - бұлардың барлығы іске дәлелдеме ретінде тіркелуі тиіс. Алайда бұл материалдардың көпшілігі бұлтты серверлерде сақталады, ал кейбіреулері шетелдік юрисдикциядағы компаниялардың платформаларында орналасқан. Мұндай жағдайда тергеушілердің Meta (Facebook, Instagram), Google, TikTok сияқты трансұлттық компаниялардан заңды жолмен сұраныс жасауына қажетті халықаралық құқықтық тетіктері шектеулі.

Төртіншіден, дәлел жинау процесінде ҚР ҚПК-нің 110-бабы бойынша электрондық ақпарат құралдарын алу, қарап шығу және бекіту арнайы ережелерге бағынуы тиіс. Тергеуші бұлтартпас дәлелдемелерге ие болғанда ғана іс қозғау туралы шешім шығара алады. Алайда дәлелдемелердің сандық сипаты олардың манипуляциялану мүмкіндігін арттырады. Сондықтан оларды тексеру үшін арнайы IT-сараптама қажет. Бірақ бұл салада білікті кадрлар тапшылығы сезіледі, ал сараптаманың жүргізілу мерзімі істің жылдамдығына кері әсер етеді.

Бесіншіден, кибергруминг бойынша қылмыстық іс қозғаудың тағы бір ерекшелігі - бұл әрекеттің баланың психологиялық жағдайына тікелей әсері.

ҚПК нормаларына сәйкес, жәбірленушінің қатысуымен тергеу әрекеттерін жүргізу кезінде оның жас ерекшелігі мен психоэмоционалдық жағдайы ескерілуі тиіс. Алайда көп жағдайда бала тергеуге психологиялық тұрғыда дайын болмайды, бұл тергеу нәтижелеріне әсер етуі мүмкін. Сондықтан бала психологиясын білетін, арнайы даярлықтан өткен мамандардың (психологтар, педагогтар) қатысуымен әрекеттерді жүргізу - істі қозғау кезінде міндетті талап болуы тиіс [24].

Халықаралық тәжірибеде кибергрумингке қатысты қылмыстық істер факт бойынша емес, ниет бойынша да қозғалуы мүмкін. Мысалы, Германияда жыныстық сипаттағы әңгіме жүргізіп, нақты жыныстық қатынасқа итермелеу әрекеті - қылмыстық ниеттің дәлелі ретінде бағаланып, іс қозғауға жеткілікті негіз болып табылады. Қазақстанда мұндай тәсіл әлі кеңінен қолданылмайды, бұл тергеу органдарының бағалау еркіндігін шектейді.

Тағы бір өзекті мәселе - қылмыстың трансшекаралық сипаты. Кибергрумерлер жиі түрде өз елінен тыс орналасқан серверлер мен аккаунттарды пайдаланады. Бұл жағдайда істі қозғау мен тергеу үшін халықаралық құқықтық көмек тетіктері іске қосылуы қажет. Алайда Қазақстан әлі күнге дейін Будапешт конвенциясына қосылмаған, бұл өз кезегінде электрондық дәлелдемелерге қолжетімділікті күрделендіреді. Тіпті іс қозғалған жағдайда да, күдіктінің деректеріне қол жеткізу айтарлықтай уақыт алады, кейде мүлдем мүмкін болмайды.

Қорытындылай келе, кибергруминг бойынша қылмыстық істі қозғау - бұл дәстүрлі құқық қорғау тәсілдерімен толық қамтыла бермейтін, сандық дәуірдің жаңа қылмыстық формасына бейімделуді талап ететін ерекше процесс. Бұл бағытта Қазақстанға қажетті қадамдар мыналар болуы тиіс:

1. Кибергрумингті Қылмыстық кодексте дербес қылмыстық құрам ретінде енгізу;
2. Істі қозғау үшін ниет пен виртуалды әрекеттердің жеткіліктілігін құқықтық түрде бекіту;
3. Электрондық дәлелдерді жедел алуға мүмкіндік беретін процессуалдық механизмдерді жетілдіру;
4. Киберқылмыстармен айналысатын арнайы мамандандырылған тергеу топтарын құру;
5. Бала жәбірленушілермен жұмыс істеудің стандартталған, психологиялық бейімделген әдістемелерін енгізу.

Кибергрумингке қатысты істерді қозғау мәселесінде Қазақстан Республикасының құқық қорғау тәжірибесінде бірнеше жүйелік түйткіл қалыптасқан. Бұл түйткілдер қылмыстың табиғи күрделілігімен қатар, құқықтық реттеудің жеткіліксіздігі, процессуалдық тетіктердің әлсіздігі, кадрлық және техникалық даярлықтың шектеулілігімен байланысты.

Мәселен, қылмыстық іс қозғау кезеңінде тергеуші ҚПК-нің 179-бабына сәйкес, қылмыстық құқық бұзушылық белгілері бар кез келген хабарлама бойынша тексеру жүргізіп, 3 тәулік ішінде (қажет болса 10 тәулікке дейін

ұзартылып) шешім қабылдауы тиіс. Алайда кибергруминг фактілері бойынша жедел тексеру шаралары кезінде қылмыс құрамының болу-болмауы анықталмаған күйде қалатын жағдайлар жиі кездеседі. Себебі, мұндай әрекеттер әлі физикалық сипаттағы күш қолданумен ұштаспай, тек ниет деңгейінде немесе виртуалды байланыс шеңберінде шектеліп жатады. Бұл құқық қорғау органдарына нақты шешім қабылдауды қиындатады, ал уақыт өткен сайын электрондық іздердің жойылу қаупі артады.

Осыған байланысты ғылыми және тәжірибелік орталарда «виртуалды ықтимал қатер» негізінде іс қозғау стандарты жайлы ойлар туындап отыр. Бұл дегеніміз - тергеуші тек нақты қылмыстық актіге емес, жыныстық сипаттағы ниеттің, әрекетке итермелеудің немесе кәмелетке толмағанды эмоционалды манипуляция арқылы азғыру белгілерінің болуына сүйене отырып іс қозғауы мүмкін. Мұндай көзқарас Батыс Еуропа елдерінде кеңінен таралған. Мысалы, Ұлыбританияда «Sexual communication with a child» бабы бойынша, егер ересек адам жасөспірімге сексуалдық сипаттағы хабарламалар жіберіп, кездесуге шақырса немесе интимдік контент сұраса - бұл факт іс қозғауға жеткілікті деп танылады, жыныстық қатынастың болуы міндетті емес [12].

Қазақстанда осы үлгіге жақындату үшін заңнаманы нақтылау қажет. Қазіргі ҚК 124-бабында «азғыру» ұғымы түсіндіріледі, бірақ ол негізінен нақты ұсыныс немесе әрекетпен байланысты. Алайда кибергрумингте ұсыныс жанама болуы мүмкін: мысалы, «сен ересек сияқтысың», «егер сен мені жақсы көрсең, фотосуретіңді жібер» сияқты фразалар. Мұндай жасырын сексуализацияланған хабарламалар заң тұрғысынан дәлелдеу үшін күрделі, бірақ қылмыскердің ниетін білдіреді. Сондықтан да Қылмыстық кодекске «интернет арқылы жыныстық мақсаттағы байланыс орнатуға талпыну» деген жаңа құқықтық категория енгізу ұсынылады.

Бұған қоса, кибергруминг бойынша істерді қозғауда ерекше мәнге ие фактор - қылмыстық құқық бұзушылық туралы ақпараттың дәлдігі мен қайнар көзі. Қазіргі кезде мұндай істердің едәуір бөлігі ата-аналар немесе мұғалімдер тарапынан келіп түскен хабарламалар негізінде тіркеледі. Алайда бұл - субъективті және кешіктірілген ақпарат көзі. Ең тиімді жол - автоматты мониторинг құралдарын қолдану. Кейбір елдерде, мәселен, Канада мен Израильде, мемлекеттік органдар Google, TikTok және Instagram платформаларымен ынтымақтастық орнатып, балалармен байланыс орнатқан күдікті аккаунттар туралы нақты уақыт режимінде хабарлама алып отырады. Бұл - превентивті құқық қорғау моделі.

Қазақстанда мұндай механизмдер әлі қалыптаспаған. Тергеушілер тек факті бойынша жұмыс істейді. Сондықтан іс қозғау тек реактивті сипатта жүргізіледі, ал алдын алу шаралары жеткіліксіз. Бұл жағдайда мемлекетке IT-компаниялармен келісім негізінде жасөспірімдермен байланыс орнатуға тырысқан күдікті аккаунттар туралы алдын ала хабарландыру жүйесін енгізу тиімді болар еді [25].

Кибергруминг істерін қозғау барысында ерекше назар аударылатын тағы бір мәселе - жәбірленушінің психоэмоционалды жағдайы. Қазақстанда балалар тергеу шараларына қатыстырылған кезде олармен жұмыс істеу үшін заңмен көзделген арнайы психолог немесе педагог маманның қатысуы қажет. Алайда іс жүзінде бұл талап әрдайым орындала бермейді. Жәбірленуші баланың айғақтары - кибергруминг ісіндегі ең маңызды дәлелдердің бірі. Сондықтан оның қатысуымен жүргізілетін процессуалдық әрекеттер кезінде арнайы әдістемелер мен бейімделген сұхбат тәсілдерін қолдану қажет. Мысалы, Оңтүстік Кореяда арнайы «Child Friendly Interview Rooms» құрылып, бала өзіне таныс ортада, ойын формасында, психологиялық қысымсыз жауап береді. Қазақстан да осындай тәжірибені қолдана алады [26].

Кесте 2 - Кибергруминг бойынша қылмыстық істерді қозғаудың ерекшеліктері

№	Ерекшелігі немесе фактор	Сипаттамасы	Қиындық деңгейі	Құқықтық мәні
1	Латенттілік деңгейінің жоғары болуы	Жәбірленушілер өз еркімен арыз бермейді, ұялады, қорқады	Жоғары	Іс қозғау субъективті факторларға тәуелді
2	Құқықтық құрамның болмауы	ҚР ҚК-де кибергруминг нақты қылмыс ретінде танылмаған	Жоғары	Қылмыстық саралауда құқықтық белгісіздік
3	Сандық дәлелдердің сипаты	Скриншот, хат алмасу, медиафайлдар; жойылуы мүмкін	Жоғары	Электрондық дәлелдемелерді бекіту қиындығы
4	Юрисдикциялық шектеулер	Деректер көбіне шетелдік серверлерде сақталады (Meta, Telegram, т.б.)	Орташа	Халықаралық құқықтық көмек қажет
5	Жәбірленушінің жасы мен жағдайы	Бала психологиялық күйзеліске бейім, жауап беруі қиын	Жоғары	Арнайы субъект ретінде құқықтық қорғалуы тиіс
6	Дәлелдеме жинау динамикасы	Қылмыстық байланыс ұзақ уақытқа созылады, үздіксіз байланыс болмайды	Орташа	Қылмыстық ниетті дәлелдеуде уақытша фактор маңызды

7	Тергеу тәжірибесінің әркелкілігі	Тергеушілердің бағалауы, тәжірибесі, техникалық сауаттылығы әртүрлі	Жоғары	Бірыңғай тергеу практикасы жоқ
8	Істі қозғау бастамасының көзі	Ата-ана, педагог, платформа әкімшілігі немесе баланың өзі	Орташа	Ақпараттың дәлдігі мен формасы шешуші фактор
9	Іс қозғау мерзіміндегі кідіріс	Цифрлық дәлел жойылып кетуі мүмкін, жедел шешім қажет	Жоғары	Процессуалдық мерзімді сақтау қиын
10	Құқықтық стандарттың болмауы	Виртуалды ықтимал қатерді қалай бағалау керек екені айқын емес	Жоғары	Қылмыс құрамының қалыптасу шегі анық емес

Сонымен қатар, кибергруминг фактілерін тіркеудің өзі әлі де күрделі мәселе күйінде қалып отыр. Құқық қорғау органдары ішкі статистика жүргізгенімен, бұл қылмыстар нақты түрде "кибергруминг" ретінде бөлек тіркелмейді, олар жалпы жыныстық сипаттағы қылмыстар қатарында есепке алынады. Бұл ғылыми және аналитикалық тұрғыдан бағалау жасауға кедергі келтіреді. Сондықтан Қазақстанда қылмыстық құқықбұзушылықтар тізілімінде «жыныстық сипаттағы киберқылмыстар» деген жаңа санат енгізу - криминологиялық мониторингті жақсартуға мүмкіндік берер еді [27].

Істі қозғау барысында тергеу юрисдикциясының нақты анықталуы да өзекті мәселе болып табылады. Кибергруминг қылмыскерлері VPN, прокси-серверлер, Tor желісі сияқты анонимдеу технологияларын қолданатындықтан, олардың нақты орналасу орнын анықтау - техникалық жағынан күрделі, ал кейде мүмкін емес. Егер қылмыскер шетелде орналасқан болса, іс қозғау Қазақстан аумағында жүзеге аса ма, әлде халықаралық деңгейде сұраныс жолдана ма - бұл сұрақ құқықтық вакуум тудырады. Осы орайда Қазақстан Будапешт конвенциясына қосылса, трансшекаралық ынтымақтастық негізінде істі қозғау мен дәлелдеме жинау әлдеқайда жеңіл болар еді.

Кибергруминг әрекеттері бойынша қылмыстық істерді қозғау — қылмыстық процестің ең жауапты әрі құқықтық мағынада күрделі кезеңдерінің бірі. Бұл қылмыстың цифрлық ортада, яғни көбінесе әлеуметтік желілер мен мессенджерлер сияқты жабық платформаларда жүзеге асырылатыны, ал әрекеттердің көпшілігі латентті сипатқа ие болатыны іс қозғау процесін айтарлықтай қиындатады. Мұндай іс-әрекетті анықтау үшін жедел-іздестіру құралдарының классикалық жиынтығы жеткіліксіз, ал дәлел жинау мен

құқықтық саралау барысында шекарасыздық, дереккөздердің цифрлық сипаты және қылмыстың динамикалық құрылымы құқық қорғау жүйесіне ерекше талаптар қояды [28].

Кибергруминг, әдетте, физикалық қатынасқа ұласқанға дейінгі кезеңде іске асады. Бұл жағдай қылмыстық істі қозғау мәселесінде басты кедергілердің біріне айналады. Себебі, Қазақстан Республикасының Қылмыстық-процессуалдық кодексінің 179-бабында көрсетілгендей, қылмыстық іс тек қылмыстық құқықбұзушылық белгілері анықталған жағдайда ғана қозғалады. Алайда кибергрумингтің бастапқы кезеңінде мұндай белгілердің айқын әрі тікелей көрінісі болмауы мүмкін. Тергеуші көбіне болжамды қасақана ниет пен оның даму процесін ғана тіркейді. Бұл жағдай, өз кезегінде, дәлелдеу шегі мен құқықтық шешім қабылдауға қажетті жеткіліктілік стандартын төмендетеді.

Қылмыстық әрекеттің латенттілігі кибергрумингтің ең маңызды сипаттарының бірі болып табылады. Жәбірленушілердің көпшілігі - жасөспірімдер немесе жас балалар. Олардың психологиялық дайындығы, құқықтық санасы мен әлеуметтік тәжірибесі мұндай әрекетті түсінуге және оның салдарын бағалауға жеткіліксіз болуы мүмкін. Олар көбінесе өзін кінәлі сезінеді, қысым көреді немесе қоғамнан қорқады. Бұл қылмыстың тіркелуін тежейді және құқық қорғау органдарының ақпарат алу мүмкіндігін шектейді. Мұндай жағдайда қылмыстық істі қозғау бастамасы тек жәбірленушінің тарапынан емес, көбіне үшінші тарап - ата-аналар, педагогтар, психологтар немесе интернет платформалар әкімшілігі арқылы жүзеге асады. Алайда бұл сыртқы дереккөздерге тәуелді болу іс қозғау процесінің уақытын ұзартады әрі дәлелдеме жинау жылдамдығын төмендетеді [29].

Процессуалдық тәжірибе көрсеткендей, кибергрумингке қатысты қылмыстық істердің басым бөлігі интернет желісіндегі хат-хабарламалар, аудио және бейнежазбалар, әлеуметтік желідегі әрекеттер арқылы анықталады. Бұл деректердің бәрі цифрлық форматта болғандықтан, оларды заңды түрде алу, тіркеу және процессуалдық дәлелдеме ретінде бекіту үшін нақты рәсімдер қажет. ҚР ҚПК-де цифрлық дәлелдерді қолдану тәртібі нақты реттелмегенімен, электрондық ақпарат құралдарын алу мен қарау 125-бапта бекітілген жалпы нормаларға сүйенеді. Алайда бұл нормалар цифрлық дәлелдердің жылдам жойылып кету қаупін ескере бермейді.

Қылмыстық істі қозғау сатысында тергеу органдары үшін айрықша маңызға ие аспект — бұл істі дұрыс құқықтық саралау. Себебі кибергрумингтің құқықтық құрамы ҚК-де нақты көрсетілмеген. Тергеушілер бұл әрекетті ҚК-нің 124-бабының (кәмелетке толмағанды азғыру), 123-бабының (жыныстық сипаттағы күш қолданбай жасалған әрекеттер), не болмаса 126-бабының (адамды бопсалау) контексінде қарастыруға мәжбүр. Бірақ бұл баптар, негізінен, әрекеттің нәтижесіне — яғни жәбірленушінің қандай да бір нақты әрекетке баруына немесе зиян көруіне негізделген. Кибергрумингтің ерекшелігі сол — мұнда ниет пен процестің өзі қылмыстық мәнге ие болады, ал салдары кейде

материалдық түрде болмауы да мүмкін. Осыдан келіп, дәлелдеме жинау мен істі қозғауға қатысты құқықтық шеңбердің жеткіліксіздігі көрініс табады [30].

Тағы бір күрделі аспект - интернет платформаларынан және IT-компаниялардан қажетті ақпаратты алу мәселесі. Халықаралық юрисдикция шеңберінен тыс орналасқан деректер базасына қол жеткізу көп жағдайда мүмкін болмайды немесе ұзақ уақыт алады. Google, Meta, Apple, Telegram сияқты компаниялар қолданушылардың құпиялығын алға тартып, қылмыстық істер бойынша мәлімет беруден бас тартады немесе тек халықаралық келісімдер негізінде ғана әрекет етеді. Қазақстанның мұндай жағдайларда әрекет ету мүмкіндігі шектеулі болғандықтан, қылмыстық іс қозғау процессі де кідірістерге ұшырайды.

Кейбір жағдайларда тергеушілер іске қажет деректерді жәбірленуші мен оның ата-анасының ұсынған скриншоттары, хаттар немесе жадта сақталған фотосуреттер арқылы алады. Бірақ бұл дәлелдердің процесуалдық мәртебесі құқықтық тұрғыдан әрдайым тең деп танылмайды. Себебі олар өзгертілуі немесе қолдан жасалуы мүмкін деген күмән тудыруы мүмкін. Сондықтан іс қозғау кезінде тергеуші мұндай дәлелдерді сот-сараптама мекемелерінің растауын қажет етеді, бұл қосымша уақыт пен ресурстар талап етеді [31].

Іс қозғау кезеңінде тағы бір өзекті проблема — қылмыстық қудалау органының іс-әрекетінің стандартталмағандығы. Әр түрлі аумақтық құрылымдарда тергеушілердің іс-қимылы мен бағалау деңгейі біркелкі емес, бұл қылмыстық істерді қозғау бойынша бірыңғай тәжірибенің қалыптаспауына алып келеді. Бір тергеуші бірдей іс-әрекетті «қылмыстық ниет» деп таныса, басқа тергеуші мұны «құқық бұзушылық емес, моральдық этикаға жат әрекет» деп бағалауы мүмкін. Бұл - қылмыстың дәл сол сипатта бір өңірде тіркеліп, екінші өңірде тіркелмеуіне әкелетін қылмыстық қудалау теңсіздігі. Мұндай тәжірибе қылмыстың шынайы статистикасын бұрмалап, латенттіліктің ұлғаюына әсер етеді [32].

Қылмыстық істі қозғау процесінің тағы бір елеулі ерекшелігі — бұл кибергруминг әрекеттерінің дәлелдемелік мазмұнының динамикасы. Басқа қылмыстарда оқиға болған орны мен уақыты нақты белгіленсе, кибергруминг жағдайында байланыс виртуалды болғандықтан, ол бірнеше күн, апта немесе айға созылуы мүмкін. Бұл іс жүргізу мерзімін бағалауға, дәлелдемелердің релеванттылығын анықтауға, әрекеттер арасындағы себеп-салдар байланысын орнатуға кедергі келтіреді. Тергеу материалдарында байланыстың үзілуі, платформаның ауысуы немесе чаттардағы жазбалардың өшірілуі - дәлелдеу процесіне нұқсан келтіретін қосымша факторлар.

Кибергруминг бойынша қылмыстық істі қозғау — бұл тек процесуалдық акт қана емес, ол тергеу органдарының қылмыстық ниетті ерте кезеңде тану, құқықтық контекстті дұрыс бағалау, цифрлық дәлелдерді жинау және сақтау, жәбірленушінің жас ерекшелігіне бейімделген құқықтық тактиканы қолдану сияқты кешенді әрекеттерді қамтитын көп деңгейлі үдеріс болып табылады. Бұл кезеңдегі кез келген қателік қылмыстың толық ашылмауына, қылмыскердің

жауаптылықтан жалтаруына немесе жәбірленушінің қосымша психологиялық зақым алуына алып келуі мүмкін. Сол себепті кибергрумингке байланысты істерді қозғау тәжірибесі — құқық қорғау жүйесінің технологиялық және құқықтық бейімделуінің маңызды индикаторы ретінде қарастырылуы тиіс [33].

2.2 Сандық дәлелдемелерді жинау және талдау әдістері

Кибергрумингке байланысты қылмыстық істердің ерекшелігі - олардың басым бөлігі тек виртуалды кеңістікте жүзеге асырылуында. Бұл жағдай тергеу процесінде дәстүрлі дәлелдемелерге емес, ең алдымен сандық (электрондық) дәлелдемелерге жүгінуді талап етеді. Сандық дәлелдемелер - бұл киберқылмыстың ізін анықтаудың, әрекет ету фактісін дәлелдеудің, қылмыскердің тұлғасын және жәбірленушімен байланысын ашудың басты құралы. Осыған байланысты кибергруминг істерін тергеуде дәл осы сандық іздермен жұмыс істеудің әдістемесі мен құқықтық регламенттері ерекше маңызға ие.

Сандық дәлелдеме ұғымы қазіргі қылмыстық іс жүргізу жүйесінде әлі де қалыптасу үстінде. ҚР ҚПК-де бұл ұғым нақты заңдық категория ретінде берілмегенімен, заңда электрондық ақпарат құралдарына қатысты арнайы тергеу әрекеттері сипатталады. Сандық дәлелдемелердің кең мағынасы - бұл тергеуге маңызы бар, цифрлық түрде сақталған және арнайы техникалық құралдармен алынатын ақпарат. Оларға: электрондық хат алмасу, әлеуметтік желідегі жазбалар, мессенджердегі хабарламалар, фотосуреттер, бейнематериалдар, құрылғылардан алынған логтар, IP-адрестер, браузер тарихы және интернет-трафик туралы мәліметтер жатады.

Кибергрумингке тән қылмыстық байланыс көбінесе Facebook, Instagram, WhatsApp, Telegram, TikTok, Omegle сияқты платформаларда жүзеге асырылады. Қылмыскерлер мен жәбірленушілердің арасындағы коммуникация жазбаша хат алмасу түрінде, кейде аудио немесе бейнеқоңырау форматында жүреді. Тергеуші үшін басты міндет - осы байланыстарды дәлел ретінде бекітіп, олардың шынайылығын, өзгертілмегенін және заңды жолмен алынғанын қамтамасыз ету.

Сандық дәлелдемелермен жұмыс істеу үш негізгі кезеңнен тұрады: (1) жинау, (2) сақтау және бекіту, (3) талдау және бағалау. (кесте 3)

1. Жинау. Сандық дәлелдемелерді жинау қылмыстық іс жүргізудің бастапқы кезеңінен бастап басталады. Ол көбінесе жәбірленушінің немесе оның ата-анасының ұсынған скриншоттары, хат жазбалары арқылы басталуы мүмкін. Дегенмен, бұл дәлелдердің процессуалдық мәртебесін қамтамасыз ету үшін оларды арнайы процессуалдық әрекет аясында алу талап етіледі. Мысалы, құрылғыны (смартфон, планшет, компьютер) алу және тексеру ҚПК-нің 218-бабы бойынша тінту немесе алу хаттамасы арқылы рәсімделеді. Бұл кезде құрылғының тұтастығы мен деректердің бастапқы күйі арнайы техникалық құралдар арқылы бекітілуі тиіс - мысалы, хэш-кодтар есептеледі.

Егер қылмыстық байланыс әлеуметтік желі немесе мессенджер арқылы жүзеге асырылған болса, тергеуші құқық қорғау органдары атынан тиісті платформаларға ақпараттық сұраныс жолдайды. Бірақ Meta, Google, Telegram секілді трансұлттық компаниялар бұл сұраныстарға тек халықаралық құқықтық көмек көрсету аясында немесе өздерінің ішкі саясатына сай ғана жауап береді. Бұл - дәлел жинаудың уақытын кешіктіреді әрі олардың толық болмауына себеп болады. Көптеген жағдайларда тергеу органдары қолданушының өз құрылғысынан немесе браузер кэшінен қалған іздерді іздеуге мәжбүр болады [34].

2. Сақтау және бекіту. Сандық дәлелдемелердің дәлдігін қамтамасыз ету үшін оларды жинаған сәттен бастап бұзылмайтындай етіп сақтау - аса маңызды. Әрбір цифрлық файлдың метадеректері (құрылған күні, өңделген уақыты, құрылғы атауы, файл өлшемі және т.б.) тергеу үшін аса маңызды. Бұл деректерді сақтау үшін арнайы бағдарламалық құралдар - EnCase, FTK Imager, Magnet AXIOM сияқты киберсараптау бағдарламалары қолданылады. Бұл бағдарламалар тергеушіге құрылғының немесе сервердің барлық ақпаратын бейтарап түрде көшіріп алуға және оны кейінгі сараптама үшін пайдалануға мүмкіндік береді.

Көп жағдайда дәлелдемелер бұлтты серверлерде сақталады (Google Drive, iCloud, Dropbox және т.б.), оларды алу үшін авторизация қажет, бұл жағдайда ақпаратты жәбірленушінің өзі немесе сот санкциясы негізінде сұратуға болады. Осы кезде сандық дәлелдемелердің дереккөзін растау - олардың заңдылығын қамтамасыз етудің басты кепілі болып табылады. Мұндай дәлелдемелер сотта қабылдануы үшін, олардың заңды жолмен алынғаны және шынайылығы күмән тудырмауы тиіс.

3. Талдау және бағалау. Сандық дәлелдемелерді жинап, бекіткеннен кейінгі келесі маңызды кезең - оларды криминалистикалық талдау. Бұл процесс тек техникалық емес, құқықтық және психологиялық мәнге де ие. Кибергрумингке тән әрекеттер — балаға сенім білдіру, интимдік сипаттағы хабарлама жіберу, кездесуге итермелеу — бәрі мәтін ішінде жанама формада берілуі мүмкін. Сондықтан сандық дәлелдемелердің мәтіндік мазмұнын семантикалық және психолингвистикалық сараптама арқылы талдау қажет болады. Бұл сараптама күдіктінің қылмыстық ниетін, хабарламалардың астарлы мағынасын және баланың қабылдау ерекшелігін түсінуге мүмкіндік береді.

Кейбір жағдайларда бейнежазбалар немесе фотосуреттер қосымша дәлел ретінде ұсынылады. Бұл жағдайда файлдардың шығу тегі, олардың монтаждалмағаны, өңделмегені техникалық сараптама арқылы дәлелденуі тиіс. Сандық дәлелдердің шынайылығын растайтын тағы бір маңызды құрал - IP-адрес арқылы геолокация. Егер қылмыскер өз аккаунтын жасырын түрде қолданса да, белгілі бір IP-адресті тіркеу арқылы оның нақты орналасқан жерін анықтау мүмкіндігі бар [35].

Кесте 3 - Сандық дәлелдемелерді жинау және талдау әдістері

№	Процесс кезеңі	Негізгі әрекеттері	Қиындықтар / Тәуекелдер	Құқықтық негіз / Процессуалдық мәні
1	Жинау	Электрондық хаттар, мессенджерлердегі чаттар, скриншоттар, файлдар, IP-адрес, логтар алу	Жойылу қаупі, шетелдік серверлерге қол жеткізудің қиындығы	ҚР ҚПК; тінту, алу, сұраныс жолдау
2	Сақтау және бекіту	Дәлелдерді техникалық құралмен бекіту (FTK, EnCase, Magnet), хэш-функциялар есептеу	Өзгертілуі немесе бұрмалануы мүмкін	Электрондық дәлелдердің аутентификациясын талап етеді
3	Сараптамалық өңдеу	Метадеректер, файл тарихы, құрылғы ID-лары, уақыт коды, браузер логтары арқылы талдау жүргізу	Арнайы IT-сарапшының қажеттілігі, техникалық дайындық керек	Цифрлық криминалистика әдістері
4	Лингвистикалық талдау	Хат мазмұнындағы азғыру белгілерін анықтау, сөздердің контекстуалды сипатын бағалау	Субъективтік интерпретацияның ықтималдығы	Психолингвистикалық сараптама
5	Заңдылықты қамтамасыз ету	Дәлелдерді процессуалдық рәсімдермен заңдастыру (хаттамалар, сараптама актілері)	Заңсыз алынған дәлел сотта жарамсыз деп танылуы мүмкін	ҚР ҚПК 112-125-баптар

6	Соттағы қолданылуы	Дәлел ретінде ұсыну, оның сенімділігін қорғау, күмән келтірмеу	Файлдың өзгертілуі/авторсыздығы дәлел күшін әлсіретуі мүмкін	Дәлелдемелік стандарттар мен құқықтық тәртіп
7	Халықаралық аспектілер	Шетелдік платформалардан (Meta, Google, Apple) ақпарат сұрату	Уақытша кідіріс, дереккөзге қол жеткізбеу	Сот-құқықтық көмек туралы келісімдерге тәуелділік
8	Уақыт факторымен жұмыс	Электрондық іздердің жоғалуын болдырмау, кешікпей әрекет ету	Скриншоттардың кеш жіберілуі немесе деректердің өшірілуі	Жеделдік қағидаты

Сандық дәлелдемелердің құқықтық табиғаты ерекше. Олар физикалық объект емес, ақпараттық объект ретінде бағаланады. Бұл олардың дәлел ретіндегі қабылдануын өзгеше сипаттайды. Дәлел ретінде пайдаланылатын әрбір электрондық файлдың — қай құрылғыдан алынғаны, қалай алынғаны, қашан және кіммен бекітілгені — барлық осы факторлар процессуалдық заңдылық тұрғысынан айрықша маңызға ие.

Сондай-ақ, сандық дәлелдемелермен жұмыс істеуде уақыт факторына баса назар аударылады. Электрондық жазбалар кейде автоматты түрде өшіп кетуі мүмкін, ал кейбір платформалар пайдаланушының сұрауымен деректерді жоя алады. Осы себепті тергеуші цифрлық іздерді жинауда жедел әрекет етуге міндетті. Кешігу немесе кідіріс құнды дәлелдердің жоғалуына әкелуі мүмкін.

Кейбір жағдайларда тергеуші дәлел ретінде цифрлық құрылғылардың ішкі деректерін (мысалы, cookie-файлдар, браузер тарихы, log-файлдар, қолданба метадеректері) қолданады. Бұл элементтер адам мінез-құлқын талдауға, қылмыскер мен жәбірленушінің байланыс жиілігін, уақыты мен сипатын анықтауға мүмкіндік береді. Әсіресе, кибергруминг істерінде «жүйелі байланыс» дәлел ретінде маңызды: хабарламалардың жиілігі, мағынасы және дамуы қылмыстық ниеттің бар екеніне жанама дәлел бола алады.

Сонымен қатар, сандық дәлелдемелер кибертергеу барысында басқа дәлелдемелермен кешенді байланыста қарастырылуы тиіс. Мысалы, жәбірленушінің берген айғақтары мен құрылғыдан алынған хат алмасу арасындағы сәйкестік - дәлелдің сенімділігін арттырады. Ал егер жәбірленуші ескі құрылғыны жоғалтып алған болса, платформаның серверлік жазбаларына жүгіну - балама шешім болады [36].

Сандық дәлелдемелер кибергруминг қылмыстарын дәлелдеудің негізгі құралы болғанымен, олардың құқықтық мәртебесі мен дәлелдемелік салмағы

қылмыстық іс жүргізуде бірқатар күрделі сұрақтар туындатады. Бұл, ең алдымен, олардың ақпараттық, өзгертілуі мүмкін сипатымен және дәстүрлі дәлелдемелерден айырмашылығы бар процестік табиғатымен байланысты. Мұндай дәлелдемелердің заңдылығын қамтамасыз ету үшін оларды жинау, сақтау және талдау әрекеттері нақты процессуалдық тәртіпке сәйкес жүзеге асырылуы тиіс.

ҚР ҚПК-де «сандық дәлелдеме» ұғымы терминологиялық түрде бекітілмегенімен, 125-бап және басқа да баптар шеңберінде электрондық ақпарат құралдарын қолдану, алу және процессуалдық тіркеу ережелері жанама түрде регламенттеледі. Алайда бұл нормативтік база халықаралық тәжірибеге қарағанда толыққанды әрі егжей-тегжейлі сипатқа ие емес. Соның салдарынан тергеу мен сот тәжірибесінде бірізділік жетіспейді. Бір өңірде белгілі бір сандық файл сотта дәлел ретінде қабылданса, басқа өңірде дәл сол файл дәлел ретінде есепке алынбауы мүмкін. Бұл сандық дәлелдемелердің құқықтық бағалауында субъективизм мен процестік еркіндіктің кеңдігіне әкеледі.

Сандық дәлелдемелердің сотта қолданылу мәселесі - олардың дәлелдемелік күшін анықтау сұрағын туындатады. Қылмыстық іс жүргізу теориясы бойынша, кез келген дәлелдеме мынадай критерийлерге сай келуі керек: заңдылық, жарамдылық, сенімділік, дәлелдемелік мән. Сандық дәлелдемелер осы талаптардың әрқайсысына жеке-жеке жауап беруі тиіс. Алайда олардың өзгертілу мүмкіндігі, бастапқы дереккөздің шынайылығын растаудың техникалық күрделілігі мен деректерді өңдеу тізбегінің ашық болмауы - дәлелдеменің сенімділігіне күмән келтіруі мүмкін. Мысалы, скриншот өздігінен дәлел ретінде қаралмайды, егер ол техникалық тұрғыдан расталмаса - яғни, оның дереккөзін, құрылғыны, авторды және хронологияны дәлелдеу мүмкін болмаса, ол сотта қабылданбай қалуы ықтимал [37].

Бұл жағдайлар құқық қорғау тәжірибесінде сандық дәлелдемелердің аутентификация ұғымын өзекті етеді. Аутентификация - бұл файлдың өзгертілмегенін, оның түпнұсқа екенін және нақты қылмыстық оқиғаға қатысты екенін техникалық және процессуалдық жолмен дәлелдеу процесі. Аутентификация үшін хэш-функциялар, лог-файлдардың тарихы, метадеректер, құрылғы журналдары және серверлік деректер жиі қолданылады. Алайда бұл тәсілдер арнаулы техникалық білім мен ресурсты талап етеді. Тергеушілер немесе сарапшылар сандық іздерді іздеу мен бекіту кезінде арнайы құралдарды - мысалы, FTK, EnCase, X-Ways Forensics, Magnet AXIOM секілді бағдарламаларды қолдануға мәжбүр.

Тағы бір маңызды аспект - сандық дәлелдемелерді алу мен ұсыну форматының бірізділігі. ҚР ҚПК мұндай материалдарды істің материалдарына енгізу үшін хаттамалармен бекіту қажет екенін анық көрсетеді. Бұл дегеніміз: әрбір цифрлық файл (мысалы, Telegram чаты, Instagram-дағы хат алмасу, бейнежазба) тергеуші тарапынан ресми түрде қаралып, процессуалдық құжатпен (хаттама, сараптама қорытындысы, сұраныс жауабы және т.б.) рәсімделуі керек.

Егер бұл тәртіп бұзылса немесе дәлел көзінің алынуы күмән тудырса - сот ондай деректі қабылдамауы мүмкін.

Сандық дәлелдемелердің құқықтық табиғаты Қазақстанның қолданыстағы құқық жүйесінде ерекше. Бұл дәлелдемелер классикалық түсініктегі "заттай дәлелдемеден" өзгеше. Олар - виртуалды, дискретті, ақпараттық құрылым. Демек, оларды бағалау да дәстүрлі тәсілдермен емес, кешенді, технологиялық-құқықтық өлшемдермен жүзеге асырылуы тиіс. Бұл жерде қылмыстың күрделілігі мен тергеудің сапасы тікелей техникалық базаның жеткіліктілігіне, тергеушілер мен сарапшылардың IT-салада бағдарлау деңгейіне байланысты болады [38].

Сот тәжірибесінде де сандық дәлелдемелердің рөлі күннен-күнге артып келеді. Кибергруминг істері бойынша соттарда шешім қабылдау барысында дәл осы электрондық файлдар мен байланыс логтары шешуші рөл атқарады. Мысалы, белгілі бір істің шешімі тек хат алмасудың мазмұнына сүйеніп қабылдануы мүмкін. Бұл ретте судья дәлелдің тек мазмұнын ғана емес, оның пайда болу контексін, тілдік құрылымын, эмоционалдық реңкін де ескереді. Осыған байланысты лингвистикалық және психологиялық сараптама түрлері сандық дәлелдемелерге қосымша сипат береді. Бұл әсіресе бала жәбірленушіге жасалған ықпалдың деңгейін және теріс әсерін дәлелдеуде маңызды.

Цифрлық дәлелдерді сотқа дейінгі тергеу кезінде жинақтау кезінде технологиялық бейтараптық қағидаты да сақталуы тиіс. Бұл қағидат - дәлелді жинау барысында қолданылған техникалық құралдардың құқықтық процеске әсер етпейтіндігін білдіреді. Мәселен, дәлел EnCase немесе басқа лицензиялық емес бағдарлама арқылы алынған болса, бірақ оның шынайылығы мен техникалық дұрыстығы дәлелденсе - ондай файл да сотта жарамды деп танылуы мүмкін. Бұл технологиялардың көптүрлілігін мойындау және құқықтық жүйенің оған икемделу қажеттігін білдіреді.

Қылмыстық процесс тұрғысынан алғанда, сандық дәлелдемелердің өзіне тән ерекшелігі - оның көпқабатты мәнінде. Бір ғана файл бірнеше дереккөздің орнына жүруі мүмкін: ол әрі заттай дәлел, әрі куәлік, әрі контекстуалды дәлел бола алады. Мысалы, жәбірленуші мен күдікті арасындағы хат алмасу: оның мәтіні - субъективті қарым-қатынас фактісі, лог-файлы - нақты уақыт пен IP-адрестің дәлелі, ал тіркелген скриншоттар - визуалды мазмұнды дәлел. Бұл күрделілік электрондық дәлелдемелерді кешенді қараудың маңыздылығын арттырады.

Ақпараттың цифрлық сипаты оны тарату, көшіру және өзгерту мүмкіндігін жеңілдетеді. Бұл фактор кейде қылмыстық процесте сандық дәлелдерді бұрмалау тәуекелін тудырады. Осындай жағдайларда сараптамалық институттардың дербес рөлі артады. Сарапшының қорытындысы, яғни файлдың түпнұсқалығы, құрылымдық тұтастығы және өзгертілмеуі туралы дәлелі - сот үшін басты бағдар болуы мүмкін. Сараптамалық зерттеу нәтижесінде дәлелдің процессуалдық жарамдылығы бекітіледі.

Кибергруминг қылмыстарының трансшекаралық сипаты сандық дәлелдемелерді алудағы халықаралық әріптестік мәселесін де өзекті етеді. Егер платформа шетел юрисдикциясында орналасса, Қазақстан тарапы сот-құқықтық көмек көрсету туралы халықаралық келісімдерге сүйенуі тиіс. Бұл жағдайда дәлелдерді алуға сұраныс дипломатиялық жолмен немесе халықаралық процедуралар арқылы жүзеге асырылады. Осы кезеңде уақыт факторы және халықаралық нормалардың үйлесімділігі тергеу тиімділігіне тікелей әсер етеді.

2.3 Құқық қорғау органдарының интернет-платформалармен өзара әрекеттестігі

Цифрлық технологиялар кеңістігінде кибергруминг секілді қылмыстардың негізгі платформасы ретінде әлеуметтік желілер мен мессенджерлер қызмет етеді. Қылмыстық әрекеттердің виртуалды ортада, көп жағдайда трансұлттық юрисдикция шеңберінде орын алуы құқық қорғау органдарының жұмысын жаңа деңгейге шығарды. Бұл жағдай, бір жағынан, тергеу және жедел-іздестіру мүмкіндіктерін кеңейтсе, екінші жағынан - оларды күрделендіреді. Осы тұрғыдан алғанда, құқық қорғау органдары мен интернет-платформалар арасындағы өзара әрекеттестік киберқылмыстардың ашылу және дәлелдену тиімділігінің маңызды факторы болып табылады.

Қазақстан Республикасының қылмыстық-процестуалдық заңнамасы интернет-платформалармен өзара әрекеттестік мәселесін жанама түрде ғана реттейді. Яғни, тергеу органына қажетті ақпарат алу үшін тек сұраныс хаттар мен сот санкциясы шеңберінде әрекет етуге рұқсат берілген. Алайда, мұндай сұраныстардың орындалуы - интернет-платформаның юрисдикциясына, ішкі саясатына және халықаралық құқықтық міндеттемелерге тәуелді. Көптеген ірі технологиялық компаниялар - Meta (Facebook, Instagram), Google (Gmail, YouTube), Apple, Telegram және т.б. - Қазақстан аумағында тіркелмеген және олардың өкілдіктері жоқ. Бұл өз кезегінде сұраныстардың орындалуын күрделендіреді немесе мүлдем мүмкін емес етеді.

Бұдан бөлек, аталған платформалар деректерді беру туралы сұраныстарды тек белгілі бір халықаралық құқықтық негізде қарастырады. Мұндай негіздердің қатарына Будапешт конвенциясы, Еуропа Кеңесінің киберқылмысқа қарсы келісімдері немесе екіжақты құқықтық көмек шарттары жатады. Қазақстан бұл ретте Будапешт конвенциясына қосылмағандықтан, ішкі тергеу органдары көптеген сұраныстарды тек дипломатиялық немесе дипломатиялық емес жолмен, баяу және күрделі тәртіппен жүзеге асыруға мәжбүр болады. Бұл - кибергруминг секілді жедел әрекет етуді талап ететін қылмыстар үшін елеулі қауіп.

Практика көрсеткендей, интернет-платформалармен әрекеттестік келесі бағыттар бойынша жүзеге асырылады:

1. Қылмыстық істер бойынша ақпарат алу - бұл сұраныстар хат-хабар алмасу, аккаунт иесінің IP-адресі, құрылғысы, логтар және геолокация туралы мәліметтерді қамтуы мүмкін.

2. Күмәнді контентті бұғаттау немесе жою - әсіресе, жәбірленушінің интимдік фотосуреттері немесе балалар порнографиясы таралған жағдайда.

3. Аккаунттарды уақытша тоқтату немесе сақтау - дәлелдемелер жойылып кетпес үшін процессуалдық шара ретінде қолданылады.

Бұл әрекеттердің барлығы нақты нормативтік база мен техникалық хат алмасуға тәуелді. Алайда платформалар қолданушылардың жеке деректерін қорғауды басымдық санайды және тек ауыр қылмыстар бойынша, көбіне сот шешімі негізінде ғана дерек ұсынады. Мысалы, Meta компаниясы өзінің Transparency Report есебінде Қазақстаннан түскен сұраныстардың тек аз бөлігіне ғана жауап беретінін және дерек беруден жиі бас тартатынын көрсеткен.

Telegram сияқты кейбір платформалар пайдаланушының құпиялылығы мен шифрлауды басты құндылық ретінде санап, құқық қорғау органдарына ешқандай дерек бермейтін саясат ұстанады. Бұл әсіресе кибергруминг жағдайында - қылмыскер мен құрбан арасындағы жазбалар құпия түрде, «secret chat» немесе «self-destruct» функциялары арқылы жүргізілетіндіктен - тергеуді жүргізуді айтарлықтай қиындатады.

Осыған байланысты құқық қорғау органдары шын мәнінде өзара әрекеттестікке емес, күрделі делдалдыққа жүгінеді. Яғни, интернет-компаниялармен тікелей байланыс орнына, көп жағдайда Google Transparency Team, Facebook Law Enforcement Portal сияқты арнайы жүйелер арқылы ақпарат сұрауға мәжбүр. Бұл жүйелерде тек ағылшын тілінде әрекет етуге, халықаралық заңнаманы білуге, формалды талаптарды сақтауға дайын тергеушілер ғана табысты жұмыс істей алады. Алайда мұндай дайындық деңгейі Қазақстанда барлық деңгейдегі тергеу құрылымдарында бірдей емес.

Батыс елдерінде, мысалы Германия, Ұлыбритания, Нидерландыда құқық қорғау органдары мен ірі IT-компаниялар арасында тұрақты байланыс жүйелері, соның ішінде реагенттік топтар, API-доступ және «төменгі шекті» жедел жауап хаттамалары енгізілген. Бұл жүйелерде нақты бір жағдайға байланысты сұраныс түскенде, бірнеше сағат ішінде деректер беріледі немесе әрекет жасалады. Бұл - жеделдік қағидатын толық сақтауға мүмкіндік береді.

Қазақстанның бұл бағыттағы ахуалы өзгеше. Тергеушілердің мүмкіндіктері шектеулі, өйткені қолданыстағы құқықтық база платформа әкімшілігіне ықпал ету немесе олармен келіссөз жүргізу құралдарын бермейді. Ақпаратты жедел алу мүмкін болмаған жағдайда тергеу мерзімдері кешіктіріледі, дәлелдемелер жоғалады немесе кибергруминг әрекетінің жалғасуына жол беріледі.

Сондай-ақ, қазіргі кезде Қазақстанда балаларды интернетте қорғауға бағытталған ұлттық деңгейде жұмыс істейтін уәкілетті орган немесе орталықтандырылған мониторинг жүйесі жоқ. Көптеген елдерде балаларға қарсы цифрлық қылмыстарды ерте кезеңде анықтау үшін «CyberTipline» (АҚШ),

«INHOPE» (ЕО) сияқты құрылымдар мен платформалар жұмыс істейді. Олар IT-компаниялардан келіп түскен дабыл белгілерін өңдеп, оны құқық қорғау органдарына жедел бағыттайды. Мұндай механизм Қазақстанда әзірге қарастырылмаған.

Қосымша ескерер жайт - қазіргі интернет-платформалардың автоматты фильтрация және контент анықтау алгоритмдерінің сапасы мен тиімділігі әртүрлі. Жыныстық сипаттағы хат-хабарламаларды автоматты түрде анықтау үшін нейрожелілер мен машиналық оқыту технологиялары қолданылса да, бұл жүйелер баланың нақты жәбірленуші ретіндегі жағдайын тани алмайды. Яғни, адам тарапынан сараптама жасалмаса, алгоритм көп жағдайда қауіпті контентті өткізіп жіберуі немесе, керісінше, зиянсыз хабарламаларды бұғаттауы мүмкін.

Цифрлық кеңістікте кибергруминг қылмыстарының көбеюі құқық қорғау органдары мен интернет-компаниялар арасындағы өзара әрекеттестікке жаңа институционалдық тәсілдерді қажет етеді. Себебі бұл қылмыстың сипаты - интерактивті, жасырын, динамикалық. Қылмыскерлер әртүрлі платформалар арасында оңай ауысып отырады, жалған аккаунттар ашады, VPN немесе шифрланған арналар пайдаланады. Бұл құқық қорғау органдарының реактивті емес, проактивті жұмыс істеуін талап етеді. Бірақ мұндай жұмысқа құқықтық база мен техникалық ресурстар жетіспейді.

Құқық қорғау органдары мен интернет-платформалар арасындағы өзара әрекеттестіктің қазіргі күйі кибергруминг сияқты жоғары латенттілікке ие қылмыстарды ашуда елеулі кедергілер туындататыны даусыз. Себебі бұл қылмыстық әрекет дәстүрлі қоғамдық кеңістікте емес, жеке, сандық және алгоритмдермен реттелетін ортада жүзеге асады. Мұндай жағдайларда құқық қорғау құрылымдарына жүктелетін міндет тек тергеу жүргізу ғана емес, сонымен қатар күрделі цифрлық инфрақұрылыммен әрекеттесу қажеттілігін де қамтиды.

Алайда тергеу органдарының құқықтық және техникалық әлеуеті платформа әкімшіліктерінің ішкі саясаты мен техникалық архитектурасына тәуелді болып қалуда. Ірі технологиялық компаниялар (Big Tech) — Meta, Google, TikTok, Apple және Telegram сияқты — өздерінің дербес деректерді сақтау, қорғау және ұсыну стандарттарын ұлттық заңнамадан гөрі халықаралық немесе корпоративтік актілер арқылы реттейді. Бұл компаниялардың заңды жауап беруі немесе ақпарат ұсыну туралы сұраныстарға реакциясы көбінесе АҚШ заңнамасына (мысалы, Stored Communications Act) немесе Еуроодақтың Жалпы деректерді қорғау регламентіне (GDPR) тәуелді. Мұндай асимметриялық құқықтық реттеу ұлттық юрисдикцияны жүзеге асыруды шектейді, бұл әсіресе Қазақстан сияқты цифрлық егемендігін енді ғана дамытып жатқан елдер үшін үлкен мәселе.

Осы контексте құқық қорғау органдары көбінесе тергеу жүргізудің классикалық әдістерінен тыс әрекеттерге жүгінуге мәжбүр болады. Мысалы, кейбір жағдайларда тергеушілер жәбірленушінің құрылғысына тікелей кіру арқылы әлеуметтік желідегі хат-хабар алмасуды скриншоттау, бейнежазба жасау немесе сыртқы жадқа көшіру тәсілін қолданады. Алайда бұл тәсілдер

дәлелдемелердің шынайылығына күмән келтіріп, олардың сотта жарамдылығына қауіп төндіреді. Мұндай жағдайда дәлелдеменің заңдылығын қамтамасыз ету тек процессуалдық рәсімдердің қатаң сақталуына байланысты болады.

Интернет-платформалармен әрекеттесу барысында ақпараттың құқықтық мәртебесі де әрқашан нақты бола бермейді. Қылмыстық іс жүргізу тәжірибесінде жиналған деректерді дәлел ретінде пайдалану үшін олар нақты қай дереккөзден алынғаны, қандай жолмен алынғаны, кіммен расталғаны және қай уақытта бекітілгені анықталуы тиіс. Егер бұл талаптар сақталмаса, дәлелдемелер "жарамсыз" деп танылып, істің дәлелдеу базасына енгізілмеуі мүмкін. Әсіресе, сандық кеңістікте алынған материалдардың түпнұсқалығын анықтау - ең күрделі мәселелердің бірі.

Цифрлық іздермен жұмыс істеу барысында құқық қорғау органдары көп жағдайда бірнеше платформамен қатар әрекеттесу қажеттілігіне тап болады. Себебі қазіргі қылмыскерлер байланысу үшін тек бір ғана қосымшаны қолданбайды, олар бірнеше платформа арасында оңай ауысып, қылмыстық ізді жасыру мақсатында виртуалды «мозаикалық коммуникация» құрайды. Бұл құбылыс тергеу барысында әр платформаға жеке сұраныс жолдауды, олардың әртүрлі жауап беру форматына бейімделуді және жиналған ақпаратты біріктіріп талдау қабілетін талап етеді. Яғни тергеу процесі классикалық сызықты моделден көп арналы, тармақталған құрылымға айналады.

Интернет-платформалармен әрекеттестік мәселесінің тағы бір елеулі аспектісі — бұл уақыт пен процедура арасындағы қайшылық. Тергеу барысында жедел әрекет етуді талап ететін сәттер жиі туындайды. Мысалы, жәбірленушінің жеке фотосуреті Telegram арнасында жарияланған жағдайда оны мүмкіндігінше тез бұғаттау қажет. Бірақ мұндай әрекеттер үшін көп жағдайда сот санкциясы немесе халықаралық сұраныс қажет етіледі, ал бұл бірнеше аптаға созылуы мүмкін. Осы аралықта дәлел жойылуы, ақпарат таралуы немесе қылмыскер әрекетін жалғастыруы мүмкін. Бұл - жеделдіктің процессуалдық заңдылықпен қайшы келетінін көрсететін нақты мысал.

Сонымен қатар, қазіргі интернет-платформалардың алгоритмдік басқару сипаты тергеу әрекеттеріне қосымша тосқауылдар туғызады. Әлеуметтік желілердің көпшілігі қолданушыларға арналған «end-to-end encryption» (соңғыдан соңғыға дейін шифрлау) технологиясын пайдаланады. Бұл технология деректерді тек жіберуші мен алушы ғана оқи алатындай етіп шифрлайды, ал платформаның өзі де бұл хабарламалардың мазмұнын көре алмайды. Осы себепті құқық қорғау органдары қылмыскер мен жәбірленушінің арасындағы нақты диалогты анықтай алмай, сандық дәлелдерден айырылып қалады. Бұл тек құқықтық емес, техникалық сипаттағы шектеу болғандықтан, оны жеңу үшін халықаралық деңгейде криптографиялық реттеу нормалары талап етіледі.

Мұндай жағдайда құқық қорғау органдары мен платформалар арасындағы өзара әрекеттестік біржақты құқықтық реттеуге бағынбайтын, әрбір платформа мен мемлекет арасындағы саяси, дипломатиялық және экономикалық

келісімдерге тәуелді құбылысқа айналады. Демек, бұл қарым-қатынасты тек құқықтық планда ғана емес, цифрлық егемендік және ақпараттық қауіпсіздік контекстінде қарастыру қажет. Мемлекеттің ақпараттық кеңістікті бақылау мүмкіндігі тек заңмен ғана емес, сонымен қатар техникалық және институционалдық құралдармен де анықталады.

Осы шындықтарды ескере отырып, құқық қорғау органдарының интернет-платформалармен әрекеттесу жүйесі қазіргі уақытта формалды-кеңестік сипатта қалуда. Яғни сұраныс жіберу, жауап алу, сот санкциясын күту — бұның бәрі ұзақ әрі бюрократиялық тізбекте қалып отыр. Бұл жағдай киберқылмыстардың, әсіресе кәмелетке толмағандарға қарсы бағытталған әрекеттердің дер кезінде ашылмауына, кейде мүлдем тіркелмей қалуына алып келеді. Ал тергеу процесінде уақытша кідірістер — дәлелдердің жойылуына, куәгерлердің ұмытшақтығына, жәбірленушінің психологиялық жағдайының нашарлауына себеп болады.

Демек, кибергруминг сияқты қылмыстық әрекеттерді тергеу үшін интернет-платформалармен әрекеттесу тек техникалық немесе құқықтық мәселелер жиынтығы ғана емес, бұл - цифрлық әлемде қылмыстық әділеттілікті жүзеге асыру қабілетінің өлшемі. Бұл қабілеттілік ұлттық заңнама мен құқық қорғау тәжірибесінің ғана емес, мемлекеттің цифрлық кеңістіктегі субъектілік деңгейінің көрсеткіші ретінде бағалануы тиіс.

Кибергрумингке байланысты қылмыстарды тергеу қазіргі кезеңдегі құқық қорғау қызметінің аса өзекті және күрделі бағыттарының бірі болып табылады. Екінші бөлім шеңберінде осы санаттағы істерді тергеудің ерекшеліктері, сандық дәлелдемелермен жұмыс істеу әдістері және құқық қорғау органдарының интернет-платформалармен өзара әрекеттесу тәжірибесі жан-жақты зерттелді. Зерттеу нәтижелері кибергрумингті ашу мен дәлелдеу үшін классикалық тергеу әдістері жеткіліксіз екенін, ал цифрлық ортада әрекет етудің құқықтық және техникалық тәсілдері жеткілікті деңгейде дамымағанын көрсетті.

Бөлімнің бірінші тармағында кибергруминг бойынша қылмыстық істерді қозғау мәселелері талданды. Бұл санаттағы қылмыстардың латентті сипаты, жәбірленушілердің жас ерекшелігі мен психоэмоционалдық жағдайы, сондай-ақ нақты қылмыстық құрамның ҚР Қылмыстық кодексінде болмауы іс қозғаудың күрделі әрі көп факторлы сипатқа ие екенін көрсетті. Тергеушілер көбіне жәбірленушінің субъективті арызына, ата-аналар немесе педагогтар тарапынан келіп түскен хабарламаларға сүйенуге мәжбүр. Бұл өз кезегінде іс қозғау процесін тұрақсыз және біркелкі емес етеді.

Бөлімнің екінші тармағы сандық дәлелдемелерді жинау және талдау әдістеріне арналды. Кибергруминг виртуалды ортада жүзеге асатын қылмыс болғандықтан, дәлелдемелердің негізгі бөлігі электрондық форматта кездеседі: хат алмасу, фотосуреттер, бейнематериалдар, лог-файлдар, IP-адрестер және құрылғылардың техникалық метадеректері. Сандық дәлелдемелердің шынайылығын, өзгертілмегенін, заңды жолмен алынғанын дәлелдеу үшін арнайы құралдар мен сараптамалық әдістер қажет. Тергеу тәжірибесінде бұл

құралдардың қолданылуы жиі техникалық және кадрлық шектеулерге байланысты қиындатылады. Сонымен қатар, дәлелдемелердің құқықтық статусы әрқашан айқын бола бермейді, ал оларды дұрыс рәсімдемеу сотта жарамсыз деп танылу қаупін туғызады.

Үшінші тармақта құқық қорғау органдары мен интернет-платформалар арасындағы өзара әрекеттестіктің ерекшеліктері сараланды. Қазіргі таңда кибергруминг әрекеттері жүзеге асатын негізгі орта - бұл халықаралық юрисдикцияға жататын әлеуметтік желілер мен мессенджерлер (Meta, Google, Telegram, TikTok және т.б.). Тергеушілердің бұл платформалардан қажетті ақпаратты алу мүмкіндігі көбіне олардың ішкі саясаты мен халықаралық келісімдерге сүйенуіне тәуелді. Қазақстан Будапешт конвенциясына қосылмағандықтан, көптеген сұраныстарға жауап алу процесі ұзаққа созылады немесе мүлдем нәтиже бермейді. Бұл фактор тергеудің тиімділігін төмендетіп, дәлелдемелердің жойылуына немесе қылмыстың толық ашылмауына әкелуі мүмкін.

Сонымен қатар, интернет-платформаларда end-to-end шифрлау, өздігінен өшірілетін хабарламалар сияқты құпиялылық функцияларының белсенді қолданылуы қылмыстық әрекетті тергеу процесін одан әрі қиындатады. Қылмыскерлердің виртуалды кеңістіктегі анонимділігі, фейк аккаунттар мен VPN технологияларын пайдалану тергеу субъектілерінің нақты сәйкестенуін қиындатады. Бұған қоса, құқық қорғау органдары мен IT-компаниялар арасындағы әрекеттестік әзірге формалды, стандартталмаған сипатта болып отыр, бұл - жедел әрекет етуді талап ететін қылмыстар үшін қолайсыз жағдай туғызады.

Жалпы алғанда, екінші бөлімнің нәтижелері қазіргі таңда кибергрумингке қарсы қылмыстық-құқықтық реакцияны жүзеге асыруда **процессуалдық, техникалық және институционалдық кемшіліктер** бар екенін анық көрсетті. Тергеудің тиімділігі тек жедел-іздестіру шараларына емес, сонымен қатар интернет-платформалармен жүйелі және жедел өзара әрекеттестіктің мүмкіндігіне, сандық дәлелдемелермен жұмыс істеудің жоғары кәсіби деңгейіне, әрі құқықтық нормалардың нақты регламентациясына байланысты. Мұндай күрделі қылмыс түрін ашу мен дәлелдеуде құқықтық жүйе қазіргі заманның цифрлық шындығына бейімделуге міндетті. Бұл бейімделу - тек заң шығару емес, сонымен қатар тергеу тәжірибесінің өзгеруін, IT-құзыреттілікті арттыруды және мемлекетаралық ынтымақтастықты талап ететін көпқырлы процесс.

3. Кибергрумингті тергеуді жетілдіру мәселелері мен перспективалары

3.1 Кибергрумингке байланысты қылмыстарды саралау және дәлелдеу қиындықтары

Қылмыстық құқық саласындағы саралау (квалификация) процесі - құқық қолдану жүйесінің маңызды буыны болып табылады. Ол нақты әрекетті Қылмыстық кодекстің сәйкес бабына сәйкестендіріп, құқықтық жауапкершілікті айқындауға негізделеді. Алайда кибергрумингке байланысты құқықбұзушылықтарды саралау барысында теориялық та, практикалық та сипаттағы елеулі қиындықтар туындауда. Бұл қиындықтар, ең алдымен, кибергрумингтің құқықтық табиғатының ерекшелігіне, әрекеттердің виртуалды ортада жүзеге асуына, қылмыстың латенттілігіне, сондай-ақ балалардың жәбірленуші ретіндегі психологиялық және құқықтық осалдығына байланысты.

Кибергруминг - бұл дәстүрлі түсініктегі сексуалдық қылмыстардан өзгеше, көбінесе байланыс орнату, сенімге кіру және жасөспірімді манипуляциялау арқылы жүзеге асатын психо-әлеуметтік процестің құқыққа қарсы көрінісі. Бұл әрекеттің күрделілігі - оның нақты физикалық актімен міндетті түрде ұштаспайтындығында. Яғни, қылмыскердің ниеті - жыныстық қатынас немесе басқа да сексуалдық әрекет болуы мүмкін, бірақ іс жүзінде ол тек виртуалды деңгейде қалып, балаға психологиялық әсер ету, интимдік контент сұрау, кездесуге шақыру түрінде көрініс табады. Дәл осы жағдай құқық қорғау органдары үшін қылмыс құрамын нақты анықтауды қиындатады.

Қазіргі қолданыстағы Қазақстан Республикасының Қылмыстық кодексі кибергруминг ұғымын жеке қылмыстық құрам ретінде белгілемеген. Бұл жағдайда тергеушілер мен прокурорлар кибергруминг сипатындағы әрекеттерді көбінесе ҚК-нің 122-бабы («он алты жасқа толмаған адаммен жыныстық қатынас немесе сексуалдық сипаттағы өзге де әрекеттер»), 123-бабы («жыныстық сипаттағы күш қолданбай жасалған әрекеттер») немесе 124-бабы («кәмелетке толмағанды азғыру») бойынша саралауға мәжбүр. Алайда бұл баптардың қолданылу аясы көбінесе нақты әрекет жасалған, яғни материалдық құрам болған жағдайда ғана іске асады. Ал кибергруминг жағдайында, атап айтқанда, қылмыстық ниет пен алдын ала дайындық белгілері ғана болған кезде, бұл баптардың қолданылу мүмкіндігі шектеулі болады.

Мәселен, 124-бапта көрсетілген «азғыру» термині нақты ұсынысты немесе мәжбүрлеу әрекетін білдіреді. Алайда кибергруминг барысында қолданылатын фразалар көбінесе жанама, манипуляциялық сипатқа ие. Қылмыскерлер, мысалы: «Сен маған ұнайсың», «Сенімен сөйлескім келеді», «Суретіңді көрсете аласың ба?» деген сияқты бейкүнә көрінетін, бірақ астарында сексуалдық ниет жатқан хабарламалар жібереді. Мұндай сөздер нақты қылмыс құрамы тұрғысынан тікелей дәлел ретінде бағалану үшін жеткіліксіз. Осы жағдай саралау процесін құқықтық тұрғыдан белгісіздік жағдайына әкеліп отыр.

Қылмыстық заңнамада әрекеттің сараланауына әсер ететін басты компоненттердің бірі - қоғамға қауіптілік деңгейі. Кибергруминг виртуалды түрде жүзеге асқанымен, оның салдары - баланың психикалық денсаулығына әсері, кейінгі мінез-құлқындағы ауытқулар, сенім дағдарысы - нақты және ауыр. Демек, қоғамға қауіптілік дәрежесі бойынша бұл әрекет ауыр қылмыстар санатына жатқызылуы тиіс. Алайда заңдық тұрғыдан саралау нақты қылмыс құрамының болуына байланысты болғандықтан, көптеген кибергруминг жағдайлары құқықтық жауапкершілікке тартылмай қалуда.

Құқық қорғау тәжірибесінде кибергрумингтің қылмыстық әрекет пен заңды қарым-қатынастың шекарасында орналасқандығы жиі байқалады. Қылмыскердің сөзі мен әрекеті кейде жыныстық мазмұнды ашық білдірмейді, ал бала бұл әрекетті қылмыс ретінде қабылдамайды. Бұл мәселе тергеушілердің іс-әрекетті дұрыс құқықтық тұрғыда бағалауын, ниет пен қылмыстың субъективтік жағын дәл анықтауын қиындатады. Сонымен қатар, кибергрумингтің жасырын

сипаты (латенттілік) бұл әрекетті заңдық жолмен ашуға және дәлелдеуге қосымша кедергілер тудырады.

Салыстырмалы құқықтық талдау барысында көрініп отырғандай, кибергруминг көптеген елдерде дербес қылмыстық құрам ретінде танылған. Мәселен, Германияның ҚК-нің 176-бабының 4-бөлімі, Ұлыбританияның 2003 жылғы Жыныстық қылмыстар туралы заңы (Sexual Offences Act), Канададағы Criminal Code баптары кибергрумингті әрекетке дейінгі кезеңде-ақ қылмыстық ниет пен онлайн байланыс арқылы саралауға мүмкіндік береді. Бұл елдерде кибергруминг фактісі балаға жыныстық мақсатта виртуалды түрде жақындау, жыныстық қатынасқа дайындау немесе жыныстық сипаттағы хабарламалар жіберу арқылы жасалған кез келген әрекет деп танылады.

Қазақстанда мұндай заңдық нақтылықтың болмауы құқық қорғау органдарын қылмыстың алдын алуға емес, тек салдарын тергеуге мәжбүрлейді. Бұл жағдай қылмыскерлердің жазадан оңай жалтаруына, жәбірленушілердің қорғану мүмкіндігінің төмендеуіне және қоғамда құқыққа сенім деңгейінің әлсіреуіне алып келеді.

Кибергруминг әрекеттеріне қатысты қылмыстық істерді дәлелдеу - қылмыстық процесс саласындағы ерекше маңызы бар, әрі құқық қолдану жүйесінде күрделі мәселелердің бірі. Бұл қылмыстардың спецификалық сипаты - олар физикалық әрекетсіз, виртуалды кеңістікте жасалатындықтан, дәлелдеу базасының қалыптасуы тек сандық және психологиялық дәлелдермен шектеледі. Мұндай жағдайда тергеу органдары дәлелдемелердің дәстүрлі түрлерінен гөрі, сандық, лингвистикалық және индиректілік сипаттағы дәлелдерге сүйенуге мәжбүр болады.

Кибергрумингті дәлелдеуде негізгі құрал - бұл сандық дәлелдемелер. Олар өз ішінде хат-хабар алмасу, әлеуметтік желідегі жазбалар, мессенджердегі диалогтар, фотосуреттер, аудио/видео хабарламалар, лог-файлдар, IP-адрестер, құрылғы метадеректері сияқты құрамдастардан тұрады. Сандық дәлелдердің артықшылығы - олардың нақты уақытқа тіркелуі, қай құрылғыдан, қай желіден жіберілгені және байланыс жиілігіне дейінгі барлық ақпараттың сақталуында. Алайда, бұл дәлелдер өзгертуге, өшіруге, қолдан жасауға бейім, ал оларды бекіту мен сараптау үшін арнайы техникалық құралдар мен IT-сараптама қажет. Осы себепті кибергрумингке қатысты істерде дәлелдің аутентификациясы - яғни, оның шынайылығы мен өзгертілмегенін техникалық растау - шешуші рөл атқарады.

Бұл тұрғыда дәлелдеу процесінде ҚР ҚПК нормалары мен практикада қолданылатын арнайы криминалистикалық әдістемелер арасында белгілі бір алшақтық байқалады. ҚР ҚПК-де дәлелдеменің заңдылығы, жарамдылығы және сенімділігіне қойылатын талаптар нақты көрсетілгенімен, сандық дәлелдемелермен жұмыс істеудің егжей-тегжейлі регламентациясы жоқ. Нәтижесінде тергеуші сандық дәлелді процесуалдық тұрғыдан бекіту үшін әртүрлі құқықтық және техникалық тәсілдерді үйлестіріп қолдануға мәжбүр

болады. Бұл - тергеу сапасына, сот процесіндегі дәлелдің жарамдылығына және іс нәтижесіне айтарлықтай әсер ететін фактор.

Кибергруминг әрекеттерін дәлелдеуде тағы бір маңызды мәселе - бұл қылмыскердің ниетін дәлелдеу. Егер жыныстық қатынас немесе бопсалау фактісі нақты жүзеге аспаса, онда оның ниетін дәлелдеу тек жазбаша немесе ауызша формадағы контентке байланысты болады. Бұл кезде психолингвистикалық сараптама, семантикалық талдау, хат алмасу стилінің сараптамасы маңызды дәлел көзіне айналады. Алайда мұндай сараптамалар, біріншіден, ұзақ мерзім алады, екіншіден, субъективті элементтерге тәуелді болуы мүмкін. Осылайша, дәлелдеменің дәлдігін дәлелдеуші сарапшының біліктілігі мен бейтараптығына байланысты тәуекелдер туындайды.

Кибергруминг қылмыстарының жәбірленушісі - көбінесе кәмелетке толмаған тұлға болғандықтан, дәлелдеме ретінде оның айғақтары ерекше құқықтық режимге бағынады. Баланың психологиялық жағдайы, эмоционалдық қабылдауы және жас ерекшелігі ескеріліп, процессуалдық әрекеттер арнайы мамандардың - балалар психологтарының немесе педагогтарының қатысуымен жүзеге асырылуы тиіс. Бұл міндет ҚР ҚПК-де көзделгенімен, іс жүзінде барлық тергеу органдарында қажетті кадрлық ресурстар мен бейімделген процедуралар жоқ. Баланың куәлік беруі кибергруминг фактісінің дәлелденуінде маңызды рөл атқарады, алайда ол эмоционалдық тұрғыдан қиын және баланың қайта жарақат алу қаупін тудырады. Мұндай жағдайда тергеуші жауап алу кезінде сенімді, бейтарап әрі психологиялық қысымсыз тәсілдер қолдануы тиіс, бұл - тек арнайы дайындықтан өткен кадрлардың мүмкіндігі.

Дәлелдеу процесіндегі келесі күрделі элемент - бұл электрондық дәлелдемелердің құқықтық мәртебесі. Қазіргі уақытта Қазақстан заңнамасында электрондық және сандық дәлелдер үшін бірегей регламент жоқ. Тек жалпы дәлелдеме нормаларына сүйене отырып, тергеуші скриншоттар, мәтіндер мен медиафайлдарды хаттамамен тіркеп, сараптамаға жібереді. Бұл материалдарды сот дәлел ретінде қабылдай ма, жоқ па - бұл судьяның ішкі сеніміне, тәжірибесіне және дәлелдеменің процессуалдық тазалығына байланысты. Егер электрондық файлдың алыну жолы күмәнді немесе заңсыз деп танылса, ол істен алып тасталуы мүмкін. Бұл - дәлелдеу базасын әлсірететін айтарлықтай қауіп.

Кейбір жағдайларда құқық қорғау органдары платформалардың ішкі деректеріне - мысалы, тіркеу IP-адресі, пайдаланушы әрекеттері туралы логтар, аккаунттың құрылу уақыты, құрылғы идентификаторы - қол жеткізе алмайды. Бұл - шетелдік платформалармен әрекеттестіктің шектеулі болуымен байланысты. Мұндай жағдайда дәлелдердің толық еместігі іс бойынша айып тағуға кедергі келтіреді, ал қылмыскердің жазадан жалтаруына себеп болады. Дәл осы себепті құқық қорғау органдары прямой дәлелдерден гөрі жиынтық дәлелдемелік жүйені құруға мәжбүр. Бұл тәсіл бірнеше жанама деректерге сүйеніп, біртұтас логикалық құрылым жасауға негізделеді.

Тағы бір назар аударарлық жайт - дәлелдемелердің уақытша сипаты. Көптеген платформалар өзінде сақталған мәліметтерді белгілі бір мерзімнен

кейін автоматты түрде жояды немесе пайдаланушының сұрауы бойынша өшіреді. Бұл жағдай тергеу органдары үшін цифрлық іздерге дереу қол жеткізудің маңызын арттырады. Қылмыстық іс қозғалмай тұрып-ақ дәлелдерді жою ықтималдығы жоғары болғандықтан, деректерді уақытылы жинау - құқық қорғау жүйесінің жеделділігі мен дайындық деңгейіне тікелей байланысты.

Жоғарыда аталған барлық қиындықтар кибергрумингке байланысты қылмыстарды дәлелдеу процесінің мультидисциплинарлық сипатын айқындайды. Бұл салада құқық, психология, ақпараттық технология, тіл білімі сияқты ғылымдардың тоғысуы міндетті. Тергеуші тек заңгер ретінде ғана емес, сонымен қатар цифрлық ортада бағдарлай білетін, баламен тіл табыса алатын, техникалық құралдармен жұмыс істей алатын маман болуға тиіс. Тек осындай көп қырлы дайындық арқылы ғана кибергруминг істерінде нақты әрі сенімді дәлелдемелер базасын қалыптастыру мүмкін болады.

Кибергрумингке байланысты қылмыстарды саралау және дәлелдеу тәжірибесі тек заңнамалық шектеулермен ғана емес, сонымен қатар нақты құқық қолдану практикасындағы жүйелік олқылықтармен күрделене түседі. Бұл бағыттағы істердің ерекшелігі - олардың құқықтық табиғатының жаңалығы, дәлелдеу базасының күрделілігі және жәбірленушінің ерекше субъект ретіндегі процесуалдық жағдайы. Сондықтан да сот тәжірибесінде кибергруминг әрекеттерін саралау мен дәлелдеуде тұрақсыздық пен бірізділіктің болмауы жиі кездеседі.

Қазақстан Республикасының сот практикасы кибергрумингті дербес қылмыстық іс ретінде емес, жалпы жыныстық қылмыстар шеңберінде қарастырады. Бұл жағдай істі қарау кезінде судьяның істің мән-жайына қатысты бағалауы көбінесе дәлелдемелердің жеткіліктілігіне, қылмыстық ниеттің айқындылығына және қолданылатын баптың мазмұнына байланысты болатынын көрсетеді. Көп жағдайда сот тергеуінде күдіктінің нақты физикалық әрекетке барғаны болмаса, тек виртуалды хат алмасу немесе сөз жүзіндегі мазмұн қылмыстық жауаптылық үшін жеткіліксіз деп танылады. Мұндай тәсіл заң жүзінде түсінікті болғанымен, бұл баланың құқықтарын қорғау мен киберортадағы қылмыстың алдын алу тұрғысынан алғанда - әлсіз позиция.

Мысал ретінде, ел ішіндегі бірнеше істерде күдікті кәмелетке толмаған қыз балаға жыныстық сипаттағы хабарламалар жолдағаны, интимдік фотосуреттер сұрағаны, тіпті онымен кездесуді жоспарлағаны анықталған. Алайда нақты жыныстық қатынас немесе күш қолдану әрекеті болмағандықтан, кейбір соттар істі ҚК-нің 123-бабы немесе 124-бабы бойынша сараламай, құрам болмағандықтан қылмыстық жауапкершіліктен босату шешімін қабылдаған. Бұл жағдай қылмыстық әрекеттің виртуалды формаларына құқықтық жауап берудің қазіргі стандарттары жеткіліксіз екенін дәлелдейді.

Сонымен қатар, кибергруминг істерінде соттар көп жағдайда баланың айғақтарына күмәнмен қарайды. Бұл процессуалдық тұрғыдан түсінікті болғанымен, жәбірленушінің жасы, психологиялық күйі және әлеуметтік тәжірибесінің аздығы айғақтардың толық болмауына себеп болуы мүмкін.

Мұндай жағдайда дәлелдемелердің басым бөлігі скриншоттар, мессенджерлердегі хат-хабарлар мен сараптамаларға сүйенеді. Бірақ сот тәжірибесінде электрондық дәлелдемелердің заңды рәсімделмегені, олардың шынайылығы дәлелденбегені немесе нақты дереккөз анықталмағаны үшін жарамсыз деп танылған жағдайлар да кездеседі. Бұл - соттарға цифрлық дәлелдермен жұмыс істеудің процессуалдық регламентінің жеткіліксіз екендігін көрсетеді.

Халықаралық сот практикасы, керісінше, кибергрумингке қатысты істерде айып тағу үшін жыныстық әрекеттің орындалуы міндетті емес деген ұстанымды бекем ұстанады. Мәселен, Германияда және Ұлыбританияда кибергруминг - бұл жәбірленушімен онлайн байланыс орнату арқылы жыныстық мақсат көздеу әрекеті. Бұл елдерде электрондық хаттар, әлеуметтік желілердегі диалогтар, тіпті жыныстық сипаттағы бейнелер сұрау әрекеті - айып тағуға жеткілікті дәлел ретінде қабылданады. Тиісінше, соттар күдіктінің әрекетінің мотиві мен байланыс логикасына ерекше мән береді, ал дәлелдемелердің электрондық формасы олардың дәлелдік күшін төмендетпейді.

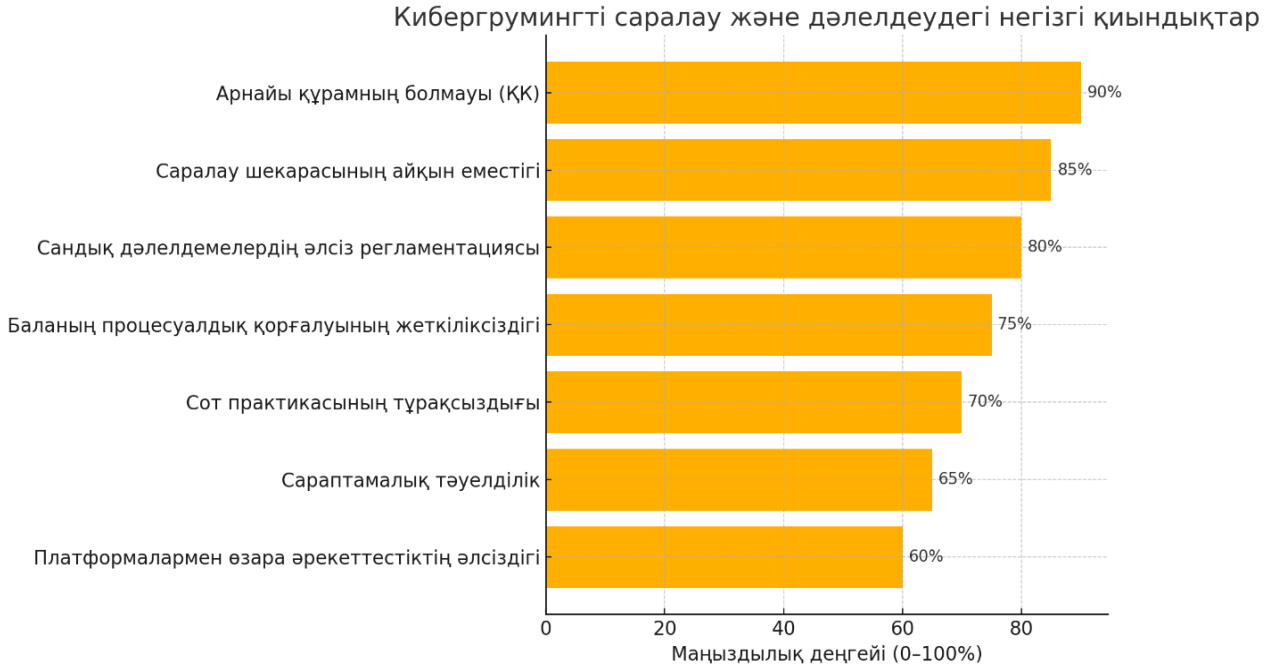
Қазақстанда мұндай стандарттар мен түсініктер әлі толық қалыптаспады. Соттардың қылмыстық ниетті дәлелдеудегі көзқарасы біркелкі емес, ал кейде қылмыстық заңның тармағын қатаң қолдану баланың құқығын қорғауда елеулі шектеу болып тұр. Мысалы, виртуалды азғыру әрекеті нақты жыныстық сипатта болмаса да, баланың психологиялық саулығына зиян келтіретін әрекет ретінде қарастырылмауы мүмкін. Бұл жағдай кибергрумингке қарсы күресте соттардың формалды-құқықтық әдісті басшылыққа алатынын көрсетеді.

Сот процесінде тағы бір проблема - сараптамалық тәуелділік. Көп жағдайда дәлелдің жарамдылығы сарапшының қорытындысына негізделеді. Бұл өз кезегінде сараптама ұйымдарының жүктемесіне, кадрлық даярлық деңгейіне және техникалық жарақталуына тәуелді. Егер сарапшы жеткіліксіз білікті болса немесе қолданылған әдіснама жаңартылмаған жағдайда, дәлелді толық ашып көрсету мүмкін болмайды. Мұндай жағдайларда сот шешімі тек шектеулі деректерге негізделіп, әділ сот төрелігіне кедергі келтіруі ықтимал.

Сонымен қатар, кибергруминг бойынша қозғалған істердің сотқа дейінгі кезеңінде-ақ тоқтатылуы - кең таралған тәжірибелердің бірі. Көбінесе дәлелдемелердің жеткіліксіздігі, жәбірленушінің арызын қайтарып алуы немесе құқық қорғау органдарының іс-әрекетінің пассивтілігі себеп болады. Бұл жағдай құқықтық жүйенің киберортадағы қауіптерге жауап беруге дайын еместігін және құқық қорғау-сот тәжірибесінде нақты алгоритмдердің қалыптаспағанын көрсетеді.

Сот тәжірибесіндегі мұндай олқылықтар тек жекелеген істер бойынша емес, жалпы жүйелі құқық қолдану тәжірибесінде салалық стандарттардың болмауын және процессуалдық құралдардың әлсіздігін көрсетеді. Бұл әсіресе киберқылмыстарға қатысты істерде, оның ішінде кәмелетке толмағандарға қарсы бағытталған виртуалды қылмыстық әрекеттерде ерекше сезіледі. Соттар, прокуратура, тергеу органдары мен сараптама мекемелері арасындағы

процессуалдық және институционалдық өзара іс-қимыл жүйесі - бұл қылмыстық процестің тиімділігінің басты көрсеткіші. Кибергруминг істерінде бұл жүйенің әлі де жетілмегені анық байқалады.



Сурет 1 - Кибергрумингті саралау және дәлелдеудегі негізгі қиындықтар

Жоғарыда келтірілген талдаулар кибергрумингке байланысты қылмыстарды саралау мен дәлелдеу процесінің қазіргі құқық қорғау жүйесі үшін бірқатар күрделі және жүйелі сипаттағы қиындықтарға толы екенін айқын көрсетті. Бұл қиындықтар, ең алдымен, заңнамалық регламентацияның жеткіліксіздігімен, құқық қолдану тәжірибесінің біркелкі болмауымен және дәлелдемелердің ерекшеліктеріне байланысты туындайды.

Кибергруминг әрекеттерінің құқықтық табиғаты әлі де болса нақты құқықтық түсінікке ие емес, ал Қылмыстық кодексте мұндай әрекетті дербес қылмыс ретінде айқындайтын нақты баптың болмауы тергеушілер мен прокурорлар үшін саралау процесін күрделендіреді. Қолданыстағы 122, 123 және 124-баптар тек нақты сексуалдық әрекет жасалған жағдайда ғана қолданылуға бейімделген, ал кибергруминг - бұл ниет деңгейіндегі психологиялық және манипуляциялық ықпал, яғни қылмыстық жауапкершілікті талап ететін ерекше сипаттағы мінез-құлық.

Кибергрумингке қатысты қылмыстарды дәлелдеу процесі де күрделі. Сандық дәлелдемелермен жұмыс істеудің құқықтық регламенті, техникалық сараптама әдістері, дәлелдің аутентификациясы мен жарамдылығы сияқты аспектілер Қазақстан құқық қорғау жүйесінде әлі де толық қалыптаспаған. Сонымен қатар, жәбірленуші ретінде кәмелетке толмаған тұлғаның процесуалдық қорғанысы, оның психологиялық ахуалы мен куәлік беру қабілеттілігі - дәлелдеуге қосымша кедергі келтіретін факторлар болып

табылады. Мұндай жағдайда тергеуші мен соттың кәсіби даярлығы, сараптамалық базаның жеткіліктілігі және платформа әкімшіліктерімен өзара әрекеттестіктің тиімділігі шешуші мәнге ие.

Құқық қолдану тәжірибесі кибергруминг әрекеттерін ашуда және сотқа дейін жеткізуде жиі дәлелдеме жеткіліксіздігі, қылмыстық ниеттің дәлелденбеуі, қылмыс құрамының анықталмауы сияқты себептермен шектеліп қалатынын көрсетеді. Бұл өз кезегінде қоғамда мұндай әрекеттерге құқықтық тосқауылдың әлсіздігін білдіреді, ал бұл - әсіресе кәмелетке толмағандардың цифрлық кеңістіктегі қауіпсіздігіне тікелей қатер.

Салыстырмалы құқықтық тәжірибе (Германия, Ұлыбритания, Канада) көрсеткендей, кибергрумингті алдын ала кезеңде-ақ құқықтық тұрғыдан бағалау мен жауапқа тарту — құқықтық саясаттың пәрменділігін арттырады. Бұл елдерде қылмыстық әрекет жасалмаған күннің өзінде жыныстық мақсаттағы онлайн байланыс фактісі қылмыстық жауапкершілікке әкеледі. Мұндай тәсіл Қазақстан үшін де өзекті.

Қорыта келгенде, кибергрумингке байланысты қылмыстарды саралау мен дәлелдеу процесі — қазіргі цифрлық дәуірдегі құқық қорғау саласының шынайы сын-қатері. Бұл салада құқықтық нормалардың нақтылығы, тергеу және сот практикасының бірізділігі, сандық дәлелдемелермен кәсіби жұмыс істеу дағдысы, жәбірленушінің құқығы мен психологиялық қауіпсіздігі басты мәнге ие. Мұндай әрекеттермен күрес - тек заңмен емес, құқық қолданудың барлық буынының үйлесімді қызмет етуімен жүзеге асатын кешенді жүйе екенін уақыт дәлелдеуде.

3.2 Кибергруминг істері бойынша сот практикасы: талдау және үрдістер

Кибергруминг қылмыстарының сот тәжірибеде қаралуы - қазіргі қылмыстық әділет жүйесі үшін ең өзекті және күрделі салалардың бірі болып отыр. Мұндай істер бойынша қабылданатын сот актілері тек бір нақты істің тағдырын ғана емес, сонымен қатар құқықты түсіндірудің, дәлелдемелерді бағалаудың, баланың құқықтық мәртебесін танудың сапасын көрсетеді. Сонымен қатар, бұл істер сот жүйесінің цифрлық кеңістікке бейімделу деңгейін, балалардың құқықтарын қорғауға деген институционалдық дайындығын көрсететін индикатор ретінде де қызмет атқарады.

Қазақстандағы сот тәжірибесі кибергрумингке қатысты істер бойынша әлі толық қалыптаспаған. Бұл қылмыстардың латентті сипаты, нақты құқықтық құрамның болмауы, сонымен қатар дәлелдеу базасының техникалық күрделілігі сотқа жеткен істер санының шектеулі болуына алып келуде. Жеке өңірлерде бірлі-жарым істер тіркелгенімен, олардың құқықтық сарапануы мен сот шешімдерінің құрылымы бірыңғай стандартқа бағынбайды. 2020-2023 жылдар аралығында ҚР Жоғарғы Сотының құқықтық статистика мәліметтерінде кибергруминг нақты тіркелген қылмыс ретінде көрсетілмеген, ал бұл санаттағы істер көбінесе ҚК-нің 123-бабы (жыныстық сипаттағы күш қолданбай жасалған

әрекеттер) немесе 124-бабы (кәмелетке толмағанды азғыру) аясында қарастырылады.

Сотта қаралған істерді сараптай отырып, бірнеше тұрақты үрдісті байқауға болады. Біріншіден, соттар күдіктінің нақты әрекетін саралау барысында физикалық байланыс болмаған жағдайда, айыпты жеңілдетуге немесе істі тоқтатуға бейім. Бұл - кибергрумингтің виртуалды сипаты мен ниет арқылы жасалған қауіптің толық бағаланбайтынын көрсетеді. Көп жағдайда хат алмасу, онлайн сөйлесу, кездесуге шақыру немесе интимдік сипаттағы фото сұрау секілді әрекеттер «моральдық норманы бұзу» немесе «этикалық емес қылық» ретінде бағаланып, Қылмыстық кодексте көзделген қоғамдық қауіпті әрекет ретінде қарастырылмайды. Осылайша, қылмыстық жауапкершілік орнына әкімшілік немесе тәртіптік шаралармен шектелетін жағдайлар да кездеседі.

Екіншіден, сот тәжірибесінде дәлелдемелерге қатысты көзқарас біркелкі емес. Электрондық дәлелдемелер - кибергруминг істеріндегі негізгі айғақ көзі болғанымен, олардың заңды түрде алынуы, сақталуы және процессуалдық рәсіммен тіркелуі нақты талаптарға бағынбаған жағдайда, кейбір соттар оларды дәлел ретінде қабылдамай жатады. Мысалы, жәбірленушінің ата-анасы ұсынған скриншот, фото немесе бейнежазба сотта жеткіліксіз деп танылып, егер олар техникалық сараптамамен расталмаса, іске қосылмай қалуы мүмкін. Бұл, өз кезегінде, қылмыстық процестің дәлелдемелік базасын әлсіретеді және соттың ішкі сенімін қалыптастыруға кедергі келтіреді.

Үшіншіден, баланың соттағы процесуалдық рөліне қатысты да тәжірибеде бірыңғайлық жоқ. Қазақстанда кәмелетке толмаған жәбірленушімен тергеу немесе сот процесінде жұмыс істеу үшін арнайы мамандардың (психолог, педагог) қатысуы заңмен көзделгенімен, бұл талап жиі формалды түрде орындалады немесе мүлде ескерілмейді. Сотта баланың айғақ беруі эмоционалдық қысыммен, стресс жағдайында өтуі мүмкін, бұл оның көрсетулерінің дәлдігіне және психологиялық қауіпсіздігіне кері әсер етеді. Сонымен қатар, жәбірленушінің жасы мен тәжірибесі ескерілмей, классикалық сұрақ-жауап форматы сақталған жағдайда, баланың жауабы толық ашылмайды және іс үшін маңызды дәлелге айналмайды.

Кесте 4 - Кибергрумингке қатысты сот практикасының ерекшеліктері мен үрдістері

№	Талдау нысаны	Қазақстан сот тәжірибесінде көрінісі	Халықаралық сот тәжірибесімен салыстыру	Құқықтық салдары
1	Қылмыстық құрамның сарапануы	ҚК 123, 124 баптарымен, нақты сексуалдық әрекетсіз істерде	Арнайы баптар бар (Германия, Ұлыбритания)	Жаза қолдануда біркелкілік жоқ, жауаптылық жиі алынып тасталады

		саралау қиындайды		
2	Электрондық дәлелдерге көзқарас	Скриншот, чат, логтар жиі күмән тудырады, сараптама міндетті	Электрондық дәлелдер негізгі айғақ ретінде қолданылады	Дәлелдеме базасы әлсірейді, үкімге сенімділік төмендейді
3	Жәбірленушінің процесуалдық рөлі	Баланың жауаптары шектеулі пайдаланылады, психолог қатысуы формалды	Арнайы бейімделген бөлмелер, балаларға арналған протоколдар	Баланың құқығы мен қауіпсіздігі жеткілікті қорғалмайды
4	Моральдық зиянды бағалау	Сирек қарастырылады, психологиялық сараптама жиі жүргізілмейді	Зиянды бағалау тұрақты жүргізіледі	Қылмыстың шынайы салдары ескерілмейді
5	Соттардың IT-құзыреттілігі	Тергеуші мен судьялар арасында цифрлық дәлелмен жұмыс істеуде айырмашылық бар	Мамандандырылған судьялар немесе бөлімдер бар	Үкім сапасы сараптамалық қорытындыға шамадан тыс тәуелді
6	Сот үкімдерінің бірізділігі	Аймақтарда тәжірибе әркелкі	Құқық қолдану - прецеденттік, нормаға бағытталған	Құқықтық сенімсіздік, әділетсіздікке жол берілуі мүмкін
7	Тенденциялар мен оң өзгерістер	Электрондық дәлелдерді қабылдау, IT-құзыреттілік артуда	Цифрлық ортаға бейімделу тұрақты жүзеге асып жатыр	Жаңа тәжірибе қалыптасуда, алайда ол баяу әрі фрагменттелген

Төртіншіден, сот сараптамасына тәуелділік деңгейі өте жоғары. Кибергруминг істерінде, әсіресе психолингвистикалық сараптама, IT-сараптама және психологиялық сараптама негізгі рөл атқарады. Бірақ бұл сараптамалардың қорытындылары әртүрлі болуы мүмкін, себебі нақты әдіснамалық база

жетілмеген. Кейбір жағдайларда сарапшы күдіктінің ниетін «астыртын сексуалдық сипаттағы» деп бағаласа, басқа сарапшы оны бейтарап немесе достық қарым-қатынас ретінде сипаттай алады. Бұл жағдай сот шешімінің субъективтілік деңгейін арттырып, дәлелдемелерге сенімділікпен баға беру мүмкіндігін шектейді.

Халықаралық сот тәжірибесімен салыстырғанда, Қазақстанда кибергрумингке қатысты істердің қаралуы сақтықпен және құқықтық минимализммен жүргізілетінін байқауға болады. Германияда, Ұлыбританияда, Канадада соттар кибергруминг әрекетін жеке бап аясында қарап, айыпталушының қылмыстық ниетін дәлелдеу үшін тек хат мазмұнын ғана емес, оның жиілігін, ұзақтығын, хабарламалардағы контекст пен баланың жауап реакциясын да ескереді. Сонымен қатар, бұл елдерде жыныстық сипаттағы әңгіме бастау, онлайн байланыс орнату фактісінің өзі - айып тағуға жеткілікті. Соттар баланың психологиялық осалдығын, ақпараттық манипуляцияға бейімділігін, онлайн тәуекелдерге бейім екенін басшылыққа алады. Мұндай әдіс - қылмыстың алдын алу мақсатында әрекет етуді көздейтін прецеденттік юриспруденцияның көрінісі.

Қазақстанда мұндай прецеденттер әлі де қалыптасу үстінде. Бірақ соңғы жылдары соттар электрондық дәлелдемелерді қабылдау, баланың процестік құқығын кеңейту және сараптама қорытындыларын кешенді бағалау сияқты аспектілерге біртіндеп мән бере бастағаны байқалады. Бұл - сот практикасының қазіргі таңда цифрлық кеңістіктегі құқықтық қатынастарға бейімделу кезеңінде екенін көрсетеді. Дегенмен, бұл үдеріс баяу жүріп жатыр, ал құқықтық жүйенің кеш жауап беруі - киберортадағы кәмелетке толмағандардың құқықтарының осалдығына әкелуі мүмкін.

Сот тәжірибесінің қазіргі даму сатысында бірнеше үрдістерді бөліп көрсетуге болады: электрондық дәлелдемелердің құқықтық мәртебесінің танылуы; соттардың моральдық зиян мен психологиялық қысымды ескеруі; саралау практикасын біріздендіруге ұмтылыс; судьялардың IT-құзыреттілігін арттыру; жәбірленуші балалардың сотқа қатысуын жеңілдететін процессуалдық құралдарды қолдану. Бұл үрдістер отандық сот жүйесінің құқықты адамға бағытталған түсіндіру форматына қарай бет бұра бастағанын айғақтайды.

Сот тәжірибесінде байқалып отырған тағы бір маңызды тенденция — бұл электрондық дәлелдемелерге деген көзқарастың біртіндеп оң сипатқа ие болуы. Егер бұрын соттар тек материалдық (құжат, куәлік, сараптама) дәлелдерге сүйенсе, қазіргі таңда киберқылмыстар, соның ішінде кибергруминг істері бойынша цифрлық ақпараттың дәлел ретіндегі рөлі айқындала бастаған. Скриншоттар, онлайн хат алмасу, лог-файлдар, құрылғы метадеректері - барлығы сот тәжірибесінде бағалаудың өз алдына бір саласына айналуда. Алайда бұл дәлелдемелердің процесуалдық тұрғыдан заңды түрде алынуы мен тіркелуі шешуші рөл атқарады.

Кейбір сот актілерінде электрондық дәлелдер нақты сараптамалық қорытындымен расталмаған жағдайда, олар сот үшін «күмәнді» сипатқа ие

болып, іс материалдарынан шығарылған. Бұл мәселе - тергеу органдарының техникалық құралдармен жұмыс істеу деңгейінің әркелкілігіне, ал кейде құқықтық негіздемелердің жеткіліксіздігіне байланысты. Цифрлық дәлелдемелердің шынайылығы мен өзгертілмегенін растау үшін арнайы IT-сараптамалар жүргізілуі тиіс, алайда олардың өткізілуі көп жағдайда тергеу мерзімін ұзартады немесе сарапшылардың кәсіби деңгейіне тәуелді болады. Соған байланысты сотта дәлелдеме ретінде ұсынылатын материалдың процессуалдық мәні жиі дау туғызады.

Сонымен қатар, кибергруминг істерінде соттар тарапынан моральдық зиянның бар-жоғын бағалау, жәбірленушінің психологиялық жағдайын ескеру деңгейі де тұрақты емес. Кейбір істерде баланың эмоционалдық зақымдануы нақты сараптамамен дәлелденсе, басқа жағдайларда мұндай аспект мүлде ескерілмейді. Бұл - кәмелетке толмаған жәбірленушінің құқығы мен мүддесін толық қорғауға кедергі келтіретін фактор. Халықаралық тәжірибеде, мысалы Ұлыбританияда, баланың интернеттегі әрекеті нәтижесінде туындаған психологиялық бұзылыстар мен сенім жоғалту жағдайлары айыпталушыға қосымша жауапкершілік жүктеу үшін пайдаланылуы мүмкін.

Сот тәжірибесінде байқалатын тағы бір келеңсіз құбылыс - бұл жәбірленушінің арызынан бас тартуы немесе ата-анасының талап қоюдан бас тартуы жағдайында істің тоқтатылуы. Кибергруминг істері көп жағдайда балалар тарапынан түсінілмейтін, қорқынышпен, ұялатын сезіммен қабылданатын әрекеттерге байланысты болады. Сондықтан бала не болғанын нақты түсінбестен, немесе қылмыскердің қысымымен, қылмыстық әрекет туралы айтуға батпайды. Мұндайда сот органдары мен тергеушілер істі объективті зерттеп, жәбірленушінің мінез-құлқын әлеуметтік-психологиялық контексте түсінуге міндетті. Әйтпесе, сот тәжірибесінде әділеттілік қағидаттары жүзеге аспай қалуы мүмкін.

Кейбір өңірлік соттарда кибергрумингке қатысты істер бойынша үкімдердің тым жеңіл болуы немесе шартты жаза тағайындалуы да байқалады. Бұған дәлел ретінде, мысалы, айыпталушы тараптың әрекеттері баланың өміріне немесе денсаулығына тікелей зиян келтірмеді деген уәждер келтіріледі. Алайда бұл - интернет кеңістігінде жасалатын қылмыстың салдарын бағаламаудың көрінісі. Цифрлық зорлық-зомбылықтың әсері көбінесе физикалық емес, психологиялық деңгейде байқалатындықтан, оның қауіптілік деңгейі нақты және ұзақмерзімді сипатқа ие болуы мүмкін.

Қазіргі таңда кибергрумингке байланысты сот тәжірибесінде бірнеше қалыптасып келе жатқан үрдістерді атап өтуге болады:

1. Соттар электрондық дәлелдерді қабылдауға икемделіп келеді, бірақ оларды бағалау үшін техникалық сараптама мен процессуалдық ресімдеудің болуына баса назар аударылады.

2. Жәбірленушінің көрсетулері мен психологиялық жай-күйі сот актілерінде көбірек ескерілуде, алайда бұл тәжірибе біркелкі емес.

3. Моральдық зиян мәселесі әлі де болса толықтай ескерілмей келеді, бұл — жәбірленушінің құқығын қалпына келтірудегі елеулі олқылық.

4. Судьялардың IT саласына байланысты құзыреттері артып келеді, бірақ бұл бүкіл сот жүйесінде біркелкі деңгейде дамымаған.

5. Кибергруминг әрекеттерінің құқықтық сараланuына қатысты соттарда құқықтық түсініктеме беру тәжірибесі қалыптасуда, бірақ ол әлі де болса ҚК нормаларының жетілмеуіне тәуелді.

Қазақстан соттары кибергрумингпен байланысты істерге қатысты күрделі тәжірибелік, нормативтік және дәлелдемелік қиындықтармен бетпе-бет келуде. Бұл сот тәжірибесінің нақты құқықтық шешімдерге қол жеткізуіне, сондай-ақ кәмелетке толмағандардың құқықтарын тиімді қорғауға қатысты әлеуетін әлсіретеді. Осы жағдайларда соттар құқықты қатаң формалистік тәсілмен емес, адам құқықтарына негізделген, балаға бағытталған және цифрлық қауіп-қатерлерді ескеретін тәсілмен қолдануға көшуі қажет.

3.3 Заңнаманы және халықаралық ынтымақтастықты жетілдірудің болашағы

Кибергрумингке қарсы күрес қазіргі заманғы құқық қорғау саласының кешенді реформалар мен халықаралық үйлесімділікті талап ететін бағыттарының бірі болып отыр. Бұл қылмыс түрі - өзінің жасырын, виртуалды және трансшекаралық сипаты арқылы құқық жүйесінің дәстүрлі тәсілдеріне түбегейлі сын тудыратын құбылыс. Зерттеу барысында анықталғандай, Қазақстан Республикасының қолданыстағы заңнамасы кибергруминг әрекеттеріне толыққанды жауап беруге дайын емес, ал халықаралық ынтымақтастық тетіктері фрагменттелген сипатта қалып отыр. Осыған байланысты ұлттық заңнама мен құқықтық саясатты жаңғырту, сондай-ақ халықаралық деңгейдегі интеграциялық процестерге белсенді қатысу - кибергрумингпен тиімді күрестің басты алғышарттарына айналуы тиіс.

Бүгінгі таңда Қазақстан Республикасының Қылмыстық кодексінде кибергруминг қылмысы нақты терминологиялық және құрамдық тұрғыдан көрініс таппаған. Бұл - құқық қолдану органдары үшін елеулі проблема, себебі қылмыстық құқық нормалары нақты, алдын ала айқындалған және болжамды болуға тиіс. Қазіргі таңда ҚК-нің 122, 123 және 124-баптары арқылы кибергрумингке ұқсас әрекеттер ішінара сараланuы мүмкін болғанымен, олар бұл құбылыстың шынайы және толық құрылымын қамти алмайды. Сондықтан Қылмыстық кодекске «Кибергруминг» деп аталатын жеке бапты немесе 124-бапқа толықтыру енгізу арқылы бұл әрекетті жыныстық мақсатпен кәмелетке толмағанмен интернет арқылы байланыс орнату, сенімге кіру және жыныстық сипаттағы іс-әрекетке итермелеу ретінде анықтау орынды. Мұндай құқықтық қадам сот және тергеу органдарына қылмысты нақты және жүйелі түрде саралау мүмкіндігін береді, сондай-ақ құқықтық алдын алу тетіктерін іске қосады.

Осы ретте Қылмыстық-процестуалдық кодекс нормалары да цифрлық қылмыстармен күресте жетілдіруді талап етеді. Сандық дәлелдемелермен жұмыс істеу тәртібі нақты және егжей-тегжейлі реттелмегендіктен, тергеу органдары әртүрлі интерпретацияларға сүйенуге мәжбүр болады. Бұл дәлелдемелердің жарамдылығы мен заңдылығына қатысты сот процесінде күмән туындатып, жаза қолданудың әділеттілігіне кері әсерін тигізеді. Осыған байланысты ҚР ҚПК-не арнайы бап немесе тарау енгізу арқылы электрондық және сандық дәлелдемелерді жинау, сақтау, сараптау және сотта пайдалану тәртібін нақтылау қажет. Мұндай өзгеріс тергеу процесінің процессуалдық тазалығын күшейтеді әрі сот тәжірибесінің бірізділігін қамтамасыз етеді.

Кәмелетке толмаған жәбірленушілерге қатысты тергеу мен сот өндірісіндегі процесуалдық кепілдіктерді күшейту - заңнамалық реформаның тағы бір өзекті бағыты. Бала жәбірленушілердің қатысуымен жүргізілетін тергеу әрекеттерінде психолог пен педагогтың қатысуы формалды сипатта ғана емес, мазмұндық жағынан толыққанды көмек көрсетуді қамтамасыз етуі тиіс. Тергеу кезінде бейімделген жауап алу бөлмелерінің қолданылуы, баланың эмоциялық қауіпсіздігін қамтамасыз ету, тергеушінің арнайы дайындықтан өтуі - мұның бәрі халықаралық стандарттар деңгейінде қарастырылуы қажет.

Кибергрумингке қарсы заңнаманы жетілдіру тек ұлттық деңгеймен шектелмеуі тиіс. Бұл бағыттағы халықаралық тәжірибе, атап айтқанда Еуропа Кеңесінің Будапешт конвенциясы (2001) мен Ланзароте конвенциясы (2007), сондай-ақ АҚШ-тың Protect Act және ЕО-ның Directive 2011/93/EU құжаттары балаларды онлайн кеңістіктегі жыныстық қылмыстардан қорғауға арналған тиімді құқықтық тетіктер ұсынатынын көрсетеді. Будапешт конвенциясы электрондық дәлелдемелермен алмасу және трансшекаралық тергеу жүргізудің бірыңғай процедураларын қалыптастырады. Қазақстан бұл конвенцияға қосылмағандықтан, Meta, Google, Telegram сияқты шетелдік платформалардан тергеу мақсатында ақпарат алу заңнамалық негізге сүйенбейді. Бұл өз кезегінде тергеу мен дәлелдеуді күрделендіреді, дәлелдемелердің жойылуына немесе толық жиналмауына себеп болады.

Қазақстанның Будапешт конвенциясына қосылуы тергеу органдарының трансұлттық серіктестермен деректер алмасуын жеңілдетіп, киберқылмыстармен күреске халықаралық құқықтық негіз қалыптастырады. Сонымен қатар, Ланзароте конвенциясы Қазақстан заңнамасына кәмелетке толмағандарға қарсы жыныстық сипаттағы әрекеттерге қатысты алдын алу, білім беру және жәбірленушіге қолдау көрсету бағытында жаңа міндеттемелер енгізуге мүмкіндік береді. Бұл - қылмыстық реакциядан гөрі, превентивті құқықтық саясатқа көшудің қажеттілігін айқындайтын маңызды бағыт.

Халықаралық құқықтық ынтымақтастық шеңберінде Қазақстан құқық қорғау органдары үшін IT-компаниялармен өзара әрекеттесу алгоритмдерін формализациялау қажет. Meta, TikTok, Telegram, Discord сияқты платформалармен меморандумдар мен келісімдер арқылы құқық қорғау сұраныстарын қабылдау және өңдеу ережелерін нақтылау, аккаунттарды

бұғаттау, мәліметтерді сақтау мерзімдерін келісу - қылмыстық процестің тиімділігі үшін маңызды құрал болмақ. Бұған қоса, Интерпол, Еуропол, ТМД шеңберіндегі құқықтық көмек жүйелерін жаңғырту және бірлескен цифрлық қауіпсіздік стандарттарын қалыптастыру - кибергрумингпен күреске жаңа институционалдық қуат береді.

Осы негізде Қазақстан үшін кибергрумингке қарсы құқықтық механизмдерді жетілдіруге бағытталған нақты ұсыныстар кешенін былайша жинақтауға болады:

- Қазақстан Республикасының Қылмыстық кодексіне «Кибергруминг» ұғымын енгізіп, жеке баппен қылмыстық құрам ретінде белгілеу;
- ҚР ҚПК-не «Сандық дәлелдемелерді жинау, сақтау және пайдаланудың тәртібі» туралы нақты нормалар қосу;
- Кәмелетке толмағандармен тергеу әрекеттері кезінде арнайы бейімделген процедуралар мен стандарттарды бекіту;
- Қазақстанның Будапешт және Ланзароте конвенцияларына қосылу мәселесін саяси-құқықтық деңгейде шешу;
- Бас прокуратура немесе ІІМ жанынан киберқылмыстармен күрес жөніндегі үйлестіруші орган құру;
- Судьялар мен тергеушілерге арналған киберқұқық және цифрлық дәлелдемелер бойынша мамандандырылған оқыту бағдарламаларын енгізу.

Қазақстан Республикасында кибергрумингке қарсы күрестің тиімділігін арттыру және кәмелетке толмағандардың цифрлық кеңістіктегі қауіпсіздігін қамтамасыз ету мақсатында келесі заңнамалық және институционалдық шараларды қабылдау ұсынылады:

1. Қазақстан Республикасының Қылмыстық кодексіне өзгеріс енгізу:

Жаңа бап енгізу - 124-1-бап «Кибергруминг»

Жыныстық мақсатта кәмелетке толмаған адаммен интернет, ақпараттық жүйе немесе басқа да электрондық коммуникациялар арқылы байланыс орнату, сеніміне кіру, оны азғыру немесе жыныстық сипаттағы іс-әрекеттерге тартуға әрекет жасау - үш жылға дейін бас бостандығынан айыруға жазаланады.

Негіздеме:

Қолданыстағы ҚК-нің 124-бабында интернет арқылы жасалған әрекеттер нақты көрсетілмеген. Кибергруминг виртуалды ортада жүзеге асатын, бірақ қоғамдық қауіптілігі жоғары әрекет ретінде танылуы қажет. Бұл қылмыстық құрамды дербес заңдастыру тергеу мен сот практикасының нақты әрі бірыңғай тәсілдерге көшуіне мүмкіндік береді.

2. Қазақстан Республикасының Қылмыстық-процестуалдық кодексіне толықтыру енгізу:

«Сандық (электрондық) дәлелдемелерді жинау, сақтау және пайдалану тәртібі» бабымен толықтыру.

Сандық дәлелдемелерді алу, сақтау және зерттеу кезінде олардың өзгертілмегені хэш-сома, лог-файл, метадеректер және өзге де техникалық

құралдар арқылы расталуы тиіс. Мұндай дәлелдемелер сотта дәлел ретінде арнайы сараптамамен расталғаннан кейін ғана пайдаланылуы мүмкін.

Негіздеме:

Сандық дәлелдемелерді құқықтық рәсімдеудің нақты тәртібі ҚПК-де белгіленбеген. Бұл олардың жарамдылығы мен сотта қолданылуын қиындатып, процессуалдық құқық бұзушылықтарға әкелуі мүмкін.

3. «Баланың құқықтары туралы» Қазақстан Республикасының Заңына толықтыру енгізу:

Жаңа норма енгізу - кәмелетке толмаған жәбірленушілермен тергеу әрекеттерін жүргізу тәртібі туралы:

Кәмелетке толмаған жәбірленушілермен тергеу әрекеттері арнайы жабдықталған балаларға арналған бөлмелерде жүргізіледі және бұл әрекеттерге психолог пен педагогтың қатысуы міндетті болып табылады.

Негіздеме:

Интернеттегі сексуалдық сипаттағы азғыру әрекеттеріне ұшыраған балалардың психологиялық әлсіздігі мен жарақат алу қаупі ескеріліп, оларға қатысы бар тергеу шараларының барынша бейімделген және қауіпсіз ортада жүргізілуі тиіс.

4. «Ақпараттандыру туралы» Қазақстан Республикасының Заңына толықтыру енгізу:

Ақпараттық жүйе иелеріне (әлеуметтік желілер, мессенджерлер, веб-платформалар) қатысты жаңа талап:

Ақпараттық жүйе иелері кәмелетке толмағандарға қатысты қауіп туғызатын контентті, виртуалды азғыру белгілерін анықтау және жою бойынша ішкі мониторинг және алдын алу алгоритмдерін енгізуге міндетті.

Негіздеме:

Ірі цифрлық платформалар тарапынан пайдаланушылардың мінез-құлқын бақылау және заңсыз әрекеттерге уақытылы тосқауыл қою — балалардың цифрлық құқықтарын қорғаудың заманауи механизміне айналуы тиіс.

5. Қазақстан Республикасының халықаралық шарттар саласындағы міндеттемелерін кеңейту:

Қазақстан Республикасының Будапешт және Ланзароте конвенцияларына қосылу рәсімін бастау

- Будапешт конвенциясы (2001 ж.) - киберқылмыстар мен электрондық дәлелдемелерге қатысты халықаралық құқықтық құрал.
- Ланзароте конвенциясы (2007 ж.) - кәмелетке толмағандарға қатысты жыныстық сипаттағы қылмыстарды алдын алу және жәбірленушілерді қорғау туралы.

Негіздеме:

Бұл конвенцияларға қосылу Қазақстанның тергеу органдарына трансұлттық IT-компаниялармен құқықтық негізде әрекет етуге, сондай-ақ кибергрумингпен күресте халықаралық тәжірибені енгізуге мүмкіндік береді.

6. Қазақстан Республикасының Үкіметі, Бас прокуратурасы және Ішкі істер министрлігі деңгейінде нормативтік-құқықтық актілер қабылдау:

Келесі шараларды қабылдау ұсынылады:

- Кибергрумингке байланысты қылмыстық істерді тергеу бойынша арнайы әдістемелік нұсқаулық әзірлеу;
- Прокурорлар, тергеушілер мен судьяларға арналған цифрлық дәлелдемелер, балалармен жұмыс және халықаралық құқықтық сұраныстар бойынша оқу бағдарламаларын енгізу;
- ІІМ немесе Бас прокуратура жанынан киберқылмыспен күрес жөніндегі ұлттық үйлестіруші орган құру.

Негіздеме:

Іс жүзінде қолданылатын нұсқаулықтар мен кәсіби оқыту бағдарламалары құқық қорғау органдарының кәсіби құзыреттілігін арттырады. Арнайы органның құрылуы мемлекеттік деңгейде киберқауіптерге шоғырланған әрекет етуді қамтамасыз етеді.

Жоғарыда келтірілген талдаулар мен ұсыныстар кибергрумингке қарсы құқықтық саясаттың қазіргі күйі мен оны реформалаудың басым бағыттарын айқындауға мүмкіндік береді. Қазақстан Республикасының қолданыстағы заңнамасы, әрине, жыныстық бопсалау мен балалардың құқықтарын қорғау саласында белгілі бір құқықтық база қалыптастырғанымен, ол цифрлық ортада орын алатын жаңа буындағы қауіптерге - соның ішінде кибергрумингке - жедел әрі нақты жауап бере алмай отыр.

Кибергрумингтің табиғаты мен қылмыстық мәні оның дәстүрлі құқықтық түсініктер аясынан тыс тұрғанын көрсетеді. Ол - физикалық байланыссыз, бірақ психологиялық манипуляцияға және саналы түрде кәмелетке толмағанды сендіруге бағытталған әрекеттердің жиынтығы. Мұндай сипаттағы әрекеттердің заңмен тікелей тыйым салынбауы құқық қорғау органдарын құқықтық бағалауда қиын жағдайға әкеліп отыр, ал бұл өз кезегінде жазасыздыққа, қылмыстың қайталануына және жәбірленушілердің екінші мәрте жарақат алуына себеп болуда.

Бұдан бөлек, тергеу мен сот өндірісі процестерінде кибергрумингті дәлелдеуге арналған құқықтық және әдістемелік құралдардың шектеулілігі анық байқалады. Сандық дәлелдемелердің аутентификациясы, оларды заңды жолмен алу, сақтау және процессуалдық тұрғыдан дұрыс рәсімдеу іс жүзінде оңай емес. Мұның барлығы тергеушілер мен прокурорлардан арнайы IT-құзыреттілікті талап етеді, ал судьялар тарапынан да осындай материалдарды кәсіби деңгейде бағалай алатын дайындық қажет.

Осы ретте, халықаралық тәжірибе Қазақстан үшін үлгі ретінде қызмет ете алады. Германия, Ұлыбритания, Канада сияқты елдерде кибергрумингке қатысты әрекеттер арнайы қылмыстық құрам ретінде қарастырылады, ал құқық қорғау органдары мен интернет-платформалар арасында тұрақты ақпарат алмасу тетіктері заңмен және келісімдермен бекітілген. Қазақстан мұндай тәжірибені бейімдеу арқылы киберортадағы кәмелетке толмағандардың құқықтарын шынайы қорғау жүйесін қалыптастыра алады.

Сонымен қатар, Қазақстан халықаралық құқықтық алаңда өзінің белсенді қатысуын кеңейтуі тиіс. Будапешт конвенциясына қосылу арқылы еліміз электрондық дәлелдемелерге трансшекаралық қолжетімділік алады және IT-компаниялармен құқықтық байланыс орнатуға мүмкіндік туындайды. Ланзароте конвенциясын ратификациялау арқылы Қазақстан кәмелетке толмағандардың цифрлық қауіпсіздігіне бағытталған кешенді бағдарламаларды, оның ішінде алдын алу, білім беру, ақпараттандыру және қолдау көрсету құралдарын енгізе алады.

Тұтастай алғанда, кибергрумингпен күресте заңнамалық өзгерістер - бұл тек құқық нормасын жаңарту ғана емес, сонымен қатар ұлттық құқықтық жүйенің технологиялық дамуға, халықаралық стандарттарға және адамның цифрлық кеңістіктегі бостандығы мен қауіпсіздігіне бейімделуінің көрсеткіші. Мемлекет бұл бағытта пәрменді қадамдар жасай отырып, өзінің басты міндеттерінің бірі - балалар құқығын толық және тиімді қорғауды жүзеге асыруы тиіс.

Кибергрумингке қарсы күрестің тиімділігі тек жедел-тергеу амалдарымен ғана емес, сонымен қатар қылмысты дұрыс саралау, дәлелдемелерді сапалы жинау және бағалау, құқық қолдану тәжірибесінің жүйелілігі мен құқықтық негіздердің жетілдірілуімен тығыз байланысты. Үшінші бөлім аясында жүргізілген талдау көрсеткендей, Қазақстан Республикасында бұл бағытта нақты жетістіктер болғанымен, жүйелік деңгейдегі бірқатар шешілмеген мәселелер сақталып отыр.

Бірінші кезекте, кибергрумингке қатысты әрекеттерді қылмыстық-құқықтық тұрғыдан саралау іс жүзінде күрделі міндетке айналған. Қазіргі Қылмыстық кодексте мұндай әрекетті нақты қылмыс ретінде танитын арнайы қылмыстық құрам қарастырылмаған. Қолданыстағы баптар - 122, 123 және 124-баптар - нақты физикалық әрекеттерді талап етеді, ал кибергруминг көбінесе виртуалды кеңістікте, жанама түрде жүзеге асады. Бұл жағдай құқық қорғау органдарының әрекетті дұрыс құқықтық бағалауына кедергі келтіріп, бірізді сот практикасының қалыптасуына тосқауыл болады. Сонымен қатар, жыныстық ниетті дәлелдеу мен оның құқықтық тұрғыда мойындалуы көбіне электрондық хат-хабар немесе жанама дәлелдерге сүйенетіндіктен, дәлелдеу шегін анықтау қиындық туғызады.

Екінші тармақта қарастырылғандай, дәлелдемелермен жұмыс істеу барысында тергеушілер мен сот органдары сандық (электрондық) дәлелдердің құқықтық мәртебесіне қатысты көптеген әдістемелік және техникалық қиындықтарға тап болуда. Сандық дәлелдердің ерекшелігі - олардың оңай бұрмалануы, жойылуы және техникалық растаусыз жарамсыз болып танылуы мүмкіндігі. Мұндай дәлелдерді жинау және сақтау кезінде хэш-сома, метадеректер, лог-файлдар сияқты аутентификация құралдарын қолдану қажет, алайда бұл тәжірибе барлық жағдайда қолданылып отырған жоқ. Сонымен қатар, балалардың психологиялық жағдайын ескере отырып жүргізілетін тергеу

әрекеттері жиі түрде формалды сипат алып, баланың процесуалдық қорғанысын толық қамтамасыз ете алмауда.

Үшінші тармақ - кибергруминг бойынша сот тәжірибесі - бұл салада ұлттық құқық қолдану жүйесінің әлі де қалыптасу сатысында екенін айғақтайды. Істердің саны шектеулі, сот шешімдерінде дәлелдемелерге баға беру біркелкі емес, кей жағдайларда жыныстық ниет пен қылмыстық мақсат сот тарапынан дұрыс бағаланбайды. Сонымен қатар, баланың жауаптарын толық пайдалану, моральдық зиянды бағалау және сараптама қорытындыларына тәуелділік мәселелері де шешімін таппаған. Бұл сот практикасының бірізділігі мен әділеттілігіне теріс әсер етеді.

Осы мәселелерді ескере отырып, бөлім аясында кибергрумингке қарсы құқықтық механизмдерді жетілдіруге бағытталған нақты ұсыныстар қалыптастырылды. Атап айтқанда, Қылмыстық кодекске «Кибергруминг» деп аталатын жаңа бап енгізу, ҚПК-не сандық дәлелдемелерге қатысты арнайы норма қосу, балалармен тергеу жүргізудің бейімделген процедураларын заңмен бекіту, IT-компаниялармен өзара әрекеттесу тетіктерін құқықтық негізге қою ұсынылды. Сонымен қатар, Қазақстанның Будапешт және Ланзароте конвенцияларына қосылуы - халықаралық ынтымақтастықты нығайту мен киберқылмыстармен күрестегі ұлттық әлеуетті арттырудың өзекті бағыты ретінде негізделді.

Қорыта айтқанда, үшінші бөлімнің зерттеу нәтижелері кибергрумингке қарсы күресте құқықтық, процессуалдық және институционалдық аспектілердің өзара байланысын көрсетеді. Бұл күрделі қылмыс түріне қарсы тиімді әрекет ету үшін заңнаманы жаңғырту, халықаралық тәжірибені бейімдеу, сондай-ақ құқық қорғау органдары мен соттардың кәсіби дайындығын арттыру - алдағы кезеңдегі негізгі стратегиялық басымдықтар болуы тиіс.

ҚОРЫТЫНДЫ

Диссертациялық зерттеу жұмысы «Кибергрумингке қарсы күрестің теориялық-құқықтық және әдістемелік аспектілері» тақырыбында жүргізіліп, кәмелетке толмағандарға қатысты интернет арқылы жасалатын сексуалдық сипаттағы қылмыстардың ерекшеліктерін, оларды саралау мен дәлелдеу мәселелерін, тергеу әдістемесін және халықаралық ынтымақтастықтың рөлін кешенді түрде қарастырды.

Зерттеу барысында анықталғандай, кибергруминг - бұл дәстүрлі жыныстық қылмыстардан өзгеше, цифрлық ортада жүзеге асатын, жасөспірімдердің психикасына нысаналанған, жасырын және алдын ала дайындықпен жүргізілетін әлеуметтік-құқықтық қауіпті құбылыс. Оның құқықтық табиғатын ашу үшін тек қылмыстық құқық шеңберінде емес, сонымен бірге криминология, процессуалистика, ақпараттық технология және балалар құқығын қорғау салалары тоғысында зерттеу жүргізу қажет.

Диссертацияда келесі негізгі ғылыми тұжырымдар жасалды:

1. Кибергруминг ұғымы мен мәні нақты ғылыми-теориялық тұрғыдан негізделіп, оның қылмыстық әрекет ретіндегі элементтері (жыныстық ниет, виртуалды байланыс, сенімге кіру, азғыру, эксплуататитвті мақсат) құрылымдық түрде сипатталды.

2. Қазақстан Республикасының Қылмыстық кодексінде кибергруминг дербес қылмыстық құрам ретінде қарастырылмағаны салдарынан, құқық қорғау органдары саралау мен дәлелдеу процесінде елеулі қиындықтарға тап болуда. Қолданыстағы 124-бап кибергрумингтің заманауи формаларын қамтымайды.

3. Сандық дәлелдемелермен жұмыс істеу тәртібі заңнамалық деңгейде нақты регламенттелмеген, бұл олардың заңды күшке ие болуына кедергі келтіреді және сотта қолданылуын қиындатады.

4. Кибергрумингке қатысты істерді тергеу барысында кәмелетке толмаған жәбірленушінің психоэмоционалдық жағдайы, жауап алу әдістемесінің жетілмегендігі, мамандандырылған тергеу кадрларының тапшылығы — тергеу сапасына тікелей әсер ететін факторлар ретінде танылды.

5. Қазақстандағы сот тәжірибесі кибергрумингке байланысты істер бойынша тұрақты және бірізді емес. Электрондық дәлелдемелердің қабылдануы мен бағалануы әртүрлі аймақтарда біркелкі жүргізілмейді. Баланың жауабы мен сараптама қорытындыларына тәуелділік өте жоғары.

6. Халықаралық тәжірибе (Германия, Ұлыбритания, Канада, ЕО елдері) кибергрумингті құқықтық алдын алу тәсілдерімен, дербес қылмыстық құрам ретінде тану арқылы тиімді реттеп отырғанын көрсетті.

7. Қазақстан Республикасының Будапешт және Ланзароте конвенцияларына қосылуы электрондық дәлелдемелермен трансшекаралық әрекеттесу, кәмелетке толмағандарды қорғау саласында халықаралық стандарттарды енгізуге мүмкіндік береді.

ПАЙДАЛАНЫЛҒАН ДЕРЕККӨЗДЕРДІҢ ТІЗІМІ

1 Борисенко Е.В., Дозорцева Е.Г., Бадмаева В.Д., Чибисова И.А. Показатели виктимности у несовершеннолетних потерпевших от сексуального насилия и злоупотребления // Психология и право. - 2021. - Т. 11. № 2. - С.132-145.

2 Қазақстан Республикасының Қылмыстық кодексі.2014 жылғы 3 шілдедегі №226-V ҚРЗ [Электрондық ресурс] – Айналыс режимі: https://adilet.zan.kz/kaz/docs/K1400000226 - (жүгінген күні: 09.02.2025).

3 Мальцева Т.В. Психологические портреты лиц, совершивших или пытавшихся совершить сексуальное преступление в отношении несовершеннолетних // Прикладная психология и педагогика. - 2024. - Т. 9. № 3. С. 51-56.

4 EU Kids Online 2020: Survey results from 19 countries. - 2020. - [Электронный ресурс] – Режим доступа: https://eprints.lse.ac.uk/103294/1/EU_Kids_Online_2020_March2020.pdf (дата обращения: 09.02.2025).

5 Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: научно-практический комментарий и перевод текста закона. 2-е издание. - Москва: Проспект, 2014. – 637. с.
6 Thorn. Self-Generated Child Sexual Abuse Material: Attitudes and Experiences. Complete findings from 2019 qualitative and quantitative research among 9-17 year olds and caregivers. - 2020. – [Электронный ресурс] – Режим доступа: https://info.thorn.org/hubfs/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf . (дата обращения: 12.02.2025).
7 Годовой отчет 2019 Детского фонда ООН (ЮНИСЕФ) в Казахстане. - Алматы, 2019. - [Электронный ресурс] – Режим доступа: https://www.unicef.org/kazakhstan/media/5476/file/Годовой%20отчет%202019.pdf. (дата обращение: 20.02.2025).
8 Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы «Дербес деректер және оларды қорғау туралы». [Электрондық ресурс] – Айналыс режимі: http://10.61.42.188/kaz/docs/Z1300000094 - (жүгінген күні: 09.02.2025).
9 FBI Releases 2022 Crime in the Nation Statistics. - 2023. [Электронный ресурс] - Режим доступа: https://www.fbi.gov/news/press-releases/fbi-releases-2022-crime-in-the-nation-statistics?utm_source. (дата обращение: 27.02.2025).
10 Қазақстан Республикасының Бас прокуратурасы. Қылмыстық статистика жылнамасы. - Астана, 2023. – 120 б.
11 Исследование детского контента в Казахстане. - Астана: НАО «Казахстанский институт общественного развития», 2023. – 182. с.
12 Circular No. 2017/01. TITLE: Sexual Communication with a Child: Implementation of Section 67 of the Serious Crime Act 2015. - 2017. -[Электронный ресурс] Режим доступа: https://assets.publishing. service.gov.uk/media/ 5a7500cae5274a3cb2868e4e/circular-commencement-s67-serious-crime-act-2015.pdf. (дата обращение: 10.03.2025).
13 Джакишева Х.М. Опыт Германии по профилактике вовлечения несовершеннолетних в совершение уголовных правонарушений посредством сети Интернет // Международный научный журнал «Вестник науки». - 2024. - №7 (76). - С. 89-92.
14 Нургазинов Б.К., Баймухаметов Е.И. Совершенствование норм, касающихся противодействия уголовным правонарушениям против половой неприкосновенности несовершеннолетних // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. - 2016.№9 - С. 110-114.
15 Сейджанов О.Т. Расследование в цифровых условиях // Сборник научных трудов Международной научно-практической конференции «Опыт и традиции подготовки полицейских кадров». - Волгоград, 2023. – С.145-149.
16 Калкаева Н., Избасова А., Бұғыбай Д. Некоторые вопросы профилактики кибербуллинга в Республике Казахстан // Вестник Евразийского национального университета имени Л.Н. Гумилева. - 2023 - С. 91-99

17 Europol. 2020 EU IRU Transparency Report. - 2021. Publications Office of the European Union, Luxembourg.
18 Годовой отчет 2022 Детского фонда ООН (ЮНИСЕФ) в Казахстане. - Алматы, 2022. [Электронный ресурс] - Режим доступа: https://www.unicef.org/kazakhstan/media/10411/file/Годовой%20отчет%20Детского%20Фонда%20ООН%20(ЮНИСЕФ)%20в%20Казахстане%20%7C%202022%20год.pdf
19 Сафуанов Ф.С., Назарова Е.А. Сравнительный анализ различных методов составления психологического портрета предполагаемого преступника // Психология и право. - 2011. С. 1-11.
20 Годовой отчет 2021 Детского фонда ООН (ЮНИСЕФ) в Казахстане. - Алматы, 2021 [Электронный ресурс] - Режим доступа: https://www.unicef.org/kazakhstan/media/8921/file/Annual%20Report%202021%20RU.pdf.
21 Плаксина К.Ю. Оценка правонарушений несовершеннолетних в цифровой среде // Международный научный журнал «Вестник науки». - 2018. - № 8 (8). - Т. 2. - Ноябрь. - С. 108-113.
22 Медведева А.С., Дозорцева Е.Г. Роль и участие родителей в процессе кибергруминга // Психология и право. - 2021. - Т. 11. № 2. – С.146-159.
23 Пинкевич Т.В. Криминальные угрозы и криминогенные риски преступлений, совершаемых в отношении несовершеннолетних с использованием цифровых технологий // Вестник Казанского юридического института МВД России. - 2024. - № 2. - С.137-145.
24 Защита детей от насилия. Международная научно-практическая конференция «Актуальные проблемы защиты прав несовершеннолетних жертв насилия». - Университет Нархоз, Алматы, 12.2023 г. [Электронный ресурс] - Режим доступа: https://online.zakon.kz/Document/?doc_id=31961799&utm_source=chatgpt.com&pos=3;-88#pos=3;-88. Дата обращение: 17.03.2025.
25 Papoyan V., Galstyan A., Muradyan E., Poghosyan R., & Manukyan M. Adolescent Behavior on Social Networks in the Context of Safety // Bulletin of Yerevan University E: Philosophy, Psychology. - 2024. 15(1) (43), 65-75.
26 Сустина Т.И. Информационная безопасность детей: особенности правового регулирования. // Аграрное и земельное право. - 2021. № 9 (201). - С. 226-229.
27 Медведева А.С. Кибергруминг и способы противодействия ему // Цифровая гуманитаристика и технологии в образовании (DHTE 2020). Сборник материалов Всероссийской научно-практической конференции с международным участием. - 2020. - С. 292-296.
28 Рахымжанова Д.М. Кибербуллинг және кибергрумингке қарсы ұлттық құқықтық тетіктер // Заң және мемлекет. - 2023. - №4. - С.16-21.
29 Ғабдуллин Е.М. Кәмелетке толмағандарға қарсы қылмыстардың криминологиялық сипаттамасы. - Алматы, 2021. - 132. с.
30 Нарикбаев М. Проблемы квалификации преступлений против несовершеннолетних // Вестник КазГЮУ. - 2022. - №2. - С. 45-49.

31 Ахметов Н. Сот тәжірибесінде дәлелдемелерді бағалау проблемалары // Заң журналы. - 2021. - №3. - С. 23-29.
32 Мұқанова Г.Ц. Электрондық дәлелдемелердің заңдылығы: теория мен практика // ҚазҰУ Хабаршысы. - 2021. - №3. - С. 31-36.
33 Әбуов Р. Қазақстан Республикасының киберқауіпсіздік саясаты: құқықтық аспектілер. - Алматы: Эверо, 2020. – 144. с.
34 Tanczer L.M. Online Harms and Platform Responsibility. - Oxford: Hart Publishing, 2022. - 118 p.
35 Baines V., Wall D. The Challenges of Digital Evidence // British Journal of Criminology. - 2020. - Vol. 60, №1. - P. 98-112.
36 Смагулов Н.С. Киберқылмыстармен күресудің құқықтық негіздері. - Алматы: Заң, 2022. – 224. с.

ҚОСЫМША 1

Жоба

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БАС ПРОКУРАТУРАСЫНЫҢ ЖАНЫНДАҒЫ ҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫ АКАДЕМИЯСЫ

«Кибергрумминг» қылмыстарын тергеу бойынша ұсынылатын АЛГОРИТМ

Қосшы қ., 2025 ж.

Мазмұны

КІРІСПЕ

Ақпараттық технологиялардың қарқынды дамуы қоғам өмірінің барлық саласына әсер етіп, құқық қорғау саласы үшін де жаңа сын-қатерлер туындатты. Интернет кеңістігіндегі қауіптер әсіресе кәмелетке толмаған балалар мен жасөспірімдерге қатысты аса өзекті болып отыр. Соңғы жылдары балаларды интернет арқылы арбау, яғни кибергруминг құбылысы алаңдататын деңгейге жетті. Бұл — әлеуметтену және коммуникация құралдарын теріс пайдалану арқылы баланың сеніміне кіріп, жыныстық сипаттағы әрекеттерге итермелеуді білдіретін күрделі, жасырын және көп сатылы процесс.

Кибергруминг қылмыстары көбіне әлеуметтік желілер, мессенджерлер, бейне чаттар немесе онлайн ойындар арқылы жасалады. Мұндай жағдайларда қылмыскер жасөспірімнің сеніміне кіріп, оған түрлі уәделер беріп, психологиялық манипуляция арқылы өзін жақын дос, тіпті құрбы ретінде көрсетуі мүмкін. Бұл процестің ерекшелігі — оның виртуалды ортада жасырын түрде өтуі, сондықтан да мұндай қылмыстарды дер кезінде анықтап, тергеу жүргізу күрделі іс болып табылады.

Қазақстан Республикасында кибергруминг ұғымы заңнамалық деңгейде нақты белгіленбеген. ҚР Қылмыстық кодексінде кәмелетке толмағандарға қатысты жасалатын жыныстық сипаттағы әрекеттерге арналған баптар бар болғанымен, интернет арқылы жүзеге асатын дайындық әрекеттерді жеке қылмыстық құрам ретінде тану мәселесі ашық қалып отыр. Бұл тергеу мен дәлелдемелерді жинау барысындағы құқықтық олқылықтарға әкелуде. Сонымен қатар, қазіргі тергеу тәжірибесінде цифрлық дәлелдемелерді жинау, сақтау және құқықтық рәсімдеу мәселелері де өзекті күйде қалып отыр.

Осыған орай, бұл әдістемелік құралдың мақсаты – кибергрумингпен байланысты қылмыстарды тергеу барысында кездесетін негізгі проблемаларды ғылыми тұрғыдан жүйелеу, тергеу жүргізудің алгоритмін әзірлеу және осы салада қолданылатын құқықтық, процессуалдық және техникалық тәсілдерге талдау жасау. Құралда халықаралық тәжірибе мен қолданыстағы отандық заңнама негізінде нақты ұсыныстар мен тиімді шешім жолдары ұсынылады.

Бұл әдістемелік құрал құқық қорғау органдарының тергеу бөлімшелерінде қызмет ететін мамандарға, сонымен қатар Академия курсанттары мен магистранттарына арналған оқу-әдістемелік көмекші құрал ретінде дайындалды. Мұндағы тұжырымдар мен ұсыныстар автор жүргізген ғылыми зерттеудің нәтижелеріне негізделген және практикалық қызметте қолдануға бағытталған.

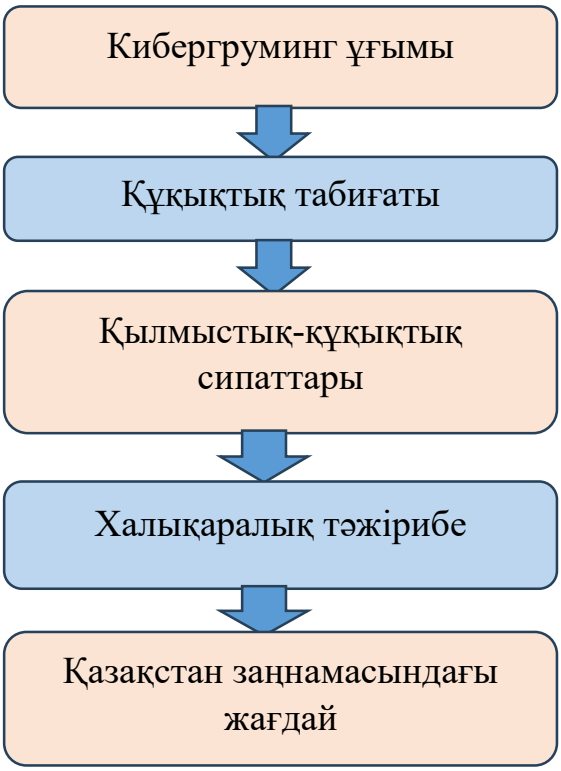
1. КИБЕРГРУМИНГТІҢ ТЕОРИЯЛЫҚ-ҚҰҚЫҚТЫҚ НЕГІЗДЕРІ

Кибергруминг – бұл кәмелетке толмаған балалар мен жасөспірімдерге қарсы интернет арқылы жасалатын жасырын, кезеңдік сипаттағы қылмыстық әрекет. Ағылшын тіліндегі “cyber grooming” сөзі тікелей аударғанда «желідегі арбау» деген мағына береді. Бұл әрекет, әдетте, қылмыскердің баламен сенімге негізделген байланыс орнатуынан басталып, біртіндеп оның жеке өміріне араласуына, жыныстық сипаттағы әрекеттерге тартуға немесе кездесуге шақыруға ұласуы мүмкін.

Кибергруминг әрекеттері негізінен әлеуметтік желілер, мессенджерлер (WhatsApp, Telegram, Instagram), онлайн ойын платформалары, бейне-чаттар арқылы жүзеге асады. Қылмыскер жалған аккаунттар пайдаланып, өзін бала немесе жасөспірім ретінде көрсетеді, сенімге кіріп, баланың психикасына әсер етеді. Бұл әрекеттер бір қарағанда қылмыс ретінде көрінбеуі мүмкін, өйткені нақты зорлық немесе физикалық байланыс орын алмайды. Дегенмен, бұл – қылмысқа дайындықтың жасырын формасы және аса қауіпті тенденция.

Психологиялық тұрғыда кибергруминг ұзақ мерзімді манипуляцияға негізделген. Ол бірнеше кезеңнен тұрады:

1. Баламен байланыс орнату;
2. Эмоционалдық сенімге кіру;
3. Жеке ақпараттар жинау (мекен-жайы, мектебі, суреттері);
4. Бейімдеу және ықпал ету;
5. Жыныстық сипаттағы сұраныстар немесе нақты әрекеттерге итермелеу.



Сурет 1. Кибергруминг ұғымы

Қазақстан Республикасының қолданыстағы қылмыстық заңнамасында «кибергруминг» термині нақты заңдық дефиниция ретінде бекітілмеген. Алайда,

бұл әрекеттердің жекелеген элементтері ҚР Қылмыстық кодексінің келесі баптарымен қамтылуы мүмкін:

- ҚР ҚК 124-бабы – Жас балаларды азғындық жолға түсіру;
- ҚР ҚК 122-бабы – Он алты жасқа толмаған адаммен жыныстық қатынас жасау немесе сексуалдық сипаттағы өзге де әрекеттер жасау;
- ҚР ҚК 147-бабы – Жеке өмірге қол сұғушылық;
- ҚР ҚК 273-бабы – Қоғамдық тәртіпке қауіп төндіретін ақпарат тарату;
- ҚР ҚК 274-бабы – Жалған ақпарат тарату;
- ҚР ҚК 125-бабы – Адам ұрлау (егер күдікті баланы кездесуге шақырса немесе алып кетсе).

Алайда бұл баптар нақты кибергруминг әрекеттерінің дайындық кезеңдерін толық қамтымайды, әсіресе физикалық байланыс орнамаған жағдайда құқық қолдану органдары нақты қылмыс құрамын дәлелдеу қиындықтарына тап болады. Сол себепті Қазақстанда кибергрумингті жеке қылмыстық құрам ретінде заңнамаға енгізу қажеттілігі туындап отыр.

Көптеген дамыған елдерде кибергруминг заңнамалық деңгейде дербес қылмыс ретінде танылған. Мысалы:

- Германия: Қылмыстық кодексінің §176-бабы бойынша, егер ересек адам интернет арқылы 14 жасқа толмаған баламен жыныстық сипаттағы әрекетке итермелеу мақсатында байланыс орнатса, бұл әрекет үшін қылмыстық жауапкершілік қарастырылады, тіпті нақты әрекет орын алмаған күннің өзінде.
- Ұлыбритания: 2003 жылғы Сексуалдық қылмыстар туралы Заңға сәйкес, кәмелетке толмаған адаммен интернет арқылы байланыс орнатып, оны кездесуге шақыру немесе сенімге кіру әрекеті – “grooming offence” ретінде танылып, нақты қылмыстық жауапкершілікке тартылады.
- АҚШ: Федералдық деңгейде “enticement of a minor” немесе “online solicitation” ретінде қарастырылып, ФБР және басқа федералдық органдар бақылау жүргізеді.

Сондай-ақ, Қазақстан Ланзароте конвенциясына (Кәмелетке толмағандарды жыныстық қанаудан қорғау туралы) және Будапешт конвенциясына (Киберқылмыс туралы) қосылмаған, бұл халықаралық ынтымақтастық пен электрондық дәлелдемелер алмасу ісінде елеулі шектеу туындатады.

Кибергруминг – бұл дайындық қылмысы ретінде күрделі заңи және психологиялық мәнге ие құбылыс. Қолданыстағы ҚР ҚК мен ҚПК-де бұл әрекетке нақты баптар арналмағандықтан, тергеушілер мен прокурорлар құқық қолдану кезінде құқықтық олқылықтарға тап болады. Осы себепті:

- ҚР ҚК-не «Кибергруминг» ұғымын жеке құрам ретінде енгізу;
- ҚР ҚПК-не сандық дәлелдемелерді жинау, тіркеу және сараптау тәртібін нақты көрсету;

- Халықаралық құқықтық келісімдерге қосылу (Будапешт, Ланзароте) – Қазақстандағы балалардың ақпараттық кеңістіктегі қауіпсіздігін қамтамасыз етудің құқықтық негізін күшейтуге мүмкіндік береді.

2. КИБЕРГРУМИНГТІ ТЕРГЕУДІҢ ӘДІСТЕМЕЛІК АСПЕКТІЛЕРІ

2.1. Тергеуді ұйымдастырудың жалпы қағидаттары

Кибергруминг қылмыстарын тергеу – бұл дәстүрлі тергеу амалдарынан өзгеше, кешенді дайындықты, құқықтық, техникалық және психологиялық білімді қажет ететін күрделі процесс. Мұндай қылмыстардың ерекшелігі – олардың виртуалды кеңістікте жасалуы, нақты физикалық байланыстың болмауы және қылмыс құрамы көбінесе дайындық немесе әлі жүзеге аспаған деңгейде қалуы. Осыған байланысты тергеуді ұйымдастыру барысында арнайы қағидаттарды сақтау маңызды.

Бірінші қағида – кәмелетке толмаған жәбірленушілерді қорғау.

Кибергруминг қылмыстарының басты құрбаны – кәмелетке толмаған балалар. Сондықтан тергеудің барлық кезеңінде ҚР ҚПК 223-бабына және ҚР «Баланың құқықтары туралы» Заңының талаптарына сәйкес, баланың құқықтары мен психологиялық жай-күйі ескерілуі тиіс. Бұл жәбірленушімен сұхбат кезінде психологтың қатысуын, бейнежазба жүргізуді және балаға психологиялық қысым жасалмауын көздейді.

Екінші қағида – тергеудің бастапқы кезеңінен бастап дәлелдемелерді қорғау.

Сандық дәлелдемелер – бұл тез өзгеретін және жойылып кетуі мүмкін ақпарат көздері. Сондықтан тергеу басталған сәттен бастап скриншоттар, хабарламалар, бейнематериалдар, электрондық хат алмасулар, лог-файлдар дереу сақталып, олардың түпнұсқалығы мен өзгеріске ұшырамауын қамтамасыз ету қажет. ҚР ҚПК 221-бабына сәйкес, дәлелдемелер заңды жолмен алынып, хаттамаланып, процессуалдық тұрғыдан бекітілуі тиіс. Бұл – сот барысында олардың жарамдылығын қамтамасыз етудің алғышарты.

Үшінші қағида – жедел-іздестіру мен процессуалдық тергеу әрекеттерін қатар жүргізу.

Кибергруминг бойынша күдіктілердің көпшілігі фейк аккаунттармен әрекет ететіндіктен, олардың тұлғасын нақтылау үшін жедел іздестіру шаралары (IP-мекенжайын анықтау, провайдерден мәліметтер сұрау, құрылғы идентификаторларын бақылау) уақытында жүргізілуі қажет. Бұл – ҚР «Жедел-іздестіру қызметі туралы» Заңы мен ҚПК 199-бабына сәйкес іске асырылады.

Төртінші қағида – мультидисциплинарлық тәсіл.

Кибергруминг – бұл тек қана құқық бұзушылық емес, ол – психологиялық, педагогикалық және техникалық аспектілерді қамтитын құбылыс. Тергеу кезінде тергеуші IT-мамандармен, психологтармен, кәмелетке толмағандар ісі жөніндегі инспекторлармен, қажет жағдайда педагогтармен бірлесіп жұмыс жүргізуі тиіс. Осындай кешенді амал – істің объективті және әділ қаралуын қамтамасыз етеді.

Бесінші қағида – жәбірленушінің құпиялылығын және қауіпсіздігін қамтамасыз ету.

Көп жағдайда кибергрумингке ұшыраған балаларда ұялу, үрейлену, өзін кінәлі сезіну синдромдары болады. Тергеуші жәбірленушінің жеке басын жарияламау, ақпараттың таралуына жол бермеу және істі жариялы түрде қараудан сақтау шараларын қарастыруы тиіс. Бұл ҚР ҚПК 201-бабына – қылмыстық процестегі құпиялылық қағидатына – сай жүзеге асырылады.

Алтыншы қағида – халықаралық өзара іс-қимыл мен техникалық көмек.

Көптеген интернет-платформалар мен сервистердің серверлері шет мемлекеттерде орналасқан. Мысалы, Meta (Facebook, Instagram), TikTok, Telegram деректерін алу үшін халықаралық құқықтық көмек тетіктерін іске қосу қажет болады. Бұл Будапешт конвенциясына қосылу қажеттігін туындатады. ҚР ҚПК 501–508-баптарында халықаралық құқықтық көмек көрсету тәртібі баяндалған.

Жетінші қағида – іс материалдарын құрылымдау және жүйелеу.

Тергеу барысында алынған дәлелдер, сараптамалар, жауаптар, сипаттамалар электрондық және қағаз нұсқада жүйеленіп, әрбір кезең нақты хронологиямен белгіленіп отыруы қажет. Бұл істі сотқа жолдаған кезде материалдың айқындылығын және дәлелдемелік базаның беріктігін қамтамасыз етеді.

Осы аталған қағидаттарды сақтай отырып жүргізілген тергеу ғана кибергруминг қылмыстарының толық әрі әділ ашылуына мүмкіндік береді. Тергеуді ұйымдастыруда жоғарыда көрсетілген қағидаларды нақты іс жүзінде қолдану – тергеушінің кәсіби біліктілігі мен заңға бағынуының көрсеткіші болып табылады.

2.2. Тергеу бастамасы: арыз, хабарлама, мониторинг

Кибергруминг бойынша қылмыстық тергеу әдетте жәбірленушінің немесе оның заңды өкілінің арызы, құқық қорғау органдарына келіп түскен анонимді хабарлама немесе интернеттегі күмәнді әрекеттерді тіркеу нәтижесінде басталады. Бұл – тергеудің бастапқы және ең маңызды кезеңі. Өйткені дәл осы сәттен бастап барлық дәлелдер заңды түрде тіркеліп, іс жүргізу процессіне айналады.

1. Арыз және хабарлама негізінде іс қозғау

Қазақстан Республикасының Қылмыстық-процестік кодексінің (ҚПК) 179-бабына сәйкес, қылмыстық құқық бұзушылық белгілері бар арыз немесе хабарлама тіркелуге тиіс. Кибергруминг жағдайында арыз көбінесе ата-аналар, туыстар немесе мектеп әкімшілігі тарапынан түседі. Арызда келесі негізгі элементтер болуы мүмкін:

- Балаға бағытталған күмәнді хат-хабарлар (мессенджердегі скриншоттар);
- Құқыққа қайшы мінез-құлыққа шақыру немесе сұраныстар;
- Бала психикасына теріс әсер еткен интернеттегі оқиға.

Арыз тіркелгеннен кейін құқық қорғау органы қылмыстық құқық бұзушылық белгілері бар-жоғын тексереді. Бұл кезеңде жедел-іздестіру іс-шараларын бастауға болады (ҚПК 190-бап).

2. Ішкі және сыртқы мониторинг тетіктері

Көп жағдайда жәбірленуші кибергрумингтің құрбаны болғанын түсінбейді немесе бұл туралы айтуға қорқады. Осы себепті тергеу органдарының өз бетінше проактивті әрекет етуі аса маңызды.

Ішкі мониторинг – бұл Қазақстан Республикасының ішкі ақпараттық жүйелері арқылы жүзеге асады. Бұған жататындар:

- Мектептер мен білім беру мекемелерімен байланыс (психологтардың есебі);

- «Киберқадағалау» бөлімшелерінің деректерін талдау;

- Бұрын тіркелген ұқсас қылмыстар бойынша күдіктілер базасымен жұмыс.

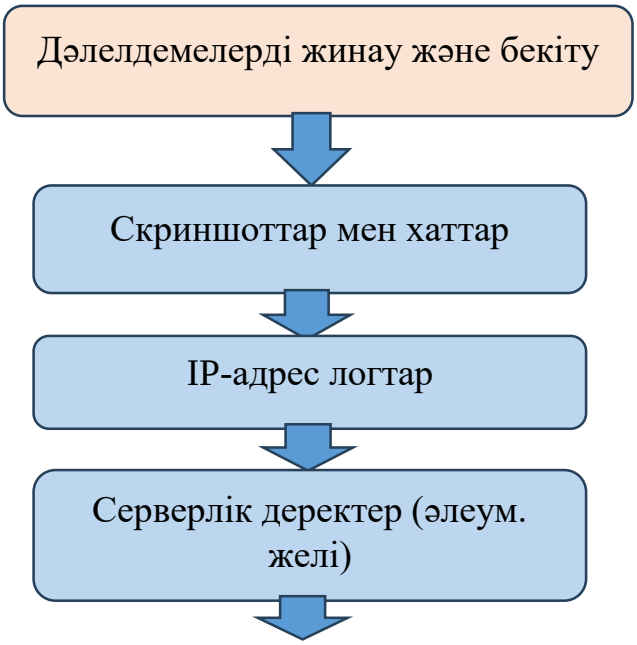
- Сыртқы мониторинг – бұл ашық интернет кеңістігі мен әлеуметтік желілерді қадағалауға негізделеді:

- Әлеуметтік желілер мен мессенджерлердегі күмәнді аккаунттарды бақылау;

- Telegram, Instagram, TikTok платформаларындағы ашық топтар мен форумдарды сараптау;

- Интернет-провайдерлермен бірлескен жұмыс.

Бұл ретте ҚР ІІМ жанынан құрылған Киберқылмысқа қарсы күрес басқармасының техникалық ресурстары кеңінен қолданылады. Жеке тұлғалар туралы деректерді талдау, IP-адресті нақтылау және лог файлдарды алу – алғашқы дәлелдер жинауда шешуші рөл атқарады.



Сурет 2. Дәлелдемелерді жинау және бекіту

3. Қылмыстық іс қозғау шарттары

ҚР ҚПК 179-бабына сәйкес, іс қозғау үшін жеткілікті негіздер қажет. Кибергруминг жағдайында бұл негіздер ретінде мыналар танылады:

- Цифрлық скриншоттар немесе экран жазбалары;
- Жәбірленушінің жауаптары немесе куәлік етуі;
- Техникалық сараптама қорытындылары (қажет болса – алдын ала тексеру барысында);
- Психологтың қорытындысы (балаға әсер деңгейі жөнінде).

Тергеуші бұл дәлелдерді жинақтап, ҚР ҚПК 179-бабы 2-бөлігінің негізінде қылмыстық іс қозғау туралы қаулы шығарады. Бұдан кейін процессуалдық әрекеттердің келесі кезеңі басталады: дәлелдерді заңды жолмен жинау, сараптама тағайындау және жауап алуды ұйымдастыру.

4. Мониторинг нәтижелерімен жедел әрекет ету

Интернетте таралған кез келген күмәнді хабарлама, мысалы, жасөспірімдермен ашық флирт, сексуалдық сипаттағы сөйлемдер, жеке деректерді сұрау секілді белгілер тергеу органы тарапынан жедел әрекет ету үшін жеткілікті негіз болып табылады.

Мұндай жағдайларда тергеу органы мынадай шаралар қолдануы мүмкін:

- Әлеуметтік желі әкімшілігіне ресми сұраныс жіберу;
- Аккаунт иесін нақтылау мақсатында IP-адрес пен құрылғы идентификаторын сұрату;
- Хат алмасулардың көшірмесін алу;
- Скриншоттарды хэш-сомамен бірге тіркеу.

5. Тергеу әрекеттерін кешіктірмеу принципі

Кибергруминг – бұл тез жойылып кететін электрондық іздермен байланысты қылмыс. Сондықтан ҚР ҚПК 24-бабы негізінде, тергеу әрекеттері «дер кезінде және тиімді» жүргізілуі тиіс. Кешігу – дәлелдердің жойылып кетуіне немесе күдіктінің жасырынуына алып келуі мүмкін.

2.3. Сандық дәлелдемелермен жұмыс

Кибергруминг істері бойынша тергеудің нәтижелігі ең алдымен сандық дәлелдемелерді дұрыс жинау, сақтау және талдау процесіне байланысты. Бұл дәлелдер – қылмыс жасалған интернет кеңістігінен алынатын ақпараттар жиынтығы. Олардың ішінде: әлеуметтік желідегі хат алмасулар, мессенджердегі скриншоттар, лог-файлдар, IP-мекенжайлар, бейнежазбалар, мультимедиа файлдары және құрылғылардан алынған техникалық деректер бар.

Сандық дәлелдемелердің түрлері

№	Түрі	Қысқаша сипаттамасы
1	Скриншоттар	Экран суреттері – визуалды дәлел, хронологияны береді
2	Хат-хабар журналдары	Мессенджерлердегі хат алмасу – оқиға динамикасын көрсетеді
3	IP-адрестік логтар	Күдіктінің құрылғысының орналасқан жерін анықтауға мүмкіндік береді
4	Фото/бейнефайлдар	Қылмыстық әрекетті дәлелдейтін тікелей материалдар
5	Серверлік мәліметтер	Провайдерлерден алынатын техникалық ақпараттар
6	Метадеректер	Файлдың жасалған уақыты, авторы, құрылғы түрі және басқа да техникалық сипаттамалар

1 - кесте

2. Сандық дәлелдемелерді жинау тәртібі

Сандық дәлелдемелер ҚР ҚПК-нің 125-бабына және 221-бабына сәйкес заңды түрде рәсімделуі тиіс. Бұл үшін тергеуші:

- Скриншот немесе басқа да цифрлық файлдарды түпнұсқалық сақталған күйде алуы тиіс (хэш-сома арқылы);
- Құрылғыны алу кезінде техникалық маманның қатысуын қамтамасыз ету;
- Хаттама жасай отырып дәлелдемені тіркеу (құжатта кімнен, қашан, қандай жолмен алынғаны көрсетілуі тиіс);
- Электрондық ақпаратты қайта жазуға жол берілмейтін тасымалдаушыға көшіру.

Ескерту: Тергеу барысында алынған скриншоттарды нотариалды куәландыру қажет емес, бірақ оларды растау үшін техникалық сараптама мен куәгерлердің түсініктемелері қолданылады.

3. Дәлелдемелердің өзгермегенін дәлелдеу (хэш)

Цифрлық файлдың түпнұсқалығын сақтау мақсатында хэш-сома (MD5 немесе SHA256) қолданылады. Бұл – кез келген файл үшін берілетін бірегей сандық «із». Егер файл өзгерсе – хэш те өзгереді. Сондықтан:

- Скриншоттар мен файлдарды алып жатқанда хэш мәні есептеліп, хаттамада көрсетілуі қажет;
- Бұл процесс сараптама тағайындау алдында жүргізіледі;
- Хэш есептеу үшін құқық қорғау органдарында қолданылатын лицензияланған бағдарламалар (мысалы, Autopsy, FTK Imager) пайдаланылады.

4. Провайдерлермен және платформалармен өзара іс-қимыл

Көптеген кибергруминг жағдайларында тергеу барысында мессенджерлер мен әлеуметтік желі әкімшіліктерінен мәліметтер алу қажет болады. Бұл:

- IP-адрес пен тіркелген құрылғы туралы ақпарат;
- Хат-хабардың серверлік көшірмелері;
- Аккаунт ашылған уақыт пен белсенділік тарихы.

Қазақстан Республикасында бұл әрекеттер «Байланыс туралы» Заң мен ҚР ҚПК 248-бабына сәйкес сұраныс арқылы орындалады. Алайда Meta (Facebook, Instagram), Telegram, TikTok секілді шетелдік платформалармен ақпарат алмасу үшін халықаралық құқықтық көмек тетіктерін іске қосу қажет болады.

5. Сандық сараптама

Жинақталған сандық дәлелдемелер ҚР ҚПК 277-бабына сәйкес сараптама тағайындау арқылы зерттеледі. Сандық сараптама кезінде:

- Құрылғылардан алынған файлдардың түпнұсқалығы тексеріледі;
- Файлдардың редакцияланған, жойылған-жойылмағаны анықталады;
- Скриншот немесе хабарламаның нақты уақыт бойынша сәйкестігі талданады.

Сараптама қорытындысы істің дәлелдеу базасының ажырамас бөлігіне айналады және оның сапасына тергеудің нәтижесі тікелей байланысты.

6. Сандық дәлелдемелерді сақтау және құпиялылық

Тергеуші алған барлық сандық материалдар:

- Қауіпсіз серверде немесе ақпаратты заңды сақтау орны (мысалы, ІІМ орталық сервері) арқылы сақталуы тиіс;
- Үшінші тұлғаларға қолжетімсіз болуы керек;
- Құпиялылық режимінде жүргізіледі (ҚР ҚПК 201-бабы).

Сандық дәлелдемелер – кибергруминг істеріндегі басты әрі шешуші фактор. Олармен жұмыс жүргізу – заң талаптарына қатаң сәйкестікпен, арнайы техникалық біліммен және жоғары дәлдікпен жүргізілуі тиіс. Тергеуші дәлелдемелердің жарамдылығын қамтамасыз ету үшін тек жинақтап қана қоймай, оларды дұрыс рәсімдеп, процессуалдық тұрғыдан сенімді етуге міндетті.

2.4. Арнайы сараптамалар

Кибергрумингпен байланысты қылмыстық істерді тергеу барысында арнайы сараптамалар – дәлелдемелерді нақтылау мен оқиғаның мән-жайын объективті анықтаудың ажырамас құралы болып табылады. Бұл қылмыс түрінің күрделілігі, жасырын түрде интернет кеңістігінде жүзеге асуы және жәбірленушінің кәмелетке толмағандығы – тергеушіден тек құқықтық емес, сонымен қатар психологиялық және техникалық терең талдау жүргізуді талап етеді. Сондықтан бірнеше сараптама түрі міндетті түрде қолданылады.

1. Психологиялық сараптама

Мақсаты:

Жәбірленушінің психологиялық жай-күйін, қорқыныш деңгейін, психикалық жарақатты және кәмелетке толмаған тұлғаның оқиғаға көзқарасын бағалау.

Міндеттері:

- Баланың жыныстық сипаттағы ұсыныстарды қалай қабылдағанын анықтау;
- Қылмыстық әрекеттің бала психикасына әсерін бағалау;
- Балаға қысым, қорқыту, сенімге кіру әрекеттерінің болған-болмағанын талдау.

Құқықтық негіз:

ҚР ҚПК 275-бабына сәйкес, егер зерттеу объектісі адам психикасы мен мінез-құлқына қатысты болса, сот-психологиялық сараптама тағайындалады.

Сараптаманы тағайындау кезінде ескерілетін сұрақтар:

- Жәбірленуші кибергруминг элементтерін түсіне алды ма?
- Оған психологиялық қысым жасалды ма?
- Жәбірленуші өз еркімен хат-хабар алмасуға барған ба?
- Жәбірленушінің психикалық даму деңгейі жас ерекшелігіне сәйкес келе ме?
- Сіз бұл адаммен қалай және қайда таныстыңыз?
- Ол адам сізбен қандай тақырыпта сөйлесті?
- Сізден қандай фотоларды немесе ақпараттарды сұрады?
- Ол сізге қысым көрсетті ме немесе қорқытты ма?
- Оның айтқандары сізге қандай эмоция тудырды?
- Ол сізді жеке кездесуге шақырды ма?
- Осы жағдай сіздің көңіл-күйіңізге, ұйқыңызға, сабағыңызға әсер етті ме?

2. Психолингвистикалық сараптама

Мақсаты:

Хат алмасулар мен мәтіндік материалдардағы жасырын мағына, ниет және коммуникативтік ықпал деңгейін анықтау.

Міндеттері:

- Мәтін ішінде жыныстық сипаттағы немесе азғындыққа итермелейтін жасырын астарды анықтау;

- Сенімге кіру немесе манипуляция жасау тәсілдерін лингвистикалық тұрғыдан сипаттау;
- Хабарламалардың адресатқа бағытталғанын және қандай ниетпен жазылғанын саралау.

Қолданыс:

Бұл сараптама WhatsApp, Telegram, Instagram, TikTok сияқты платформалардағы хат алмасуларға жүргізіледі. Психолингвист мамандар белгілі сөз қолданыстары, контекст, метафоралар, агрессия не жұмсақ сендіру стратегияларын анықтайды.

Сараптамалық сұрақтар мысалдары:

- Хатта жыныстық сипаттағы ниет байқала ма?
- Бұл мәтін баланың сеніміне кіру мақсатында жазылған ба?
- Автордың ниеті қандай?
- Талдауға ұсынылған мәтіндерде кәмелетке толмаған тұлғаға қатысты жыныстық сипаттағы мазмұн бар ма?
- Бұл хабарламаларда азғыру, жыныстық қатынасқа итермелеу элементтері байқала ма?
- Қолданылған лексика мен фразеологизмдер қай мазмұнды білдіреді?
- Мәтінде қандай сөйлеу актілері (сұраныс, бұйрық, уәде, қорқыту, сендіру) бар?

3. Компьютерлік-техникалық сараптама

Мақсаты:

Цифрлық дәлелдердің техникалық параметрлерін, файлдардың түпнұсқалығын және олармен қандай құрылғы арқылы жұмыс жасалғанын анықтау.

Міндеттері:

- Скриншоттардың, бейнематериалдардың өзгертілмегенін анықтау;
- Құрылғылардан алынған деректердің метаақпараты арқылы файлдың қашан жасалғанын және қандай бағдарламамен ашылғанын дәлелдеу;
- Аккаунт иесінің IP-адресі мен құрылғы идентификаторын нақтылау.

Құқықтық негіз:

ҚР ҚПК 277-бабы бойынша техникалық сараптама тағайындалады, сарапшы лицензияланған мемлекеттік немесе жекеменшік сараптама орталықтарынан шақырылады.

Сараптамалық сұрақтар мысалдары:

- Бұл файл қай құрылғыда жасалған?
- Бұл бейнематериал өңделген бе, жоқ па?
- Скриншоттарда көрсетілген уақыт пен жүйелік дерек сәйкес келе ме?

4. Медициналық сараптама (қажет болған жағдайда)

Кибергруминг кей жағдайларда оффлайн кездесуге алып келуі мүмкін. Мұндай жағдайда жәбірленушіге қатысты медициналық сараптама

тағайындалып, физикалық немесе сексуалдық зорлық белгілерінің бар-жоғы анықталады. Бұл сараптама тек дәрігердің көрсетімі бойынша, баланың және ата-анасының рұқсатымен жүргізіледі.

5. Сараптама тағайындау тәртібі

Сараптама тергеушінің қаулысы арқылы тағайындалады және ҚР ҚПК 273-бабы бойынша ресімделеді. Қаулыда міндетті түрде мыналар көрсетілуі тиіс:

- Іс нөмірі және тергеуші туралы мәліметтер;
- Сараптаманың түрі мен зерттелетін объект;
- Сарапшыға қойылатын нақты сұрақтар;
- Зерттеу мерзімі және материалдардың тізімі.

Сарапшының қорытындысы жазбаша түрде ұсынылады және сот процесінде дәлел ретінде пайдаланылады (ҚПК 288-бап).

Кибергруминг қылмыстарын тергеу барысында сараптамалар шешуші рөл атқарады. Әсіресе психологиялық және лингвистикалық сараптамалар тергеудің объективтілігін арттырып, қылмыстық ниетті дәлелдеуге мүмкіндік береді. Тергеуші сараптамаларды уақтылы, заңға сәйкес және сапалы түрде ұйымдастыруы – істің сотта заңды қаралуының кепілі болып табылады.

2.5. Жәбірленушімен (кәмелетке толмағанмен) жұмыс

Кибергруминг қылмыстары бойынша тергеу кезінде жәбірленушінің көп жағдайда — кәмелетке толмаған бала екені белгілі. Сондықтан мұндай істерде тергеушінің басты міндеттерінің бірі – баланың психологиялық қауіпсіздігін қамтамасыз ете отырып, оны процеске заңға сай, адамгершілікпен тарту. Жәбірленушімен жұмыс жасау — жай ғана жауап алу емес, бұл — баланың ішкі күйін түсіну, оған эмоционалдық қолдау көрсету және оның құқықтарын толық қорғау жүйесін қамтамасыз ету.

1. Заңнамалық негіз

Қазақстан Республикасының Қылмыстық-процестік кодексінің (ҚПК) 223-бабына сәйкес, кәмелетке толмағандардан жауап алу ерекше тәртіппен жүргізіледі:

- Жауап алу психологтың және заңды өкілдің (ата-анасы, қамқоршысы немесе мұғалімі) қатысуымен жүргізілуі тиіс;
- Жауап алу баланың жасына, психикалық дамуына және моральдық жағдайына сай бейімделуі қажет;
- Бір тергеу әрекеті бірнеше мәрте қайталанбауы керек;
- Тергеу барысында баланың құқықтары мен заңды мүдделері бұзылмауы тиіс.

2. Психологиялық факторларды ескеру

Кибергрумингке ұшыраған балалар жиі мынадай күйге түседі:

- Өздерін кінәлі сезінеді;
- Қорқады және болған жағдайды айтуға ұялады;

- Қылмыскермен байланысты үзуге қиналады (эмоционалды байланыс орнауы мүмкін);
- Қоғамдық реакциядан және әке-шешенің жазалауынан қорқады.

Осы себепті баламен жұмыс істегенде эмпатия, шыдамдылық, сенімділік және құпиялылық сақталуы тиіс. Психолог баланы алдын ала дайындық сұхбатынан өткізіп, оның жай-күйін тергеушіге хабарлайды. Кейбір жағдайларда тергеу әрекеті мүлде жүргізілмеуі немесе кейінге қалдырылуы мүмкін (ҚПК 214-бабы).

3. Арнайы жабдықталған бөлмелер және бейнежазба

Кәмелетке толмаған жәбірленушіден жауап алу балаларға бейімделген арнайы бөлмелерде (interview room) жүргізілуі тиіс. Мұндай бөлмелерде:

- Бейне және аудиожазба жүргізіледі;
- Қатысушылар саны барынша шектеледі (тергеуші, психолог, заңды өкіл);
- Балаға жайлы атмосфера жасалады — ойыншықтар, жұмсақ орындықтар, су, т.б.

Бейнежазбаның болуы — жауаптың дәлдігі мен қайталанбауын қамтамасыз етеді. Бұл баланың психологиялық саулығына оң әсер етеді.

4. Сұрақ қою әдебі

Сұрақтар баланың жас ерекшелігін ескере отырып, қарапайым, бейтарап және бағыттаушы емес формада қойылуы керек. Мысалы:

- Қате: «Сен оның айтқанын орындадың ба?»
- Дұрыс: «Ол саған не жазды? Сен не деп жауап бердің?»

Жәбірленушіні айыптау, қысым көрсету, кінәлау — қатаң тыйым салынған.

5. Құпиялылықты сақтау және екінші рет жарақат алмау принципі

Баланың жеке деректері (аты-жөні, мекенжайы, мектеп атауы) тергеу материалдарында жария етілмеуі тиіс. Тергеу мен сот процесінде:

- Бала мен оның отбасының қауіпсіздігі сақталуы тиіс;
- Журналистер мен қоғамдық ұйымдардың қатысуы шектеледі;
- Іс бойынша жабық сот отырысы өткізілуі мүмкін (ҚПК 29-бап).

Бұдан бөлек, «қосымша жарақат» қаупі бар – бұл бала бір оқиғаны бірнеше рет айтып, қайта-қайта психологиялық күйзеліске түсуі. Мұны болдырмас үшін:

- Бірінші жауапта барынша толық мәлімет алу маңызды;
- Бейнежазбаны пайдалану арқылы кейінгі процестерде қайта сұрақ қоюдың қажеті болмайды;
- Психологтың қорытындысы қосымша түсінік ретінде қолданылады.

6. Психологиялық көмек және посттравматикалық қолдау

Кибергруминг құрбандары — оқиғадан кейін психологиялық қолдауға мұқтаж. Сондықтан тергеу аяқталған соң, бала мен оның отбасына:

- Психологпен жүйелі жұмыс жүргізу;

- Дағдарыс орталықтарына немесе мектеп психологтарына бағыттау;
- Қоғамдық ұйымдар арқылы моральдық қолдау ұйымдастыру ұсынылады.

Кейбір елдерде «виктим қолдаушы» мамандар жұмыс істейді. Қазақстанда да болашақта кәмелетке толмағандарға арналған арнайы жәбірленушілермен жұмыс тетігін дамыту қажет.

Кәмелетке толмаған жәбірленушімен жұмыс – тек құқықтық емес, моральдық және адами жауапкершілікті талап ететін тергеудің маңызды аспектісі. Жауап алу баланың психологиялық жай-күйіне зиян келтірмей, әділ әрі заңды жолмен жүргізілуі тиіс. Осы қағидаларды сақтау — баланың сенімін қалпына келтіру мен оның өміріне қауіпсіздік сезімін қайтарудың алғашқы қадамы.

Қойылатын сұрақтар:

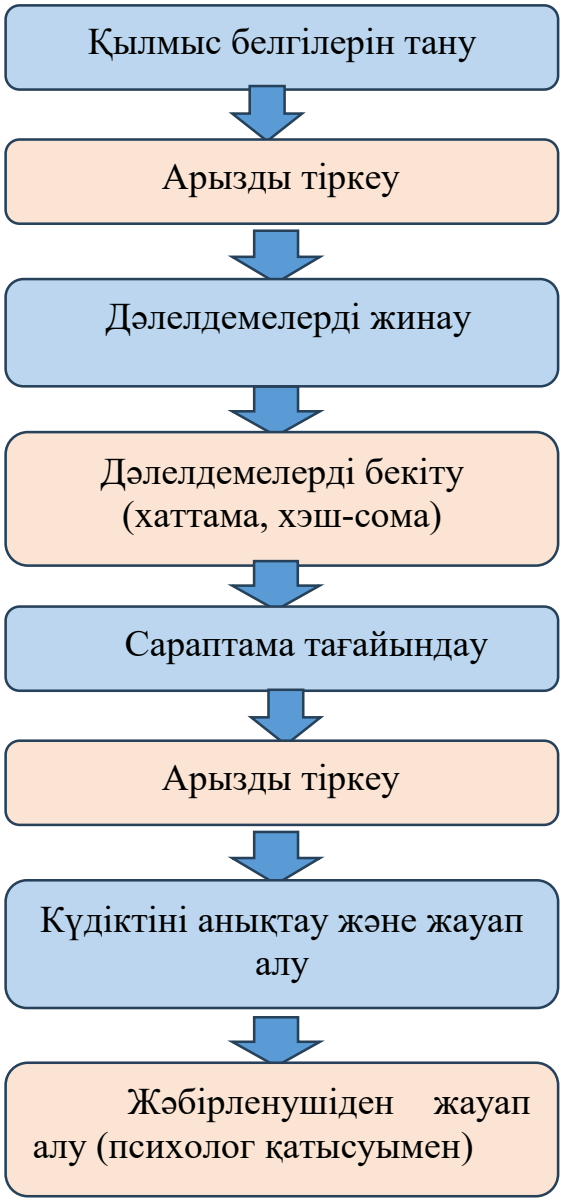
1. Таныстық пен қарым-қатынас сипаты
   - Бұл адаммен қайда және қалай таныстың?
   - Ол сенімен сөйлескенде не туралы айтатын еді?
   - Саған оның жазғандары (айтқандары) ұнады ма?
   - Ол саған жиі жазатын ба?
   - Сен оған не туралы айтатын едің?
2. Қарым-қатынас мазмұны
   - Ол сенен қандай суреттер немесе видеолар сұрады ма?
   - Саған не істе деп айтты?
   - Ол саған жеке кездесуді ұсынды ма?
   - Ол саған сыйлық немесе басқа бір нәрсе уәде етті ме?
   - Ол саған құпияда бірдеңе сақта деп айтты ма?
3. Бала реакциясы мен эмоциясы
   - Ол саған сөйлегенде өзіңді қалай сезіндің?
   - Оның жазғаны сені қуантты ма, қорқытты ма, ұялтты ма?
   - Сен ол адамға бәрін айтуға сендің бе?
   - Қазір сол адам туралы не ойлайсың?
4. Қорқыту немесе қысым
   - Ол саған қандай да бір сөзбен қорқыту, қоқан-лоқы жасады ма?
   - Егер сен оның айтқанын істемесең, не болатынын айтты ма?
   - Ол саған біреуге айтпа деп айтты ма?
5. Сенім мен қолдау
   - Бұл туралы кімге бірінші айттың?
   - Біреу саған көмектесті ме?
   - Қазір өзіңді қалай сезініп жүрсің?

3. ТЕРГЕУ ЖҮРГІЗУДІҢ АЛГОРИТМІ

3.1. Кибергруминг істерін тергеудің алгоритмі (кезең-кезеңімен)

Кибергрумингке қатысты қылмыстық істерді тергеу – күрделі және бірнеше маманның қатысуын қажет ететін процесс. Мұндай істердің ерекшелігі – олардың интернет кеңістігінде жасалуы, дәлелдемелердің көпшілігі электронды сипатта болуы және жәбірленушінің кәмелетке толмаған болуы.

Төменде ұсынылған алгоритм – тергеу барысында сақталуы тиіс негізгі сатылар мен олардың мазмұнын сипаттайды. Әр кезең нақты іс жүргізу әрекеттерімен, заңдық баптармен және практикалық қадамдармен байланыстырылған.



Сурет 3. Қылмыс белгілерін тану

Алгоритмдік кезеңдер:

1-кезең. Қылмыстық құқық бұзушылық туралы хабарлама түсуі

Құжаттық негіз: ҚР ҚПК 179-бабы

Әрекеттер:

- Ата-анадан, мектептен немесе әлеуметтік желі әкімшілігінен арыз түседі;
- Арыз ҚІЖ тіркеу кітабына енгізіледі (ЕРАП);
- Тергеуші материалдарды қарап, бастапқы талдау жүргізеді.

Мысал:

Мектеп мұғалімі оқушы қыздың WhatsApp арқылы бейтаныс адаммен ұзақ уақыт хат алмасып жүргенін байқайды. Әңгімеде қыздан сурет сұратылып, кездесуге шақырулар болған. Мұғалім бұл жайлы ата-анаға айтып, олар полицияға арыз береді.

2-кезең. Алдын ала тексеру және процессуалдық шешім қабылдау

Құжаттық негіз: ҚР ҚПК 190-бабы

Әрекеттер:

- Скриншоттар, бейнежазбалар немесе құрылғыдан алынған мәліметтер сарапталады;
- Психолог қатысуымен алғашқы түсініктемелер алынады;
- Тергеуші істі қылмыстық іс ретінде тіркейді.

Нәтиже: Қылмыстық іс қозғау туралы қаулы қабылданады.

3-кезең. Жедел-іздестіру іс-шаралары

Құжаттық негіз: ҚР «Жедел-іздестіру қызметі туралы» Заңы

Әрекеттер:

- Күдікті аккаунт бойынша IP-адрес анықталады;
- Байланыс операторларынан нөмірге тіркелген абонент туралы мәлімет сұратылады;
- Әлеуметтік желі әкімшілігіне сұрау жіберіледі.

Мысал:

IP мекенжай Алматы қаласындағы интернет-кафеге тіркелген. Бейнебақылау арқылы нақты адам анықталып, оның жеке тұлғасы расталады.

4-кезең. Сандық дәлелдемелерді жинау және бекіту

Құжаттық негіз: ҚР ҚПК 125, 221-баптары

Әрекеттер:

- Қыздың телефонын сараптамаға алу;
- Хат алмасудың түпнұсқасын сақтап, хэш-сомасын есептеу;
- Серверлік деректерді алу үшін шетелдік сервистерге сұраныс жолдау.

Маңызды: Дәлелдемелер өзгеріссіз күйінде хаттама арқылы рәсімделіп, сотта қолдануға жарамды болуы тиіс.

5-кезең. Кәмелетке толмаған жәбірленушіден жауап алу

Құжаттық негіз: ҚР ҚПК 223-бабы

Әрекеттер:

- Психолог пен заңды өкілдің қатысуымен жауап алу;
- Жауап арнайы жабдықталған бөлмеде бейнежазбамен жүргізіледі;
- Қайта жауап алу қажет болмауы үшін барлық сұрақтар бір отырыста қойылады.

Мысал:

Қыз жауап беру кезінде алғашқыда қысылып, көп сөйлемейді. Психологтың араласуымен ол қылмыскер өзін "16 жастағы жігітпін" деп таныстырып, фото мен видео сұрағанын айтады.

6-кезең. Сараптамалар тағайындау

Құжаттық негіз: ҚР ҚПК 275, 277-баптары

Сараптама түрлері:

- Психологиялық (балаға әсер деңгейін анықтау);
- Психолингвистикалық (хат мәтініндегі ниет);
- Компьютерлік-техникалық (файл түпнұсқалығы, құрылғы мәліметтері).

7-кезең. Күдіктіні анықтау және жауапқа тарту

Құжаттық негіз: ҚР ҚПК 202, 206-баптары

Әрекеттер:

- Күдіктіні ұстау, пәтеріне тінту жүргізу;
- Құрылғыларды, мобильді телефондарды алу;
- Тергеу изоляторына қамау туралы бұлтартпау шарасын қолдану.

8-кезең. Істі аяқтау және сотқа жолдау
Құжаттық негіз: ҚР ҚПК 300-бабы
Әрекеттер:

- Барлық дәлелдемелер жүйеленеді;
- Қорытынды айыптау актісі жасалады;
- Іс прокуратураға, кейін сотқа жолданады.

Кибергрумингке қатысты қылмыстық істерді тергеудің алгоритмі – бұл тек қадамдар жиынтығы емес, ол тергеушінің құқықтық, психологиялық және техникалық сауаттылығын талап ететін үйлесімді жүйе. Тергеуші әр кезеңде тек заң нормаларын ғана емес, сонымен бірге адамгершілік, этика және баланың психикалық саулығын сақтау принциптерін де басшылыққа алуы тиіс.

Кибергруминг қылмыстарын тергеу – дәстүрлі тергеу тәжірибесінен айтарлықтай ерекшеленетін, технологиялық және психологиялық тұрғыдан күрделі процесс. Себебі мұндай қылмыстар интернет кеңістігінде, көбінесе анонимді түрде жасалады және жәбірленушілердің басым бөлігі — кәмелетке толмаған тұлғалар. Сондықтан тергеу барысында әрекет ету тәртібінің нақты құрылымы мен кезеңдік жүйесі болуы — қылмыстың ашылуы мен дәлелдемелердің жарамдылығын қамтамасыз ететін басты шарт.

Осыған байланысты, кибергруминг істерінде тергеуші әрекетінің әр сатысы — бастапқы арызды қабылдаудан бастап, сараптама қорытындыларын сотқа дейін жеткізуге дейін — нақты бірізділікпен және заңға сай жүргізілуі қажет. Тергеу барысындағы дәлелдемелерді жоғалту, тиісті процесуалдық нормаларды бұзу немесе жәбірленушіге тиісті психологиялық жағдай жасамау — істің тоқтауына, қылмыскердің жазасыз қалуына немесе жәбірленушінің екінші рет психологиялық жарақат алуына әкелуі мүмкін.

Сол себепті бұл бөлімде тергеудің негізгі кезеңдері кесте түрінде, мазмұнды және құрылымдық сипатта ұсынылып отыр. Әрбір қадам нақты құқықтық баптарға, тергеуші әрекеттерінің тәртібіне және тәжірибеде қолдану ерекшеліктеріне сүйене отырып сипатталады. Мұндай алгоритм тергеу сапасын арттырумен қатар, ведомствоішілік оқыту және тәжірибелік әдістемелік жұмыс үшін де пайдалы құрал бола алады.

Тергеудің негізгі кезеңдері

Кезең атауы	**Мазмұны мен әрекеттері**	**Құқықтық негіз**
1. Қылмыс белгілерін тану	– Жәбірленушінің немесе куәгердің арызы, аноним хабарлама немесе мектеп психологының хабарлауы негізінде ақпарат келіп түседі. – Жәбірленуші кәмелетке толмаған бала екенін, әрекет интернет кеңістігінде жасалғанын және сексуалдық сипаттағы ниет барын анықтау.	ҚР ҚПК 179-бабы; ҚР ҚК 122, 124-баптары

2. Арызды тіркеу	– Арыз немесе хабарлама қабылданған соң, ол ҚІЖ (ЕРАП) тіркеу жүйесіне енгізіледі. – Тергеуші ҚПК 190-бабы аясында арыз бойынша бастапқы тексеруді бастайды. – Электронды деректер дереу сақталуы тиіс.	ҚР ҚПК 179, 190-баптары
3. Дәлелдемелерді жинау және бекіту	– Скриншоттар, хат-хабар журналдары, бейне/аудио жазбалар, әлеуметтік желі профилі, құрылғы деректері жиналады. – Дәлелдемелердің түпнұсқалығы хэш-сомалар арқылы расталады. – Сандық құрылғылардан мәліметтер алу арнайы хаттамамен жүргізіледі. – Жедел-іздестіру шаралары жүргізіледі: IP-адресті табу, логтар сұрату, интернет-провайдермен жұмыс.	ҚР ҚПК 221, 223-баптары; Жедел-іздестіру туралы Заң
4. Сараптама тағайындау	– Сандық дәлелдемелерге техникалық сараптама (скриншоттың түпнұсқалығы, файл метадеректері, құрылғы түрі). – Психологиялық сараптама (балаға әсер деңгейі). – Психолингвистикалық сараптама (мәтіннің мағынасы, ниет, астарлы мазмұн). – Қажет болса, медициналық сараптама.	ҚР ҚПК 275, 277-баптары
5. Күдікті мен жәбірленушіні жауапқа тарту	Күдіктіге қатысты:– Жеке басы анықталған соң, тінту, ұстау және жауап алу жүргізіледі. – Бұлтартпау шарасы (қамау, үйқамақ) қарастырылады. Жәбірленушіге қатысты:– Арнайы бөлмеде, бейнежазбамен, психолог пен заңды өкілдің қатысуымен жауап алу. – Қайта жауап алмау үшін барынша толық ақпарат алу.– Құпиялылық пен бала құқығы толық сақталады.	ҚР ҚПК 202, 223, 225-баптары

2 – кесте

3.2 Тергеу іс-шараларының кезеңдік тәртібі

Кибергруминг қылмыстарын тергеу іс-шаралары жүйелі әрі кезеңдік тәртіппен жүргізілуі тиіс. Бұл процестің әр кезеңі нақты құқықтық және тактикалық мазмұнға ие. Тергеу барысында әрбір қадам дәлелдемелерді толық

әрі заңды жолмен бекітіп, күдіктінің әрекеттерін дәлелдеуге бағытталуы керек. Кезеңдік тәртіп сақталмаған жағдайда, дәлелдемелер жарамсыз деп танылып, іс сотқа дейін жетпей жабылып қалуы мүмкін.

Алғашқы кезең – қылмыс белгілерін тану және тіркеу. Бұл сатыда кибергрумингке қатысты белгі байқалған немесе жәбірленушінің арызы түскен кезде, құқық қорғау органы ҚПК-нің 179-бабы негізінде қылмыстық құқық бұзушылық белгілері бар хабарламаны қабылдайды. Мұндай хабарламалар көбінесе жәбірленушінің ата-анасы, мектеп мұғалімдері немесе интернет мониторинг арқылы анықталады. Мәселен, бала өзінің әлеуметтік желідегі парақшасында бейтаныс адамнан тұрақты хат-хабар алып, фото немесе жеке ақпарат сұралғанын айтса, бұл әрекет бірден тексеруді қажет етеді. Арыз түскен бойда, ол дереу ЕРАП (электрондық тіркеу жүйесі) базасына енгізіліп, іс жүргізу басталады.

Екінші кезең – алдын ала тексеру мен қылмыстық істі қозғау. Тергеуші арыздағы мәліметтердің шынайылығын анықтау үшін бастапқы материалдарды жинайды: скриншоттар, куәгерлердің түсініктемелері, құрылғыдан алынған мәліметтер. Бұл кезеңде дәлелдердің түпнұсқалығы сақталуы тиіс. Егер қылмыстық құқық бұзушылық белгілері дәлелденсе, тергеуші ҚР ҚПК-нің 179-бабы негізінде қылмыстық істі қозғау туралы қаулы шығарады. Іс қозғалғаннан кейін тергеудің негізгі бөлімі басталады.

Үшінші кезең – дәлелдемелерді жинау және бекіту. Бұл кезеңде тергеуші кибергруминг әрекетінің дәлелдерін жүйелі түрде жинақтап, процессуалдық түрде рәсімдейді. Атап айтқанда, әлеуметтік желідегі хат алмасулар скриншотпен ғана емес, техникалық түпнұсқамен (метадеректер, уақыт белгісі, қолданылған құрылғы туралы ақпаратпен) бірге алынады. Бұл үшін мамандандырылған бағдарламалар (мысалы, FTK Imager, Autopsy) арқылы хэш-сома есептеліп, әрбір цифрлық файлдың өзгеріссіз сақталғаны дәлелденеді. Сонымен қатар, интернет-провайдерден IP-адреске тіркелген ақпарат, лог-файлдар, пайдаланушы профилі туралы мәліметтер сұратылады. Барлық дәлелдемелер ҚР ҚПК-нің 221 және 223-баптарына сәйкес хаттамамен рәсімделеді.

Төртінші кезең – жәбірленушіден жауап алу. Бұл – аса сезімтал әрі заң талаптарына қатаң бағынатын кезең. Кәмелетке толмаған баладан жауап алу тек арнайы жабдықталған бөлмеде, бейнежазба жүргізіле отырып, психолог пен заңды өкілдің қатысуымен өтеді. Сұрақтар бейтарап, бала жасына сай және бағыттаушы емес сипатта қойылады. Бұл процесс ҚР ҚПК-нің 223-бабы мен Бала құқықтары туралы конвенция талаптарына толық сай болуы тиіс. Жауап алу бір рет және жеткілікті болуы шарт, өйткені қайталап жауап алу баланың психикасына теріс әсер етуі мүмкін.

Бесінші кезең – сараптамалар тағайындау. Жиналған дәлелдерге негізделе отырып, тергеуші бірнеше сараптама тағайындайды: психологиялық (балаға әсер ету дәрежесін анықтау үшін), психолингвистикалық (хат мазмұнындағы ниет пен мағына), сандық-техникалық (файлдың өзгертілмегенін, құрылғы түрін

анықтау). Сараптамалар ҚР ҚПК-нің 275 және 277-баптарына сәйкес арнайы қаулымен тағайындалады. Сарапшы өз қорытындысын жазбаша түрде береді және бұл қорытынды дәлелдемелердің заңдылығын күшейтеді.

Келесі – күдіктіні анықтау, ұстау және жауап алу кезеңі. Бұл процесс жиналған дәлелдерге негізделе отырып жүзеге асырылады. Тергеуші ҚР ҚПК-нің 202 және 206-баптарына сәйкес, күдіктіні ұстау, оның үйінде тінту жүргізу, электрондық құрылғыларды алу және жауап алу әрекеттерін орындайды. Күдіктіден жауап алу кезінде оның құрылғыларды қалай қолданғаны, жәбірленушімен қалай байланыс орнатқаны, ниеті мен мақсаты анықталады. Егер жиналған материалдар жеткілікті болса, бұлтартпау шарасы ретінде қамауға алу немесе үйқамақ қолданылуы мүмкін.

Соңғы кезең – істі аяқтап, айыптау актісін жасап, сотқа жолдау. Барлық дәлелдемелер мен сараптама қорытындылары жүйеленіп, ҚР ҚПК-нің 300-бабы бойынша қылмыстық істің соңғы процесуалдық құжаттары дайындалады. Іс прокурорға жолданып, оның келісімімен сотқа беріледі.

Осы аталған барлық кезеңдер – өзара логикалық әрі заңды байланыста, бірізді жүргізілуі тиіс. Тергеу іс-шараларын жүргізу тәртібінің кезеңдік сипат алуы – тергеудің объективтілігі мен дәлелдердің жарамдылығына кепілдік береді. Сонымен бірге, бұл тәртіп кәмелетке толмаған жәбірленушінің психологиялық қауіпсіздігін сақтауға, оның құқығы мен абыройын қорғауға мүмкіндік береді.

3.3. Кибергрумингке қарсы күресте ведомствоаралық өзара іс-қимылдың маңызы

Кибергруминг – бұл тек бір адамның немесе жекелеген ведомстволық күшімен шешілетін қылмыс емес. Бұл – күрделі, көпқырлы, жасырын сипаты бар және интернет кеңістігін пайдалану арқылы жасалатын қылмыстық әрекет. Сондықтан оған қарсы тиімді әрекет ету үшін ведомствоаралық кешенді өзара іс-қимыл қажет. Бұл дегеніміз – құқық қорғау органдары, білім беру ұйымдары, әлеуметтік қызметтер, байланыс операторлары, интернет-платформалар және үкіметтік емес ұйымдардың үйлестірілген және бірлескен әрекеті.

Ведомствоаралық іс-қимыл үлгісі мынадай тізбекке негізделуі тиіс:

1. Мектеп немесе ата-ана күдік тудырған жағдайда дер кезінде полицияға хабарлайды.
2. Тергеуші арызды тіркеп, психологты қатыстыра отырып, алдын ала тексеру жүргізеді.
3. Цифрлық дәлелдер жинау үшін байланыс операторларына, интернет платформаларға сұраныстар жолданады.
4. Сараптамалар мен сарапшылардың қатысуын білім басқармасы мен сараптама органдары үйлестіреді.
5. Тергеу аяқталған соң, жәбірленушіні оңалту үшін әлеуметтік қызметтер мен ҮЕҰ іске қосылады.

Қорыта келгенде, кибергрумингпен күресте ведомствоаралық өзара іс-қимыл – жедел, кәсіби және үйлесімді болуға тиіс. Бұл өзара байланыс біржақты хабарлама түрінде емес, нақты үйлестірілген әрекеттер алгоритмімен реттелуі керек. Әрбір мүдделі тарап өз функциясын нақты біліп, уақтылы орындайтын жүйе ғана кибергрумингке қарсы күресте табысқа жеткізеді.

4. СОТ ПРАКТИКАСЫ МЕН ҚИЫНДЫҚТАР

Кибергруминг – Қазақстанда әлі де болса жаңа әрі толық құқықтық анықтамасы қалыптаспаған қылмыс түрі. Осы себепті сот тәжірибесі аз, ал бар істердің өзінде түрлі құқықтық және процессуалдық қиындықтар орын алған. Бұл бөлімде кибергрумингке қатысты сот істері, дәлелдемелерге қойылатын талаптар, тергеу барысында жиі кездесетін қателіктер және сот актілерінен нақты (анонимизацияланған) үзінділер қарастырылады.

4.1. ҚР сот тәжірибесі бойынша кибергруминг істері

Кибергруминг әрекеттері көбіне ҚР Қылмыстық кодексінің 122-бабы (Кәмелетке толмағанмен жыныстық қатынас), 124-бабы (Азғындық әрекеттер), 125-бабы (Адам ұрлау), 147-бабы (Жеке өмірге қол сұғу) және 274-бабы (Жалған ақпарат тарату) арқылы сараланады. Дегенмен, бұл баптардың бірде-бірінде кибергруминг ұғымы тікелей қамтылмағандықтан, тергеушілер мен прокурорлар өз қалауларымен бап таңдауға мәжбүр болады.

Мысалы, 2021 жылы Алматы қаласы Алмалы аудандық сотында қаралған бір істе (№2021/24938-ҚБ) 17 жастағы оқушы қызбен Instagram желісі арқылы байланыс орнатқан азамат оған бірнеше ай бойы "достық" қарым-қатынас ұстанып, кейін жыныстық сипаттағы бейнежазбалар жіберуге көндірген. Сот бұл әрекетті ҚК-нің 124-бабы бойынша азғындық әрекет деп таныды, дегенмен адвокат дәлелдемелердің жеткіліксіздігін алға тартып, істі тоқтатуды сұрады. Бұл істе сараптама қорытындылары мен скриншоттар басты дәлел рөлін атқарды.

Тағы бір мысал – 2022 жылы Шымкент қалалық сотында қаралған (№2022/11839-ҚБ) істе 14 жастағы баламен Telegram арқылы байланыс орнатқан күдікті оған жалған атпен тіркеліп, өзін 15 жастағы қыз ретінде көрсеткен. Уақыт өте келе сенімге кіріп, фотосуреттер сұратқан. Бұл істі сот ҚК-нің 147-бабы – жеке өмірге қол сұғу және 124-бабы – азғындық әрекеттер бойынша қарап, күдіктіні шартты жазаға кескен. Алайда соттың қорытындысында «кибергруминг» термині мүлде қолданылмаған.

4.2. Дәлелдемелердің жарамсыздығы мәселелері

Кибергрумингке қатысты істерде дәлелдемелердің көпшілігі – электрондық сипатта: скриншоттар, чаттар, бейнежазбалар, құрылғыдағы метадеректер. Алайда тергеу кезінде осы дәлелдерді заңға сай рәсімдемеу салдарынан олар сотта жарамсыз деп танылып жатады.

Негізгі кемшіліктер:

- Хат алмасулар скриншот ретінде ғана тіркеліп, серверлік түпнұсқа алынбауы;
- Скриншоттардың өзгертілмегенін растайтын хэш-сома есептелмеуі;
- Электрондық құрылғыны алу кезінде хаттама талаптарының бұзылуы;
- Тергеушінің дәлелді алу барысын бейнетіркеу арқылы рәсімдемеуі;
- Күдікті қолданған профильдің нақты иесі анықталмаған.

Мысалы, Нұр-Сұлтан қаласында 2023 жылы қозғалған қылмыстық іс бойынша (іс нөмірі көрсетілмейді, ақпарат жабық) айыпталушы WhatsApp арқылы жасөспірімге сексуалдық сипаттағы хабарламалар жіберген. Алайда тергеуші тек жәбірленушінің скриншоттарын тіркеп, байланыс провайдерінен дерек сұратпаған. Нәтижесінде сотта дәлелдеме күмәнді деп танылып, іс қысқартылған.

4.3. Тергеу барысында жиі кездесетін қателіктер

Кибергрумингке қатысты істерді тергеу кезінде жиі кездесетін келесі типтік қателіктер орын алады:

1. Бапты дұрыс таңдамай іс қозғау: Кибергруминг фактісі анық болғанымен, тергеуші оны «бопсалау» немесе «жалған ақпарат тарату» ретінде саралайды. Бұл істің мән-жайына сай келмейді.
2. Жәбірленушімен жұмыс жүргізудегі қателіктер: Жауап алу психологтың қатысуынсыз немесе бейнежазбасыз жүргізіледі, нәтижесінде баланың берген жауабы дәлел ретінде күмән тудырады.
3. Сандық дәлелдемелерді рәсімдеудегі кемшіліктер: Құрылғыны алу, хат алмасуды сақтау, файл метадеректерін талдау барысында процессуалдық тәртіп бұзылады.
4. Сараптама тағайындамау немесе кешіктіру: Психолингвистикалық сараптама кеш тапсырылып, дәлелді бекіту мерзімі өтіп кетеді.
5. Күдіктіні қадағалаусыз қалдыру: Әлеуметтік желі арқылы қылмыс жасаған тұлға уақытылы танылмаса, басқа аккаунтпен жалғастыру қаупі туындайды.

Бұл қателіктердің барлығы сот процесінде істің мәнін бұрмалап, әділетсіз шешім шығуына әкелуі мүмкін.

4.4. Сот актілерінен үзінділер (анонимизацияланған)

Сот актісі №2022/8457-ҚБ, Ақтөбе қаласы соты:

«...Сот жәбірленуші тарапынан ұсынылған скриншоттарды толыққанды дәлел ретінде қабылдамады, өйткені олар серверден алынбаған, өзгертілмегені техникалық жолмен расталмаған. Осыған байланысты сот дәлелдемелерді жеткіліксіз деп таныды және істі қосымша тергеуге қайтарды...»

Сот актісі №2021/19283-ҚБ, Қарағанды облысы:

«...Сот істі қарау барысында жәбірленушіден жауап алудың процессуалдық талаптары бұзылғанын, яғни жауап алу психологсыз, бейнежазбасыз жүргізілгенін анықтады. Баланың алғашқы жауабы кейінгі мәліметтермен сәйкес келмегендіктен, сот жауапты дәлел ретінде қабылдаудан бас тартты...»

Сот актісі №2023/3951-ҚБ, Алматы қаласы:

«...Күдіктінің Telegram аккаунты арқылы кәмелетке толмағанға азғындық сипаттағы бейнежазба жібергені анықталды. Дәлелдеме ретінде видеофайлдың хэш-сомасы ұсынылды, сараптамалық қорытынды алынған. Сот бұл дәлелдерді жарамды деп танып, ҚК-нің 124-бабы бойынша 3 жылға бас бостандығынан айыру жазасын тағайындады...»

Кибергруминг істерін тергеу мен сот тәжірибесі – Қазақстанда жаңадан қалыптасып келе жатқан, құқықтық және техникалық жағынан күрделі сала. Бұл істерде дәлелдемелердің сапасы, тергеу әрекеттерінің заңдылығы және жәбірленушінің құқықтарын сақтау – шешуші рөл атқарады. Тергеушілер мен прокурорлар жоғарыда көрсетілген сот тәжірибесін ескере отырып, нақты әдістемелік талаптар мен алгоритмдерді ұстануы тиіс.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Қазақстан Республикасының Қылмыстық кодексі: ҚР 2014 жылғы 3 шілдедегі № 226-V Заңы. – Астана: ЮРИСТ, 2023. – 472 б.
2. Қазақстан Республикасының Қылмыстық-процестік кодексі: ҚР 2014 жылғы 4 шілдедегі № 231-V Заңы. – Астана: ЮРИСТ, 2023. – 560 б.
3. Қазақстан Республикасының "Жедел-іздестіру қызметі туралы" Заңы. – Алматы: ЮРИСТ, 2022. – 36 б.
4. Қазақстан Республикасының "Бала құқықтары туралы" Заңы. – Астана: Әділет, 2022. – 28 б.
5. Қазақстан Республикасы Ішкі істер министрлігі. Киберқылмыстармен күрес бойынша әдістемелік ұсынымдар. – Астана: ҚР ІІМ, 2021. – 64 б.
6. ҚР Білім және ғылым министрлігі. Кәмелетке толмағандардың қауіпсіз интернетті пайдалануына байланысты әдістемелік ұсынымдар. – Астана: БҒМ, 2022. – 48 б.
7. Қазақстан Республикасы Жоғарғы Соты. 2021–2023 жылдар аралығындағы қылмыстық істер бойынша сот тәжірибесіне шолу. – Астана: Жоғарғы сот баспасы, 2023. – 82 б.
8. Уәлиев Қ. Кәмелетке толмағандарға қатысты сексуалдық қылмыстарды тергеу әдістемесі. – Алматы: ҚазЮИ, 2020. – 148 б.
9. Исмағұлов А. Сандық дәлелдемелер: құқықтық табиғаты мен қолдану проблемалары // Заң. – 2022. – №4. – Б. 36–42.
10. Council of Europe. Convention on Cybercrime (Budapest Convention). – Strasbourg, 2001. – [Электрондық ресурс]. Қолжетімді: https://www.coe.int/en/web/cybercrime
11. Council of Europe. Lanzarote Convention. – Strasbourg, 2007. – [Электрондық ресурс]. Қолжетімді: https://www.coe.int/en/web/children/lanzarote-convention
12. United Nations Office on Drugs and Crime (UNODC). Guidelines on Investigating and Prosecuting Cybercrime. – Vienna: UNODC, 2020. – 88 p.
13. United Kingdom. Sexual Offences Act 2003. – London: HMSO, 2003. – Section 15.
14. Germany. Criminal Code (StGB). – Berlin, 2020. – Section 176.
15. Australia. Criminal Code Act 1995. – Canberra, 2021. – Section 474.27.

16. Улзира Қ. Кибергрумингті тергеуді жетілдіру мәселелері мен перспективалары: дисс. жоба. – Астана: ҚР ІІМ Академиясы, 2024. – 80 б.

17. INTERPOL. Crimes Against Children Unit: Best Practices. – Lyon: INTERPOL, 2021. – 60 p.

18. Meta Transparency Center. Law Enforcement Guidelines. – [Электрондық ресурс]. Қолжетімді: https://transparency.meta.com

19. OECD. Protecting Children Online: Risks Faced by Children and Policies to Protect Them. – Paris: OECD Publishing, 2019. – 114 p.