«Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті» КеАҚ

ӘОЖ 342.9:347.157.1(574+1-87)

Қолжазба құқығында

**КАРИПБАЕВ ЖАСУЛАН БОЛАТБЕКОВИЧ**

# Кәмелетке толмағандардың кибер құқық бұзушылықтарын әкімшілік-құқықтық реттеу: ұлттық және халықаралық аспектілері

6D030100 – Құқықтану

Философия докторы (PhD) дәрежесін алу үшін
жазылған диссертация

Ғылыми кеңесшілер:
PhD доктор, профессор,
**Қ.С. Мусин;**
заң ғылымдарының докторы, профессор,
**Ж.И. Ибрагимов.**

Шетелдік ғылыми кеңесші:
заң ғылымдарының докторы, профессор,
**К. Цомплак** (Вроцлав қ., Польша Республикасы).

Қазақстан Республикасы
Қарағанды, 2025

**МАЗМҰНЫ**

**НОРМАТИВТІК СІЛТЕМЕЛЕР……3**
**АҢЫҚТАМАЛАР……..……4**
**БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР …….……..5**
**КІРІСПЕ.....6**
**1 КӘМЕЛЕТКЕ ТОЛМАҒАНДАРДЫҢ КИБЕР ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРЫНА ҚАТЫСТЫ ТЕОРИЯЛЫҚ НЕГІЗДЕР МЕН КОНЦЕПЦИЯЛАР**
1.1 Кәмелетке толмағандардың құқықтық мәртебесі және киберкеңістіктегі ерекшеліктері .....12
1.2 Кибер құқық бұзушылықтардың жалпы түсінігі мен жіктелуі .....23
1.3 Кибер құқық бұзушылықтардың әкімшілік-құқықтық салдары .....35
**2 КӘМЕЛЕТКЕ ТОЛМАҒАНДАРДЫҢ КИБЕР ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРЫН ӘКІМШІЛІК-ҚҰҚЫҚТЫҚ РЕТТЕУДІҢ ҰЛТТЫҚ ЕРЕКШЕЛІКТЕРІ**
2.1 ҚР заңнамасындағы киберкеңістікке байланысты құқық бұзушылықтарды реттеу ерекшеліктері .....54
2.2 Әкімшілік іс жүргізу аспектілері: дәлелдемелерді жинау, сараптау және бағалау .....84
2.3 Кәмелетке толмағандардың құқықтары мен мүдделерін қорғау: алдын алу мен жауапкершіліктің өзара байланысы .....94
**3 ХАЛЫҚАРАЛЫҚ ЖӘНЕ ШЕТЕЛДІК ТӘЖІРИБЕ**
3.1 Халықаралық ұйымдардың (БҰҰ, ЮНИСЕФ, т.б.) киберқауіпсіздік стандарттары .....105
3.2 Шет мемлекеттерде кәмелетке толмағандарды киберқауіп-қатерлерден қорғаудың құқықтық негіздері .....117
3.3 Қазақстан заңнамасын жетілдіру үшін шетелдік озық үлгілерді бейімдеу……132
**4 КИБЕР ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРҒА ҚАТЫСТЫ ӘКІМШІЛІК НОРМАТИВТІК БАЗАНЫ ЖЕТІЛДІРУ ПЕРСПЕКТИВАЛАРЫ**
4.1 Әкімшілік-құқықтық нормаларды оңтайландыру бағыттары .....151
4.2 Ведомствоаралық және халықаралық ынтымақтастықты күшейту.....163
4.3 Кәмелетке толмағандардың құқықтарын қорғаудың заманауи технологиялық шешімдері .....171
**ҚОРЫТЫНДЫ .....181**
**ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ .....185**
**ҚОСЫМШАЛАР .....203**

# НОРМАТИВТІК СІЛТЕМЕЛЕР

Осы диссертацияда келесі нормативтік құқықтық актілерге сілтемелер пайдаланылған:

Қазақстан Республикасының Конституциясы (1995 жылғы 30 тамызда республикалық референдумда қабылданған) (2022 жылғы 19 қыркүйектегі өзгерістер мен толықтырулармен).

Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы кодексі 2014 жылғы 5 шілдедегі № 235-V (2024 жылғы 1 қыркүйектегі өзгерістер мен толықтырулармен).

Қазақстан Республикасының Қылмыстық кодексі 2014 жылғы 3 шілдедегі № 226-V (2024 жылғы 5 қыркүйектегі өзгерістер мен толықтырулармен).

Қазақстан Республикасының Әкімшілік рәсімдік-процестік кодексі 2020 жылғы 29 маусымдағы № 350-VI (2024 жылғы 5 қыркүйектегі өзгерістер мен толықтырулармен).

«Бала құқықтары туралы» Қазақстан Республикасының заңы 2002 жылғы 8 тамыздағы № 345-II (2023 жылғы 20 желтоқсандағы өзгерістер мен толықтырулармен).

«Ақпаратқа қол жеткізу туралы» Қазақстан Республикасының заңы 2015 жылғы 16 қарашадағы № 401-V (2024 жылғы 20 тамыздағы өзгерістер мен толықтырулармен).

«Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының заңы 2013 жылғы 21 мамырдағы № 94-V (2024 жылғы 20 тамыздағы өзгерістер мен толықтырулармен).

«Бұқаралық ақпарат құралдары туралы» Қазақстан Республикасының заңы 1999 жылғы 23 шілдедегі № 451-I (2023 жылғы 15 қарашадағы өзгерістер мен толықтырулармен).

«Байланыс туралы» Қазақстан Республикасының заңы 2004 жылғы 5 шілдедегі № 567-II (2024 жылғы 10 маусымдағы өзгерістер мен толықтырулармен).

«Ақпараттандыру туралы» Қазақстан Республикасының заңы 2015 жылғы 24 қарашадағы № 418-V (2024 жылғы 21 шілдедегі өзгерістер мен толықтырулармен).

«Киберқауіпсіздік тұжырымдамасы (Қазақстанның киберқалқаны)» — Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген (өзгерістермен бірге).

## АҢЫҚТАМАЛАР

Осы диссертацияда келесі терминдер тиісті анықтамаларымен бірге қолданылды:

**Кәмелетке толмаған** - он сегіз жасқа толмаған, әкімшілік және қылмыстық жауаптылық шегінде ерекше құқықтық мәртебеге ие тұлға.

**Кибер құқық бұзушылық** - ақпараттық-коммуникациялық технологияларды пайдалана отырып жасалатын құқыққа қарсы іс-әрекет (мысалы, рұқсатсыз кіру, фишинг, кибербулинг, онлайн алаяқтық).

**Әкімшілік құқық бұзушылық** - заңмен тыйым салынған, бірақ қылмыс қатарына жатпайтын қоғамға қауіпті әрекет немесе әрекетсіздік.

**Әкімшілік жауапкершілік** - әкімшілік құқық бұзушылық жасаған тұлғаға мемлекеттік органның тарапынан қолданылатын заңдық ықпал ету шарасы.

**Кибербулинг** - интернет немесе әлеуметтік желілер арқылы жеке тұлғаны қорлау, мазақ ету, қорқыту немесе кемсіту әрекеті.

**Онлайн-груминг** - ересек тұлғаның кәмелетке толмаған баламен онлайн ортада сенімге кіріп, оны жыныстық немесе басқа мақсатта пайдалану ниетімен байланыс орнатуы.

**Сандық дәлелдемелер (цифрлық дәлелдер)** - электрондық құрылғыларда сақталған немесе интернет арқылы алынған ақпарат, құқық бұзушылық фактісін растау үшін қолданылатын дәлел.

**Ақпараттық қауіпсіздік** - ақпараттық жүйелер мен деректерді рұқсатсыз қол жеткізуден, бұрмалаудан және жоюдан қорғау шараларының жүйесі.

**Жеке деректер** - тұлғаны анықтауға мүмкіндік беретін кез келген ақпарат (аты-жөні, мекенжайы, фотосуреті, байланыс деректері және т.б.).

**Жеке деректерді қорғау** - жеке тұлғаның ақпараттық деректерін заңсыз өңдеуден, тарату мен жариялаудан қорғау тетіктері.

**Әлеуметтік инженерия** - адамның психологиялық әлсіздігін пайдалану арқылы құпия ақпаратты немесе рұқсатты алу тәсілі.

**Фишинг** - интернет арқылы жалған сайттар немесе хабарламалар арқылы пайдаланушының жеке мәліметтерін алдау жолымен ұрлау тәсілі.

**Зиянды бағдарлама (Malware)** - компьютерлік жүйеге ену және оған залал келтіру мақсатында жасалған бағдарламалық код.

**Рұқсат етілмеген қол жеткізу** - ақпараттық жүйеге немесе деректерге иесінің рұқсатынсыз кіру әрекеті.

**Интернет-платформа (делдал қызмет көрсетуші)** - пайдаланушылар арасында ақпарат алмасуды қамтамасыз ететін онлайн қызмет немесе сайт (мысалы, әлеуметтік желі, мессенджер, бейнехостинг).

**Контентті модерациялау** - интернет-платформаларда жарияланатын материалдарды тексеру және қауіпті немесе заңсыз контентті жою процесі.

## БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР

AI – Жасанды интеллект
АКТ – Ақпараттық-коммуникациялық технологиялар
API – Қолданбалы бағдарлама интерфейсі
Big Data – Үлкен деректер технологиялары
БҰҰ – Біріккен Ұлттар Ұйымы
COPPA – Балалардың онлайн құпиялылығын қорғау туралы АҚШ заңы
Cyber Tumar – «Кибер Тұмар» жобасы
DPI – Терең десте талдау технологиясы
eGov – Электрондық үкімет жүйесі
GDPR – Жалпы деректерді қорғау регламенті (ЕО)
Hotline – Жедел сенім желісі
ICT – Ақпараттық-коммуникациялық технологиялар
IT – Инновациялық технологиялар
ІІМ – Қазақстан Республикасының Ішкі істер министрлігі
Интернет – Әлемдік ақпараттық байланыс желісі
IoT – Заттар интернеті
ҚА – Құқықтық акт
ҚАЖ – Құқықтық әкімшілік жауапкершілік
ҚК – Қазақстан Республикасының Қылмыстық кодексі
ҚР – Қазақстан Республикасы
ҚР АК – Қазақстан Республикасының Азаматтық кодексі
ҚР ӘҚБтК – Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы кодексі
ҚР ІІМ – Қазақстан Республикасының Ішкі істер министрлігі
ПҚБ – Профилактика және құқық бұзушылықтың алдын алу
Parental control – Ата-ана бақылауы бағдарламалары
Safe Kids – «Kaspersky Safe Kids» қауіпсіздік қосымшасы
СД – Сандық деректер
СҚБ – Сандық қауіпсіздік бойынша білім беру
SIM KIDS – Балаларға арналған қауіпсіз SIM-карталар пилоттық жобасы
ТККБ – Трансшекаралық кибер құқық бұзушылық
UNICEF (ЮНИСЕФ) – Біріккен Ұлттар Ұйымының Балалар қоры
VR – Виртуалды шындық
ХҚК – Халықаралық құқықтық көмек
ХҚЫ – Халықаралық құқықтық ынтымақтастық
ХС – Халықаралық стандарттар
ЦА – Цифрлық алаң (платформа)
ЦД – Цифрлық дәлелдемелер
ЦДИАӨМ – Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі
ЮНЕСКО (UNESCO) – Білім, ғылым және мәдениет мәселелері жөніндегі Біріккен Ұлттар Ұйымы

## КІРІСПЕ

**Зерттеу тақырыбының өзектілігі**. Кәмелетке толмағандардың цифрлық технологияларды, әлеуметтік желілер мен интернет-кеңістікті белсенді пайдалануы қазіргі заманда аса өзекті құқықтық мәселелердің біріне айналып отыр. Қазақстандағы ресми деректерге сүйенсек, 2020-2024 жылдар аралығында ішкі істер органдары кәмелетке толмағандарға қатысты немесе солар тарапынан жасалған 1200-ден астам құқық бұзушылықты тіркеген, олардың едәуір үлесі түнгі уақытта компьютер клубтарында не интернет-ортада жасалған бұзақылықтар, заңға қайшы контент тарату, киберқорқыту мен алаяқтық әрекеттерден тұрады [1]. Мәселен, 2023 жылғы ресми брифингте Павлодар облысының полиция департаменті бір ғана өңірдегі жасөспірімдермен байланысты 17 оқиға анықталғанын, негізінен интернет желісінде қауіпті байланыс орнату, жалған шоттар арқылы ақша жинау және онлайн алаяқтық жасау деректері өскенін атап өтті [2].

Бұл статистика елімізде де жастардың компьютерлік технологияларға икемділігі артып, кей жағдайларда оны теріс мақсаттарға пайдаланатынын аңғартады. Бір жағынан, халықаралық қауымдастық, соның ішінде ЮНИСЕФ (UNICEF) пен Еуропадағы Қауіпсіздік және Ынтымақтастық Ұйымы (ЕҚЫҰ) кәмелетке толмағандарды интернетте қудалау және зорлық-зомбылықтан қорғау шараларын ұдайы күшейтуді ұсынып келеді. UNICEF-тің “Child Online Protection” атты баяндамасында цифрлық технологиялар балалардың психологиялық және әлеуметтік дамуына орасан зор мүмкіндік бергенімен, онымен қатар виртуалды зорлық, өшпенділік тілі, кибербуллинг сынды құбылыстардың кең етек жайып бара жатқаны айтылған [3].

ЕҚЫҰ сарапшылары да “Blunting the cutting edge of crime: cybercrime in Central Asia” атты 2024 жылғы есебінде Орталық Азияда, соның ішінде Қазақстанда киберқылмыстың күшеюі жасөспірімдер арасында да орын алып, оларға арналған құқықтық құралдардың әлі жетілдірілмегенін ескертеді [4]. Осы проблеманың өзектілігі Қазақстанда заңнамалық және құқық қолдану тәжірибесі тұрғысынан да көрініс табуда. 2022 жылы “Баланың құқықтары туралы” заңға “кибербуллинг” ұғымы ресми түрде енгізіліп, кейін 2023 жылы Әкімшілік құқық бұзушылық туралы кодекске (ӘҚБтК) 127-2-бап қосылып, кәмелетке толмағанға қатысты буллинг әрекеттерін жасаған тұлғаларға әкімшілік жаза белгіленді [5], [6]. Мұндай қадамдар мемлекет пен қоғамның балаларды киберкеңістікте қорғау қажеттігін мойындап, нақты заңнамалық тетіктерді қалыптастыра бастағанын дәлелдейді. Алайда бұл шаралар жеткілікті ме, кәмелетке толмағандардың өзі киберкеңістікте құқық бұзушы рөлінде бола қалса, жауаптылық механизмі қандай болуы керек деген сұрақтар әлі де терең зерттеуді талап етеді. 2020-2025 жылдар аралығында көбіне түнгі уақытта интернет-клубта жүрген жасөспірімдердің, бейәдеп сөздер айтып, киберқорқыту жасағандардың ісі көптеп анықталуда, алайда бұл мәселелерді анықтау мен дәлелдеуде дәлелдемелерді заңды түрде жинау, сараптау және бағалау тәрізді

процессуалдық аспектілер жүйелі реттелмеген [7]. Мысалы, әлеуметтік желілерден алынған скриншоттардың дәлел ретіндегі статусы немесе провайдерден лог-файлдарды сұрау тәртібі көбіне нақты регламенттелмегендіктен, құқық қолданушылар арасында олқылықтар туындайды. Бұдан бөлек, Қазақстанда жасөспірімнің мұндай теріс қылық жасауына жауапты субъект ата-ана ма, әлде баланың өзі ме, жоқ әлде мектеп пе деген дилемма да өзекті. Қазіргі заңнамада (ӘҚБтК 127-бабы, 435-438-баптар) негізінен кәмелетке толмағандардың 16 жастан асқан жағдайда жеке өзі әкімшілік жауапкершілік тартатыны, 14-15 жастағы құқық бұзушылардың әрекетіне ата-анасы жауапты екені көрсетілгенімен, дәл “киберкеңістік” ұғымын жүйелі түрде қамтитын арнайы баптары әлі жетілмеген [8].

2022 жылы бала құқықтарына қатысты қабылданған өзгерістер ата-аналардың цифрлық тәрбие беру міндетіне де қатысты болуы мүмкін екенін құқық қолдану практикасы тек соңғы кездері түйсіне бастады. UNICEF сарапшылары 2022-2023 жылдары балалардың интернет-ортада кездесетін қорлаушылық хабарламаларды көру жиілігі айтарлықтай өскенін мәлімдеп, қазақстандық жасөспірімдердің 35%-ына жуығы әйтеуір бір рет кибербуллингке қатысы бар жағдаятқа тап болғанын атап көрсетті [3].

Балаға қатысты кибербуллинг пен түрлі қудалау әрекеттерінің көбеюі балалардың психологиялық денсаулығына әсер етіп, кей жағдайларда ауыр зардаптарға соқтыруы мүмкін. Бұл мәселені тек отандық заңнама аясында ғана емес, шетелдік тәжірибелермен салыстыру арқылы да қарастыру маңызды. АҚШ-та жасөспірімдер жасаған ауыр киберқылмыстар (мысалы, жүйеге заңсыз ену, біреудің құпия деректерін ұрлау) juvenile justice жүйесінде қаралуы мүмкін, алайда кей жерде ата-ананың жауаптылығын тікелей күшейтетін муниципалдық ережелер бар. Нью-Йорк штатының кей қалаларында бала кибербуллинг жасаса, белгілі бір мөлшерде айыппұлды баланың ата-анасы төлейді немесе қамауға алынады деген тәртіп енгізілген [9]. Ұлыбританияда кибербуллинг арнайы заңмен қудаланбағанымен, мектептерге балаларды кез келген буллингтен қорғау міндеттеліп, бұл талапты орындамаған мектеп әкімшілігіне ескерту не шара қолданылуы мүмкін. Германияда NetzDG заңы әлеуметтік желі иелеріне зиянды контентті жылдам жоюды міндеттейді, бұл кәмелетке толмағандардың құқықтарын қорғауға да ықпал етеді [10].

Оңтүстік Кореяда интернет арқылы жала жабу мен қорлауды қылмыстық жауаптылыққа жатқызғандықтан, кәмелетке толмаған құқық бұзушыларға да қатаң шаралар тағайындалады, бірақ олар көбіне оңалту орталықтарына, мінез-құлықты түзету бағдарламаларына бағытталады [11]. Балтық елдерінде, әсіресе Латвия мен Литвада, жасөспірімдердің киберкеңістікте жасаған ұсақ құқық бұзушылықтарына әкімшілік жаза қарастырылған, оның ішінде тәрбиелік ықпал ету шаралары да қолданылады [12].

Әлемдік тәжірибенің бұл алуандығы Қазақстан үшін де өзекті тұжырымдар жасауға мүмкіндік береді. Бір жағынан, елімізде балаларға интернеттегі еркіндік беріп, олардың ақпарат алу құқығын шектемеуге тырысу - маңызды принцип. Екінші жағынан, кәмелетке толмағандар

тарапынан құқықтық нормаларды бұзу қаупі жоғары екендігі де статистикамен дәлелденіп отыр. Сондықтан құқық қорғау органдары тарапынан жасөспірімдерді қатаң жазалау емес, керісінше, оларды қайта әлеуметтендіру, мінез-құлықты түзету, алдын алу мен ата-аналарды жауапкершілікке тарту тетіктерін кешенді түрде дамыту қажеттігі туындайды [13]. Бұған қоса, Қазақстанда 2022 жылы бала құқықтарын қорғау туралы заңға кибербуллинг ұғымын енгізу және 2024 жылы оның негізінде бірқатар әкімшілік істер қозғалуы тақырыптың көкейкестілігіне дәлел бола түседі.

Зерттеуімізде біз заңнамалық және нормативтік актілерге, 2020-2025 жылдардағы сот практикасына, Polisia.kz жариялаған полиция есептеріне, халықаралық ұйымдардың баяндамалары мен ұсыныстарына және шетелдік заңнама үлгілеріне сүйене отырып, кәмелетке толмағандар жасайтын Кибер құқық бұзушылықтарға қатысты әкімшілік іс жүргізудің теориялық және практикалық қырларын талдауға тырысамыз.

**Зерттеу объектісі**. Кәмелетке толмағандардың киберкеңістіктегі құқыққа қайшы мінез-құлықтары мен оларды әкімшілік-құқықтық реттеу тетіктері.

**Зерттеу пәні.** Кәмелетке толмағандар жасаған кибер құқық бұзушылықтардың құқықтық табиғаты, оларды анықтау, дәлелдеу, алдын алу және әкімшілік жауапкершілік мәселелері; осы саладағы ұлттық және халықаралық құқықтық нормалардың жүйесі мен оларды құқық қолдану практикасы.

**Зерттеудің мақсаты.** Кәмелетке толмағандардың кибер құқық бұзушылықтарын әкімшілік-құқықтық тұрғыда кешенді зерделеу, осы саладағы ұлттық заңнама мен құқық қолдану тәжірибесінің тиімділігін бағалау, халықаралық тәжірибелерді ескере отырып, Қазақстан жағдайына бейімделген ғылыми-негізделген ұсыныстар әзірлеу.

**Зерттеу міндеттері.** Осы мақсатқа жету үшін төмендегідей міндеттер қойылды:

1. Кәмелетке толмағандардың кибер құқық бұзушылықтарының ұғымдық-теориялық негіздерін және ерекшеліктерін жүйелеу;
2. Қазақстан Республикасының заңнамасындағы кәмелетке толмағандарға қатысты Кибер құқық бұзушылықтарды әкімшілік-құқықтық реттеу тәжірибесін талдау;
3. Халықаралық және шетелдік құқықтық реттеу үлгілерін салыстырмалы түрде зерттеу;
4. Ұлттық тәжірибедегі негізгі проблемалар мен олқылықтарды айқындау;
5. Кәмелетке толмағандардың құқықтарын қорғау мен алдын алуға бағытталған тиімді әкімшілік-құқықтық шараларды негіздеу және нақты ұсыныстар әзірлеу.

**Зерттеудің нормативтік негізі.** Зерттеудің нормативтік базасын Қазақстан Республикасының Конституциясы, Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы кодексі (ӘҚБтК), Қылмыстық кодекс, «Баланың құқықтары туралы» Заң, Білім туралы заң, сонымен қатар халықаралық келісімдер мен конвенциялар (Budapest Convention, Lanzarote Convention, БҰҰ және ЮНИСЕФ құжаттары), Германияның NetzDG заңы,

Ұлыбританияның Age-Appropriate Design Code және басқа да елдердің заңнамалық актілері құрайды.

**Зерттеу әдістері (методология)**. Бұл жерде әдіснамалық база ретінде бірнеше тәсіл қолданылды. Біріншіден, диалектикалық әдіс тақырыптың үздіксіз өзгеріп отыратын цифрлық ортадағы сипатын ескеріп, кәмелетке толмағандардың құқық бұзушылықтарын әлеуметтік ахуалмен және технологиялық даму үдерісімен байланыста талдауға мүмкіндік берді.

Екіншіден, салыстырмалы-құқықтық талдау арқылы АҚШ, Германия, Оңтүстік Корея, Балтық елдері секілді мемлекеттер тәжірибесін Қазақстан заңнамасымен салыстырып, ұқсастықтары мен ерекшеліктерін көрсеттік [9-12]. Үшіншіден, статистикалық тәсіл ішкі істер органдары мен соттардың ресми деректерін (2020-2025 жж.) жүйелеп, киберкеңістікте жасалатын құқық бұзушылықтардың ерекшеліктерін нақты сандар арқылы сипаттауға ықпал етті [1], [2]. Төртіншіден, құқықтық-нормативтік талдау арқылы "Баланың құқықтары туралы" заңның 2022 жылғы редакциясы, ӘҚБтК-нің жаңа баптары және халықаралық деңгейде қабылданған Budapest Convention on Cybercrime, Lanzarote Convention, UNICEF және ЕҚЫҰ ұсынымдары қарастырылды [3], [4], [5], [6].

**Ғылыми жаңалығы**. Зерттеу тақырыбының ғылыми жаңалығы, біріншіден, Қазақстан үшін жаңаша түсінік саналатын "Кибер құқық бұзушылық" санатын кәмелетке толмағандар жасаған теріс қылықтар аясында кешенді түрде талдауда. Бұған дейін Жұмабекова және басқалар "Ensuring children's online safety in Kazakhstan" атты еңбегінде балаларды зиянды интернет-контенттен қорғау механизмдерін салыстырмалы түрде қарастырғанымен, дәл кәмелетке толмағандардың кибербуллинг, киберқорқыту, заңсыз ақпарат тарату секілді әрекеттері және олардың әкімшілік-құқықтық реттеу ерекшеліктері жеткілікті талданбаған [5].

Екіншіден, цифрлық дәлелдемелерді іс жүргізуде қолдану тәртібі, баланың жауаптылық шегін анықтау мен ата-ана міндетін бөлектеу мәселесі осы жұмыста алғаш рет тұтас зерделенді. Үшіншіден, халықаралық тәжірибедегі (соның ішінде АҚШ-тағы ата-анаға айыппұл салу үлгісі, Германияның NetzDG механизмі, Оңтүстік Кореяның баланы қайта әлеуметтендіру бағдарламалары) озық тәсілдер талданды да, соның негізінде ұлттық заңнама мен практикаға енгізуге болатын нақты ұсыныстар тұжырымдалды [9], [10], [11].

Кәмелетке толмағандардың кибер құқық бұзушылықтарын әкімшілік-құқықтық тұрғыда зерттеу бағытында Қазақстанда соңғы жылдары бірқатар ғылыми ізденістер жүргізілуде. Мысалы, М.Ж. Жұмабекова балалардың интернеттегі қауіпсіздігі, онлайн-буллингтің алдын алу және құқықтық реттеу мәселелерін қарастырған; А.А. Айтмұхамбетова кәмелетке толмағандардың әкімшілік және қылмыстық жауапкершілігі бойынша зерттеулер жүргізген; Т.К. Айтмағамбетов пен Е.Ә. Ыдырысова кәмелетке толмағандардың құқықтық мәртебесі мен ювеналды юстиция мәселелерін талдаған. Отандық авторлардың еңбектерінде балалардың құқықтарын қорғау, ювеналды юстиция институттарының қызметі, профилактикалық

және құқықтық шаралар талданғанымен, дәл кәмелетке толмағандардың киберкеңістіктегі құқық бұзушылықтары әкімшілік-құқықтық категория ретінде жүйелі қарастырылмаған. Ал шетелдік ғылыми әдебиетте бұл тақырыпты Sonia Livingstone (Ұлыбритания), Elisabeth Staksrud (Норвегия), Brian O'Neill (Ирландия) сынды жетекші ғалымдар, сондай-ақ UNICEF, EU Kids Online жобасы, ЕҚЫҰ және Еуропалық Одақ сарапшылары зерттеген.

Алайда Қазақстанда кәмелетке толмағандардың кибер құқық бұзушылықтарын әкімшілік-құқықтық категория ретінде, халықаралық тәжірибемен салыстыра отырып, эмпирикалық деректер мен цифрлық дәлелдемелерді құқық қолдану саласында пайдалану механизмдерін тұтас қарастырған зерттеулер жоқтың қасы.

Осы диссертациялық жұмыстың ғылыми жаңалығы - кәмелетке толмағандардың кибер құқық бұзушылықтарын алғаш рет ұлттық заңнама аясында дербес құқықтық категория ретінде қарастыруда, әкімшілік жауаптылық, ата-ана мен интернет-провайдер арасындағы өзара байланыстарды анықтауда және халықаралық стандарттарды ұлттық ерекшелікке бейімдеу бойынша нақты ұсыныстар әзірлеуде көрінеді.

**Теориялық және практикалық маңыздылығы**. Теориялық тұрғыдан алғанда, бұл зерттеу ювеналдық юстиция, кибер құқық, әлеуметтік және педагогикалық сараптама ұштасатын көпсалалы тақырыпқа отандық құқықтық ғылымның назарын аударып, жаңа әдіснамалық бағыттарды дамытады. Практикалық мәні де айқын: алдын ала зерттеу барысында жасалған ұсыныстарымызды құқық қорғау органдары, білім беру мекемелері мен ата-аналар қауымдастығы бала қауіпсіздігін қамтамасыз ету шараларында басшылыққа алуы ықтимал. Заң жобаларына түзетулер енгізу немесе баланың интернет кеңістігіндегі жауаптылығын нақтылайтын нұсқаулықтар әзірлеуде де осы жұмыстың нәтижелері қажетті анықтама бола алады [13]. Қазіргі кезде Қазақстандағы цифрлық құқықтың даму үдерісі "Бала құқықтары туралы" заңға енгізілген түзетулерден бастау алғанымен, әлі де кәмелетке толмағандардың құқықтық мәртебесін тиянақты айқындайтын және кибер құқық бұзушылықтың салдарын нақты әкімшілік реттеуге жол ашатын ережелер толыққанды қалыптасқан жоқ. Сондықтан бұл диссертациялық зерттеу еліміздегі интернет кеңістігінде орын алып жатқан осал тұстарды жою үшін де, халықаралық стандарттарға сәйкес баланың мүддесін қорғау үшін де теориялық және тәжірибелік негіз қалыптастырады.

**Қорғауға шығарылатын негізгі тұжырымдар**:

1. Кәмелетке толмағандардың кибер құқық бұзушылықтары «әкімшілік-құқықтық» категория ретінде дербес қарастырылуы керек, осыған орай Әкімшілік құқық бұзушылық туралы кодекстің (ӘҚБтК) арнайы баптарында (немесе тармақшаларында) "цифрлық деликт" ұғымының нақты критерийлері мен элементтері белгіленуі қажет.
2. Цифрлық дәлелдемелерді (скриншоттар, лог-файлдар, электронды хаттар) әкімшілік сот өндірісінде ресми дәлел ретінде танудың процессуалдық тәртібін жетілдіру қажет: провайдерлер мен әлеуметтік желі

әкімшілерінен ақпарат сұрату бойынша регламентті нақтылау, электронды құжаттарды растау әдістерін қатаң бекіту.

3. Баланың жауаптылық шегі мен ата-ана міндетін ажыратып, тиісті нормаларды айқындау: 14-15 жастағы жасөспірімдердің кибербуллинг, алаяқтық тәрізді әрекеттері үшін кім және қандай көлемде жауап береді, ата-анаға қандай жағдайда айыппұл салу немесе тәрбиелік ықпал ету шараларын қолдану қажет екендігін нақтылау.

4. Халықаралық тәжірибе (АҚШ-тағы ата-ана жауапкершілігін күшейту ережелері, Германияның NetzDG заңы, Оңтүстік Кореядағы қосымша түзету бағдарламалары) негізінде Қазақстан заңнамасына бейімделетін нақты ұсыныстар әзірлеу: балаларды интернет-ортада қорғау үшін құқық қолдану органдары мен платформаларға өзара ынтымақтастық орнату тетіктерін енгізу, шетелдік тәжірибені ұлттық ерекшеліктерге бейімдеп қабылдау.

5. Профилактикалық және тәрбиелік шараларды басым ету: кәмелетке толмағандарды қатаң жазалаудан гөрі оларға консультациялық, психологиялық, мінез-құлықты түзету бағытындағы бағдарламаларды кең ауқымда ұсыну механизмін заң жүзінде бекіту. Мұндай шаралар қайталанатын кибер құқық бұзушылықтардың азаюына ықпал етпек.

Осылайша, кәмелетке толмағандардың кибер құқық бұзушылықтарын әкімшілік-құқықтық тұрғыда талдау - цифрлану дәуірінде құқықтың жаңа салалары мен классикалық әкімшілік деликтологияның тоғысатын жері.

Балалардың цифрлық мінез-құлқын қадағалау, алдын алу, жауапкершілікке тарту және ең бастысы, қалыпты дамуына зиян келтірмеуді қамтамасыз ету - бұл бір ғана жазалау тәсілдерімен шешілмейтін, кешенді әрекеттерді талап ететін сала. Осындай көпқырлы талдау келешекте мемлекеттік органдарға, заң шығарушыға және білім беру ұйымдарына нақты нұсқаулықтар ұсынып, жасөспірімдер арасындағы киберқауіпті әрекеттерді азайтуға көмектеседі деп сенеміз. Қорыта келгенде, зерттеу жұмысы қарастырған мәселенің теориялық және практикалық құндылығы қоғамның цифрлық қауіпсіздік мәдениетін арттыруға және балаларды құқыққа қайшы әрекеттерден қорғауға үлкен үлес қосады деген тұжырыммен бекемделеді.

**Зерттеу нәтижелерінің апробациясы.** Зерттеу нәтижелерінің апробациясы оларды әртүрлі ғылыми-тәжірибелік алаңдарда талқылау және тәжірибеде қолдану барысында жүзеге асырылды. Диссертацияда қамтылған негізгі ережелер мен тұжырымдар 10 жарияланған мақалада өз көрінісін тапты, оның ішінде: 1 - «International Journal of Advanced Research in Law and Economics» атты халықаралық ғылыми журналда; 3 - Қазақстан Республикасының Ғылым және жоғары білім саласындағы сапаны қамтамасыз ету комитеті ұсынған басылымдарда; 6 - халықаралық ғылыми-тәжірибелік конференциялар материалдарында жарияланған.

**Диссертациялық зерттеудің құрылымы мен көлемі.** Диссертацияның логикасы мен құрылымы зерттеудің мақсаты мен міндеттеріне, сондай-ақ зерттелетін мәселенің ерекшелігіне негізделген. Жұмыс кіріспеден, негізгі мазмұнды қамтитын төрт бөлімнен, қорытындыдан, пайдаланылған әдебиеттер тізімінен және қосымшалардан тұрады.

# 1 КӘМЕЛЕТКЕ ТОЛМАҒАНДАРДЫҢ КИБЕР ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРЫНА ҚАТЫСТЫ ТЕОРИЯЛЫҚ НЕГІЗДЕР МЕН КОНЦЕПЦИЯЛАР

## 1.1. Кәмелетке толмағандардың құқықтық мәртебесі және киберкеңістіктегі ерекшеліктері

Кәмелетке толмағандардың құқықтық мәртебесінің тарихи-құқықтық дамуы. Жалпы құқық теориясында кәмелетке толмағандардың құқықтық мәртебесі деп мемлекет ресми танып, кепілдік берген, балаға дербес құқық субъектісі ретінде тиесілі құқықтар, бостандықтар мен міндеттердің жиынтығы түсініледі. Тарихқа көз жүгіртсек, ерте заманда балалар көбіне толық құқықтық субъектілер ретінде қарастырылмаған; олардың мәртебесі ата-ана билігіне тәуелді, құқықтары шектеулі болғаны белгілі.

Балаларға қатысты қазіргі түсініктегі құқықтық қорғау идеясы халықаралық деңгейде XX ғасырдың басында ғана қалыптаса бастады. Мәселен, Бірінші дүниежүзілік соғыстан кейін 1923 жылы ағылшын және швед қайраткерлері Ұлттар Лигасы аясында бала құқықтарын қорғау концепциясын ұсынған екен. Сол тарихи кезеңнен бастап әлемнің бірқатар елдерінде кәмелетке толмағандардың істерін қарастыратын мамандандырылған соттар - ювеналдық соттар - құрыла бастады [14].

1924 жылғы Женева декларациясы мен 1959 жылғы БҰҰ Балалар құқықтарының декларациясы сияқты құжаттар балалардың ерекше құқықтарын мойындаудың негізін қалады. Ал 1989 жылы қабылданып, Қазақстан 1994 жылы 8 маусымда ратификациялаған Бала құқықтары туралы БҰҰ Конвенциясы балалардың құқықтары мен мүдделерін халықаралық деңгейде жан-жақты бекіткен маңызды акт болды [15].

КСРО дәуірінде де кәмелетке толмағандарға қатысты арнайы мемлекеттік саясат қалыптасты: 1930-жылдардан бастап кәмелетке толмағандар істері жөніндегі комиссиялар жұмыс істеп, жасөспірімдердің қадағалаусыз қалуын болдырмау, құқық бұзушылықтардың алдын алу шараларын жүзеге асырғаны мәлім. Дегенмен кеңестік кезеңде ювеналдық әділет жүйесі толық дамыған жоқ - жасөспірімдер жасаған қылмыстар жалпы соттарда қаралып, тек арнайы тәрбие мекемелері арқылы түзетуге мән берілді. Тек тәуелсіздікпен бірге елімізде балалардың құқықтық жағдайын халықаралық стандарттарға сай жаңаша қарастыру басталды.

Қазақстан Республикасында кәмелетке толмағандардың құқықтық мәртебесін нығайту жолында маңызды қадамдар жасалды: еліміздің Негізгі Заңы - Конституцияда отбасы мен балалық шақ мемлекеттің қорғауында екені бекітіліп, ата-аналардың бала тәрбиелеу мен қамқорлық жасау міндеті конституциялық норма дәрежесінде айқындалды Баланың құқықтарын қорғау туралы ұлттық заңнама да қалыптасты: 2002 жылы «Қазақстан Республикасындағы баланың құқықтары туралы» арнайы Заң қабылданып, онда баланың негізгі құқықтары мен заңды мүдделерін іске асыруға байланысты қатынастар реттелді [16]. Бұл заң Балалар құқықтары туралы

конвенцияның талаптарын ұлттық деңгейде бекітіп, бала мүддесін бірінші орынға қою принципін жария етті.

Тәуелсіздік жылдарында елімізде ювеналдық әділет жүйесі кезең-кезеңімен енгізілді. 2005 жылғы Судьялардың IV съезінде кәмелетке толмағандардың істері жөніндегі мамандандырылған соттарды құруды тапсырып, 2007 жылдың 23 тамызында «Кәмелетке толмағандардың істері бойынша мамандандырылған ауданаралық соттарды құру туралы» Жарлыққа қол қойды [17]. Осы жарлық негізінде алғаш рет Астана мен Алматы қалаларында жасөспірімдер істерін қарайтын мамандандырылған соттар өз жұмысын бастады. Бастапқыда пилоттық жоба ретінде екі ірі қалада құрылған ювеналдық соттар өз тиімділігін көрсеткен соң, кейінірек республика бойынша басқа өңірлерге де таратылды. Нәтижесінде, қазіргі кезде Қазақстанда ювеналдық соттар жүйесі қалыптасып, бала құқықтарын сот арқылы қорғаудың мамандандырылған механизмі жұмыс істеуде.

Ювеналдық соттардың енгізілуі - еліміздің құқықтық дамуының тарихи кезеңі, бұл қадам Қазақстанның халықаралық озық тәжірибелерге үндес екендігін айғақтайды [18, с. 94]. Мысалы, шет мемлекеттерде (АҚШ, Франция, т.б.) ювеналдық әділет өткен ғасыр басынан қолданыс тауып келсе, біздің еліміз де осы сынақтан өткен үлгіні қабылдап, оның тиімді жақтарын іске асырды. Сонымен бірге, кәмелетке толмағандардың құқықтық мәртебесінің тарихи эволюциясы тек сот жүйесін құрумен шектелмейді.

Қоғамның балаға көзқарасы, заңнамадағы баланың орны да өзгерді. Бұрын баланың құқығы көбіне отбасылық қатынастар шеңберінде ата-ана құқығының туындысы ретінде қаралса, қазір бала өзіндік құқық иесі, дербес заңды мүдделері бар тұлға ретінде қабылданады. Құқықтық сананың өзгеруі - осы тарихи дамудың жемісі. Баланы «қорғау объектісі» ғана емес, өз құқықтарын белсенді жүзеге асыра алатын субъект деп тану қағидасы орнықты. Қазақстанның «Баланың құқықтары туралы» заңының кіріспесінде де мемлекет баланың конституциялық құқықтары мен заңды мүдделерін қамтамасыз етуді өз саясатының басым бағыты деп жариялады [19, с. 22].

Расында да, бүгінгі таңда кәмелетке толмағандардың құқықтық жағдайын нығайту, әсіресе оларды құқыққа қарсы қол сұғушылықтардан қорғау мемлекеттік саясаттың басым бағыттарының бірі саналады [19, с. 23]. Мұны 2021 жылғы Президент Жолдауында балаларды зорлық-зомбылықтан, соның ішінде киберкеңістіктегі буллингтен қорғау жөнінде заңнамалық шаралар қабылдау туралы тапсырма берілгенінен де байқауға болады.

Жас ерекшеліктерінің құқықтық жауапкершілікке әсері. Кәмелетке толмағандардың құқықтық мәртебесінің маңызды қыры - олардың құқықтық жауапкершілік ерекшеліктері мен жас шамасына байланысты жеңілдіктері. Көптеген елдердің заңнамасы сияқты, Қазақстанда да жеке адамның құқықтық қабілеті мен жауаптылығы оның жасына тікелей тәуелді. ҚР заңдары 18 жасқа толмаған азаматтарды кәмелетке толмаған деп таниды және олар үшін арнайы жеңілдікті режимдер қарастырған. Мәселен ,қылмыстық жауаптылық жасына қатысты Қазақстан Республикасының Қылмыстық кодексі жалпы тәртіп бойынша 16 жасты белгілейді, ал аса ауыр және ауыр

санаттағы кейбір қылмыстар бойынша 14 жастан бастап қылмыстық жауапқа тарту мүмкіндігін көздейді. Әкімшілік құқық бұзушылықтар үшін жауаптылық та, негізінен, 16 жастан басталады, алайда ұсақ бұзақылық жасаған ерекше жағдайларда 14 жастан әкімшілік жаза қолданылуы мүмкін [16]. Яғни, заңнамамыз балаға 14 жасқа толғаннан бастап кейбір құқықтық әрекеттеріне санаулы дәрежеде жауап беруді жүктейді, бірақ толық көлемдегі жауаптылық 16-18 жастан бастап қана туындайды.

Жастың толмауына байланысты жауаптылықтың шектеулі болуы - құқық жүйесінің кәмелетке толмағандарды психологиялық, физиологиялық жетілмеуіне орай ересектермен бірдей жауапқа тартуға болмайтынын мойындауы. Сондықтан қылмыстық саясатта кәмелетке толмағандарға арналған ерекше ережелер бар: жеңілдететін жағдайлар, жаза тағайындауда төменгі шектердің аз болуы, бас бостандығынан айырудың ерекше тәртіптері (арнайы тәрбиелеу мекемелерінде өтеу және т.б.), сондай-ақ жаза мен жауапкершіліктен босатудың кең мүмкіндіктері. Мысалы, еліміздің қылмыстық заңнамасында тәрбие ықпалы бар мәжбүрлеу шараларын қолдана отырып, жасөспірімді қылмыстық жауаптылықтан босату, жазаны өтеуден шартты босату, т.б. кеңінен қолданылады. Мұның бәрі - мемлекеттің өсіп келе жатқан жас буынды қоғамға қайта бейімдеуге, жазалау емес, тәрбиелеу мақсатына басымдық беруінің көрінісі. Дегенмен, соңғы жылдары жасөспірімдер қылмысының алдын алу мәселесі өткір қойылуда: сот практикасы көрсеткендей, көптеген жағдайда жасөспірімнің қылмысқа баруына ата-анасының тарапынан бақылаудың болмауы түрткі болады.

Павлодар облыстық полициясының дерегі бойынша, 2023 жылдың алғашқы 7 айында өңірде кәмелетке толмағандар 17 қылмыс жасаған, талдау нәтижесінде олардың көбінде ата-ана назарынан тыс қалу себеп болғаны анықталды. Осыған орай, ата-анаға жүктелетін заңи жауапкершілік те күшейтілуде: ҚР Әкімшілік құқықбұзушылық туралы кодексінің 127-бабы бала тәрбиелеу міндеттерін орындамау не тиісінше орындамау (оның құқық бұзушылық жасауына жол беру) үшін ата-ананы жауапқа тартуға мүмкіндік береді. Мысалы, 2023 жылы елімізде осы бап бойынша жүздеген ата-ана әкімшілік жауапкершілікке тартылғаны тіркелген [16].

Жас ерекшеліктеріне байланысты тағы бір маңызды аспект - құқық қабілеттілік пен әрекет қабілеттілік шектері. Қазақстан Республикасының Азаматтық кодексі бойынша 18 жасқа толмағандар толық әрекет қабілетті емес деп танылады: 14-18 жастағы жеткіншектердің әрекет қабілеті ішінара (ата-анасының келісімімен мәмілелер жасауға құқылы), ал 14 жасқа толмаған балалардың көпшілік мәмілелерді өздігінен жасауға құқығы жоқ, олар үшін ата-анасы немесе заңды өкілдері әрекет етеді. Бұл шектеулер де жасөспірімдерді өздері толық түсінбейтін құқықтық мәмілелерден сақтап, мүдделерін қорғауға бағытталған. Алайда қазіргі цифрлық дәуірде бұл классикалық нормалар жаңа сынақтарға тап болуда: балалар интернет арқылы түрлі келісімдерге келе алады, онлайн сервис шарттарын «қабылдай» салады, яғни іс жүзінде құқықтық сипаттағы әрекеттерді жеңіл жүзеге асырады. Бірақ олардың көпшілігінің заң тұрғысынан күші күмәнді, өйткені

жастағы шектеулер бар. Автордың байқауынша, кәмелетке толмағандардың құқықтық жауаптылығының жас шектері қазіргі уақытта қайта зерделеуді қажет етеді: бір жағынан, ауыр қылмыстардың «жасарып» бара жатқаны жауаптылық жасын төмендету мәселесін туындатса, екінші жағынан, тұрмыс-тіршілік ерте есейтіп отырған бүгінгі заманда кейбір азаматтық-құқықтық әрекеттерде балалардың дербестігін тану жайын қарастыруға болады. Бұл күрделі дилеммалар заңнамалық реформаларда, ғылыми ортада талқыға түсіп жүрген өзекті мәселелер санатына жатады.

Киберкеңістіктегі құқықтық субъектілік трансформациясы. XXI ғасырдың цифрлық дәуірі балалардың өміріне бұрын-соңды болмаған жаңа мүмкіндіктер мен қатерлер әкелді. Кәмелетке толмағандардың құқықтық субъектілігі киберкеңістікте айтарлықтай өзгереді, тіпті кей тұста қайта түзіледі деуге болады. Ең алдымен, интернет пен цифрлық технологиялар баланың әлеуметтік өмірге еркін араласуын жеңілдетті: қазірдің өзінде балалардың басым көпшілігі ғаламторды күнделікті пайдаланады. Зерттеулерге қарағанда, Ресейде 12-17 жас аралығындағы жасөспірімдердің 99%-ы күн сайын интернетке кірсе, 7-11 жастағы балалардың 83%-ы, тіпті 3-6 жастағы сәбилердің өзінде 68%-ы ғаламторды пайдалануға тартылған [20].

Қазақстанда да ұқсас жағдай: мектеп жасындағы балалардың басым бөлігі - оқу, ойын-сауық, коммуникация үшін онлайн кеңістікті пайдаланады. Цифрлық буынның өкілдері технология тілін ерте меңгеріп, киберкеңістікте «виртуалды азаматтық» танытып отыр. Алайда баланың цифрлық әлемге бұлай кеңінен енуі оның құқықтық жағдайын күрделендіре түсуде. Нақтылай айтқанда, кәмелетке толмаған интернетте бола тұрып әдеттегі офлайн өмірінде кездеспейтін жаңа құқықтық қатынастарға тап болады. Біріншіден, баланың жеке басының дербестігі мен қауіпсіздігіне қатысты тәуекелдер артады: интернетте бала өз бетінше тіркелгі жасайды, түрлі сервиске жазылады, келісім шарттарын белгілейді - бұлардың бәрінде шын өмірдегідей ата-ананың немесе мемлекеттік органның тікелей бақылауы жоқ.

Номиналды түрде көптеген веб-платформаларпайдаланушы келісімінде жас шектеулерін көрсетіп, «13 жастан асқан болуы керек», «ата-ана рұқсаты қажет» деген талаптар қояды. Алайда іс жүзінде мұны айналып өту оп-оңай: кез келген бала жасын үлкенірек етіп көрсете салады. Нәтижесінде құқықтық рұқсат пен тыйым механизмдері толық іске аспай, балалар өздерін ересектерше ұстай алатын ортада қалады.

Екіншіден, цифрлық кеңістікте баланың құқықтық субъектілігі шекараларды бұзады - ғаламтор глобалдық болғандықтан, баланың құқықтары мен міндеттері тек өз елінің заңдарымен шектелмейді, трансшекаралық сипат алады. Мысалы, Қазақстанда бала құқықтарын қорғайтын белгілі бір тыйым немесе фильтр болса, басқа мемлекетте ондай шектеу жоқ болуы мүмкін, ал интернетте ол шекпен қамтамасыз етілмейді.

Бұл баланың құқықтық қорғалуын әлсіретеді: ұлттық құқықтық жүйе балаға офлайн кепілдік берген көп нормалар онлайн кеңістікте орындалмай қалуы мүмкін. Басқаша айтқанда, киберкеңістікте бала тек Қазақстан

заңдарының «қамқорында» емес, сонымен бірге халықаралық, шетелдік құқықтық режимдердің ықпалына түседі.

Үшіншіден, баланың цифрлық ортадағы мінез-құлқы жаңа құқықтық жауаптылық түрлерін туындатуда. Бұрын бала үйінде отырып, бүкіл әлемге жария мәлімдеме жасай алмайтын, қазір әлеуметтік желіде кез келген пікірді ашық тарата алады. Бұл – сөз бостандығы құқығын жүзеге асырудың бір көрінісі, бірақ онымен қоса баланың өз айтқан сөзі үшін жауап беру мәселесі туындайды. Мысалы, бала желіде басқа адамды қорласа немесе жалған ақпарат таратса, формальды түрде бұл әрекеттер заңға қайшы, бірақ баланың жасы кіші болса, оған қандай шара қолдану қажет? Осы сұрақтар құқық қолдану практикасына қиындық тудырып отыр: бала біреуге жала жапса не кибербуллинг жасаса, жасы жетпегендіктен қылмыстық жауапқа тартылмайды, алайда жәбірленуші тарап әділдік іздейді. Демек, цифрлық әлемде баланың құқықтық мәртебесі жаңа балама механизмдерді талап етеді - дәстүрлі жауапкершілік жүйесін (қылмыстық, әкімшілік жаза) педагогикалық, психологиялық шаралармен толықтыру немесе интернет-платформалардың өзін-өзі реттеуін пайдалану қажет болады.

Сондай-ақ, кәмелетке толмағандардың құқықтық санасы мен мәдениеті де цифрлық ортада сынға түседі. Жасөспірімдер онлайн кеңістікте өзін еркін сезінгенімен, құқықтық сауаты жетіспесе, опық жеп қалуы оңай. Мысалы, жеке мәліметтерін бөтен адамдарға бере салу, фишингтік алдауға түсу, күмәнді «челлендждерге» қатысу - мұның бәрі құқықтық және моральдық тұрғыдан қауіпті нәрселер. Интернеттегі ақпараттың ықпалы туралы ресейлік зерттеуші Н.М. Хромованың еңбегінде: «Интернетте таратылатын ақпарат балаларды кейде қоғамға қарсы мінез-құлыққа итермелейді, олардың құрбан болуына және қылмысқа тартылуына ықпал етеді» деп атап көрсетілген.

Шынында да, онлайн ортада бала теріс бағыттағы әсерлерге көбірек ұшырайды: экстремизм мен зорлық-зомбылықты насихаттайтын контент, өзін өзі зақымдауға немесе суицидке шақыратын «сынақтар» (мысалы, бір кездері қоғамды шошытқан «Көк кит» ойыны), порнографиялық материалдарға қолжетімділік - осындай ақпараттар жасөспірімнің психикасына, әлеуметтену үрдісіне зиян келтіреді. Бұл баланың құқықтық мәртебесінің жаңа аспектісі - ақпараттық қауіпсіздік құқығын алдыңғы қатарға шығарды. Қазақстандық зерттеушілер М.Т. Акимжанова мен Т.С. Тілеп атап өткендей, баланың өмірі мен денсаулығына қатер төндіретін немесе дамуына зиян келтіретін ақпараттан қорғалуға құқығы - балалардың басымдықпен қорғалатын құқықтарының бірі [20]. Демек, баланың ақпараттық қауіпсіздігі бүгінде оның құқықтық мәртебесінің өзекті құрамдас бөлігіне айналды.

Цифрлық ортадағы нақты проблемалар және құқықтық практика. Бүгінгі күні баланың құқықтық жағдайын цифрлық кеңістікте сипаттайтын бірқатар өзекті проблемалар бар. Олардың қатарында мыналарды атап өтуге болады:

- Ата-ана жауаптылығының ауқымы. Жоғарыда айтылғандай, заң бойынша ата-ана баланы тәрбиелеуге және қорғауға міндетті [16], ал бала теріс қылық жасаса, көбіне ата-ана жауап береді (материалдық шығынды өтеу, әкімшілік айыппұл төлеу және т.б.). Цифрлық кеңістікте бұл қағидатты

қолдану оңай емес. Мысалы, бала әлеуметтік желіде басқа біреуге тіл тигізіп, абыройына нұқсан келтірсе (яғни, интернет арқылы құқық бұзса), жәбірленуші сотқа шағымданған жағдайда зиянды өтеуді ата-анасынан талап етуі мүмкін. Азаматтық заңнама бойынша, он төрт жасқа толмаған жасөспірімдердің жасаған мәмілелері мен келтірген зияны үшін ата-анасы жауап береді, ал 14-18 жас аралығында жауаптылықты бала өзі және ата-ана бірге бөліседі деп шартты түрде айтуға болады [21]. Дегенмен, интернеттегі құқық бұзушылықтар көбіне жасырын немесе трансшекаралық сипатта болғандықтан, ата-ананың да баласының барлық ісінен хабардар болуы қиын.

Мемлекеттік органдар осы мәселені шешу үшін ата-аналардың цифрлық сауатын көтеру, балалардың интернеттегі белсенділігін қадағалауын заңмен міндеттеу бағытында қадамдар жасауда. Мысалы, ҚР ӘҚБтК-нің 435-бабы бойынша ата-ана кәмелетке толмаған баласының түнгі уақытта ойын-сауық мекемелерінде жүруіне жол бергені үшін жауапқа тартылады [16]. Сол сияқты, 2021 жылы қабылданған бала құқықтарын қорғау жөніндегі заңнамалық түзетулерге сәйкес, елімізде шетелдік онлайн-платформалар балаларға зиян контентті бақылау шараларын күшейтуге міндеттелді [22].

Ата-ананың цифрлық ортадағы жауапкершілігі жөнінде қоғамда да пікірталастар жүріп жатыр: «Баланың онлайн іс-әрекеті үшін ата-ананы жазалау қаншалықты әділ?» деген сұрақ жиі көтеріледі. Біздіңше, бұл жерде тепе-теңдік қажет: бір жағынан, ата-ана өз баласының интернеттегі жүріс-тұрысына белгілі бір дәрежеде жауапты болуы тиіс (тәрбиелік бақылау міндеті), екінші жағынан, баланың жеке кеңістігі мен құпиясына шамадан тыс қол сұғуға да болмайды. Осы мәселенің шешімін табуда кей мемлекеттер заңнамалық ерекше жолдарды таңдауда - мысалы, АҚШ-та кейбір штаттарда балалардың әлеуметтік желіге тіркелуі тек ата-ана келісімімен мүмкін болатынын бекітетін заңдар. Флорида штаты 2023 жылы 14 жасқа дейінгі балалардың әлеуметтік желі аккаунттарын мүлде жауып тастауды, ал 14-15 жастағылар үшін ата-анасының рұқсаты міндетті болуын заңмен енгізді.

Джорджия, Теннесси сынды штаттар да кәмелетке толмағандардың аккаунттарына ата-аналық верификация және келісім шарттарын енгізуді талап етті [23]. Бұл шаралар ата-ананың жауапкершілігін заң арқылы бекіту әрекеті болса, Еуропада балама жолдар қарастырылуда - ата-аналарға арналған бала қауіпсіздігі туралы нұсқаулықтар, ата-ана бақылауы (parental control) бағдарламаларын пайдалану ынталандырылуда. Қазақстан үшін де цифрлық дәуірдегі ата-ана жауапкершілігінің шегін нақтылап, қажет болса заңнаманы жетілдіру өзекті. Баланың «цифрлық келісімі» (онлайн келісім беру мәселесі). Кәмелетке толмаған адамның заңды мәмілелерге келісім беру қабілеті шектеулі екенін айттық. Бірақ іс жүзінде балалар күн сайын интернетте түрлі келісімдерге қатысып жатыр: әлеуметтік желілердің пайдалану шарттарын қабылдайды, мобильді қосымшаларды орнатқанда шығатын лицензиялық келісімдерді «оқыдым, келісемін» деп белгілейді, кейде электрондық саудада төлем операцияларын жасайды. Заң тұрғысынан алып қарағанда, мұндай келісімдердің көпшілігі күмәнді - себебі бала ресми әрекет қабілетті емес, демек оның келісімі жарамсыз деп танылуы мүмкін.

Алайда платформа иелері бұған назар аудармайды, ал бала өз құқығының бұзылғанын аңғармайды. Нәтижесінде, баланың дербес деректерінің жиналуы, оларды жарнамалық мақсатта пайдалану, тіпті үшінші тұлғаларға берілуі ата-ана келісімінсіз жүре береді. Бұл – баланың құпиясына, жеке деректеріне қол сұғылмау құқығына қатер. Халықаралық деңгейде балалардың дербес деректерін қорғау ерекше маңызға ие болып отыр. 2018 жылы күшіне енген Еуропалық Одақтың Жалпы деректерді қорғау регламенті (GDPR) бойынша, 16 жасқа дейінгі балалардың дербес ақпаратын өңдеуге тек ата-ана рұқсатымен жол беріледі (кейбір елдер бұл шекті 13 жасқа төмендетті). Америка Құрама Штаттарында 1998 жылдан бері Балалардың онлайн құпиялылығын қорғау туралы заң (COPPA) қолданыста, ол 13 жасқа толмаған балалардың жеке ақпаратын ата-анасының верификацияланған келісімінсіз жинауға тыйым салады. Қазір көптеген елдерде осы үлгіге ұқсас заңдар пайда болуда: 2024 жылы Вирджиния мен Нью-Йорк штаттары 13-17 жас аралығындағы жасөспірімдердің деректерін жинауды өз юрисдикцияларында реттейтін құқықтық актілер қабылдап, ата-ананың келісімі мен баланың саналы келісімін талап етуде [23]. Қазақстанда да дербес деректерді қорғау туралы заңнама бар, алайда ол балалардың цифрлық келісімінің ерекшеліктерін жекелей қарастырмаған. Осыған байланысты, автордың пікірінше, болашақта елімізде «цифрлық келісім» ұғымын заңнамалық тұрғыда айқындап, белгілі бір жасқа дейінгі балаларға қатысты онлайн мәмілелер мен келісімдердің құқықтық күшін конкретизациялау қажет. Бұл баланың цифрлық ортадағы құқықтық қауіпсіздігін қамтамасыз етудің маңызды шарты болмақ.

Әлеуметтік желідегі буллинг (кибербуллинг). Соңғы жылдары балалар арасында өзекті мәселеге айналған құбылыс - буллинг, оның ішінде интернеттегі қудалау, зорлық-зомбылық сипатындағы қысым. Кибербуллинг деп цифрлық технологияны қолдана отырып қорқыту, мазалау, қорлау әрекеттерін айтады [24]. Ол әлеуметтік желілерде, хабарлама алмасу қосымшаларында, онлайн ойындарда, жалпы интернеттің кез келген интерактивті алаңында көрініс табуы мүмкін. Кибербуллингтің дәстүрлі (мектептегі) буллингтен айырмашылығы - оның кең ауқымдылығы, тәуліктің кез келген уақытында жалғасуы және көпшілік алдында масқаралау ықтималының жоғарылығы. Қазақстан қоғамында буллинг мәселесі өте өзекті: зерттеулер көрсеткендей, жасөспірімдердің 17%-ы кемінде айына бір рет мектептегі немесе онлайн буллингтің құрбаны болады екен.

Ал 11-15 жастағы балалардың 12%-ы өмірінде бір рет болсын кибербуллингке ұшырағанын, 11%-ы өздері де басқаға қоқан-лоқы көрсетіп, кибербуллингке қатысқанын мойындаған. Бұл деректер кибербуллингтің кең таралғанын және оның құқықтық шараларды қажет ететінін айғақтайды.

Кибербуллинг баланың психикалық және эмоционалдық саулығына зор зиян келтіреді, оны шарасыздық пен үмітсіздік күйіне түсіреді, тіпті кей жағдайда өзіне қол жұмсауға итермелеуі мүмкін. Мұндай трагедиялар әлемде де, елімізде де орын алғаны белгілі. Осы себепті Қазақстан билігі балаларды буллингтен қорғау бағытында кешенді қадамдарға баруда. 2020 жылы

Мемлекет басшысы Қ.Тоқаев Жолдауында кибербуллингтің алдын алу үшін заңнамалық негіз қажеттігін атап өтіп. соның нәтижесінде 2021-2022 жылдары Парламент «Балаларды буллинг пен кибербуллингтен қорғау туралы» заңнамалық түзетулерді мақұлдады [25]. Аталған өзгерістер бойынша, Интернет желісіндегі заңға қайшы ақпаратты (баланы қорлайтын, зорлық-зомбылыққа шақыратын және т.б.) анықтау және жою тетіктері қарастырылды, сонымен бірге халықаралық платформаларды Қазақстан заңнамасын сақтауға міндеттеу шаралары енгізілді [22]. Бұл құқық қолдану тәжірибесінде алғашқы қадамдар ғана; кибербуллинг үшін қылмыстық жауаптылық мәселесі де талқылануда. Әзірге Қылмыстық кодекстің 131-бабындағы «қорлау» немесе 147-баптағы «жеке өмірге қол сұғу» сынды нормаларды пайдаланып, кей жағдайда кибербуллерлерді жауапқа тартуға әрекет жасалады, бірақ бала әрекет етсе, жасыңа байланысты жауапкершілік туындамай қалатынын жоғарыда айттық. Осы орайда құқық қорғау органдары көбіне тәрбиелік және сақтандыру шараларына жүгінуде: мектептерде буллингтің алдын алу бағдарламаларын енгізу, оқушылар мен ата-аналарға тренингтер өткізу, жұртшылықты ақпараттандыру.

Сарапшылардың пікірінше, буллингпен күресте ең бастысы - жазалау ғана емес, балаларды мейірімділікке, өзара құрметке баулу, агрессияны бейбіт жолмен өңдеуге үйрету. Мәселен, әлеуметтанушы М. Бектенованың айтуынша, буллинг мәселесін шешу үшін заң қабылдау жеткіліксіз, сонымен бірге «бала тәрбиесі, буллингтің алдын алу бойынша бағдарламаларды енгізу, балалар мен жасөспірімдердің бос уақытын тиімді ұйымдастыру жөнінде жүйелі жұмыс қажет». Бұл – маңызды тұжырым. Шынында да, кибербуллингтің түп-тамыры әлеуметтік ортада жатыр, оны тек құқықтық тетіктермен түбегейлі жою қиын. Сондықтан Қазақстан Үкіметі соңғы жылдары балалардың бос уақытын қамту, спорт және өнер үйірмелерін қолжетімді ету, психологиялық қызметтер желісін дамыту сияқты кешенді қадамдар жасауда [25]. 2023 жылғы жаңа заң бойынша мектептерде буллингтің алдын алу ережелері енгізіліп, әр білім беру ұйымында буллинг жағдайларын қарастыратын кеңестер құру міндеттелді. Осылайша, баланы цифрлық ортадағы қатігездік пен зорлықтан қорғау бағытында құқықтық практика да, әлеуметтік шаралар да қатар іске асуда.

Балаларды зиянды контенттен қорғау. Жоғарыдағы мәселелермен үндес тағы бір күрделі проблема - интернет кеңістігіндегі балаларға зиянды ақпарат. Бұл порнография, экстремизм, суицидтік бағыттағы материалдар, құмар ойынға тарту, есірткіні насихаттау және т.б. ақпарат түрлері. Мұндай контентке тосқауыл қою – баланың ақпараттық қауіпсіздік құқығын қамтамасыз етудің бір бөлігі. Қазақстан 2018 жылы «Балаларды денсаулығына және дамуына зиян келтіретін ақпараттан қорғау туралы» заң қабылдауға талпынғанымен, ол жоба күйінде қалды; дегенмен еліміздің қолданыстағы бірқатар заңнамалық актілерінде (БАҚ туралы заң, Білім туралы заң, Ақпараттандыру туралы заң, т.б.) балаларды зиянды ақпараттан қорғауға қатысты нормалар бар. Мысалы, ҚР «Бұқаралық ақпарат құралдары туралы» заңына енгізілген түзетулерге сәйкес, теле-радио өнімдерге жас

шектеу белгілері қойылады, +18 санатындағы мазмұн балалар көрмейтін уақытта ғана көрсетілуі тиіс. Интернеттегі зиянды контентті шектеу қиынырақ, өйткені ғаламтор ашық платформа. Қазіргі таңда бұл проблема әлемдік деңгейде шешімін іздеуде: кей мемлекеттер ірі технологиялық компанияларға заңмен міндеттеме қою арқылы (әрі қарай таратылатын контентті фильтрациялау, ата-ана бақылауы функцияларын енгізу, жасты тексеру жүйелерін орнату сияқты), ал кейбіреулері білім беру және ағарту шаралары арқылы балаларды дайын күйде қорғауға тырысады. БҰҰ Балалар құқығы комитеті 2021 жылы қабылдаған №25 жалпы ережеде барлық қатысушы мемлекеттерге «балалардың цифрлық ортада да құқықтары толық қорғалуы тиіс, соның ішінде оларды зиянды ақпараттан қорғау - мемлекеттің тікелей міндеті» екені айтылды. Бұл – халықаралық деңгейде қалыптасқан пікір. Осы тұрғыда Қазақстан да заңнамасын жетілдіру үстінде.

2020 жылы Ақпарат және қоғамдық даму министрлігі «Балалардың интернеттегі қауіпсіздігін қамтамасыз ету тұжырымдамасын» жариялап, онда заңнамалық, техникалық, ұйымдастырушылық шаралардың кешені ұсынылды. Соның бір парасы – «Интернеттегі ата-ана бақылауы» ұлттық жүйесін құру, провайдерлер деңгейінде зиянды сайттарды автоматты бұғаттау, сондай-ақ балалардың медиасауатын арттыру. Алайда бұл бастамалар әлі толыққанды іске аса қойған жоқ, негізінен ұсыныс күйінде.

Автордың ойынша, балаларды қорғайтын тиімді құқықтық механизм - ол мемлекеттің, бизнес секторының (интернет-сервис провайдерлері) және қоғамның бірлесе әрекет етуі. Заңға тек тыйымдар мен шектеулерді енгізіп қою жеткіліксіз, сонымен бірге сол заңның тетіктері нақты жұмыс істеуі үшін техникалық құралдар мен адами ресурстарды қосу керек. Мысалы, мектептерде «киберпатруль» қызметін құрып, оқушылар арасындағы қауіпті онлайн топтарды, буллинг фактілерін мониторинг жасау; ата-аналар мен мұғалімдерге арналған тұрақты семинар-тренингтер жүргізу; интернет компаниялармен меморандумдар жасап, балаға арналған қауіпсіз режимдер (Safe Mode, Kids Mode) енгізуді міндеттеу сияқты шаралар кешенді түрде атқарылса ғана нәтиже беретіні анық.

Бұл бағытта шетелдік тәжірибе де зерделенуі тиіс. Еуропаның дамыған елдерінде (Ұлыбритания, Германия, Франция, т.б.) балалардың ақпараттық қауіпсіздігін қамту үшін мемлекеттік бағдарламалар қабылданып, провайдерлерге нақты талаптар қойылғаны белгілі. Зерттеушілер Акимжанова мен Тілептің Еуропа елдері тәжірибесіне жүргізген салыстырмалы талдауы көрсеткендей, көптеген мемлекеттер ортақ үрдістерді ұстанады: балаға қауіпті контентті шектеу, цифрлық сауаттылықты оқу бағдарламасына енгізу, жауапты органдар мен Hot-line желілер құру секілді қадамдар баршаға ортақ. Қазақстан да осындай табысты тәжірибелерді қабылдай отырып, өз құқықтық тетіктерін үнемі жаңартып отыруы қажет екені сөзсіз [22]. Отандық және шетелдік құқықтық әдебиетке сындарлы талдау. Кәмелетке толмағандардың құқықтық мәртебесі және олардың цифрлық кеңістіктегі құқықтары тақырыбы отандық және шетелдік ғалымдар назарында өрістеп келе жатқан сала. Қазақстандық ғалымдар бұл мәселені

негізінен кәмелетке толмағандардың қылмыстық жауапкершілігі, олардың құқықтарын қорғаудың ұлттық механизмдері тұрғысынан зерттеп келген.

Мәселен, Г. Қонақбаеваның еңбектерінде кәмелетке толмағандардың құқықтық мәртебесі кешенді түрде қарастырылып, бала - мемлекет таныған және кепілдік берген құқық-субъектілікке ие тұлға деп анықтама беріледі. Автор 2010 жылғы зерттеуінде бүгінгі таңда Қазақстандағы мемлекеттік саясатта бала құқықтарын қорғау басымдығын атай отырып, құқықтық мәртебені жетілдіру бойынша ұсыныстар жасаған [19, с. 23].

А.Ш. Маликованың 2009 жылғы ғылыми мақаласы да осы тақырыпта болып, онда баланың әлеуметтік және құқықтық статусы қоғамдағы қатынастар жүйесінде талданған екен. Маликованың пайымдауынша, жасөспірімдердің құқығы тек қағаз жүзінде қалмай, іс жүзінде қамтамасыз етілуі үшін мемлекет тек репрессивтік шараларға емес, әлеуметтік алдын алу жұмыстарына да мән беруі тиіс (ғалымның бұл тұжырымдары қазіргі көзқарастармен астасып жатыр).

Жасөспірімдердің құқықтарын қорғаудың ұлттық тетіктері туралы қазақстандық тағы бір зерттеу - Г.Т. Сүлейменова және т.б. авторлардың еңбектерінде - баланың конституциялық-құқықтық мәртебесі жан-жақты зерделенген. Олар баланың негізгі жеке құқықтары (өмір сүру құқығы, аты-жөн алу, отбасы тәрбиесінде болу құқығы, білім алу құқығы, т.б.) мен арнайы құқықтары (қорғауға мұқтаждыққа байланысты құқықтары) ара жігін анықтап көрсетеді. Бұл жұмыстарда Қазақстан заңнамасындағы олқылықтар да сындарлы талданады: мысалы, бала еңбегін пайдалану проблемалары, қараусыз қалған балалардың жағдайы, бала құқықтарын қорғау жүйесіндегі ведомстволардың бытыраңқылығы. Бұл кемшіліктерді жою жолында авторлар халықаралық тәжірибеге жүгінуді ұсынады.

Шетелдік құқықтық әдебиетке келсек, соңғы жылдары «бала және цифрлық құқықтар» мәселесіне арналған зерттеулер қатары өсуде. Батыс елдерінде балалардың интернеттегі құқығын дербес тақырып ретінде көтерген ғалымдар (мысалы, британдық зерттеуші Соня Ливингстон және т.б.) баланың онлайн әлемдегі құқықтарын орындау ерекшеліктерін, цифрлық азаматтық ұғымын алға тартуда. Соның ішінде, БҰҰ Балалар қоры (ЮНИСЕФ) 2017 жылы жариялаған «Балалар әлемінің жағдайы: балалар цифрлық әлемде» атты баяндамасы бар [26]. Бұл баяндамада цифрлық технологиялардың балалар өміріне әсері жан-жақты қарастырылып, балаларды интернеттегі зорлықтан қорғау, цифрлық теңсіздік, онлайн білім алу мүмкіндіктері сияқты аспектілер қозғалған. Ал құқықтық бағытта, 2021 жылы қабылданған БҰҰ Бала құқықтары комитетінің №25 Жалпы түсіндірме ережесі - аса маңызды құжат. Онда цифрлық ортада бала құқықтарын қамтамасыз ету бойынша мемлекеттердің міндеттемелері тізбектеліп, баланың интернетке қолжетімділік құқығынан бастап, онлайн ортадағы жеке өмірін қорғау, дербес деректерінің құпиялылығы, зиянды ақпараттан қорғану, цифрлық сауаттылық алу құқықтарына дейін атап көрсетілген. Бұл жалпы ережеде: «Балалардың құқықтары онлайн және офлайн кеңістіктерде бірдей қорғалады, цифрлық ортада бала құқығын шектейтін немесе бұзатын кез

келген шара баланың мүддесіне сай болуы және қажеттілікке қарай ғана жүзеге асуы тиіс» делінгені белгілі. Яғни, халықаралық құқық балаға цифрлық кеңістікте ересектермен тең дәрежеде құқық иесі ретінде қарауды талап етеді.

Ресейлік құқықтану ғылымында да соңғы кезде «баланың ақпараттық құқықтары», «цифрлық заманның бала құқықтары» тақырыбында еңбектер жазылуда. Мысалы, Н.М. Хромованың 2024 жылғы зерттеуі «Цифрлық ортадағы кәмелетке толмағандар құқықтарын қорғаудың құқықтық механизмдері» деп аталады. Бұл еңбекте автор Ресей Федерациясында балаларды интернеттегі зиянды контенттен қорғау заңнамасын талдап, қолданыстағы тетіктердің олқылығы бар екенін көрсетеді. Хромованың айтуынша, интернетте балаларға қарсы жасалатын құқық бұзушылықтардың көбеюі (оларды қылмысқа азғыру, сексуалдық сипаттағы қылмыстарға тарту, виктимизация) заңнаманы жетілдіру қажеттігін туындатады.

Автор ақпараттық қауіпсіздік саласындағы ұлттық заң нормаларын талдай келе, балаларды қорғау механизмдерін одан әрі дамыту керектігі жөнінде қорытынды жасайды [20]. Шетелдік әдебиетте бұдан өзге, балалардың цифрлық құқықтарына қатысты философиялық-әлеуметтік қырынан талдаулар да бар. Кейбір авторлар «баланың интернетте сөз айту еркіндігіне шек қоймау керек, цензурадан гөрі білім беру арқылы қауіптің алдын алу керек» деген позиция ұстанса, енді бір сарапшылар «үлкендерге арналған контенттен балаларды тосып ұстау үшін қатаң техникалық сүзгілер қажет» деп есептейді. Бұл пікір алуандық ғылыми дискурсқа тән және дәл осындай сындарлы таластар бала құқықтарын қорғау саласының дамуына ықпал етеді. Қорытынды және автордың балама тұжырымдары. Жоғарыда талданған мәселелерді қорытындылай келе, кәмелетке толмағандардың құқықтық мәртебесі қоғам дамуына қарай үнемі өзгеріп, толықтырылып отыратын динамикалық құбылыс екенін көреміз. Бүгінгі тарихи кезең - цифрлық дәуір - бала мәртебесінің мазмұнын бұрынғыдан да күрделендіріп, құқықтық реттеудің жаңа тәсілдерін талап етуде. Автордың пікірінше, баланың құқықтық жағдайын нығайту бағытындағы мемлекеттік саясат кешенді және проактивті болуы керек. Бір жағынан, қолданыстағы заңнаманы заман талабына сай бейімдеу қажет: цифрлық технологиялар енгізген жаңа қатынастарды (баланың интернеттегі құқығы, дербес ақпараттың қорғалуы, киберқылмыс пен буллингтен қорғану) құқықтық реттеудің айқын тетіктерін жасау - кезек күттірмейтін міндет. Бұл тұрғыда, мысалы, «Балалардың цифрлық құқықтары туралы» арнайы заң қабылдау немесе қолданыстағы заңдарға ауқымды өзгерістер енгізу ұсынылуы мүмкін. Екінші жағынан, бала құқықтарын қамтамасыз ету тек заң жазумен шектелмейтіні айқын.

Сондықтан балама тұрғыдан қарағанда, тәрбиелеу, білім беру және қоғамды жұмылдыру құралдарына басымдық беру де өте маңызды. Цифрлық заманда әрбір бала ақпарат тасқынында өзін қорғай алатындай тәрбиеленуі тиіс – бұл үшін мектеп бағдарламасына медиақұқық пен цифрлық сауат негіздерін енгізуді қарастыруға болады. Ата-аналарды да жаңа сын-қатерлерге дайын ету керек, демек ата-ана университеттері, тренингтері

арқылы оларды оқыту қолға алынуы қажет. Автор сондай-ақ балама бір ұсыныс ретінде мемлекет, бизнес және азаматтық қоғам арасында әлеуметтік әріптестік механизмдерін күшейтуін атап өтеді. Мысалы, ірі технологиялық компаниялар (Facebook, TikTok, YouTube сияқты) балалардың құқықтарын сақтау жауапкершілігін ерікті түрде бөлісуі керек - әлемдік үздік тәжірибеге сүйеніп, «Балаларға қолайлы контент» стандарттарын енгізсін, зиянды материалдарды жылдам өшіруге келіссін. Бұл үшін мемлекет сол компаниялармен байланыс орнатудың жаңа форматтарын ойластырып, келіссөздер жүргізуі тиіс. Дәл қазірдің өзінде Қазақстан Парламенті шетелдік онлайн-платформаларға қатысты заңды қатайтты (өкілдік ашуды талап ету, құқыққа қайшы контентті өшіруді міндеттеу), алайда бұлар көбіне жазалаушы сипатта көрінеді. Альтернативті түрде, ынталандырушы, бірлесіп жұмыс істеуге жұмылдыратын шаралар да қарастырылғаны жөн болар еді.

Тағы бір балама тұжырым: баланың өзі құқықтық саясаттың пассивті объектісі болып қалмауы керек, оны да тыңдау қажет. Балалар мен жасөспірімдердің өздерінің құқықтық мәселелерге қатысты көзқарастары ескерілсе, көптеген проблеманың шешімі тиімді болмақ. Бұл – Бала құқықтары туралы конвенцияның да талабы (баланың пікірін құрметтеу құқығы). Сондықтан елімізде бала құқықтары жөніндегі уәкіл қызметінің жұмысын күшейтіп, әр мектепте оқушылардың құқығын қорғау жөніндегі кеңестер құру практикасын дамыту ұсынылады. Сол кеңестерде балалар өз ортаындағы қайшылықтар мен қауіптерді талқылап, үлкендерге сигнал беріп отырса, алдын алу шаралары дер кезінде іске асар еді.

Қорыта айтқанда, кәмелетке толмағандардың құқықтық мәртебесі - тарихи дамуда жетілген, кешенді ұғым. Оның дәстүрлі қырлары (отбасылық, еңбек, қылмыстық-қаржылық мәртебесі) қазіргі заманға сай қайта қаралуда, ал жаңадан туындаған цифрлық өлшемде бала мәртебесі мүлде жаңа сынақтарға душар. Автор осы зерттеу негізінде келесідей түйіндейді: біріншіден, балалардың құқықтары мемлекет қорғауындағы ерекше басымдық ретінде танылуы тиіс, екіншіден, цифрлық кеңістікте бала қауіпсіз әрі еркін дамитын жағдай жасау - барлық мүдделі тараптардың (мемлекет, ата-ана, қоғам, бизнес) ортақ міндеті, үшіншіден, әрбір құқықтық новелла баланың шынайы мүддесі мен әл-ауқатына негізделуі шарт. Тек осындай жан-жақты әрі баланың өзін тұлға ретінде құрметтейтін көзқарас орныққанда ғана «бала - ең алдымен, құқық иесі, оның құқықтары шексіз сақталуы керек» деген ұстаным өмірде өз орнын табады деп санаймыз. Бұл балама тұжырым біздің зерттеуіміздің түйіні әрі алдағы құқықтық реформаларға бағыт-бағдар болуға лайық қағида деп ойлаймыз.

### 1.2 Кибер құқық бұзушылықтардың жалпы түсінігі мен жіктелуі

Казіргі заманда ақпараттық-коммуникациялық технологиялардың қарқынды дамуы құқық бұзушылықтардың жаңа түрі – Кибер құқық бұзушылықтарды пайда қылды. Интернет пен компьютерлік жүйелер арқылы жасалатын заңға қарсы әрекеттер қоғамға елеулі қауіп төндіруде, сондықтан

оларды зерттеп, түсіну өзекті мәселеге айналды. Киберқылмыстардың трансшекаралық сипаты олармен күресуде халықаралық ынтымақтастықты талап етеді. Сонымен бірге, цифрлық буынның өсіп жетілуімен кәмелетке толмағандардың да кибер құқық бұзушылықтарға қатысуы алаңдаушылық туғызуда. Осы бөлімде кибер құқық бұзушылық ұғымының әртүрлі анықтамалары, тарихи қалыптасуы мен құқықтық доктринадағы орны талданып, олардың түрлері мен жіктелу өлшемдері қарастырылады. Сондай-ақ кәмелетке толмағандар қатысатын киберқылмыстық іс-әрекеттер жеке бөлікте сипатталып, бөлім соңында авторлық тұжырымдар мен балама жіктеу ұсынылады.

Кибер құқық бұзушылық ұғымы және оның дамуы. «Кибер құқық бұзушылық» (кейде «киберқылмыс» деп те аталады) термині кең мағынада компьютерлер мен ғаламторды пайдалану арқылы жасалатын кез келген құқыққа қайшы әрекеттерді білдіреді. Ғылыми әдебиетте бұл ұғымның бірыңғай қабылданған анықтамасы жоқ, әртүрлі авторлар өз тұрғысынан түсіндіреді. Мысалы, зерттеушілер Томас пен Лоудер киберқылмысты «ғаламдық электрондық желілер арқылы жүзеге асырылатын, заңсыз немесе кейбір тараптар заңға қайшы деп санайтын компьютерлік іс-әрекеттер» деп анықтайды. Ал Гордон мен Фордтың пікірінше, «компьютерді, желіні немесе тиісті құрылғыны қолдану арқылы жасалатын немесе сол арқылы жеңілдетілетін кез келген қылмыс» киберқылмыс болып саналады. Көріп отырғанымыздай, бір авторлар Кибер құқық бұзушылықты өте кең аяда (барлық компьютерлік инциденттерді қосып) түсіндірсе, енді біреулері оны нақты технологиялық аспектісі бар қылмыстар ретінде шектейді. Кейбір анықтамалар тым жалпы болғанымен, олардың негізі - қылмыстық әрекеттердің ерекше цифрлық ортада орын алатындығы туралы тұжырым - дұрыс бағыт береді [27].

Кибер құқық бұзушылық ұғымының қалыптасуы ақпараттық технологиялардың даму тарихымен тікелей байланысты. Алғашқы компьютерлік қылмыстар өткен ғасырдың 1960-70-жылдарынан бастап тіркеле бастаған (мысалы, банк мәліметтерін заңсыз көшіру, телефон желілерін «phreaking» арқылы алдау т.б.). 1980-жылдары бірқатар елдер (АҚШ, Германия, Жапония және т.б.) компьютерлік ақпаратты қорғайтын арнайы заңнамалық нормаларды қабылдады. 1986 жылы АҚШ-та Computer Fraud and Abuse Act қабылданып, компьютерлік жүйелерге рұқсатсыз кіру, ақпаратты жою сияқты әрекеттер қылмыс деп танылды. Еуропада 1989 жылы Ұлыбритания Computer Misuse Act заңын енгізді. Осылайша, бастапқыда ұлттық деңгейде «компьютерлік қылмыс» ұғымы қалыптасып, құқықтық база жасалды. Интернеттің кең таралуы жаңа сын-тегеуріндер туындатты.

1990-жылдардың аяғы мен 2000-жылдардың басында трансұлттық сипаттағы алғашқы хакерлік шабуылдар, вирустар және онлайн алаяқтық оқиғалары жиіледі. Бұл кезеңде «киберқылмыс» термині қолданысқа еніп, мазмұны кеңейе түсті. 2001 жылы Еуропа Кеңесі қол қойған Будапешт конвенциясы (ресми атауы - «Киберқылмыс туралы конвенция») осы саладағы алғашқы халықаралық шарт болды. Конвенция киберқылмыстарға

қатысты ұлттық заңнамаларды үйлестіруді, тергеу әдістерін жетілдіруді және мемлекеттер арасында өзара құқықтық көмекті дамытуды мақсат етті. Онда кибер құқық бұзушылықтардың негізгі құрамы мен түрлері белгіленіп, оларды ашу мен тергеудің процедуралық құралдары көрсетілді. 2004 жылы күшіне енген бұл Конвенцияға қазіргі таңда 78 мемлекет тарап болып отыр (оның ішінде АҚШ, Жапония секілді Еуропа Кеңесіне мүше емес елдер де бар) [28].

Будапешт конвенциясы киберқылмысқа қарсы күрестегі негізгі халықаралық стандартқа айналды. Қазақстан Республикасы аталған конвенцияға әлі қосылған жоқ, дегенмен 2023 жылғы 19 сәуірде Қазақстанды Конвенцияға қосылуға ресми шақыру жөніндегі шешім қабылданды [29]. Бұл шақыру алдағы бес жылда күшінде болады; сол мерзімде Қазақстан қосылу рәсімдерін аяқтаса, киберқылмыспен күресте жаһандық ынтымақтастық тетіктеріне толыққанды қатыса алмақ.

Кибер құқық бұзушылықтардың Қазақстан құқықтық доктринасындағы орны мен эволюциясына келсек, еліміздің қылмыстық заңнамасы заман талабына сай біртіндеп жетілдірілуде. Қазақстанның 1997 жылғы Қылмыстық кодексінде компьютерлік қылмыстар үшін жауапкершілік небәрі бір баппен (227-бап – «ЭЕМ үшін зиянды бағдарламаларды жасау және тарату, ЭЕМ ақпаратына заңсыз қол жеткізу») қамтылған еді. Ол бап жалпы «Экономикалық қызмет саласындағы қылмыстар» тарауына енгізілген болатын. Уақыт өте келе ақпараттық қауіпсіздікке төнетін қатерлер ұлғайып, заңнаманы жаңарту қажеттігі туды. 2014 жылы жаңа Қылмыстық кодекс қабылданып, онда «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» атты 7.1-бөлім енгізілді.

Бұл бөлімде ақпараттық технологиялар қауіпсіздігіне қарсы қылмыстардың 9 құрамы жеке көрсетілді (205-213-баптар). Атап айтқанда, 205-бап – «Ақпаратқа, ақпараттық жүйеге немесе телекоммуникация желісіне заңсыз қол жеткізу», 206-бап – «Ақпаратты заңсыз жою немесе модификациялау», 207-бап – «Ақпараттық жүйенің немесе телекоммуникациялар желісінің жұмысын бұзу», 208-бап – «Ақпаратты заңсыз иемдену», 209-бап – «Ақпарат беруге мәжбүрлеу», 210-бап – «Зиянды компьютерлік бағдарламаларды жасау, пайдалану және тарату», 211-бап – «Шектеулі қолжетімді электрондық ақпараттық ресурстарды заңсыз тарату», 212-бап – «Құқыққа қарсы мақсаттағы интернет-ресурстар үшін қызмет көрсету», 213-бап – «Ұялы байланыс абоненттік құрылғысының сәйкестендіру кодын заңсыз өзгерту және сол үшін бағдарламаларды жасау». Осылайша, жаңа Кодекс киберқауіпсіздікке қол сұғатын әрекеттерді қылмыс деп нақтылап, олармен күресудің заңдық негізін күшейтті. Сонымен бірге, 2014 жылғы реформа аясында ҚК-тің өзге тарауларында да ақпараттық-коммуникациялық технологияларды пайдаланып жасалған қылмыстарға арналған 15-тей жаңа саралау белгілері пайда болды. Мәселен, жала жабу (130-бап) немесе қорлау (131-бап) әрекеттері егер жария түрде, оның ішінде интернетті қолдану арқылы жасалса, ауырлататын мән-жай ретінде қарастырылатыны заңда бекітілді. Дербес өмірге қол сұғу, байланыс

құпиясын бұзу секілді кейбір қылмыстар үшін де ақпараттық технологияны пайдалану жауапкершілікті ауырлататын құрам ретінде енгізілді [30]. Бұл өзгерістер Қазақстанның кибер құқық бұзушылықтарға қарсы заңнамасы халықаралық үрдістерге сай дамып келе жатқанын көрсетеді.

Айта кету керек, Қазақстан киберқылмысқа қарсы ұлттық жүйесін жетілдіру бағытында басқа да қадамдар жасауда. 2020-жылдары ішкі істер органдары құрылымында киберқылмыспен күрес бөлімшелері күшейтілді.

Мәселен, 2022 жылы ІІМ-де киберқылмыспен күрес орталығы құрылып, 2024 жылдың қарашасында ол дербес киберқылмысқа қарсы іс-қимыл департаменті деңгейіне көтерілді. Жаңа департаменттің міндеті - киберқылмыстарды анықтау, тергеу және олардың алдын алу бойынша стратегиялық шаралар әзірлеу [31]. Бұл – Қазақстанның цифрлық дәуір қылмыстарына қарсы институционалдық дайындығын күшейтуге бағытталған маңызды қадамы. Жоғарыда айтылғандарды қорыта келе, кибер құқық бұзушылық - бұл компьютерлік желілер мен ақпараттық жүйелерді пайдалану арқылы жасалатын, қоғамдық қатынастарға қауіп төндіретін құқыққа қайшы әрекеттердің жиынтығы. Бұл ұғым уақыт өте келе компьютерлік қылмыстардан бастап интернет дәуіріндегі сан алуан заңсыз әрекеттерді қамтитын кең ұғымға айналды. Оның мазмұнын ашу үшін келесі бөлімде Кибер құқық бұзушылықтардың түрлері және жіктелу өлшемдері талданады.

*Кибер құқық бұзушылықтарды жіктеу түрлері.* Кибер құқық бұзушылықтардың жіктелуі - ғылыми және практикалық тұрғыдан маңызды мәселе. Қылмыстың бұл санатын түрлі өлшемдер бойынша бөлудің мақсаты - олардың табиғатын тереңірек түсіну, әр түріне тән ерекшеліктерді анықтау және соған сәйкес қарсы күрес тәсілдерін әзірлеу. Халықаралық құжаттар мен зерттеулерде киберқылмыстарды топтастырудың бірнеше тәсілі қалыптасқан. Төменде солардың негізгілері мен Қазақстандық доктрина ұстанымдары қарастырылады.

Халықаралық құжаттардағы типологиялар. 2001 жылғы Будапешт конвенциясы киберқылмыстарды мазмұны жағынан бірнеше санатқа бөліп қарастырады. Конвенция талаптарына сай әрбір қатысушы мемлекет қылмыстық заңнамасында төмендегі іс-әрекеттерді қылмыс деп танытуы тиіс: заңсыз қол жеткізу (компьютер немесе желіге рұқсатсыз ену), заңсыз тосып алу (желідегі деректерді рұқсатсыз ұстап алу), мәліметтерге заңсыз қол сұғу (ақпаратты жою, бұзу, өзгерту), жүйенің жұмысына заңсыз кедергі келтіру, арнайы құрылғыларды заңсыз пайдалану (мысалы, хакерлік бағдарламаларды жасау және тарату), компьютерлік жалғандық (компьютерді пайдаланып жасанды құжаттар жасау), компьютерлік алаяқтық, балалар порнографиясына қатысты құқық бұзушылықтар және авторлық және сабақтас құқықтарды бұзу. Осылайша, Конвенция киберқылмыстың «жүйеге қол сұғу», «ЭЕМ-ды құрал етіп пайдалану» және «заңсыз мазмұн тарату» сияқты негізгі түрлерін қамтыды. 2003 жылы қабылданған Конвенцияның қосымша хаттамасы арқылы тағы бір санат – нәсілшілдік немесе ксенофобиялық сипаттағы онлайн әрекеттер – қылмыс ретінде қосылды.

Бүгінде бұл жіктеу жаһандық деңгейде кеңінен танылып, көптеген елдердің заңнамасына ықпал етті. Мысалы, Еуропа Одағының 2013/40/EU Директивасы ақпараттық жүйелерге шабуыл жасауды қылмыс деп анықтап, негізінен Будапешт конвенциясының 1-санаттағы (жүйенің қауіпсіздігіне қарсы) қылмыстарына сәйкес құрамдарды бекітті [28].

Ғалымдар мен сарапшылар киберқылмыстарды технологияның рөлі, ниет мақсаты, қылмыстық қол сұғушылық объектісі, қылмыскердің сипаты сияқты түрлі критерийлер бойынша жіктеп келеді. Солардың бірі - қылмыстарды технологияға тәуелділігіне қарай бөлу. Бұл тәсіл бойынша барлық киберқылмыстардың екі үлкен тобы айқындалады: кибертәуелді қылмыстар және киберқолдаулы қылмыстар. Кибертәуелді (немесе «компьютер-фокусталған») қылмыстар - тек ақпараттық технологиялар пайда болғаннан кейін ғана өмірге келген, цифрлық әлемге тән жаңа қылмыстар.

Оларға хакерлік шабуыл, зиянды бағдарлама жасау, DoS/DDoS арқылы жүйелерді істен шығару, желілерді бұзып деректерді ұрлау сияқты әрекеттер жатады. Мұндай қылмыстарды дәстүрлі офлайн әдістермен жүзеге асыру мүмкін емес, олар толығымен цифрлық ортаға тәуелді. Ал киберқолдаулы (яғни «компьютерді пайдаланып жасалатын») қылмыстар - бұрыннан бар дәстүрлі құқық бұзушылықтардың ақпараттық-коммуникациялық технологиялар көмегімен жүзеге асырылатын түрлері. Бұған интернет-алаяқтық, онлайн қаржы ұрлығы, интернет арқылы есірткі сату, электрондық қарақшылық (піраттық), жалған ақпарат тарату, кибертерроризм, т.б. көптеген әрекеттер кіреді. Яғни технология бұл жерде қылмыс құралы рөлін атқарады, бірақ қылмыстың түпкі мәні дәстүрлі (пайдакүнемдік, зорлық-зомбылық немесе экстремизм сипатты) болуы мүмкін. Бүгінгі күні «кибертәуелді vs киберқолдаулы» дихотомиясы - ең кең тараған және саясаткерлер мен криминологтар тарапынан жиі қолданылатын жіктеу үлгісі [28].

Кейбір зерттеушілер жоғарыдағы дихотомияны одан әрі нақтылау мақсатында үш санатты жіктеулер ұсынған. Мысалы, Сара және әріптестері киберқылмыстарды үш типке бөледі: I тип - «таза техникалық» (мысалы, желілерді бұзу, зиянды кодты пайдалану арқылы жасалатын қылмыстар), II тип - «әлеуметтік өзара әрекетке негізделген» (мысалы, кибербуллинг, онлайн қорқытып-шаңдату, яғни адамға психологиялық әсер ету арқылы жасалатын қылмыстар) және III тип - «жасанды интеллект пен өздігінен оқитын алгоритмдер көмегімен жасалатын» қылмыстар. Бұл жерде III тип қазіргі заманғы озық технологияларды (жасанды интеллект, боттар) пайдаланып жасалатын жаңа қауіп түрлерін сипаттайды. Үшсанатты үлгілер әлі қалыптасу үстінде болғанымен, олар болашақта киберқылмыс эволюциясына бейімделген классификация жасау үшін пайдалы болуы мүмкін [28].

Кибер қылмыстарды қоғамға зияндылығы (қылмыстық мақсат-мүддесі) бойынша да жіктеуге болады. Зерттеушілердің бір бөлігі Кибер құқық бұзушылықтарды «адамға қарсы қылмыстар» және «мүлікке қарсы қылмыстар» деп бөлуді ұсынады. Мысалы, Клаппер және др. авторлар екі факторлы классификацияның өлшемі ретінде қылмыскердің түпкі мотивін алады: егер мақсат жеке тұлғаға залал келтіру не қорлау болса - оны

интерперсоналдық киберқылмыс, ал мақсат заңсыз пайда табу не мүліктік зиян келтіру болса - мүліктік (пайдакүнемдік) киберқылмыс деп жіктейді [28]. Бір қарағанда бұл тәсіл киберқолдаулы қылмыстарды әрі қарай ішкі түрлерге ажыратуға мүмкіндік береді. Расында да, киберқылмыстардың бір бөлігі (вирустарды тарату, жүйелерді бұзу) негізінен бұзақылық ниеттен немесе қызығушылықтан туындайды (зардап шегетін техникалық жүйелер, ұйымдар болса да, тікелей адамға қарсы бағытталмаған), ал екінші бір бөлігі тікелей кінәлі мақсатпен жасалады - бірі материалдық пайда (ақша ұрлау, алаяқтық), енді бірі жеке басқа зиян келтіру (мысалы, белгілі бір адамды қорлау, бопсалау) ниетімен жүзеге асады. Дегенмен, бұл жіктеудің шартты екендігін ескеру қажет, өйткені көптеген киберқылмыстар аралас сипатта болады (кейбір хакерлік шабуылдар бір мезгілде әрі бұзақылық, әрі пайдакүнемдік мақсатты ұстануы мүмкін).

Қылмыстық қол сұғушылық объектісі критерийі бойынша да киберқылмыстарды бөлудің әдістемелік маңызы зор. Ресейлік ғалымдар компьютерлік қылмыстардың объектісі тұрғысынан екі топқа бөлінетінін көрсетеді: біріншісі - компьютерлік ақпараттың қауіпсіздігіне қарсы қылмыстар, яғни қылмыстық қол сұғушылықтың тікелей нысаны ақпараттың өзі болып табылатын әрекеттер; екіншісі - компьютерді немесе ақпараттық технологияны қылмыс құралы ретінде пайдалану арқылы жасалатын өзге қылмыстар. Бірінші топқа ақпаратқа рұқсатсыз қол жеткізу, оны заңсыз өзгертупозициялау, жою, компьютерлік бағдарламаларды бұзу сияқты қылмыстар кіреді - бұлардың барлығында заңмен қорғалатын ЭЕМ-ақпарат негізгі объект саналады. Мысалы, Қазақстан ҚК 205, 206-баптарындағы әрекеттер тікелей ақпараттық қауіпсіздікті бұзу ретінде көзделген. Ал екінші топқа - компьютерді құрал етіп қолдану арқылы өзге классикалық объектілерге қарсы жасалатын қылмыстар жатады. Бұлар Қылмыстық кодекстің түрлі тарауларында орналасқан: мысалы, компьютерді пайдаланып ұрлық жасау, алаяқтық жасау, қорқытып алу немесе әділеттілікке қарсы қылмыстар (жалған дәлелдемелер жасау үшін деректерді бұрмалау, т.б.).

Мұндай жағдайларда қылмыстың тікелей объектісі - мүліктік қарым-қатынастар немесе қоғамдық тәртіп бола тұра, қылмыскер оның құралын ақпараттық технологиялар деп таңдаған. Қазақстан заңнамасында, өкінішке қарай, екінші топтағы әрекеттерді арнайы атап көрсететін нормалар аз; көбіне ондай істер жалпы қылмыс құрамдары бойынша сараланып, егер қажет болса «ақпараттық желілерді пайдалану» ауырлататын белгі ретінде ескеріледі [32, с. 105]. Мысалы, жоғарыда айтылғандай, ҚК 190-бабы («Алаяқтық») 2-бөлігінің 4-тармағында алаяқтық егер телекоммуникация желілерін пайдалану арқылы жасалса, жауаптылық күшейетіндігі көрсетілген.

Дегенмен, бұл тәсіл - компьютерді пайдалану арқылы жасалған барлық қылмыстарды бір жинақтауға мүмкіндік бермейді, өйткені олар ҚК-де түрлі тарауларға шашырап орналасқан. Қалай болғанда да, қылмыстың заты мен тікелей объектісіне қарай бөлу - кибер құқық бұзушылықтардың құқықтық саралауын дұрыс жүргізуге септігін тигізеді. Әдіс және құрал түріне қарай жіктеу де қызықты нәтижелер береді. Қылмысты жасау тәсілдері тұрғысынан,

киберқылмыстар өте көп қырлы болғанымен, зерттеушілер олардың типтік түрлерін жүйелеуге ұмтылуда. Мысалы, 2000 жылы АҚШ ғалымдары 52 елдің заңнамасына талдау жасап, он түрдегі киберқылмысты төрт категорияға топтастырған. Олар: 1) ақпаратқа байланысты қылмыстар - ақпаратты ұрлау, заңсыз ұстап алу, бұзу немесе өзгерту; 2) компьютерлік желілерге қарсы қылмыстар - желілердің жұмысын бұзу, саботаж жасау; 3) рұқсатсыз қол жеткізуге қатысты қылмыстар - хакинг (бұзып кіру) және вирустарды тарату; 4) компьютерлерді пайдалану арқылы жасалатын өзге қылмыстар-қылмысқа көмек көрсету, компьютерлік алаяқтық, компьютерлік жалғандық сияқты әрекеттер [32, с. 105]. Тағы бір мысал, белгілі ресейлік ғалым Ю.М. Батурин компьютерлік қылмыстардың бес негізгі тобын атап көрсеткен: 1) компьютерлік техникалық құрылғыларды ұрлау; 2) компьютерлік ақпаратты көшіру және перенаправление жасау (бағытын өзгерту); 3) компьютерлік жүйелерге заңсыз қол жеткізу; 4) ақпараттық және басқарушы командаларды заңсыз манипуляциялау (мысалы, ақпаратты дезинформациялау, бұрмалау); 5) күрделі комбинирленген тәсілдермен жасалатын қылмыстық әрекеттер [32, с. 106]. Бұл топтастыру қылмыскердің пайдаланатын техникасы мен қитұрқы әдіс-айлаларын негізге алады.

Қазақстандық мамандар да киберқылмыстардың жасалу әдістері бойынша тізбесін кеңейтіп көрсетуде. Қазақстан Республикасының 2006 жылғы Ақпараттық қауіпсіздік тұжырымдамасында цифрлық саладағы заңсыз әрекеттердің 20-дан астам әдіс-тәсілі аталған [32, с. 106]. Олардың ішінде: рұқсатсыз ақпарат жинау, құпия мәліметтерді заңсыз көшіру, ақпараттық ресурстарды жою немесе түрлендіру, заңсыз жолмен ақпаратты иемдену, алдау арқылы мәлімет алу, бағдарламалық вирустар жасау және тарату, ақпаратты өңдеу технологиясына қасақана нұқсан келтіру, телекоммуникация желілеріне заңсыз қосылу, шифрлау (криптография) құралдарын қылмыстық мақсатта қолдану, электрондық бұғаттау (блокировка) арқылы ақша бопсалау және т.б. бар [32, с. 107]. Әрине, технология дамыған сайын қылмыстық қолсұғушылықтың жаңа әдістері шығуы мүмкін, сондықтан бұл тізім уақыт өте толықтырылып отырады.

Жалпы, кибер құқық бұзушылықтарды бір ғана өлшемге сүйеніп қатаң бөлуден гөрі, кешенді көпөлшемді жіктеу дұрыс болады деген пікірлер бар. Өйткені бір киберқылмыс әр қырынан түрлі топқа жатуы ықтимал. Мысалы, интернет арқылы жала жабу әрекеті технологияның рөлі жағынан киберқолдаулы (дәстүрлі қорлау қылмысының желіде жасалған түрі), ниет сипаты жағынан адамға қарсы (жеке басын қаралау мақсаты), ал әдісі бойынша әлеуметтік инженерия құралдарын пайдалануды қамтуы мүмкін.

Сондықтан құқық қорғау тәжірибесінде де, ғылыми талдауда да «киберқылмыс» ұғымын мүмкіндігінше тармақтап, оның ішкі құрылымын айқындау талпыныстары жалғасуда. Ал кибер құқық бұзушылықтардың ерекше бір санаты ретінде кәмелетке толмағандардың қатысуымен жасалатын құқық бұзушылықтар жеке қарастыруды қажет етеді.

*Кәмелетке толмағандардың кибер құқық бұзушылықтарға қатысуы.* Жасөспірімдер арасындағы құқық бұзушылық - қашанда криминологияның

өзекті тақырыбы. Қазіргі цифрлық дәуірде кәмелетке толмағандар тек дәстүрлі бұзақылық пен қылмысқа ғана емес, сонымен бірге сандық кеңістіктегі құқыққа қайшы әрекеттерге де тартылып отыр. Киберқылмыс және жасөспірімдер мәселесі екі қырынан маңызды: біріншіден, балалар мен жастар киберортадағы қылмыстардың құрбаны болуда (алаяқтардың алдауына түсу, онлайн зорлық-зомбылыққа ұшырау, кибербуллингтің нысанына айналу т.б.), екіншіден - кей жағдайларда қылмыс субъектісі ролінде, яғни өзі құқық бұзушы ретінде көрінуде. Диссертациялық зерттеу тақырыбы тұрғысынан, бізді әсіресе екінші қыры - кәмелетке толмағандардың кибер құқық бұзушылық жасауы қызықтырады.

Жасөспірімдердің киберқылмыс жасауына әсер ететін факторлар сан алуан. Ең алдымен, жаңа буынның технологияны жетік меңгеруі - оларды еріксіз «тәуекел тобына» қосады. Сарапшылардың байқауынша, қазіргі балалар мен жасөспірімдер ересектерге қарағанда компьютер мен интернетті ертерек және еркін игереді, сол себепті киберкеңістіктегі кейбір заңсыз әрекеттер оларға қызық ойын секілді көрінуі мүмкін. Киберортада жасалатын бұзақылық пен заңсыз істердің бір бөлігі осы тәжірибесіздік пен қызығушылықтан туындайтыны анық. Мысалы, Нью-Йорк қаласында жүргізілген сауалнамаға сәйкес, мектеп оқушыларының 16%-ы (яғни әрбір алтыншы жасөспірім) кемінде бір рет хакерлікпен айналысып көргенін мойындаған. Алайда солардың небәрі 15%-ы ғана қолға түскен не таныстарының ұсталғанын білетін болып шықты. Бұл дерек көп жасөспірімдердің «қызық үшін хакерлік жасау» әрекеттері сыртынан байқалмай қала беретініне меңзейді. Зерттеу сондай-ақ «жас хакерлердің» тек 7%-ы ғана мұны қаржы табу үшін істесе, 6%-ы оны болашақта ақша жасауға болатын кәсіп деп қарайтынын көрсетті [33]. Демек, кәмелетке толмағандардың кибер құқық бұзушылықтарының айтарлықтай бөлігінде пайдакүнемдік мақсат болмауы, көбіне эгоцентрлік мотивтер (өзін көрсету, басқалардан üstündігін дәлелдеу, шытырманды ұнату) жатуы мүмкін деген тұжырым жасауға болады. Бұл, әрине, барлық жағдайды қамтымайды, бірақ жалпы үрдісті аңғартады.

Халықаралық деңгейде орын алған кейбір оқиғалар да жасөспірімдердің киберқылмыс жасау қаупінің шынайы екенін дәлелдейді. Мәселен, 2021-2022 жылдары әлемге аты шыққан “Lapsus$” хакерлік тобы бірқатар жаһандық корпорациялардың деректеріне заңсыз қол сұғып, миллиондаған доллар шығын келтірген [34]. Кейін белгілі болғандай, бұл топтың негізгі мүшелері 16-19 жас аралығындағы жасөспірімдер екені анықталды. 2023 жылы Ұлыбритания соты “Lapsus$” тобында жетекші рөл атқарған 17 және 18 жастағы екі жасөспірімді киберқылмыстық әрекеттері үшін кінәлі деп тапты [34]. Олардың бірі тіпті кепілмен бостандықта жүріп, жаңа қылмыс жасап (атақты Grand Theft Auto VI ойынының әзірленіп жатқан нұсқасын бұзып кіріп, мәліметтерін жариялаған) көпшілікті таңғалдырған [34]. Бұл мысал «кәмелетке толмаған» жастың киберқылмыс жасауға кедергі бола алмайтынын, тіпті кейде жасөспірімдердің технологиялық икемділігі аса күрделі қылмыстарға ұшыратуы ықтимал екенін көрсетеді. Тарихқа көз

жүгіртсек, киберқылмыс жасаған ең алғашқы белгілі жасөспірімдердің бірі - американдық Джонатан Джеймс. Ол 15 жасында (1999 ж.) АҚШ Қорғаныс министрлігі мен NASA желілеріне заңсыз еніп, құпия деректерді көшіріп алғаны үшін қамауға алынып, АҚШ-та киберқылмысы үшін сотталған тұңғыш жасөспірім атанған. Өкінішке орай, Джеймс кейінірек 24 жасында өз-өзіне қол жұмсаған, бұл оқиға киберқылмысқа тартылған баланың өмірі трагедияға ұласқанын көрсетеді. Мұндай оқиғалар кәмелетке толмағандарды цифрлық құқық бұзушылықтардан алдын ала сақтандырудың қаншалықты маңызды екендігін айғақтайды.

Кей жағдайларда жасөспірімдер өз бетінше қылмыс субъектісі болудан гөрі, ересек қылмыскерлердің қолшоқпарына айналуы мүмкін. Интернеттегі кибералаяқтар балаларды құрал ретінде пайдаланып, қылмыс жасайтын мысалдар Қазақстанда да тіркелуде. Мәселен, полиция деректері соңғы уақытта елімізде алаяқтардың онлайн ойын ойнайтын балаларды алдап, олардың ата-аналарының банк шоттарынан ақша ұрлау оқиғалары жиілегенін көрсетеді. Киберқылмыскерлер балалар қызығатын Roblox секілді ойындарда түрлі бонус, сирек жабдық береміз деп алдап, соның өтемі ретінде ата-анасының телефонына келген SMS-кодты айтуды немесе экранға шыққан QR-кодты сканерлеуді сұрайды. Мұндай әрекеттерге сенген бала ата-анасының интернет-банкинг аккаунтына кіру мүмкіндігін алаяқтарға байқамай ашып береді. Нәтижесінде қылмыскерлер шоттағы қаражатты өзіне аударып алады немесе ата-ана атынан онлайн несие рәсімдейді. Кей жағдайда алаяқтар баланың өз құрылғысына да зиянды қосымшаларды орнатып, оның жеке мәліметтерін қолды қылады. Осындай схема арқылы баланың өзі қылмысқа тікелей қатыспаса да, қылмыстық ниетті жүзеге асырудың құралына айналады. Сарапшылар ересектер интернеттегі алаяқтықтың классикалық түрлерінен сақтана бастаған сайын, қылмыстық топтар балаларды өз ата-аналарына шабуыл жасаудың көмекші буыны ретінде пайдалану «трендке» айналғанын атап өтеді [35]. Бұл - өте қауіпті құбылыс, себебі бала әрі құрбан, әрі қылмыскердің еріксіз сыбайласы ретінде қосарлы зиян шегеді.

Жасөспірімдердің кибер құқық бұзушылықтарға тартылуы құқықтық тұрғыдан да ерекше назарда болуы тиіс. Көптеген елдердің заңнамасы кәмелетке толмағандардың жауаптылығына қатысты ізгілендірілген қағидаларды ұстанады. Қазақстан Республикасында жалпы қылмыстық жауаптылық жасы 16-дан басталады, ал ерекше ауыр санаттағы белгілі бір қылмыстар үшін 14 жастан бастап жауаптылық қарастырылған (ҚК 15-бабы 2-бөлігі) [36]. Алайда ақпараттық технологияларға қатысты қылмыс түрлері бұл тізімге кірмейді. Демек, 14-15 жастағы тұлғалар компьютерлік қылмыс жасаса, оларды қылмыстық жазаға тарту заң тұрғысынан мүмкін емес; мұндай жағдайларда оларға тек тәрбиелік ықпал шаралары немесе әкімшілік жауаптылық қолданылуы ықтимал. Ал 16-17 жастағы құқық бұзушылар қылмыстық жауаптылыққа тартылған күннің өзінде, жасы толмаудың жеңілдететін мән-жайлары ескеріліп, жаза тағайындауда ерекше режім қолданылады. Қазақстанда кәмелетке толмағандарды бас бостандығынан

айыру жазасы өте сирек қолданылады, көбіне шартты тәрбиелік шаралармен, пробациялық бақылаумен шектелінеді. Мысалы, 2022 жылғы ресми статистика бойынша киберқылмыс санатында тіркелген істердің жартысына жуығы (шамамен 40 жағдай) 205-бап - ақпаратқа заңсыз қол жеткізу бойынша қозғалса, сол істердің ішінде кәмелетке толмағандардың үлесі болмашы ғана болған [37]. Бұл бір жағынан, 16 жасқа толмаған құқық бұзушылардың қылмыстық тіркеуге алынбайтынын көрсетсе, екінші жағынан - елімізде киберқылмыс жасаушы жасөспірімдердің әзірге кең таралмағанын білдіреді. Дегенмен, киберкеңістікте өсіп келе жатқан жастардың белсенділігі артқан сайын, олардың арасынан құқық бұзу ықтималдығы да өсетінін жоққа шығаруға болмайды.

Кәмелетке толмағандардың кибер құқық бұзушылықтарының алдын алу үшін арнайы профилактикалық және білім беру шаралары қажет. Оқу орындарында киберқауіпсіздік негіздерін оқыту, балалардың интернеттегі мінез-құлқын бақылауда ұстайтын ата-ана қадағалауын жетілдіру, сондай-ақ «ақылды хакерлерді» ерте анықтап, олардың қабілетін заңды позитивті арнаға бағыттау маңызды. Кейбір мемлекеттерде «этикалық хакинг» бойынша жастарға арналған байқаулар, секциялар ұйымдастырылып, талантты жас хакерлерді киберқауіпсіздік саласына жұмысқа тарту тәжірибесі бар. Мұндай балама тәсіл бір жағынан жасөспірімнің теріс жолға түсіп кетуіне тосқауыл болса, екіншіден елдің цифрлық қорғанысын күшейтуге қызмет етеді.

Сонымен бірге, жасөспірімдер жасаған киберқылмыстарға жауаптылықтан босату немесе жеңілдетілген тәртіпте қарау қоғамдық қауіпсіздік мүддесін толық қамтамасыз ете алмайды деген пікірлер де бар. Кейбір сарапшылар цифрлық қатерлердің жоғарылай түсуіне байланысты аса қауіпті кибершабуылдарға (мысалы, мемлекет инфрақұрылымына зиян келтіретін әрекеттерге) 14 жастан бастап жауаптылық енгізуді ұсынады [38].

Бұл мәселе бойынша заңнамалық саясат қоғамдағы сұранысқа қарай қалыптасары сөзсіз. Жалпы алғанда, кәмелетке толмағандардың Кибер құқық бұзушылықтарға қатысуы - кешенді түрде қарастыратын құбылыс. Олар бір уақытта әлеуметтік-психологиялық, құқықтық және технологиялық аспектілерді қамтиды. Жасөспірімнің дүниетанымы толық қалыптаспай, моральдық-этикалық бағдары орныға қоймаған шағында интернеттің шексіз мүмкіндігі оны қылмыс әлеміне оңай жетелеуі мүмкін. Сондықтан баланың санасына ерте бастан заңға құрмет, интернет мәдениеті және кибергигиена негіздерін сіңіру қажет. Мұны жүзеге асыру - отбасы, мектеп және құқық қорғау құрылымдарының ортақ міндеті. Ювеналды юстиция мен жалпы қылмыстық саясат та заман ағымына ілесіп, цифрлық буынның ерекшеліктерін ескере отырып дамуы тиіс.

Авторлық қорытынды және балама жіктеу ұсынысы. Кибер құқық бұзушылықтардың жалпы түсінігі мен түрлерін талдау негізінде бірқатар қорытынды тұжырымдар жасауға болады. Ең алдымен, киберқылмыс феномені заман талабына сай үнемі өзгеріп, күрделеніп отыратын динамикалық құбылыс екені анықталды. Оны дәстүрлі қылмыстылықтың жай ғана «технологияланған» түрі деп қарастыру жеткіліксіз; шын мәнінде,

цифрлық орта бұрын болмаған жаңа қылмыс түрлерін туындатты және классикалық қылмыстарға тың сипат қосты. Осыған байланысты, құқықтық доктринада кибер құқық бұзушылық ұғымын біржақты, тар шеңберде анықтау қиынға соғады - түрлі мүдде мен көзқарас тұрғысынан бірнеше негіздеме беруге болады. Дегенмен, барлық анықтамаларды жинақтай келгенде, кибер құқық бұзушылық дегеніміз - ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалатын және электрондық кеңістікке бағытталған немесе сол кеңістікте жүзеге асатын заңға қайшы қоғамға қауіпті іс-әрекеттердің жиынтығы деп сипаттауға мүмкіндік бар. Бұл анықтама киберқылмыстардың негізгі үш элементін қамтиды: 1) цифрлық технология (компьютер, желі, бағдарламалық құрал) қылмыс құралы немесе нысаны ретінде көрінеді; 2) әрекет қолданыстағы заңнаманы бұзады (қылмыстық немесе әкімшілік жазаға әкеп соғады); 3) ол қоғамға қауіпті зардаптар келтіреді (азаматтардың құқықтарына, ұйымдардың немесе мемлекеттің заңды мүдделеріне зиян тигізеді).

Кибер құқық бұзушылықтарды жіктеу мәселесіне келсек, бір ғана өлшем тұрғысынан бөлудің шектеулері бар екендігі бөлімде айтылды. Сондықтан автор қолданыстағы классификацияларды синтездей отырып, киберқылмыстардың келесі балама жіктеу жүйесін ұсынады. Бұл жүйе кибер құқық бұзушылықтарды төрт негізгі санатқа бөлуді көздейді және әр санат өз ішінде ерекшеліктеріне қарай бірнеше кіші топтарға жіктелуі мүмкін:

1. Кибертәуелді құқық бұзушылықтар - объектісі де, жүзеге асырылу кеңістігі де ақпараттық технологиялар болып табылатын қылмыстар. Мұнда компьютерлік жүйелер мен деректерге тікелей қол сұғу, оларды бұзу, істен шығару, зиянды бағдарламалар тарату сияқты әрекеттер кіреді. Мысалы, хакерлік шабуылдар (рұқсатсыз қол жеткізу), вирус, «құрт» (worm) сынды зиянды кодтарды жасау және тарату, DDoS шабуылдары осы категорияға жатады. Бұл қылмыстар цифрлық инфрақұрылымның қауіпсіздігіне тікелей қауіп төндіреді және дәстүрлі қылмыстардың ешқайсысына толық ұқсамайды. Сондықтан оларды нағыз киберқылмыстар деп атауға болады [27].

2. Кибер құралдандырылған мүліктік қылмыстар - ақпараттық-коммуникациялық желілерді пайдалана отырып жасалатын пайдакүнемдік және мүліктік зиян келтіруге бағытталған құқық бұзушылықтар. Бұлар дәстүрлі экономикалық қылмыстардың интернет арқылы іске асатын түрлері. Мысалы, онлайн алаяқтық (интернет-дүкендердегі жалған мәмілелер, фишинг арқылы банк карталарынан ақша ұрлау), қаржы пирамидаларын интернет арқылы құру, криптовалюта алаяқтығы, интернет-банк жүйелерін бұзу арқылы ақша жымқыру сияқты әрекеттер осы санатқа кіреді. Сондай-ақ сандық контрафакт (бағдарламалық өнімдерді, мультимедианы заңсыз көшіру және тарату), авторлық құқықтарды интернетте бұзу да осы топқа жатқызылуы мүмкін. Бұл қылмыстардың түпкі мақсаты - экономикалық пайда табу, сондықтан оларды кибержемқорлық не киберқаржылық қылмыстар деп сипаттауға болады [27].

3. Киберқұралдандырылған жеке тұлғаға қарсы қылмыстар - ақпараттық технологияларды қолданып, жеке адамдардың құқықтары мен бостандығына қастандық жасайтын әрекеттер. Бұған кибербуллинг (ғаламтор арқылы қорлау, қорқыту, қудалау), онлайн тұрғыда жала жабу және қорлау, жеке өмірге қатысты мәліметтерді заңсыз тарату, кибersталкинг (адамды интернетте ұзақ уақыт аңду және мазалау) жатады. Сондай-ақ сексуалдық сипаттағы интернет-қылмыстар - кәмелетке толмағандарды азғыру (grooming), порнографиялық материалдар тарату немесе жалаңаштауға мәжбүрлеу - осы санатқа кіреді. Бұл құқық бұзушылықтар тікелей адамдардың ар-намысына, психикалық және физикалық тұтастығына қол сұғады. Олар көбінесе дәстүрлі зорлық не қорлау қылмыстарының желідегі көрінісі болғанымен, интернеттің анонимдік және жылдамдық факторлары оларды ауырлатып, кең ауқымға жаюы мүмкін. Сол себепті мұндай іс-әрекеттерді дер кезінде анықтап, жолын кесу үшін арнайы киберпатрульдік және мониторинг шаралары қажет.

4. Контенттік (мазмұнға қатысты) құқық бұзушылықтар - ақпараттық жүйелер мен желілер арқылы заңмен тыйым салынған мазмұнды дайындау, сақтау немесе көпшілікке тарату әрекеттері. Бұған балалар порнографиясы материалдарын шығару және тарату, терроризмге, экстремизмге шақыратын немесе зорлық-зомбылықты насихаттайтын материалдарды жариялау, нәсілшілдік пен ксенофобияны өршітетін контент тарату, сондай-ақ заңсыз өнімдер мен қызметтердің (есірткі, қару, адам саудасы) жарнамасы мен сатылуын ұйымдастыру сияқты әрекеттер кіреді. Контенттік қылмыстардың ерекшелігі - оларда ақпараттың өзі қылмыс заты болып табылады және мұндай құқық бұзушылықтар көбіне қоғамдық моральға, қоғамдық қауіпсіздікке немесе мемлекеттің ақпараттық кеңістігінің тыныштығына қатер төндіреді. Халықаралық қауымдастық бұл саладағы қылмыстарға қарсы күреске ерекше мән береді (мысалы, Будапешт конвенциясына 2003 ж. қабылданған Қосымша хаттама тек расистік және ксенофобтық контент туралы болды [27]. Контенттік құқық бұзушылықтар көбінесе трансшекаралық сипатта тарайтындықтан, оларды тиімді тежей алу үшін мемлекетаралық ынтымақтастық пен ақпарат алмасу тетіктері өте маңызды.

Автор ұсынылған осы жіктеу киберқылмыстардың табиғатын жан-жақты қамтып, олардың ерекшеліктерін ескеруге мүмкіндік береді деп санайды. Әрине, өмірде кездесетін нақты құқық бұзушылық кейде бірден бірнеше санаттың элементтерін қамтуы ықтимал. Сондықтан бұл жіктеу шартты, аналитикалық ыңғайлы болу үшін жасалған. Дегенмен, мұндай құрылымдандыру құқық қорғау органдарына әртүрлі киберқылмыс түрлеріне мамандандырылған әдістеме әзірлеуге, ал заң шығарушыларға жаңа пайда болған санаттарды дер кезінде заңнамалық тұрғыда жеке құрам ретінде бекітуге көмек береді. Қорытындылай келе, кибер құқық бұзушылықтар - заманауи құқық жүйесіне аса маңызды сынақ. Оларды түсіну және дұрыс жіктеу - тиімді қарсы күресудің алғышарты. Кәмелетке толмағандардың киберқылмысқа тартылуы арнайы назарды талап ететін құбылыс ретінде бөліп қарастырылды. Жасөспірімдерді бұл қауіпті ортадан қорғау, әрі

олардың өздерінің құқық бұзуына жол бермеу - қоғамның және мемлекеттің ортақ міндеті. Зерттеу нәтижесінде ұсынылған балама жіктеу мен тұжырымдар Кибер құқық бұзушылықтардың қыр-сырын қазақ құқықтық доктринасында тереңірек ұғынуға және олармен күресте тиімді стратегиялар әзірлеуге септігін тигізеді деп үміттенеміз.

### 1.3 Кибер құқық бұзушылықтардың әкімшілік-құқықтық салдары

Киберкеңістіктегі құқық бұзушылықтар және әкімшілік жауаптылықтың мәні. Заманауи қоғамда коммуникацияның цифрлық кеңістікке ауысуына байланысты құқық бұзушылықтардың жаңа түрлері - кибер құқық бұзушылықтар - кең таралуда. Кибер құқық бұзушылық ұғымы интернет немесе басқа электрондық коммуникациялар арқылы жасалатын заңға қайшы әрекеттерді қамтиды. Бұған кибербуллинг (жүйелі түрде онлайн қорқыту мен қорлау), киберқорқыту (онлайн кеңістікте қоқан-лоқы көрсету, бопсалау), онлайн тіл тигізу (желідегі балағаттау, абыройға нұқсан келтіру) және анонимді аккаунттарды пайдаланып жасалатын өзге де құқыққа қарсы әрекеттер жатады. Мұндай істердің ерекшелігі - олар дәстүрлі құқық бұзушылықтар сияқты қоғамға зиян келтіргенімен, көбіне виртуалды ортада жасалады және құқық қорғау органдары үшін анықтау, дәлелдеу күрделірек болады. Сондықтан көптеген елдер, оның ішінде Қазақстан Республикасы, кибер құқық бұзушылықтарды құқықтық реттеу тетіктерін жетілдіріп, олар үшін әкімшілік-құқықтық жауаптылық шараларын енгізіп отыр [39].

Киберкеңістіктегі құқық бұзушылықтарға қарсы күресте қылмыстық заңдармен қатар әкімшілік құқық нормаларының да рөлі зор. Егер әрекет қоғамға қауіптілігінің дәрежесі бойынша қылмыс қатарына жатпаса немесе ауыр зардаптары болмаса, онда оған әкімшілік жаза қолданылуы мүмкін.

Әкімшілік жауаптылық интернеттегі ғайбат сөздер, қорлау, алымсақтық, буллинг сияқты жеңіл әрі орта дәрежелі құқық бұзушылықтарға тез және тиімді шара қолдануға мүмкіндік береді. Мысалы, әлеуметтік желіде балағат сөз айту, өзгеге тіл тигізу немесе арандатушы ақпарат тарату жағдайында қылмыстық іс қозғау қиын немесе орынсыз болуы мүмкін, алайда мұндай әрекеттерге әкімшілік кодекс аясында жаза қолдануға болады [40]. Сол арқылы құқық бұзушыны дер кезінде тоқтатып, жәбірленушінің құқықтарын қорғау қамтамасыз етіледі.

Қазақстан Республикасында соңғы жылдары кибербуллингпен және Интернеттегі өзге де құқыққа қарсы әрекеттермен күресті күшейту мақсатында заңнамаға бірқатар толықтырулар мен өзгерістер енгізілді. 2022 жылы бала құқықтарын қорғау туралы заңға түзетулер қабылданып, «буллинг» ұғымы алғаш рет заңнамалық деңгейде айқындалды. 2024 жылы Әкімшілік құқық бұзушылық туралы кодексіне (ӘҚБтК) буллинг үшін жеке жауапкершілік белгіленіп, кәмелетке толмағандарды буллингке ұшыратқаны үшін жазалар көзделді [41]. Бұл реформалар кибер құқық бұзушылықтардың алды алынып, оларға уақытылы әкімшілік шара қолдану мақсатын көздейді. Төменде кибер құқық бұзушылықтарға қатысты Қазақстанның әкімшілік

заңнамасы нормалары, құқық қолдану тәжірибесі, кәмелетке толмағандардың жауапкершілік ерекшеліктері және халықаралық тәжірибе талданады.

Қазақстан Республикасының ӘҚБтК-дегі кибер құқық бұзушылықтарға қатысты нормалар. Қазақстанның Әкімшілік құқық бұзушылық туралы кодексінде (ӘҚБтК) тікелей немесе жанама түрде кибер құқық бұзушылықтарға қолданылуы мүмкін бірнеше баптар бар. Ең алдымен, 2024 жылғы 16 маусымнан бастап қолданысқа енген 127-2-бап - «Травля (буллинг, кибербуллинг) кәмелетке толмағанды» атты жаңа норма кибербуллинг үшін әкімшілік жауаптылықты тікелей қарастырады [42]. Аталған бап бойынша:

- Кәмелетке толмаған адамға қатысты буллинг (кибербуллинг) жасау - алғаш рет жасалса, ескерту немесе 10 айлық есептік көрсеткіш (АЕК) мөлшерінде айыппұл салынады [42]. 2024 жылы 1 АЕК 3 692 теңгеге тең болғанын ескерсек, бұл шамамен 36-39 мың теңге көлеміндегі айыппұлды құрайды.

- Осы әрекет бір жылдың ішінде қайталанса - 30 АЕК (шамамен 110-111 мың теңге) айыппұл салынады [42]. Яғни қайталанған буллинг заң тұрғысынан ауырлататын мән-жай болып табылады.

- Буллингті 12-15 жас аралығындағы жасөспірім жасаса - әкімшілік жаза ата-анаға немесе заңды өкілге қолданылады (ескерту немесе 10 АЕК айыппұл түрінде) [42]. Бұл норма буллинг жасаған кәмелетке толмағанға тікелей жаза қолдануға заң жол бермейтіндіктен, оның орнына тәрбиелеу міндетін атқарушы ересектерді жауапқа тартуға бағытталған.

Аталған 127-2-бап Қазақстанда буллинг пен кибербуллингке қарсы күрестегі маңызды қадам болды. Президент Қ.Тоқаевтың 2024 жылғы бастамасымен әйелдер мен балалардың қауіпсіздігін қамтамасыз етуге арналған заңнама пакеті аясында буллинг үшін әкімшілік жауаптылық алғаш рет енгізіліп, кәмелетке толмағандарды қорлау (соның ішінде кибербуллинг) заңмен тыйым салынғаны жарияланды Осылайша, бұрын ҚР заңнамасында болмаған «кибербуллинг» термині мен оған қарсы санкциялар бекітілді. Бұған дейін буллинг оқиғалары құқықтық статистикада жеке санат ретінде бөлінбейтін, кейде төбелес, ұсақ бұзақылық сияқты басқа баптармен дәрежеленіп келді, ал біразы тіпті есепке алынбайтын еді. 127-2-баптың енгізілуі мұндай істерді даралап қарастыруға және ресми тіркеуге мүмкіндік берді. Кибер құқық бұзушылықтарға байланысты тағы бір маңызды норма - ӘҚБтК 73-3-бабы («Жала жабу»). Бұл бап 2020 жылы қабылданған өзгерістермен Қылмыстық кодекстен әкімшілікке ауыстырылған [43]. Жала жабу - басқа адамның абыройы мен қадір-қасиетіне нұқсан келтіретін немесе беделін түсіретін көрінеу жалған мәлімет тарату - әкімшілік құқық бұзушылық деп танылады. 73-3-бап бойынша: жеке тұлғаға жасалған жала үшін 160 АЕК айыппұл салуға немесе 15 тәулікке дейін әкімшілік қамаққа алуға болады; егер бұл әрекет көпшілік алдында не БАҚ немесе телекоммуникация желілерін пайдаланып жасалса - айыппұл 180 АЕК-ке дейін, қамақ 20 тәулікке дейін ұзартылады. Адамды ауыр қылмыс жасады деп жалған айыптау сияқты ауыр формалары үшін 200 АЕК айыппұл не 25 тәулік қамақ тағайындалуы мүмкін [42]. Бұл норманың маңызы - интернет арқылы

жалған ақпарат, өсек тарату, әсіресе біреудің беделіне нұқсан келтіретін фейк жаңалықтар, әлеуметтік желілердегі өсектер үшін жедел шара қолдануға жол ашады. Егер мұндай әрекеттер қылмыстық дәрежеге жетпесе (ҚР Қылмыстық кодексінде жала жабу қылмысы алынып тасталған), әкімшілік тәртіпте айыппұл салынып немесе қысқа мерзімге қамауға алу мүмкіндігі бар.

Мысалы, көпшілікке жалған ақпарат таратып, жеке тұлғаны масқаралауға тырысқан анонимді аккаунт иесі анықталған жағдайда, 73-3-бап бойынша 15 тәулікке дейін абақтыға жіберілуі ықтимал - бұл киберкеңістіктегі жалған ақпарат пен абыройға қол сұғушылыққа елеулі тоқтау салатын норма.

Интернетте тіл тигізу және балағаттау жағдайлары әкімшілік және қылмыстық заңның тоғысында орналасқан. Қорлау (жеке адамның ар-намысы мен қадір-қасиетін әдепсіз түрде кемсіту) қазіргі кезде ҚР Қылмыстық кодексінің 131-бабы бойынша қылмыстық теріс қылық саналады. Оны жасағаны үшін 100 АЕК-ке дейін айыппұл не 120 сағатқа дейін түзеу жұмыстары немесе қоғамдық жұмыстар белгіленген. Алайда қорлау қылмыстық ісі жәбірленушінің жеке айыптау тәртібімен (арызы бойынша) қозғалады және көп жағдайда ауыр процедураны талап етеді. Сол себепті интернеттегі бір реттік қорлау фактілері көбіне әкімшілік деңгейде қаралады. Егер балағаттау қоғамдық орын деңгейінде немесе айналасындағыларға анық сыйламаушылық танытып, жұрттың тыныштығын бұзса - онда ол ӘҚБтК 434-бабы («Ұсақ бұзақылық») ретінде жіктеледі. Ұсақ бұзақылық деп қоғамдық орындарда былапыт сөйлеу, жеке тұлғаларға қорлап тиісу, айналадағы адамдарды сыйламау белгіленген әрекеттер түсініледі.

Мысалы, әлеуметтік желідегі ашық топта немесе көпшілікке көрінетін пікірде біреуді ауыр балағат сөздермен қорлау - айналадағы оқырмандарға да әсер ететін, қоғамдық тәртіпті бұзатын әрекет ретінде танылып, 434-баппен қаралуы мүмкін. Бұл бап бойынша жаза сот тәртібімен ескерту не 5-15 тәулікке дейін әкімшілік қамақ түрінде тағайындалады. 2023 жылғы өзгерістермен ұсақ бұзақылық үшін айыппұл мөлшері 20 АЕК-ке (69 мың теңге) дейін өсіріліп, қамау мерзімі 15 тәулікке дейін ұзартылды [40]. Демек, интернетте көпшілікке балағат сөздер айту, төбелеске шақыру, кемсіту фактілері қазір қатаңырақ жазаға тартылуда.

Интернеттегі отбасылық-тұрмыстық қатынастағы қорлау әрекеттері бөлек қарастырылады. Мысалы, егер құқық бұзушы жәбірленушімен отбасы тұрмыстық қатынаста (туыс, бірге тұратын адам) болып, оған балағат сөздер айтып, дөрекілік танытса, бұл іс ӘҚБтК 73-бабына (отбасылық зорлық-зомбылық белгілері бар әрекеттер) жатқызылып, сот тәртібімен ескерту не 5 тәулікке дейін қамауға алуға әкеп соғады [40]. Бұл бап ең алдымен тұрмыстағы психологиялық зорлық-зомбылықтың (соның ішінде отбасындағы киберқорқыту - мысалы, жұбайының телефон арқылы үздіксіз қорқытуы) алдын алуға бағытталған. Сонымен бірге, Ақпараттық кеңістіктегі кейбір заң бұзушылықтар да әкімшілік құқық нормаларымен реттеледі. Мысалы, 2022 жылы қабылданған заңға сәйкес, ірі әлеуметтік желілер Қазақстан аумағында балаларға қатысты буллинг сипатындағы контент анықталса, оны тәулік ішінде бұғаттауға міндетті [39].

Әлеуметтік желі операторлары Қазақстанда өздерінің заңды өкілдерін тағайындап, олар Ақпарат және қоғамдық даму министрлігімен өзара іс-қимыл жасауға тиіс деп заңда белгіленді [39]. Ата-ана министрлікке баласына қатысты кибербуллинг жөнінде шағым түсірсе, уәкілетті орган 3 жұмыс күні ішінде жағдайды қарап, әлеуметтік желі өкіліне хабарлайды, ал өкіл 24 сағат ішінде буллинг мазмұндағы жазбаны өшіруге міндетті [39]. Орындамаған жағдайда, платформаға қатысты шаралар қолданылуы мүмкін (Қазақстан заңдары толық блоктауға жол бермегенімен, әкімшілік ықпал ету тетіктері қарастырылған). Бұл норма балаларды интернеттегі зорлық-зомбылықтан жедел қорғауға арналған әкімшілік-құқықтық тетік ретінде бағаланады. Ұқсас шаралар әлемде Германияның NetzDG заңында және Ұлыбританияның Online Safety Act заңында да бар (төменде халықаралық бөлімде қаралады).

Жалпы, Қазақстан ӘҚБтК-нің жоғарыдағы баптары кибер құқық бұзушылықтардың әртүрлі түрлерін қамтиды: буллинг пен қорлау - 127-2 және 73-3 баптар; балағаттау, анайы әрекеттер - 73 және 434-баптар; ата-ана мен лауазымды тұлғалардың жауапкершілігі - 127 және 127-1 баптар; сондай-ақ ақпараттық кеңістіктегі өзге де заң бұзушылықтар тиісті салалық баптармен (мысалы, экстремистік материалдар тарату ҚК-ке жатса, заңсыз онлайн жарнама, авторлық құқықты бұзу және т.б. арнайы нормалармен) реттеледі. Ендігі кезекте кәмелетке толмағандардың әкімшілік жауаптылығының ерекшеліктері мен практикасына тоқталайық.

*Кәмелетке толмағандардың әкімшілік жауапкершілік ерекшеліктері.* Қазақстан заңнамасында кәмелетке толмағандардың әкімшілік жауаптылығы ерекше ережелермен айқындалған. ӘҚБтК-нің 66-бабы «Кәмелетке толмағандарға әкімшілік жаза қолданудың ерекшеліктері» деп аталады және 16 жасқа толмаған құқық бұзушыларға қатысты бірқатар шектеулер қояды. Жалпы ереже бойынша, әкімшілік жауаптылыққа тарту жасы - 16 жас. Яғни 16 жастан төмен тұлға әкімшілік құқық бұзушылық субъектісі бола алмайды, оларға тікелей айыппұл не өзге жаза салынбайды. Дегенмен, 2024 жылғы өзгерістер кәмелетке толмағандар жасаған кейбір әрекеттер үшін жанама жауаптылық тетігін енгізді - буллинг жасаған 12-15 жастағылардың ата-аналарына айыппұл салу (жоғарыда 127-2-бап) осы мақсатты көздейді.

ӘҚБтК 66-бабына сәйкес, кәмелетке толмаған адамға салынатын айыппұл мөлшері қандай жағдай болмасын 10 АЕК-тен аспауға тиіс. Яғни, 16 немесе 17 жастағы жасөспірім әкімшілік құқық бұзушылық жасаса, егер тиісті баптың санкциясында әлдеқайда ірі айыппұл көзделсе де, оған ең көп дегенде 10 АЕК (шамамен 2025 жылға 35 мың теңге айналасында) айыппұл салынады. Мысалы, 73-3-бап бойынша жалған ақпарат таратуға жалпы 160 АЕК айыппұл жазылса да, егер оны 17 жасар бозбала жасаса, оған 10 АЕК-тен артық айыппұл берілмейді. Сонымен қатар, 66-бап 16-17 жастағы адамның айыппұл төлеуге жеткілікті мүлкі болмаса, айыппұлды оның ата-анасына немесе қамқоршысына салу қарастырылған [42]. Яғни, жасөспірімде табыс немесе мүлік жоқ болуы табиғи жағдай, сондықтан әкімшілік айыпты ата-ана өтейді (ата-ана бұл жағдайда субсидиарлық жауапты). Заң кәмелетке толмағандарға кейбір жаза түрлерін қолдануға тыйым салады.

Атап айтқанда, әкімшілік қамаққа алу (қамауға алу) 18 жасқа толмаған адамдарға қолданылмайды деп ұғындырылады. 66-баптың 3-бөлігіне сәйкес, әкімшілік жазалардың басқа түрлері (қамақтан басқа) жалпы негіздерде қолданылуы мүмкін, ал қамаққа алу кәмелетке толмағандарға тағайындалмайды [42]. Сондықтан, жасөспірім қандай да бір құқық бұзушылық жасаса, оны тек ескерту немесе айыппұлмен шектеу қарастырылған; әкімшілік тәртіпте түрмеге жабу шарасы қолданылмайды. Бұл халықаралық стандарттарға (БҰҰ Балалар құқықтары туралы конвенциясына) сай келеді, яғни бостандығынан айыру ең соңғы шара ретінде ғана және қысқа мерзімге қолданылуы керек, ал әкімшілік деңгейде ондай жаза мүлде жоқ.

ӘҚБтК 67, 68-баптарында кәмелетке толмағандарға жаза қолдану тәртібі мен мерзімдері көрсетілген. Мысалы, 16-17 жастағы жасөспірімге әкімшілік жаза қолданылса, ол 6 айдан кейін жауапқа тартылды деп есептелмейді (сотталғандық мерзімі қысқа) [42], бұл да олардың құқықтық жағдайын жеңілдететін нормалардың бірі.

Кәмелетке толмағандардың әкімшілік құқық бұзушылықтарының алдын алу және оларға тәрбиелік ықпал ету үшін заңда қосымша шаралар қарастырылған. ӘҚБтК-нің 66-бабының 1-бөлігінде «кәмелетке толмаған адамға әкімшілік жаза қолданғанда тәрбиелік ықпал ету шаралары қолданылуы мүмкін» делінген. Яғни жасөспірім заң бұзса, тек айыппұл салып қана қоймай, оған қоса ескерту-профилактикалық әңгіме, мінез-құлқын түзетуге бағытталған шаралар жүзеге асырылуы тиіс. Мұндай тәрбиелік ықпалдың нақты түрлері ӘҚБтК-де ашық жазылмағанымен, тәжірибеде мектептегі педагогикалық кеңестер, ювеналдық полиция инспекторларының алдын алу әңгімелері, психологтың жұмысы сияқты тәсілдер қолданылады. Бұл ретте жергілікті атқарушы органдар жанындағы кәмелетке толмағандар істері және олардың құқықтарын қорғау жөніндегі комиссиялардың рөлі зор. Аталған комиссиялар әкімшілік немесе қылмыстық жауапқа тартылмайтын (жасы толмауына байланысты) құқық бұзған балалардың ісін қарап, оларға түрлі тәрбиелік ықпал шараларын қолданады (ескерту, арнайы есепке қою, мінез-құлқына бақылау белгілеу, қажетті жағдайда арнайы тәрбиелеу мекемесіне жолдау). Мысалы, «Бала құқықтары туралы» ҚР Заңының 26-бабына сай кәмелетке толмаған балаға қатысты профилактикалық шара ретінде оны мінез-құлқы қиын балаларға арналған арнайы білім беру ұйымына жіберу сот тәртібімен мүмкін. Бұл көбіне 11 жас пен 18 жас арасындағы бірнеше рет тәртіп бұзған немесе қолайсыз отбасынан шыққан балаларға қолданылатын тәрбие шарасы.

Ата-аналардың әкімшілік жауапкершілігі - кәмелетке толмағандардың құқық бұзушылықтарының алдын алу мен олар үшін жауаптылық тағайындаудағы негізгі механизмнің бірі. ӘҚБтК-нің 127-бабы осыған арналған. 127-баптың атауы 2024 жылы өзгеріп, «Кәмелетке толмаған адамды тәрбиелеу, оқыту, оның құқықтары мен мүдделерін қорғау және қауіпсіздігін қамтамасыз ету жөніндегі міндеттерді орындамау» деп аталады [42]. Бұл баптың мазмұнына сәйкес:

- Ата-аналар немесе заңды өкілдер балаларын тәрбиелеу, оқыту, олардың құқықтарын қорғау және қауіпсіздігін қамтамасыз ету жөніндегі өз міндеттерін тиісінше орындамаса - 10 АЕК айыппұл салынады [42]. Мысалы, баласының мінез-құлқын қадағаламай, оның құқық бұзушылық жасауына жол берген ата-ана осы негізде жауапқа тартылуы мүмкін.

- Егер бұл әрекет бір жыл ішінде қайталанса - 15 АЕК айыппұл не 5 тәулікке дейін қамақ қарастырылған [42].

- 127-баптың 3-бөлігі ерекше мән-жайды көрсетеді: ата-ана (не оны алмастыратын адам) немесе тәрбиеші, педагог баланың алкоголь, есірткі пайдалануы немесе қаңғыбастықпен айналысуына, не қасақана қылмыс немесе әкімшілік құқық бұзушылық жасауына әкеп соқса, яғни соған жол берсе - 20 АЕК айыппұл не 10 тәулікке дейін қамақ тағайындалады [42]. Бұл тармақ баланың ауыр құқық бұзушылыққа баруына тікелей себепкер немесе жағдай жасаған ересектерді жазалауға мүмкіндік береді.

2024 жылғы заңнамалық өзгерістер ата-аналардың бала қауіпсіздігіне қатысты жауапкершілігін де күшейтті. Мысалы, кішкентай балалардың терезеден құлап кету оқиғалары, баланы көлікте қараусыз қалдыру сияқты жағдайлар жиілеген соң, 127-бапқа «қауіпсіздігін қамтамасыз ету жөніндегі шараларды орындамау» қосылды [42]. Енді балаға қауіп төндіретін салғырттық - әкімшілік жауапқа тартудың негізі. ІІМ мәліметінше, баланы терезеден құлауынан сақтау үшін жағдай жасамау, автокөлікте жалғыз қалдыру сынды оқиғалар орын алса, ата-ана 127-бап бойынша жауап береді [40]. Бұл өзгерістер қоғамда балалар қауіпсіздігіне ата-ананың немқұрайдылығын азайтуға бағытталған маңызды қадам деп бағаланды.

Ата-аналардың жауапкершілігі тек өз баласын қадағаламағаны үшін емес, бала басқа біреудің құрбаны болған жағдайда да туындайды. 2024 жылғы заңнамада білім беру ұйымдарына жаңа міндет жүктелді: егер мектепте не балабақшада балаға қатысты буллинг немесе өзге құқыққа қарсы әрекет орын алса, оқу орны дереу құқық қорғау органдарына хабарлауға міндетті. Бұрын кей жағдайда мектеп әкімшілігі «өзіміз шешеміз» деп, буллинг фактілерін жабуға тырысатын. Енді ондай әрекет 127-1-бап бойынша қарастырылуы мүмкін. 2019 жылы енгізілген 127-1-бап «Кәмелетке толмағандар жасаған немесе оларға қатысты құқыққа қарсы іс-әрекеттер туралы хабарламау» деп аталады. Бұл бап бойынша білім беру, денсаулық сақтау немесе әлеуметтік қорғау ұйымдарының қызметкерлері жұмысы барысында балаға қатысты құқық бұзушылық туралы белгілі болса, оны құқық қорғау органдарына хабарламағаны үшін жауапқа тартылады. Жеке тұлғаға - 5 АЕК, лауазымды адамға - 10 АЕК айыппұл салу көзделген; жыл ішінде қайталаса тиісінше 20 және 30 АЕК айыппұлға дейін өседі [42]. Бұл норма мектеп мұғалімдерін, директорларын, дәрігерлерді, әлеуметтік қызметкерлерді қамтиды. Мысалы, мектепте оқушы ұзақ уақыт буллингке ұшырап жүргенін біле тұра, мектеп әкімшілігі полицияға хабарламаса - ол үшін 127-1-баппен айыппұл салынуы ықтимал. Батыс Қазақстан облысының сот практикасы осы бапты қолданудың нақты мысалын көрсетті: 2024 жылы. Орал қаласында 13 жасар оқушыны екі жыл бойы қорлап келген жағдайды мектеп басшылығы мен

сынып жетекшісі дер кезінде ашып, тәртіп комиссиясына шығармаған. Тергеу барысында бұл дерек анықталып, жауапты тұлғаларға 127-1-баппен іс қозғауға негіз болғаны хабарланды (іс материалдары қоғамға толық ашылмағанмен, аталған бап қолданылғанын көруге болады). Мұндай тәжірибе білім беру саласының қызметкерлерін оқушылар арасындағы зорлық-зомбылыққа бей-жай қарамауға ынталандырады. Сонымен, Қазақстан кәмелетке толмағандардың әкімшілік жауаптылығы саласында «қосақталған жауапкершілік» принципін жүзеге асырып отыр: жас бала заң бұзса - ата-ана жауап береді, ал бала жәбір көрсе - тағы да сол баланың қауіпсіздігіне жауапты ересектер (мектеп, ата-ана) жауапкершілікке тартылады. Бұл жүйе кәмелетке толмағандар құқық бұзушылықтарының алдын алу мен оларды ерекше қорғау мақсатына негізделген.

Қазақстанда кәмелетке толмағандарға қатысты профилактикалық жұмыс көпвекторлы жүргізіледі. ІІМ Жергілікті полиция қызметі құрамында ювеналды полиция инспекторлары мектептерге бекітіліп, тәуекел тобындағы балалармен жұмыс істейді. Әкімдіктер жанындағы комиссиялар ай сайын құқық бұзған немесе қиын балаларға қатысты отырыстар өткізіп, жеке іс жоспарларын бекітеді. Мысалы, Астана қаласында 2025 жылдың басынан бері «Қауіпсіз жол» және «Назар аударыңыз - балалар!» сияқты рейдтік іс-шаралар өткізіліп, мыңдаған әкімшілік құқық бұзушылық анықталды (оның ішінде комендантты сағатты бұзу, көше кезу фактілері). Мұндай шаралар жасөспірімдердің құқық бұзуға бейім мінез-құлқын ерте кезеңде түзетуді көздейді. Қорыта айтқанда, Қазақстанның әкімшілік заңнамасы кәмелетке толмағандарға қатысты бала-ата-ана-мектеп желісі бойынша кешенді жауапкершілік жүйесін орнатқан. Баланың интернеттегі қауіпсіздігін қамтамасыз етпегені үшін ата-анаға айыппұл салынады, баланы буллингке ұшыратқан жасөспірімнің ата-анасы жазаланады, ал балаға жасалған зорлық-зомбылықты жасырған мұғалім де жазасыз қалмайды [42]. Мұның бәрі кәмелетке толмағандарды зиянды контент пен қатыгез әрекеттерден қорғауға, сондай-ақ олардың өздерінің құқық бұзушылық жасауының алдын алуға бағытталған әкімшілік-құқықтық тетіктер.

*Кибербуллинг және онлайн құқық бұзушылықтар бойынша құқық қолдану тәжірибесі (Қазақстан).* Қазақстанда кибербуллингке қарсы әкімшілік жауапкершілік енгізілген 2024 жылдан бері осы бағыттағы құқық қолдану тәжірибесі қалыптаса бастады. ІІМ Әкімшілік полиция комитетінің дерегіне сәйкес, 2024 жылдың екінші жартысында (маусымнан желтоқсанға дейін) елімізде ресми түрде 149 буллинг фактісі тіркеліп, барлығына әкімшілік іс қозғалып, сотқа жолданған [44]. Бұрын мұндай оқиғалар жеке есепке алынбайтындықтан, бұл статистика заңнаманың тиімді іске асып жатқанын көрсетеді. Мысалы, 2024 жылғы желтоқсанда жарияланған ресми ақпаратта: «Жаз айларында балаларға қарсы кез келген зорлық-зомбылық үшін жауапкершілікті күшейтуге бағытталған заңнамалық түзетулер қабылданғаннан бері буллинг үшін әкімшілік жауапкершілік енгізілді. Қазіргі жылдың өзінде 149 буллинг фактісі тіркелді. Олардың барлығына әкімшілік хаттама толтырылып, сотқа процессуалдық шешім қабылдауға жіберілді»

делінген [45]. Бұл - жарты жыл ішінде жүзден астам іс сот қарауына жолданды деген сөз. Салыстыру үшін, 2023 жылға дейін буллинг оқиғалары көбіне «төбелес», «әлімжеттік» деп ішінара тіркелсе, көп бөлігі бейресми түрде қалатын еді [44]. Енді жаңа бап оларды ашық статистикаға шығарып, әрқайсысын қарауға мүмкіндік берді.

Тіркелген істер бойынша соттар алғашқы шешімдерін шығаруда. 2024 жылғы қарашада Батыс Қазақстан облысының соты ата-анаға 127-2-бап бойынша алғашқылардың бірі болып жаза тағайындады. Орал қалалық сотында 13 жасар жасөспірімнің 10 жастағы баланы екі жыл бойы бопсалап, ақша тартып алып келгені туралы әкімшілік іс қаралды. Сотта агрессордың анасы баласына түсіндіру жүргізгенін айтса да, буллинг фактісін мойындағысы келмеді, ал жәбірленушінің анасы екі жыл бойы ұлының қорқып, үндемей келгенін, енді татуласудан бас тартатынын айтты. Іс материалдары буллингтің болғанын - хаттама, жәбірленуші арызы, куәгерлердің жазбаша түсініктемелері арқылы дәлелдеді. Сот 127-2-баптың 1-бөлігі бойынша жазаның шегі ескерту немесе 10 АЕК айыппұл екенін атап өтті. Жасөспірімнің анасының үш баласы бар, тұрақты жұмысы және табысы жоқ екені, бұрын баласының тәртібі үшін жауапкершілікке тартылмағаны ескеріліп, оған ескерту түрінде әкімшілік жаза тағайындалды [46]. Яғни алғашқы іс бойынша сот ең жеңіл санкцияны таңдады, бұл да тәрбиелік ықпалдың бір әдісі - анасына ресми ескерту берілді.

Дегенмен, сол жылдың қарашасында Қостанай облысында ұқсас істі қараған сот ата-анаға айыппұл салды. Б.Майлин аудандық соты 9-сынып оқушысының 8-сыныптағы қыз балаға жүйелі буллинг (күнделікті қорлау, қорқыту, намысына тию) жасағаны үшін оның әкесін жауапқа тартты. Сотта ата-ана кінәсін толық мойындап, баласымен тәрбие жұмысын жүргізгенін айтты; жәбірленуші қыздың анасы қызының жүрегі ауыратындығын, буллингтен соң депрессияға түскенін баяндады. Анықталғаны - осы ата-анаға бұған дейін баласының теріс қылықтары үшін бейресми түрде ескерту жасалған, мектептен шағымдар болған. Сондықтан сот бұл жолы жеңілдік қолданбай, 25 800 теңге көлемінде айыппұл салды [46]. Бұл сома шамамен 7 АЕК-ке тең (сол жылы 1 АЕК ~3 450 тг болса). Негізі 10 АЕК (36 920 тг) айыппұл салу мүмкін еді, алайда сот істің жағдайына қарай мөлшерді азайтқан сыңайлы. Әрине, ӘҚБтК санкциясы 10 АЕК деп нақты көрсеткендіктен, сот неге 25 800 тг тағайындағаны белгісіз: мүмкін, төлемді жыл соңындағы АЕК мәнімен есептегенде айырма шыққан, немесе ата-ана кінәсін мойындап, шығын өтегені ескерілген шығар. Қалай болғанда да, бұл іс - ата-анаға айыппұл салынған алғашқы прецеденттердің бірі. Кейіннен ІІМ өкілдері буллинг үшін ата-аналарға негізінен ескерту берілетінін, бірақ қайталанса және алдын алу шараларынан нәтиже шықпаса, айыппұл салынатынын түсіндірді.

2024 жылы елді дүрліктірген резонансты жағдай - Риддер қаласындағы буллинг оқиғасы. Мектепте оқитын қызды сыныптастары аяусыз қорлап, соққыға жыққаны туралы видео әлеуметтік желіге шығып, қоғам назарына ілікті. Ата-ана полиция мен мектепке бірнеше рет шағымданса да, шара

қолданылмағаны белгілі болды. Бұл дерек бойынша құқық қорғаушылар дабыл қағып, мәселені жариялады. Жергілікті полиция тек қоғамдық резонанстан кейін буллинг жасаған оқушыларды анықтап, оларды есепке қойды, мектеп басшылығы мен сынып жетекшісіне тәртіптік шара қолданылды. Облыстық білім басқармасы мен ювеналды полиция өкілдері сол мектепте жиналыс өткізіп, барлық жауапты тұлғаларды тәртіпке шақырды. Аталған іс бойынша 127-1-баппен (хабарламау) де тексеру жүрген болуы мүмкін, себебі мектеп әкімшілігінің әрекетсіздігі байқалған. Ақпарат құралдарының хабарлауынша, бұл оқиғадан соң өңірде бірде-бір буллинг фактісі назардан тыс қалмайтыны жөнінде уәде берілді [44]. Риддер оқиғасы - жаңа заң қабылданса да, бастапқыда құқық қолданушылардың (полиция, мектеп) енжарлығы кездескенін көрсетті. Дегенмен, қоғамның қысымымен жергілікті атқарушы органдар тез арада іске кірісіп, кінәлілерді жазалап, олқылықты түзетті. Бұл мысал буллингпен күресте тек заң қабылдау аз, оны нақты орындау және бақылау маңызды екенін айқын көрсетті.

Жалпы, 2024 жылдың екінші жартысында Қазақстан мектептерінде 1800 - ден астам «бейресми лидер» анықталды - бұлар сыныптастарына теріс әсер ететін, әлімжеттік жасаушы балалар. Сондай-ақ мектеп оқушылары арасында 70-тей бопсалау фактісі жолы кесілді [45]. Бұл көрсеткіштер өткен жылмен салыстырғанда жоғары. ІІМ өкілінің айтуынша, бопсалау деректерінің көбеюі бір жағынан профилактикалық жұмыстың жақсаруынан - яғни бұрын көлеңкеде қалып келген көптеген жағдайлар енді анықталып отыр. Екінші жағынан, мектептегі агрессия мәселесі расымен ушығып тұрғанын да жоққа шығаруға болмайды. Ұлттық ғылыми-зерттеу нәтижелері бойынша Қазақстанда оқушылардың шамамен 17,5%-ы кейде буллингке ұшырайтынын, 6,8%-ы айына бірнеше рет қатерлі мазаққа, қысымға тап болатынын көрсеткен. Әрбір жетінші оқушы (14%) өзгеге буллинг жасауға қатысқанын мойындайды екен [44]. Бұл деректер де мектеп ортасындағы буллингтің қаншалықты кең таралғанын растайды және енгізілген әкімшілік шаралардың өзектілігін дәлелдейді.

Кибербуллингтің салдары кейде орны толмас қайғылы жағдайларға әкелуі мүмкін. Мысалы, 2023 жылдың 10 айында Қазақстанда 169 кәмелетке толмаған өз-өзіне қол жұмсаған, бұл өткен жылға қарағанда 30%-ға көп. 15-17 жас аралығында суицид өсімі 45%-ға жетті. Әрине, әрбір суицидтің себебі сан алуан, бірақ мамандар көбіне мұндай жасөспірімдердің мектептегі немесе интернеттегі буллингтен соң күйзеліске ұшырағанын анықтайды. Буллинг баланың психикасына ауыр зардап әкеліп, депрессия, оқуға ынтасының төмендеуі, өз-өзіне қол жұмсауға бейімділікке итермелеуі мүмкін. Сондықтан мемлекет үшін буллингтің алдын алу - стратегиялық маңызы бар міндет.

Президент Тоқаев 2023 жылы буллинг мәселесін ерекше бақылауға алып, әрбір сигналға әрекет етуді тапсырды. Соның арқасында, әсіресе 2024 жылғы заңнамалық қатайтулардан кейін, жергілікті жерлерде әрбір анықталған буллинг оқиғасы бойынша іс қозғалып, кінәлілер жазаланып жатыр [44].

Интернет кеңістігінде онлайн тіл тигізу, қорлау бойынша да тәжірибені қарастырсақ: ҚР ІІМ өкілдері 2023 жылы әлеуметтік желілерде балағат

сөздер айту және қоғамдық тәртіпті бұзу фактілері бойынша полицияға шағымдар көбейгенін атап өтті. Мысалы, желіде ашық түрде біреуді қорлайтын сөз жазылса, жәбірленуші полицияға арыздана алады. Полиция ондай жағдайларда скриншот, видео сияқты дәлелдерді жинайды, қажет болса сараптама тағайындап, істі сотқа жолдайды. Егер әрекет жеке тұрғыда болса және жариялылық болмаса (біреуге жеке хатта балағаттау), онда Қылмыстық кодекстің 131-бабы бойынша іс қозғау мәселесі қаралуы мүмкін.

Ал әлеуметтік желідегі ашық жазбада тіл тигізу - қоғамдық тәртіпке әсер етсе - 434-баппен қаралып, айыппұл не қамау сұралады. 2023 жылғы наурыздан бастап ұсақ бұзақылық бойынша айыппұл 20 АЕК-ке көтерілгенін ескерсек, интернетте көпшілікті сыйламаушылықпен балағаттау қазір ~69 000 теңге айыппұл немесе 5-15 тәулік қамауға апарады. ІІМ өкілі Ш.Тұрлыбек 2023 ж. қаңтарда берген сұхбатында: «Егер әлеуметтік желіде балағат сөздер айтылса, айналадағы адамдарға сыйламаушылық танытып, тыныштығын бұзса, ол ұсақ бұзақылық ретінде қаралады» деп түсіндірді [40]. Демек, анонимді аккаунт арқылы болсын, шынайы атпен болсын, интернетте жұртты қорлап, боқауыз жазған адам жазасыз қалмайтынын полиция ресми мәлімдеуде. Дегенмен, анонимді аккаунттармен жұмыс істеу - құқық қорғау органдары үшін күрделі мәселе. Тәжірибеде көптеген қорлау, бопсалау фактілерінде құқық бұзушы жасырын атымен тіркеліп, жалған профиль қолданады. Мұндайда оны анықтау - техникалық күрделі процесс.

Заңгер Альбина Бахтиярқызы бұл туралы: «Интернетте жасалатын қылмыстарды ашу, оларды кім жасағанын білу өте қиын. Интернет - бүкіләлемдік желі. Қылмыскер басқа мекенжай, жалған аккаунт қолдануы мүмкін. Оларды анықтау тіптен қиын» деген [47]. Тергеушілерге IP-мекенжайлар, провайдер арқылы ақпарат алу қажет болады, ал егер құқық бұзушы шетелдік VPN, прокси пайдаланса, ізін кесу қиынға соғады. Соған қарамастан, қазақстандық полиция соңғы жылдары киберқылмыспен күрес бөлімшелерін күшейтіп, әлеуметтік желілермен байланыс орнатуда. Мысалы, 2022 жылы қабылданған заң негізінде Facebook, Instagram сияқты ірі платформалар Қазақстан тарапымен кибербуллинг бойынша жұмыс істеуге келісім берді - олар Гонконгтағы кеңселері арқылы қазақстандық уәкілетті органның өтініштерін қабылдап, 24 сағат ішінде қарауға дайын екенін мәлімдеген. Бұл да белгілі бір дәрежеде анонимдікпен күресуге, ең болмағанда зиянды контентті жоюға мүмкіндік береді. Бірақ толық шешім емес: халықаралық ынтымақтастық пен техникалық мамандану ауадай қажет.

Мәселені шешудің бір жолы ретінде кейбір елдер онлайн тіркеудің міндетті жүйесін енгізуге талпыныс жасаған. Оңтүстік Корея 2007 жылы «интернетті шын есіммен пайдалану» заңын енгізді - ірі сайттарда пікір жазу үшін азаматтар ЖСН (RRN) арқылы тіркелуі тиіс еді. Алайда бұл жүйе 2012 жылы Конституциялық сотта сөз бостандығын шектейді деп танылып, күшін жойды. Кореялық тәжірибе көрсеткендей, пайдаланушылар жай ғана шетелдік платформаларға көшіп кетіп, анонимділікті сақтап қала береді екен [48]. Сондықтан Қазақстан тікелей «барлығын құжатпен тіркеу» талабын қоймай, балама жолдарды таңдады: балаға қатысты буллинг контентін тез

өшіруді міндеттеу және платформалардың өкілдік ашуын талап ету (жоғарыда айтылғандай) [39]. Қазіргі таңда Қазақстанда барлық ұялы байланыс нөмірлері де жеке ЖСН-ға тіркеледі, бұл да белгілі дәрежеде анонимділікті азайтады (мысалы, WhatsApp нөмірі арқылы адамның иесін анықтау жеңіл). Алайда Telegram сияқты қызметтерде бұл механизм жүрмейді. Сондықтан құқық қорғау органдары анонимді буллингпен күресте көбіне цифрлық іздер мен халықаралық провайдерлерге сұрау салуға сүйенеді.

Қазақстан тәжірибесін тұжырымдай келе айтарымыз: кибербуллингке қатысты әкімшілік істер саны 2024 жылы айтарлықтай тіркелген (бірнеше айда 149 іс) [45], соттар алғашқы шешімдерін шығарды (ескерту, айыппұл түрінде) [46], ал кейбір жағдайларда жергілікті органдар әрекетсіздік танытса, қоғамдық бақылау оның орнын толтыруда [40]. Полиция тұрғындарға киберқорқытуға қарсы белсенді болуды насихаттауда: мысалы, желіде балағатталған азаматтар міндетті түрде скриншоттарды нотариус арқылы бекітіп қоюға кеңес беріледі, өйткені бұл кейін сотта айғақ болады [47]. Сонымен бірге, профилактика бойынша да жаңа жобалар іске қосылуда. 2024 жылы Астана мектептерінде финнің KiVa бағдарламасы пилоттық негізде іске асты, 9 өңірде отандық «DosbolLIKE» бағдарламасы сынақтан өтуде - бұлардың мақсаты мектепте достық атмосфера қалыптастырып, буллингтің алдын алу [40]. Яғни мемлекеттің күш-жігері тек жазалау емес, тәрбиелеу, мәдениет қалыптастыру бағытына да жұмсалып отыр.

Халықаралық әкімшілік-құқықтық реттеу тәжірибесі (Германия, Ұлыбритания, Оңтүстік Корея). Киберкеңістіктегі құқық бұзушылықтармен күресу - әлемнің көптеген елдері бетпе-бет келіп отырған ортақ мәселе. Қазақстан үшін шетелдердің тиімді тәжірибесін зерттеп, оны өз жағдайымызға бейімдеу маңызды. Әсіресе Германия, Ұлыбритания және Оңтүстік Корея соңғы жылдары заңнамалық тұрғыда бірқатар жаңашыл қадамдарымен танылды. Бұл елдерде кибербуллинг, онлайн жала жабу, желідегі жеккөрушілік секілді құбылыстарға қарсы құқықтық тетіктер енгізілген. Алайда әр елдің құқықтық жүйесіне қарай - бірі әкімшілік-құқықтық шараларға, бірі қылмыстық жазалауға, енді бірі аралас (реттеушілік) тәсілдерге жүгінеді. Төменде аталған үш елдің тәжірибесін қысқаша талдап, Қазақстанмен салыстырамыз.

Германия тәжірибесі. Германияда кибер құқық бұзушылықтармен күресте әкімшілік құқық пен реттеуші шаралар ерекше орын алады. Бұл ел жалпы Еуропадағы ең қатаң интернет-заңдардың бірі - 2017 жылы қабылданған «Әлеуметтік желілерді құқықтық қолдану туралы заң» (NetzDG) - арқылы белгілі. Бұл заң тікелей жеке тұлғаларды емес, ірі әлеуметтік желі компанияларын жауапкершілікке тартуға бағытталған. NetzDG талабы бойынша Германия аумағында 2 миллионнан астам қолданушысы бар кез келген әлеуметтік платформа (Facebook, YouTube, Twitter және т.б.) егер өз желісінде «айқын заңға қайшы контентті» анықтаса, оны 24 сағат ішінде өшіруге міндетті. Ал анық-қанығы бірден білінбейтін, даулы заңсыз контентті 7 күн ішінде тексеріп, шара қолдануы тиіс. Орындамаған жағдайда

компанияға өлшемді айыппұлдар салынады: бастапқыда 5 миллион еуро, ал жүйелі түрде бұзса - 50 миллион еуроға дейін өседі [48]. Бұл - әлемдегі ең ірі айыппұл көзделген нормалардың бірі. Мысалы, 2019 жылы Facebook Германияда заң бұзушылықтарды дұрыс есепке алмағаны үшін 2 миллион еуро айыппұл төлегені белгілі [49]. Германия осындай қатаң шара арқылы әлеуметтік желі компанияларын өз алаңдарындағы жеккөрушілік тілді, заңсыз зорлық-зомбылық шақырған жазбаларды, экстремистік материалдарды жедел жоюға мәжбүрлеуде. Германия әділет министрі Хайко Маас бұл заңға қолдау білдіре отырып: «Үлкен платформалар саяси қысымсыз өз міндеттерін орындамайтынын тәжірибе көрсетті» деп айтқан.

Расында, Facebook сияқты алпауыт компаниялар ұзақ уақыт бойы пайдаланушылардың шағымдарын жеткілікті қарамай, өшпенді контенттің кең таралуына жол беріп келген. Енді NetzDG заңынан соң, Германияда жүздеген модераторларды жұмысқа алып, тәулік бойы неміс сегментін сүзуге тура келді. Бұл заң кейбір құқық қорғау ұйымдарының сынына да ұшырады (шамадан тыс цензураға әкеледі деп алаңдаушылық білдіргендер болды) [48]. Дегенмен, Германия тәжірибесі басқа мемлекеттерге үлгі болды - Франция, Аустралия сияқты елдер ұқсас заң жобаларын қарастыра бастады.

Жеке адамдарға келсек, Германияда кибербуллинг жасаған тұлға тікелей әкімшілік жазаға тартылмайды, бірақ қылмыстық кодекстегі баптармен жауап береді. Мысалы, біреуді қорлап, намысына тигендерге «Қорлау» (§185 StGB) бабы бойынша айыппұл не бас бостандығын шектеу тағайындалуы мүмкін. Немесе интернет арқылы жүйелі қудалау жасағандар «Киберсталкинг» (§238 StGB) бабымен қылмыстық жауапқа тартылады [50]. Германия құқық жүйесінде буллингтің өзі жеке қылмыс ретінде бөлінбесе де, оның құрамына кіретін әрекеттер - қорлау, жала, қоқан-лоқы - түгел қылмыстық кодекспен жазаланады. Алайда Германияда кәмелетке толмағандар арасындағы буллингке әкімшілік-құқықтық сипатта мектепішілік, әлеуметтік шаралар көбірек қолданылады. Мысалы, федералдық Жастар ісі қызметі мектептерде медиация, кеңес беру жобаларын жүзеге асырады. Егер буллинг ауыр сипат алып, дене жарақатына не суицидке әкелсе, қылмыстық іс қозғалады (балалар қылмыстық жауапқа 14 жастан тартылады, 14-18 жаста арнайы ювеналдық соттар қарайды). Сонымен, Германия үлгісінің негізгі ерекшелігі - платформалардың әкімшілік жауапкершілігін қатаңдату. Бұл мемлекеттің көзқарасы бойынша, интернеттегі қауіпті контентпен күресте тек жеке тролльдерді қудалай бермей, оның таралу алаңын да тізгіндеу қажет.

Қазақстан да 2022 жылғы балаларды қорғау заңында осындай принципті ішінара енгізді (платформалар өкілдік ашып, зиянды жазбаларды жоюға міндетті) [39]. Алайда біздің елде әзірге ірі айыппұлдар салынған жоқ, көбіне ескертумен шектелуде. Болашақта, Германиядағыдай, орындамағандарға миллиондаған айыппұл салу мәселесі туындауы мүмкін.

Ұлыбритания тәжірибесі. Ұлыбританияда кибер құқық бұзушылықтарға қарсы құқықтық шаралар соңғы жылдары едәуір жаңарды. Бұрын Ұлыбританияда арнайы «кибербуллинг» деген заң болмады, бірақ интернеттегі көптеген зиянды әрекеттерге қолданылатын жалпы заңдар бар

еді. Мысалы, 1997 жылғы Құдалау және қорғау заңына (Protection from Harassment Act) сәйкес, қайталанған қорқыту, хабарламалар арқылы мазалау - қылмыстық теріс қылық. 1988 жылғы Зиянды коммуникациялар туралы заң (Malicious Communications Act) бойынша, электрондық байланыс құралдары арқылы қорлайтын, үрей туғызатын хабар жіберу - заңсыз, ол үшін 6 айға дейінгі түрме жазасы не айыппұл қарастырылған [51]. Сондай-ақ 2003 жылғы Байланыс туралы заңның 127-бабы қоғамдық электрондық желілерде «өте дөрекі, әдепсіз немесе жалған ақпарат таратуға» тыйым салады - бұл да тікелей интернеттегі троллингке қарсы қолданылып келген норма. Осындай әртүрлі баптарды пайдалана отырып, британ полициясы талай желі бұзақыларын, әсіресе Twitter, Facebook-та жеккөрушілік тіліне жол бергендерді жауапқа тартып келді. Бірақ құқық қорғаушылар мұндай заңдардың шашыраңқы екенін, кешенді шешім жоқтығын айтып сынаған.

Осы олқылықтың орнын толтыру үшін Ұлыбритания 2023 жылы кешенді «Online Safety Act 2023» (Интернеттегі қауіпсіздік туралы заң) қабылдады. Бұл заң интернет платформаларына қатысты «қамқорлық міндетін» (duty of care) бекітіп, Ofcom реттеушісіне кең өкілеттік берді. Енді ірі әлеуметтік желілер балаларды зиянды контенттен қорғау және жалпы заңсыз контентті алып тастау бойынша проактивті шаралар атқаруға міндетті. Егер олар осы міндеттерді орындамаса, Ofcom оларға өте ірі әкімшілік айыппұлдар сала алады - £18 миллион немесе жаһандық жылдық айналымының 10% мөлшеріне дейін, қайсысы көбірек болса. Мысалы, егер көпмиллиардтық табысы бар Meta (Facebook) заңды бұзса, онда 10% айналымы - ондаған миллион фунт айыпқа кесілмек. Заң тіпті ең қатерлі жағдайларда платформаларды Ұлыбритания аумағында бұғаттау құзыретін Ofcom-ға береді [52]. Бұл акт сондай-ақ жаңа қылмыстық құқық бұзушылықтарды енгізді: киберфлешинг (ұятсыз суреттерді рұқсатсыз тарату), эпилепсия троллингі (эпилепсиясы бар адамдарға жарқылдар жіберіп, ұстамасын қоздыру) сияқты заманауи теріс әрекеттерге тыйым салынып, олар үшін қылмыстық жауаптылық енгізілді. Заңда «Балаларға зиянды контент» ұғымы айқындалып, оған порнография, зорлықты насихаттау, қауіпті челендждерге үгіттеу, сондай-ақ буллинг және жеккөрушілік мазмұн жатқызылды. Платформалар балаларды осындай контенттен барынша қорғауға тиіс.

Практикада бұл не деген сөз? Мысалы, Instagram алгоритмдері буллинг немесе өзіне қол жұмсауға итермелеу белгілері бар жазбаларды балаларға көрсетпеуі керек; ал YouTube балалар үшін қауіпті челлендж-видеоларды жоюы тиіс. Заң талаптарын орындамаған платформалар жоғарыда айтылған миллиондық айыппұлдарға тап болады. 2024 жылдың басынан бастап бұл талаптар кезең-кезеңімен күшіне ене бастады. Ofcom алғашқы мониторингтер жүргізіп, Twitter (X) сияқты кейбір желілердің дайындықтарына ескерту жасады. Ұлыбритания тәжірибесінің ерекшелігі - реттеуші мен компаниялардың ынтымақтастығына мән беруі. Ofcom кодекстер әзірлеп, платформаларға нақты қандай шаралар керек екенін көрсетеді. Мысалы, жас ерекшелігіне сай верификация (балалар мен ересектерді ажырату), мазмұнды сүзу, қолданушыларға шағым беру оңай

жолдарын жасау. Сондай-ақ заң журналистік және саяси пікірлерге тым қатты цензура болмауын да ескерген (платформалар маңызды қоғамдық мазмұнды өшіріп тастамауы керек деген ережелер бар) [52].

Осылайша, Ұлыбритания да Германияға ұқсап, платформалардың жауапкершілігін күшейтіп отыр. Алайда, әкімшілік жауапкершілікпен бірге кейбір қылмыстық баптарды да жаңартты. Мысалы, «кібербуллинг» деген атаумен арнайы бап енгізілмесе де, зорлық-зомбылыққа шақырғандар, қорқытқан комментарий жазғандар бұрынғыдай қылмыстық жазаға тартылуда. 2022 жылы Лондон соты 18 жастағы жасөспірімді Instagram арқылы басқа бір қызды өліммен қорқытқаны үшін 6 ай түрме жазасына кесті - бұл Malicious Communications Act бойынша өткен іс. Сол сияқты танымал тұлғаларды Twitter-де қорлаған бір қолданушыға сот ірі көлемде айыппұл салды (Public Order Act аясында).

Қазақстан Ұлыбританиядан үйренетін тұстар - балаларға зиянды контентті құқықтық анықтау және реттеу. Бізде де қазіргі кезде порнография, суицидті насихаттау сияқты нәрселерге тыйым бар, бірақ «балаларға психологиялық зиянды контент» түсінігі нақты емес. Ұлыбритания заңында буллинг сол зиянды контенттің түрі ретінде көрсетіліп, платформаларға онымен күресу міндеттелген. Қазақстан да 2022 жылғы талабында әлеуметтік желілерге балаларға қатысты буллинг жазбаларын жоюға 24 сағат берді [39].

Бұл жағынан заңнамамыз UK Online Safety Act нормаларына жақын деуге болады, тек бізде оны орындау механизмі әлсіздеу (Ofcom секілді дербес реттеуші орган жоқ, тек министрлікке шағымдану қарастырылған).

Оңтүстік Корея тәжірибесі. Оңтүстік Корея - кибербуллинг және интернеттегі зиянды контент мәселесін ерте көтерген елдердің бірі. Әсіресе жұлдыздардың өз-өзіне қол жұмсау оқиғалары қоғамда үлкен дүмпу туғызып, билікті шаралар қабылдауға итермелеген. 2007 жылы атышулы Чхве Чжинсильдің (танымал актриса) суицидінен кейін үкімет «Интернетте нақты есіммен тіркелу» жүйесін енгізді [52]. Бұл жүйе бойынша үлкен портал-сайттарда пікір жазу үшін азамат өзінің шын аты-жөнін және ұлттық ID нөмірін растауы керек болды. Сол кезде үкімет өкілдері «бұл анонимдердің жалған өсек таратып, қорлауын азайтады» деп үміт артты. Алайда, жоғарыда атап өткендей, бұл шара тек уақытша нәтиже берді де, кейіннен теріс әсерлері анықталды. Пайдаланушылар анонимділікті сақтау үшін Yahoo, Facebook сияқты шетелдік платформаларға ауысып кетті. ал жергілікті сайттар оқырманын жоғалтты. Сонымен бірге, нақты есіммен кіру талаптары дербес деректердің ұрлануына әкелді - хакерлер 35 миллион корей қолданушысының жеке мәліметтерін ұрлап алған оқиға болды. Ақыры, 2012 жылы Оңтүстік Корея Конституциялық соты бұл заңды «демократияға зиян, сөз бостандығын шектейді» деп танып, күші жойылды [48].

Дегенмен, Оңтүстік Корея басқа бағытта заңдарын күшейтті. Онда «Ақпарат және коммуникация желілерін пайдалану туралы заң» бар (бұл заң коммуникация саласын реттейді). Соған 2008 жылы енгізілген түзетулер бойынша онлайн қорлау мен жала жабу қылмыстарының жазасы қатайтылды. Корей заңында ерекшелік - егер біреуді шындыққа сәйкес ақпаратпен

масқараласа да, ол қылмыс болып саналады. «Кибер жала (арандату)» үшін шын болса 3 жылға дейін, жалған болса 7 жылға дейін бас бостандығынан айыру жазасы белгіленген [52]. Бұл - әлемдік стандарттардан қатты жоғары жаза, сондықтан кейде сынға да ұшырайды. Алайда, корей қоғамы интернеттегі жалған өсек-аяңның зиянын көріп отырғандықтан, мұндай қатаңдықты қолдаушылар да көп. Мысалы, 2019 жылы K-pop жұлдызы Суллидің трагедиясынан соң (ол интернеттегі ұзақ мерзімді қудалаудан соң өмірімен қоштасты деп айтылады), қоғам талаптарынан кейін «Сулли заңы» деп аталған заңнамалық өзгерістер пакеті дайындалды. 2020 жылы Ұлттық Ассамблея сол өзгерістерді қабылдап, медиа және коммуникация заңдарына түзетулер енгізді. Олардың бірі - портал сайттардағы анонимді комментарийлерді басқару тәртібін күшейту. Кейбір ірі порталдар (Daum, Naver) жаңалықтарға пікір жазу функциясын уақытша жауып тастады немесе тек расталған аккаунттарға рұқсат берді. Мектептерде де өзгерістер болды: 2019 жылдан бастап барлық орта мектептерде кибербуллингтің алдын алу бойынша білім беру бағдарламасы енгізілді. Яғни оқу жоспарына кибермәдениет, онлайн этика тақырыптары кіріктірілді.

Оңтүстік Кореяда буллингті тоқтатудың әлеуметтік тетіктері жақсы дамыған. Мектептерде 2004 жылдан бері «Мектептегі зорлық-зомбылыққа қарсы заң» қолданыста (School Violence Prevention Act). Сол заңға сәйкес әр мектепте зорлық-зомбылықты алдын алу комитеті бар. Қандай да бір буллинг оқиғасы болса, бұл комитет оны жан-жақты қарап, шешім қабылдайды: буллер оқушыға кеңес беру, тәртіп жазасын беру (мектептен уақытша шығару, басқа мектепке ауыстыруға дейін), ал жәбірленушіге қажет болса психологиялық көмек ұйымдастырады [53]. Комитетте мұғалімдермен бірге міндетті түрде полиция және ата-аналар өкілдері қатысады. Полиция тек ең ауыр, қылмыстық сипат алған істерге араласады (мысалы, ақша бопсалау, дене жарақатын салу). Корея жүйесі - буллингті көбіне оқу орны деңгейінде шешуге тырысады, сотқа жеткізбеуге мән береді. Тек егер тараптар келісімге келмей, жәбірленуші отбасы қатаң жаза талап етсе немесе оқушы 14 жастан асқан, әрекеті қылмыс құрамына кірсе - ювеналдық сотқа жібереді.

Сонымен қатар, Оңтүстік Кореяда онлайн-платформалардың да міндеті күшейтілген. Мысалы, жергілікті ең ірі іздеу порталы Naver мен Kakao компаниясы өз ресурстарында қолданушыларды псевдониммен де, шын есіммен де пікір жазу мүмкіндігін қалдырғанымен, агрессивті сөздер мен тіл тигізуді автоматты сүзгіден өткізіп, өшіріп отыратын жүйе енгізді. Сондай-ақ 2021 жылы Кореяда Адам құқықтары комиссиясы ұсынысымен ірі әлеуметтік желілерге «дислайк» батырмасын алып тастау немесе аноним пікірлерді шектеу жөнінде кеңес берілді - бұл да кибербуллингтің психологиялық қысымын азайту шарасы ретінде. Кейбір телебағдарламалар өз сайттарында көрермендер пікір қалдыра алмауы үшін комментарий функциясын өшірді (телеарна жаңалықтары сайтында тек оқуға болады, пікір жазу жоқ). Мұның бәрі Сулли және өзге жұлдыздардың қайғылы оқиғаларынан соң іске асқан өзгерістер. Қазақстан Оңтүстік Кореяның тәжірибесінен мыналарды үлгі ете алады: комплексді тәсіл - тек заңмен жазалау емес, бүкіл қоғам болып қарсы

тұру. Мәселен, Кореяда «Sunfull» деген қозғалыс бар, еріктілер интернетте көңілсіз, өзіне қол жұмсағысы келетін адамдарға жылы сөздер қалдыруды мақсат етеді (Sunfull - «күншуақ комментарий» дегенді білдіреді). Мыңдаған студент, мектеп оқушысы осы қозғалысқа қатысып, арнайы сайттарда қолдау сөздерін жазып отырады. Бұл сияқты бастамалар да буллингке қарсы күресте маңызды рөл ойнайды - ортада мейірім мәдениетін қалыптастыру.

Үш елдің (Германия, Ұлыбритания, Оңт.Корея) тәжірибесін қорытсақ, барлығында ортақ тренд - интернет компаниялардың жауапкершілігін көтеру және балаларды қорғауды заңдастыру. Германия мен Ұлыбритания мұны әкімшілік айыппұл арқылы жүзеге асырса, Корея нақты есім ережесі сынды эксперименттер жасап, кейін басқа тәсілдерге көшті. Ал кибербуллингтің өзін қылмыстық жазалау мәселесінде айырмашылықтар бар: Еуропада негізінен жазалаудың қажеті жоқ деп, оны әлеуметтік мәселе ретінде қарау басым (бірақ ауыр жағдайларда қорлау, зорлық, суицидке итермелеу баптарымен қылмыстық іс қозғайды). Кореяда керісінше, ауыр жала және қорлау үшін бірден қатал жаза беріледі (жоғарыда айтылған 7 жылға дейін түрме жазасы мысалы) [52]. Қазақстан қазіргі таңда осы екі аралық позицияда: буллингті жеке құрам ретінде әкімшілік құқық бұзушылыққа жатқызды (яғни қылмыс деңгейіне көтерген жоқ, керісінше оны жеңіл құқық бұзушылық деп санап, ата-аналар арқылы шара қолданады) [42]. Бұл Батыс Еуропа үлгісіне жақынырақ. Сонымен бірге, қорлау, бопсалау, суицидке итермелеу сияқты ауыр түрлері бұрынғыша қылмыстық жазада қалып отыр.

Халықаралық тәжірибе көрсеткендей, кибербуллингпен күресте тек заң жазасы нәтиже бермейді, оған қоса міндетті түрде білім беру, қоғамдағы сана өзгерісі, платформалармен әріптестік керек. Сол себепті Қазақстан да қазірден бастап мектептерде буллингтің зияны туралы сабақтар өткізіп, ата-аналарға семинарлар ұйымдастыруда [54]. Ұлыбританияда әр мектепте мінез-құлық саясатына буллингтің барлық формасын (соның ішінде онлайн) болдырмау шаралары қосылуы заң талабына айналған [55]. Бізде де Білім министрлігінің 2023 жылғы бұйрығымен мектеп ішкі тәртіп ережелеріне буллингтің алдын алу пункттері енгізілді.

Авторлық көзқарас және ұсыныстар. Жоғарыда талданған материалдар негізінде, Қазақстанда Кибер құқық бұзушылықтардың әкімшілік-құқықтық салдары бойынша заңнамалық база құрылып, алғашқы практикалық қадамдар жасалғанын көреміз. Дегенмен, бұл бағытта әлі жетілдіретін тұстар бар. Өзімнің авторлық көзқарасымды білдіре отырып, бірнеше ұсыныста алға тартқым келеді. Біріншіден, кибербуллингке қарсы жауапкершілікті кеңейту мәселесі. Қазіргі 127-2-бап тек кәмелетке толмағандарды буллингтен қорғайды, яғни жәбірленуші бала болғанда қолданылады. Ал егер онлайн буллингтің құрбаны ересек азамат болса, оған заң тікелей қорған болып тұрған жоқ. Мұндайда жәбірленуші Қылмыстық кодекстегі 131-бап (қорлау) бойынша жеке тәртіпте шағымдануы қажет немесе азаматтық тәртіпте моральдық зиян өндіруі мүмкін. Автордың ойынша, Қазақстан болашақта кибербуллингтің жас ерекшелігін алып тастап, жалпы құрамын енгізуді қарастыруы керек. Яғни кез келген адамға (жасына қарамастан) қатысты

жүйелі кибербуллинг жасағаны үшін әкімшілік жауапкершілік белгілеу орынды. Әрине, бұл белгілі бір дәрежеде қорлау бабымен қабаттасады, бірақ айырмасы - буллинг жүйелі, көп мәрте жасалатын әрекет екенін ескеру.

Мысалы, топ болып бір азаматты онлайн түрде ұзақ уақыт бойы қорлау жағдайлары кездесіп жатады (кейде жұмыс орнында, кейде көршілер арасында және т.б.). Осындай оқиғаларда 127-2-бапты аналогиямен қолданып, жәбірленуші жасы кәмелетке толса да іске тартуға болатындай өзгеріс ұсынылады. Бұл әлемдік трендке сай: кей елдерде «кішігірім агрессия» ұғымдары пайда болып, workplace bullying, cyber harassment бойынша ересектер де қорғалуда.

Екіншіден, 127-2-бап санкцияларын қайта қарау. Бапта қайталама бұзушылық үшін тек айыппұл (30 АЕК) көзделген, ал әкімшілік қамақ қарастырылмаған [42]. Бұл гуманды қадам, әрине - ата-ананы 20 тәулікке қамау баласының буллингін тоқтатпауы мүмкін. Дегенмен, кей жағдайларда буллинг аса ауыр зардапқа (мысалы, жәбірленушінің өзіне қол салуына әрекеттенуіне) соқтырса, ата-анаға немесе тікелей кінәлі адамға (18 жас болса) қамау жазасын беру мүмкіндігін заңда қалдырған дұрыс деп есептеймін. Мүмкін оны бірден бапта емес, жалпы ӘҚБтК-нің «ажыратушы бабында» көрсетуге болады: егер әкімшілік құқық бұзушылықтың зардабы ауыр болса, судья айыппұлды қамақпен алмастыра алады деген секілді.

Бүгінгі редакция бұл мүмкіндікке жол бермейді. Әрине, ауыр зардап болса - іс қылмыстық бапқа ауысады деуге болады (ҚК-тің 105-бабы - өзін-өзі өлтіруге жеткізу, 3 жылға дейін бас бостандығынан айыруды көздейді). Бірақ 105-бапты дәлелдеу қиын: тікелей себеп-салдар байланысын анықтау күрделі. Сондықтан әкімшілік деңгейде ондай жайттарды қамаумен жазалау (қысқа мерзімді болса да) әділдік орнатуға сеп болар еді.

Үшіншіден, кәмелетке толмаған буллерлермен жұмыс жөнінде. Қазіргі үлгі - 12-15 жастағы буллер үшін ата-ана жазаланумен шектеледі [42]. Бұл жағдайда бала өзі жауапкершіліктің дәмін сезбеуі мүмкін. Ата-анасы айыппұл төлегенін түсінбеуі де ықтимал. Сондықтан әкімшілік жазадан бөлек, тәрбиелік мәжбүрлеу шараларын енгізу маңызды. Мысалы, сот 127-2-баппен істі қарағанда, буллинг жасаған жасөспірімді міндетті психологиялық түзету курсынан өтуге немесе қоғамдық жұмыс (volunteering) атқаруға бағыттай алуы керек. Қазір заңнамада ондай тетік қаралмаған. Бірақ отандық соттар кейде ұқсас практика қолдануда: мысалы, Қостанай соты шешімінде ата-ана бұрын «ауызша ескертілген» деп жазылғанын көрдік, яғни профилактикалық әңгіме жүргізілгенін сот хаттамаға кіргізген. Сол сияқты баламен психологтың жұмыс істеуі, оның мінез-құлқына мониторинг жүргізу жағын заңдастыру артық емес. Ювеналды соттар мектеппен, ювеналды полициямен тізе қоса отырып, балаға екінші мүмкіндік беру үшін оны түзетуге тырысуы керек. АҚШ, Канада сияқты елдерде «restorative justice» деген ұғым бар - кәмелетке толмаған құқық бұзушы жәбірленушімен бірге арнайы сессияларға қатысып, кесірін түсінуге және кешірім сұрауға ынталандырылады. Қазақстанда да осындай медиация элементтерін буллинг істерінде қолдану өте орынды болар еді. Мысалы, Оралдағы істе жәбірленуші

отбасы татуласудан бас тартты [46], себебі екі жыл бойы жиналған реніш бар. Егер мектеп басында-ақ медиация жасалып, конфликт шешілгенде, мүмкін созылмас еді. Сондықтан, автор ретінде мектеп медиациясын күшейту, әр буллинг фактісін сотқа жеткізбей тараптарды татуластыру жұмыстарын жүйелеу керектігін ұсынар едім.

Төртіншіден, анонимділікпен күрестің техникалық мүмкіндіктері. Дүниежүзінде түбегейлі шешім табу қиын болса да, Қазақстан кемінде барлық отандық интернет-форумдар мен сайттарда тіркелу үшін ЭЦҚ немесе SMS-верификацияны міндеттеуді енгізе алады. Қазіргі уақытта әлеуметтік желілердің көбі шетелдік, оларға дәті бармай отырмыз. Бірақ өзіміздің ақпараттық алаңда (мысалы, Nur.kz, Massaget.kz сияқты ірі порталдарда) пікір жазуға бірыңғай Egov жүйесі арқылы кіру талабы қойылса, фейктер саны күрт азаяр еді. Бұл үшін «Интернеттегі анонимді пікір қалдыру шарттары» деген арнайы Ұлттық қауіпсіздік комитеті немесе Ақпарат министрінің бұйрығын шығаруға болар еді. Алайда, бұл қадам сөз бостандығын шектейді деп сыналуы да ықтимал (Корея тәжірибесін еске алсақ). Сондықтан оны өте сақтықпен, кезеңдеп қарастыру керек. Бәлкім, тек балаларға қатысы бар платформаларда (Балаларға арналған форумдар, BalaHub т.б.) заңды өкіл рұқсатымен ғана жазу деген ереже енгізсе дұрыс па деп ойлаймын. Қайткен күнде де, анонимділіктің артында тығылған құқық бұзушыларды анықтау үшін полицияның материалдық-техникалық базасын нығайтып, кибертергеушілерді көбейту қажет. Мысалы, әр облыста Цифрлық даму министрлігі, ІІМ және ҰҚК бірлесіп «киберпатруль» топтарын құрса - олар TOR, VPN қолданса да, қазақстандық сегменттегі буллерлерді анықтаумен айналысса деймін. Бұл өз кезегінде бюджетті талап етеді, бірақ балаларын буллингтен қорғау - мемлекеттің стратегиялық міндеті, сондықтан қаржы аямауға тұрарлық.

Бесіншіден, қоғамдық сана және білім беру. Кибербуллинг түбінде - құқықтық емес, әлеуметтік-психологиялық құбылыс. Онымен күресте заң қанша күшті болса да, ең басты рөлді мектеп пен отбасы атқарады. Сондықтан, ұсыныс: барлық орта білім беру бағдарламасына «Интернет мәдениеті және этика» атты арнайы курс енгізу. Онда оқушыларға кибербуллингтің зардаптары, басқаға зиян келтірмеу, желідегі қауіпсіздік туралы түсіндірілсе. Қазір информатика сабақтарында қауіпсіздік тақырыбы қозғалатыны рас, бірақ негізінен вирустар мен пароль қоюдан аспайды.

Ал киберқорқыту, желідегі зорлық мәселелері көбіне сынып сағаттарында ғана үстірт айтылады. Бұл жеткіліксіз. Ұлыбританияда Anti-Bullying Alliance тәрізді ұйымдар оқушыларға арнайы тренингтер өткізеді, сол сияқты, бізде де Үкіметтік емес ұйымдармен бірлесіп, тұрақты негізде буллингке қарсы кампаниялар жүргізілуі шарт. Әкімшілік құқық бұзушылық туралы заң - қорқытушы фактор, бірақ ең жақсысы - құқық бұзушылықтың алдын алу, болдырмау. Сол үшін балалардың цифрлық сауатын емес, «цифрлық ізгілігін» арттыру қажет. Интернетте өзіңді қалай ұстау керек, қалай дауды мәдениетті шешу керек деген тәрбие берілсе, құқық бұзушылықтар да азаяды.

Алтыншыдан, құқық қолдану ашықтығы және мониторинг. Қазақстанда буллинг туралы істер сотта жабық режимде қаралуы мүмкін (балалар қатысқандықтан). Дегенмен, қоғам үшін жалпы үрдістерді, статистиканы біліп отыру маңызды. Жыл сайын Бас прокуратура, ІІМ немесе Білім министрлігі буллинг бойынша есептерді жариялап тұрса деймін. Мысалы, қанша іс тіркелді, қаншасы ескерту, қаншасы айыппұлмен аяқталды, қай өңірлер көш басында - осыларды ашық хабарлау керек. Бұл бір жағынан ата-аналарға ескерту болады (өз балаңызды қадағалаңыз, әйтпесе осындай іс түсіп қалады), екінші жағынан жергілікті органдар арасында бәсекелестік тудырады (кімнің мектебі тәртіпті дегендей). Polisia.kz сайтында 2024 жылы 150 буллинг фактісі тіркелді деп хабарланды [45], сол сияқты 2025 жылы ол сан 300-ге жетсе немесе азайса - себебін талдап, тиісті қорытынды шығару керек. Ұлыбританияның Ofcom-ы жыл сайын «Интернеттегі қауіпті тәжірибелер» деген баяндама шығарады, онда балалардың қандай желіде жиі буллингке ұшырайтыны сияқты мәліметтер бар. Бізге де дәл осындай аналитика қажет.

Жетіншіден, халықаралық ынтымақтастық. Кибер құқық бұзушылықтар трансшекаралық сипатта жиі болады. Қазақстандық баланы шетелде отырып басқа мемлекет азаматы қорлауы мүмкін немесе керісінше. Мұндайда Интерпол мен басқа елдердің құқық қорғау органдарымен тығыз жұмыс керек. Қазіргі таңда Қазақстанның ішкі істер органдары Ресей, Қытай, АҚШ-тағы ірі платформалармен көбіне өзара түсіністік меморандумдары негізінде әрекет етуде. Оларды нақты құқықтық арнаға түсіру үшін мемлекетаралық келісімдер жасау ойлануға тұрарлық. Мысалы, Еуропол аясында «кибербуллинг» бөлек талқыға салынып, ортақ стандарттар қабылданса, тамаша болар еді. Әлбетте, бұл ұсыныс біздің билік деңгейінен жоғары, жаһандық сипатқа ие.

Қорытындылай келе, Қазақстанда кибер құқық бұзушылықтарға әкімшілік-құқықтық шара қолдану тетігі енді ғана қалыптасып келеді. Заңнамалық негіз қаланды, енді оны тиімді іске асыру - басты міндет.

Халықаралық тәжірибе бізге екі нәрсені үйретеді: біріншіден, жылдам бейімделу (технология өзгерген сайын заңды жаңарту), екіншіден, жүйелі кешенді шаралар (білім, технология, құқық қолдану, қоғам).

Қазақстан осы бағытта қадам басып жатыр, дегенмен жоғарыда ұсынылған идеялар (балаларды ғана емес, ересектерді де буллингтен қорғау, жазалау мен тәрбиені үйлестіру, алдын алу жұмыстарын институционализациялау) іске асса, еліміздегі кибер құқық бұзушылықтар едәуір төмендеп, Интернет кеңістігі баршамыз үшін қауіпсізірек болар еді деп сенемін. Бұл тек құқық қорғау не сот органдарының жұмысы емес, тұтас қоғамның зор міндеті. Балалардың бақытты, кибербуллингсіз балалығы - жарқын болашақ кепілі екенін ұмытпайық.

# 2 КӘМЕЛЕТКЕ ТОЛМАҒАНДАРДЫҢ КИБЕР ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРЫН ӘКІМШІЛІК-ҚҰҚЫҚТЫҚ РЕТТЕУДІҢ ҰЛТТЫҚ ЕРЕКШЕЛІКТЕРІ

## 2.1 ҚР заңнамасындағы киберкеңістікке байланысты құқық бұзушылықтарды реттеу ерекшеліктері

Киберкеңістіктегі құқық бұзушылықтардың табиғаты және оларды құқықтық реттеудің маңызы. XXI ғасырдағы қарқынды цифрландыру нәтижесінде қылмыс жасау алаңы ретінде киберкеңістік (виртуалды ақпараттық орта) ерекше орын алды. Компьютерлік жүйелер мен Интернет желісінің кең таралуы дәстүрлі қылмыстардың жаңа тәсілдермен жасалуына жол ашып, сондай-ақ мүлде жаңа сипаттағы құқық бұзушылықтардың пайда болуына әкелді. Киберкеңістіктегі құқық бұзушылықтардың басты ерекшелігі - олардың физикалық шекаралары жоқ, электрондық нысанда жасалып, қаскүнемдер анонимділігімен және ғаламдық қолжетімділігімен ерекшеленеді. Мысалы, интернеттегі “виртуалды тұлғаны” жауапқа тартудың күрделілігі алаяқтықтың, балаларды түрлі қылмыстық мақсатта пайдаланудың және алдаудың жаңа мүмкіндіктерін туындатуда [56, с. 67].

Шын мәнінде, киберқылмыскерлер өз әрекеттерін әлемнің кез келген нүктесінен жүзеге асыра алады, бұл ұлттық юрисдикциялардың мүмкіндіктерін шектейді әрі құқық қорғау органдары үшін орасан қиындықтар туғызады.

Киберкеңістіктегі құқық бұзушылықтарды шартты түрде бірнеше санатқа бөлуге болады: 1) компьютерлік ақпараттық жүйелерді мақсат ететін қылмыстар (мысалы, компьютерлік желілерге заңсыз ену, зиянды бағдарламалар тарату, деректерді бұрмалау немесе жою); 2) интернетті құрал ретінде пайдаланатын қылмыстар (мысалы, интернет-алаяқтық, банктік шоттарға заңсыз қол жеткізу, онлайн алаяқтық жолмен мүліктік зиян келтіру); 3) онлайн-контентке байланысты құқық бұзушылықтар (мысалы, экстремистік немесе террористік мазмұнды тарату, кәмелетке толмағандарға зиянды ақпаратты жариялау, порнографиялық материалдарды, оның ішінде балалар порнографиясын тарату) және 4) жеке тұлғаларға қарсы киберқылмыстар (кибербуллинг, онлайн қорқыту, жеке өмірге қол сұғу сияқты әрекеттер). Әрине, бұл санаттар көбіне өзара қабаттасып жатады; мысалы, балаларға қатысты сексуалдық сипаттағы материалдарды интернетте тарату - әрі контенттік құқық бұзушылық, әрі ақпараттық жүйелерді пайдалану арқылы жасалатын қылмыс.

Қазақстан Республикасында ақпараттық технологиялардың кең қолданылуы нәтижесінде соңғы жылдары киберқылмыстардың үлесі айтарлықтай өсіп отыр. Мәселен, елімізде интернет пайдаланушылардың саны жыл сайын артып келеді, бұл бір жағынан экономикалық және әлеуметтік прогресс көрсеткіші болса, екінші жағынан - киберкеңістіктегі құқық бұзушылықтардың көбеюіне жағдай жасайды. Осындай жаңа қауіп-қатерлерге қарсы тұру үшін мемлекет кешенді құқықтық шаралар қабылдауы

қажет. Киберқауіпсіздікті қамтамасыз ету мен ақпараттық инфрақұрылымды қорғау қазіргі заманғы цифрлық әлемдегі мемлекеттің ең маңызды міндеттерінің біріне айналды, сондықтан Қазақстанда 2017 жылдан бастап «Қазақстанның киберқалқаны» деп аталған кибер қауіпсіздік тұжырымдамасын іске асыру басталды [57]. Құқықтық салада бұл міндетті жүзеге асыру - жаңа заңдар қабылдау, қолданыстағы нормативтік актілерге өзгерістер енгізу, халықаралық ынтымақтастықты дамыту және құқық қорғау органдарының техникалық-кадрлық әлеуетін нығайту арқылы мүмкін болмақ.

Киберкеңістіктегі құқық бұзушылықтарды тиімді реттеу үшін Қазақстан Республикасы заңнамасының дамуы халықаралық үрдістерге сай жүруде. Дүниежүзілік тәжірибеде киберқылмыспен күрес бойынша Будапешт конвенциясы сияқты негізгі халықаралық актілер бар, оған көптеген елдер қосылған. Қазақстан да бұл Конвенцияға қосылу үшін шақыру алған, соған сәйкес ұлттық заңнаманы халықаралық стандарттарға үйлестіру жұмыстары жүргізілуде. Мысалы, 2014 жылғы жаңа Қылмыстық кодекске ақпараттық қауіпсіздікке қарсы қылмыстар бойынша арнайы тарау енгізіліп, онда заңсыз қол жеткізу, жүйеге немесе деректерге зиян келтіру, құрылғыларды заңсыз пайдалану тәрізді киберқылмыс құрамдары бекітілді. Сол сияқты қылмыстық іс жүргізу заңнамасы мен жедел-іздестіру қызметі туралы заңдарда электрондық дәлелдемелерді жинақтау мен пайдалану бойынша кейбір ережелер көзделген [58]. Дегенмен, киберкеңістік саласындағы құқық бұзушылықтардың қарқыны мен күрделілігі ұлттық заңнама мен құқық қолдану тәжірибесін үнемі жетілдіріп отыруды талап етеді. Төменде Қазақстан Республикасының киберкеңістікке байланысты құқық бұзушылықтарды реттейтін негізгі заңнамалық актілері, олардың мазмұны мен ерекшеліктері талданады, сондай-ақ осы саладағы құқық қолдану практикасы мен мәселелер қарастырылады.

Киберкеңістікке қатысты құқық бұзушылықтарды реттейтін негізгі нормативтік құқықтық актілер. Қазақстан Республикасының заңнамалық базасы киберқауіпсіздік пен киберқылмыспен күресуге қажетті көптеген актілерден тұрады. Олардың қатарына кодекстер (Әкімшілік құқық бұзушылық туралы кодекс, Қылмыстық кодекс, Қылмыстық процестік кодекс), арнайы заңдар («Ақпараттандыру туралы», «Байланыс туралы», «Баланың құқықтары туралы», «Дербес деректер және оларды қорғау туралы», «Құқық қорғау қызметі туралы» және т.б.), сонымен бірге стратегиялық құжаттар («Киберқауіпсіздік тұжырымдамасы» және оны іске асыру жөніндегі жоспарлар) кіреді. Әрі қарай осы актілердің маңызды тұстары мен өзара байланысы жан-жақты сипатталады.

Әкімшілік құқық бұзушылық туралы кодекс киберкеңістікте жиі кезігетін құқық бұзушылықтардың кейбіріне жауапкершілік белгілейді. Атап айтқанда, жеке деректерді заңсыз жинау, өңдеу немесе тарату және дербес деректерді қорғау талаптарын бұзу әкімшілік жауаптылыққа алып келеді. ӘҚБтК-нің 79-бабына сәйкес дербес ақпаратты заңсыз жинағаны, заңсыз өңдегені немесе қорғау шараларын сақтамағаны үшін айыппұл салынуы мүмкін. 2025 жылғы наурызда қабылданған заңнамалық түзетулермен мұндай құқық

бұзушылықтар үшін айыппұл мөлшері екі-үш есеге арттырылғаны хабарланды, ауыр жағдайларда айыппұл сомасы 14 500 еуроға дейін жетуі мүмкін [59]. Бұл өзгерістер мемлекет тарапынан жеке деректердің қорғалуын күшейтуге бағытталған қадам болып отыр.

ӘҚБтК жақында электрондық құжаттар мен электрондық цифрлық қолтаңба (ЭЦҚ) туралы заңнама талаптарының бұзылуына қатысты да арнайы нормамен толықтырылды. Мысалы, Кодекстің 640-бабына жаңа тармақ енгізіліп, басқа тұлғаның атына тіркелген электрондық цифрлық қолтаңбаны пайдаланғаны үшін әкімшілік жауаптылық көзделді. Бұрын ұйым басшылары өздерінің ЭЦҚ-ларын бухгалтерге немесе басқа қызметкерге жұмыс процесін жеңілдету үшін бере салу жиі тәжірибеде кездесетін. Енді мұндай әрекет заң бұзу болып саналады және жеке тұлғаларға шамамен 700 еуродан 1 500 еуроға дейін айыппұл салынуы мүмкін [59]. Бұл өзгеріс электрондық қолтаңбаның құқылық маңызын арттырып, оны заңсыз пайдалануды шектеуге бағытталған.

Цифрлық дәуірде аса өзекті проблемалардың бірі - онлайн кеңістікте жалған ақпарат тарату. Қазақстан заңнамасы соңғы жылдарға дейін интернетте жалған немесе заңсыз ақпарат таратуға тыйым салғанымен, оны бұзғаны үшін нақты жаза қарастырмаған болатын. 2023 жылы «Онлайн платформалар және онлайн жарнама туралы» заң қабылданғанда, әлеуметтік желілерде және интернет-платформаларда «заңсыз материалдарды онлайн жариялауға тыйым салу» енгізілді, бірақ тыйымды бұзған адамдарды жауапқа тарту тетіктері айқын болмады. Осы құқықтық олқылықты жою мақсатында 2025 жылы Ішкі істер министрлігі Интернетте заңсыз контент тарату үшін әкімшілік жауапкершілік енгізу туралы ұсыныс жасап, Мәжілісте тиісті заң жобасы қаралды. Аталған өзгерістер қабылданған соң, ӘҚБтК-те интернетте жалған ақпарат, экстремистік не өзге де тыйым салынған мазмұн таратқаны үшін айыппұл салу механизмі пайда болады деп күтілуде. Шетелдік тәжірибеге қарасақ, көршілес Қырғызстан да жалған ақпарат таратқаны үшін осындай айыппұлдар енгізуді жоспарлап отырғаны атап өтіледі [60].

Қазақстандық заң шығарушы органдар бұл қадамды ақпараттық кеңістікті зиянды контенттен тазарту және қоғамдағы қауіпсіздікті қамтамасыз ету талпынысы ретінде түсіндіреді. 2023 жылы ұлттық заңнамаға енгізілген өзгерістерге сәйкес, тәулігіне 100 мыңнан астам қолданушысы бар әлеуметтік желі провайдерлері Қазақстанда ресми өкілдік ашуға және “қасақана жалған ақпаратты” өшіруге міндеттелді, орындамаған жағдайда платформаны бұғаттау қаупі бар [61]. Сонымен бірге жалған ақпарат тарату әрекеттерінің өздеріне де әкімшілік жаза белгіленді. Бұл нормалар жалған ақпарат мәселесін тежеуге бағытталғанмен, қоғам тарапынан сөз бостандығына ықтимал қысым ретінде сынға алынуда.

Әкімшілік кодекстегі өзге де киберкеңістікке қатысты ережелер қатарына байланыс саласындағы тәртіп бұзушылықтар (мысалы, байланыс желілерін заңсыз пайдалану, тіркелмеген абоненттік құрылғыларды қолдану), ақпараттық қауіпсіздік талаптарын орындамау және авторлық құқықты бұзатын материалдарды онлайн тарату жатады. Мысалы, Қазақстанда ұялы

телефон IMEI-кодтарын тіркеу талаптары қойылған, оны айналып өтетіндерге әкімшілік шара қарастырылған. 2025 жылдың наурызынан бастап заңсыз әкелінген немесе ұрланған ұялы телефондарды «қара тізімге» енгізіп, ұялы байланысын бұғаттау тәртібі күшіне енді - яғни тіркелмеген құрылғыны пайдалануға тыйым салынады. Бұл ереже байланыс туралы заң мен оған сәйкес актілерде бекітілген тәртіптердің әкімшілік-құқықтық әдіспен қамтамасыз етілуінің мысалы бола алады. Жалпы, ӘҚБтК нормалары киберқауіпсіздік талаптарын бұзу сияқты әрекеттерге жедел ықпал етуге мүмкіндік береді, алайда олардың тиімділігі құқық қолдану органдарының белсенділігі мен техникалық мүмкіндіктеріне тікелей тәуелді.

Қазақстан Республикасының Қылмыстық кодексінде киберкеңістікте жасалатын ауыр құқық бұзушылықтардың құрамы нақты қамтылған. 2014 жылы қабылданып, 2015 жылы күшіне енген жаңа Қылмыстық кодексте «Ақпараттық технологиялар саласындағы құқық бұзушылықтар» деп аталатын жеке тарау енгізілді (VII тарау) [58]. Бұл тарауда төмендегідей киберқылмыс түрлері үшін қылмыстық жауаптылық көзделген:

- Ақпаратқа заңсыз қол жеткізу: ҚК 148-бабы мен 205-бабы ақпараттық жүйеге рұқсатсыз ену немесе онда сақталған ақпаратты заңсыз иемдену әрекеттерін қылмыс деп таниды. Мұндай іс-әрекеттер (мысалы, бөтен адамның электрондық поштасын немесе әлеуметтік желісін бұзу) жүйенің иесіне немесе пайдаланушыға зиян келтірсе, қылмыстық жазаға тартылады.

- Ақпаратты заңсыз ұстап алу (перехват) және тыңшылық: Электрондық ақпаратты оның иесінің келісімінсіз ұстап қалу немесе жасырын тыңдау, оқып отыру әрекеттері де қылмыстық жауаптылыққа жатады. ҚК 147-бабының 3-бөлігі, 148-бабының 2-бөлігі және 223-бабы электрондық ақпаратты заңсыз ұстап қалу (мысалы, электрондық хат-хабарды заңсыз оқу, трафикті аңду) қылмыс екенін көрсетеді [58].

- Деректерді бұрмалау немесе жою (деректерге қол сұғу): ҚК 206-бабының 1-бөлігі ақпаратқа заңсыз әсер ету, оның ішінде деректерді жою, өзгерту немесе бұғаттау әрекеттерін қылмыс деп бекітеді [58]. Бұған компьютерлік вирустарды пайдалану арқылы басқа тұлғаның файлдарын бүлдіру немесе жою, жүйенің жұмысын бұзу жағдайлары кіреді.

- Жүйенің жұмысына заңсыз кедергі жасау: ҚК 207-бабында ақпараттық жүйелердің қалыпты жұмысына кедергі келтіру (мысалы, серверлерге жасалатын DDoS-шабуылдар арқылы) қылмыстық әрекет ретінде анықталған [58]. Мұндай шабуылдар ұйымдардың, банктердің, мемлекеттік органдардың сайттарын істен шығарып, үлкен зиян тигізуі мүмкін.

- Құралдарды заңсыз пайдалану немесе дайындау: ҚК 210 және 213-баптарында қылмыс жасауға арналған арнайы компьютерлік бағдарламаларды немесе техникалық құралдарды дайындау, тарату үшін жауаптылық көрсетілген [58]. Яғни, зиянды бағдарламалық қамтылым (malware) әзірлеушілер мен таратушылар, немесе құпия мәліметтерді заңсыз алу құралдарын (мысалы, кардшимер, тыңшы бағдарлама) жеткізушілер қылмыстық жазаға тартылады.

- Интернетті пайдаланып жасалатын дәстүрлі қылмыстар: Қылмыстық кодексте дәстүрлі қылмыстардың интернет арқылы жасалған түрлері де қарастырылған. Мәселен, алаяқтық құрамы (190-бап) егер ол электрондық желілерді пайдалану арқылы жасалса, бұл жағдай ауырлататын мән-жай ретінде ескеріледі [58]. Сол сияқты қылмыс жолымен алынған табыстарды жылыстату, қаржылық пирамидалар ұйымдастыру, есірткі құралдарын насихаттау сияқты баптарда егер әрекет интернет арқылы жасалса, жауаптылық күшейе түседі.

- Контенттік қылмыстар: ҚК 174-бабы (әлеуметтік, ұлттық, діни алауыздықты қоздыру), 256-бабы (терроризмді насихаттау) сияқты қоғамға қауіпті ақпарат таратумен байланысты қылмыстар интернетте жасалған жағдайда жазаның ауырлығы артады немесе арнайы нормалар арқылы сараланады [61]. Балалар порнографиясы бойынша жеке қылмыс құрамы ҚК 312-бабында бекітілген - кәмелетке толмағандардың порнографиялық бейнесі бар материалдарды дайындау, тарату ауыр қылмыс деп танылып отыр [58]. Сондай-ақ авторлық және сабақтас құқықтарды бұзу (ҚК 198-бабы) және заңсыз кәсіпкерлік, құмар ойын бизнесін заңсыз ұйымдастыру сияқты әрекеттер интернетті қолдану арқылы жасалса, арнайы сараланууы мүмкін.

- Жеке өмірге қол сұғу және кибербуллинг: Қылмыстық кодексте жала жабу, қорлау баптары 2020 жылы декриминализацияланып (жала жабу - ӘҚБтК бойынша қаралатын болды), бірақ “кәмелетке толмағанға қатысты қорлау, қудалау” сияқты тікелей кибербуллингке қатысты арнайы бап әлі күнге жоқ. Дегенмен, жалпы қорқыту, бопсалау (ҚК 194-бап) немесе адамның жеке өмірі мен дербес деректерін заңсыз тарату (ҚК 147-бап) арқылы кибербуллинг жасаған тұлғаларды қылмыстық жауапқа тартуға болады.

Мысалы, әлеуметтік желіде біреуді жүйелі түрде қорқытып, жеке мәліметтерін рұқсатсыз жариялау әрекеттері осы баптар бойынша сараланууы мүмкін. Бүгінде қоғамда кибербуллинг үшін жеке жауапкершілік қарастыратын арнайы нормалар қабылдау қажеттігі туралы пікірлер айтылуда, бұл туралы 2.1.4 бөлімінде талданады.

Қорыта айтқанда, Қазақстанның Қылмыстық кодексі киберкеңістіктегі ең қауіпті құқық бұзушылықтарды қылмыс деп танып, оларға қатаң жаза белгілеген. Кейбір жағдайларда заң әкімшілік және қылмыстық жауаптылық шегін айқын ажыратады: мысалы, жалған ақпарат тарату егер қоғамдық тәртіпке елеулі қатер төндірсе немесе ауыр зиян келтіруі мүмкін болса, қылмыстық іске айналып (ҚК 274-бабы бойынша) 7 жылға дейін бас бостандығынан айыруға соқтыруы ықтимал, ал егер ондай ауыр салдарлар болмаса - жаңартылған ӘҚБтК аясында айыппұл салумен шектелуі мүмкін [61]. Мұндай екісатылы модель құқық бұзушылықтың ауырлығына қарай сараланған реакция жасауға мүмкіндік береді.

Балаларды киберкеңістіктегі қауіптен қорғау - Қазақстан заңнамасының маңызды бағыттарының бірі. 2002 жылы қабылданған «Қазақстан Республикасындағы баланың құқықтары туралы» Заң - бала құқықтарын кешенді қорғаудың негізін қалаған акт. Онда мемлекеттің бала денсаулығына, психикасына зиян келтіретін ақпараттан қорғау жөніндегі міндеттері жалпы

түрде айқындалған. Ата-аналардың да балаларды тәрбиелеуде олардың рухани және адамгершілік дамуына залал келтірмеу міндеті көрсетілген (атап айтқанда, осы Заңның 36-37 баптарында және ҚР Неке (ерлі-зайыптылық) және отбасы кодексінде ата-аналар балалардың психикалық денсаулығына зиян келтіретін ақпарат беруге тыйым салынатыны жазылған болуы мүмкін). Дегенмен, 2000 жылдардың басында интернет қолжетімділігі шектеулі болғандықтан, бұл жалпы нормалардың киберкеңістіктегі нақты қауіп-қатерлерге тікелей бағытталуы байқалмайды.

Уақыт өте келе ақпараттық орта түбегейлі өзгеріп, балалар үшін жаңа қатерлер көбейді: порнографиялық материалдардың ашық таралуы, “суицидтік топтар”, онлайн-әлімжеттік (кибербуллинг), зиянды діни-экстремистік үгіт-насихат, т.б. Осыған байланысты балаларды ақпараттық зияннан қорғауға арналған арнайы заңнамалық шаралар қажеттілігі туындады. 2015 жылы Парламент депутаттары «Балаларды денсаулығына және дамуына зиян келтіретін ақпараттан қорғау туралы» заң жобасын енгізіп, кеңінен талқылау басталды. Нәтижесінде 2018 жылы №169-VI заң болып қабылданған «Балаларды денсаулығы мен дамуына залал келтіретін ақпараттан қорғау туралы» Қазақстан Республикасы Заңы күшіне енді [56]. Бұл заң - баланың қауіпсіз ақпараттық кеңістікке деген құқығын іске асыруға бағытталған арнайы акт болып табылады.

Аталған 2018 жылғы Заңның мақсаты - баланың құқықтары мен мүдделерін ақпараттық зияннан қорғауды қамтамасыз ету, соның ішінде халықаралық стандарттарға сай тетіктер енгізу. Заңда балаларға арналған ақпараттық өнімдерді жас ерекшеліктеріне қарай жас санаттарына бөлу, зиянды контенттің (porno, зорлық-зомбылық көріністері, есірткі насихаты, суицидке итермелеу және т.б.) тізбесін анықтау, сондай ақпаратты таратуға шектеулер қою мәселелері реттелген. Атап айтқанда, “18+” белгілері, көрсетілім уақытын шектеу, контентті арнайы белгілеу талаптары, масс-медиа мен интернет провайдерлерінің балаларға зиянды контентті таратпауы бойынша міндеттері қарастырылған болуы ықтимал [56]. Заңның орындалуын қамтамасыз ету үшін уәкілетті органдар (Балалардың құқықтарын қорғау комитеті, Ақпарат министрлігі және Байланыс саласындағы реттеушілер) мониторинг жүргізуге және қажет болған жағдайда сайттарды, контентті шектеу шараларын қолдануға уәкілеттік алды.

Дегенмен, балаларды интернеттің зиянды әсерінен қорғау саласындағы заңнамада әлі де олқылықтар бар екені ғылыми зерттеулерде атап өтіледі. 2024 жылы қазақстандық зерттеушілер жүргізген салыстырмалы талдау көрсеткендей, Қазақстанның қолданыстағы актілерінде балаларға зиянды онлайн-контентті сүзгілеп, жоюдың нақты механизмдері жеткіліксіз, сондай-ақ интернет-платформалардың жауапкершілігі толық қарастырылмаған.

Мысалы, Германия 2020 жылы өзінің Жастарды қорғау туралы заңына толықтырулар енгізіп, интернет компанияларына балаларды сексуалдық қанаудан, кибербуллингтен, алдап-арбаудан қорғау бойынша нақты міндеттер жүктеді - соның ішінде кибербуллинг белгілері бар ақпаратты қадағалау және жою, заң талаптарын орындамағаны үшін заңи жауаптылыққа тарту

шараларын бекітті. Ұлыбритания 2021 жылы Балаларға арналған интернеттік қызметтердің жасқа лайық дизайн кодексін қабылдап, әлеуметтік желілер мен онлайн сервистерге балалардың жеке деректерін қорғау, зиянды жарнамадан қорғану, қауіпті функцияларды (геолокация, жеке хабарламалар) өшіру сияқты міндеттемелер қойды. Австралия алғашқылардың бірі болып 2015 жылы “E-Safety” атты дербес мемлекеттік агенттік - Балалардың электрондық қауіпсіздігі жөніндегі Комиссар қызметін құрды, ол әлеуметтік платформаларда балаларға қатысты зиянды мазмұнды жедел жоюға өкілетті және провайдерлерден есеп талап ете алады [56].

Бұл елдердің тәжірибесі Қазақстан үшін өте пайдалы үлгі бола алады. Қазірдің өзінде билік органдары балаларды киберкеңістік қатерлерінен қорғауды күшейту мақсатында жаңа бастамаларды қолға алуда. 2022 жылы Қазақстанда балалардың құқықтарын қорғау, білім беру, ақпарат және informatizaciya мәселелері бойынша заңдарға өзгерістер пакеті қабылданды.

Осы өзгерістер аясында мектептерде және жоғарғы сыныптарда “кибермәдениет” және онлайн-қатерлердің алдын алу бойынша сабақтар енгізу, ақпараттық өнімдерге жас санаты бойынша белгі қою тәртібін жетілдіру, интернет-платформалардың зиянды контентті өшіруі үшін үш күндік мерзім белгілеу сияқты шаралар қамтылған. Ақпарат және қоғамдық даму министрлігі ірі IT-компаниялармен (Facebook, Instagram, т.б.) балаларға зиянды контентті жедел жою жөнінде уағдаластық жүргізіп, кибербуллинг оқиғаларын анықтау және оларға қарсы әрекет ету тетіктерін іске қосты.

Министрліктің талабымен белгілі бір әлеуметтік желідегі кибербуллинг жағдайы анықталса, сол желінің өкілі мен уәкілетті орган бірлесіп үш күн ішінде тиісті шара қолдануы тиіс екендігі белгіленген. Бұл реформаның қисынды жалғасы ретінде “Кибербуллинг жөніндегі арнайы уәкілді” тағайындау да ұсынылуда - ол жедел түрде буллинг мәселелерін үйлестіріп, қажетті әрекеттерді қадағалайтын тұлға болмақ. Мұндай арнайы комиссар туралы идеяны ғалымдар да қолдайды, оны жүзеге асыру Қазақстандағы онлайн әлімжеттікпен күресті жүйелеуге жәрдемдеседі деп күтілуде [56].

Қорыта келе, «Баланың құқықтары туралы» жалпы заң және 2018 жылғы балаларды зиянды ақпараттан қорғау туралы арнайы заң негізінен баланың ақпараттық қауіпсіздігін қамтамасыз етуге бағытталған құқықтық базаны құрды. Алайда цифрлық әлемдегі қатерлер үнемі өзгеріп отырғандықтан, бұл саладағы заңнаманы халықаралық тәжірибеге сай жетілдіру қажеттігі туындауда. Қазақстанда балалардың онлайн қауіпсіздігі бойынша заңнаманы одан әрі дамыту үшін арнайы заң актісін қабылдау немесе қолданыстағы заңға ауқымды толықтырулар енгізу ұсынылады, онда жоғарыда аталған Ұлыбритания, Германия тәжірибесіндегі тәрізді міндеттемелер мен санкциялар жүйесі қамтылуы тиіс [56]. Бұл бағыттағы ресми жұмыстар басталып та кетті: 2025 жылы ақпанда Астанада Үкімет, ІІМ, Білім, Ақпарат министрліктері және UNICEF бірлесіп «Интернеттегі зорлық-зомбылықтан балаларды қорғау» атты екі жылдық бағдарламаны іске қосқанын жариялады. Сол жиында сарапшылар балаларды цифрлық ортада қорғау үшін заңдарды күшейту және білім беру шараларын жетілдіру керектігін атап өтті. Балалар

құқығын қорғау комитетінің төрайымы Nasymzhan Ospanova қолданыстағы шараларға қосымша, балаларды интернетте қорғауды қамтамасыз ететін жаңа заңдар әзірлеу қажеттігін ерекше айтты [62]. Демек, заңнамалық негізді дамыту қажеттігі мемлекет деңгейінде де мойындалып отыр, ал алдағы уақытта бұл бағытта нақты реформалар жүзеге асады деп күтіледі.

«Ақпараттандыру туралы» 2015 жылғы Заң – Қазақстанның цифрлық кеңістігін құқықтық реттеудің негізгі тіректерінің бірі. Бұл заң ақпараттандыру саласындағы қоғамдық қатынастарды реттей отырып, мемлекеттік органдардың, жеке және заңды тұлғалардың ақпараттық жүйелерді құру, дамыту және пайдалану кезіндегі құқықтары мен міндеттерін белгілейді. Заңда «ақпараттық қауіпсіздік» ұғымы алғаш рет кешенді түрде енгізіліп, электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымды ішкі және сыртқы қатерлерден қорғау жағдайы деп анықталады [63]. Ақпараттық қауіпсіздікті қамтамасыз ету мемлекет үшін ұлттық қауіпсіздіктің ажырамас бөлігі ретінде танылады, сондықтан бұл заңда уәкілетті органдардың ақпараттық қауіпсіздік саласындағы құзыреті мен функциялары нақты жазылған.

Заң бойынша уәкілетті орган - цифрлық даму саласындағы орталық атқарушы орган (қазіргі кезде Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі болуы мүмкін) ақпараттандыру және «электрондық үкімет» аясында жалпы саясатты жүзеге асырады. Ал ақпараттық қауіпсіздікке қолдау көрсету жөніндегі уәкілетті орган ретінде үкімет айқындаған орталық атқарушы орган (бұл функцияны бұрын Қорғаныс және аэроғарыш өнеркәсібі министрлігі, қазір мүмкін сол Цифрлық даму министрлігі немесе оның Ақпараттық қауіпсіздік комитеті атқарады) белгіленген [63]. Яғни, ақпараттық қауіпсіздік мәселелерін үйлестіру үшін арнайы мемлекеттік құрылымдар қарастырылған. Бұған қоса, Ұлттық қауіпсіздік комитетіне де (арнайы орган ретінде) өз құзыреті шегінде ақпараттық қауіпсіздікті қамтамасыз ету міндеттері жүктелген (мысалы, мемлекеттік құпиялар мен аса маңызды инфрақұрылымды қорғау).

«Ақпараттандыру туралы» заңда цифрлық дәуірде ерекше мәнге ие бірнеше институттар бар. Солардың бірі - «қорғалған ақпараттық жүйелер» және «маңызды ақпараттық-коммуникациялық инфрақұрылым объектілері» ұғымдары. 2022 жылы заңға енгізілген түзетулер арқылы «аса маңызды ақпараттық-коммуникациялық инфрақұрылым объектісі (АСАҚИО)» ұғымының анықтамасы кеңейтілді. Енді Қазақстанда жеке меншік болсын, мемлекеттік болсын - егер қандай да бір ұйымның ақпараттық жүйесінде шектелген қолжетімділік дербес деректер сақталса (қызметкерлердің, клиенттердің жеке мәліметтері және т.б.), онда ол жүйе аса маңызды инфрақұрылым санатына жатқызылуы мүмкін [64]. Мұндай статус автоматты түрде сол компанияға немесе мекемеге бірқатар міндетті талаптарды жүктейді:

- Біріншіден, ақпараттық қауіпсіздік бойынша операциялық орталық (SOC) құру немесе сыртқы провайдерден мұндай қызметті сатып алу міндеті [64]. Яғни, әрбір маңызды инфрақұрылым иесі өзінің желісіндегі

кибероқиғаларды тәулікбойы бақылайтын және оларға жедел жауап беретін мамандандырылған орталықты ұстауы тиіс (немесе ұлттық провайдер - KZ-CERT сияқты ұйымдардың қызметін пайдалануы керек).

- Екіншіден, деректер базаларының сақтық көшірмелерін уәкілетті органдарға беру талабы [64]. Бұл аса маңызды жүйелердегі ақпараттың қолжетімділігі мен тұтастығын қамтамасыз ету үшін мемлекеттің бақылау тетігі ретінде енгізілген талап - мысалы, белгілі бір мекеме өзінің деректер резервін мемлекеттік цефтрде сақтау қажет болуы мүмкін, сонда кибершабуыл не апат болған жағдайда мәліметтер жоғалмайды.

- Үшіншіден, жыл сайын ақпараттық қауіпсіздік аудитінен өту талабы [64]. АСАҚИО иелері тәуелсіз немесе мемлекеттік аккредиттелген сарапшыларға өз жүйелерінің қауіпсіздігін тексертіп, оның нәтижелерін уәкілетті органға тапсыруы керек. Бұл инфрақұрылымның осал тұстарын уақтылы анықтап, нығайтуға бағытталған шара.

- Төртіншіден, киберқауіпсіздік оқиғалары (инциденттері) туралы уәкілетті органға хабарлау міндеті [64]. Егер жүйеде дербес деректердің бұзылуы, тарап кетуі немесе сайттың істен шығуы сияқты кибероқиға орын алса, оны жедел түрде мемлекеттік органға хабарлап, тиісті әрекеттерді келісуі қажет. Бұрынғы заңнамада дербес деректердің бұзылуы туралы зардап шегушілерге немесе органдарға хабарлау талабы болмаған, енді бұл олқылық жойылуда.

- Бесіншіден, шетелдік серверлерде орналасқан корпоративті коммуникация құралдарын пайдалануға тыйым салынуы. Мысалы, егер компания аса маңызды инфрақұрылым қатарына кірсе, онда оның ішкі қызметтік хат алмасу, жиналыс өткізу үшін Outlook, Skype, Zoom, Teams сияқты кең таралған, бірақ серверлері шетелде орналасқан сервистерді қолдануына шектеу қойылуы мүмкін. Оның орнына серверлері Қазақстан аумағында орналасқан балама құралдар қолдану ұсынылады (мұндай талап 2022 жылғы Үкімет қаулысымен нақты бекітілгені хабарланған [64]. Бұл шектеу кибертыңшылық қаупін азайту мақсатында енгізілсе де, бизнес қауымдастық тарапынан сын тудырған, себебі ол коммуникация тиімділігіне кері әсер етуі мүмкін.

Жалпы, «Ақпараттандыру туралы» заң цифрлық инфрақұрылымды дамыту мен оны қорғаудың заңнамалық негізін қалыптастырады. Онда «электрондық ақпараттық ресурстар», «интернет-ресурс», «ақпараттық жүйе», «аппараттық-бағдарламалық кешен» сияқты негізгі түсініктер анықталып, ақпараттық жүйелердің мемлекеттік тіркелімі, ашық үкіметтің деректер порталы, электрондық құжат және электрондық қолтаңба мәселелері реттеледі. Айрықша мән берілген бір аспект - «ақпараттық қауіпсіздік инциденті» ұғымы және оларға жауап беру құрылымы. Заң бойынша «ақпараттық қауіпсіздік оқиғасы» деп ақпараттық инфрақұрылымның қалыпты жұмысын бұзуы мүмкін немесе заңсыз қол жеткізу, көшіру, жою, модификациялау, блоктау сияқты құқыққа қарсы әрекеттерге жағдай туғызатын оқиғалар түсініледі. Мұндай оқиғаларды анықтап, уақытылы әрекет ету үшін ақпараттық қауіпсіздік мониторингі

жүйесі және инциденттерге әрекет ету қызметтері (CERT) қарастырылған. Қазақстанда ұлттық CERT (Computer Emergency Response Team) - KZ-CERT құрылып, жұмыс істейді. Ол ақпараттық қауіпсіздік оқиғаларын жинақтап, талдап, ескерту жасап, індеттің таралуына қарсы шаралар қолданады. Сонымен бірге әр салада (қаржы секторы, көлік, энергетика т.б.) салалық ақпараттық қауіпсіздік орталықтары құру мүмкіндігі заңда бекітілген [63].

Дербес деректердің қауіпсіздігі және деректердіLocalization (жергіліктендіру). Қазақстан ақпараттық заңнамасының маңызды бөлігі - дербес деректерді қорғау мәселесі. 2013 жылы қабылданған «Дербес деректер және оларды қорғау туралы» Заң жеке тұлғалардың дербес мәліметтерін жинау, өңдеу, сақтау тәртібін бекітті. Ол дербес деректерді жинау үшін субъектінің келісімін алу қағидасын орнатты, сондай-ақ дербес ақпараттың Қазақстан аумағында сақталуы талабын енгізді [65]. 2015 жылғы «Ақпараттандыру туралы» заң осыны нақтылай түсті: Қазақстан азаматтарының дербес деректерін қамтитын дерекқорлар, егер олар шетелдік онлайн платформаларда болса, Қазақстан аумағында орналасқан серверлерде сақталуы тиіс деген талап қойылды. Дербес деректерді еліміздің шекарасы ішінде сақтау талабы (кейде «деректерді жергіліктендіру талабы» деп аталады) бір жағынан азаматтардың жеке мәліметтерінің шетелде заңсыз пайдаланылмауын қамтамасыз етуге бағытталған. Алайда бұл талап халықаралық IT-компанияларға қосымша техникалық-қаржылық жүк түсіретіні де айтылуда. Дегенмен, қазіргі кезде көптеген шетелдік әлеуметтік желілер мен мессенджерлер (Instagram, Telegram, TikTok, т.б.) Қазақстандағы пайдаланушылардың деректерін локализациялау мәселесін ішінара орындауға кірісті немесе өкілетті органмен келіссөздер жүргізуде.

Дербес деректерді қорғау талаптарын бұзу Қазақстанда құқық бұзушылық ретінде танылғаны жоғарыда айтылды (ӘҚБтК 79-бап). Ал егер дербес деректер заңсыз мақсатта пайдаланылып, ауыр зардап келсе (мысалы, мәліметтерді ұрлау арқылы алаяқтық жасалса), онда қылмыстық жауаптылыққа тарту мәселесі де туындайды. Қылмыстық кодекстің 147-бабы адамның жеке өміріне қол сұғу және жеке мәліметтерін рұқсатсыз тарату үшін жауапкершілік белгілейді. Соңғы жылдары цифрлық технологиялар дамыған сайын дербес деректерді қорғау нормативтері күшейтілуде. 2022 жылы Сенат мақұлдаған заң жобасы бойынша кез келген сайтында немесе серверінде жеке деректер сақтайтын компания ақпараттық-коммуникациялық инфрақұрылымның сыни объектісі деп танылып, жоғарыда аталған қатаң талаптарға бағынуы мүмкін [64]. Бұл бизнес тарапынан алаңдаушылық тудырғанымен, мемлекеттік органдар оны еліміздің кибертұрақтылығын арттыру қадамы деп түсіндіреді. Мұндай өзгерістер нәтижесінде жеке деректердің қауіпсіздігіне жауапты тұлғалар (компаниялар) ақпараттық қауіпсіздік шараларына қомақты инвестиция салып, өз жүйелерін нығайтуға мәжбүр болады, бірақ бұл жалпы қоғам үшін позитивті нәтиже - азаматтардың дербес деректері бұрынғыдан жақсы қорғалады деп күтілуде.

«Байланыс туралы» 2004 жылғы Заң телекоммуникация саласындағы қызметті құқықтық реттейтін негізгі акт болып табылады. Ол байланыс

операторларының құқықтары мен міндеттерін, мемлекеттік органдардың байланыс инфрақұрылымын реттеу өкілеттіктерін және пайдаланушылардың құқықтарын анықтайды [63]. Киберкеңістік тұрғысынан қарағанда, бұл заңда байланыс желілерін пайдалану барысында қауіпсіздік пен құқықтық тәртіпті қамтамасыз етуге бағытталған маңызды нормалар бар.

Ең алдымен, абоненттік құрылғыларды тіркеу және сәйкестендіру талабы. Қазақстанда ұялы байланыс абоненттері өздерінің SIM-карталарын жеке сәйкестендіріп (ЖСН арқылы) тіркеуге міндетті. Сондай-ақ әрбір мобильді құрылғының бірегей IMEI-кодын тіркеу жүйесі енгізілді. 2019 жылдан бері тіркелмеген телефондары желіде қызмет көрсетуден ажыратылатын тәртіп қолданыста. 2025 жылғы наурызда "қара тізім" ережесі күшіне еніп, елімізге заңсыз әкелінген немесе ұрланған мобильді телефондары анықталса, олар толығымен бұғатталатын болды [66]. Бұл талаптар ұялы құрылғылардың ұрлануын азайту, қылмыскерлердің анонимділік мүмкіндігін шектеу мақсатында енгізілген. Шынында да, тіркелмеген SIM карталар мен "көмескі" телефондар көбіне интернет-алаяқтық, жалған ақпарат тарату сияқты құқық бұзушылықтарда қолданылатыны белгілі; сондықтан олардың жолын кесу - жалпы киберқылмыспен күресудің бір тетігі.

Екіншіден, байланыс желілерін бұғаттау және трафикті шектеу мәселелері. «Байланыс туралы» заңның мемлекет қауіпсіздігі мен қоғамдық тәртіпті қорғауға қатысты баптарында, төтенше жағдай кезінде немесе сот шешімі бойынша заңға қайшы контентті таратып жатқан ресурстарға қолжетімділікті шектеу шаралары көзделген. Мысалы, терроризмге, экстремизмге шақыратын не өзге де заңсыз ақпаратты тарататын веб-сайттарға сот шешімімен тыйым салына алады, оны орындау үшін уәкілетті орган байланыс операторларына сол ресурстарды бұғаттау туралы нұсқау береді. Бұған қоса, 2020 жылдан бастап Бас прокуратураға адам саудасына қатысты интернет-сайттарды сотсыз бұғаттау құқығы берілді.

Бас прокуратура әзірлеген «Киберқадағалау» ақпараттық жүйесі арқылы мемлекет органдары адам саудасының белгілері бар сайттарды анықтаған бойда, бір күн ішінде бұғаттауға мүмкіндік алды. Бұрын заңсыз сайттарды жабу бірнеше айға созылатын, қазір бұл іс бір күнде атқарылады - 2020 жылдың шілдесінен бері осы жүйе іске қосылып, өткен жылы күмәнді 6 сайт осылайша жабылды. Бұл - байланыс инфрақұрылымы арқылы таралатын заңсыз контентті тежеу үшін «Байланыс туралы» заң және прокуратура органдарының өкілеттіктері шеңберінде қолданылған тиімді тәжірибе.

Үшіншіден, байланыс операторларының арнайы қызметтермен ынтымақтасу міндеті. Елдің ұлттық қауіпсіздігін қамтамасыз ету мақсатында байланыс заңында операторлардың жедел-іздестіру шараларын жүргізуге мүмкіндік беретін жабдық орнату талабы бар (ведомстволық актілерде «СОРМ» - скрытый обзор и запись материалов, яғни жедел іздестіру шараларының техникалық құралдарын орналастыру талабы). Осы талапқа сәйкес ұялы байланыс, интернет-провайдерлер Ұлттық қауіпсіздік комитетінің техникалық құралдарын өз желілеріне кірістіруге тиіс, бұл

терроризм мен басқа да қылмыстардың алдын алу үшін байланыс трафигін заңда көзделген тәртіпте бақылауға мүмкіндік береді. Әрине, бұл бақылау тек сот санкциясымен немесе заңмен рұқсат етілген жағдайларда жүргізілуі қажет; бірақ мұндай инфрақұрылымның болуы киберқылмыстарды ашуда маңызды рөл атқаратыны анық.

Төртіншіден, электр байланысы желілерінің тұтастығын және пайдаланушылардың құқықтарын қорғау. Байланыс операторлары ақпаратты беруде құпияны сақтау (пайдаланушылардың хат-хабар құпиясы конституциялық құқық ретінде қорғалған), спам таратпау, заңсыз мақсаттарға арналмаған жүйелерді қолданбау жөніндегі талаптарды орындауы тиіс. Егер байланыс саласында осы талаптар бұзылса (мысалы, оператор абоненттің келісімінсіз жеке байланыс деректерін бергені анықталса), әкімшілік не азаматтық-құқықтық жауапкершілік туындауы мүмкін.

Жалпылай алғанда, «Байланыс туралы» заң киберкеңістіктің техникалық негізі болып табылатын телекоммуникация желілерінің қауіпсіз әрі заңға сәйкес пайдаланылуын қамтамасыз етуге бағытталған. Соның арқасында интернеттің өзінде құқық бұзушылықтардың алдын алу мен жолын кесуге негіз қаланады. Байланыс инфрақұрылымы неғұрлым қауіпсіз әрі реттелген болса, киберқылмыспен күрес те соғұрлым тиімді болмақ.

«Құқық қорғау қызметі туралы» 2011 жылғы Заң құқық қорғау органдарындағы қызметтің өтелу тәртібін, кадрларды іріктеу, даярлау, аттестациялау, әлеуметтік қамсыздандыру шарттарын реттейді. Бұл заң тікелей киберқылмыспен күресу шараларын айқындамаса да, құқық қорғау жүйесін заманауи қауіп-қатерлерге бейімдеудің институционалдық негізі саналады. Соңғы жылдары Қазақстанның құқық қорғау органдарында сандық технологияларды пайдалану және цифрлық дағдыларды дамыту бағытына баса назар аударылуда. Заңға 2019-2021 жылдары енгізілген өзгерістер полиция мен өзге органдар қызметкерлерін даярлау жүйесін жаңғыртуға жол ашты – атап айтқанда, мамандарды қайта даярлау, әр үш жыл сайын аттестациядан өткізу талабы (оның ішінде цифрлық сауаттылықты тексеруді қоса) енгізілгені мәлім [67].

Қазақстанның Ішкі істер министрлігі 2010 жылдардың соңында құрылымында киберқылмыспен күрес бөлімшелерін құра бастады. Бүгінде ІІМ-де Киберқылмысқа қарсы күрес басқармасы қызмет атқарады, оның аумақтық департаменттерде өз бөлімдері бар. Мысалы, ІІМ Криминалдық полиция комитетінің құрамында жоғары технологиялық қылмыстармен айналысатын арнайы бөлім жұмыс істейді. 2025 жылы ақпандағы UNICEF-тің дөңгелек үстелінде ІІМ Киберқылмыспен күрес департаменті басшысының орынбасары Аслан Өскембаев сөз сөйлеп, «балаларға қатысты киберқылмыстарға тек әрекет ету ғана емес, алдын алу шаралары да қажет» екенін атап өтті [62]. Бұл – құқық қорғау органдарының киберқауіптерге көзқарасының өзгергенінің белгісі: енді олар қылмыс жасалған соң тергеп қана қоймай, оны болдырмауға тырысуда. Сол үшін полиция жастармен, оқу орындарымен, ата-аналармен тығыз жұмыс жүргізуде.

Бас прокуратура - құқық қорғау жүйесінің үйлестіруші органы ретінде - киберкеңістіктегі құқық бұзушылықтардың алдын алу және жолын кесу бағытында бірқатар бастамалар көтерді. Жоғарыда айтылған «Киберқадағалау» жүйесі - соның айқын мысалы. Прокуратураның қадағалау функциясы аясында Интернетте заңсыз контентті анықтау, талдау және қажет болса бұғаттау жұмыстары жолға қойылған. Прокурорлар сонымен қатар полиция қозғаған киберқылмыс істерін заңдылық тұрғысынан қадағалап, сотқа жолдануын қамтамасыз етеді. Мысалы, ІІМ-де тіркелген интернет-алаяқтық фактілері бойынша әкімшілік іс қозғалса да, оны сотқа жібермес бұрын прокурор қарап, дәлелдердің заңдылығын тексереді - бұл барлық істердің прокуратура мақұлдауынан өтуі керек деген ІІМ өкілі Игорь Лепеханың түсіндірмесінен белгілі [60]. Сондай-ақ Бас прокуратура 2020-2021 жылдары «Кибербуллингті қадағалау» пилоттық жобасын қолға алып, интернеттегі балаларға қатысты қудалау оқиғаларын мониторингтен өткізгені айтылады. Прокуратура органдары заңнамаға ұсыныстар дайындау, Парламентке жаңа бастамалар енгізу жұмыстарында да белсенді (мысалы, 2023 жылы прокуратураның ұсынысымен заңға киберқауіпсіздікке қатысты түзетулер енгізілгені хабарланған.

Жергілікті полиция қызметі - өңірлерде құқық тәртібін қамтамасыз ететін негізгі буын. Дәстүрлі қылмыстармен қатар, қазір әр аймақтағы полицияға интернет-алаяқтық, желі арқылы бопсалау сияқты фактілер бойынша көптеген арыз-шағымдар түсуде. Мәселен, соңғы жылдары елімізде интернет арқылы жасалатын алаяқтық (банктік шоттарды алдау арқылы ақша жымқыру, жалған интернет-дүкендер құру арқылы адамдарды алдау) кең тарағаны сонша, полиция департаменттері жанынан азаматтарды бұл туралы ескерту үшін арнайы брифингтер өткізіледі. Жергілікті полиция халықпен тікелей жұмыс істегендіктен, тұрғындарға түсіндіру және алдын алу шараларын атқарады - мектептерде, жоғары оқу орындарында «Интернеттегі қауіпсіздік» сабақтарын, дәрістерін ұйымдастыру, брошюралар тарату, әлеуметтік желілерде сақтық туралы роликтер жариялау сияқты.

Мысалы, Батыс Қазақстан облысының полиция департаменті 2023 жылы кибералаяқтықпен толыққанды күресу үшін өңірде IT-мамандарды тартумен арнайы топ құрылғанын хабарлады [68]. Сол сияқты жергілікті полиция бөлімдері құрамында компьютерлік технологиялар бойынша сарапшылар штатын ұлғайту мәселесі күн тәртібінде тұр. Бұл – ІІМ орталық аппаратына қарасты жоғары технологиялық қылмыстарға қарсы бөлімшелердің аймақтарда тиімді әрекет етуін қамтамасыз ету үшін жасалып жатқан шара.

Киберкеңістіктегі құқық бұзушылықтардың алдын алу тек құқық қорғау органдарының міндеті емес, бұл – кешенді әлеуметтік жұмыс. Мектептер, колледждер және университеттер жастардың негізгі білім алу ортасы ретінде цифрлық сауаттылық пен кибергигиена мәдениетін қалыптастыруы тиіс. Білім және ғылым министрлігі 2022 жылдан бастап оқу бағдарламасына «Цифрлық сауаттылық» пәнін біртіндеп енгізіп, онда оқушыларға интернеттегі қауіпсіздік ережелері, кибербуллингтен қорғану, күмәнді контентті тану сияқты тақырыптар оқытылуда. Мысалы, Астана қаласының

мектептерінде «Киберқауіпсіздік апталығы» өткізіліп, онда ІІМ мамандары мен сарапшылар балаларға интернеттің қауіпті тұстары туралы дәрістер оқыды. Жоғары оқу орындарында да заңгерлік, IT мамандықтарының оқу жоспарларында Кибер құқық негіздері, ақпараттық қауіпсіздік заңнамасы модульдері пайда болуда.

Әкімдіктер - жергілікті жердегі атқарушы билік - бұл процессте қолдау көрсетуші маңызды құрылым. Облыстар мен қалалар әкімдері жанынан құқық бұзушылықтардың алдын алу жөніндегі ведомствоаралық комиссиялар бар, олардың жұмысына киберқылмыстың алдын алу мәселелері де енгізілуде. Мысалы, көптеген өңірлерде әкімдік пен полиция бірігіп «Абайлаңыз, интернет-алаяқтар!», «Қауіпсіз Интернет» сияқты ақпараттық кампаниялар өткізді. Әкімдіктер сондай-ақ жастар ресурстық орталықтары арқылы жасөспірімдер арасында кибермәдениет тәрбиелеуге атсалысады.

Бұдан бөлек, әлеуметтік қызметтер (қорғаншылық органдары, психологтар) интернетте зорлық-зомбылыққа ұшыраған не буллингтің құрбаны болған балаларға көмек беру жұмысын ұйымдастыруда. 2025 жылы басталған «Интернеттегі зорлық-зомбылықтан балаларды қорғау» бағдарламасы аясында да жергілікті атқарушы органдар белсенді рөл атқаратыны айтылды - олар үкіметтік емес ұйымдармен, бизнес-секторымен бірге балаларға қауіпсіз цифрлық орта қалыптастыруға үлес қосады [62].

Халықаралық және үкіметтік емес ұйымдардың қолдауы. Құқық қорғау органдары мен мемлекеттік мекемелерге халықаралық ұйымдар да әдістемелік көмек көрсетуде. Мысалы, UNICEF пен «Safe Online» қорының қолдауымен Қазақстан үкіметі аталған екі жылдық бағдарламаны қолға алды, оның шеңберінде шетелдік сарапшылардың қатысуымен тренингтер, заңнамалық ұсыныстар әзірлеу, техникалық құралдармен жабдықтау көзделген [62]. OSCE (ЕҚЫҰ) Қазақстанға электрондық дәлелдемелермен жұмыс, трансшекаралық ынтымақтастық бойынша оқыту жобаларын ұсынды - 2024 жылы Орталық Азия елдерінде E-vidence атты электрондық дәлелдемелер бойынша әлеуетті арттыру жобасы басталып, соның шеңберінде Қазақстанда да қажетті заңнамалық, техникалық реформалар талқылануда. ҮЕҰ-дар арасында «Зорлық-зомбылықсыз балалық шақ», «Интернеттегі қауіпсіздік» бастамалары аясында қоғамдық бақылау жүргізіп, заңнамалық ұсыныстар енгізіп жүргендер бар. Осындай көпжақты ынтымақтастық құқық қорғау органдарының күш-жігерін толықтырып, киберкеңістіктегі құқық бұзушылықтарға қарсы күресте кешенді тәсілдің жүзеге асуына көмектеседі.

**Киберкеңістіктегі құқық бұзушылықтарды қолдану практикасы және мысалдар.** Жоғарыда сипатталған заңнамалық база іс жүзінде қаншалықты тиімді жұмыс істеуде? Бұл сұраққа жауап беру үшін Қазақстандағы құқық қолдану практикасына талдау жасап көрейік. Соңғы жылдары киберкеңістіктегі құқық бұзушылықтар саны артып келе жатқаны байқалады, солардың кейбір резонансты түрлеріне және мемлекет қолданған шараларға тоқталайық. 2020-2023 жылдары Қазақстанда тіркелген интернет-алаяқтық деректері ондаған есеге өсті деп хабарланды. Әсіресе COVID-19

пандемиясы кезінде көп адамның онлайн қызметтерге көшуі, цифрлық банк карталарын белсенді пайдалануы алаяқтарға мүмкіндік туғызды.

Кибералаяқтар банк атынан қоңырау шалып, құпия кодтарды сұрау, жалған интернет-дүкендер арқылы алдын ала төлем алдырып алдау, әлеуметтік инженерия әдістерімен азаматтардың интернет-банкинг аккаунттарына қол сұғу сияқты қитұрқылықтарды қолданды. Мұндай істер Қылмыстық кодекстің 190-бабы («Алаяқтық») бойынша тергеледі.

Полиция көптеген топтарды ашты: мысалы, 2022 жылы Алматы қаласында Telegram арқылы арзан автомобильдер сату туралы жалған хабарландырулар таратып, ондаған адамды алдаған топ құрықталды - оларға қатысты қылмыстық іс қозғалып, сот кінәлілерді 5 жылға дейін бас бостандығынан айырды. Дегенмен, көптеген жағдайда интернет-алаяқтар шетелде отырып әрекет ететіні анықталды (Нигерия, Ресей т.б.), бұл тергеуге кедергі келтіреді. ІІМ Интерпол арнасы арқылы халықаралық іздестіру жұмыстарын да жүргізуде.

2021-2022 жылдары Қазақстанда бірнеше ірі дербес деректердің таралып кету оқиғалары тіркелді. Мысалы, 2021 жылы бір хакерлік топ мемлекеттік органдардың ашық деректер порталындағы осалдықты пайдаланып, миллиондаған азаматтың ЖСН, телефон нөмірлері, мекенжайлары сияқты деректерін жымқырды деген мәлімет тарады. Бұл факті бойынша Қылмыстық кодекстің 205-бабы («Заңсыз қолжеткізу») және 210-бабы («Құралдарды дайындау») бойынша іс қозғалып, Киберполиция бірнеше күдіктіні ұстады.

Тергеу барысында ел тарихында алғаш рет цифрлық сот-сараптамасы тағайындалып, айғақ ретінде сервер жазбалары, желілік трафик талдауы қолданылды. Бұл іс электрондық дәлелдемелерді сотта пайдалану бойынша маңызды сынақ болды. Нәтижесінде кінәлілер шартты мерзімге сотталды, ал бұл оқиға мемлекеттік органдарды ақпараттық қауіпсіздікке аса мән беруге итермеледі - көптеген жүйелерге аудит жүргізіліп, осалдықтар жабылды.

Интернетте радикалдық идеологияны тарату фактілері бойынша да қылмыстық істер қозғалып келеді. 2018-2019 жылдары әлеуметтік желілерде террористік ұйымдардың идеяларын насихаттағаны үшін бірнеше Қазақстан азаматы сотталды. Әдетте, мұндай тұлғалар YouTube, VKontakte сияқты платформаларда тыйым салынған материалдарды (ДАИШ ұйымының видеолары, радикал уағызшылардың жазбалары) жариялаған. Оларға Қылмыстық кодекстің 256-бабы («Терроризмді насихаттау») бойынша 5 жылдан 7 жылға дейінгі жаза кесілді. Бұған қоса, ұлттық қауіпсіздік органдары мұндай материалдарды анықтап, дереу жойдырумен айналысады - Мәдениет және ақпарат министрлігі мен Бас прокуратура Facebook, YouTube әкімшіліктеріне сұраныс жіберу арқылы ондаған аккаунт пен жазбаны өшіртті. Freedom House ұйымының «Интернет еркіндігі - 2024» баяндамасына сәйкес, 2023 жылы Қазақстан үкіметі жалған ақпарат пен экстремистік материалдарды жою жөнінде жаңа әкімшілік жазалар енгізіп, бір жыл ішінде көптеген сайттар мен парақшаларды бұғаттаған. Осындай шаралардың арқасында экстремистік идеологияның кең таралуының алды алынғанымен, кей жағдайда олар азаматтық белсенділер мен оппозициялық

көзқарастағылардың пікірлерін шектеу үшін де қолданылып отыр деп сыналды [61]. Соңғы жылдары қоғамда резонанс тудырған оқиғалардың бірі - мектеп оқушыларының суицидтері мен буллинг фактілерінің интернеттегі зиянды қауымдастықтармен байланысы. 2018-2020 жылдары бірнеше оқушының өзіне қол жұмсауына байланысты «Синий кит» сияқты қауіпті ойындардың әлеуметтік желілерде таралуы күдік тудырды. Тергеу барысында кейбір балалар ВКонтакте желісіндегі жабық топтарда арандатушы тапсырмалар орындауға мәжбүр болғаны анықталды. Бұл істер бойынша Қылмыстық кодекстің 105-бабы («Өзін-өзі өлтіруге итермелеу») бойынша қылмыстық істер қозғалып, топ администраторлары табылмады (көпшілігі шетелде еді).

Алайда, осы оқиғалар билікті тез арада әрекет етуге мәжбүрледі: мектептерде психологтар жұмысы күшейтілді, ІІМ «Кибербуллинг» жағдайларын анықтау үшін мониторингті жолға қойды, Білім министрлігі әлеуметтік желілермен тікелей байланыс орнатып, қауіпті топтарды жаптыруға қол жеткізді. 2021 жылы кәмелетке толмағандарға интимдік сипаттағы қысым жасап, суреттерін таратамын деп бопсалаған 40 жастағы азамат ұсталды - ол Instagram арқылы бірнеше қызды қорқытқаны анықталды. Сот оны ҚК 194-бабы («Бопсалау») бойынша кінәлі деп тауып, 6 жылға бас бостандығынан айырды. Бұл прецедент кибербуллингті қылмыстық-құқықтық жолмен жазалаудың мысалы болды. Дегенмен, көптеген ата-ана мен сарапшылар кибербуллинг үшін нақты заң баптарының жоқтығын, полицияның мұндай істерді көбіне ӘҚБтК бойынша (ұсақ бұзақылық ретінде) жауып тастайтынын алға тартып, заңнаманы күшейтуді талап етті. Мұндай қоғамдық сұраныс нәтижесінде 2022-2023 жылдары Парламентте «кибербуллингке қарсы арнайы заң қабылдау қажет пе?» деген мәселе көтерілді [56]. Үкімет әзірге бөлек заңға бармай, қолданыстағы нормативтермен реттейміз деген ұстанымда, алайда қоғам талабы мұнымен шектелмей отыр - жақын болашақта бұл бағытта жеке заң қабылдануы да ғажап емес.

Интернеттегі тағы бір кең таралған құқық бұзушылық - авторлық құқық объектілерін заңсыз тарату (фильмдер, бағдарламалар, музыкалар). Қазақстанда танымал “torrent” сайттарын пайдалану, болмаса Telegram арналар арқылы кітаптарды, бейнематериалдарды рұқсатсыз бөлісу деректері көп. Құқық қорғау органдары негізінен ірі көлемдегі, коммерциялық зиян келтірген жағдайларға назар аударады. Мысалы, 2019 жылы “Меломан” компаниясының шағымы бойынша лицензиясыз контент ұсынған бірнеше веб-сайт әкімшілері анықталып, қылмыстық жауапқа тартылды.

Олар ҚК 198-бабы бойынша (авторлық құқықты бұзу) айыпталып, шартты жаза алды, ал сайттары жабылды. 2020 жылы “Kinokz” атты ірі пираттық сайттың иелері ұсталып, серверлерінен жүздеген терабайт заңсыз фильмдер тәркіленді - бұл іс бойынша кінәлілер 3 жылға шартты түрде сотталды және оларға интернет саласында қызметпен айналысуға тыйым салынды. Мұндай істер қоғамға контентті заңды жолмен тұтыну қажеттігін көрсетті, әрі мемлекет зияткерлік меншік құқығын қорғау халықаралық

міндеттемелерін орындауға ынталы екенін аңғартты. Кибершабуылдардың нысаны ретінде тек жеке азаматтар немесе компаниялар ғана емес, мемлекеттік органдар да зардап шегіп жүр. 2018 жылы белгісіз хакерлер Қазақстанның бірнеше мемлекеттік органының ресми веб-сайтына бұзып кіріп, басты беттеріне саяси ұрандар орналастырған оқиға болды. Бұл оқиға үлкен резонанс туғызды - ҰҚК дереу тергеу бастады, анықталғандай шабуыл шетелдік IP-адрестерден келген және белгілі "Анонимус" хактивистер тобының стиліне ұқсас болған. Тергеу нәтижесі көп жарияланбады, алайда осыдан кейін мемлекеттік техникалық қызмет (GTS) барлық меморгандар сайттарына DDoS-қорғаныс орнатты, веб-сайттарды екі факторлы аутентификациямен қорғау, әкімшілік панельдерге қолжетімділікті шектеу тәрізді шараларды қабылдады. 2022 жылы белгілі APT41 деп аталатын Қытаймен байланысты хакерлік топ Қазақстанның телекоммуникация операторлары инфрақұрылымына екі жыл бойы жасырын кіріп келгені анықталды [61]. Олар желілерден үлкен көлемде деректер шығарып отырды деген күдік бар. Бұл ақпарат киберқауіпсіздік саласының мамандары дабыл қағуына себеп болды. Үкімет араласқан соң, барлық негізгі байланыс операторлары желілерінде аудит және залалсыздандыру жүргізілді, нәтижесінде сол зиянды қол жетім (backdoor) жолдары жабылды деп хабарланды. Мұндай мысалдар мемлекеттің киберқауіпсіздікке ұжымдық күш жұмсауы қажеттігін көрсетеді, және соның салдары ретінде 2022 жылы еліміз киберқауіпсіздік бойынша ұлттық үйлестіру орталығын (Ұлттық киберқауіпсіздік орталығы) құру жұмысын бастады.

Жоғарыдағы мысалдар Қазақстанның киберкеңістіктегі қауіптерге жауап беруге талпынып жатқанын, кей жағдайларда айтарлықтай табыстарға жеткенін көрсетеді. Алайда, практикада бірқатар түйткілді мәселелер де бар:

- Істерді ашу көрсеткіші төмен. Статистикаға сүйенсек, интернет-алаяқтық сияқты қылмыстардың 50%-дан астамы ашылмаған күйі қала береді, өйткені қаскүнемдер көбіне басқа мемлекеттерден әрекет етеді немесе анонимайзер, криптовалюта секілді ізін жасыру технологияларын пайдаланады. Полицияның техникалық із кесу мүмкіндіктері шектеулі болған жағдайда, істі ашу қиын.

- Халықтың хабардарлығы төмен. Көптеген азаматтар цифрлық қауіпсіздік қағидаларын жетік білмейді, сол себепті қылмыскерлердің қарапайым айла-амалдарына алдана береді (жалған банк қызметкері қоңырау шалса, деректерін айтып қою, фишинг сілтемеге өтсе, картасы мәліметтерін енгізу, т.б.). Бұл ретте, алдын алу шаралары күшейтілгенімен, әлі де қоғамның барлық сегментін қамтымай отыр.

- Трансшекаралық ынтымақтастықтың қиындығы. Көптеген киберқылмыстар халықаралық сипатта болғандықтан, шетелдік әріптестермен бірлесіп әрекет ету қажет. Қазақстан құқық қорғау органдарының Интерпол, ТМД желілері бойынша келісімі бар, бірақ, мысалы, Еуропа немесе АҚШ-та орналасқан компаниялардан деректер алуда бюрократиялық кедергілер туындайды. Қазақстан әлі Будапешт конвенциясына қосылмағандықтан, электрондық дәлелдемелерді жедел

алмасу бойынша құқықтық база толық емес. Сол себепті, мысалы, Facebook немесе Google-ға ресми сұраулар жіберу апталар, айлар алады, ал қылмыскер сол арада ізін суытып үлгереді.

- Ресурстық шектеулер. Киберполиция бөлімдерінің штат саны көп емес және барлық облыста толық жабдықталмаған. Сандық криминалистика бойынша сарапшылар жеткіліксіз, арнайы жабдық (деректерді қалпына келтіру, шифрды бұзу құрылғылары) саны да шектеулі. Бар мамандар үлкен жүктememен жұмыс істейді - кейбір облыстарда бір тергеушіге ондаған киберқылмыс ісі келеді. Сараптамалар да ұзаққа созылуы мүмкін, өйткені арнайы зертханалар тек Астана мен Алматыда орналасқан.

Осы мәселелерді шешу үшін мемлекет бірқатар қадамдар жасауда: Мысалы, 2022 жылы ІІМ құрылымында Киберполицияның жеке департаментін құрып, оған қосымша штат берді; 2023 жылдан бастап өңірлік полиция департаменттерінде ақпараттық технологиялар бойынша жедел уәкіл деген лауазым енгізілді. 2024 жылы Қазақстан Будапешт конвенциясына қосылу процедураларын бастағаны хабарланды - бұл жүзеге асса, халықаралық ынтымақтастық жақсара түседі. Сондай-ақ, 2025-2027 жылдарға арналған Киберқауіпсіздікті қамтамасыз ету жөніндегі жол картасы бекітіліп, онда құқық қорғау органдарының материалдық-техникалық базасын нығайту, цифрлық криминалистика зертханаларын көбейту жоспарланған.

**Кибер құқықтық реттеу саласындағы олқылықтар, қайшылықтар және ғылыми сын тұрғысынан талдау.** Қазақстанның киберкеңістікке қатысты заңнамасы соңғы жылдары едәуір дамып, жетілдірілгенімен, әлі де бірқатар заңнамалық олқылықтар мен қайшылықтар орын алуда. Ғылыми тұрғыдан сын көзбен қарағанда, бұл кемшіліктерді жою - ақпараттық қоғамдағы құқық тәртібін қамтамасыз ету үшін өте маңызды. Төменде сондай проблемалық тұстар талданып, әрқайсысына қатысты мүмкін шешімдер мен қарсы уәждер қарастырылады.

1. Арнайы заңнаманың фрагментарлығы және “киберқылмыс” ұғымының айқындалмауы. Қолданыстағы қылмыстық және әкімшілік заңнама киберкеңістіктегі көптеген іс-әрекеттерді қамтығанымен, онда “киберқылмыс” немесе “кибер құқық бұзушылық” ұғымдарының анықтамасы жоқ. Заңнамалық деңгейде ортақ терминологияның болмауы құқық қолдануда түсінбестік тудыруы мүмкін. Мысалы, бірқатар заңдарда “ақпараттық қауіпсіздікке қарсы қылмыстар”, “жариялауға тыйым салынған ақпарат” деген түрлі тұжырымдар кездеседі, бірақ “киберқауіпсіздік” терминінің өзі заңда анықталмаған (тек тұжырымдамада бар). Ғылыми ортада кейбір мамандар “киберқылмыс” ұғымын заңға енгізуді және оның құрамдарына ортақ ережелер белгілеуді ұсынады. Алайда қарсы пікір де бар: егер барлық қылмыстарды «кибер» деп бөлек бөлектейтін болсақ, заң тым күрделеніп, әр бапты жаңарту қажет болады. Сондықтан қазіргі тәсіл - қолданыстағы баптардың диспозициясына “ақпараттық технологияларды пайдалана отырып” деген сөздер қосу - қолайлы деген уәж айтылуда. Бұл жерде маңыздысы - тәжірибе жүзінде дұрыс қолдану: құқық қорғау

органдары судьяларды және тергеушілерді оқытып, жаңа қауіптердің қылмыстық заңнаманың қай баптарына жататынын түсіндірсе, терминологияның болмауы аса қиындық туғызбайды деп санауға болады.

2. Әкімшілік пен қылмыстық жауаптылықтың шекаралары және қайталауы. Кейбір құқық бұзушылықтар бойынша әкімшілік және қылмыстық нормалардың арасында үйлесімсіздік байқалады. Мысалы, жоғарыда айтылған жалған ақпарат тарату бойынша: ауыр зардаптары болса - ҚК 274-баппен (7 жылға дейін), ал болмаса - енді ӘҚБтК-ге енгізілетін баппен айыппұл. Дегенмен "ауыр зардап" мен "әлеметтік алауыздық туғызу қаупі" түсініктері субъективті болуы мүмкін, бұл құқық қолданушыға кең дискреция береді. Сол сияқты дербес деректерді заңсыз тарату ісінде: егер ол жеке өмірге қол сұғу арқылы жасалса, ҚК 147-баппен (5 жылға дейін) қамалады, ал егер "құқыққа сыйымсыз, бірақ ауыр зардапсыз" болса - ӘҚБтК 79-баппен айыппұл [59]. Практикада қай бапты қолдану керектігі кейде түсініксіз болады. Мұндай қосарлануды болдырмас үшін заңнамашы әкімшілік құқық бұзушылықтардың құрамдарын барынша нақтылап, қылмыстық баптармен жігін ажыратып көрсетуі керек. Заң теориясында "әкімшілік преюдиция" принципін қолдану ұсынылады - яғни, адам киберкеңістікте алғаш рет құқық бұзса (мысалы, алғаш рет жалған ақпарат таратса) - әкімшілік жаза берілсін, қайталаса - қылмыстық жауапқа тартылсын. Бұл тәсіл кейбір баптарда бар (қайталау ауырлататын белгі ретінде), бірақ жүйелі түрде іске аспай отыр.

3. Цифрлық дәлелдемелерге қатысты рәсімдердің кемшілігі. Қылмыстық-процестік кодексте электрондық (цифрлық) дәлелдеме деген ұғым құқықтық тұрғыда толық ашылмаған. Іс жүзінде, электрондық пошталар, лог-файлдар, чат хаттамалары сияқты айғақтар дәстүрлі "құжат" немесе "заттай дәлел" ретінде ұсынылады. Алайда бұл көзқарас цифрлық деректердің ерекшелігін ескермейді. Мысалы, ұялы телефоннан алынған деректерді қарау кезінде тергеушілер көбіне оны «қарап шығу (осмотр) хаттамасын» толтырады, ал шын мәнінде телефонды ашып, ішіндегі мәліметтерді алу - бұл іздестіру мен тінтуге көбірек ұқсайды. Зерттеуші Д. Үтеповтың пікірінше, қолданыстағы қылмыстық процесте "қарап шығу" тергеу әрекеті электрондық ақпаратты алу үшін жарамсыз, сондықтан мұндай жағдайда міндетті түрде тінту немесе алу (выемка) жүргізу туралы санкция қажет [69]. Яғни, "цифрлық дәлелдерді жинау" процессуалдық тұрғыда нақты регламенттелмеген. Бұл мәселені шешу үшін заңға өзгеріс дайындау қажет. 2022 жылы мамандар «Цифрлық дәлелдемелер туралы» заң жобасын ұсынды, онда электрондық ақпаратты процессуалдық бекіту тәртібін енгізу көзделген болатын. Мысалы, электрондық мәліметтердің түпнұсқалығын растау үшін хэш-сумма есептеу, цифрлық қолтаңба қолдану, бұлттық сервистерден деректерді алу процедурасын келісу секілді нормалар керек. Мұндай арнайы заң Өзбекстанда 2024 жылы қабылданды және ол Қылмыстық-процестік кодексті толықтырып, электрондық дәлелдеме ұғымын енгізді. Қазақстанға да осындай жаңарту қажет деп есептеледі. Қазіргі уақытта OSCE-нің E-vidence жобасы аясында Қазақстанда цифрлық дәлелдемелер бойынша

қажеттіліктерді бағалау миссиясы жоспарланғаны мәлім [70]. Бұл миссия қорытындысы заңнамаға ұсыныстар беріп, мүмкін жаңа заң қабылдануына түрткі болады.

4. Халықаралық ынтымақтастықтың шектеулілігі. Қазақстан әзірше Киберқылмыс жөніндегі Будапешт конвенциясына ресми қосылмаған мемлекеттердің қатарында, дегенмен 2018 жылдан бері қосылуға дайындық жүргізуде. Конвенцияға қосылмау - шетелдік серіктестермен электрондық айғақтарды жедел алмасу, трансшекаралық із кесу істерінде қиындық тудырады. Мысалы, АҚШ құқық қорғау органдары Конвенция аясында Қазақстан сұрау салса, анықтамаларды тезірек берер еді, ал қазіргі жағдайда Mutual Legal Assistance Treaty (Құқықтық көмек туралы екіжақты шарттар) шеңберінде уақыт ұзап кетеді. Бұл олқылықты мойындаған Қазақстан 2022 жылы Конвенцияға қосылу туралы заң жобасын парламентке енгізді деп хабарланды, ал 2023 жылы арнайы жол картасы бекітілді. Дегенмен бұл процесс баяу жүруде, оған себеп - кейбір мемлекеттік органдар конвенция ережелерінің ұлттық егемендікке ықтимал әсеріне алаңдайды (мысалы, шетелдік органдардың біздің провайдерлерден тікелей ақпарат сұрауы мүмкін деген сияқты). Бұл жерде қарсы уәж ретінде: Конвенция аясындағы рәсімдер ұлттық заңнаманың шеңберінде орындалатынын, егемендікті бұзбайтынын айтуға болады. Керісінше, Қазақстан үшін халықаралық ынтымақтастық артықшылық болады - ауыр киберқылмыстарды ашуда шетелдердің көмегіне жүгіну оңайлайды. Сондықтан ғылыми қауымдастық пен сарапшылар елдің тезірек Конвенцияға қосылуын ұсынады [58]. Бұл ұсынысты енді саяси шешім деңгейінде қолдау қажет.

5. Контентті реттеу мен сөз бостандығы арасындағы тепе-теңдік мәселесі. Соңғы уақыттағы заңнамалық бастамалар (онлайн платформалар туралы заң, жалған ақпарат үшін айыппұлдар және т.б.) қоғамда екіұшты баға алуда. Бір тарап - мемлекет пен көптеген ата-аналар - балаларды зиянды контенттен, қоғамды жалған ақпараттан қорғауды көздейтін қатаң шараларды қолдайды, себебі «адамдардың санасын улайтын, тыныштықты бұзатын контентке тосқауыл қажет» дейді. Екінші тарап - құқық қорғаушылар мен кейбір сарапшылар - бұл шаралар цензураға ұласып кетуі мүмкін деп алаңдайды.

«Кибербуллинг - шын проблема ма, әлде цензураны қатайту сылтауы ма?» деген сауал қоғамдық дискурста талқылануда [56]. Мысалы, 2022 жылы қабылданған балаларды кибербуллингтен қорғау нормаларының аясында әлеуметтік желілерден кез келген «зиянды» деп бағаланған жазбаны өшіруді талап етуге болады. Мұндай талаптарды атқарушы билік саяси сын мен балама пікірді де «зиянды» деп бағалап, өшіртуге қолдануы ықтимал деген қауіп бар. Расында да, 2023 жылы кейбір белсенді журналистердің әлеуметтік жазбаларына «жалған ақпарат» бабы бойынша іс қозғалып, сот оларды айыппұлға кескен оқиғалар болды [61]. Бұл жағдайлар мемлекетке берілген құралдардың оппозицияны тұншықтыруға пайдаланылуы мүмкін екенін көрсетеді. Дегенмен, мемлекеттік өкілдер «бұл заңдар бірінші кезекте халықты жалған ақпарат пен қауіпті контенттен қорғауға арналған, ал сөз бостандығына шектеу қою ниеті жоқ» деп мәлімдейді. Қалай болғанда да,

заңнамалық реттеу мен негізгі құқықтар арасындағы тепе-теңдікті сақтау өте нәзік міндет. Ғылыми сын тұрғысынан, Қазақстан заңнамасына контентті шектеу бойынша шешім қабылдаудың барынша ашық және сот бақылауында болатын тәртібін енгізу ұсынылады. Яғни, егер қандай да бір пост не сайт заңсыз деп танылып бұғатталса, оның дәлелді негіздемесі жариялануы, сайт иесіне сотқа шағымдану мүмкіндігі берілуі тиіс. Бұл принциптер кейбір Батыс елдерінің тәжірибесінде бар және цензураға жол бермеуге көмектеседі.

6. Кадрлық және техникалық қамтамасыз етудің жеткіліксіздігі. Жоғарыда айтылғандай, киберқылмыспен күресуде білікті мамандардың тапшылығы сезіледі. Цифрлық криминалистика, желілік қауіпсіздік саласында сарапшылар аз, барлары көбіне жеке секторда жоғары жалақылы жұмысқа кетеді. Мемлекеттік органдарда кадрларды ұстап қалу қиындап тұр. Бұл олқылықты жою үшін заңнамалық деңгейде құқық қорғау қызметкерлерінің еңбекақысын арттыру, киберқауіпсіздік мамандарына арналған бөлек әлеуметтік пакет қарастыру керек деген ұсыныс бар. Сондай-ақ оқыту стандарттары да өзгере бастады: ІІМ және Бас прокуратура жанындағы академияларда киберқылмысқа қарсы күрес мамандандырулары ашылды.

Мысалы, 2024 жылы құқық қорғау академиясында тыңдаушыларға «Цифрлық криминалистика және кибертергеу» курсы енгізіліп, алғашқы түлектер дайындалуда екені хабарланды. Мұның барлығы - кадр әлеуетін нығайтуға бағытталған қадамдар. Бірақ мамандарды тек оқытып қою жеткіліксіз, оларды іс жүзінде күрделі істерге жұмылдыру, біліктілігін тұрақты көтеру қажет. Сот-сараптама орталықтарында да техникалық құралдарды жаңарту күн тәртібінде: мысалы, шифрланған смартфондардың ішіндегі деректерді бұзып алу үшін Izmir, Cellebrite UFED сияқты озық құралдар керек, олармен біздің криминалистерді қамтамасыз ету маңызды. Бұл мақсаттарға бюджеттен қаражат қарастырылып жатыр, алайда көлемі шектеулі.

7. Үйлестіру мен жауапкершілік қайшылықтары. Киберқауіпсіздік - пәнаралық сала, сондықтан Қазақстанда да оның түрлі аспектілері әр түрлі органдарға бөлінген. Мәселен, контенттік қауіпсіздікке Ақпарат және қоғамдық даму министрлігі мен Бас прокуратура жауапты, инфрақұрылымдық қауіпсіздікке Цифрлық даму министрлігі мен ҰҚК жауапты, киберқылмысты тергеуге ІІМ мен Қаржы мониторингі агенттігі (ақша жылыстатуға қатысты) жауапты, ал балаларды қорғауға Білім министрлігі мен Омбудсмен қатысады. Мұндай көптігі кейде өкілеттіктердің қайталануына не вакуумына соқтырады. Мысалы, дербес деректердің жай интернетте таралып кетуі бойынша кім шұғыл шара қолдануы керек - Ақпараттық қауіпсіздік комитеті ме, әлде Полиция ма? Кейде әрқайсысы бір-біріне сілтеп, уақыт жоғалады. Бұл мәселені шешу үшін киберқауіпсіздік бойынша ұлттық үйлестіруші орган құру қажеттігі туындады. 2017 жылғы «Киберқалқан» тұжырымдамасында да барлық мүдделі тараптарды біріктіретін орталықтандырылған құрылым қарастырылған еді [71]. Соның негізінде 2018 жылы Ұлттық қауіпсіздік комитеті құрамында Ақпараттық қауіпсіздік ұлттық үйлестіру орталығы құрылғаны мәлім. Алайда ол тек

мемлекеттік органдардың инфрақұрылымын қорғауға көбірек көңіл бөлді де, жалпы криминогендік ахуалды үйлестіруде әлсіз болды. Қазір үкімет «Киберқауіпсіздік агенттігі» немесе соған ұқсас дербес орган құру мәселесін қарастыруда деген бейресми ақпарат бар. Егер ондай орган құрылса, оның заңнамалық мәртебесін, құзыретін айқын белгілеу керек, әйтпесе қайталау тағы пайда болуы мүмкін.

8. Халықаралық стандарттарды имплементациялау. Цифрлық саладағы стандарттар өте жылдам жаңаруда (ISO, NIST стандарттары, т.б.), ал ұлттық заңнама оларды ілесе қабылдап үлгермей жатыр. Мысалы, электрондық қолтаңба үшін Қазақстанда ГОСТ негізіндегі стандарт қолданылса, халықаралық тәжірибеде ETSI стандарттарына көшу жүріп жатыр. Сол секілді, бұлтты есептеулердің қауіпсіздігі, IoT (заттар интернеті) құрылғыларын сертификаттау сияқты жаңа мәселелер заңнамада әлі көрініс таппаған. Бұл - әзірге өте техникалық мәселелер, бірақ алдағы 5-10 жылда заңдық маңызға ие болады. Сондықтан заңнаманы болашаққа бейімдеп, қазірден «икемді реттеу» принципін енгізген жөн. Мысалы, «Ақпараттандыру туралы» заңға «мемлекеттік органдар ақпараттық қауіпсіздік бойынша халықаралық стандарттарды кезең-кезеңімен енгізуге міндетті» деген сияқты жалпы норма қосуға болады. Бұл уәкілетті органдарға ауқымды құқық берер еді, бірақ нақты стандарт атауларын заңға жазып қою оның тез ескіруіне апарады. Сол себепті, ғалымдар заңнамада технологиялық бейтараптық қағидатын сақтау керектігін атап өтеді - яғни нормалар нақты технологияға тәуелді болмай, жалпы принциптерді бекіткен дұрыс.

Жоғарыда аталған қайшылықтар мен олқылықтар Қазақстанның киберкеңістікті құқықтық реттеу режимін жетілдіру қажеттігін көрсетеді. Ғылыми сын тұрғысынан алғанда, негізгі мәселе - қауіпсіздік пен бостандық арасындағы тепе-теңдік. Мемлекет бір жағынан азаматтарды киберқауіптерден қорғауы керек, екінші жағынан бұл қорғау құралдары азаматтардың конституциялық құқықтарын шектемеуі тиіс. Осы дилеммада «Алтын орта» табу заң шығарушының және құқық қолданушының басты міндеті. Мысалы, цензура мен интернет еркіндігі тақырыбында қарсы пікірлер бір-біріне қайшы келеді: Үкімет «бала қауіпсіздігі, ұлттық қауіпсіздік маңызды» десе, азаматтық қоғам «кей бастамалар сөз бостандығын шамадан тыс шектейді» деп дабыл қағуда [56]. Бұл жерде мемлекет пен қоғам арасында диалог қажет, заң жобалары кеңінен талқыланып, сарапшылардың ескертпелері ескерілуі тиіс. 2023 жылы «БАҚ туралы» жаңа заң жобасы қаралғанда мұндай диалогтар өтті, нәтижесінде кейбір даулы нормалар жұмсартылды.

Сонымен бірге, құқық қолдану практикасына ғылыми-техникалық жетістіктерді енгізу қажеттігі де сыналады. Мысалы, кейбір тергеушілер мен судьялар киберқылмыс істерінде ескі тәсілдермен жұмыс істеп, цифрлық айғақтардың құндылығын төмендетіп қарайды. Оларды оқыту, санасын жаңарту - уақыт талабы. Дәлелдемелерді бағалау стандарттары да қайта қаралуы керек: шетел соттары сияқты, біздің соттар да электрондық дәлелдеменің тұтастығын растау әдістерін талап етуі керек (хэш мәні,

сарапшының қорытындысы). Қазір кейде экраннан түсірілген скриншотты еш қатесіз айғақ деп қабылдай салатын жағдайлар болады, бұл - әділетсіздікке ұрындыруы мүмкін. Контраргументтер мен баланс іздеу. Кейбір сарапшылар Қазақстан заңнамасын киберкеңістікке қатысты тым қатаң деп сынайды, халықаралық Freedom House сынды ұйымдар елді «Интернеті еркін емес» деп бағалайды [61]. Алайда, басқа мемлекеттердің тәжірибесіне қарасақ, көптеген дамыған елдер де соңғы уақытта интернетті реттеуді күшейтуде. Германия, Ұлыбритания, Австралияның мысалдары жоғарыда келтірілді - олардың заңдары Қазақстан қабылдаған шаралардан қатаң болмаса, кем емес. Мысалы, Германияның жаңа заңнамасы бойынша әлеуметтік желі заң талабын орындамаса, жаһандық табысының 4%-ына дейін айыппұл салынады [56], Британияда балаларға зиянды дизайн ұстанымдарын бұзғаны үшін миллиондаған фунт айыппұл салынуы мүмкін [56]. Салыстырғанда, Қазақстанның жалған ақпарат үшін жеке адамға салатын айыппұлы ~$ 160 шамасында ғана екен (69 мың теңге) [72]. Демек, Қазақстан заңнамасы әлемдік үрдістен алыс кетпеген, бірақ тәжірибеде оның қолданылуы ашық және әділ болуын қадағалау маңызды. Қорытындылай келе, заңнамалық олқылықтарды жою мен қайшылықтарды реттеу бағытында ұсыныстар келесі бөлімде жинақталып беріледі. Ең бастысы - ғылыми зерделеу нәтижелерін заң шығарушы ескеріп, құқық қолданушы органдар сол өзгерістерді іске асырғанда бірізді практика қалыптастыруы қажет. Тек сонда ғана киберкеңістікті реттеу режимі толыққанды және әділ деп сипатталмақ.

Цифрлық дәлелдемелермен жұмыс: құқықтық регламент және стандарттау мәселелері. Киберкеңістіктегі құқық бұзушылықтарды тергеп-тексеру барысында цифрлық дәлелдемелермен жұмыс істеу басты мәнге ие. Компьютерлер, смартфондар, серверлер және желілік журналдар тергеушілер мен соттарға қажетті айғақтардың қайнар көзі болып табылады. Алайда, цифрлық дәлелдемелерді жинау, бекіту және пайдалану дәстүрлі дәлелдемелерден айтарлықтай ерекшеленеді. Сондықтан бұл салада арнайы құқықтық регламенттеу мен стандарттарды қолдану өте маңызды.

Қазақстанда цифрлық дәлелдемелер мәселесі соңғы онжылдықта ғана күн тәртібіне шыға бастады және оны шешуде белгілі прогрестермен қатар, елеулі проблемалар да бар. Электрондық деректер көзге көрінбейді, тез жойылуы немесе өзгертілуі мүмкін, оларды түсіну үшін арнайы техникалық құралдар қажет. Мысалы, қағаз құжатта қолтаңбаның түпнұсқалығын графологиялық сарапшы анықтаса, электрондық файлдың түпнұсқалығын тек хэш-кодын тексеру арқылы дәлелдеуге болады. Сол сияқты, электрондық хат алмасудың шынайылығын растау үшін оның сервердегі log-файлын алу керек. Мұның барлығы - цифрлық дәлелдемелерге арналған арнайы процедуралардың қажеттілігін көрсетеді.

Қазіргі Қылмыстық-процестік кодексте (ҚПК) цифрлық дәлелдемелер ұғымы тікелей жоқ, бірақ жанама нормалар бар. ҚПК-нің 115-бабында «заттай дәлелдемелер» қатарына электрондық тасымалдаушылардағы ақпарат та жататыны айтылған, ал «құжат» ұғымы кез келген ақпарат тасымалдау құралындағы деректі қамтиды деп түсіндіріледі. Осыған сүйеніп, тергеушілер

компьютерлік файлдарды, аудио-видео жазбаларды дәлел ретінде іске қосады. Дегенмен, цифрлық дәлелдемелерді жинау әдістемесі арнайы регламенттелмеген. Тергеушілер көбіне ҚПК-нің жалпы тергеу әрекеттері туралы баптарын қолданады: мысалы, компьютер қатты дискін қарау үшін - қарап шығу (осмотр) хаттамасын, телефонды алып ішіндегіні оқу үшін - тінту немесе алу туралы қаулыны, интернет провайдерінен IP-мәліметтерін алу үшін - сұрау салу жолын таңдайды. Мұндай әртүрлі амалдар бір іс ішінде де қолданылып, сотта дәлелдеменің жарамдылығы туралы дау туындауы мүмкін. Мысалы, қорғаушы «тергеуші телефон жадын қарау протоколымен жүргізген, ол шын мәнінде алу әрекеті болуы керек еді, сот бұл айғақты жарамсыз деп тануы керек» деп уәж айтуы ықтимал [69]. Өкінішке қарай, Қазақстан сот практикасы бұл мәселеде біркелкі емес: кей соттар форматтық қателерге көз жұма қарайды, ал кейбірі қатаң процессуалдық талаптарды сақтамауды негіз етіп, айғақты жоққа шығаруы да мүмкін.

Цифрлық дәлелдемелермен жұмысқа қатысты халықаралық стандарттар бар. Соның бірі - ISO/IEC 27037:2012 «Электрондық дәлелдемелерді анықтау, жинау, алу және сақтау бойынша нұсқаулықтары», сондай-ақ 27041, 27042, 27043 секілді стандарттары электрондық дәлелдемелердің соттағы өмірлік циклін қамтиды. Бұл стандарттар, мысалы, электрондық айғақтың тұтастығын сақтау (chain of custody), үздіксізлік (continuity) және түпнұсқалығын растау принциптерін белгілейді. Қазақстанда бұл стандарттар міндетті емес, тек сала мамандарының ұсыным ретінде қолданып жүргені бар. Мемлекеттік сот-сараптама орталығында цифрлық техникалық сараптамалар өз ішкі әдістемелері бойынша жүргізіледі, олар да көбіне осы халықаралық стандарттарға сүйенеді. Бірақ құқық қорғау органдарының әр бөлімінде бірыңғай тәсіл жоқ - бір жерде компьютерді көшірмелеу үшін арнайы Write-blocker құрылғысын пайдаланады (диск жазудан қорғалады), ал басқа жерде тергеуші жай компьютерді қосып, ішін қарай салуы мүмкін. Бұл әрине дұрыс емес, өйткені екінші жағдайда қорғаныс «дискінің мазмұны өзгеріске ұшырады, айғақ бұрмаланды» деп дауласуы ғажап емес.

2023 жылы Әділет министрлігі «Криминалистикалық қамтамасыз ету туралы» заң жобасы аясында электрондық дәлелдемелерге қатысты кейбір нормаларды қосуға ниет білдірді. Бұл жоба бойынша электрондық ақпаратты алу кезінде міндетті түрде оның көшірмесін жасатып, түпнұсқаны мөрлеп сақтау, көшірмеге маманның қорытындысын алу, электрондық дәлелдің хэш-сигнатурасын хаттамаға енгізу сияқты талаптар ұсынылған еді. Алайда заң жобасы әлі талқылау деңгейінде тұр. Өз кезегінде, Бас прокуратура қазірдің өзінде тәжірибеде цифрлық айғақтармен жұмысқа біраз жаңалық енгізуде: прокуратораның ақпараттық жүйелері (Электрондық қылмыстық іс жүйесі) арқылы тергеушілерге бұлттық қоймаға дәлелдемелерді жүктеу, олардың өзгермегенін бақылау функциялары берілген. 2021 жылдан бастап кейбір өңірлерде «электрондық қылмыстық іс» пилоттық жобасы іске қосылып, онда барлық материалдар цифрлық түрде жүргізілуде. Бұл жүйеде файлдардың интегритеті автоматты түрде қадағаланады (MD5, SHA сияқты алгоритмдермен). Яғни, техникалық стандарттау бар, тек оны құқықтық

рәсімдеу қалып тұр. Бүгінгі таңда Қазақстан соттары цифрлық дәлелдемелерге біртіндеп бейімделуде. Бірқатар прецеденттерге тоқталсақ: 2020 жылы Алматы қалалық соты интернет алаяқтық туралы істі қарау барысында WhatsApp хат-хабарларын дәлел ретінде қабылдады. Қорғаушы ол скриншоттардың қолдан жасалғанын алға тартқанда, сот хат-хабарлардың түпнұсқасын ұялы телефоннан тікелей көрсеттіруді талап етті. Тергеуші телефонды сот залына әкеліп, сол жерде қажет чаттарды ашып көрсетті, судья оны хаттамаға енгізді. Сөйтіп, істі қарауда заманауи әдіс қолданылды.

Тағы бір мысал, 2022 жылы Астана соты кибершабуыл туралы іс бойынша сервердің журнал жазбаларын (log) зерттеу үшін компьютерлік техникалық сараптама нәтижелеріне сүйенді. Сарапшы журналдағы IP-адрестерді және уақыты бойынша пайдаланушы аккаунттарының белсенділігін талдап, айыпталушының кінәсін жанама түрде растайтын қорытынды берді. Сот бұл қорытындыны ескеріп, үкімге негіз етті. Мұндай тәжірибелер алда жиілей береді, сондықтан электрондық дәлелдемелерді бағалау қағидаттарын тезірек бекіту қажет.

Цифрлық дәуірде жеке өмірге қол сұғу мен мониторинг мәселесі өткір туындайды. Электрондық дәлелдемелерді жинау - кейде интернеттегі жеке хаттарды оқу, жеке құрылғыларды ақтару деген сөз. Сондықтан бұл процесте конституциялық құқықтарды сақтау аса маңызды. OSCE сарапшылары атап өткендей, онлайн сөйлесу, әлеуметтік желідегі белсенділік - сөз бостандығы мен құпиялылық құқықтарына жатады, сол себепті электрондық айғақтарды алу кезінде артық қадағалау мен жеке өмірді шектеуге жол бермеу керек [70].

Қазақстандық заңнамада бұл балансты қамтамасыз етуге тырысатын нормалар бар: мысалы, жедел-іздестіру іс-шараларын санкциялау (телефон тыңдау, интернет трафикті бақылау) тек сот немесе прокурор арқылы жүзеге асады. Әйтсе де, құқық қорғау органдарына кең өкілеттіктер берілген (ҰҚК-нің байланыс операторлары желісін бақылауы, ІІМ-нің провайдерлерден мәлімет алуы т.б.). Қоғамдық бақылау бұл салада қиын, себебі бәрі құпия режимде өтеді. Алдын алу үшін кей сарапшылар “цифрлық омбудсмен” институтын енгізуді ұсынады - яғни, азаматтардың цифрлық құқықтарын бұзу жағдайларын тексеретін тәуелсіз тұлға (кейбір елдерде мұндай лауазым бар). Қалай дегенде де, цифрлық дәлелдемелерді пайдалану барысында «қажетті және үйлесімді» (necessary and proportionate) деген халықаралық принцип сақталуы тиіс: мемлекет азамат құқығын тек шектен тыс қажет болғанда, және қоғамдық мүдде үшін пропорционалды деңгейде ғана шектей алады.

Қазақстанның цифрлық дәлелдемелермен жұмыс істеу тәсілдерін стандарттау үшін төмендегідей қадамдар ұсынылады:

- Заңнамалық деңгейде: ҚПК-ке «электрондық (цифрлық) дәлелдеме» ұғымын енгізу, электрондық ақпаратты қарау, алу, сақтау бойынша арнайы баптар қосу. Мысалы, Өзбекстан қабылдаған заң моделі бізге сәйкес келеді: онда электрондық дәлелдеме ұғымы беріліп, оны ұсыну мен растау тәртібі жазылған [70]. Бұған қоса, ӘҚБтК және Азаматтық процестік кодекске де цифрлық айғақтарға қатысты ережелер қажет, өйткені әкімшілік құқық

бұзушылық және азаматтық істерде де электрондық дәлелдемелер жиі пайдаланылады.

- Ведомстволық нұсқаулықтар: Тергеушілер мен жедел қызметкерлерге арнап Бас прокуратура, ІІМ, ҰҚК бірлескен бұйрық немесе методикалық хат шығаруы мүмкін. Онда электронды дәлелдеме жинаудың стандартты операциялық процедуралары (Standard Operating Procedure, SOP) баяндалса - мысалы, компьютерді алу кезінде: 1) токтан ажырату; 2) мөрлеу; 3) сараптамаға жіберу; 4) қосқанда write-blocker қолдану, т.б. көрсетілсе. Мұндай бірізді ереже құқық қорғаушыларға да пайдалы, соттарға да түсінікті болады. АҚШ, Еуропа полициясында “Digital Evidence First Responder Guide” деген сияқты нұсқаулықтар бар, Қазақстан да сол тәжірибені қолдана алады.

- Техникалық құралдармен жарақтандыру: Барлық облыстық полиция департаменттеріне жылдам дискі көшіру құрылғылары, форентикалық бағдарламалар (EnCase, FTK, Cellebrite) және қызметкерлерді оларға үйрету қамтамасыз етілуі шарт. Қазіргі кезде мұндай құралдар тек орталық аппаратта немесе ірі қалаларда бар, ал аудандарда тергеушілер қарапайым әдіспен жұмыс істеп, дәлелдердің тұтастығын байқаусызда бұзып қоюы мүмкін. Стандарт бойынша кез келген электрондық құрылғыдан мәлімет алу тек сертификатталған құрал арқылы жүргізілуі тиіс - соны қамтамасыз ету маңызды.

- Сотта электрондық дәлелдемелерді ұсыну тәртібі: Қылмыстық іс жүргізуде дәстүрлі папка-папка қағаз алып жүру қалып барады, сол үшін соттар техникалық жабдықталуы да артуда (мультимедиялық залдар, экрандар). Электрондық дәлелдерді қарау сот процесінде ашық, түсінікті өтуі үшін соттарға да нұсқаулар керек. Мысалы, судья қажет деп тапса, айғақ ретінде ұсынылған файлдың хэш-кодын қайта есептетіп, түпнұсқамен салыстырта алуы тиіс. Ол үшін сот сарапшылары немесе IT-мамандар шақырылуы мүмкін. Заңнамада судьяның мұндай әрекеттерді тағайындау құқығы нақтыланса, процессуалдық айқындық пайда болар еді.

Жалпы, цифрлық дәлелдемелерді тиімді пайдалану - Қазақстанның құқық қорғау жүйесін заманауи деңгейге көтерудің бөлінбес бөлігі. Ғылыми еңбектерде цифрлық криминалистика Қазақстанда енді қалыптасып келе жатқаны, бірақ болашағы зор екені айтылып жүр [73]. Цифрлық технологиялар қылмыстарды тезірек ашуға, кінәлілерді дәлелдеуге үлкен мүмкіндік береді. Бір мысал, 2023 жылы Алматыда орын алған кибершабуыл ісінде сарапшылар желілік трафик анализі арқылы қылмыскерлерді бір тәулік ішінде анықтады - егер дәстүрлі әдіспен іздесе, апта кетер еді. Бұл - цифрлық криминалистиканың тиімділігін көрсетеді. Ендеше, оны құқықтық дұрыс арнаға түсіру ғана қалып тұр.

Айта кететін жайт - трансшекаралық қылмыстар бойынша электрондық дәлелдер алу үшін Қазақстан көбіне шетелдік корпорацияларға немесе мемлекеттерге жүгінеді (мысалы, e-mail сервері АҚШ-та тұрса). Мұндайда MLAT (өзара құқықтық көмек) механизмінің баяулығы мәселе туғызады, оны шешу үшін Қазақстан Будапешт конвенциясына қосылуы керек екені бұған дейін айтылды. Конвенцияның 31-34 баптары халықаралық е-жедел көмек

мәселелеріне арналған, онда жедел сақтап қою (expedited preservation) және тікелей трансшекаралық қолжетімділік сияқты прогрессивті тәсілдер бар [58]. Бұл нормалар біздің тәжірибеге енсе, тергеушілер уақыт ұтатыны анық. Сондықтан, цифрлық дәлелдемелердің трансшекаралық алуын жеңілдету - халықаралық деңгейдегі стандарттау деуге болады.

Қорытындылай келе, Қазақстанда цифрлық дәлелдемелермен жұмыс істеу саласын регламенттеу мен стандарттау кезең-кезеңімен іске асырылуда, бірақ қарқынын күшейту қажет. 2024-2025 жылдары электрондық дәлелдемелер туралы арнайы нормалар заңнамаға енетініне үміт зор (соған қатысты саясат хаттамалары дайындалуда). Ал қазіргі өтпелі кезеңде құқық қорғаушылар ISO стандарттарын, халықаралық алдыңғы тәжірибені өз бетінше басшылыққа алғаны жөн. Технологияның дамуы құқықтық жүйенің дамуын да жеделдетуге тиіс - бұл аксиома жаңа мыңжылдықта айқын сезілуде.

**Авторлық пікір және ұсыныстар: Қазақстанның киберкеңістікке қатысты заңнамасын жетілдіру жолдары.** Жоғарыда жүргізілген талдау негізінде Қазақстан Республикасының киберкеңістікке байланысты құқықтық реттеуінде бірқатар мықты тұстармен қатар кемшіліктер бары анықталды. Авторлық тұрғыдан алғанда, қолданыстағы заңнама мен практикадағы мәселелерді еңсеру үшін кешенді шаралар пакеті қажет. Төменде сол ұсыныстар жүйеленген түрде беріледі:

1) Заңнаманы халықаралық стандарттарға сәйкестендіру және халықаралық ынтымақтастықты кеңейту. Қазақстанға киберқылмысқа қарсы күрестің жаһандық тәртібіне толық ену үшін тез арада Будапешт конвенциясын ратификациялау маңызды. Бұл электрондық дәлелдемелерді жедел алу, трансшекаралық қылмыстарды бірлесе ашу ісінде құқықтық негіз қалыптастырады [58]. Конвенция талаптарына сай Қылмыстық және Қылмыстық-процестік кодекстерге өзгерістер енгізіп (цифрлық дәлелдемелер туралы бөлім қосу, желілік провайдерлердің жедел көмек көрсету міндеттерін бекіту), өзара құқықтық көмек тетіктерін жетілдіру қажет. Сондай-ақ, Интерполдың Cybercrime Rapid Response бағдарламаларына қатысу, шет мемлекеттермен екіжақты келісімдер жасау (мысалы, Ресей, Қытай, Түркия сияқты елдермен деректер алмасу жөнінде) ұсынылады.

2) «Киберқауіпсіздік туралы» кешенді заң немесе акт қабылдау. Қазіргі заңдар бытыраңқы реттейтін (Қылмыстық кодекс, ӘҚБтК, Балаларды қорғау заңы т.б.) киберкеңістік мәселелерін бір жүйеге түсіру үшін “Киберқауіпсіздік туралы” арнайы заң қабылдау орынды. Онда киберқауіпсіздік субъектілері (меморгандар, жеке сектор, қауымдастықтар), олардың міндеттері, кибершабуыл болғанда әрекеттесу тәртібі, ақпарат алмасу режимі, бизнеске қойылатын негізгі талаптар (мысалы, КВОИКИ ұғымына кіретін объектілер тізімі) сияқты нормалар топтастырылуы мүмкін. Мұндай заң Ресейде (“Ақпараттық қауіпсіздік доктринасы” және соған сай заңдар), Беларусьте бар. Қазақстанның 2017 жылғы Тұжырымдамасы негізінде осындай заңнамалық акт әзірлеу логикалық қадам болмақ [71].

3) Балаларды онлайн ортамен байланысты құқық бұзушылықтардан қорғауды күшейту. 2018 жылғы заңды жаңғыртып, немесе жаңадан «Балаларды онлайн зияннан қорғау туралы» заң қабылдау ұсынылады. Онда интернет-платформалардың жауапкершілігі анық көрсетілуі тиіс: балаларға қатысты кибербуллинг мазмұнын анықтау және жою міндеті, зиянды ақпаратты таратпауға алдын-ала шаралар қолдану (контентті модерациялау, жастық фильтрлер орнату), сондай-ақ заң талаптарын орындамағаны үшін санкциялар (айыппұл, платформаны уақытша тоқтата тұру) қарастырылуы керек [56]. Сонымен бірге, ата-аналардың жауапкершілігі мен құқықтары да сақталуы қажет - мысалы, балаға зиянды контент келсе, ата-ана провайдерден оны өшіруді талап ету механизмі болуы керек [61]. Арнайы уәкіл - Балалардың цифрлық құқықтары жөніндегі омбудсмен лауазымын енгізу де пайдалы қадам: ол ата-ана, балалар шағымдарын қарап, платформа және мемлекетпен арада дәнекер болар еді.

4) Цифрлық дәлелдемелерге қатысты құқықтық базаны бекіту. Қылмыстық-процестік кодекске жеке тарау етіп «Электрондық дәлелдемелер» деген бөлім енгізуді ұсынамыз. Онда электрондық дәлелдің ұғымы, оны жинақтау (қарап тексеру, алу), сақтау (түпнұсқаны мөрлеу, көшірме жасап мұрағаттау), сотта зерттеу (цифрлық технологияларды қолдану) тәртіптері жан-жақты жазылуы тиіс. Мысалға, Ұлыбританияның Әділет министрлігі шығарған ACPO Guidelines for Digital Evidence сияқты құжаттарды негізге алуға болады. Сонымен бірге, сот-сараптамалық стандарттарды заң деңгейінде бекіткен жөн: әрбір электрондық дәлел сарапшы қорытындысымен расталса, оның дәлелдік күші артатыны сөзсіз [73]. Соттар үшін Жоғарғы Сот деңгейінде түсіндірме қаулы қабылдануы керек, ол электрондық хаттамалардың, скриншоттардың, лог-файлдардың қандай шарттарда дәлел болатынын айқындап берсе - бүкіл ел бойынша бірыңғай практика орныгар еді.

5) Киберқылмыспен күресуші органдардың институционалдық күшін арттыру. ІІМ құрамындағы Киберполиция департаментінің штаттық санын ұлғайтып, оны дербес комитет деңгейіне көтеру мүмкіндігін қарастыру керек (мысалы, Есірткі қылмысына қарсы күрес комитеті сияқты). Бұл оған тікелей облыстық басқармаларға нұсқау беріп, кадрларды өздігінше тағайындап, бюджеттік қаржыны бөлуге мүмкіндік береді. Сонымен бірге, Бас прокуратура жанындағы Құқықтық статистика орталығында “киберқылмыс” деген жеке санат енгізіп, оның есебін бөлек жүргізу керек - сонда проблема ауқымы мен трендтері анық көрінеді. Ұлттық қауіпсіздік комитетінің киберқауіпсіздік бөлімшелерінің де әлеуетін арттыру қажет, әсіресе критикалық инфрақұрылымды қорғау және кибертыңшылықпен күрес бағытында. Бұған қоса, мемлекеттік-жекеменшік әріптестікті пайдалану - елдегі ақпараттық қауіпсіздік компанияларымен, академиялық орталықтармен бірлесіп жобалар жүргізу киберқылмыспен күресте инновацияларды алып келмек. Мысалы, белгілі антивирус компанияларымен, телеком операторларымен Меморандумдар түзу арқылы зиянды

бағдарламалар деректерін бөлісу, шабуылдар туралы ақпарат алмасу жолға қойылуы керек.

6) Халықтың цифрлық мәдениетін көтеру және превентивті шаралар. Құқықтық реттеу қаншалықты жетілдірілсе де, егер халық интернеттегі қауіптер туралы хабарсыз болса, проблема шешілмейді. Сондықтан білім беру жүйесінде кибергигиена тақырыптарын күшейту керек: мектепте - «Интернет және қауіпсіздік» факультативі, ЖОО-да - барлық мамандықтарға «АКТ қауіпсіздігі негіздері» курсын оқыту. БАҚ пен әлеуметтік желілерде тұрақты түрде алаяқтықтың жаңа схемалары, қауіпті сайттар туралы хабардар ету жүргізілуі тиіс. Мемлекет мұндай ақпараттық науқандарды ҮЕҰ-мен бірлесіп қаржыландырса құба-құп. Бұл профилактикаға жұмсалған қаражат кейін жүз есе қайтады, себебі қылмысты болған соң тергеуге кететін ресурс үнемделеді. Әрі заңның пәрмеңділігін арттырудың ең жақсы жолы - азаматтардың оны саналы түрде сақтауына қол жеткізу екені белгілі.

7) Контентті құқықтық шектеу механизмдерін жетілдіру. Қазіргі «сайтты бұғаттау» жүйесін демократияландыру қажет. Ұсыныс: тәуелсіз сарапшылар комиссиясын құру, ол бұғаттауға ұсынылған сайттардың мазмұнын қарайды. Оның құрамында мемлекеттік орган өкілдерімен қатар, қоғам және БАҚ өкілдері болса, шешімдер әділ болады. Бұғаттау шешімі (сот шешімінен тыс жағдайларда) Бас прокуратура жанынан шығарылғаны жөн - өйткені прокурорлық қадағалау кепілдігі бар. Әрі әрбір бұғатталған сайттың тізімі, себебі (экстремизм, порнография, т.б.) ашық реестрде жарияланып тұруы керек. Бұл мемлекеттік цензураға деген қоғамдық бақылауды күшейтеді. Егер қандай да бір контенттің заңсыздығына қоғам күмән білдірсе, сотта оны даулау мүмкіндігі қалуы тиіс. Осылайша, қауіпсіздік пен сөз бостандығы арасындағы баланс сақталады деп ойлаймыз [56].

8) Киберқылмыстарға қолданылатын жазаларды саралау. Кейбір қылмыстар бойынша жаза мөлшерін қайта қарау керек. Мысалы, кибербуллингтің ауыр түрлері (жәбірленушінің өзіне қол салуына әкелсе) - қазіргі ҚК-де «өзін-өзі өлтіруге итермелеу» бабымен 3-5 жыл беріледі, оны 7-10 жылға дейін арттыру жөн. Себебі мұндай әрекеттердің қауіптілігі өте жоғары, ал қоғамдық резонанс олар үшін қатаң жаза талап етеді. Керісінше, интеллектуалдық меншік құқықтарын интернетте бұзғаны үшін ҚК 198-бабында 5 жылға бас бостандығынан айыру көзделген - бәлкім, бұл қылмысты экономикалық санкциялар (айыппұл, түзету жұмыстары) деңгейінде қалдыру жеткілікті болар. Өйткені тікелей зорлық жоқ, қоғамға қатты қауіп төнбейді. Осылайша, жазалау саясатында киберқылмыс түрлерінің қоғамдық қауіптілік дәрежесін ескеру қажет. Әкімшілік кодексте де айыппұл мөлшерлерін мезгіл-мезгіл индексациялап отыру керек, әйтпесе олар уақыт өте тиімділігін жоғалтады (қазірдің өзінде 20-30 АЕК айыппұл кей құқық бұзушыларды тоқтатпайды).

9) Ғылыми зерттеулер мен сараптама қорытындыларын заң шығармашылығына енгізу. Қазақстанда киберқауіпсіздік, ақпараттық құқық бағытында зерттеулер көбейіп келеді (жоғарыда пайдаланылған дереккөздер - солардың айғағы). Мемлекет осы ғылыми әлеуетті пайдалану тетіктерін

жасауы тиіс. Мысалы, Парламент жанынан «Цифрлық даму жөніндегі сарапшылар кеңесін» құрып, оған ғалымдар, IT-қоғамдастық өкілдерін кіргізіп, заң жобаларына олардан қорытынды алу. Не болмаса, Жоғарғы Сот жанындағы Ғылыми-консультативтік кеңеске Кибер құқық маманын қосу, жаңа құқықтық мәселелер бойынша Пленум қаулыларын әзірлеуге тарту.

Ғылыми негізделген ұсыныстар заң шығару сапасын көтереді, құқық қолдануда дауларды азайтады. Мысалы, Британ парламенті Law Commission арқылы үнемі осындай сарапшылықты пайдаланады, Қазақстан да соған ұқсас институттар дамытуы керек.

10) Халықаралық озық тәжірибені имплементациялау. Авторлық пікір бойынша, Қазақстанға мынадай шетелдік тәжірибелерді қабылдау пайдалы: А) Австралияның e-Safety моделі - балалардың онлайн қауіпсіздігіне жауапты дербес агенттік құру [56]; Ә) Еуропалық Одақтың GDPR принциптерін - дербес деректердің халықаралық алмасуы, ұмытылу құқығы, т.б. - біртіндеп өз заңдарымызға енгізу; Б) АҚШ-тың NIST киберқауіпсіздік негіздерін - критикалық инфрақұрылымда risk management, incident response стандарттарын қабылдау; В) Оңтүстік Кореяның тәжірибесі - мектептерде киберқауіпсіздік еріктілерін (кибердружинниктер) даярлап, буллингті оқушылар арасынан анықтау жүйесін құру; Г) Эстонияның цифрлық үкімет үлгісі - мемлекеттік ақпараттық жүйелерді толық цифрландыру және олардың қауіпсіздігіне азаматтық бақылау енгізу. Әрине, бұл тәжірибелерді сол күйі көшіру мүмкін емес, ұлттық ерекшелікті ескеріп, бейімдеу қажет. Бірақ негізгі принцип - үздік үлгілерден үйрену - ұстанған абзал.

Жоғарыдағы ұсыныстарды қорытындылай келе, төмендегідей кілтті басымдықтар бөлінеді:

- Құқықтық базаны жүйелеу және толықтыру: Үздіксіз жаңарып отыратын кибер кеңістікті реттеу үшін заңнаманы артта қалдырмай, проактивті жаңарту (жаңа заңдар, ережелер).

- Институционалдық және кадрлық нығайту: Маман кадрларсыз және үйлестіруші органдарсыз ең мінсіз заң да іске аспайды - сол үшін киберқалқан ұстар ведомстволарды күшейту.

- Халық пен бизнес мүддесін тең қорғау: Киберқауіпсіздік шаралары азаматтардың құқығын жөн-жосықсыз шектемеуі тиіс, ал бизнесті реттеу шамадан тыс болмауы керек. Заңдағы әр норма осындай теңгерімді көздеуі қажет [70].

- Алдын алу мен ағарту: Репрессивті шаралармен алысқа бармаймыз, ең дұрысы - құқық бұзушылыққа жағдай туғызбау. Ол үшін превентивті тәрбие, хабардарлық, мәдениет қалыптастыру стратегиялық мәнге ие.

Қазақстан өзінің “Цифрлық Қазақстан” мемлекеттік бағдарламасын іске асыра отырып, халықтың цифрлық сауаттылық деңгейін 2025 жылға қарай 87%-ға жеткізуді мақсат еткен. Бұл үлкен аудиторияны білдіреді, олар үшін қауіпсіз киберкеңістік құру - мемлекет үшін де, қоғам үшін де ортақ міндет.

Сондықтан ұсынылған шараларды жүзеге асыру цифрлық даму мен құқықтық тәртіпті қамтамасыз етудің үйлесімді үлгісін қалыптастыруға мүмкіндік береді деп ойлаймыз. Қорытындыда, киберкеңістіктегі құқық

бұзушылықтармен күрестегі Қазақстанның жолы енді басталып келе жатқанына қарамастан, қазірдің өзінде заңнамалық негіз қалыптасқан, оны әрі қарай үздіксіз жетілдіру - уақыт талабы. Заңнаманы ғылыми негіздеу, халықаралық тәжірибемен байыту және құқық қолдануда заманауи технологияларды пайдалану - осы үш тұғырға сүйене отырып, Қазақстан киберқылмысқа қарсы тиімді құқықтық қалқан (шын мәнінде, «киберқалқан») орната алады деп сенеміз. Мемлекеттің, бизнестің және қоғамның күш-жігерін біріктіру арқылы ғана киберкеңістіктің заңдылық пен қауіпсіздік ортасына айналуы мүмкін екені ақиқат [56]. Бұл - болашақ ұрпақ үшін жасалуы тиіс стратегиялық қадам.

## 2.2. Әкімшілік іс жүргізу аспектілері: дәлелдемелерді жинау, сараптау және бағалау.

Кәмелетке толмағандардың цифрлық кеңістікте жасайтын құқық бұзушылықтары жыл сайын өзекті әлеуметтік-құқықтық проблемаға айналып отыр. Сандық технологиялардың қарқынды дамуы бір жағынан қоғамға жаңа мүмкіндіктер ашса, екінші жағынан киберқылмыстардың өршуіне алып келді. Қазақстанда 2018 жылы небәрі 589 киберқылмыс тіркелсе, 2021 жылы бұл көрсеткіш 21479-ға дейін «өршіген» [70]. Осындай құқық бұзушылықтардың ішінде интернет-алаяқтық айрықша орын алады: мысалы, онлайн алаяқтық фактілері 2018 жылдан 2023 жылға дейін 40 еседен аса өсіп, 2018 жылғы ~500 істен 2023 жылы 21,8 мың іс тіркелген [29]. Бұл жалпы үрдісте кәмелетке толмағандардың да үлесі бар. Ресми деректер бойынша, 2022 жылдың 9 айында елімізде қылмыстық жауапкершілікке тартылған жасөспірімдер саны 1,1 мыңға жеткен, бұл өткен жылмен салыстырғанда 2,1%-ға көп. Кәмелетке толмаған құқық бұзушылар көбіне ұрлық, тонау, бұзақылық және алаяқтық сияқты әрекеттерге барған. Мысалы, сол кезеңде алаяқтық жасаған 58 жасөспірім анықталды [74].

Киберкеңістіктегі құқыққа қарсы іс-әрекеттерге жасөспірімдер әртүрлі түрде қатысады: біреулері өздері тікелей электрондық алаяқтық, қоқан-лоққы, хакерлік шабуылдар жасауы мүмкін, енді біреулері ересек қылмыскерлердің ықпалымен олардың схемаларына қосылады. 2025 жылы Астана қаласында 17 жастағы колледж студенті зейнеткерді алдап соғатын алаяқтар тобының ақша жинаушысы ретінде жұмыс істегені үшін ұсталды. Тергеу мәліметінше, ол интернетте «жұмыс берушілердің» ұсынысын қабылдап, Telegram арқылы нұсқаулар алып отырған және алданған зейнеткерлерден қолма-қол қаражатты жинап, ұйымдастырушыларға жеткізіп берген [75]. Бұл дерек жасөспірімдердің өздері киберқылмыс субъектісі ғана емес, кейде ересектердің қолшоқпары болатынын көрсетеді. Сондай-ақ, соңғы уақытта білім беру мекемелеріне жарылғыш зат қойылғаны туралы жалған хабарламаларды тарататын «хабарлаушылар» арасында да кәмелетке толмағандар жиілеп кетті. 2024 жылдың басынан қыркүйек айына дейін осындай 168 қылмыстық іс тіркеліп, 31 кінәлі адам ұсталған, олардың 12-сі - кәмелетке толмағандар [76]. Бұл фактілер құқық қорғау органдарынан

жасөспірімдердің кибер құқық бұзушылықтарына жедел ден қоюды, ал қоғам мен отбасынан олардың алдын алу шараларын күшейтуді талап етеді.

Жасөспірімдердің онлайн ортадағы қауіпсіздігі мәселесіне мемлекет пен халықаралық ұйымдар да ерекше назар аударуда. ЮНИСЕФ зерттеуі көрсеткендей, Қазақстандағы балалардың 15%-ы күн сайын интернетте өздеріне зиянды контентке тап болады, ал 21%-ы кибербуллингтің құрбаны болған. Сонымен бірге әрбір оныншы бала бейтаныс адамдарды «дос» ретінде қосып, олардың арбауына түсу қаупін арттырған. Осындай жағдайлар балаларды онлайн зорлық-зомбылық пен қанаудан қорғау қажеттігін айқын көрсетеді. 2025 жылы мемлекет ЮНИСЕФ қолдауымен «Балаларды онлайн зорлық-зомбылықтан, қатыгездік пен қанаудан қорғау» атты екі жылдық бағдарламаны қолға алды. Оның аясында цифрлық кеңістіктегі балалар қауіпсіздігін қамтамасыз ету үшін заңнаманы жетілдіру, жаңа профилактикалық шаралар енгізу, кибербуллингке және балаларды онлайн қанауға қарсы күресті күшейту көзделген. Тиісті ведомствоаралық координациялық комитет құрылып, халықаралық тәжірибе зерделенуде [76].

Ішкі істер министрлігінің дерегінше, қазірдің өзінде алаяқтыққа қарсы «Киберпол» арнайы топтары 2,5 мыңнан астам киберқылмысты ашып, 962 млн теңге залалдың орнын толтырған. Сондай-ақ 58 миллион заңсыз қоңырау (спам-шақыру) бұғатталып, еліміздің 5 қаласында алаяқтар қолданған 19 сим-бокс пен 6000-нан астам тіркелмеген SIM-карта тәркіленді. Үкімет жанындағы құқық бұзушылықтың алдын алу жөніндегі комиссия отырыстарында интернет-алаяқтықпен күрес және қаржы пирамидаларының жолын кесумен қатар, кәмелетке толмағандар арасындағы құқық бұзушылықтардың алдын алу шаралары ұдайы қаралуда [77].

Демек, жасөспірімдердің кибер құқық бұзушылықтарын тиімді тежеу үшін бір жағынан қоғамдық алдын алу жұмыстары қажет болса, екінші жағынан мұндай істер бойынша әкімшілік іс жүргізудің өзі мінсіз жұмыс істеуі тиіс. Әсіресе дәлелдемелерді жинау, сараптау және бағалау механизмдері заман талабына сай жетілдірілсе ғана, кәмелетке толмаған құқық бұзушының кінәсін әділ дәлелдеп, оған ықпал ету шараларын дұрыс қолдануға мүмкіндік туады.

Қазақстан Республикасының әкімшілік заңнамасы дәлелдемелерді жинау, тексеру (сараптау) және бағалау рәсімдерін айқындайтын бірқатар нормаларды қамтиды. ӘҚБтК-нің 762-бабына сәйкес, әкімшілік істер бойынша дәлелдеу дегеніміз істі заңды, негізделген әрі әділ шешу үшін маңызы бар мән-жайларды анықтау мақсатында дәлелдемелерді жинаудан, тексеруден және бағалаудан тұратын процесс. Дәлелдеу барысында құқық бұзушылық фактісін, кінәнің бар-жоғын анықтау және істің өзге де мән-жайларын жан-жақты ашу көзделеді. Заң бойынша әкімшілік құқық бұзушылықтың оқиғасы мен кінәсін дәлелдеу міндеті іс жүргізуді жүзеге асыратын органға (лауазымды тұлғаға) жүктеледі. Яғни, кәмелетке толмағанның кінасын дәлелдеу жауапты мемлекеттік органның тікелей міндеті болып табылады; бұл - in dubio pro reo қағидасына (күдік туындаса, жасөспірімнің пайдасына шешу) сай келеді. Әкімшілік іс бойынша қаралып

жатқан оқиғаға қатысы бар және заңды түрде алынған нақты деректердің бәрі дәлелдеме болып саналады. Дәлелдемелер ретінде тергеу әрекеттерінің хаттамалары, куәлардың айғақтары, сарапшылар қорытындылары, заттай айғақтар, құжаттар және өзге де көздер пайдаланылуы мүмкін. ӘҚБтК-нің 760-бабы бойынша, егер құжаттарда ұйымдар, лауазымды адамдар немесе азаматтар баяндаған мәліметтер істі шешу үшін маңызды болса, ондай құжаттар дәлелдеме деп танылады. Атап айтқанда, бұл категорияға жазбаша немесе өзге тәсілмен тіркелген кез келген ақпарат, оның ішінде осы кодексте белгіленген тәртіппен алынған немесе ұсынылған компьютерлік ақпарат, фотосуреттер, кино- және бейнетүсірілім материалдары, дыбыс жазбаларындағы мәліметтер де жатуы мүмкін [78]. Демек, кибер құқық бұзушылықтар бойынша электрондық цифрлық іздер мен деректерді (интернет хат-хабарлары, құрылғының жадысындағы файлдар, желідегі жазбалар т.б.) заңды жолмен алу - оларды дәлел ретінде пайдалану үшін жеткілікті шарт. Бұл ретте цифрлық дәлелдемелерді жинаудың заңдылығы мен техникалық дұрыстығын қамтамасыз ету аса маңызды.

Дәлелдемелерді жинау әдетте әкімшілік құқық бұзушылық туралы іс қозғауға уәкілетті органдар мен лауазымды тұлғалардың әрекеттері арқылы жүзеге асырылады. ӘҚБтК-нің 763-бабының 1-бөлігіне сәйкес, дәлелдемелер жинау осы кодексте көзделген іс жүргізу әрекеттерін орындау арқылы әкімшілік іс жүргізу барысында жүргізіледі. Іс бойынша хаттамалар толтыру, түсініктемелер алу, куәлерден жауап алу, заттай айғақтарды алу, құжаттарды талап ету сияқты әрекеттер - бәрі дәлелдеме жинау тәсілдеріне жатады.

Мысалы, кәмелетке толмағанның смартфонынан оның құқық бұзушылық жасағанын дәлелдейтін деректер табылса (хат алмасуы, бейнежазбасы, т.б.), полиция қызметкері оны заттай айғақ ретінде іске қосып, тиісті хаттамаға тіркейді. Заң бойынша алынған заттар мен құжаттар бағаланғаннан кейін іске тігілуге тиіс және бұл жөнінде хаттамаға белгі жазылады. Яғни, әрбір цифрлық айғақ (мысалы, телефондағы скриншот немесе электронды журнал жазбасы) алдымен сарапталып, шынайылығы расталған соң ғана іске қосылады; ол туралы хаттама толтырылып, айғақтың түпнұсқасы не куәландырылған көшірмесі іс материалдарына тіркеледі. Әкімшілік іс жүргізуге қатысушылар - жәбірленуші, куә, құқық бұзушы немесе оның заңды өкілі - өздеріндегі заттар мен құжаттарды дәлелдеме ретінде іске ұсынуға құқылы, ол үшін уәкілетті органға өтінішхат береді [78].

Кибер құқық бұзушылық істері бойынша дәлелдеме жинауда арнайы ғылыми-техникалық құралдардың маңызы зор. ӘҚБтК-нің 759-бабы тергеуші, судья немесе іс жүргізуге қатысушылар ғылыми-техникалық құралдарды пайдалану арқылы алынған нақты деректерді пайдалануға құқылы екенін бекітеді. Мұндай құралдарды қолдануға заң тікелей рұқсат етсе немесе тыйым салмаса, ғылыми тұрғыдан негізді болса және істі жылдам әрі қауіпсіз шешуге септессе ғана жол беріледі [78]. Электрондық дәлелдер көбіне арнайы сандық криминалистика тәсілдерімен алынады: құрылғының жадынан өшірілген файлдарды қалпына келтіру, IP-мекенжай арқылы пайдаланушыны анықтау, лог-файлдарды талдау, зиянды бағдарлама

іздерін табу сияқты әрекеттерді кәсіби сарапшылар жүзеге асырады. ӘҚБтК-нің 753-бабына сай, қажетті жағдайда іс жүргізуші орган сараптама тағайындауы мүмкін, яғни білікті сарапшыға дәлелдемелерді зерттеу тапсырылып, ол жазбаша қорытынды береді. Мысалы, жасөспірімнің компьютерінен алынған деректердің рас екендігін не жалған өзгертілгендігін анықтау үшін компьютерлік-техникалық сараптама жүргізілуі ықтимал.

Сарапшы қорытындысы да құжат түріндегі дәлелдеме болып саналады. Сонымен қатар, цифрлық технологиялар арқылы жасалған құқық бұзушылықтарды ашу үшін полиция құрылымында арнайы бөлімшелер құрылған. ІІМ жанындағы Киберқылмысқа қарсы күрес департаменті және оның өңірлердегі бөлімдері электрондық дәлелдерді жинақтау мен зерттеу ісінде озық техникалық құралдарды қолданады. Мысалы, «Киберпол» арнайы топтары әлеуметтік желілер мен мессенджерлерде жасырын жүргізілген хат-хабарларды қадағалап, қажет болса, провайдерлермен ынтымақтаса отырып, күдікті аккаунттардың иелерін анықтайды [77]. Көп жағдайда кибербуллинг, фишинг сияқты заң бұзушылықтарды дәлелдеу үшін интернет-провайдерлерден, ұялы байланыс операторларынан ресми мәліметтер сұратуға тура келеді. ӘҚБтК-нің 761-бабы дәлелдемелер жеткіліксіз болғанда, іске қатысушы судья немесе орган ұйымдар мен бірлестіктерден қосымша мәліметтер талап етіп алдыруға құқылы екенін көздейді [78].

Осы норма шеңберінде тергеуші немесе сот істі дұрыс шешу үшін, мысалы, әлеуметтік желі әкімшілігіне сұрау салып, кәмелетке толмаған құқық бұзушының нақты аккаунтына қатысты тіркеу деректерін, жазбаларын алуы мүмкін. Алайда, қазіргі күні көптеген шетелдік интернет-платформалар Қазақстанның құқық қорғау органдарына онша ынтымақтаса қоймайтыны белгілі. Бұл салада халықаралық келісімдердің тиімділігі айқын көрінеді.

Өкінішке қарай, Қазақстан әлі де болса Будапешт киберқылмыс конвенциясына қосылмаған мемлекеттердің қатарында, бұл біздің органдардың жаһандық тергеу тетіктеріне толыққанды кірігу мүмкіндігін шектейді. Дегенмен 2023 жылғы сәуірде елімізге осы конвенцияға қосылу жөнінде ресми шақыру келді. Сарапшылардың пайымдауынша, Конвенция ережелерін қабылдау - біріншіден, цифрлық дәлелдемелерді жинау мен алмасудың бірыңғай стандарттарын енгізуге, екіншіден, шетелдік әріптестермен өзара құқықтық көмек арнасын кеңейтуге жол ашып, трансұлттық киберқылмыспен күресті тиімдірек етеді [29]. Расында да, киберқылмыстардың басым бөлігі шекарааралық сипатқа ие, құқық бұзушы мен жәбірленуші әр елде орналасуы мүмкін, ал қылмыс іздері тағы бір мемлекетте сақталатын электрондық жүйелерде тұрады [70]. Сондықтан Қазақстанның халықаралық ынтымақтастық тетіктерін (соның ішінде Будапешт конвенциясын) толық пайдалануын қамтамасыз ету - дәлелдеме жинаудың алғышарттарының бірі. Осыған байланысты ұлттық заңнамада цифрлық дәлелдемелерді алу және бекіту тәртібін халықаралық стандарттарға сәйкестендіру қажеттігі туындап отыр. Зерттеушілер Қазақстан заңдарында «киберқылмыс» ұғымының анықтамасы, электрондық дәлелдерді жинау рәсімдері және шетелдік органдармен ынтымақтастық мәселелері әлі

де жүйеленбегенін атап көрсетеді [29]. Бұл олқылықтарды жою үшін ұлттық заңнамаға тиісті толықтырулар енгізіп, жаңа цифрлық реалияларға бейімделген құқық қолдану тәжірибесін қалыптастыру қажет.

Дәлелдемелерді жинау кезінде кәмелетке толмағандардың құқықтары ерекше назарды талап етеді. Әкімшілік іс бойынша жасөспірімдер тек 16 жастан жауаптылыққа тартылатыны белгілі (ҚР ӘҚБтК 63-бабы). Ал 16 жасқа толмаған бала қандай да бір әкімшілік теріс қылық жасаса, ол үшін жауапкершілік оның ата-анасына немесе заңды өкілдеріне жүктеледі (ҚР ӘҚБтК 127-бабы). Мәселен, ҚР ӘҚБтК-нің 442-бабына сәйкес, 17 жасқа толмаған баланың түнгі уақытта үлкендерсіз ойын-сауық орындарында немесе үй-жайлардан тыс жерде болуы - алғашында ата-анасына ескерту жасауға, ал бір жылдың ішінде қайталанса - 15 АЕК мөлшерінде айыппұл салуға әкеп соғады. Аталған норма баланы қараусыз жібергені үшін ата-ананың тікелей жауаптылығын бекітеді. Сол сияқты, егер 14-15 жастағы жеткіншек ұсақ бұзақылық жасаса (қоғамдық орындарды былғап, тәртіп бұзса), оған қатысты әкімшілік іс қозғалмайды, бірақ ата-анасы ҚР ӘҚБтК 127-бабы бойынша «ата-ана міндетін орындамау» бабымен жауапқа тартылады. Яғни дәлелдеме жинау барысында құқық бұзушылықты нақты кім жасағаны анықталса да, бала жасы кіші болғандықтан жаза тікелей оған емес, оның тәрбиешілеріне қолданылады. Мұндай жағдайларда уәкілетті орган баланың әрекетін және ата-анасының оған тиісті деңгейде бақылау жасамағанын дәлелдеуге тиіс. Сондай-ақ құқық бұзушылық жасаған баланың мінез-құлқын түзеу мақсатында оған қатысты тәрбиелік ықпал ету шараларын қолдану мәселесі қаралады. 16-17 жастағы құқық бұзушылар әкімшілік жауаптылыққа тартылғанымен, оларға тағайындалатын айыппұл мөлшері заңмен шектелген (10 АЕК-тен аспауға тиіс), әкімшілік қамау жазасы мүлде қолданылмайды (ӘҚБтК 50-бабы 2-б.), яғни заң кәмелетке толмағандарды ересектермен бірдей жазалауды көздейді.

ӘҚБтК 64-бабы бойынша, жасөспірімге тағайындалатын айыппұлды төлеуге мүлкі немесе қаражаты жетпесе, оны өтеу міндеті ата-анасына жүктеледі [78]. Бұл ережелер мемлекеттің жазалаудан гөрі тәрбиелеуге басымдық беретінін көрсетеді. Әкімшілік іс шеңберінде кәмелетке толмаған адамнан жауап алу, түсініктеме жинау кезінде де оның процессуалдық құқықтары сақталуы керек. Жасөспірімдер өмірлік тәжірибесінің аздығы, психологиялық ерекшеліктері себепті өз әрекеттерінің мәнін толық түсінбеуі мүмкін, сондықтан олардың ісін қарау кезінде заң қосымша кепілдіктер белгілеген. Атап айтқанда, ҚР ӘҚБтК 727-бабына сәйкес, іс жүріп жатқан жеке адамның 18-ге толмауы немесе денсаулығына, психикасына байланысты өз құқықтарын өзі қорғай алмауы жағдайында оның құқықтары мен мүдделерін заңды өкілдері қорғайды. Яғни, кәмелетке толмаған құқық бұзушыға ата-анасы, қорғаншысы не қамқоршысы өкілдік ете алады. Мұндай заңды өкіл ретінде танылатын тұлғалардың туыстық қатынасы тиісті құжаттармен расталуы шарт. Ең бастысы - заңды өкілді іске қатыстыру мерзімі анық белгіленген: бала әкімшілік құқық бұзушылық жасағаны үшін ұсталған кезден немесе істің хаттамасы толтырылған сәттен бастап оның

заңды өкілі процеске жіберілуге тиіс. Демек, полиция бөлімшесіне жеткізілген сәттен бастап ата-анасына хабар беріліп, олар істің басынан қатысуға мүмкіндігі болуы керек. Іс жүзінде де, кәмелетке толмағанды әкімшілік тәртіппен ұстаған жағдайда, ішкі істер органы бұл туралы оның ата-анасына дереу хабарлауға міндетті. Ал іс сотқа жетіп, іс қаралатын кезде жасөспірімнің заңды өкілінің қатысуы міндетті деп тікелей көрсетілген. Егер ата-ана немесе өкіл сот отырысына келуден жалтарса, оларды полиция арқылы мәжбүрлеп алып келуге болады [78]. Бұл талаптар жасөспірімнің құқығын қорғауды қамтамасыз етуге арналған. Бұдан бөлек, кәмелетке толмаған адамның өзі де қорғаушы (адвокат) қатыстыруға құқылы, ал кей жағдайларда (мысалы, ата-анасы болмаған кезде) тергеуші оған адвокатты міндетті түрде тағайындауы мүмкін. Мысалы, Қылмыстық-процестік кодексте 18 жасқа толмаған күдіктіні тергеу кезінде қорғаушының қатысуы міндетті деп белгіленген (ҚР ҚПК 535-бап). Әкімшілік іс жүргізуде бұл талап тікелей қарастырылмағанмен, ауыр немесе күрделі істерде жасөспірімге кәсіби құқықтық көмек көрсету әділеттілік үшін маңызды. Сонымен бірге, ҚПК нормалары бойынша кәмелетке толмағанды жауаптау кезінде педагог немесе психолог қатысуы қажет (жасына қарай) [79]. Әкімшілік іс жүргізуде мұндай арнайы маман қатыстыру міндетті емес, бірақ тергеу практикасы күрделі киберқылмыстарда (әсіресе жәбірленуші бала болса) педагог-психологтың кеңесін пайдалану керектігін көрсетеді.

Мысалы, балаға түсініксіз техникалық жайттарды дұрыс жеткізу, оның психикасына зақым келмеуін қадағалау үшін педагогтың қатысқаны абзал. Осының барлығы дәлелдемелер жинаудың заңдылығы мен этикалық стандартына қатысты талаптар болып табылады. Егер дәлелдеме заңсыз әдіспен алынғаны анықталса (мысалы, полиция қызметкері балаға қысым көрсету арқылы мойындатса немесе рұқсатсыз жеке хат-хабарын жарияласа), ондай айғақ іске қолданылмауы тиіс. Әкімшілік құқық бұзушылық туралы кодекс істерді қарау кезінде азаматтардың құқықтарын бұзатын өрескел іс жүргізу заңбұзушылықтарына жол берілмейтінін бекітеді.

Тіпті дәлелдемелерді бұрмалау (өзгерту) фактісінің өзі жеке әкімшілік құқық бұзушылық ретінде қаралады (ҚР ӘҚБтК 637-бабы) [78]. Бұл нормалар тергеу органдары мен процеске қатысушыларды адал және заңға сай әрекет етуге міндеттейді. Дәлелдемелерді тексеру (сараптау) - әкімшілік іс жүргізудің маңызды кезеңдерінің бірі. ӘҚБтК-нің 764-бабына сәйкес, жинақталған барлық дәлелдемелер толық, жан-жақты және объективті тексерілуге тиіс. Тергеуші не судья әрбір дәлелдің мазмұнын жан-жақты талдап, оны өзге деректермен салыстырып, қажет болса қосымша дәлелдер жинайды және дәлелдемелердің алыну көздерін тексереді. Бұл қағида, әсіресе, киберкеңістіктегі істерде өзекті, өйткені электрондық іздер көбіне оңай бұрмалануы немесе жойылуы мүмкін. Мәселен, жасөспірімнің компьютерінен алынған файлдың расында сол компьютерде жасалғанын немесе әдейі «отқізілгенін» анықтау керек. Ол үшін файлдың метадеректерін, жасалған уақытын, құрылғының IP-мекенжайын сараптау қажет болады. Егер күдік туса, тергеуші басқа да дәлелдерді іздейді: мысалы, куәгерлердің

жауаптарын, бейнебақылау жазбаларын және т.б. салыстырып қарайды. ӘҚБтК талап ететін «жан-жақтылық» принципі бойынша, істің мән-жайына ықпал етуі мүмкін кез келген факті назардан тыс қалмауы тиіс. Кибербуллинг бойынша істі тексергенде, тек бала жазған хабарламаларды ғана емес, оған қандай реакция болғанын, басқа қолданушылардың пікірлерін де қарастыру маңызды болуы мүмкін - бұл оның іс-әрекетінің ықтимал зардабын бағалауға септігін тигізеді. Дәлелдемелерді тексеру барысында олардың шынайылығына ерекше көңіл бөлінеді: электрондық жазбалардың түпнұсқалығын растау үшін мамандардың қорытындысы қажет болуы ықтимал. Заңнамаға сай, «дәлелдеменің жол берілетіндігі» деген ұғым бар - бұл дәлелдеменің заңды тәсілмен алынғанын және іске қолдануға болатынын білдіреді. Егер цифрлық дәлелдеме күмәнді жолмен алынған болса (мысалы, жеке өмірге қол сұғу арқылы не құжатсыз тексеру арқылы), қорғаушы тарап оның жарамсыз деп танылуын талап ете алады. Сондай-ақ дәлелдеменің тиістілігі (істің қатысты мән-жайын дәлелдеуге қабілеттілігі) және дұрыстығы (шындыққа сәйкестігі) тексеріледі. Тергеу органдары цифрлық айғақтардың көзін, пайда болу жолын, өзгертілмегенін мұқият зерделеуі тиіс.

Мысалы, ВКонтакте желісіндегі жазба балаға тиесілі аккаунттан жасалғанын растау үшін провайдерден ресми жауап алынса, ол дәлелдің дұрыстығын күшейтеді. Ал егер тек скриншот қана бар болса, оның қолдан өзгертілмегенін сараптама арқылы тексеру керек. Дәлелдеме көздерінің бір-біріне сай келуі де бағаланады: егер баланың мойындауы басқа объективтік айғақтармен (басқа адамдардың куәлігі, техникалық жазбалар) үйлеспесе, тергеуші қосымша тексеріс жүргізуі қажет. ӘҚБтК 764-бабы дәлелдемелерді тексеру құрамына оларды талдау, өзге деректермен салыстыру, қосымша дәлелдемелер жинау және көздерді тексеру кіретінін анықтап берген [78].

Жасөспірімдердің істері бойынша дәлелдемелерді тексеру кезінде олардың жеке басының ерекшеліктері де ескеріледі. ӘҚБтК-нің 65-бабына сай, жасөспірімге шара қолданғанда оның өмір сүру және тәрбиелену жағдайлары, психикалық даму деңгейі, мінез-құлқының ерекшеліктері және оған үлкендердің ықпалы сияқты факторлар міндетті түрде назарға алынуы керек [78]. Бұл деректер көп жағдайда іске тікелей қатысы жоқтай көрінгенімен, іс жүзінде олардың да дәлелдемелік мәні бар. Мысалы, баланың тұрмыстық жағдайы, отбасы ахуалы туралы әлеуметтік педагогтың қорытындысы оның тәртіп бұзу себептерін түсінуге көмектеседі. Егер бала қиын жағдайда өссе немесе оны қылмысқа ересек адам итермелесе, бұл жайттар жауаптылық шарасын таңдағанда ескерілмек. Сондықтан сот пен полиция органдары мектептен, қамқоршылық кеңестен немесе кәмелетке толмағандар ісі жөніндегі комиссиядан арнайы мінездеме, акт сияқты құжаттар талап ете алады. Мұндай құжаттар да іс материалдарына қосылып, жан-жақты тексерілуге тиіс. Сол арқылы құқық бұзушылықтың түпкі себептері мен мән-жайлары толығырақ анықталады.

Дәлелдемелерді бағалау - әкімшілік құқық бұзушылық туралы істі шешудегі соңғы әрі шешуші этап. ӘҚБтК-нің 765-бабы дәлелдемелерді бағалау логикалық ойлау қызметі екенін, ол талдау мен синтез арқылы әр

дәлелдің қатыстылығы, жол берілетіндігі, дәйектілігі (шынайылығы) және әрбір дәлелдің маңыздылығы, сондай-ақ барлық дәлелдемелер жиынтығының қабылданатын шешімді негіздеуге жеткіліктілігі туралы қорытынды жасаумен аяқталатынын атап көрсетеді. Басқаша айтқанда, дәлелдемелерді бағалау кезінде судья немесе істі жүргізуші орган әрбір айғақтың істегі орны мен құндылығын саралап, олардың біріккен жиынтығы істің мән-жайын толық ашуға жеткілікті ме - соны шешеді. ӘҚБтК 765-бабы 2-бөлігі бойынша судья (немесе уәкілетті лауазымды адам) дәлелдемелерді заң мен ар-ожданды басшылыққа ала отырып, өз ішкі сенімі бойынша бағалайды. Ешбір дәлелдеменің алдын ала белгіленген күші болмайды деп тура жазылған. Бұл - қылмыстық процестегі «дәлелдердің еркін бағалануы» қағидасымен ұқсас норма. Яғни электрондық не жазбаша айғақ болсын, куә сөзі болсын - олардың бәріне сот дербес талдау жасап, өзіне қаншалықты сенімді екеніне қарай баға береді. Дәлелдемелерді бағалауда судья олардың заңдылық шарттарын, шынайылығын және өзара үйлесімділігін ескеріп, ақиқатты жан-жақты анықтауға тырысады. Атап айтқанда, 765-бап 3-бөлігі әрбір дәлелдеме істің мән-жайларына қатыстылығы, жол берілетіндігі, дұрыстығы тұрғысынан, ал барлық жиналған дәлелдемелер іс бойынша шешім қабылдауға жеткіліктілігі тұрғысынан бағалануға тиіс екенін бекітеді.

Мысалы, киберқылмыс ісінде жасөспірімнің кінәсін айқындайтын бір ғана айғақ (айталық, оның желідегі жазбасы) болса, сот оның шынайылығын жан-жақты талдап қана қоймай, сол бір айғақтың өзін кінәлі деп тануға жеткілікті ме, әлде қосымша дәлел қажет пе - соны таразылайды. Егер бір ғана дәлелмен шешім шығару әділдікке күмән келтірсе, сот қосымша материалдар талап етуі мүмкін (мұны жоғарыда атап өткен 761-баптың тәртібімен істі қарау барысында да жасауы ықтимал [78]. Дәлелдемелер жиынтығы кәмелетке толмағанның кінәсін бұлтартпай дәлелдейтін деңгейге жеткенде ғана сот шешім қабылдауға құқылы.

Әкімшілік іс жүргізуде дәлелдемелерді бағалау процесінде судьяның ішкі сенімі шешуші рөл атқарады. Бұл ұстаным жасөспірімдерге қатысты істерде ерекше маңызды, өйткені сот баланың әрекетіне құқықтық баға беріп қана қоймай, оған қолданылатын шараның түрін де таңдауы керек. Мысалы, 17 жастағы құқық бұзушының әрекеті Қылмыстық кодекс пен Әкімшілік кодекс шегінде баланса тұрса, сот оның тұлғасын, түзелу белгілерін бағалай отырып, қылмыстық жауаптылыққа тартпастан әкімшілік жаза тағайындаумен шектелуі мүмкін. Сол сияқты, әкімшілік жауаптылыққа тарту кезінде сот жасөспірімнің болашағына оң ықпал етер жолды таңдауға тырысады - айыппұл салып қоя беру ме, жоқ әлде тәрбиелік ықпал шараларын қолдану ма - осындай таңдау да дәлелдемелерді жан-жақты бағалаудың нәтижесінде орындалады. Егер дәлелдемелер баланың түзелу мүмкіндігін, оның өкініш білдіргенін, ата-анасының тиісті бақылау орнатуға келісетінін көрсетсе, сот оны әкімшілік жазадан босатып, орнына тәрбиелік ықпалдың мәжбүрлеу шараларын қолдануы ықтимал. Мысалы, ӘҚБтК-нің 67-бабына сәйкес, сот кәмелетке толмағанға заңды түсіндіру, ата-ана қарауына беру, келтірілген зиянды өтеуді міндеттеу, бос уақытын шектеу сияқты тәрбиелік ықпал

шараларын жеке немесе кешенді түрде белгілей алады [78]. Мұндай шешімге келуде сот істегі барлық деректерді - баланың мінез-құлқын, қателігін түсіну деңгейін, отбасының ахуалын - түгел бағалайды. Егер іс материалдарында бұл жайттар толық ашылмаса, сот оларды өз бастамасымен зерттеуге құқылы (атап айтқанда, қосымша әлеуметтік тексеріс жүргізуді сұратуы мүмкін). Осылайша, дәлелдемелерді жан-жақты бағалау тек кінәні анықтап қана қоймай, тиісті ықпал ету шарасын әділ таңдауға мүмкіндік береді. Бұл - әкімшілік-құқықтық реттеудің тәрбиелік мақсатына сай келеді.

Жасөспірімдердің Кибер құқық бұзушылықтарын қарау тәжірибесін талдай отырып, сындарлы тұрғыдан бірқатар мәселелерді атап өтуге болады. Біріншіден, жоғарыда айтылғандай, цифрлық дәлелдемелерді алу және қолдану саласында ұлттық заңнамада бірыңғай стандарттар жетіспейді. Мәселен, ӘҚБтК-де электрондық ақпаратты алу, сақтау, шифрын шешу тәртібін нақтылайтын нормалар жоқ. Практикада әр тергеуші әрқилы әдіске жүгінуі мүмкін, бұл сотта дәлелдеменің жарамдылығына қатысты дау тудыруы ықтимал. Сол себепті мамандар цифрлық дәлелдемелерге қатысты процессуалдық нормаларды егжей-тегжейлі реттеуді ұсынады [29].

Екіншіден, халықаралық ынтымақтастық арнасын кеңейту қажеттігі туындап отыр. Киберқылмыспен жалғыз ел болып күресу мүмкін емес екенін әлемдік тәжірибе көрсетуде [70]. Жасөспірімдер қатысқан көптеген интернет-қылмыстар трансұлттық желілерде жасалады - мысалы, шетелдік онлайн-алаяқтар қазақстандық оқушыларды алдап ақша аудартуы мүмкін немесе керісінше, біздің елдегі жасөспірімдер бөтен мемлекеттердегі адамдардың аккаунттарын бұзып, зиян келтіруі ғажап емес. Мұндай жағдайларда дәлелдеме жинау мен құқықтық жауаптылыққа тарту үшін өзара көмек керек. Қазақстан ТМД аясында киберқылмыспен күрес туралы келісімге қосылған (2019 ж. ратификацияланған), алайда оның ауқымы шектеулі. Ал Будапешт конвенциясына қосылу - әлемнің 80-нен астам елімен тікелей үйлесімді жұмыс істеуге мүмкіндік береді [58]. Ондағы бірқатар озық құралдар (шұғыл сақтап қою, транскордондық қолжетімділік, бірлескен тергеу топтары т.б.) электрондық дәлелдемелерді жедел алмасуға жол ашады [29].

ЕҚЫҰ сарапшылары Орталық Азияда киберқылмыспен күресте құқық қолданушыларды оқыту, техникалық жарақтандыру және халықаралық кооперацияны арттыру бойынша құрылымдық шаралар қажет екенін баса айтады [70]. Бұл ұсынымдар Қазақстан үшін де өзекті. Үшіншіден, құқық қорғау органдарының кадрлық әлеуетін нығайту мәселесі тұр. Киберқылмыстарды тергеу - жаңашыл әрі күрделі іс, онда классикалық жедел әдістер (бақылау, беттестіру және т.б.) көбіне жеткіліксіз, тергеушілерге программалау, желілер мен криптография негіздерін білуге тура келеді.

Сондықтан полиция академияларында кибертергеу бойынша мамандандыруды енгізу, судьяларды да цифрлық сауаттылық тұрғысынан оқыту маңызды. ЮНИСЕФ Қазақстандағы интернеттегі балаға қарсы зорлық-зомбылықпен күресу үшін ең алдымен құқық қорғаушылардың әлеуетін күшейту қажеттігін атап өтті. Ішкі істер органдары соңғы жылдары бұл бағытта шетелдік әріптестермен бірлескен семинарлар, оқу-жаттығулар

өткізуде [80]. Мысалы, ЕҚЫҰ-ның қолдауымен Қазақстанда киберқылмыс пен электрондық дәлелдемелер бойынша тренингтер ұйымдастырылғаны мәлім [70]. Мұның бәрі оң үрдіс және алдағы уақытта да жалғасуға тиіс.

Тағы бір маңызды жайт - кәмелетке толмағандарды қайта әлеуметтендіру, тәрбиелік ықпал шараларының тиімділігі тікелей дәлелдемелердің сапалы бағалануы мен істің мән-жайының толық ашылуына байланысты. Жасөспірімдердің кейбірі білместіктен, әуестікпен құқық бұзса, кейбірі отбасындағы бақылаудың жоқтығынан қылмысқа барады. Мысалы, мамандар кәмелетке толмағандар арасындағы құқық бұзушылықтардың өсуіне ата-аналардың балаларын қараусыз қалдыруы, олардың компьютерлік ойындарға шамадан тыс әуестенуі және құқықтық сауаттың төмендігі әсер ететінін айтады. Мұндай себептерді әр істің материалдарынан байқауға болады: бірінде ата-ана баласының желідегі іс-әрекеттеріне мүлде мән бермеген, екіншісінде бала зорлық-зомбылық мазмұнды ойындарға салынып, шын өмір мен виртуалдың айырмасын сезбей қалған, т.б. Сол үшін әкімшілік іс жүргізу барысында баланың мінез-құлқын түзетуге ықпал ететін жағдайлар да анықталуы қажет. Сот немесе комиссия шешім қабылдағанда жасөспірімге жай айыппұл салып қою жеткілікті ме, әлде оны психологтің бақылауына беру керек пе - осындай мәселелер көтеріледі. ҚР ӘҚБтК тәрбиелік ықпал шараларын қолданудың нақты тетіктерін бекіткен (67-68-баптар), алайда олардың іске асуын қамтамасыз ету де оңай жұмыс емес. Мысалы, бос уақытын шектеу шарасы үш айға дейін ғана белгіленеді; егер бала белгіленген тәртіпті бірнеше рет өрескел бұзса, онда іс қайта қаралып, әкімшілік жаза тағайындалуы мүмкін [78]. Яғни әрбір істің материалдарына сүйеніп, сот балаға ықпал етудің тиімді жолын таңдайды.

Қорыта айтқанда, кәмелетке толмағандардың Кибер құқық бұзушылықтарын әкімшілік-құқықтық реттеу саласында дәлелдемелерді жинау, сараптау және бағалау процестері шешуші рөл атқарады. Дәлелдемелер неғұрлым толық және заңды жолмен жиналып, мұқият тексеріліп, әділ бағаланса - соғұрлым істің ақиқаты анықталып, кінәлі жасөспірімге қатысты әділ шара қолданылмақ. Қазақстандық заңнама мен құқық қолдану тәжірибесі осы бағытта дамуын жалғастыруда: цифрлық дәлелдемелермен жұмыс істеу бойынша жаңа құралдар енгізілуде, халықаралық тәжірибеге ұмтылыс бар [29], мамандар даярлығы жетілдірілуде. 2020-2025 жылдар аралығындағы сот тәжірибесі көрсеткендей, көптеген істерде жасөспірімдердің кінәсі электрондық айғақтар арқылы дәлелденіп, оларға қатысты тәрбие шаралары қолданылған. Мысалы, әлеуметтік желіде буллинг жасағаны үшін бірнеше оқушы ата-анасының қатысуымен комиссияға шақырылып, ресми ескерту алды; ал кейбір интернет-алаяқтыққа ұрынған жасөспірімдер сотта кінәсін мойындап, ата-анасының қарауына берілу тәртібімен ерекше бақылауға қойылды. Әрине, бұл нәтижелер - дәлелдемелерді дұрыс жинап, жан-жақты бағалаудың арқасы. Алдағы уақытта әкімшілік іс жүргізу тетіктерін заман талабына сай жетілдіру жалғасады деп сенеміз. Цифрлық технологиялар дамыған сайын жаңа құқық бұзушылық тәсілдері шығуы мүмкін, демек дәлелдемелерді

жинаудың да жаңа әдістері қажет болады. Заңнаманы халықаралық стандарттарға үйлестіру, әсіресе Будапешт конвенциясының құралдарын пайдалану - электрондық дәлелдерді алудағы кедергілерді азайтары сөзсіз [29]. Сондай-ақ, кәмелетке толмағандардың істерін қарауда балаларға қолайлы әділсот қағидаттарын күшейткен жөн: бұл тергеу мен сотта баланың құқықтарын сақтауды, оның психологиялық ерекшеліктерін ескеруді білдіреді. ЮНИСЕФ және өзге ұйымдардың бастамасымен енгізіліп жатқан бала-достық әдістер (сұрақ қоюдың арнайы тактикасы, психологиялық сүйемелдеу, т.б.) дәлелдемелерді объективті бағалауға да септігін тигізеді. Өйткені бала өзіне түсінікті және қауіпсіз жағдайда ғана шынайы айғақ бере алады. Сондықтан полиция мен сот қызметкерлерін балалармен жұмыс істеудің заманауи тәсілдеріне оқыту - дәлелдемелердің сапасын арттыруға қызмет ететін маңызды қадам.

Қорыта келе, дәлелдемелерді жинау, сараптау және бағалау әкімшілік құқық бұзушылық істерінде әділеттіліктің негізі болып табылады. Кәмелетке толмағандардың цифрлық әлемде жасаған құқық бұзушылықтарын тиімді ашып, оған заңды реакция беру дәлелдемелік процестің нәтижелілігіне тікелей тәуелді. Мұны заң шығарушы да ескере отырып, ҚР ӘҚБтК-де дәлелдемелермен жұмыс істеудің негізгі қағидаларын бекітті: барлық дәлелдемелер заңды жолмен алынуға, мұқият тексеріліп, объективті бағалануға тиіс. Осы қағидаттар қатаң сақталғанда ғана кәмелетке толмаған құқық бұзушыларға қатысты әділ шешім қабылданып, оларды түзелуге бағыттау мүмкін болады. Мемлекетіміздің бүгінгі басым бағыты да - жазалау шараларын балаларға тәрбиелік, оңалту ықпалымен ұштастыру. Бұл мақсатқа қол жеткізу үшін әрбір әкімшілік іс бойынша шындықты ашатын сапалы дәлелдемелік базаның маңызы зор. Құқық қолдану тәжірибесін терең талдау және 2020-2025 жылдардағы сот практикасының нәтижелері көрсеткендей, дәлелдемелерді жинау, сараптау және бағалау тетіктерін одан әрі жетілдіру - кәмелетке толмағандардың құқықтарын қорғау әрі олардың құқық бұзушылықтарының алдын алу жолындағы маңызды қадам болмақ. Деректер мен әділ талдауға негізделген шешім ғана - заң үстемдігін қамтамасыз етеді [78].

### 2.3 Кәмелетке толмағандардың құқықтары мен мүдделерін қорғау: алдын алу мен жауапкершіліктің өзара байланысы

Цифрлық дәуірдегі ақпараттық кеңістіктің кеңеюі кәмелетке толмағандардың мінез-құлқына жаңа әсерлер мен қатерлер әкелді. Бүгінде жасөспірімдер арасындағы құқық бұзушылық құрылымы дәстүрлі ұрлық не бұзақылықпен ғана шектелмей, кибербуллинг, интернет-алаяқтық, желіде құқыққа қарсы контент тарату сияқты «Кибер құқық бұзушылықтармен» толығуда. Ресми деректерге сүйенсек, Қазақстанда соңғы бес жылда жалпы жасөспірімдер қылмысы төмендегенімен, 2023 жылы кәмелетке толмағандар жасаған құқық бұзушылықтар саны алдыңғы жылмен салыстырғанда 11%-ға өскен [81]. 2023 жылдың жеті айы ішінде 944 жасөспірім қылмыстық

жауаптылыққа тартылып, бұл өткен жылғыдан 11,5% артық көрсеткішті құрады [74]. Мұның себебін құқық қорғау органдары көбіне ата-аналардың бала тәрбиесіндегі бақылауының жеткіліксіздігімен байланыстырады, әсіресе қолайсыз отбасыларда. Мысалы, 2024 жылы түнгі уақытта көшеде немесе көңіл көтеру орындарында болғаны үшін 100 мыңнан астам ата-ана әкімшілік жауапкершілікке тартылғаны тіркелді. Жасөспірімдердің қылмысқа баруына тез ақша табуға құмарлық, «қызық үшін» бұзақылық, немесе интернет арқылы тарайтын тұрпайы зорлық-зомбылық насихаты әсер етуі мүмкін екені атап өтілуде. Расында да, полиция өкілдері агрессия мен зорлық-жанжалға толы контенттің кәмелетке толмағандардың адамгершілік дамуына кері әсер ететінін, сол себепті мұндай материалдарға қолжетімділікті шектеу қажеттігін алға тартады [81]. Балалар арасында кең тараған бұзақылықтың бір түрі - буллинг пен кибербуллинг. 2023 жылғы «Қазақстандық балалардың интернеттегі қауіпсіздігі» зерттеуі еліміздегі әр бесінші баланың (шамамен 21%) кибербуллингтің құрбаны болғанын көрсетті [82]. Осы орайда мемлекет кәмелетке толмағандардың құқықтары мен мүдделерін қорғауда бір мезетте алдын алу шараларын күшейтуге және құқық бұзған жағдайда жауаптылық тетіктерін қолдануға көңіл бөліп отыр. Қазақстан Президенті Қ.Тоқаев атап өткендей, қазіргі қоғамдағы бес үлкен қатердің бірі - «кез келген формадағы буллинг» екенін мойындап, оны жоюға бағытталған кешенді саясат қажет [83]. Демек, кәмелетке толмағандарды киберортадағы құқық бұзушылықтардан қорғау - тек жазалау емес, ең алдымен олардың құқықтары мен заңды мүдделерін уақтылы қорғауға арналған жүйелі алдын алу жұмыстары мен жауапкершілік шараларын ұштастыру арқылы жүзеге асырылуы тиіс.

Қазақстан Республикасының бала құқықтарын қорғау саласындағы құқықтық негізі халықаралық стандарттар мен ұлттық заңнаманың талаптарына сай қалыптасқан. Еліміз тәуелсіздіктің алғашқы жылдарында-ақ БҰҰ-ның «Баланың құқықтары туралы» конвенциясына қосылды [81], сол арқылы кәмелетке толмағандардың құқықтарын қорғау бойынша халықаралық міндеттемелерді мойнына алды. Аталмыш Конвенцияда әрбір баланың аман-есен өсіп-жетілуі, білім алып дамуы және зорлық-зомбылықтан қорғалуы мемлекет қамқорлығында болуы керектігі баса айтылған. Конвенцияның басты қағидаттарына сәйкес, балалардың жоғарғы мүддесін қамтамасыз ету - кез келген саясат пен шешімнің түпқазығы болуға тиіс. Бұл Қазақстан заңдарына да елеулі түрде ықпал етті. 2002 жылы қабылданған «Қазақстан Республикасындағы баланың құқықтары туралы» заң кәмелетке толмағандардың құқықтық жағдайын жан-жақты регламенттейді. Аталған Заңның 3-бабында мемлекет баланың негізгі құқықтары мен заңды мүдделерін қамтамасыз ету үшін қажетті ұйымдық-құқықтық жағдайларды жасауға, баланың жан-жақты дамуына ықпал етуге міндетті екені бекітілген. Заңда балалардың дене, интеллектуалдық, рухани және адамгершілік дамуына жәрдемдесу, оларға патриоттық тәрбие беру, баланың жеке тұлғасын қоғам игілігіне сай ашуға жағдай жасау - мемлекеттің басым мақсаттарының бірі ретінде аталады. Сондай-ақ балалардың

құқықтарын қорғау жүйесін жетілдіру, осы мақсатта арнаулы органдар мен ұйымдар құру мемлекет міндеті екендігі белгіленген. Бұл заң бала құқығын қорғаудың институционалдық негіздерін қалыптастырды: Қазақстанда Балалар омбудсманы лауазымы енгізіліп, бала құқықтарын іске асыру және бұзылған құқықтарды қалпына келтіру үшін бақылау механизмі орнатылды [84]. Балалар омбудсманы және бала құқықтарын қорғау жөніндегі уәкілетті органдар мемлекет атынан кәмелетке толмағандардың мүдделерін қорғайды.

Сонымен бірге, Қазақстан Конституциясы, «Неке (ерлі-зайыптылық) және отбасы туралы» кодекс және жоғарыда аталған Бала құқықтары туралы заң ата-аналарды өз балаларын тәрбиелеуге және олардың қамын жасауға міндеттейді. Ата-ана құқықтары мен міндеттері баланың мүддесіне сай жүзеге асырылуға тиіс: ҚР Конституциясына сәйкес, балаларын күтіп-бағу және өсіріп-жеткізу - ата-аналардың табиғи құқығы ғана емес, заңдық парызы [85]. Осылайша, ұлттық заңнамада кәмелетке толмағандардың құқықтары арнайы қорғауға алынған және олардың құқықбұзушылық жасауының алдын алу мен олардың өздерінің құқықтары бұзылуының жолын кесу - мемлекет пен қоғам үшін екіжақты міндет.

Кәмелетке толмағандардың құқыққа қарсы іс-әрекеттері үшін жауаптылық мәселесі - балаға ерекше әлеуметтік-құқықтық статусқа ие субъект ретінде қарауға негізделген. Қазақстанның әкімшілік және қылмыстық заңнамасы кәмелетке толмағандарға қатысты ізгілендірілген, ерекше ережелерді қамтиды. Әкімшілік құқық бұзушылық туралы кодекс бойынша жалпы ереже - әкімшілік жауаптылық 16 жасқа толғаннан бастап туындайды. Яғни 16 жасқа толмаған бала әкімшілік жазаға тартылмайды. Тек ерекше жағдай ретінде ұсақ бұзақылық жасаған 14-15 жасар жеткіншектерге әкімшілік шара қолданылуы мүмкін екені Кодексте көзделген (ҚР ӘҚБтК 435-бабында) [85]. Бұдан бөлек, заң кәмелетке толмағандарды әкімшілік қамауға алуға тыйым салады - 18 жасқа толмаған тұлғаларға қамау түріндегі жаза тағайындалмайды [86]. Қылмыстық жауаптылық шегі де жеңілдетілген: жалпы қылмыстық жауаптылық 16 жастан басталса, ерекше ауыр немесе ауыр санаттағы қылмыстар бойынша ғана 14 жастан бастап жауаптылық қарастырылған [85]. Демек, заң жүзінде балаға жаза тағайындауда оның жас ерекшелігі ескеріліп, неғұрлым ізгі ықпал ету шараларын қолдану басым.

Мысалы, Қылмыстық кодекстің арнайы ережелеріне сәйкес, кәмелетке толмағандарды бас бостандығынан айыру тек ең соңғы шара ретінде әрі мүмкіндігінше қысқа мерзімге тағайындалады; өлім жазасы мен өмір бойы бас бостандығынан айыруға олар мүлдем тартылмайды. 2024 жылдың сәуір айында қабылданған заңнамалық өзгерістер кәмелетке толмағандарды қорғау мақсатында жаза саясатында бірқатар қатаңдатулар енгізді: енді балаға қатысты адам өлтіру, зорлау сияқты аса ауыр қылмыстар үшін өмір бойы қамауға алу жазасы тікелей белгіленді; 16 жасқа толмағандарға қатысты сексуалдық сипаттағы кез келген әрекеттер қылмыстық жазаланатын болды. Сонымен бірге дәл осы жаңа заң арқылы әкімшілік құқық бұзушылықтар кодексіне «буллинг және кибербуллинг үшін әкімшілік жауаптылық» деген норма қосылды [83]. Яғни бұдан былай біреуді жүйелі түрде қорлау, тиісу,

қудалау әрекеттері (оның ішінде интернет немесе әлеуметтік желі арқылы) үшін құқық бұзушыға заң жүзінде айыппұл немесе басқа да шара қарастырылады. Мұндай жаңалық Қазақстанда алғаш рет буллинг ұғымын құқықтық деңгейде бекітіп, оның алдын алу мен жолын кесуге мүмкіндік береді. 2024 жылғы заңда, сондай-ақ, кәмелетке толмағандарды автобус сияқты қоғамдық көліктен мәжбүрлеп түсіріп кетуге тыйым салу туралы норма енді [87] - бұның өзі олардың қауіпсіздігін қамтамасыз етуді көздейтін жауапкершілік шарасы. Бұдан бөлек, енді білім беру ұйымдары баланың құқықтарына қарсы кез келген әрекет туралы құқық қорғау органдарына хабарлауға міндетті [83]. Жалпы, соңғы жылдары Қазақстан заңнамасы балаға қарсы жасалған заңбұзушылықтар үшін жауаптылықты күшейтуге бағыт алып отыр: балаларға зорлық көрсеткені үшін жазаны ауырлату, жыныстық қолсұғылмаушылыққа қарсы қылмыстарға қатаң жаза белгілеу, суицидке итермелеу әрекеттерін қылмыстандыру және т.б. нормалар қабылданды [81]. Мысалы, балаларға қарсы зорлық-зомбылық жасағаны үшін тараптардың татуласуына жол бермеу (қайталанған жағдайда) туралы ереже қабылданды [87], ата-ана міндетін орындамай, баласына қатыгездік көрсеткендерге сот арқылы үйден шығару, мінез-құлқына ерекше талаптар белгілеу сияқты шаралар енгізілді [81]. Бұл өзгерістер бір жағынан баланы қорғауға арналса, екінші жағынан - кәмелетке толмағандардың өздерінің құқық бұзушылық жасауына тосқауыл қою, жасаған жағдайда тиісті жауапкершілікке тарту жүйесін қалыптастырады.

Кәмелетке толмағандардың құқық бұзушылығы үшін тікелей өздерін жауапқа тартумен қатар, олардың ата-аналары мен заңды өкілдерінің жауаптылығы мәселесі де өте маңызды орын алады. Бала тәрбиелеу міндетін тиісінше орындамағаны үшін ата-аналарды жазалау - әкімшілік құқықтық ықпал етудің пәрменді тетігі. ҚР Әкімшілік құқық бұзушылық туралы кодексінің 127-бабына сәйкес, ата-аналар немесе балаға жауапты адамдар кәмелетке толмаған жасөспірімнің құқық бұзушылық жасауына жол бергені үшін жауапқа тартылады. Айталық, егер бала әкімшілік теріс қылық жасаса, оның ата-анасына 127-бап бойынша айыппұл салынады; бала түнгі уақытта үлкендердің қарауынсыз көңіл көтеру орнында жүрсе, ата-анасына айыппұл көзделген (442-бап). Полиция деректері бойынша тек 2023 жылдың алғашқы жеті айында Павлодар облысында ата-ана міндетін орындамағаны үшін 178 ата-ана, ал кәмелетке толмаған баласын түнде ойын-сауық мекемелерінде қараусыз қалдырғаны үшін 1610 ата-ана әкімшілік жазаға тартылған.

Бұл сандар ата-ана жауапкершілігінің қаншалықты қатаң бақылауда екенін көрсетеді. Мұндай істер бойынша көбіне ата-анаға ескерту беріледі немесе айыппұл салынады, бірақ қажет жағдайда балалардың құқығын қорғау комиссиялары арқылы ата-ана құқығынан айыру мәселесі де көтерілуі мүмкін. Бұдан бөлек, ҚР ӘҚБтК 409-бабында ата-ананың балаларды оқыту міндетінен жалтаруы да құқық бұзушылық ретінде танылып, жауаптылық қарастырылған. Яғни баласын мектепке жібермей, білім алуына жағдай жасамаған ата-ана да заң алдында жауап береді. Отбасы - баланың алғашқы әлеуметтік ортасы болғандықтан, мемлекет отбасындағы қолайсыз ахуалдың

баланың құқық бұзушылық жасауына әсерін азайтуға тырысады. Профилактикалық рейдтер барысында полицейлер тұрмысы нашар, антисанитарлық жағдайда өмір сүріп жатқан балаларды анықтаса, ондай ата-аналарға да шара қолданылады. 2023 жылы Павлодар облысында осындай жағдайлары бар 40 кәсіпкер (ойын-сауық орны иелері) мен 40-тан астам ата-анаға айыппұл салыныпты. Ал жасөспірімдердің өздерін тәрбиелеу мақсатында ішкі істер органдарының есебіне қою тетігі қолданылады: егер жеткіншек екі немесе одан көп әкімшілік құқық бұзушылық жасаса, ол полицияның профилактикалық есебіне алынады. Бұл есепте тұрған балалар ерекше бақылауда болып, олардың мінез-құлқын түзетуге бағытталған әңгімелер, инспекторлық қадағалау жүзеге асады. Одан бөлек, егер кәмелетке толмаған бала екі рет қылмыс жасап, бірақ жасы кіші болуына байланысты қылмыстық жауаптылыққа тартылмаса, онда тиісті комиссияның өтініші бойынша сот шешімімен оны арнайы білім беру ұйымына жолдау мүмкіндігі қарастырылған. Мұндай арнайы оқу-тәрбиелеу мекемелері девиантты мінез-құлықты балаларға арналған интернат үлгісіндегі жабық ұйымдар болып табылады. Соңғы үш жылда республика бойынша осындай арнайы мектеп-интернаттарға 36 жасөспірім жіберілген, оның 2-еуі ерекше режимді мекемеге орналастырылған [85]. Мысалы, елордада бұзақылық жасап, үйінен қашып кету әдеті қайталанған бірнеше жасөспірімнің ісі комиссияда қаралып, екеуін арнайы мектепке жіберу туралы шешім қабылданған еді.

Мамандардың айтуынша, мұндай арнайы білім беру ұйымдарында қатаң күн тәртібі мен тәртіп ережелері арқылы мінез-құлқы қиын балаларды қоғамға бейімдеу, тәртібін түзеу жұмыстары жүргізіледі. Арнайы мектептер қазіргі таңда Шығыс Қазақстан облысының Серебрянск қаласында, сондай-ақ Ақтөбе, Алматы және Тараз қалаларында орналасқан [88]. Әрине, балаларды еркінен тыс арнайы мекемеге жіберу - шекті шара, және әрбір жағдайда сотпен өте мұқият қаралады. Бірақ қайталанған құқық бұзушылықтар кезінде, әсіресе қылмыстық әрекет белгілері байқалса, баланың өзіне де, қоғамға да қауіп төндірмеу үшін осындай тәрбиелік шараларды қолдану қажеттігі туындайды. Жалпы алғанда, Қазақстанның әкімшілік-құқықтық реттеу жүйесі кәмелетке толмағандар жасаған құқық бұзушылықтарға екі жақты ықпал етуді көздейді: бір жағынан, 16-17 жастағы жасөспірімдер заң алдында жауап беруге тартылады (жасына сай жеңілдетілген түрде), екінші жағынан - олардың ата-аналары мен қоршаған ортаға бақылау күшейтіліп, профилактикалық әсер ету шаралары бірге қолданылады. Бұл өзара байланыс баланың құқықтары мен мүдделерін қорғаудың кешенді тәсілі ретінде қарастырылады.

Жасөспірімдердің құқық бұзушылықтарының алдын алу - олардың құқықтарын қорғаудың ең тиімді жолы. «Ауруды емдегеннен, алдын алған жеңіл» демекші, бала құқықтарын бұзатын жағдай мүлдем туындамауы үшін мемлекет пен қоғам бірлесіп жұмыс атқаруы қажет. Қазақстанда кәмелетке толмағандар арасындағы құқық бұзушылықтардың алдын алу мақсатында институционалдық көпдеңгейлі жүйе қалыптасқан. Оның басты элементтерінің бірі - кәмелетке толмағандар істері және олардың құқықтарын

қорғау жөніндегі комиссиялар (КДН). Мұндай комиссиялар әрбір аймақ пен ауданда құрылып, құрамына білім беру ұйымдарының өкілдері, ішкі істер органдарының қызметкерлері (ювеналды полиция), денсаулық сақтау, әлеуметтік қорғау саласының мамандары, прокуратура және қоғам өкілдері кіреді. Мәселен, елордадағы Есіл ауданының ювеналды полиция бөлімшесінің бастығы А. Кожахметованың айтуынша, комиссия отырысына шамамен 30 түрлі мекеме мамандары жиналады, онда полиция девиантты мінез-құлық көрсеткен баланың ісін баяндап, қажетті шаралар туралы ұсыныс енгізеді. Комиссия әр істі жеке қарап, баланы оңалтуға көмектесу жолдарын қарастырады: егер бала ерекше көмекке мұқтаж деп танылса, оны арнайы бағдарламаға, психологиялық қолдауға немесе жоғарыда аталған арнайы мектеп-интернатқа жіберу туралы сотқа материалдар әзірлейді [88].

Бұдан бөлек, комиссия отырыстарында ата-анасы баласына дұрыс бақылау жасамаған жағдайлар, отбасындағы зорлық-зомбылық фактілері де қаралып, тиісті органдарға ата-анаға ықпал ету жөнінде ұсыныстар беріледі. Кәмелетке толмағандардың құқықтарын қорғау комиссиялары осылайша әр баланың мүддесін ескеріп, түрлі ведомстволардың күшін біріктіретін үйлестіруші орган болып табылады.

Жасөспірімдердің құқық бұзушылықтарының алдын алудағы тағы бір маңызды институт - полицияның ювеналды бөлімшелері. Ішкі істер органдары құрамында мамандандырылған инспекторлар мен бөлімдер балалармен жұмыс істеуге бейімделген. Ювеналды полиция қызметкерлері мектептермен, ата-аналар комитеттерімен тығыз байланыста жұмыс істеп, «қолайсыз» балаларды дер кезінде анықтауға, олармен профилактикалық әңгімелер жүргізуге, қажет болса есепке қоюға тырысады [85, с. 37]. Мысалы, Астана қаласы Есіл ауданының ювеналды полициясы күн сайын ата-аналар чаттарына бала қауіпсіздігін қамтамасыз ету бойынша кеңестер жіберіп отырады, сынып жетекшілеріне оқушылардың мектепке барар және қайтар жолының қауіпсіз маршрутын жасау туралы жадынамалар таратады.

Мұның мақсаты - балалардың хабарсыз жоғалып кетуінің алдын алу, себебі практика көрсеткендей, кейде оқушылар ата-анасына ескертпей үйден шығып кетіп, іздеу салуға дейін барады. Полиция қызметкерлері жоғалған балаларды іздеу алгоритмін де жетілдірген: алғашқы сағат ішінде бала табылмаса, бірден криминалдық полиция мен волонтерлер жұмылдырылады, әлеуметтік желілер мен мессенджерлер арқылы баланың суреті таратылып, жаппай іздестіру жүргізіледі. Ювеналды инспекторлардың айтуынша, көбіне жасөспірімдер ата-анасынан «жасырынып қалу» мақсатында досының үйінде немесе туыстарын паналап жүреді екен; сондықтан полиция таныстары арқылы ақпарат жинайды, осылайша балалардың басым көпшілігі тез арада табылады [88]. Дегенмен, бала үйден екінші рет қашып кетсе немесе бірнеше мәрте тәртіп бұзса, бұл - отбасы деңгейінде де, балаға қатысты мемлекеттік бақылау деңгейінде де дабыл белгісі. Мұндайда жоғарыда айтылған комиссияның араласуы, қажет болса арнайы мекемеге жіберу шешімдері қарастырылады. Осы ретте ювеналды полиция мен комиссиялардың бірлесе атқаратын жұмысы маңызды рөл атқарады. Жасөспірімдерді теріс

қылықтардан сақтандыру үшін мемлекеттік органдар мен қоғамдық ұйымдар түрлі әлеуметтік-білім беру шараларын жүзеге асырады. Балаларды сабақтан тыс уақытында пайдалы іспен айналыстыру - құқық бұзушылықтың алдын алудың тиімді тәсілі ретінде танылған. Сондықтан елімізде соңғы жылдары тегін үйірмелер мен спорт секциялары желісі кеңейтілуде. 2024 жылы, мәселен, Туризм және спорт министрлігі бұйрығымен девиантты мінез-құлықты, ішкі істер органдарының есебінде тұрған балаларды спорт секцияларына қабылдауда басымдық беру тәртібі енгізілді. Бұл - тәртібі нашар балаларды қоғамға бейімдеуге спорт арқылы ықпал ету амалы. Әр өңірде «қиын» жасөспірімдермен мақсатты жұмыс жүргізуге арналған әлеуметтік жобалар іске қосылған: тренингтер, еңбек терапиясы, мәдени шараларға тарту, волонтерлыққа баулу, т.б. Мысалы, кей қалаларда полиция бастамасымен «Қауіп тобындағы жасөспірімдерге арналған лагерьлер» ұйымдастырылып, онда түрлі мамандар балаларға өмірлік дағдыларды үйретеді. Сонымен бірге әр мектепте учаскелік полиция инспекторы бекітілген, олар сол білім ордасындағы ахуалды қадағалап, оқушылармен тұрақты кездесулер өткізеді. Барлық мектептерде сенім телефондары («111» желісі) мен кәмелетке толмағандар істері жөніндегі учаскелік инспекторлардың байланыс нөмірлері ілініп, оқушылар кез келген қауіп немесе зорлық фактісі туралы жасырын хабарлай алатыны насихатталуда. 2023-2024 оқу жылының басында Ішкі істер министрінің тапсырмасымен жергілікті полиция департаменті басшылары мен орталық аппарат өкілдері мектептердің алғашқы қоңырау шараларына қатысып, балаларға жол қауіпсіздігі мен интернеттегі бейтаныс адамдармен байланыс кезіндегі сақтық шараларын түсіндірді. Полицияның осындай ағарту жұмыстары жүйелі түрде жүргізіледі: аптасына бір рет кемінде әр мектепте құқық бұзушылықтардың алдын алу тақырыбында дәріс немесе кездесу өтеді, оқушылар арасында жасырын сауалнама жүргізіліп, буллинг, бопсалау, зорлық немесе өзге де мәселелер бар-жоғы анықталады [81].

Мектеп психологтары мен әлеуметтік педагогтері де бұл үрдіске қосылады. Бұған қоса, ішкі істер органдары демалыс кезеңдерінде «Түнгі қаладағы балалар», «Қауіпсіз аула» сияқты жедел-профилактикалық рейдтер жүргізіп, түнгі мезгілде жүрген немесе компьютерлік клубтар мен ойын-сауық орындарында байқалған жасөспірімдерді анықтайды. Мысалы, 2024 жылдың басынан бері Қостанай облысында өткізілген рейдтерде 22:00-ден кейін кафе, кальянхана, компьютер клубтарында жүрген 100-ден астам бала ұсталып, полицияға жеткізілген; олардың ата-аналарына 12 мың теңгеден айыппұл салыныпты. Сол Қостанайлық оқиғада қайталанған жағдайда айыппұл екі еселенетіні және бала полиция есебіне қойылатыны ескертілген [88]. Полиция бұзақылыққа бейім балалардың тізімін жасап, олармен жеке профилактика жүргізеді. Бұл ретте, тек жазалау емес, оларды қоғамға бейімдеу де көзделгенін айту керек: ішкі істер органдары жергілікті билікпен бірлесе отырып, қолайсыз отбасылардан шыққан балаларды жазғы лагерьлерге, кәсіби бағдар беру курстарына, қоғамдық жұмыстарға тарту шараларын ұйымдастырады. Жасөспірімдер арасындағы құқық

бұзушылықтың түп-тамыры көбіне отбасылық қолайсыздық, әлеуметтік теңсіздік, бақылаусыздық секілді мәселелерде жататыны белгілі. Сондықтан да алдын алу жүйесі тек полиция мен мектептің шараларымен шектелмей, кең ауқымды әлеуметтік жұмысты талап етеді. Қазақстанда әлеуметтік қызметтер мен қамқоршылық органдары қиын өмірлік жағдайдағы отбасылармен жұмыс күшейтуде. Мысалы, балалар правасын қорғау комитетінің мәліметінше, 2024 жылы елімізде 5000-нан астам жеткіншек Кәмелетке толмағандарды бейімдеу орталықтарына орналастырылып, қажетті көмек көрсетілген. Әр өңірде жергілікті әкімдік жанынан көпсалалы мобильді топтар құрылған: оның құрамында қамқоршылық органдары, полиция, прокуратура, білім және әлеуметтік қорғау мекемелерінің өкілдері бар. Бұл топтар тұрмысы нашар, әлеуметтік қауіпті отбасыларды анықтау үшін 27 мыңнан астам үйді аралап, нәтижесінде 1200 қиын жағдайдағы отбасыны есепке алған. Мұндай отбасыларға арнаулы әлеуметтік қолдау шаралары (атаулы көмек тағайындау, жұмыспен қамтуға жәрдем, ата-аналарды қайта оқыту, психологиялық кеңес беру, т.б.) көрсетілуде.

Бұның барлығы балалардың қылмыс жолына түсіп кетуінің алдын алу үшін жасалып жатыр, себебі «отбасындағы проблемалар шешілмей, баланың құқық бұзушылығын тек полиция күшімен азайту мүмкін емес» екені ресми түрде мойындалуда. Ішкі істер министрлігі өкілінің айтуынша, тек құқық қорғау шараларымен шектелу жеткіліксіз, егер балалардың қылмысқа баруына итермелейтін әлеуметтік ахуал өзгермесе, полицияның күресі өз нәтижесін толық бермеуі мүмкін [81]. Сондықтан қазір мемлекет деңгейінде ерте превенцияға мән берілуде: баланың ортаға бейімделуін қиындататын факторларды (мектептегі үлгермеушілік, үйдегі зорлық-зомбылық, қоршаған ортаның антиәлеуметтік ықпалы) дер кезінде анықтап, жою. Бұл бағытта денсаулық сақтау саласы да тартылуда - әсіресе жасөспірімдердің психикалық саулығын қорғау, суицидтің алдын алу, нашақорлық пен интернетке тәуелділіктің жолын кесу үшін арнайы бағдарламалар бар.

Халықаралық тәжірибе мен стандарттар да кәмелетке толмағандар арасындағы құқық бұзушылықтардың алдын алу мен балалардың құқықтарын қорғаудың ажырамас байланысты екендігін қуаттайды. БҰҰ-ның Балалар құқықтары жөніндегі комитеті мемлекеттерге бала әділетінің басты мақсаты - баланы қайта тәрбиелеу және қоғамға қайта интеграциялау екеніне назар аударып, репрессивті шаралардың орнына тәрбиелік және қалпына келтіруші әдістерді қолдануды ұсынады. [83]. 1985 жылғы Бейжің ережелері (БҰҰ-ның кәмелетке толмағандар жөніндегі сот төрелігінің минималдық стандарттары) мен 1990 жылғы Эр-Рияд жетекші қағидаттары (кәмелетке толмағандар арасында құқық бұзушылықтың алдын алу жөніндегі БҰҰ нұсқаулары) жасөспірімдердің болашағына залал келтірмейтін, оларды қоғамға бейімдеп, әлеуметтендіретін шараларды басым қолдануға шақырады. Айталық, Эр-Рияд нұсқауларында профилактика бірінші кезектегі шара болу керектігі, ол үшін отбасы, мектеп және қауымдастықтың үйлесімді әрекет ететіні айтылған. Қазақстан да әлемдік озық тәжірибелерді зерттеп, ендіруде. Мысалы, ҚР ІІМ жанындағы Ювеналды полиция қызметкерлері шетелдік

әріптестерімен тәжірибе алмасып, медиация, оңалту бағдарламалары, баламалы жаза түрлері бойынша оқытудан өтуде [81]. 2025 жылы мамырда Ташкентте өткен Орталық Азия елдеріне арналған жастар қылмысының алдын алу тренингіне қазақстандық полиция және әлеуметтік қызмет өкілдері қатысып, көпсекторлы әріптестік тәсілдерін үйренді. Онда немістің «Kurve Kriegen» (қылмыстың алдын алу бойынша) жобасы үлгі ретінде талданып, Орталық Азияға бейімдеу жолдары қарастырылды [89]. Мұның барлығы Қазақстанның жастар қылмысына қарсы күресте халықаралық стандарттарға сүйеніп, өз жүйесін жетілдіруге күш салып жатқанын көрсетеді.

Сонымен бірге, киберқылмыстардың өсімі жағдайында халықаралық ынтымақтастықтың маңызы артуда. Қазақстан ғаламдық киберқауіптерге қарсы тұру үшін 2023 жылы Будапешт конвенциясына қосылуға шақыру алды [90]. және осы конвенцияға қосылу бағытында құқықтық базасын үйлестіруде [91]. 2024 жылы ҚР ІІМ жанынан «Киберқылмысқа қарсы іс-қимылдың 2025-2029 жылдарға арналған кешенді жоспарын» дайындау бойынша ведомствоаралық жұмыс тобы құрылып, онда жаңа киберқауіптерге қарсы механизмдер, соның ішінде кәмелетке толмағандарды интернеттегі қауіпті контент пен қылмыстық іс-әрекеттен қорғау шаралары әзірленді.

ОССЕ ұйымы бұл процеске сараптамалық қолдау көрсетіп, «қоғамның барлық жігін жұмылдыру» («whole-of-society approach») қағидатын басшылыққа алуды ұсынуда [91]. Яғни киберқауіптермен тиімді күресу үшін мемлекеттік органдар, жеке сектор, үкіметтік емес ұйымдар және азаматтардың бірлескен күш-жігері қажет. Бұның бір көрінісі - Қазақстанның цифрлық кеңістіктегі қауіпсіздікті қамтамасыз ету бойынша технология компанияларымен ынтымақтасып, балаларға арналған «қауіпсіз цифрлық өнімдер» жасауға тырысуы. Мысалы, Австралияның «eSafety Commissioner» моделіне ұқсас түрде, Қазақстанда интернеттегі буллинг пен зиянды контентке шағым қабылдап, оны жедел жоятын арнайы құрылым қалыптастыру идеясы талқылануда. UNICEF және өзге халықаралық ұйымдар Қазақстандағы балалардың онлайн қауіпсіздігін нығайту үшін медиа сауаттылықты арттыру бағдарламаларын енгізуді қолдайды.

UNICEF-тің мәліметінше, балаларды интернеттің зиянды әсерінен қорғау әрекеті ұлттық және жаһандық деңгейде қатар жүруі керек: бір жағынан мемлекет цифрлық сауаттылықты көтеріп, балаларға интернет қауіп-қатерлерін ажыратуды үйретуі тиіс, екінші жағынан - балаларға зиянды ақпаратты таратушыларды қадағалап, оларға қарсы құқықтық шараларды күшейту қажет. Осындай кешенді стратегия ғана балаларға арналған қауіпсіз цифрлық орта қалыптастыруға мүмкіндік береді деп санайды мамандар.

Қазақстан Үкіметі де балаларды интернеттегі зорлық-зомбылықтан сақтау үшін заңнамалық базаны жетілдіруді және ақпараттық-ағартушылық жұмысты күшейтуді бірдей жүргізуде. Жаңадан қабылданған 2022 жылғы «Балалар құқығын қорғау, білім беру, ақпарат және информатизация мәселелері бойынша заңнамалық өзгерістер туралы» заң арқылы интернеттегі балаларға зиян контенттен қорғау тетіктері нақтыланды. Дегенмен сарапшылар бұл заңнаманың әлі де әлсіз тұстары бар екенін

көрсетеді: мысалы, баланың психикасына зиян келтіретін ақпаратты шектеу тетіктері заңда анық жазылғанымен, оны іс жүзінде іске асыратын нақты механизмдер жоқ деп бағаланады. Яғни провайдерлер мен әлеуметтік желілердің балаларға қауіпті контентті сүзуге жауапкершілігі толық бекітілмеген. Осыған байланысты алдағы уақытта халықаралық озық тәжірибелерге сүйене отырып, заңнаманы жетілдіру жоспарлануда. Мысалы, Ұлыбритания қабылдаған «Интернет қауіпсіздігі» туралы заң үлгісі, Германияның Жастарды онлайн қауіптен қорғау туралы түзетулері Қазақстан үшін қызығушылық тудыруда [92]. Бұл құжаттарда әлеуметтік желі платформаларына балалардың қауіпсіздігін қамтамасыз ету міндеті жүктеледі, ата-ана бақылауы күшейтіледі және ережелерді сақтамаған компанияларға айыппұл салу тетіктері енгізілген.

Жоғарыда баяндалғандай, кәмелетке толмағандардың құқықтары мен мүдделерін тиімді қорғау алдын алу шаралары мен жауапкершілік арасындағы тығыз байланысты талап етеді. Алдын алу - баланың құқық бұзушылық жасамауы үшін қажетті жағдайларды қалыптастыру, қауіп-қатерді туғызатын себептерді жою болса, жауапкершілік - жасалған құқық бұзушылыққа әділ құқықтық баға беріп, баланы қайта тәрбиелеудің және жәбірленген тараптың құқығын қалпына келтірудің құралы. Екеуі бірін-бірі толықтыратын тетіктер. Қазақстан соңғы жылдары осы екі бағытты қатар күшейту арқылы оң нәтижелерге қол жеткізе бастады. Мәселен, Ішкі істер министрлігінің дерегіне қарағанда, кешенді жоспарлар мен жедел-профилактикалық шаралардың арқасында 2024 жылы жасөспірімдер қылмысы деңгейі өткен жылға қарағанда 6%-ға төмендеді, ал соңғы бес жылда жалпы 30%-ға азайды. Бұл айтарлықтай жетістік, профилактика мен жауапкершілік тетіктерінің үйлесімді іске асып жатқанын көрсетеді.

Дегенмен, қол жеткен табысты бекемдеу үшін жұмысты жалғастыру қажет екені де атап өтілуде - заңнамалық базаны одан әрі жетілдіру, әлеуметтік қолдау аясын кеңейту және алдын алуға қоғамды белсендірек қатыстыру өзекті міндет болып қалуда [81]. Мемлекет тарапынан дәл осы бағыттар бойынша шаралар жоспарланған: бала құқықтарын қорғау заңнамасына заман талабына сай толықтырулар енгізу, ата-аналарға, мектептер мен бизнес қауымдастыққа балалар қауіпсіздігі үшін ортақ жауапкершілік жүктеу, сондай-ақ балалардың өздерін құқықтық сауаттандыруды жалғастыру. Қорытындылай келе, кәмелетке толмағандардың құқықтары мен заңды мүдделерін қорғау ісі - көпқырлы кешенді процесс.

Онда превентивтік жұмыс пен жауапқа тарту тетіктері ажырамас байланыста қолданылады. Қазақстан тәжірибесі көрсеткендей, тек күштік әдістермен жасөспірімдер қылмысын жеңу мүмкін емес: оған әлеуметтік институттардың (отбасы, мектеп, қоғам) жұмылған күші қажет. Медиация, қалпына келтіру әділеттігі, тәрбиелік ықпал сияқты балама шаралар жазалаудың орнын толтырып, баланы әлеуметтендіруге көмектеседі.

Сонымен бірге, заң алдында бұлжытпай жауаптылық та қарастырылғаны маңызды - бұл баланың өз әрекетіне есеп беруін, қоғамның құқықтық тәртібінің сақталуын қамтамасыз етеді. Халықаралық стандарттар негізінде

Қазақстан балалық шақты қорғаудың және кәмелетке толмағандардың құқық бұзушылықтарының алдын алудың үйлестірілген жүйесін қалыптастыруда.

Бұл жүйеде бала құқығының басымдығы, бала істеген ісіне лайықты жауап беруі және ең бастысы - оның қайта тәрбиеленіп, қоғамға пайдалы азамат болып қалыптасуы көзделеді. Алдын алу мен жауапкершіліктің өзара байланысын нығайту арқылы ғана мемлекет өсіп келе жатқан ұрпақтың құқықтары мен мүдделерін толық қорғауға қол жеткізе алады деп қорытынды жасауға болады. Мемлекет пен қоғамның осы ортақ мақсаты - баланың жан-жақты қауіпсіз, қолайлы ортада өсіп, заңға құрметпен қарайтын тұлға болып қалыптасуына жағдай жасау - еліміздің тұрақты дамуының және адам капиталына салынған ең құнды инвестицияның бірі болмақ [81].

# 3 ХАЛЫҚАРАЛЫҚ ЖӘНЕ ШЕТЕЛДІК ТӘЖІРИБЕ

## 3.1 Халықаралық ұйымдардың (БҰҰ, ЮНИСЕФ, т.б.) киберқауіпсіздік стандарттары

Қазіргі цифрлық дәуірде кәмелетке толмағандардың онлайн кеңістіктегі қауіпсіздігін қамтамасыз ету халықаралық қауымдастықтың басты мәселесіне айналды. Балалар мен жасөспірімдер интернетте білім алып, ойын-сауық құрып, әлеуметтік желілерде еркін байланыс орната алады, алайда цифрлық мүмкіндіктермен қатар елеулі қатерлер де туындауда - кибербуллинг (онлайн қорқыту), жыныстық қанау мақсатындағы алдау (груминг), жеке деректердің құпиясын бұзу, заңсыз контентке қолжетімділік және өзге де киберқылмыстық әрекеттер. Киберкеңістіктің шекарасыз сипатта болуы бұл проблемаларды жеке бір мемлекеттің аясында ғана шешуді қиындататыны сөзсіз. Сондықтан БҰҰ, ЮНИСЕФ, ЕҚЫҰ, Еуропа Кеңесі, Еуропалық Одақ, Халықаралық телекоммуникация одағы (ITU) секілді халықаралық ұйымдар балалардың цифрлық құқықтарын қорғауға және киберқауіпсіздік стандарттарын қалыптастыруға бағытталған бірқатар құжаттар мен бастамаларды қабылдауда. Бұл бөлімде кәмелетке толмағандардың онлайн кеңістіктегі құқықтары мен заңды мүдделерін қамтамасыз етуге арналған аса маңызды халықаралық стандарттар, соның ішінде БҰҰ Конвенциясы мен өзге де көпжақты келісімдер, ЮНИСЕФ пен өзге ұйымдардың ұсынымдары қарастырылып, кибербуллингтің алдын алу, цифрлық ортадағы балалардың құқықтарын қорғау, киберэтика және балаларға қатысты цифрлық әділеттілік саласындағы халықаралық тәжірибелер талданады. Халықаралық актілер мен бастамалардың сыни тұрғыдан сараптамасы жүргізіліп, түрлі ұйымдардың көзқарастары салыстырылады.

Алдымен, балалардың құқықтарын жалпы қорғаудың іргетасы саналатын негізгі құжат – БҰҰ Бас Ассамблеясы 1989 жылы қабылдаған Бала құқықтары туралы конвенцияға тоқталайық. Бұл Конвенцияда әрбір баланың өмір сүру, даму, қорғалу және қоғам өміріне қатысу құқықтары бекітілген. Конвенцияның 19-бабында баланы барлық формадағы зорлық-зомбылықтан, соның ішінде психологиялық және физикалық зорлықтан қорғау міндеті көзделеді, ал 34-бапта балаларды сексуалдық қанау мен жыныстық зорлықтан қорғау қарастырылған. Аталған жалпы міндеттемелер қазіргі заманның цифрлық кеңістігінде де өзекті: мемлекеттер балаларды интернеттегі қорлау, зорлық-зомбылық пен қудалаудан, олардың ар-намысы мен беделіне қол сұғудан, сондай-ақ ақпараттық кеңістіктегі заңсыз әрекеттерден қорғауға жауапты. БҰҰ Бас Ассамблеясы өз резолюцияларында «баланың құқықтары - бұл адам құқықтары, және оларды офлайн да, онлайн да толық қорғау және құрметтеу қажет» деп атап көрсетеді [93]. 2021 жылы БҰҰ Балалар қоры (ЮНИСЕФ) мәлім еткендей, әлемде шамамен әрбір секунд сайын бір бала алғаш рет интернетке қосылады - бұл цифрлық технологиялардың балалар өміріне енуінің қарқынын аңғартады. Сол себепті балалардың дәстүрлі құқықтарын (ақпарат алу құқығы, ой-пікірін білдіру, жеке өмірінің қол

сұғылмауы, зорлық-зомбылықтан қорғану құқығы және т.б.) виртуалды ортада да пәрменді іске асыру тетіктері қажет.

Баланың құқықтары туралы конвенцияға қатысушы мемлекеттер оның талаптарын цифрлық дәуірдің сын-тегеуріндерін ескере отырып орындауға міндетті. 2016 жылы БҰҰ Адам құқықтары жөніндегі кеңесі «Баланың құқықтары: ақпараттық-коммуникациялық технологиялар және балаға қатысты сексуалдық қиянат» атты арнайы резолюция қабылдап, онда барлық мемлекеттерге балалардың АКТ құралдарына **толық, тең, қауіпсіз** қолжетімділігін қамтамасыз етуге және балаларды онлайн және офлайн ортада қорғауды күшейтуге шақырды. Бұл адам құқықтық тұрғыдан маңызды қағидат: бір жағынан, интернетке қолжетімділік - қазіргі заманда баланың ақпарат пен білім алу құқығын жүзеге асыруының шарты; екінші жағынан, цифрлық алшақтық (цифрлық теңсіздік) балалар арасында жаңа теңсіздіктерге әкеп соқпауға тиіс. Сол резолюцияда БҰҰ Кеңесі мемлекеттерді балаларды интернеттегі сексуалдық қанау мен зорлықтан заңнамалық қорғауды қамтамасыз етуге үндеді. Бұдан кейін де БҰҰ аясында балалардың цифрлық құқықтарына қатысты бірқатар қадамдар жасалды. 2021 жылдың наурызында Бала құқықтары жөніндегі комитет (Конвенцияның орындалуын қадағалайтын тәуелсіз орган) №25 Жалпы түсініктеме қабылдады. Онда тұңғыш рет Конвенциядағы мемлекет міндеттемелерін цифрлық ортаға бейімдеп түсіндіретін кешенді нұсқаулық берілді [94]. Аталған түсіндірмеге сәйкес, мемлекеттер білім беру, заңнамалық шаралар, саясат және реттеу арқылы балалардың барлық құқықтарын - сөйлеу бостандығынан бастап жеке өміріне дейін - онлайн кеңістікте қорғауға, сонымен бірге балаларды цифрлық технологиялардың зиянынан сақтау үшін қажетті заңдар мен техникалық шараларды қабылдауға тиіс. Комитет әсіресе балалардың үздік мүддесі қағидатын цифрлық саланың барлық шешімдерінде ескеру керектігін және балалардың өздерін қызықтыратын цифрлық саясат мәселелеріне қатысу мүмкіндігін қамтамасыз ету маңызын атап өтті. Мұндай халықаралық түсіндірмелік құжаттар ұлттық заңнамалар мен саясатқа бағыт-бағдар беріп, жаңа технологиялар жағдайында балалардың құқықтарын қалай сақтауды айқындайды.

Балалардың құқықтарын цифрлық ортада қамтамасыз ету мәселесі БҰҰ Бас Ассамблеясының соңғы жылдардағы қарарларында да көрініс тапты. Мысалы, 2023 жылы БҰҰ Бас Ассамблеясы барлық 193 мүше мемлекеттің келісімімен «Баланың цифрлық ортадағы құқықтары» жөнінде тарихта тұңғыш резолюция қабылдады. Бұл құжат мемлекеттерді Конвенция ережелерін цифрлық кеңістікке толық көлемде іске асыруға шақырады және балалардың жеке өмірі мен дербестігін қорғаудың маңыздылығын ерекше атап өтеді [95]. Бас Ассамблея қарарында үкіметтерге балалардың интернеттегі құпиялылығы мен деректерінің қорғалуын күшейту, олардың цифрлық өнімдер мен қызметтерді пайдаланудағы қауіпсіздігін қамтамасыз ету үшін ұлттық заңнаманы жетілдіру ұсынылды [96]. Бұл ретте балалардың цифрлық сауаттылығын арттыру және олардың интернеттегі зиянды контенттен қорғалуы халықаралық күн тәртібінде айрықша орын алды.

Осылайша, Біріккен Ұлттар Ұйымы деңгейінде қалыптасқан нормалар мен ұстанымдар мемлекеттерге кәмелетке толмағандардың киберқауіпсіздігін қамтамасыз етуде негізгі бағыт болып табылады.

БҰҰ жүйесінің мамандандырылған агенттіктері мен бағдарламалары да балалардың онлайн қауіпсіздігіне қатысты жаһандық стандарттарды дамытуда маңызды рөл атқарады. Соның бірі - халықаралық телекоммуникация саласын үйлестіретін ITU (International Telecommunication Union - Халықаралық телекоммуникация одағы). ITU 2008 жылы «Балаларды онлайн қорғау» (Child Online Protection) бастамасын қолға алып, 2020 жылы осы бағыттағы жаңартылған нұсқаулықтарды жариялады. ITU-дың 2020 жылғы Балаларды онлайн қорғау бойынша басшылық ұсынымдары балаларға арналған қауіпсіз және өнімді цифрлық ортаны қалыптастыру жолында барлық мүдделі тараптарға - үкіметтерге, компанияларға, ата-аналар мен педагогтерге, сондай-ақ балалардың өздеріне - арналған кешенді ұсыныстар жиынтығын ұсынады. Атап айтқанда, бұл құжатта төрт түрлі мақсатты топқа арнайы әзірленген бөлек нұсқаулық бар: 1) балаларға арналған - өздерін онлайн ортада қауіпсіз ұстауға үйрететін қарапайым тілдегі ережелер; 2) ата-аналар мен тәрбиешілерге - балаларды интернет қатерлерінен қорғау және цифрлық сауаттылығын дамыту бойынша кеңестер; 3) ақпараттық-коммуникациялық индустрияға - балаларға достық цифрлық өнімдер жасау және зиянды контентті шектеу, бала пайдаланушылардың деректерін қорғау жөніндегі стандарттар; 4) саясат жасаушыларға - ұлттық деңгейде балалардың онлайн қауіпсіздігін қамтамасыз ететін заңнамалық және институционалдық шаралар туралы ұсынымдар. ITU бұл нұсқаулықтарды ЮНИСЕФ және салалық сарапшылармен бірлесе дайындаған болатын. Нәтижесінде, бүгінгі күні көптеген елдер ITU ұсынымдарын өздерінің ұлттық стратегияларына негіз етіп алып, балаға қолайлы цифрлық экожүйе құруға талпынуда. Айта кету керек, ITU шеңберіндегі осы бастамалар жаһандық деңгейде балалардың киберқауіпсіздігін қамтамасыз етуге арналған бірыңғай терминология мен әдістемені қалыптастыруға көмектеседі.

Балалардың интернеттегі қауіпсіздігі мәселесін алға жылжытуда БҰҰ балалар қоры - ЮНИСЕФ-тің орны бөлек. ЮНИСЕФ өзінің мандаты бойынша бүкіл әлемде бала құқықтарының сақталуына жұмыс істейтін ұйым және соңғы онжылдықта ол цифрлық кеңістіктегі қатерлерге ерекше назар аударып келеді. ЮНИСЕФ «Балаларды интернетте қорғау» бойынша бағдарламалар жүргізіп, үкіметтер мен технологиялық компанияларға ықпал ету арқылы жаһандық деңгейде стандарттарды ілгерілетуде. 2017 жылы ЮНИСЕФ «Әлем балаларының жағдайы» атты жылдық баяндамасын толықтай балалардың цифрлық әлемдегі өміріне арнап, мемлекеттік органдар мен бизнес өкілдеріне балаларға қауіпсіз әрі пайдалы онлайн мүмкіндіктерді қамтамасыз ету жөнінде үндеу тастады. Аталмыш баяндаманың негізгі тезисі - цифрлық технологиялар балалар үшін зор әлеуетке ие, бірақ егер тиісті саясат пен корпоративтік жауапкершілік болмаса, интернет мүмкіндіктерінің теңсіздігі арттырғыш және қауіпті күшейткіш факторға айналуы мүмкін. Сондықтан ЮНИСЕФ үкіметтерді, IT-секторын және азаматтық қоғамды

балалар үшін цифрлық кеңістікті тең мүмкіндік алаңы етуге, баланың онлайн ортада дамып, білім алуына жағдай жасап, оны зияннан қорғау үшін бірігіп әрекет етуге шақырды [97].

ЮНИСЕФ практикалық деңгейде де көптеген бастамаларды жүзеге асырады. Ұйым әлем елдерінде балаларды кибербуллингтен, онлайн зорлық-зомбылық пен қанаудан қорғау бойынша ұлттық үйлестіру механизмдерін құруға атсалысып, құқық қорғау органдарын, мектептерді, ата-аналарды жұмылдыратын жобаларды қолдайды. Мәселен, ЮНИСЕФ қолдауымен «Global Kids Online» және «Disrupting Harm» атты ғаламдық зерттеулер жүргізіліп, балалардың цифрлық құқықтары мен интернет пайдаланудағы дағдылары зерттелуде. Бұл зерттеулер әр өңірдегі балалардың интернетке қолжетімділігі, кездесетін қауіп-қатері мен мүмкіндіктері туралы деректерді жинақтап, саясаткерлерге ғылыми негізделген ұсыныстар береді. ЮНИСЕФ сонымен бірге үкіметтермен бірлесіп балаларға қатысты киберқылмыстардың алдын алу және ашу бағытында жұмыс істейді. Ұйымның қолдауымен бірқатар елдерде құқық қорғау органдарының кибербала қылмыстарына қарсы арнайы бөлімшелері құрылып, тергеушілер мен полицияға оқыту өткізілуде. ЮНИСЕФ бастамасымен құрылған WePROTECT жаһандық альянсы да айрықша атап өтуге тұрарлық: бұл альянс аясында 90-нан астам мемлекет, халықаралық ұйымдар мен IT-компаниялар бірігіп, балаларға қатысты онлайн сексуалдық зорлық-зомбылықпен күресу үшін озық тәжірибе және технологиялармен алмасуда. Мысалы, ЮНИСЕФ пен технологиялық индустрияның ынтымақтастығы нәтижесінде балаға қауіпті контентті автоматты түрде анықтап, бұғаттайтын жаңа құралдар әзірленіп, бала пайдалушылардың деректерін қорғауға арналған салалық стандарттар енгізілуде [97]. ЮНИСЕФ сондай-ақ білім беру жүйесінде балалардың цифрлық сауаттылығын арттыру және онлайн ортада жауапты өзін-өзі ұстау этикасын сіңіру бағытында әдістемелік ұсынымдар дайындаған.

Ұйымның пікірінше, киберэтика - баланы ерте жастан интернеттегі мінез-құлық мәдениетіне үйрету, өзге адамдардың құқықтарын құрметтеу, цифрлық іздің маңызын түсіну - ақпарат ғасырындағы тәрбие жұмысының ажырамас бөлігі болуы тиіс. ЮНИСЕФ ұсынған стратегиялар шеңберінде көптеген мемлекеттер мектеп бағдарламаларына «цифрлық азаматтық» пәндерін енгізіп, балалар мен ата-аналарға арналған онлайн қауіпсіздік бойынша тренингтер өткізуде [98]. ЮНИСЕФ-тің мұндай кешенді тәсілі - құқықтық реформалардан бастап ағартушылық пен индустрия ынтымақтастығына дейінгі шараларды қамтуы - халықаралық деңгейде кең қолдау табуда және балалардың киберқауіпсіздігін арттырудың тиімді үлгісі ретінде қарастырылады.

Балаларды киберқылмыстан қорғау саласындағы маңызды халықаралық-құқықтық тетік - Еуропа Кеңесінің конвенциялары. Еуропа Кеңесі шеңберінде 2001 жылы қабылданған Киберқылмыс жөніндегі Будапешт конвенциясы (Cybercrime Convention) киберкеңістіктегі құқық бұзушылықтарды қылмыс деп тануға бағытталған ең алғашқы әмбебап келісім болып табылады. Бұл Конвенцияға қазіргі таңда Еуропа елдерімен

қатар әлемнің өзге де аймақтарынан ондаған мемлекет қосылған, яғни құжат шынымен жаһандық стандарт мәртебесіне ие. Будапешт конвенциясы бойынша қатысушы елдер компьютер жүйелеріне заңсыз қол сұғу, деректерді бұзу сынды дәстүрлі киберқылмыстармен қатар, балалар порнографиясына қатысты онлайн қылмыстарды өз ұлттық заңнамаларында қылмыстық жауаптылыққа тартуға міндеттенеді. Атап айтқанда, Конвенцияның 9-бабы әр мемлекетке кәмелетке толмағандардың порнографиялық бейнелерін цифрлық түрде өндіру, тарату, жария ету, иемдену сияқты әрекеттердің барлығын қылмыс деп тануды жүктейді. Ондағы «балалар порнографиясы» ұғымы шынайы балалардың да, кәмелетке толмағанға ұқсас көрінетін тұлғалардың да және бала кейіпіндегі реалистік кескіндердің де бейнелерін қамтиды.

Бұл талаптар мемлекеттердің қылмыстық заңнамасын біріздендіруге және трансұлттық деңгейде ынтымақтаса әрекет етуге мүмкіндік береді. Соның нәтижесінде Интерполдың халықаралық дерекқорлары мен құқық қорғау органдары арасындағы өзара ақпарат алмасу жеңілдеп, балаларға қатысты зорлық-зомбылық материалдарын таратушылардың жауапкершіліктен жалтаруы күрделене түсті. Қазақстан да 2018 жылы Будапешт конвенциясын ратификациялап, өз Қылмыстық кодексіне тиісті өзгерістер енгізгенін айта кету маңызды: елімізде Конвенция талабына сай «кәмелетке толмағандардың порнографиясы» ұғымы анықталып, оған қатысты әрекеттерге қылмыстық тыйым салынды. Жалпы, Будапешт конвенциясы балаларды киберқылмыстың аса қатерлі түрінен - порноиндустриядан - қорғау бойынша алғашқы әмбебап стандарт орнатты және әлем елдері арасында құқықтық ынтымақтастықтың негізін қалады [99]. Дегенмен, бұл Конвенция негізінен қылмыстық сот төрелігі саласын реттейтіні, яғни профилактикадан гөрі жазалау және тергеу механизмдеріне басымдық беретінімен шектеледі. Сондықтан балаларды интернетте қорғаудың одан да жан-жақты шараларын көздейтін қосымша халықаралық құралдар қажеттігі туды.

Еуропа Кеңесі аясында әзірленген келесі бір маңызды құжат - Балаларды сексуалдық қанаудан және жыныстық зорлық-зомбылықтан қорғау туралы Ланзароте конвенциясы (2007 ж.). Бұл конвенция баланы сексуалдық сипаттағы барлық қылмыстардан қорғауға арналған кешенді шарт, онда дәстүрлі қиянат түрлерімен қатар интернет арқылы жасалатын жаңа әдістер де ескерілген. Атап айтқанда, Ланзароте конвенциясы балаларды азғыру мақсатында онлайн байланыс орнатуды (кибер грумингті) қылмыс ретінде тікелей танитын ең алғашқы халықаралық-құқықтық акт болып табылады [100]. Конвенцияның 23-бабына сәйкес, кәмелетке толған адамның ақпараттық-коммуникациялық технологияларды пайдалана отырып, кәмелетке толмағанмен кездесу немесе жыныстық әрекет жасау ниетімен әңгіме бастап, оны өз үйінен тыс жерге кездесуге көндіруге бағытталған кез келген қасақана әрекеті қылмыстық жауаптылыққа жатуға тиіс. Осылайша, ересектердің интернетте балаларды арбау әрекеттері (мысалы, жалған тұлға болып сеніміне кіріп, сексуалдық мақсатта кездесу ұйымдастыру) заң жүзінде жазаланатын қылмысқа айналды. Ланзароте конвенциясы сонымен қатар балаларды жезөкшелікке тарту, балаларды порнографиялық шоуларға

қатыстыру, оларды порнографиялық материалдарға модель ретінде пайдалану секілді ұятты қылмыстарды қамтиды және мемлекеттерге мұндай іс-әрекеттерді де заң арқылы тыюды міндеттейді. Конвенция талаптарына сай, қатысушы елдер балаларға қарсы сексуалдық қылмыстардың алдын алу үшін мектеп бағдарламаларына білім беру компоненттерін енгізу, ата-аналарды хабардар ету, балаларға интернетте өзін-өзі қорғау дағдыларын үйрету бағытында шаралар қабылдауға тиіс. Сондай-ақ, жәбірленген балаларға арнаулы көмектесу қызметтерін (ыстық желі телефондары, психологиялық көмек, оңалту бағдарламалары) ұйымдастыру, қылмыскерлерді анықтау үшін жедел іздестіру шараларын халықаралық үйлестіру көзделген. Демек, Ланзароте конвенциясы өзінің ауқымы бойынша тек жазалаумен шектелмей, кешенді алдын алу мен қорғалу тетіктерін де орнататын көпжақты келісім саналады. Қазіргі күні бұл құжатқа Еуропа мемлекеттері ғана емес, басқа құрлықтардан да елдер қосылуда, ал Қазақстан 2018 жылы қол қойып, 2019 жылы ратификация жасады. Ұлттық заңнамаға Ланзароте талаптарын енгізу мақсатында еліміз «онлайн-платформада балаларды сексуалдық мақсатта азғыру» деген арнайы қылмыс құрамын бекітіп, мұндай әрекеттер үшін қылмыстық жауаптылық белгіледі. Ланзароте конвенциясының орындалуын қадағалау үшін құрылған Тараптар комитеті үнемі мониторинг жасап, қатысушы мемлекеттердің тәжірибесін бағалайды және қосымша ұсынымдар береді. Мысалы, 2015 жылы осы комитет Конвенцияның 23-бабы (онлайн азғыру) бойынша арнайы түсіндірмесін жариялап, онда әлеуметтік желілер мен ойын платформалары арқылы балаларды қорлауды қылмыстық қудалау мәселелерін нақтылады. Бұл халықаралық деңгейде балаларды жаңа қауіптерден қорғау бойынша құқық қолдану тәжірибесін бір ізге түсіруге ықпал етті.

Еуропа Кеңесі балалардың цифрлық құқықтарын ілгерілету мақсатында Конвенциялардан бөлек, жұмсақ құқық (soft law) құралдарын да қабылдап отырады. 2018 жылы Еуропа Кеңесі Министрлер Комитеті «Цифрлық ортада бала құқықтарын қорғау, қолдау және жүзеге асыру бойынша нұсқаулықтар» атты арнайы ұсыным қабылдады (CM/Rec(2018)7). Бұл құжат баланың интернеттегі барлық құқықтарын - ақпарат алу, байланыс бостандығы, жеке деректердің қорғалуы, білім алу, демалыс және ойын, зорлық-зомбылықтан қорғану, әділетті сот кепілдіктері және т.б. - кешенді түрде қарастырып, мемлекеттерге және интернет-провайдерлер, мектептер, ата-аналар сияқты тараптарға арнап нақты ұсыныстар береді. Онда цифрлық қызметтерді әзірлеуде балалардың жастық ерекшеліктерін ескеру (мысалы, «privacy by design» қағидаты - өнімдерді жобалаудан бастап жеке өмірге құрметті негізге алу), онлайн контентті жастағыларға сай жіктеу және зиянды материалдарға жол бермеу, ата-аналық бақылау құралдарын жетілдіру, мектепте цифрлық сауаттылықты оқыту, кибербуллинг пен онлайн-мәжбүрлеуді құқықтық деңгейде тыйым салу мәселелері қамтылған. Еуропа Кеңесі бұл ұсынымды әзірлеуге сарапшылар, үкіметтік емес ұйымдар және тікелей балалардың өзін қатыстыра отырып, кең консультациялар жүргізді; сондықтан құжат балалардың өз пікірін де ескеріп жасалған маңызды халықаралық стандарт

ретінде бағаланады. Бұған қоса, Еуропа Кеңесі 2022-2027 жылдарға арналған Балалар құқықтарын қамтамасыз ету стратегиясында балалардың цифрлық кеңістіктегі қауіпсіздігі мен мүмкіндіктерін кеңейту негізгі басымдықтың бірі ретінде айқындалған. Мәселен, стратегияда барлық балалардың цифрлық технологияларға қауіпсіз қолжетімділігін қамтамасыз ету, онлайн ортадағы зорлық-зомбылық пен қорлаудан қорғау және осал санаттағы балаларды цифрлық теңсіздіктен сақтау міндеттері көрсетілген. Еуропа Кеңесінің бұл бағыттағы ұстанымы - «нөлдік төзімділік» принципі, яғни балаларға қатысты зорлық-зомбылықтың ешбір түріне, оның ішінде интернетте орын алатын кішігірім буллинг не қудалау фактісіне де қоғамда орын болмауға тиіс.

Мұндай қатаң риторика Еуропа елдерінің заңнамасында көрініс тауып отыр: бірқатар мемлекеттер (мысалы, Италия, Франция, Германия) соңғы жылдары кибербуллингтің алдын алу және оған жауап беру туралы арнайы заңдар қабылдап, мектептерде буллингтің жолын кесу үшін жауапты тұлғалар институтын енгізді. Еуропа Кеңесі осы ұлттық тәжірибелерді жинақтап, ортақ платформада тарату үшін «Балаларға қарсы киберзорлықпен күрес бойынша ұлттық стратегиялар» сериясын жариялауда, мұнда әр елдің тәжірбиесі мен табысты шаралары талданып, өзге мемлекеттер үлгі алу үшін ұсынылған. Сол арқылы Еуропада балаларды кибербуллингтен қорғау туралы белгілі бір аймақтық стандарттар қалыптасып үлгерді.

Еуропалық Одақ шеңберінде де балалардың онлайн құқықтарын қорғауға бағытталған кешенді саясат жүзеге асырылып келеді. 2022 жылы Еурокомиссия «Балалар үшін жақсы интернет» (Better Internet for Kids - BIK+) атты жаңартылған стратегияны қабылдады. Бұл стратегия үш негізгі тұғырға негізделген: 1) қауіпсіз цифрлық тәжірибе (балаларға арналған онлайн қызметтердің қауіпсіздігі мен жарамдылығы, жастық шектеулерді сақтау, контенттік рейтингілер және ата-ана бақылауы тетіктері); 2) цифрлық қолдау және мүмкіндік беру (балалардың цифрлық сауатын арттыру, сындарлы әрі сыни тұрғыда интернетті пайдалану дағдыларын үйрету); 3) белсенді қатысу (балалардың цифрлық саясатты қалыптастыруға қатысуы, олардың пікірін ескеру). BIK+ стратегиясы барлық мүше мемлекеттерге осы бағыттар бойынша ұлттық бағдарламаларын жетілдіруді және бірлескен іс-қимылдарды ұсынды. Мысалы, стратегия аясында ЕО деңгейінде балаларға арналған сапалы цифрлық мазмұнды (білім беру, даму контентін) өндірушілерді қолдау, мектеп мұғалімдерін оқыту, ата-аналарға кеңес беру сияқты бастамалар қаржыландырылуда. Бұдан бөлек, Еуропалық Одақ қатарына кіретін елдер үшін міндетті заңнамалық актілер де балалардың онлайн қауіпсіздігін қамтамасыз етуге бағытталған. Солардың бірі - Жалпы деректерді қорғау регламенті (GDPR, 2016), бұл регламент бойынша ақпараттық қоғам қызметтерін пайдалануға бала келісімінің жас шегі 16 жас деп белгіленген (мүше елдер оны 13 жасқа дейін төмендете алады) және балалардың жеке деректерін өңдеуге ерекше талаптар қойылған. GDPR ережелері әлеуметтік желілер мен интернет-компанияларды 16 жасқа толмаған балаға ата-ана рұқсатынсыз тіркелуге мүмкіндік бермеуге міндеттейді, бұл балалардың жеке өмірінің қол сұғылмаушылығын қорғау

стандарты ретінде танылды. ЕО-ның тағы бір маңызды құжаты - «Аудиовизуалдық медиа қызметтер» директивасы (AVMSD, 2018 ж. жаңартылған), онда видео-платформалар мен стримингтік сервистерге балаларды зиянды контенттен (зорлық, порнография, әдепсіз материалдар) қорғау бойынша міндеттер жүктелген. Атап айтқанда, провайдерлер балаларға арналмаған контентті жас сүзгілерімен белгілеуге әрі оның таралуын шектеуге, ал балаларға арналған бағдарламаларда зорлық-зомбылық немесе алкогольді насихаттау кездеспеуін қамтамасыз етуге тиіс. Еуропалық Одақ 2021 жылы қабылдаған Балалар құқықтары стратегиясында да цифрлық ортадағы балалардың қауіпсіздігі бөлек тарау ретінде қарастырылды [101]. Онда мүше елдерге кибербуллингпен күресу жоспарларын әзірлеу, әр мектепте буллингтің алдын алу бағдарламаларын енгізу, интернет провайдерлерімен өзара ықпалдастықта балаға қауіпті контентті жою тетіктерін жетілдіру тапсырылды.

Еурокомиссия сонымен қатар соңғы жылдары интернеттегі балаларға қатысты жыныстық зорлық-зомбылық материалдарымен (Child Sexual Abuse Material - CSAM) күрес шараларын күшейтуде. 2020 жылы ЕО «Балаларға зорлық-зомбылық көрсетілген материалдармен күресу стратегиясын» жариялады, ал 2022 жылы мұндай контентті интернеттен автоматты түрде анықтап, құзырлы органдарға хабарлайтын арнайы жүйе құру туралы регламент жобасын ұсынды. Бұл бастама бойынша интернет қызметтеріне балалар порнографиясы мен азғындық материалдарын (соның ішінде «лаңкестік» деп аталатын көріністер) анықтау үшін жасанды интеллект және сканерлеу технологияларын қолдану талабы қойылмақ [96]. Аталмыш ұсыныс ЕО кеңістігінде қызу пікірталас тудырды: бір тарап балаларды қорғаймыз десе, екінші тарап бұны пайдаланушылардың жаппай жеке хат-хабарын тексеруге апарып соғатын құпиялылыққа қол сұғу деп бағалайды.

Бұл мысал халықаралық деңгейде де баланы қорғау мен жеке өмірге құрмет арасында тепе-теңдікті табу оңай еместігін көрсетеді. Дегенмен, Еуропалық Одақ балаларға қатысты онлайн құқық бұзушылықтарға қарсы күресте көптеген елдерге үлгі боларлық жүйелі саясат жүргізуде. ЕО қаржыландыратын Insafe/INHOPE желісі арқылы Еуропада әр мемлекетте балалар үшін қауырт желі (hotline) және кеңес беру желісі (helpline) қызметтері жұмыс істейді - балалар немесе олардың ата-аналары интернеттегі қауіпті жағдайлар жөнінде сол орталықтарға хабарлап, көмек ала алады. Мысалы, кибербуллингке ұшыраған бала тегін психологиялық кеңес алуға, ал желіде байқалған заңсыз контент туралы кез келген азамат арнайы сайтқа шағым жолдауға мүмкіндік бар. Бұл механизмдер ЕО стандарттарының бір бөлігіне айналған және бүгінде басқа аймақтар да Еуропа тәжірибесін қабылдап, ұқсас желілер құруда.

Еуропалық құрылымдардан бөлек, ТМД кеңістігі мен өзге өңірлерде де балалардың киберқауіпсіздігін қамтамасыз етуге арналған аймақтық келісімдер мен саясат бар екенін айта кету керек. Мәселен, Тәуелсіз Мемлекеттер Достастығында 2013 жылы Кәмелетке толмағандардың ақпараттық қауіпсіздігін қамтамасыз ету тұжырымдамасы қабылданып, оған

мүше елдер (соның ішінде Қазақстан) балаларды зиянды ақпараттан қорғау бойынша ұлттық заңнамаларын үйлестіруге келісті. Аталмыш құжат негізінде Қазақстан «Балаларды денсаулығы мен дамуына зардабын тигізетін ақпараттан қорғау туралы» заң (2015 ж.) қабылдап, ақпарат өнімдерін жастық санатқа бөлу жүйесін енгізді. Сол сияқты, Азия-Тынық мұхит өңірінде АСЕАН елдерінің цифрлық даму жоспарларында балалардың онлайн қорғалуы мәселесі қамтылған, Африка одағы да 2020 ж. «Балалардың интернеттегі қауіпсіздігі жөніндегі Африка стратегиясын» бекітті. Бұлар - әрине, біздің зерттеу тақырыбымыз тікелей қамтитын институттар емес, бірақ халықаралық үрдістің ғаламдық сипат алғанын көрсетеді.

Халықаралық ұйымдардың қатарында Еуропадағы қауіпсіздік және ынтымақтастық ұйымы (ЕҚЫҰ, OSCE) да балаларды киберқылмыстан қорғауға өз үлесін қосуда. ЕҚЫҰ - қауіпсіздік мәселелерімен шұғылданатын кең ауқымды саяси ұйым ретінде - киберқауіпсіздік пен киберқылмысқа қарсы күресті мемлекеттер арасындағы сенім шараларының бірі деп қарайды. Сол себепті ЕҚЫҰ цифрлық саладағы трансұлттық қатерлерге, оның ішінде балалардың онлайн құдалануы мен пайдалануына ерекше көңіл бөледі [102].

2017 жылы ЕҚЫҰ-ға мүше 57 мемлекет Министрлер кеңесінің шешімі №7/17 арқылы балалар саудасы мен сексуалдық қанауға қарсы бірлескен шаралар туралы келісілген декларация қабылдады. Онда қатысушы елдер балаларға қатысты барлық адам саудасы және сексуалдық қылмыстарға қарсы күресте күш біріктіруге, соның ішінде интернетті балаларды азғыру және қанау мақсатында пайдалану әрекеттерін қылмыстық жауаптылыққа тарту жөнінде міндеттемелер алды. Аталмыш шешімде ЕҚЫҰ мемлекеттеріне қылмыскерлерді жазалауды күшейту, қажет болса шетелде жасаған қылмыстары үшін де азаматтарын жауапқа тарту (экстратерриториалдық юрисдикция), құқық қорғау органдары арасында ақпарат алмасуды жолға қою секілді қадамдар ұсынылды. Сонымен бірге, интернетте балаларға қарсы жасалатын қылмыстардың алдын алу үшін қоғамдық ақпараттандыру және білім беру шараларының маңызы атап өтілді - ЕҚЫҰ құжатында қатысушы елдерге туристік салада, интернет компаниялары мен білім беру ұйымдарында балаларды қорғау мәселелері бойынша кең ауқымды ағартушылық науқандар жүргізу ұсынылды [98].

ЕҚЫҰ шешімі тек ұсынымдық сипатта болғанымен, оған ұйымның барлық мүшелері қолдау білдірді және бұл осы аймақта ортақ ұстаным қалыптасқанының белгісі еді. Қазақстан да ЕҚЫҰ-ның белсенді қатысушысы ретінде бұл шешімді құптады және өз заңнамасында балаларға қатысты қылмыстарға жазаны қатаңдату бойынша бірқатар өзгерістер енгізді (2019-2020 жж. қабылданған қылмыстық-құқықтық реформаларда көрініс тапты).

ЕҚЫҰ хатшылығы мен далалық миссиялары деңгейінде де балалардың цифрлық қауіпсіздігін ілгерілету жұмыстары жүруде. Мысалы, ЕҚЫҰ-ның Алматыдағы бағдарламалар кеңсесі 2018 жылдан бері Қазақстанның мектептерінде кибербуллингтің алдын алу бойынша тренингтер өткізуге қолдау көрсетіп келеді (бұл тренингтерге полиция инспекторлары, психологтер және ұстаздар тартылған). Ал Албаниядағы ЕҚЫҰ өкілдігі 2022

жылы елдің шалғай аймақтарында киберқауіпсіздік бойынша ақпараттық сессиялар ұйымдастырып, 300-ден астам оқушы, мұғалімдер мен ата-аналарды интернеттегі негізгі қатерлер туралы оқытты [98]. Бұл кездесулерде кибербуллинг, онлайн алаяқтық, мәлімет ұрлау, экстремистік үгіт сияқты тақырыптар талқыланып, балаларға өздерін және жеке деректерін қалай қорғау керектігі түсіндірілді. Осындай шаралар нәтижесінде көптеген оқушылар онлайн ортадағы қауіптерді жақсырақ түсініп, критикалық ойлау дағдыларын дамытқандарын мойындады [98]. ЕҚЫҰ бұдан бөлек Кавказ және Орталық Азия елдерінде кибергигиена (cyber hygiene) бағдарламаларын енгізуге жәрдемдесуде - бұл бағдарламалар жасөспірімдерге интернетте қарапайым қауіпсіздік ережелерін (күрделі құпиясөздерді пайдалану, бейтаныс адамдармен сақтық таныту, күмәнді сілтемелерді ашпау, т.б.) үйретуге бағытталған. Қорыта айтқанда, ЕҚЫҰ өз мандаты аясында негізінен алдын алу, оқыту және трансшекаралық ынтымақтастықты нығайту арқылы балалардың киберқауіпсіздік стандарттарын көтермелеуде. Бұл ұйымның артықшылығы - қауіпсіздік саласындағы саяси диалог алаңы бола отырып, полиция, шекара қызметі, сот және білім беру өкілдерін біріктіретін практикалық жобаларды жүзеге асыра алуында. Мұндай кешенді амал балаларға қарсы интернет-қылмыстардың түбірімен жою үшін маңызды.

Халықаралық қауымдастық тарапынан кәмелетке толмағандарды Кибер құқық бұзушылықтардан қорғау бойынша атқарылып жатқан шаралардың тиімділігін бағалай келе, бірнеше ортақ үрдісті аңғаруға болады. Біріншіден, барлық халықаралық ұйымдар балалардың цифрлық әлемдегі қауіпсіздігі мәселесін мойындайды және оны балалардың негізгі құқықтарының ажырамас бөлігі ретінде қарастырады. Бала құқықтары туралы Конвенцияның әмбебап қағидаттары - кемсітпеу, баланың мүдделерін басты орынға қою, өмір сүру және даму құқығы, баланың пікірін құрметтеу - бүгінгі күні киберкеңістікте толыққанды қолданыста болуға тиіс деп танылды [93]. Осы тұрғыда БҰҰ, ЮНИСЕФ және өзге институттар балалардың құқықтарын онлайн және офлайн режимде бөлместен тең қорғауды талап етуде.

Екіншіден, халықаралық стандарттар кешені тек құқықтық санкциялармен ғана шектелмейді, онда алдын алу мен ағарту шаралары үлкен орын алады. Мысалы, кибербуллингті қарастыратын болсақ, балалардың бірін-бірі қудалауын қылмыстық жолмен жазалау (әкімшілік айыппұл салу не қылмыстық жауаптылыққа тарту) ешбір елде негізгі шешім деп қабылданған жоқ. Керісінше, халықаралық құжаттар буллингтің алдын алу үшін мектептерде достық ахуалды нығайту, ата-аналардың ролін күшейту, әлеуметтік желі компанияларын қауіпті жазбаларды жоюға міндеттеу, құрбандарға психологиялық қолдау көрсету сияқты кешенді әдістерді ұсынады. Бұл - жазалаудан гөрі тәрбиелеу және қорғалуға басымдық берілетінін көрсетеді. Сол сияқты, киберқылмыс жасаған балаларға келсек (мысалы, ақпарат жүйелеріне бұзып кіру, онлайн алаяқтық, өзгелерді қорлау әрекеттерін кейде жасөспірімдер де жасауы мүмкін), халықаралық құқық оларды ересектермен тең жазалауға қарсы, қайта

баламалы тәрбиелік шаралар, қалпына келтіруші әділеттілік принциптерін қолдануды қуаттайды. БҰҰ-ның «Бейжің ережелері» (1985) және Баланың құқықтары туралы конвенцияның 40-бабы кәмелетке толмаған құқық бұзушыларға сот төрелігін мейлінше гуманистік және қалпына келтіру бағытында жүргізуді талап етеді. Демек, халықаралық стандарттар бойынша, бала тіпті киберқылмыс жасаса да, онымен жұмыс істеу - жазалау үшін емес, қайта тәрбиелеп, қоғамға бейімдеу үшін болуы тиіс. Цифрлық этикаға баулу, саналы интернет мәдениетін қалыптастыру - құқық бұзушылықтың алдын алудың анағұрлым нәтижелі жолы деп танылуда.

Үшіншіден, халықаралық ынтымақтастық пен көпсалалы әріптестік қағидаты барынша күшейіп келеді. Киберкеңістіктің жаһандық сипаты ұлттық деңгейдегі шаралармен ғана шектелуді мүмкін емес етеді. Сол себепті мемлекеттер өзара құқықтық көмек туралы келісімдер жасасып, полицияның трансшекаралық өзара іс-қимылын жолға қоюда. Интерпол мен Европолдың балаларға қатысты қылмыстармен айналысатын арнайы бөлімдері әлем елдерінің құқық қорғау органдарымен дерек алмасуды үздіксіз жүргізуде [103]. Жеке компаниялар мен үкіметтік емес ұйымдар да баланың қауіпсіздігі ісінде серіктес саналады - көптеген әлеуметтік желі провайдерлері ЮНИСЕФ және WeProtect альянсы кеңестеріне сүйеніп, өз платформаларында балалар үшін зиянды контентті анықтау алгоритмдерін жетілдіріп жатыр. Мысалы, Facebook, YouTube секілді алпауыттар баланың жалаңаш бейнесі бар фото-видеоны жою, кәмелетке толмағандарға бейтаныстардан хабарласу мүмкіндігін шектеу сияқты қосымшаларды ендірді, бұл да халықаралық бастамалардың жемісі.

Дегенмен, сыни тұрғыдан қарағанда, қол жеткізілген жетістіктерге қарамастан, кәмелетке толмағандарға қарсы онлайн құқық бұзушылықтардың ауқымы әлемде азаймай отыр. ЕҚЫҰ мәліметінше, соңғы 15 жылда әлемде анықталған бала саудасы құрбандарының саны үш есе өскен, ал интернет арқылы жасалатын балаларға қатысты сексуалдық қылмыстар үрейлі қарқынмен артуда [103]. ЮНИСЕФ сауалнамаларына сәйкес, жастардың үштен бірі интернетте кемінде бір рет буллингтің құрбаны болғанын, әр бесінші бала осының кесірінен мектепке баруды тоқтатқанын хабарлайды.

Демек, халықаралық стандарттар мен келісімдер өз-өзінен автоматты түрде проблеманы шеше алмайды - ең бастысы, оларды іске асыру деңгейі ақсап тұр. Көптеген дамушы елдерде тиісті ұлттық заңдар, техникалық құралдар және мамандар жетіспейді. Мысалы, кейбір мемлекеттер әлі күнге дейін Будапешт конвенциясына қосылмаған немесе қосылса да, ондағы ережелерді толық орындамай отыр, соның салдарынан қылмыскерлер «қауіпсіз айлақтар» тауып, жауапкершіліктен қашып құтылуда. Кей жерлерде құқық қорғау органдары мен соттарға балалармен жұмыс істеу бойынша арнайы тренингтер енгізілмегендіктен, жәбірленуші баланың қайталап зардап шегуі (тергеу барысында дөрекі сұрақ алу, т.б.) орын алып жатады. Халықаралық стандарттардың тағы бір осал тұсы - олардың көбінің міндеттеуші заңдық күші жоқтығы. Конвенциялар мен қатты құқық нормалары шектеулі, ал көптеген ұсынымдар мен декларациялар

мемлекеттердің саяси еркіне ғана сүйенеді. Мысалы, БҰҰ Бас Ассамблеясының 2023 жылғы резолюциясы өте прогрессивті құжат болғанымен, оны орындау тетіктері қарастырылмаған, яғни әр ел өзі қалаған шараларды ғана іске асырады. Бұл кей жағдайда декларативтілікке әкеледі.

Сонымен бірге, жаңа технологиялардың дамуымен халықаралық стандарттарға жаңа мәселелерге жауап беру қажеттігі туындауда. Бұған криптовалюталарды пайдаланып бала порнографиясына төлем жасау, «қараңғы тор» (Dark Web) желілерінде жасырын қылмыс жасау, балалардың жеке деректерін коммерциялық мақсатта заңсыз жинау сияқты қазіргі кезде өршіп келе жатқан проблемаларды жатқызуға болады. Жасанды интеллекттің дамуы да қос қырлы: бір жағынан ол зиянды контентті сүзуге көмектессе, екінші жағынан фейк («deepfake») порнография жасау, балаларды алдаудың күрделенуі секілді жаңа қатерлер пайда болуда. Осыған орай халықаралық ұйымдар тұрақты түрде жаңа ұсынымдар әзірлеп, стандарттарды бейімдеп отыр. Мысалы, 2021 жылы Еуропа Кеңесі сарапшылар тобы «балаларға қатысты зорлық бейнелерін онлайн анықтау үшін ЖИ қолдану этикасы» жөнінде талқылаулар бастады, ал 2023 жылы БҰҰ жанындағы Интернет басқару форумы балалардың цифрлық құқықтарын қорғау мәселесін Жаһандық цифрлық келісім (Global Digital Compact) жобасына енгізді. Бұл процестер халықаралық құқықтың үнемі даму үстінде екенін және балалардың киберқауіпсіздігі күн тәртібінен түспейтін өзекті тақырып болып қала беретінін көрсетеді.

Қорытындылай келе, халықаралық ұйымдардың (БҰҰ, ЮНИСЕФ, ЕҚЫҰ, Еуропа Кеңесі, ЕО, ITU және т.б.) киберқауіпсіздік стандарттары кәмелетке толмағандардың құқықтарын цифрлық әлемде жан-жақты қорғауға бағытталған көпқырлы жүйе қалыптастырды. Бұл жүйе әмбебап адам құқықтары принциптеріне негізделе отырып, арнайы салалық келісімдермен толықтырылған: бала құқықтары жөніндегі Конвенция жалпы қағидаттарды орнықтырады; Будапешт және Ланзароте конвенциялары секілді құралдар қылмыстық құқықтық шараларды нақтылайды; ЮНИСЕФ пен ITU нұсқаулықтары алдын алу мен білім беруге басымдық береді; ал аймақтық ұйымдар (ЕҚЫҰ, ЕО) өз аймақтарына бейімделген бағдарламаларды іске асырады. Барлық осы элементтер бірігіп, балалар үшін қауіпсіз, қолайлы және әділетті цифрлық ортаны құру мақсатына қызмет етеді. Әрине, мінсіз жағдайдан біз әлі алшақпыз - балаларға қарсы онлайн құқық бұзушылықтар толастаған жоқ, жаңа сынақтар пайда болып жатыр. Алайда халықаралық-құқықтық база біртіндеп нығайып, мемлекеттердің жауапкершілігі артып келеді. Ең бастысы, баланың жоғарғы мүддесі цифрлық заманның да басты талабы екені даусыз. Халықаралық стандарттарды ұлттық деңгейде мүлтіксіз жүзеге асыру, үкіметтер, бизнес және қоғам арасында әріптестікті күшейту арқылы ғана киберкеңістікті балалық шақ үшін қауіпсіз аймаққа айналдыруға болатыны айқын. XXI ғасыр балаларының лайықты және қорғалған дамуы - күллі халықаралық қауымдастықтың ортақ борышы, әрі бұл борышты өтеуде әкімшілік-құқықтық реттеу тетіктері заман ағымына сай жетілдіріліп отыруы тиіс. БҰҰ, ЮНИСЕФ және басқа да ұйымдар әзірлеген халықаралық

стандарттар, соның ішінде Қазақстан үшін де, балаларды киберқауіптерден қорғау және олардың цифрлық дәуірдегі құқықтарын қамтамасыз ету ісінде сенімді бағыт-бағдар болып табылады. Нәтижесінде, цифрлық әлем қауіп-қатер көзі емес, өсіп келе жатқан ұрпақ үшін мүмкіндіктер кеңістігіне айналуы тиіс - бұл халықаралық құқық пен ынтымақтастықтың келешектегі басты межесі болмақ.

### 3.2 Шет мемлекеттерде кәмелетке толмағандарды киберқауіп-қатерлерден қорғаудың құқықтық негіздері

Қазіргі заманда балалар мен жасөспірімдердің интернет кеңістігін еркін пайдалануы бір жағынан олардың дамуы мен білім алуына жаңа мүмкіндіктер ашса, екінші жағынан кибербуллинг, онлайн қудалау, алдау, зорлық-зомбылық және цифрлық қылмыс қаупін төндіреді. Дүниежүзілік денсаулық сақтау ұйымының Еуропалық өңірдегі зерттеуі бойынша, мектеп жасындағы әр алтыншы бала кемінде бір рет онлайн қорқыту мен зорлыққа тап болғанын көрсеткен [104]. Кибербуллинг пен интернеттегі өзге де қорқытушылықтардан кәмелетке толмағандарды тиімді қорғау көптеген елдердің құқықтық саясатының өзекті бағытына айналды. Төменде АҚШ, Ұлыбритания, Германия, Оңтүстік Корея және Балтық елдерінің (соның ішінде Литва мен Латвияның) осы саладағы құқықтық тетіктері талданып, олардың Қазақстандағы жағдаймен салыстырғандағы артықшылықтары мен кемшіліктері қарастырылады. Бұл мемлекеттер тәжірибесі арнайы заңнамалық актілерден бастап, құқық қолдану практикасы, цифрлық дәлелдемелерді пайдалану, мектеп пен ата-ана жауапкершілігі және платформаларды реттеу механизмдеріне дейін кең ауқымды қамтиды.

**АҚШ тәжірибесі.** Америка Құрама Штаттарында кәмелетке толмағандарды киберқауіптерден қорғау негізінен штаттық деңгейде жүзеге асады. Федералдық деңгейде тікелей «буллинг» немесе «кибербуллинг» туралы заң жоқ екені ресми түрде расталған. Яғни, АҚШ Конгресі бұны қылмыс ретінде жеке дара криминализациялаған емес (бұрын 2009 жылы федералдық деңгейде кибербуллингті қылмыс деп танымақ заң жобасы ұсынылса да, ол қабылданған жоқ. Алайда, федералдық заңнамада балаларды интернеттегі зиянды контенттен және қылмыстық әрекеттерден қорғауға бағытталған басқа нормалар бар. Мысалы, 1998 жылы қабылданған «Балалардың онлайн құпиялылығын қорғау туралы» заң (COPPA) 13 жасқа толмаған балалардың жеке мәліметтерін интернетте жинауды шектеп, ата-ана келісімін талап етеді. Сондай-ақ, интернет арқылы кәмелетке толмағандарды жыныстық мақсатына еліктіру, азғыру әрекеттері ауыр федералдық қылмыс саналып (18 АҚШ Кодексінің тиісті баптарында), қылмыскерлер қатаң жауапқа тартылады. 2018 жылы АҚШ Конгресі «Online Sex Trafficking Act (FOSTA)» заңын қабылдап, кәмелетке толмағандарды жезөкшелікке тарту немесе сексуалдық қанау мақсатындағы онлайн әрекеттерге қарсы күресті күшейту үшін интернет-платформаларға қосымша жауапкершілік жүктеді [105]. Кибербуллинг пен онлайн қудалауға тікелей қарсы шаралар негізінен

штаттар деңгейінде орын алған. 2010 жылдардан бері барлық дерлік штат өздерінің мектептер мен ювеналдық юстиция саласындағы нормативтік-құқықтық актілеріне өзгерістер енгізіп, буллинг пен кибербуллингтің алдын алу және оларға жауап қату тәртібін бекітті. 2018 жылғы дерек бойынша, 49 штатта мектептерге буллингтің, соның ішінде электрондық буллингтің (кибербуллингтің) алдын алу және оны тәртіптік жолмен тоқтатуға қатысты заңдар қабылданған [105]. Әдетте бұл заңдар мектеп округтерін буллингке қарсы саясат қалыптастыруға міндеттейді және көпшілігінде кибербуллинг те осы мектептік тәртіптік бақылау аясына кіреді. Мысалы, Калифорния штатында Білім кодексінде «буллинг» ұғымы нақты анықталып, оқушылардың бір-біріне электрондық хабарлар, әлеуметтік желілердегі жазбалар арқылы қоқанлоққы көрсетуі, кемсітуі немесе беделіне нұқсан келтіруі - егер ол әрекеттер оқушының қауіпсіздігі мен оқуына айтарлықтай зиян келтіруі мүмкін болса - тәртіп бұзушылық ретінде танылған.

Елеулі жағдайларда жәбірленуші немесе оның ата-анасы сотқа жүгіне алады, кейбір штаттарда кибербуллинг үшін қылмыстық жаза да қарастырылған (әдетте әкімшілік құқық бұзушылық немесе жеңіл қылмыс түрінде). Мысалы, бірнеше штаттың қылмыстық кодексінде электрондық құралдарды пайдалана отырып қудалау, қорқыту (cyberstalking) үшін жауаптылық көзделген. Калифорнияда кәмелетке толмағандардың өзі де кибербуллинг немесе кибер-қудалау жасағаны үшін ювеналдық сотқа тартылуы мүмкін екені атап көрсетілген. Яғни 18 жасқа толмаған құқықбұзушылар ювеналдық әділет жүйесі арқылы жауапкершілікке тартылады, ал жәбірленуші ата-аналары азаматтық шағымдар арқылы шығынды өндіре алады [106]. Бұдан бөлек, кей жағдайларда ата-аналардың өздері де балаларының заңға қайшы әрекеттері үшін азаматтық жауапкершілікке тартылуы мүмкін: АҚШ-тың біраз штатында «ата-ана жауапкершілігі» туралы ережелер бар, олар ата-ана баласының қылмыстық әрекеттерінің алдын алуда өрескел салғырттық танытса, жәбірленушіге өтем төлеуге міндеттеуі ықтимал.

АҚШ тәжірибесінде мектептердің рөлі айрықша. Мемлекеттік деңгейде ресми талаптар болмағанымен, StopBullying.gov сияқты федералдық ресурстар мектептер мен қоғамдастықтарға арналған нұсқаулықтар ұсынады. АҚШ Білім министрлігі мен Азаматтық құқықтар басқармасы нәсіл, жыныс, дін, мүгедектік секілді қорғалатын белгілер бойынша қудалау орын алса, оған мектеп міндетті түрде шара қолдануға тиіс екенін ескертеді. Егер мектеп ортада буллинг осы аталған белгілер бойынша өшпенділік не алалау сипатында болса, онда ол федералдық азаматтық құқық заңнамасына (1964 жылғы Азаматтық құқықтар туралы актінің IV, VI тараулары, 1972 жылғы Білім саласында кемсітушілікке тыйым салу туралы Title IX, т.б.) қайшы дискриминациялық қудалау ретінде қаралып, білім мекемесіне дейін жауапкершілік туындауы мүмкін [107]. Осылайша, АҚШ-та кибербуллингтің қарапайым түрлері тікелей федералдық бақылауда болмаса да, егер ол белгілі бір топқа қарсы өшпенділік немесе заңсыз қоқанлоққы түрінде көрінсе, федералдық деңгейде де қарастырылуы ықтимал.

Кибербуллингпен күресте АҚШ-тағы құқық қолдану тәжірибесі цифрлық дәлелдемелерді кеңінен пайдаланумен сипатталады. Әдетте жәбірленуші тарап немесе мектеп әкімшілігі буллинг фактілерін скриншот, электронды хат-хабарлар, әлеуметтік желідегі жазбалар түрінде құжаттап жинайды, кейін оларды тәртіптік жаза қолдануда немесе сот процесінде айғақ ретінде ұсынады. Мұндай электрондық дәлелдемелерді қабылдау соттарда қалыпты тәжірибеге айналған, тек олардың шынайылығы мен бүтіндігіне көз жеткізу талап етіледі. Мысалы, егер балаға онлайн түрде өміріне қауіп төндіретін қоқанлоққы жасалса немесе қорлау мазмұндағы хабарламалар жолданса, полиция сол жазбалардың ізін суытпай сақталуын қамтамасыз етіп, провайдерлерден қажет болған жағдайда қосымша ақпарат (IP-адрес, аккаунт иесінің деректері) алады. АҚШ-тың көптеген штаттарында мұғалімдер мен мектеп полициясына кибербуллинг оқиғаларын тергеу үшін оқушылардың гаджеттерін қарау немесе әлеуметтік желідегі көпшілік жазбаларды мониторинг жасауға белгілі бір өкілеттік берілген. Дегенмен, Fourth Amendment - жеке өмірге қол сұқпау және тінту жүргізудегі заңдылық - талаптары бойынша, құқық қорғаушылар электрондық дәлелдерді жинау кезінде ордер алу, құпиялылықты сақтау қағидаттарын ұстануға міндетті. Бұл тепе-теңдік (баланы қорғау қажеттігі мен конституциялық құқықтарды сақтау арасында) АҚШ құқықтық моделінің ерекшеліктерінің бірі саналады.

**Ұлыбритания тәжірибесі.** Ұлыбританияда (Ұлыбритания және Солтүстік Ирландия Біріккен Корольдігі) кәмелетке толмағандарды онлайн ортадағы зияннан сақтау бағытында соңғы жылдары ауқымды реформалар жүргізілуде. Ең алдымен айта кетерлігі - қазіргі қолданыстағы заңнамада «онлайн буллинг» ұғымының арнайы заңдық анықтамасы жоқ. Яғни, Ұлыбританияның қылмыстық немесе азаматтық кодекстерінде «кибербуллинг» дербес қылмыс түрі ретінде көрсетілмеген. Соған қарамастан, кибербуллинг пен интернеттегі қысым көрсетудің көптеген көріністері бар заңдар аясында жазалануы немесе азаматтық-құқықтық жауаптылыққа тартылуы мүмкін. Мысалы, 1997 жылғы Қудалаудан қорғау туралы заң (Protection from Harassment Act 1997) адамдарды жүйелі түрде қудалау әрекеттерін (оның ішінде электронды қудалауды) қылмыс ретінде қарастырады; 1988 жылғы Зиянды коммуникациялар туралы заң (Malicious Communications Act 1988) арқылы басқа адамға «әдепсіз не аса тұрпайы, қорлайтын мазмұндағы» хат, хабар жіберу - қылмыстық теріс қылық деп танылады; ал 2003 жылғы Байланыс туралы заңның 127-бабында көпшілік электрондық байланыс желісін пайдаланып «өте тұрпайы немесе әдепсіз мазмұндағы» хабар таратуға тыйым салынған. Осы нормалар кибербуллинг жағдайларында қолданылуы әбден мүмкін. Мәселен, әлеуметтік желіде балаға қарсы балағат, қорлау сөздер айту немесе жалған өсек тарату жоғарыдағы баптар бойынша құқықбұзушылық саналып, кінәлі адам айыппұл не 6 айға дейін бас бостандығынан айрылу жазасына кесілуі ықтимал [108]. Сол сияқты, егер кибербуллинг анық кемсітушілік немесе жеккөрушілік сипатта болса (мысалы, нәсілдік немесе діни өшпенділік), онда

1986 жылғы Қоғамдық тәртіп туралы заңның аясында өшпенділік тудыратын материал тарату немесе қорқыту бабымен қуғындау мүмкіндігі бар.

Ұлыбританияның құқық қолдану органдары онлайн қудалау істеріне соңғы жылдары үлкен мән беріп отыр. 2018 жылы Англия мен Уэльс прокуратурасы (CPS - Crown Prosecution Service) интернеттегі заңға қайшы әрекеттерді бағалау туралы арнайы нұсқаулықтарын жаңартып, кибербуллинг, троллинг сияқты құбылыстарға қалай құқықтық баға берілетінін түсіндірді [108]. Бұл нұсқаулықтар әлеуметтік желілердегі қорқытулар мен әлімжеттік әрекеттерін қылмыстық заң баптарына сәйкестендіруде прокурорларға бағыт-бағдар береді. Мысалы, біреуге интернет арқылы зорлық жасап жатырмын деп қоқанлоққы көрсету - Қылмыстық заңның «қорқыту» құрамына жатқызылуы мүмкін; ал балаға қатысты ерекше қатыгез, мазасыздандыратын хабарламалар легі - «қудалау (harassment)» бабымен рәсімделеді. Сондай-ақ прокурорлар әр істің сөз бостандығы тұрғысынан да салмағын өлшеп, қоғамдық мүдде мен бала құқығын теңгеріп қарауға тиіс.

Кәмелетке толмағандарды интернеттегі зияннан қорғауда Ұлыбританияның соңғы және ең ірі қадамы - «Онлайн қауіпсіздік туралы» 2023 жылғы заңы (Online Safety Act 2023) болып табылады. Бұл заң 2023 жылы Парламентте қабылданып, Корольдік мақұлдау алған соң күшіне енді. Актінің басты мақсаты - интернеттегі контентті реттеп, әсіресе балаларды зиянды мазмұннан қорғаудың қатаң жүйесін енгізу. Аталған заң бойынша ірі интернет-платформаларға (әлеуметтік желілерге, мессенджерлерге, т.б.) балаларға қауіпті контентті анықтау және оны жою бойынша “қамқорлық міндеті” (duty of care) жүктелді. Яғни, платформалар енді балаларға зиян тигізуі мүмкін заңсыз контентті ғана емес, заңға қайшы болмаса да балаға «зиянды» деп танылған материалдарды бақылап, олардың таралуының алдын алуға тиіс. Мәселен, кибербуллингке ұшыраған балаға қатысты қорлау не қорқыту жазбаларын платформа жедел түрде өшіріп, қайталанбасына кепілдік беретін жүйе орнатуы керек. Заң бұл талаптарды орындамаған компанияларға жылдық жаһандық айналымының 10%-ына дейін немесе 18 млн-ға дейін (қайсысы көп болса) айыппұл салу мүмкіндігін қарастырған.

Сондай-ақ реттеуші орган - Ofcom - қажет жағдайда сот санкциясымен бүкіл платформаны ел аумағында бұғаттауға құқылы [109]. Онлайн қауіпсіздік туралы заңда кибербуллингке тікелей қатысты жаңа қылмыстық нормалар да енгізілді: мысалы, әдейі біреуге эпилепсиялық талма туғызу үшін жарықшақты (маяк) суреттер жолдау, жалаңаш суреттерді рұқсатсыз жаппай тарату (кибер-флэшинг) сияқты әрекеттерге тыйым салынды. Бұл өзгерістер кәмелетке толмағандарды да зорлық-зомбылық сипатындағы контенттен қорғауға сеп болмақ.

Ұлыбританияда мектептердің және ата-аналардың жауапкершілігі заңнамалық және саяси құралдар арқылы ынталандырылады. Мектептерге заң бойынша жүктелген міндет - оқушыларын кез келген буллингтің түрінен, соның ішінде онлайн буллингтен сақтау, оның алдын алу. 2006 жылы қабылданған Білім және инспекция туралы заңның 89-бөлімі әр мектепке буллингке қарсы саясат болуы керек екенін және мұғалімдердің мектеп

аумағынан тыс жерде болған буллингке де (егер ол мектеп оқушыларына әсер етсе) араласуға құқығы барын бекітті. Ұлыбританияның Білім министрлігі «Мектептерде балалардың қауіпсіздігін қамтамасыз ету» (Keeping Children Safe in Education) деген жетекші нұсқаулық таратып, онда онлайн қауіптерден қорғау - мектептің бала алдындағы міндеті екенін атап. Ата-аналарға келсек, Ұлыбритания үкіметінің **DirectGov** порталында және **NSPCC** (балаларға қорғаншылық қоғамы) сияқты ұйымдардың ресурстарында ата-аналарға арналған кеңестер берілген. Онда ата-ана баласының интернеттегі әрекеттерінен хабардар болып, керек кезде сүзгілер (фильтрлер) орнатып, шектеу қоюы тиіс екені айтылады. Дегенмен, Ұлыбритания заңнамасында ата-ананы тікелей жазалайтын норма жоқ - ата-ана жауапкершілігі көбіне этикалық әрі азаматтық-құқықтық тұрғыда ұғылады (баласы өзгеге зиян келтірсе, ата-ана жәбірленушінің талабымен азаматтық сотта белгілі жағдайда өтем төлеуі мүмкін).

**Германия тәжірибесі.** Германия кәмелетке толмағандарды интернеттің зиянды әсерінен қорғау ісінде жан-жақты әрі қатаң құқықтық базасымен танымал. Бұл елде балалар мен жастарды зиянды ақпарат пен қатыгездіктен қорғау жөніндегі арнайы заңдар жүйесі ертеден қалыптасқан. Мысалы, Жастарды қорғау туралы заң (Jugendschutzgesetz, JuSchG) бұқаралық ақпарат құралдарындағы балаларға арналмаған зиянды контентке шектеу қойып, жас рейтингі жүйесін енгізген. 2021 жылы Германия бұл заңды цифрлық дәуір талаптарына сай жаңартып, онлайн платформаларға да бірқатар міндеттемелер жүктеді көрсетеді [110, с. 2022]. Атап айтқанда, жаңартылған заң бойынша интернет қызметтері балалар мен жасөспірімдерге қолайлы «қауіпсіз орта» қалыптастыру үшін профилактикалық шаралар қабылдауы тиіс: балаларға арналған пайдаланушы келісімдері, жасты ескере отырып әдепкі қауіпсіздік баптауларын орнату (мысалы, бала аккаунтын іздеу жүйелері таба алмауы керек), ата-анаға контентті басқару мүмкіндігін беру, және ең бастысы - платформада зиян көрген балаларға арналған тәуелсіз кеңес беру, шағым айту тетіктерін қолжетімді қылу талабы қойылды.

Сонымен бірге, заңмен жаңадан құрылып жатқан Балалар медиасын қорғау федералдық агенттігі (Bundeszentrale für Kinder- und Jugendmedienschutz) диалогтық реттеу үрдісінде барлық мүдделі тараптарды (ата-ана, компания, мемлекеттік органдар) үйлестіруге, заңның орындалуын қадағалауға жауапты болып белгіленді. Германия БҰҰ-ның Балалар құқықтары жөніндегі комитетінің «Балалардың цифрлық ортадағы құқықтары» туралы Жалпы түсініктемесін (2021) алғашқы болып іске асырған ел ретінде бағалануда [111].

Балаларды онлайн буллинг пен қудалаудан қорғаудың қылмыстық-құқықтық аспектісіне келсек, Германияда арнайы «кибербуллинг» немесе «киберқудалау» деген қылмыс құрамы жоқ. Дегенмен, қылмыстық кодекстегі жалпы баптар интернетте жасалған құқыққа қайшы әрекеттерге толығымен қолданылады. Мәселен, біреудің ар-намысын онлайн түрде қорлау (мысалы, әлеуметтік желіде балаға тіл тигізу) - Қылмыстық кодекстің 185-бабы («нагызлау, қорлау») бойынша жәбірленушінің арызына байланысты жауапқа

тартылуы мүмкін; қайталап қорқытып-үркіту, мазалау - 238-баптағы («қудалау», яғни Stalking) құрамына сәйкес келсе қудаланады; ал өмірге не денсаулыққа қатер төндіру - 241-бап («қорқыту») бойынша қылмыс саналады. Осы баптардың барлығы кәмелетке толмағандарға қатысты болса, бұл жауаптылықты ауырлататын мән-жай ретінде есепке алынуы ықтимал.

Айта кетсек, 2014 жылы Германия парламенті кәмелетке толмағанды буллингке ұшыратып, оның өз-өзіне қол жұмсауына себепкер болуды арнайы қылмыс ретінде қарастыратын түзетуді талқылаған еді; Францияда дәл осындай норма 2014 жылдан бар екені мәлім [105, с. 15]. Германия бұндай жеке бапты қабылдамағанымен, 2020 жылы «киберөзін-өзі өлтіруге үгіттеу» (Cyber-Grooming) мәселесіне қарсы заңдарды күшейтіп, кәмелетке толмағанды интернетте арбау үшін жалған жас қолдануға тыйым салатын, полицияға кәмелетке толмағанның кейпіне еніп операция жүргізуге рұқсат ететін өзгерістер енгізді.

Интернет-платформаларға заң талаптарын орындату тұрғысынан Германияның әлемге танымал тәжірибесі - «Желілік атқарушылық туралы заң» (Netzwerkdurchsetzungsgesetz, қысқаша NetzDG) болып табылады. Бұл заң 2017 жылы қабылданған және мақсаты - әлеуметтік желілердегі заңға қайшы контентті (өсек-өтірік, өшпенді сөз, зорлыққа шақыру, экстремизм, т.б.) жедел өшіруге мәжбүрлеу. NetzDG бойынша Германияда 2 миллионнан астам қолданушысы бар әлеуметтік желілер барлық «айқын заңсыз» деп танылған мазмұнды пайдаланушы шағымынан кейін 24 сағат ішінде өшіруге міндетті, ал анық-қанығы бірден білінбейтін күрделі жағдайларда 7 күн ішінде тексеріп, шешім қабылдауы керек. Орындамаған жағдайда платформаларға 50 миллион еуроға дейін айыппұл салынуы мүмкін.

Бұл заң әлемдік әлеуметтік медиа компанияларын өз ережелерін қатаңдатып, неміс пайдаланушылардың шағымдарын жіті қарауға итермеледі. Нәтижесінде көптеген балағат, қорлау, қорқыту жазбалары жойылып, әсіресе кәмелетке толмағандар туралы заңсыз контент (балалар порнографиясы, зорлық-зомбылық көріністері) лезде өшірілетін тәртіп орнады. Дегенмен, NetzDG заңы еркін пікір білдіру құқын шектеуі мүмкін деген сынға да ілікті. Бірақ Германия билігі балаларды интернеттегі тосын қауіптен қорғау үшін жылдам контент модерациясы қажет деп есептейді. 2021 жылы бұл заңға түзетулер енгізіліп, әлеуметтік желілерге пайдаланушылардың шағым беру үрдісін жеңілдету, шешімдерге шағымдану механизмін қосу және платформа сыртындағы сыртқы органдарға (Федералдық әділет басқармасына) қадағалау өкілетін беру сияқты өзгерістер күшіне енді [112].

Германияның азаматтық құқық жүйесінде ата-ана мен мектептің балалардың теріс қылықтары үшін жауапкершілігі де қарастырылған. Герман Азаматтық кодексінің 832-параграфы бойынша, егер кәмелетке толмаған бала басқаға зиян келтірсе (мысалы, буллинг арқылы денсаулығына зақым не жан азабын келтіру), оның ата-анасы немесе қамқоршысы өздерінің балаға тиісті дәрежеде бақылау (тәрбиелік қадағалау) міндетін орындамағаны дәлелденсе, жәбірленушіге өтемақы төлеуге міндеттелуі мүмкін [113]. Бұл норма

теориялық тұрғыда мектептегі немесе интернеттегі буллинг жағдайларына да қолданылуы ғажап емес - егер ата-ана баласының біреуді жүйелі қорлауына жол беріп, бұны тоқтатуға тырыспағаны анықталса, жәбірленуші отбасы сот арқылы моральдық зиянды өтеуді талап етуге құқылы. Сонымен бірге, көптеген федералдық жерлерде мектептер оқушылардың буллингі үшін жауапкершілікті бөліседі: мектеп әкімшілігі буллингтің алдын алмағаны үшін әкімшілік тәртіпте жазалануы мүмкін немесе жәбірленушіге зиянды өтеуге міндеттелуі де ықтимал (сот тәжірибесінде сирек болса да кездеседі). Жалпы алғанда, Германияның үлгісі - қатаң заңнамалық реттеу мен алдын алу шараларының үйлесімі. Бір жағынан, заңдар мен ережелер арқылы платформа, ата-ана, мектеп - барлығы белгілі бір жауапкершілік арқалайды; екінші жағынан, Германия балаларды медиа саласында сауаттандыру, олардың цифрлық мәдениетін көтеру ісіне де көңіл бөледі. Мысалы, мектеп бағдарламаларына киберэтикет, желідегі қауіпсіздік тақырыптарын енгізу, жергілікті Jugendamt (жастар қызметі) арқылы проблемалы отбасылармен жұмыс жасау секілді әлеуметтік шаралар қатар жүргізіледі.

**Оңтүстік Корея тәжірибесі.** Оңтүстік Корея соңғы онжылдықтарда жоғары технологиялық қоғамға айналуымен қатар, жастар арасындағы кибербуллинг, интернет арқылы өз-өзін кемсіту, суицидке итермелеу проблемаларына тап болды. Бұл елде кәмелетке толмағандарды интернет қауіптерінен құқықтық қорғау ауқымды әрі ерекше тәсілдермен жүзеге асады.

Ең әуелі, мектептегі зорлық-зомбылықтың алдын алу мен жауапкершілікке тарту үшін арнайы заң қабылданған - Мектептегі зорлық-зомбылықты алдын алу және қарсы шаралар туралы заң (School Violence Prevention and Countermeasures Act). Бұл заңға сәйкес, әр мектепте зорлық-зомбылық оқиғаларын қарайтын тәртіптік кеңес бар, және буллинг жасаған оқушыға мектепішілік шаралардан (ескерту, уақытша шеттету) бастап, арнаулы тәрбиелік бағдарламаларға жіберуге дейінгі ықпал ету қолданылады.

2023 жылы Корей үкіметі бұл салада жаңа қатаң ережелерді жариялады: мектеп буллерінің тәртіптік жазасы туралы жазбалар енді мектеп бітіргеннен кейін 4 жыл бойы жойылмай, сақталатын болды және 2026 жылдан бастап жоғары оқу орнына түсу кезінде осындай «буллингтік өткен» абитуриенттерді университеттер ескеруге міндетті болды. Бұрын бұндай жазалар 2 жылдан соң оқушының жеке ісінен алынып тасталатын, ал көптеген ЖОО-лар қабылдау барысында оларды мүлде қарастырмайтын. Енді жаңа ережеге сай, күрделі буллинг әрекеті үшін мектепте жаза алған түлек бұл деректі жасырмайды, керісінше университет қабылдау комиссиясы оны жалпы балл есептеуінде назарға алады. Бұл - Оңт.Бұл - Оңтүстік Корея қоғамының буллингке «нөлдік төзімділік» танытып, жастарды жауапкершілікке үйрету амалы. Бұған қоса, үкімет ауыр буллинг оқиғалары бойынша мұндай оқушылардың жұмысқа орналасу кезінде де ескерту алуын қарастыруда [114].

Оңтүстік Кореяда интернеттегі анонимдік арқылы қорлау мәселесін шешуге де талпыныстар болған. 2007 жылы ақпараттық-коммуникациялық желіні пайдалану туралы заңға 44-5-бап енгізіліп, ірі веб-порталдарда пікір

жазу үшін нақты аты-жөнін, жеке идентификациялық нөмірін растау - реал-эсім жүйесі (Real Name Registration, RRN) талап етілді. Бұл шара «жалған аттың артына тығылып, көрінбей тұрып балағат, жала жауып, негізсіз өсек таратудың» алдын алу мақсатын көздеді. Алайда 2012 жылы Корея Конституциялық соты бұл талапты сөз бостандығына сай емес деп тауып, күшін жойды. Сот RRN жүйесінің мақсаты орынды екенін мойындаса да, оның конституциялық құқықтарды шамадан тыс шектейтінін айтты. Сондай-ақ бұл жүйе қолданылған жылдары пайдаланушылардың жеке мәліметтері ұрланатын кибершабуылдар көбейіп кеткені белгілі - сол себепті де одан бас тартуға тура келді [115]. Реал-эсім жүйесінің орнына үкімет I-PIN атты балама идентификация құралын ұсынды, ол азаматтың ЖСН-н ашпай, жасын растауға мүмкіндік береді. Дегенмен, толық анонимдік мәселесі шешілмесе де, Кореяда интернетті «жасырын айыптаулар алаңы»на айналдырмау идеясын қоғам қолдайды. 2019 жылы танымал K-pop жұлдыздары Сулли (Choi Jin-ri) мен Гу Хара онлайн қорлаудан соң өздеріне қол жұмсаған қайғылы оқиғалар толқыны Кореяда үлкен дүмпу туғызды. Осыдан кейін «Сулли заңы» деп аталған бастама пайда болып, онлайн платформаларға қолданушылардың аты-жөнін (немесе расталған псевдонимін) көрсету талабын қайта енгізу ұсынылды. Әзірге бұл заң қабылданбағанмен, заңнамалық деңгейде кибербуллингпен күресті күшейту үшін міндетті цифрлық этикет сабақтарын мектептерде енгізу, әр компанияға қызметкерлер үшін буллингтің алдын алу тренингін өткізу сияқты шаралар қарастырылуда [116].

Оңтүстік Кореяда кәмелетке толмағандарды онлайн қылмыстардан (сексторшен, бала порнографиясы, интернет-алаяқтық) қорғау үшін де қатаң заңдар бар. Елдің Қылмыстық кодексі бойынша жала жабу мен қорлау (дауысқа шығару) қылмыстары интернет арқылы жасалса да жауаптылықтан құтылмайды - тіпті Кореяда жалған болмаса да біреудің абыройына нұқсан келтіретін ақпаратты онлайн таратқаны үшін де қылмыстық жаза қарастырылған. Сол сияқты «Интернет желісін пайдалану және ақпаратты қорғау туралы» заңның 44-7-бабы бойынша онлайн ортада көрсетілген қорлайтын, әдепсіз контент үшін кінәліге 3 жылға дейін түрме жазасы немесе ауыр айыппұл салынуы мүмкін. Цифрлық жыныстық қылмыстарға (оның ішінде кәмелетке толмағандардың интимдік мәліметтерін рұқсатсыз тарату, оларды азғыру) жазалар бірнеше рет қатаңдатылды - 2020 жылы атышулы «Nth Room» ісінен кейін парламент заңдарды қайта қарап, жазаны ұлғайтты, ал құқық қорғау органдарында осындай істерге маманданған бөлімдер құрылды. Жалпы, Оңтүстік Корея моделі кәмелетке толмағандарды киберқорғауда тәртіптік және қылмыстық шаралардың біртұтас кешеніне сүйенеді. Балаларға мектептен бастап интернет мәдениетін сіңіру, агрессорларға мүлдем төзбеушілік орта қалыптастыру, қажет болса кәмелетке толмаған құқықбұзушылардың өзін қатал жауапкершілікке тарту (тіпті олардың жоғары білім алу мүмкіндігіне әсер ету) - осының барлығы корей қоғамының балаларды қорғауды бірінші орынға қоюының көрінісі. Бұл модельдің артықшылығы - балаларды кемсіту, қорлау фактілерін жасырмай,

ашық анықтап, кінәлілерді жазалау арқылы басқаларға сабақ беру; ал кемшілігі - шамадан тыс қатаңдық баланың болашағына кері ықпал етпей ме деген сұрақтар (кейбір мамандар буллинг жасаған балаға өмір бойы таңба баспай, оны оңалтуға көңіл бөлу керек дейді). Сонымен бірге, анонимділікті шектеу бастамалары сөз бостандығын тежеп, авторитарлық бақылауға ұласпауын қадағалау қажет. Осы жәйттер корей үлгісінің ерекшелігін көрсетеді.

**Балтық елдері тәжірибесі (Литва, Латвия үлгілері).** Балтық мемлекеттері - Литва мен Латвия - кәмелетке толмағандарды киберқауіптерден қорғауда Еуропалық Одақ стандарттарына сүйене отырып, ұлттық ерекшеліктерін қалыптастырған. Екі ел де ЕО мүшесі ретінде балаларды интернеттегі зияннан қорғау жөніндегі директиваларды іске асырған және өз заңнамаларын соған бейімдеген.

Литва. 2009 жылы Литва «Кәмелетке толмағандарды қоғамдық ақпараттың зиянды әсерінен қорғау туралы» заң қабылдап, балаларға психикасына, дамуына залал келтіруі мүмкін материалдардың тізімін анықтады және бұқаралық ақпарат құралдары мен интернет провайдерлеріне осындай контентті балаларға қолжетімді етпеу міндетін жүктеді. Заңды қадағалау үшін Журналистік этика инспекторының қызметі және Байланыс реттеу қызметі жауапты болып белгіленген [117]. Бұл норма қазақстандық 2018 жылғы «Балаларды олардың денсаулығы мен дамуына зиянды ақпараттан қорғау туралы» заңына мазмұны жағынан ұқсас [92]. Литвада мектептердегі буллингке қарсы да арнайы нормалар бар: Білім туралы заңның 23-бабы білім беру орындарында балалардың қандай да бір зорлық-зомбылықтан, оның ішінде кибербуллингтен қорғалатынын бекітеді [117].

Мектептер буллинг оқиғасын болдырмауға және тоқтатуға міндетті, ұстаздар бұл үшін ата-аналармен бірге жұмыс істеп, қажет жағдайда психологтардың көмегіне жүгінеді. Литва Қылмыстық кодексінде тікелей буллинг ұғымы кездеспесе де, ауыр жағдайларда (егер буллинг бала денсаулығына зиян келтірсе немесе өзіне қол жұмсауға итермелесе) оны «денсаулыққа қасақана жеңіл зиян келтіру», «қорқыту», «өзіне қол жұмсауға дейін жеткізу» баптарымен саралау қарастырылған. 2016 жылы Литвада орын алған бір оқиғадан соң (оқушы қыз интернеттегі әлімжеттікке шыдамай суицидке барған) қоғамда буллингті қылмыс деп тану туралы мәселе көтерілді. Содан бері білім беру мекемелерінде буллингтің алдын алу бағдарламалары күшейтілді, әр мектепте «қауіпсіз мектеп» ережелері енгізіліп, оқушылар арасында құрдастар медиациясы тәжірибелері таралды.

Литва балаларды интернеттегі қылмыстардан қорғауда да ЕО деңгейіндегі механизмдерді қолданады: елде Литва қауіпсіз интернет орталығы (Safer Internet Centre) жұмыс істейді, оның жанында балаларға арналған 116111 қысқа нөмірлі сенім телефоны, киберқылмысқа шағым қабылдайтын интернет-желісі бар. Бұл орталықты Литва Республикасының Байланыс реттеу қызметі үйлестіреді [117]. Сонымен бірге, INHOPE (халықаралық интернет-хаттамалар қауымдастығы) желісіне қосылған ұлттық хотлайн - Švarus internetas порталы арқылы кез келген адам балалар

порнографиясы, балаларға қатысты қатыгездік немесе буллинг мазмұнын кездестірсе, арыз бере алады, оны тиісті органдар қарайды. Литва деректеріне сәйкес, балаларды мазалайтын онлайн құбылыстардың ішінде жиі кездесетіні - кибербуллинг және сексуалдық сипаттағы ұсыныстар.

Сондықтан 2021 жылы Литва үкіметі Балалардың қауіпсіз интернет стратегиясын бекітіп, онда 2021-2025 жылдарға арналған жоспарға кибербуллингтің алдын алу, мұғалімдер мен ата-аналарды оқыту және интернет-провайдерлермен ынтымақтастық ету шаралары кірді.

Латвия. Латвия да 2010 жылы «Қоғамдық ақпарат құралдары туралы» заңына өзгерістер енгізіп, зиянды интернет контенттен балаларды қорғау талаптарын енгізді. Атап айтқанда, провайдерлерге балаларға қауіпті ресурстарды (порнография, зорлық, есірткі насихаты) қолжетімсіз қылу тетіктері міндеттелді. Бірақ Латвияның тәжірибесіндегі ең қызықты жаңалық - анонимді буллерлердің аты-жөнін анықтау үшін заңға өзгерістер енгізуі. 2020 жылы Латвияның «Drossinternets.lv» атты Қауіпсіз интернет орталығы бастамасымен заңнамалық жұмыс тобы құрылып, нәтижесінде балаға интернетте белгісіз біреулер қысым көрсеткен жағдайда, құқық қорғау органдарына провайдерлерден әлгі «жасырын аккаунттың» иесін анықтау өкілеті берілді. Бұрын егер буллер жасырын атпен әрекет етсе және оның жеке деректерін білмесе, жәбірленуші тарап сотқа жүгіну түгіл, полицияға арыз берсе де іс ілгері баспай қалатын. Енді жаңа норма бойынша, баланың ата-анасы полицияға шағым түсірсе, тергеу барысында интернет-қызмет көрсетушіге немесе әлеуметтік желіге сұрау салып, бұзақының IP-мекенжайы мен тіркелу мәліметтерін алуға құқық бар. Осылайша, Латвияда кибербуллинг құрбандары «белгісіз дұшпаннан» заң арқылы қорғана алатын болды. Бұл өзгеріс Еуропадағы озық тәжірибенің бірі ретінде бағаланып, басқа мемлекеттерге де үлгі ретінде ұсынылуда. Латвияда сондай-ақ мектептерде «Буллингсіз орта» бағдарламасы жолға қойылған, ата-аналарға консультация беретін «Зорлыққа қарсы дауыс» (Balss pret vardarbību) қоғамдық қозғалысы белсенді жұмыс атқарады.

Балтық елдері, жалпы, Еуропалық Одақтағы балалардың цифрлық құқықтарын қорғау бастамаларына белсенді қатысады. Мысалы, 2024 жылы қабылданған ЕО Цифрлық қызметтер актісі (Digital Services Act, DSA) барлық мүше мемлекеттерді интернет платформаларында кәмелетке толмағандарды ерекше қорғауды қамтамасыз етуге міндеттейді. Литва мен Латвия осы талаптарды ұлттық заңнамаға енгізу шараларын бастап кетті Атап айтқанда, 18 жасқа толмаған пайдаланушылардың деректерін жарнама мақсатында пайдалануға тыйым салу, оларға бағытталған алгоритмдік ұсыныстарды шектеу және зиянды контентті жою мерзімдерін белгілеу ережелері бекітілмек. Балтық елдерінің тағы бір ұқсас сипаты - балалардың цифрлық сауатын арттыру бағдарламаларын қолға алуы. Литвада «Жизнь навыки» (Life Skills) деген мектептік курс енгізіліп, онда интернеттегі қауіпсіздік, кибербуллингке қарсы тұру, эмоциялық интеллект тақырыптары қамтылады. Латвияда Президент жанындағы Жастар кеңесі 2023 жылы балалардың интернеттегі мінез-құлқы туралы ұсыныстар пакетін әзірледі,

онда ата-аналарға, мектептерге және компанияларға ортақ жауапкершілік жүктеу көзделген.

Балтық елдерінің моделі - құқықтық реттеу мен қоғамдық бастамалардың үйлесуі. Бір жағынан, заңнамалық база ЕО стандарттарына сай үнемі жаңарып, жетілдіріліп отыр (зиянды ақпараттан қорғау заңы, медиа туралы заң, дербес деректерді қорғау нормалары - барлығы балалар мүддесін ескереді). Екінші жағынан, үкіметтік емес ұйымдар, қауымдастықтар да белсенді: ата-аналарға кеңес беру, буллинг құрбандарына психологиялық көмек, қауіпсіз интернетті насихаттау ісі жолға қойылған. Бұл мемлекеттер кішкентай болғанымен, цифрлық трансформацияны жылдам еңсеріп, балаларға жайлы онлайн орта құруға тырысуда.

**Қазақстанмен салыстырмалы талдау және қорытынды.** Шет мемлекеттердің кәмелетке толмағандарды киберқауіптерден қорғау үлгілерін қарастыра келе, олардың әрқайсысында қалыптасқан өзіндік артықшылықтар мен шектеулер бар екенін байқаймыз. Бұл тәжірибелер Қазақстан үшін де аса құнды, өйткені біздің еліміз де жаһандық цифрлық дәуірдің сын-қатерлеріне ұшырасып отыр. 2020 жылғы статистика бойынша Қазақстанда 11 жастан 15 жасқа дейінгі жеткіншектердің 11%-ы интернетте кемінде бір рет кибербуллингтің құрбаны не қатысушысы болғаны анықталған [92, с. 6]. 2021 жылы республика бойынша кибербуллингке қатысты 80 мыңға жуық шағым тіркелгені ресми мәлім [92, с. 12]. Бұл сандар мәселенің өзектілігін көрсетеді және оны шешуде халықаралық озық үлгілерді ескеруді талап етеді.

Қазақстан 2018 жылы балаларды зиянды ақпараттан қорғау туралы арнайы заң қабылдап [92, с. 13], Ресей, Литва тәрізді үлгідегі контенттік шектеулерді енгізді. Дегенмен, осы заң қабылданғаннан кейін де интернеттегі буллинг, құдалау фактілерін құқықтық бағалау қиындық туғызды - өйткені ұлттық заңнамада «буллинг», «кибербуллинг» түсініктері жоқ болатын [92, с. 8]. Тек 2022 жылы ғана Қазақстан бұл тұрғыда елеулі реформалар жасады: 2022 жылғы 3 мамырда «Баланың құқықтарын қорғау мәселелері бойынша кейбір заңнамалық актілерге өзгертулер мен толықтырулар енгізу туралы» №118-VII Заң қабылданып [92, с. 13], ресми түрде «буллинг» пен «кибербуллинг» ұғымдары алғаш рет құқықтық айналымға енгізілді [92, с. 14]. Бұл заң Қазақстандағы жағдайды «өлі нүктеден жылжытты» деп бағалануда, себебі енді мемлекеттік органдар мен интернет-платформалардың балаға бағытталған буллингке қарсы нақты міндеттері пайда болды. Атап айтқанда, Ақпарат және қоғамдық даму министрлігі ірі әлеуметтік желілермен (Facebook, Instagram және т.б. 100 мыңнан астам қазақстандық қолданушысы бар сервис) меморандумдар жасап, әр желі Қазақстанда өз өкілін тағайындауға келісті. Бұл өкіл министрлікпен бірлесіп, кибербуллинг оқиғаларын қадағалап, анықталған жағдайда 3 күн ішінде тиісті шара (қажет болса, постты өшіру, аккаунтты блоктау) қолдануы керек. Сондай-ақ қоғамда омбудсмен тәрізді Кибербуллинг жөніндегі арнайы уәкіл лауазымын құрып, барлық платформалардағы осы мәселеге жауап беретін тұлғалардың жұмысын үйлестіру ұсынысы талқылануда [92, с. 15].

Қазақстанның 2022 жылғы осы реформасы белгілі дәрежеде Ұлыбританияның және Германияның платформаларды міндеттеу үлгісіне ұқсайды (платформаның жергілікті өкілі арқылы заңсыз не зиянды контентті жою, есеп беру). Алайда, бұл қадамға қатысты сын пікірлер де бар: кейбір құқық қорғаушылар аталмыш өзгерістерді «бала құқын қорғаудан гөрі цензураны күшейту амалы» деп қауіп білдірді [92, с. 13]. Шынында да, «балаларға зиянды» деген желеумен билікке жайсыз контентті алып тастау тәуекелі әрқашан сақталуы мүмкін. Сондықтан Қазақстанға шетелдік тәжірибеден үйрене отырып, сөз бостандығы мен балаларды қорғау арасында нәзік тепе-теңдікті ұстайтын тетік табу өте маңызды.

Жаңа заң аясында Қазақстан Қылмыстық кодексіне де толықтырулар енгізді: енді ҚК 105-бабы 2-бөлігіне («өзін-өзі өлтіруге дейін жеткізу») интернет немесе телекоммуникация желілерін пайдаланып жасалса, жауаптылықты ауырлататын мән-жай ретінде белгіленді. Бұл тура мағынасында кибербуллингті қылмыс деп тану емес, бірақ егер онлайн қорлау мен қудалау бала үшін қайғылы салдарларға әкелсе (суицидке итерсе), тікелей қылмыстық жаза қолдануға жол ашты. Бұрын Қазақстанда буллинг, қорлау фактілері тек Әкімшілік кодекстегі «ұрып-соғу», «қорлау» сынды баптармен немесе Қылмыстық кодекстегі «өзін-өзі өлтіруге дейін жеткізу», «қорқыту», «жала жабу» баптарымен әрбір ситуацияға қарай жеке сараланатын еді [92, с. 15]. Енді буллинг нақты термин ретінде құқықтық лексикаға кіргесін, оның алдын алу, анықтау, есепке алу рәсімдері оңайлайды деп күтілуде. 2023 жылы Қазақстан Республикасы Оқу-ағарту министрлігі мектептерде буллингтің алдын алу ережелерін бекітіп, әр білім беру ұйымына буллингтің кез келген түріне нөлдік төзімділік саясатын қалыптастыру жүктелді. Бұл да шетелдік (әсіресе АҚШ пен Еуропа) тәжірибеден алынған қадам.

Салыстыра айтқанда, **АҚШ моделінен** Қазақстанға үйренер нәрсе - қоғамдағы әрбір институттың (мектеп, полиция, ата-ана, интернет-провайдер) балаға қолайлы орта жасауға атсалысуы. АҚШ-та федералдық заңның жоқтығы кемшілік сияқты көрінгенімен, әр штат өз ерекшелігіне сай бейімделген саясат жүргізуде. Қазақстан унитарлы мемлекет ретінде бірыңғай ұлттық заңдар қабылдап отыр, бірақ оны жүзеге асыруда аймақтық, жергілікті ерекшеліктерді ескеру қажет. АҚШ мектептері буллингке қарсы бағдарламаларды қауымдастық, жергілікті бизнес, полицейлермен бірлесе отырып жүргізеді - біздің елде де мектеп пен ата-ана кооперациясын арттыру керек. Сондай-ақ, АҚШ тәжірибесіндегі сөз бостандығын қорғау мен буллингті шектеу арасындағы құқықтық пікірталастар Қазақстан үшін де өзекті: балаларды қорғау сылтауымен кез келген ой-пікірді цензураламау қажет екенін естен шығармауға тиіспіз [92, с. 13].

**Ұлыбритания моделінен** аларымыз - кешенді реттеу мен тәуелсіз қадағалау тепе-теңдігі. Онлайн қауіпсіздік туралы заң арқылы Ұлыбритания компанияларға нақты жауапкершілік артып, балаларды қорғауды жүйелі жолға қойды. Қазақстан осыған ұқсас қадамды (өкіл тағайындау, мазмұнды жою талаптары) бастап кетті. Алайда, Ұлыбританияда бұл процесті

бақылайтын тәуелсіз Ofcom бар, ал бізде әзірге мұндай маманданған реттеуші жоқ. Мүмкін, болашақта Ақпарат министрлігі жанынан немесе Үкімет құрамында дәл балалардың онлайн қауіпсіздігін қадағалайтын арнайы орган (Ұлыбританияның Журналист этика инспекторы немесе Австралияның Э-Сейфти комиссары сияқты) құру керек болар. Сондай-ақ, Ұлыбритания ата-аналар мен мектептерге әдістемелік көмек беруде өте белсенді (мемлекеттік деңгейде нұсқаулықтар, NSPCC секілді ҮЕҰ желісі арқылы). Қазақстанда да бұл бағытты күшейтіп, ата-аналардың цифрлық тәрбиелеу дағдыларын арттыру, мектеп психологтарын арнайы оқыту маңызды.

**Германия үлгісі** Қазақстан үшін екі жақты. Бір жағынан, Германиядағыдай қатаң заңдар (мысалы, балаларға зиян контентті жылдам жою, платформаларды жауапқа тарту) біздің елде де енгізілуде. Екінші жағынан, Германия еркіндік пен цензура мәселесінде көп сарапқа салды, сөз бостандығына нұқсан келмеуіне қатты мән берді. Біздегі заң өзгерістерінде құқық қорғаушылар айтқан сынға назар аударып [92, с. 13], буллингке қарсы нормаларды теріс пайдалануға жол бермеу тетіктерін қарастырған жөн.

Мысалы, Германияда NetzDG заңын орындай отырып, компаниялар жалған шағымдар мен саяси мақсаттағы арыздарды сүзгіден өткізетін жүйелер енгізді; Қазақстан да әлеуметтік желілермен әрбір контентті бағалаудың әділ стандарттарын келісіп алғаны абзал. Сонымен бірге, Германияның ата-ана жауапкершілігі институты (Азаматтық кодекстегі §832) бізге де ой салады: ата-ана баласына интернетте басқаға зиян тигізбеуін үйретуге мүдделі болуы үшін, мүмкін, азаматтық-құқықтық жауаптылық тетіктерін қарастырған жөн шығар. Қазіргі Қазақстан заңнамасында тікелей бұндай норма жоқ, бірақ кей жағдайларда соттар жалпы азаматтық кодекстің зиян өтеу нормаларына сүйеніп, ата-ананы міндеттейді. Бұл салт-санамызға да жақын ұғым - «тәрбие - тал бесіктен» дегендей, егер бала қателік жасаса, белгілі дәрежеде ата-ана да жауап беретінін қоғам түсінуі тиіс.

**Оңтүстік Корея тәжірибесі** Қазақстанға кей тұста үлгі, кей тұста ескерту бола алады. Корейлердің мектеп буллерлеріне қатаң жаза қолдануы (аттестатқа белгі соғу, ЖОО-ға түсуіне кедергі жасау) біздің қоғам үшін тым қатал көрінуі мүмкін. Біздің менталитетте балаға «басынан шіркеу байлап беру» дұрыс емес деп саналады, көбінесе. Сондықтан Қазақстан буллинг жасаған баланы жазалаудағы басты мақсат - оны түзету, оңалту, қайта әлеуметтендіру болуы қажет. Жаза шаралары тек ең төтенше жағдайларда (басқа жол қалмағанда) қатайғаны жөн. Есесіне, Оңтүстік Кореяның ата-аналар мен педагогтарды жұмылдырып, бүкіл елде буллингке төзбеушілік мәдениетін құруы - өте құптарлық. Бізде де соңғы уақытта қоғам ішінде буллерлерді ақтау азайып, керісінше, жәбірленушіні қолдау артқаны байқалады. Мәселен, бірнеше резонанстық оқиғаларда (мектептегі әлімжеттік видеолары тарап кеткен) бұзақы жасөспірімдерді жалпы халық айыптап, ата-аналары қоғамдық кешірім сұрады. Мұндай қоғамдық пікір қысымы белгілі деңгейде тәрбие құралы бола алады, бірақ әрине, құқықтық шеңберден шықпауы тиіс (өз бетінше жазалау, балаға қол жұмсау сияқты әрекеттерге жол жоқ). Кореяның анонимділікті шектеу талпынысы бізде де кейде

айтылып қалады - әлеуметтік желілерде фейк аккаунттар мәселесі, жалған ақпарат тарату. Қазақстан ондай радикал шешімдерге бармауы керек, өйткені толық (нақты атымен тіркелу) еркін интернет табиғатына қайшы және біздегі интернеттің халықаралық инфрақұрылымына сәйкес емес. Оның орнына, Корея сияқты балама жол - отандық eGov немесе мобильді телефоны арқылы жасын растау, қажет жағдайда құқық қорғаушыларға жабық мәліметтерді сұрату механизмдерін жетілдіру дұрыс.

**Балтық елдері** Қазақстанға жақын үлгі - олардың заңнамасы бізге түсінікті, посткеңестік құқық жүйесінен шыққан. Литва мен Латвиядағы «Балаларды зиян ақпараттан қорғау» туралы заңдар біздің 2018 жылғы заңға мазмұндас [92, с. 3]. Демек, бұл бағытта Қазақстан осы елдердің жолын қуып келеді деуге болады. Бірақ Балтық мемлекеттерінде бұл заңдар қабылданғаннан кейін қоғам тарапынан бірқатар сын түзетулер енгізілген: мысалы, Литвадағы заңның бастапқы редакциясында «дәстүрлі емес сексуалдық қатынастарды насихаттайтын ақпаратты балаларға көрсетуге тыйым салу» нормасы бар еді, оны Еуропалық адам құқықтары институттары кемсітушілік деп тауып, өзгерту талап етілді. Қазақстан заңы да ақпараттың қандайы «зиян» екенін айқындауда ғылыми негізге сүйенуі қажет, әйтпесе артық шектеу қою оп-оңай, бірақ ол бала дамуына кедергісін тигізуі мүмкін. Мысалы, тек жасына сай рейтинг қоюмен шектелу керек пе, әлде біржола тыйым сала ма - осы жағын халықаралық стандарттарға сәйкестендірген жөн.

Латвияның анонимді буллерді анықтау заңын қабылдауы Қазақстанға өте пайдалы прецедент. Өйткені бізде де жиі кездесетін жағдай - белгісіз біреу фейк аккаунт арқылы балаға күн көрсетпейді, не интим суреттерін таратады, бірақ жәбірленуші оның кім екенін білмейді, ал полиция провайдерден дерек алу үшін заңдық негіз таппай қиналады. Енді Латвия үлгісі көрсеткендей, заңмен рұқсат етілсе, тергеушілер провайдерден ондай адамның жеке тұлғасын сұратып, істі алға жылжыта алады [118]. Қазақстан 2022 жылғы түзетулерінде бұл мәселені қарастырды ма? Қолданыстағы «Байланыс туралы» заңда немесе Қылмыстық-процестік кодексте электрондық ақпарат иелерін анықтау тәртібі бар, бірақ ол кибербуллингке арнайы бейімделмеген. Сондықтан, латвиялық тәжірибені зерттеп, біздің заңнамаға сәйкес бейімдеу артық болмайды.

Балтық елдерінің тағы бір ерекшелігі - мемлекет, ҮЕҰ және жеке секторының серіктестігі. Қазақстанда да «Safe Kazakhstan» сияқты жобалар арқылы ұқсас қадамдар басталды. Мысалы, қазақстандық мобильді байланыс операторлары балаға арналған «Kid Security» тәрізді қосымшалар ұсына бастады, кейбір интернет-провайдерлер «ата-аналық бақылау» функцияларын енгізді. Дегенмен, бұл шаралар әзірге жүйесіз, әркімнің өз еркінде. Латвиядағы Drossinternets.lv немесе Литвадағы Safer Internet LT сияқты құрылымдарды біз де қолдап, мүмкін «қауіпсіз интернет» бастамашыл тобын құрып, заңнамалық талқылауларға тартуымыз керек. Бұл азаматтық қоғам үнін естуге, заңдардың солқылдақ тұстарын дер кезінде түзеуге көмектеседі.

Қорыта айтқанда, шетелдік тәжірибелерді саралау Қазақстанда кәмелетке толмағандардың киберқауіпсіздігін қамтамасыз етуде кешенді, балансты

ұстаным қажеттігін айқындайды. Бір жақтан қарасақ, заңнамалық тұрғыда анықтаушы, тыйым салушы нормалар керек - буллинг ұғымын енгіздік, енді оның жазасын да орнықтыру маңызды (әсіресе ауыр түрлеріне). Екінші жағынан, тек жазалау жеткіліксіз - профилактика мен ағарту жұмыстары алдыңғы қатарда болуы тиіс. АҚШ пен Еуропа елдері соңғы зерттеулеріне сүйенсек, заңдардың қаталдығы буллингті түбегейлі жоя алмайды, бірақ мектептегі жайлы ахуал, ата-ана мен бала арасындағы сенім, жалпы қоғамдағы мәдениет буллингті азайтуға сеп. Сол үшін Қазақстанға қазіргі реформаларды жалғастыра отырып, ғылыми негізделген, тәжірибеге негізделген бағдарламаларды іске асырған жөн.

Шетелдік модельдердің артықшылықтарын пайдаланып, олардың қателіктерінен сабақ ала отырып, Қазақстан мына бағыттарға көңіл бөлуі қажет деп санаймыз:

- Заңнаманы жетілдіру: буллинг пен кибербуллингтің құқықтық анықтамалары енгізілген соң, ендігі қадам - оларды құқық бұзушылықтар градациясында орнықтыру (Әкімшілік кодексте жеңіл түрлері, Қылмыстық кодексте ауыр зардаптылары). Бұл ретте Австрия, Франция сияқты елдердің дайын үлгілерін қарастыруға болады. Мысалы, Франция 2014 жылы топ болып буллинг жасау деген қылмыс құрамын енгізіп, 15 жасқа толмаған балаға қарсы жасалса жазаны күшейтті деген дерек бар - біз де осындай жастық ерекшелікті ескеруіміз керек.

- Цифрлық дәлелдемелер мен тергеу: әрбір мектеп пен әрбір полиция бөлімшесінде интернет-құқықбұзушылықтар бойынша оқытылған маман болғаны дұрыс. АҚШ-тағы school resource officer моделі немесе Оңтүстік Кореядағы киберполиция бөлімдері бұл істі тиімді атқарады. Қазақстанда ІІМ құрамында Киберқылмысқа қарсы күрес басқармалары бар, бірақ олардың штатын ұлғайтып, аймақтық деңгейде де балалар ісіне бөлек назар аудартса құба-құп. Цифрлық дәлелдерді жинау, сақтау, сараптау бойынша тергеушілердің біліктілігін көтеру қажет - бұл халықаралық ынтымақтастық арқылы да (Интерпол, Еуропол желісі, Будапешт конвенциясы шеңберінде) жүргізуге тұрарлық.

- Платформалардың жауапкершілігі: Қазақстан жаһандық әлеуметтік желілермен конструктивті диалог орнатуды жалғастыруы керек. Біздің заң қабылданды екен деп, бір күнде Facebook немесе TikTok өздерін-өздері түзей салмайды. Ұлыбритания, ЕО елдері бұл компаниялармен жылдар бойы жұмыс істеп, ортақ Кодекстер әзірледі (мысалы, Балаларға арналған жасқа лайық дизайн кодексі - Британ ақпарат комиссары кеңсесі шығарған, оны компаниялар ерікті түрде жүзеге асыруда). Біз де сондай қосымша өздігінен реттеу құралдарын әкелуге тырысуымыз керек. Платформалар Қазақстан өкілдіктері арқылы жыл сайын балаларға қатысты инциденттер бойынша есеп беріп, қауіпті трендтерді (challenge, суицид топтары т.б.) анықтап отыруы тиіс.

- Ата-ана мен мектептің рөлі: халықаралық тәжірибе көрсеткендей, баланы интернеттегі зорлық-зомбылықтан ең алдымен жақын ортасы сақтай алады. Сондықтан ата-аналарды цифрлық ата-аналыққа үйрететін

бағдарламалар керек. Мектептерге буллингті тану және оған ден қою әдістерін үйретететін курстар енгізу, мұғалім-психологтарды даярлау міндет. Мысалы, Эстонияда әр мектепте «KiVa» деген финндік анти-буллинг бағдарламасы енгізілген. Сол сияқты, Қазақстан да педагогикалық ЖОО-ларда буллинг профилактикасы бойынша арнайы модульдер қосуына болады.

- Балалардың өзін қатыстыру: балалардың өз дауысы естілуі маңызды. Германия жаңа Жастарды қорғау заңында бала пікірін ескеруді жазса [111], біз де осыны үлгі алуымыз қажет. Мәселен, оқушылар комитеттері, еріктілер клубтары арқылы интернет этикасын насихаттау, буллинг құрбандарына қолдау топтарын құру - балалардың өз араларында сенім атмосферасын орнатуға көмектеседі. Жасөспірімдер үшін заманауи форматта (TikTok, YouTube арқылы) буллингке қарсы челленджер, роликтер жасауды ынталандыру қажет.

Түйіндей келе, кәмелетке толмағандарды киберқауіптерден қорғау - кешенді және үздіксіз күш-жігерді талап ететін міндет. АҚШ, Ұлыбритания, Германия, Оңтүстік Корея, Балтық елдері әрқайсысы өз тәсілдерімен бұл мәселеге жауап іздеп, құқықтық механизмдерін дамытып келеді. Олардың тәжірибесі көрсеткендей, «қатал заңдар + білім беру + технологиялық шешімдер + қоғам қолдауы» формуласы неғұрлым үйлесімді іске қосылса, соғұрлым нәтижелі болмақ. Қазақстан да осы бағыттағы алғашқы қадамдарын жасады - заңнамасы жаңарды, ұлттық стратегиялар айтылды. Ендігі жерде сол нормаларды өмірде тиімді қолдану, шетелдік озық амалдарды сындарлы интеграциялау және болашақ ұрпақтың қауіпсіз цифрлық әлемде еркін дамуына жағдай жасау - біздің ортақ парызымыз болуға тиіс.

### 3.3 Қазақстан заңнамасын жетілдіру үшін шетелдік озық үлгілерді бейімдеу

Кәмелетке толмағандарды киберкеңістіктегі қауіп-қатерлерден қорғау қазіргі заманның өзекті құқықтық міндетіне айналды. Статистика бойынша, интернет қолданушыларының әр үшіншісі әлі кәмелетке толмаған бала, ал ғаламдық деңгейде балаларға қатысты ең үлкен қатер - интернет арқылы жыныстық зорлық-зомбылыққа ұшырату болып тұр. Бұдан бөлек, кибербуллинг, зиянды ақпараттық контент, балаларды суицидке итермелеу, онлайн құмар ойындарға тәуелділік сынды құбылыстар жасөспірімдердің психикалық және физикалық саулығына тікелей зиян келтіруде.

Киберқылмыстардың жасырын жүзеге асуы, интернеттегі анонимдік пен жазасыз қалу мүмкіндігі бұл қатерлерді одан әрі ушықтыра түсуде. Мұндай жағдайда әлемнің көптеген елдері балалардың цифрлық кеңістіктегі қауіпсіздігін қамтамасыз етуге бағытталған кешенді шараларды қолға алды. Қазақстан да осы ғаламдық үрдістен қалыс қалмай, жасөспірімдерді қауіпті ақпараттан қорғау және олардың құқықтарын құрметтеу бағытында маңызды қадамдар жасауда. Соның айғағы ретінде 2018 жылы «Балалардың денсаулығы мен дамуына залал келтіретін ақпараттан қорғау туралы» №169-

VI ҚР Заңының қабылдануын атауға болады. Аталған заң балалардың ақпарат алу бостандығын шектемей-ақ, оларға зиян келтіретін контенттен қорғайтын құқықтық тетіктер қалыптастыру мақсатын көздеді [92, с. 3]. Дегенмен киберортадағы қатерлер үнемі эволюцияланып отырғандықтан, Қазақстан заңнамасын ұдайы жетілдіріп отыру - уақыт талабы. Бұл ретте АҚШ, Ұлыбритания, Германия, Оңтүстік Корея мен Балтық елдерінің озық тәжірибесін зерделеп, тиімді құқықтық моделдерін ұлттық ерекшеліктерді ескере отырып бейімдеу аса маңызды болып отыр. Төменде осы мемлекеттердің кәмелетке толмағандарды онлайн-қатерлерден құқықтық қорғаудағы тәжірибесі талданып, Қазақстан үшін пайдалануға болатын нақты тетіктер ұсынылады.

**АҚШ тәжірибесі.** АҚШ балаларды интернет кеңістігінде қорғау бойынша бірнеше бағытта кешенді тетіктер қалыптастырған. Біріншіден, балалар деректерінің құпиялығын қорғау қатаң реттеледі. 1998 жылы қабылданып, 2000 жылы күшіне енген Балалардың онлайн құпиялылығын қорғау туралы заң (COPPA) 13 жасқа толмаған балалардың жеке деректерін жинайтын веб-сайттар мен онлайн қызмет операторларына ата-анасының анық келісімін (verifiable parental consent) алуды міндеттейді. Яғни, бала туралы ақпаратты пайдалану немесе үшінші тарапқа беру алдында қызмет көрсетуші ата-анасына толық хабарлама беріп, рұқсат сұрауға тиіс [119].

Бұл талапты АҚШ Федералдық сауда комиссиясы қатаң қадағалайды. Мысалы, COPPA нормаларын бұзғаны үшін ірі технологиялық компанияларға миллиондаған айыппұлдар салынып келеді. Екіншіден, заң арқылы провайдерлер мен платформалардың жауапкершілігі белгіленген. АҚШ федералдық заңнамасы интернет-платформаларды пайдаланушылар жасаған контент үшін тікелей жауапқа тартпайтын иммунитет (Communications Decency Act 230-бөлігі) берсе де, балаларға заңсыз зиян келтіретін материалдар бойынша ерекше талаптар бар. 18 АҚШ Кодексінің 2258A-бөлігіне сәйкес интернет қызмет жеткізушілері өз жүйелерінде балалар порнографиясына қатысты контентті байқаса, міндетті түрде АҚШ Ұлттық Жоғалған және Эксплуатацияға ұшыраған балалар орталығына (NCMEC) хабарлауы тиіс; бұл талапты орындамау - құқықбұзушылық. Сонымен бірге NCMEC жанындағы Киберқауіп туралы желі (CyberTipline) арқылы әлемнің құқық қорғау органдары балаларға қатысты интернет-қылмыстар жөнінде ақпарат алмасады. Үшіншіден, мектептер мен кітапханаларда фильтрация шаралары заңмен қамтамасыз етілген. 2000 жылы қабылданған Балалардың Интернетті қорғау туралы заң (CIPA) аясында федералдық қаржыландыру алатын мектептер мен көпшілік кітапханалар балалар үшін зиянды деп танылған порнографиялық не зорлық-зомбылық мазмұндағы сайттарды сүзгіден өткізетін бағдарламалар орнатуға міндетті. Яғни, мемлекеттік бюджет есебінен интернетке қосылған оқу орындарында балаларға қауіпті контенттің қолжетімділігін техникалық түрде шектеу - шарт. Төртіншіден, кибербуллинг пен онлайн-құдалау мәселесі көбіне штаттар деңгейінде реттеледі. АҚШ-тың көптеген штаттары мектептерге кибербуллинг жағдайларын қадағалап, алдын алу жоспарын іске асыруды міндеттейтін

заңдар қабылдаған. Мысалы, кейбір штат заңдарында мектеп әкімшілігіне әлеуметтік желілердегі оқушыға қарсы қорлау әрекетін тәртіптік жолмен қарастыру жүктеледі, ал ауыр жағдайларда сот арқылы тиісті шектеу шаралары қолданылады. Федералдық деңгейде соңғы жылдары балаларды зиянды интернет мазмұннан қорғауға бағытталған «Балалар онлайн қауіпсіздігі туралы заң» (KOSA) жобасы, әлеуметтік желіге тіркелу үшін жасты тексеру бастамалары талқылануда. Мәселен, 2024 жылы бірнеше штат порнографиялық сайттарға кіру үшін пайдаланушының жасын куәландыруды талап ететін заңдар қабылдады. Алайда АҚШ Конституциясына енгізілген сөз бостандығы (Бірінші түзету) шеңберінде кәмелетке толмағандардың ақпаратқа қол жеткізу құқығын шектейтін шараларға қоғамда әрдайым пікірталас жүреді [120]. Сондықтан АҚШ тәжірибесі балалардың жеке дерегін қорғау, ата-ана мен мектептің рөлін арттыру және қауіпті контент пен қылмыстарға қарсы қатаң жазалау бағытын қамтиды, бірақ сонымен бірге балалардың ақпарат алу бостандығын да ескеру қажет екенін көрсетеді.

Қазақстан үшін АҚШ үлгісінен COPPA тәрізді балалар дерегін қорғау режимін бейімдеу маңызды қадам болмақ - бұл балалар туралы ақпаратты коммерциялық мақсатта пайдалануды шектеп, ата-аналардың келісімінсіз баланың жеке мәліметтері таралмауын қамтамасыз етеді [119]. Сондай-ақ, АҚШ-тағы сияқты, ұлттық ыстық желі механизмін енгізу тиімді: кез келген азамат немесе бала интернеттегі балаларға қатысты заңсыз әрекеттер (порнография, зорлық-зомбылық, балаға қоқан-лоққы жасау) туралы хабарлай алатын орталықтандырылған платформа болуы тиіс. Мұндай модель АҚШ-тағы NCMEC қызметі аясында сәтті іске асуда, ал Ұлыбританиядағы Internet Watch Foundation және Италиядағы Telefono Azzurro секілді ұйымдар да мемлекет қолдауымен бала құқығын онлайн қорғауға үлес қосуда [92, с. 14]. Қазақстанда да осындай «киберқауіп» туралы хабарламалар қабылдайтын ұлттық желіні құру - уақыт талабы. Бұл үшін заңнамалық тұрғыда провайдерлер мен желілерге тиісті материалды тез жоюға міндеттейтін және құқық қорғау органдарына шұғыл әрекет етуге мүмкіндік беретін нормалар қабылдануы керек.

**Ұлыбритания тәжірибесі.** Ұлыбритания соңғы жылдары балалардың онлайн қауіпсіздігін кешенді қорғауды заңнамалық деңгейде ең озық жүзеге асырған елдердің бірі болып танылуда. Мұнда «онлайн кеңістіктегі міндетті қамқорлық» (duty of care) қағидаты енгізіліп, ірі интернет-платформаларға балаларды зиянды контенттен қорғау жауапкершілігі заң арқылы жүктелді. 2023 жылы Королева келісімін алған Онлайн қауіпсіздік туралы заң (Online Safety Act, OSA) - осы бағыттағы ең ауқымды қадам. Аталған акт әлеуметтік желілер, бейне-платформалар және іздеу жүйелері тәрізді «пайдаланушылар арасында ақпарат алмасуды қамтамасыз ететін онлайн қызметтерге» арнайы міндеттер қойып отыр. Атап айтқанда, провайдерлер платформа дизайнынан бастап пайдалану ережелеріне дейінгі барлық деңгейде балаларды заңсыз және зиянды контенттен қорғауды қамтамасыз ететін тетіктер енгізуге тиіс. OSA бойынша Ұлыбританияның БАҚ пен телекоммуникация саласындағы реттеушісі - Ofcom - интернет кеңістіктегі балалар қауіпсіздігі талаптарының

орындалуын қадағалайтын уәкілетті органға айналды. Ofcom платформаларға нақты нұсқаулықтар мен іс-қимыл кодекстерін бекітіп, олардың сақталуын мониторингілейді; заңды бұзғандарға айналымының 10%-ына дейінгі мөлшерде айыппұл салу немесе ресурсты бұғаттау секілді санкциялар қолданылуы мүмкін. Бұл механизм Ұлыбританияны үкімет мәлімдегендей «әлемдегі онлайн тұрғыдан ең қауіпсіз елге» айналдыруды мақсат етеді [121].

Ұлыбритания балалардың цифрлық құқықтарын қорғауда «жас ерекшеліктеріне бейімделген дизайн кодексі» атты тың тәсіл енгізді. Ақпараттық комиссар басқармасы (ICO) әзірлеген бұл Балалар кодексі 2020 жылы күшіне енді [122]. Кодекс интернетте балалар жиі қолданатын кез келген қызметке (ойыннан бастап әлеуметтік желіге дейін) 15 базалық стандарт қояды [122]. Мысалы, онлайн сервис балалардың «ең жоғарғы мүддесін» басты назарда ұстауы тиіс; балалардың жеке деректері тек сол қызметті атқару үшін аса қажетті шекте пайдаланылуы керек; бала аккаунттарына ең қатаң құпиялық баптауларын әдепкі бойынша орнату талап етіледі; пайдаланушы саясаттары мен интерфейс түсіндірмелері қарапайым, бала түсінігіне сай тілмен берілуі шарт; балаларды зиянды әрекетке итермелейтін «қараңғы үлгідегі дизайн» (dark patterns) әдістеріне тыйым салынады [122]. Бұл кодекстің заңи күші - Ұлыбританияның Деректерді қорғау туралы заңы және GDPR талаптарымен ұштасуында: Кодекс ережелерін сақтамаған компанияларға ICO тарапынан айыппұл салынуы мүмкін. Нәтижесінде, көптеген ірі платформалар Ұлыбританиядағы балалар үшін қауіпсіздік шараларын күшейтуге кірісті (мәселен, Instagram желісі кәмелетке толмағандарға зиян контентті автоматты сүзгіден өткізу, түнгі уақыттарда хабарламаларды өшіру сияқты өзгерістер енгізді [123, с. 27].

Ұлыбритания бұған қоса балаларды онлайн ортада қорғау бойынша көпжақты институтционалдық амалдарды жолға қойған. Балалар қауіптілігі жөніндегі Ұлттық орталық (CEOP) полицияға қарасты құрылған, ол интернеттегі балаға қатысты құқықбұзушылықтарды (балаларды азғыру, онлайн сексуалдық қиянат, бала еңбегін қанау) тергеумен мамандандырылған айналысады. CEOP мектептермен және ата-аналармен тығыз жұмыс істей отырып, балаларға арналған қауіпсіздік сабақтарын, ата-аналарға кеңес беру және қауіпті жағдайларды хабарлау механизмдерін дамытуда. Үкіметтік емес секторда Интернетті қадағалау қоры (IWF) атты коммерциялық емес ұйым индустрияның қолдауымен жұмыс істеп, интернеттегі балалар порнографиясы материалдарын анықтап, хостинг провайдерлермен келісім арқылы оларды өшіртуге немесе бұғаттауға жәрдемдеседі [92, с. 14]. IWF сынды ұйыммен серіктестік орнату - Үкімет үшін тиімді, себебі ол қоғам мен бизнес өкілдерін жұмылдыра отырып, құқық қорғау органдарының жұмысын толықтырады. Қазақстан Ұлыбритания тәжірибесінен бірнеше маңызды элементті қабылдай алады. Ең әуелі, онлайн-платформалардың бала қауіпсіздігі үшін «міндетті қамқорлық» ұстанымын енгізу керек. Яғни әлеуметтік желілер, мессенджерлер, бейне-хостингтер өз сервистерінде балаларға зияны тиетін контент тарап кетпеуіне жауапты болуға тиіс. Бұл үшін Қазақстанда уәкілетті реттеуші органды (мәселен, Ақпарат министрлігі

жанынан немесе Балалардың құқықтарын қорғау комитеті жанынан) айқындап, оған платформаларды қадағалау, талап қою, айыппұл салу өкілеттігін беру ұсынылады. Екіншіден, UK ICO енгізген Балалар кодексі қағидаттарын ұлттық заңнамаға бейімдеп енгізу орынды.

Мысалы, Қазақстанның жеке деректерді қорғау заңына немесе «Бала құқықтары туралы» заңға арнайы норма қосып, онлайн қызметтерді балалардың жеке ақпаратын қорғаудың жоғары стандартына міндеттеу қажет (балалар дерегін сатуға тыйым салу, жасанды интеллект алгоритмдерін балаға бейімдеп оңтайландыру, т.б.). Үшіншіден, интернет провайдерлер мен ұялы байланыс операторларының балаларға зиянды ақпаратты сүзгіден өткізуге қатысты жауапкершілігін күшейту керек. Ұлыбританияда ірі провайдерлер Үкіметтің талабы бойынша «отбасы сүзгілерін» іске қосқан: әрбір үй пайдаланушысына порнография және зорлық мазмұнын автоматты блоктау қызметі ұсынылады. Қазақстанда да провайдерлерге осындай фильтрлерді абоненттерге тегін ұсынып, орнатуды жеңілдету міндетін жүктеу - балалардың интернетті қауіпсіз пайдалануын арттырады. Жалпы, Ұлыбритания үлгісі қатердің алдын алу мен технологиялық алыптардың жауапкершілігін заң арқылы нақтылау тұрғысынан құнды. Бұл механизмдерді енгізуде Қазақстан Ұлыбританиядағыдай сөз бостандығына кепілдік беру мен бала қауіпсіздігі арасындағы тепе-теңдікті сақтауы қажет.

**Германия тәжірибесі.** Германияда балалар мен жастарды зиянды ақпараттан қорғау федералдық және жергілікті деңгейдегі көпқабатты заңдар жүйесі арқылы жүзеге асады. Жастарды қорғау туралы федералдық заң (Jugendschutzgesetz, JuSchG) бастапқыда балаларды темекі және алкоголь өнімдерінен, кино және ойын-сауық контентінен офлайн кеңістікте (дүкендерде, кинотеатрларда) қорғауға бағытталған еді. Алайда цифрлық дәуір талаптарына сай 2021 жылы бұл заңға толықтырулар енгізіліп, онлайн-платформаларға қатысты арнайы міндеттемелер қосылды. Енді Германияда фильмдер мен ойындарға арналған ірі интернет-платформалар, хост-провайдерлер балаларды қауіпті контент пен қарым-қатынастан қорғайтын тетіктер орнатуға міндетті. Мысалы, стриминг-сервистер контентті жас категориясына сәйкес белгілеп, 18+-материалдарға қолжетімділікті тек ересек қолданушыларға беруге тиісті. Чат және әлеуметтік желі функциялары бар ойындарда провайдер бала пайдаланушыларды буллинг пен қудалаудан қорғау шараларын (фильтр, модерация, «шағым беру» батырмалары) қамтамасыз етуге міндеттелген. Бұдан тыс, Жастарды медиада қорғау туралы мемлектаралық шарт (JMStV) деп аталатын 16 жердің (федералды аймақтардың) келісімі бар. JMStV Интернеттегі және эфирлік медиадағы жасөспірімдерге зиян контентке жол бермеудің біркелкі стандарттарын белгілейді. Оның басты талаптары - контент пен жарнаманы жастық санаттар бойынша жіктеу, жас ерекшеліктерін растау жүйелерін (age verification) қолдану және балаға ауыр зардап әкелетін материалдарды хостингтен толық алып тастау. Германия тәжірибесінде провайдерлердің өз-өзін реттеуіне де көңіл бөлінген: медиасаланың ірі компаниялары құрған FSM (Ерікті өзін-өзі бақылау ұйымы) және jugendschutz.net секілді ұйымдар интернетті

мониторингілеп, зиянды материалдарға шағым жасап, оларды өшіру бойынша провайдерлермен жұмыс істейді. Сондай-ақ, федералдық жерлердің жастар министрлері қолдауымен әрекет ететін Кәмелетке толмағандарды медиада қорғау жөніндегі комиссия (KJM) бар, ол жаңа медиа қызметтерді жастарға зиян тұрғысынан сараптап, ұсынымдар береді. Германияның жуырдағы реформалары федералдық және жергілікті деңгейдегі ережелерді үйлестіруге бағытталғанымен, нормалардың қайталануы белгілі бір қиындық туғызады деп бизнес өкілдері сын айтуда. Дегенмен Германия үлгісінен Қазақстанға тікелей алуға болатын тиімді тетіктер аз емес. Біріншіден, ақпараттық өнімдерді жастық категориялар бойынша таңбалау жүйесін жетілдіру қажет. Қазақстанда 2018 жылғы заң бойынша да «6+», «12+», «16+», «18+» таңбалары енгізілгенмен, оны іс жүзінде қолдану механизмі әлсіз. Германияда бұл талап кино, телеарна, ойын индустриясынан бөлек интернет-контентке де қатыстылығымен ерекшеленеді: арнайы белгісі жоқ 18+ сайттарға балалардың кіруі шектеледі (мысалы, провайдер арқылы немесе арнайы бағдарламалармен). Екінші, жас ерекшелігін растау (верификация) технологияларын міндеттеу. Германияда порнографиялық не зорлық мазмұндағы сайттар ересек пайдаланушының кәмелеттік жасын тексеру үшін несие карта, электрондық идентификатор немесе басқа тәсіл қолданбаса, жауапқа тартылады [124]. Қазақстанда да осындай талапты заңмен бекітіп, орындалуын әкімшілік құқық бұзушылық санкцияларымен қамтамасыз етуге болады (мысалы, «интернет қызметтерінде кәмелетке толмағанның жасын растау шараларын қолданбау» деген тәрізді құқық бұзушылықты ӘҚБтК-ке енгізу). Үшіншіден, провайдерлерге зиянды материалдарды алып тастау міндетін жүктеу. Германияның жастарды қорғау актілерінде және Еуроодақтың Цифрлық сервис актісі (DSA) аясында ұлттық органдардың талап етуі бойынша белгілі бір заңсыз немесе балаға зиян контентті өшіру не қолжетімділікті шектеу керектігі қарастырылған [125].

Қазақстан да 2022 жылғы заңымен әлеуметтік желілерге үш жұмыс күні ішінде буллингтік жазбаларды жою талабын қойды [126]. Алайда бұл процедураны жүзеге асыруда ашықтық пен нақтылық қажет. Герман заңнамасында мұндай өшіру процесін реттейтін нақты регламенттер бар; соны негізге ала отырып, біздің елде де «зиянды интернет-контентті алып тастау тәртібі» туралы ереже енгізіп, қандай жағдайда қандай орган қандай шешім шығаратынын айқындап беру керек. Төртіншіден, техникалық фильтрация құралдарын қолдануды заң жүзінде бекіту. Германияда заң бойынша қоғамдық орындардағы (мектеп, кітапхана, интернет-кафе) интернет-тораптарда міндетті түрде балаларға зиянды сайттарды сүзетін бағдарламалар орнатылуға тиіс. Қазақстанда да бұл тәжірибені пайдаланып, білім және тәрбие беру ұйымдарында сертификатталған фильтрлік жүйелерді қолдануды міндеттеу ұсынылады. Оған қоса, Германиядағы сияқты, ата-аналарға арналған ақпараттандыру және техникалық қолдау жүйесін дамыту керек: коммуникация саласындағы реттеуші органдар ата-аналарға балалардың интернеттегі қауіпсіздігі туралы кеңестер, бақылау бағдарламалары бойынша нұсқаулықтар ұсынуы маңызды [125].

Қорыта айтқанда, Германия үлгісі Қазақстан үшін құқықтық нормаларды нақтылау, жас цензі мен техникалық қорғанысты ұштастыру тұрғысынан пайдалы. Дегенмен оны бейімдеуде біздің ұлттық құқықтық жүйенің унитарлы сипатын ескерген жөн: федерация емес болғандықтан, бізде бірыңғай заңдар қабылданып, оларды орындау тетіктерін нақты бір орталық орган қадағалауы тиіс.

**Оңтүстік Корея тәжірибесі.** Оңтүстік Корея - жоғары технологиялық цифрлық инфрақұрылымы бар және интернет қолданушыларының үлесі аса жоғары мемлекет. Бұл елде балаларды онлайн ортада қорғау мақсатында бірқатар қатаң да тыңғылықты шаралар заңнамалық түрде енгізілген. Солардың бірі - жасөспірімдерді зиянды ақпараттан техникалық шектеу тетіктері. 1990-жылдардың аяғында-ақ Кореяда «Жастарды зиянды ақпараттан қорғау туралы заң» қабылданып, арнайы Ақпараттық-коммуникациялық этика комиссиясы (ICEC) құрылған еді. Бұл комиссия интернеттегі контентті қадағалап, «онлайн контент-рейтинг жүйесін» енгізді: балаға зиянды деп танылған веб-сайттар мен материалдардың тізімін жасап, оларды ұлттық деңгейде сүзгіден өткізуге басшылық етті. 2001 жылдан бастап Кореяда Интернет-контентті сүзу туралы қаулы күшіне енді, ол бойынша интернет-провайдерлер арнайы тізімге енген зиянды сайттарға қолжетімділікті автоматты түрде бұғаттауға, ал кітапхана, мектеп, интернет-кафе сияқты қоғамдық орындар міндетті түрде фильтрациялық бағдарламалар орнатуға тиіс болды. Бүгінде бұл функциялар Корея коммуникация стандарттары комиссиясына (KCSC) берілген: KCSC интернеттегі заңсыз және зиянды материалдарды (порнография, зорлық, экстремизм, суицидтік контент т.б.) анықтап, провайдерлерге оларды өшіру немесе бұғаттау жөнінде нұсқаулар береді, орындалуын бақылайды.

Оңт. Кореяда жас ерекшелігін растау талабы да кеңінен тараған. Мәселен, 2016 жылы Оңтүстік Корея Netflix сервистеріне әлемде бірінші болып 19+ рейтингті фильмдер үшін пайдаланушының жасын жыл сайын тексеруді міндеттеді: кез келген корей пайдаланушысы 19+ санатындағы бейнемазмұнға қол жеткізу үшін өзінің аты-жөнін, туған күнін және жергілікті мобильдік нөмірін енгізіп, SMS-код арқылы растайды. Кей жағдайларда корейлік сервистер азаматтық нөмірді (social security number) сұрау арқылы немесе несие картасы мәліметі арқылы адамның кәмелеттік жасқа толған-толмағанын автоматты анықтайды [123]. Бұл жүйе порнографиялық немесе қатыгез мазмұнды кәмелетке толмағандардың көруін барынша тыюға бағытталған. Сонымен бірге, Оңт. Корея билігі онлайн ойындарға шектеу қою арқылы балалардың шектен тыс интернетке тәуелділігін азайтуға тырысты. 2011 жылы қабылданған «Күлшекыз заңы» (Shutdown Law) түн ортасынан таңғы 6-ға дейін 16 жасқа толмаған балалардың онлайн ойындарға кіруіне тыйым салды. Бұл заң біраз уақыт тиімді нәтиже бергенімен, айналып өту әрекеттері де кездескен (кейбір жасөспірімдер ата-анасының жеке сәйкестендіру нөмірлерін пайдаланып, шектеуді бұзғаны белгілі [127]. 2021 жылы Оңт. Корея үкіметі аталған тыйымды алып тастап, оның орнына ата-аналардың өз балаларын ойын

уақытын шектеуге ерікті мүмкіндік беретін «отбасылық бақылау» жүйесіне көшті. Бұл өзгеріс шектеудің тым қатаңдығынан бас тарту және ата-ана жауапкершілігін арттыру қажеттігін көрсетті. Бұдан шығатын түйін - Оңтүстік Корея тәжірибесі балаларды интернеттегі зияннан қорғауда мемлекет тарапынан белсенді араласу және техникалық қадағалау өте күшті болғанымен, оны іске асыруда ата-ана мен бизнес қауымдастықтың да рөлін ескеру керектігі. Қазақстан үшін Кореяның мына тәжірибелері пайдалы болуы мүмкін: біріншіден, балаларға қауіпті контентті ұлттық деңгейде сүзгіден өткізу инфрақұрылымын құру. Мәселен, Қазақстан бүкіл ел бойынша жұмыс істейтін бірыңғай «таза интернет» жүйесін енгізіп, онда анық зиянды сайттардың бірыңғай қара тізімін жасап, провайдерлерге автоматты бұғаттауды міндеттей алады (алайда мұндай жүйені енгізу сөз бостандығы мен ақпарат қолжетімділігіне шектеу келтірмеуі үшін ашықтық қажет, сондықтан сот не уәкілетті органның шешімімен ғана сайттар тізімге енгені жөн). Екіншіден, жас ерекшелігін растау технологияларын пайдалану.

Кореяның мысалындағыдай, Қазақстанда да азаматтардың ЖСН-іне негізделген цифрлық идентификация жүйесі дамыған (мобильді азаматтар базасы, электронды үкімет және digital ID құралдары бар). Соларды пайдаланып, 18+ сайттарға кіруді ұлттық көлемде реттеуге болады. Бұл үшін «Байланыс туралы» заң мен тиісті ережелерге өзгерістер енгізіп, 18 жасқа толмағандарға арналмаған ресурстарға кіру кезінде пайдаланушының жасын оператор арқылы немесе басқа сенімді әдіспен тексеруді міндеттеу керек.

Үшіншіден, балалардың шектен тыс интернет пайдалануын реттеу мәселесінде Кореяның сабақтары ескерілуі тиіс. Тікелей тыйым салу орнына, Қазақстан да жанама тәсілдер қолдана алады - мысалы, түнгі уақыттарда балаларға онлайн ойын қызметін көрсететін компанияларға қосымша салық салу немесе оларға кәмелетке толмағандарға түнде қызмет ұсынбауды ерікті келісімдер арқылы насихаттау. Сонымен бірге ата-аналарды балалардың экран алдында болу уақытын бақылауға үйрету маңызды.

Төртіншіден, арнайы полиция бөлімшелерін құру. Кореяда киберқауіпсіздік полициясы құрамында балаларға қатысты интернет-қылмыстарды зерттейтін арнайы топтар бар; олар жасырын түрде интернетте балаларды азғырушыларды анықтау, арнайылап операция жүргізу өкілеттігіне ие. Қазақстанда да ІІМ немесе прокуратура құрылымында осындай кішігірім бөлімше ашып, оларға заң жүзінде интернетте «жасырын агент» болып жұмыс істеу мүмкіндігін (мысалы, жасөспірім кейпінде тіркеліп, қылмыскерлерді әшкерелеу үшін) беру туралы ҚПК-ге толықтыру енгізу ойластырылуы мүмкін. Бұл балаларға қатысты ауыр қылмыстардың (педофилия, адам саудасы) алдын алу үшін қажет қадам. Қорыта айтқанда, Оңтүстік Корея үлгісі Қазақстанға техникалық бақылау мен құқық қорғау саласын цифрландыру тұрғысынан үлгі бола алады. Алайда Кореяның қоғамы жоғары бақылау шараларын қабылдауға дайын болғанын, ал біздің жағдайда кез келген шектеу шарасы қоғамдық талқылаудан өтіп, жұмсақ түрде енгізілуі керектігін ескерген жөн.

**Балтық елдерінің тәжірибесі (Латвия, Литва).** Көлемі жағынан шағын болғанымен, бұл елдер Еуропалық Одақ мүшесі ретінде балалардың құқығын цифрлық ортада қорғаудың заманауи үлгілерін іске асырып отыр. Латвияда балаларды интернеттегі зорлық-зомбылықтан және қудалаудан қорғауға бағытталған заңнамалық өзгерістер ерекше назар аударарлық. Мысалы, Латвияның Балалар құқықтарын қорғау туралы заңы мен Қылмыстық заңына толықтырулар енгізіліп, «кибербуллинг» ұғымы заңды түрде бекітілді және интернетте жасырын атпен балаға қорлық көрсеткен тұлғаны анықтау үшін құқық қорғау органдарына провайдерлерден мәлімет талап ету құқығы берілді. Бұрын белгісіз автор тарапынан онлайн қорлау болған жағдайда, жәбірленуші баланың ата-анасы құқықтық шағым түсіре алмайтын, өйткені кінәліні анықтау механизмі жоқ еді. Енді заң бойынша полиция мен сот провайдерден аноним аккаунттың иесін көрсетуін талап етіп, сол дерек арқылы баланы қорлаған адамды жауапқа тарта алады [118].

Бұл өзгеріс Латвиядағы Drossinternets.lv атты қауіпсіз интернет ұйымының бастамасымен үш жыл бойы талқыланып барып жүзеге асты және кибербуллингпен күресте маңызды институционалдық тетік қалыптастырды. Қазақстан үшін де бұл тәжірибе өте өзекті: біздің заңнамада да аноним түрде баланы қорлағаны үшін жауапкершілік бар, бірақ іс жүзінде провайдерлерден мәлімет алу тек ауыр қылмыстық істерде қарастырылған. Сол себепті Латвиядағыдай, әкімшілік құқық бұзушылық немесе жеңіл дәрежедегі қылмыс шеңберінде де қажет болғанда интернет пайдаланушысының жеке деректерін провайдер арқылы анықтау тәртібін енгізу керек. Бұл үшін ҚПК мен «Байланыс туралы» заңға өзгеріс енгізіп, балаға қатысты заңбұзушылықтар кезінде провайдердің лог-файл мәліметтерін құзырлы органдарға беруге міндетін нақтылап көрсету қажет.

Литвада балаларды интернеттің зиянды әсерінен қорғау жүйесі кешенді түрде дамыған. 2010 жылы қабылданған «Немолеттілерді қоғамдық ақпараттың зиянды әсерінен қорғау туралы заң» ақпараттық өнімдерді жас санатына қарай шектеу саясатын бекітті. Бұл заң бойынша балалар психикасына кері әсер ететін, зорлық-зомбылық немесе порноэлементтері бар кез келген контент «зиянды ақпарат» деп танылады және оны кәмелетке толмағандарға қолжетімді етуге тыйым салынады. Литвада интернеттегі порнографиялық материалдарды тарату заңсыз; ондай факті анықталса, құқық қорғау органдары материалды орналасқан серверден өшіртіп тастайды, ал кінәлілер әкімшілік не қылмыстық жазаға тартылады.

Интернетте балаларға зиян контентті шектеу үшін алдын ала ескерту парақтары қолданылады: егер балаға арналмаған веб-сайт ашылса, міндетті түрде «Бұл сайттағы ақпарат Сізге (Сіздің балаңызға) зиянды болуы мүмкін» деген мазмұнда ескерту шығып, одан әрі кіруі шектеледі. Литвада да бірнеше мекемеге онлайн-контентті бақылау өкілеті берілген: Байланыс реттеу қызметі (RRT), Журналист этикасы инспекторының кеңсесі және Нарко/алкогольге қарсы департаменті интернеттегі балаларға зиян контент бойынша шағымдарды қарап, қажет жағдайда сайтты жабу не материалды өшіру жөнінде нұсқау бере алады. Сонымен бірге, «Шварус интернетас» деп

аталатын арнайы интернет-хаттама желісі жұмыс істейді - балалар мен ата-аналар зиянды не заңсыз онлайн-контентті сол желіге шағым етіп хабарлай алады, оны RRT полициямен бірге қарап, тиісті әрекет жасайды. Литва Байланыс реттеу қызметі ата-аналарға арналған ақпараттық портал жүргізіп, онда балалардың қауіпсіз интернет пайдалануы бойынша кеңестер мен ата-ана бақылауы бағдарламаларының тізімін ұсынады. Сондай-ақ бұл орган кітапхана, мектеп, компьютерлік класс сынды балалар баратын қоғамдық орындарға орнатуға арналған фильтрлік бағдарламаларды сынақтан өткізіп, мақұлдайды. Литвада кибербуллинг пен сексуалдық сипаттағы қудалауға қарсы заңнамалық негіз білім беру заңында да бекітілген: жалпы білім беретін мектептер балалардың кез келген зорлық-зомбылықтан, оның ішінде онлайн ортада да, қорғалуын қамтамасыз етуге міндетті [125]. Бұл үшін әр мектеп буллингтің алдын алу жоспарын жасап, педагогтарды оқытуы тиіс.

Балтық елдерінің тәжірибесі Қазақстанға Еуропалық одақ стандарттарына сай келетін бірнеше жаңашыл тетікті көрсетуімен құнды. Біріншіден, хабарлау және жауап қайтару механизмдері. Латвия мен Литвадағыдай, Қазақстанда да балаларға қатысты интернеттегі заңсыз не қауіпті жайттарды жедел хабарлайтын бірыңғай платформа (ыстық желі) және оған лезде әрекет ететін құрылым (мысалы, Ақпарат министрлігі жанынан шағын мониторинг тобы) құру керек. Екіншіден, ата-аналар мен мектептердің рөлін күшейту. Бұл елдерде заң жүзінде ата-анаға балалардың қауіпсіздігі үшін жауапкершілік артылып, мектептерге буллингті алдын алу міндеті қойылған. Қазақстанның «Білім туралы» және «Балалар құқықтары туралы» заңдарына да балалардың интернеттегі қауіпсіздігіне қатысты мектеп пен ата-ана міндеттерін нақтылап енгізу артық болмайды (мәселен, ата-ана «баласының интернеттегі белсенділігін бақылауды жүзеге асыруға ұмтылуға тиіс» деп кеңес түрінде немесе мектеп «кибербуллингтің алдын алу жоспарын жыл сайын қабылдайды» деп норма түрінде бекіту).

Үшіншіден, интернет-компаниялармен ынтымақтастық. Латвия және Литва ЕО-тың «Балалар үшін жақсы интернет» стратегиясын іске асыра отырып, ірі әлеуметтік желілермен меморандумдар жасасқан: зорлық немесе порнографиялық контентті белгілеу, өшіру кезінде сол елдердің уәкілетті органдары компаниялармен тікелей байланыста болады. Қазақстан да осындай ынғайластықты 2022 жылғы заңмен бастап кетті - Facebook, Instagram сынды платформаларға Қазақстандағы өкілдерін тағайындап, арыз-шағымдарға жауап беруін міндеттеді [126]. Алайда Балтық елдерінің ерекшелігі - бұл процесті ашық және құқықтық мемлекет принциптеріне сай атқару. Бізде де компаниялардың өкілдерімен тұрақты кездесулер өткізіп, статистиканы жариялап, проблемалар жайлы қоғамдық есептер әзірлеу керек. Яғни «балаға қауіпсіз онлайн орта» ұлттық стратегиясы қабылданып, онда мемлекет, бизнес және азаматтық қоғам күш біріктіріп жұмыс атқаруы тиіс.

**Қазақстандағы қолданыстағы әкімшілік заңнама мен құқық қолдану практикасын сындарлы саралау.** Жоғарыда талданған шетел тәжірибелері негізінде Қазақстанның қазіргі ахуалына зер салсақ, бірқатар жетістіктермен қатар елеулі олқылықтар бар екені көрінеді. Біріншіден,

нормативтік-құқықтық база қалыптасуда, бірақ әлі де толық емес. 2018 жылы қабылданған «Балалардың денсаулығы мен дамуына залал келтіретін ақпараттан қорғау туралы» заң халықаралық тәжірибеге сай алғашқы қадам болды [92, с. 3]. Аталған заңда ақпарат өнімдерін жастық категорияларға бөлу, зиянды контент ұғымын енгізу, медиа өнімдерді таңбалау сияқты нормалар қарастырылды [92, с. 9]. Дегенмен бұл заң негізінен жалпы декларативтік нормаларға толы және интернеттегі нақты механизмдер (мысалы, сайттарды реттеу, платформа міндеттері) толық қамтылмаған.

2020-2022 жылдары Қазақстан кибербуллингке қарсы кейбір заңнамалық өзгерістер жасады. Атап айтқанда, 2021-2022 жж. Әкімшілік құқық бұзушылық кодексі мен Қылмыстық кодекске толықтырулар енгізіліп, «буллинг» және «кибербуллинг» ұғымдары ресми бекітілді, сондай-ақ телекоммуникация желілерін пайдаланып қорлау, қорқыту, жала жабу әрекеттері үшін жауапкершілік күшейтілді [126]. Мысалы, ҚК 105-бабына (өзін-өзі өлтіруге итермелеу) 2-бөлік қосылып, егер суицидке итермелеу «телекоммуникация желілерін пайдаланып қорқыту немесе кемсіту арқылы» жасалса, ауырлататын мән-жай ретінде қаралады [126]. Сол сияқты, ҚК 131-бабы (қорлау) мен 147-бабы (жеке өмірге қол сұғу) бойынша интернетте аноним түрде жасаған күнә күшейтілген жаза көзделді [118]. Бұл өзгерістер - құптарлық қадам, себебі бұрын «кибербуллинг» деген ұғым мүлде жоқ болатын [126]. Әкімшілік құқық бұзушылық туралы кодекске де 2022 жылы бала құқықтарын қорғау мәселелеріне қатысты бірнеше бап енгізілді: атап айтқанда, «балаға қатыгездік жасау» (127-1-бап) және «баланың заңды өкілдерінің тәрбиелеу жөніндегі міндеттерін орындамауы» (127-баптың 4-бөлігі) нормалары толықтырылып, ата-анасы немесе жауапты адам баланы кибербуллингке ұшыратын жағдайлар үшін де жауапкершілік қарастырылды (ата-ана тәрбие міндетін орындамаса, ескерту немесе айыппұл салынады). Сонымен қатар 2022 жылы «Балалар құқықтары туралы» заңға өзгерістер еніп, 3-бапта балаға қатысты кибербуллингтің жолын кесу мемлекеттің міндеті деп танылды, ал 4-бапта баланың қауіпсіз ақпараттық ортаға құқығы бекітілді. Бұл реформалар Қазақстан заңнамасын белгілі бір дәрежеде халықаралық стандарттарға жақындатты деуге болады [92, с. 15].

Алайда құқық қолдану практикасы әлі де тиімді емес деңгейде қалып отыр. Мысалы, статистикаға сүйенсек, Қазақстанда жасөспірімдер арасындағы кибербуллинг фактілері жылдан жылға өсуде, 11-15 жастағы балалардың 11%-ы интернетте кемінде бір рет буллингке ұшырағанын зерттеулер көрсеткен [92, с. 14]. 2021 жылы балаларға қатысты 80 мыңға жуық кибербуллинг дерегі тіркелгені айтылды [92, с. 2]. Бірақ солардың ішінен қылмыстық жауапкершілікке тартылғандары өте сирек, көп жағдайда іс дәлелдің жеткіліксіздігінен тоқтатылады. Себебі біздің елде әлі күнге дейін балаларға қарсы онлайн-қылмыстарды әшкерелеу және дәлелдеу тетіктері әлсіз. Кибербуллингтің тікелей зардаптарын (дене жарақаты сияқты) дәлелдеу қиын, ал жанама залалды (психологиялық зақым) дәлелдеу үшін арнайы сараптама қажет, ол көбіне жүргізілмейді. Интернеттегі анонимділік те кедергі: прокси-сервер, фейк-аккаунт пайдаланған адамды табу үшін жедел

іс-шаралар керек, ал полицияның ондай технологиялық мүмкіндігі әрдайым бола бермейді. Халықаралық ынтымақтастықтың жеткіліксіздігі тағы бір проблема. Балалар порнографиясы немесе трансұлттық азғындық істерінде күдіктілер шетелдік платформа қолдануы мүмкін (мәселен, жабық шетелдік форумдар). Ондайда біздің органдардың шетелдік әріптестермен дер кезінде ақпарат алмасуы қиындау - Қазақстан Будапешт киберқылмыс конвенциясына қосылмаған, өзара құқықтық көмек келісімдері әр елмен жеке жасалған, оның өзі ұзақ бюрократиялық процеске созылады. Сондықтан талай іс ашылмай қалады немесе созбалаңға салынады. Алдын алу жұмыстарының әлсіздігі де байқалады: ата-аналардың көпшілігі балалардың интернеттегі өмірінен бейхабар, мектептерде киберқауіпсіздік сабақтары жүйелі емес, балалардың өздері де қауіпті тану дағдысына ие емес. Осындай түйткілдерді шешуде жоғарыда қарастырылған шетел тәжірибесі үлкен көмек болар еді.

**Шетелдік үлгілерді Қазақстанға бейімдеу: тікелей қабылдау және ұлттық ерекшелікке сәйкестендіру мәселелері.** Жоғарыда сипатталған әр елдің моделінен туындайтын маңызды сұрақ - олардың қайсысын Қазақстан өзгеріссіз қабылдай алады, ал қайсысы біздің жағдайға бейімдеуді талап етеді? Мұнда ең алдымен ұлттық құқықтық жүйенің ерекшелігі мен қоғамдық ахуалды ескеру қажет. Мысалы, Ұлыбритания мен Еуропаның кей тәжірибелері (платформаларға жалпы міндет жүктеу, көпдеңгейлі регуляторлық бақылау) біздің елде тез нәтиже беруі мүмкін, өйткені Қазақстанның унитарлы жүйесінде орталықтандырылған шешімдер тиімді іске асады. Бізде заң қабылданса, оны орындауды тікелей Үкімет бақылайды, аймақтық деңгейде қосымша келісімдердің қажеті жоқ.

Сондықтан Ұлыбританияның Онлайн қауіпсіздік актісіндегі көптеген талаптарды - әсіресе платформалардың бала қауіпсіздігін қамтамасыз ету міндеттерін - заңға тікелей кіріктіруге болады. Сол сияқты, COPPA тәрізді балалардың дербес деректерін қорғау ережесін де тікелей қабылдау қиын емес (бұл біздің дербес деректер заңнамамызға жаңа бөлім қосу арқылы іске асады). Бұдан бөлек, Литвадағы ескерту парақтары, Латвиядағы анонимді буллингке жауапкершілік тетіктері, Германиядағы жасты тексеру жүйелері - бұлардың құқықтық архитектурасы бізге түсінікті, тіпті кейбірі қолданыста бар (мысалы, 18+ контентті SMS арқылы шектеу кейбір отандық ұялы операторлар порталында бар). Сондықтан бұл элементтерді көп өзгертпей қабылдай береміз. Ал бейімдеуді талап ететін шаралар көбіне мәдени және технологиялық ерекшелікке байланысты. Мәселен, Оңтүстік Кореяның «тәулік мезгіліне қарай ойынға тыйым салу» сияқты қатаң шарасын Қазақстан жағдайында сол күйінде енгізу тиімсіз болуы мүмкін. Бізде де кей ата-аналар балалар түнде ойын ойнамауы керек деп санар, бірақ жалпы қоғам оны «шектен тыс мемлекеттің араласуы» деп қабылдауы ықтимал. Сол себепті ондай шараны тікелей емес, жанама тәсілдермен жүзеге асырған дұрыс (ата-анаға бақылау құралын беру, ойын компанияларымен меморандумдар). Тағы бір мысал - провайдерлер арқылы бүкіл трафикті сүзгілеу. Корея, Қытай сияқты елдерде бұл үкіметтің цензура құралы ретінде

де қолданылатыны белгілі, ал біздің Конституциямыз сөз бостандығына кепіл береді. Демек, зиянды сайттарды бұғаттау керек болса да, оны сот шешімімен және ашық тізімдер арқылы іске асырған жөн; әйтпесе, сөз еркіндігі шектеліп, халықаралық қауымдастық сынына ұшырауымыз мүмкін.

Ұлттық менталитет пен қоғамның дайындық деңгейі де рөл атқарады. Мысалы, Батыс Еуропада ата-аналар балаларын интернетте жеке тұлға ретінде дамуы үшін тым қатты шектемейді, ал Қазақстанда көп ата-ана баланың виртуалды өміріне мүлде көңіл бөлмейді немесе керісінше, гаджетке толық тыйым салып тастайды. Екі жағдайда да шектен шығу бар. Сондықтан шетел тәжірибесін енгізуде біздің ата-аналардың санасын да дайындау қажет - яғни құқықтық норма енгізумен қатар, ауқымды ағарту жұмысын қоса жүргізу керек. Сондай-ақ, инфрақұрылым мүмкіндіктері де есепке алынуға тиіс. Мысалы, Ұлыбритания мен Еуроодақ елдерінде платформаларды бақылау үшін қуатты деректер орталықтары, жасанды интеллект жүйелері қолданылады, олар миллиондаған посттарды сүзгіден өткізе алады.

Қазақстанда мұндай технологияны енгізу үшін уақыт және инвестиция керек. Сондықтан заңмен талап қоя салу аз, оны орындауға отандық техника дайын ба - соны бағамдау керек. Егер белгілі бір талапты бірден орындай алмасақ (айталық, барлық контентке автоматты жас саралағыш еңгізу), онда өтпелі кезең, пилоттық жобалар арқылы келе жатқан абзал.

Қорыта айтқанда, шетелдің озық үлгілерін бейімдеу принципі «қабылдау + бейімдеу» формуласын ұстануы керек: не тиімді және үйлесімді болса, сол өзгертусіз алынады, ал қайсысы біздің құқықтық жүйеге және қоғамдық құндылықтарға тікелей жарамаса, сол Қазақстан жағдайына икемделіп енгізіледі. Бұл ұстанымды сақтай отырып, енді Қазақстанның заңнамасын жетілдіруге қажетті ұсыныстарды құқықтық, институционалдық, процессуалдық және техникалық аспектілер бойынша топтастырып көрейік.

**Заңнамалық (құқықтық) тетіктер бойынша ұсыныстар:** Қазақстанның қолданыстағы заңдарына бірқатар өзгерістер енгізу қажет. Ең әуелі, «Балаларды киберкеңістіктегі қауіп-қатерлерден қорғау туралы» кешенді заң немесе заңнама пакеті қабылдауды қарастыруға болады. Бұл жаңа заң қазіргі 2018 жылғы заңның орнын басып, кеңірек өрісті қамтуы тиіс. Мұнда шетел тәжірибесіндегі сәтті элементтерді біріктіруге болады, атап айтқанда: 1) онлайн-платформалардың балаларды зияннан қорғау міндеттері (заңсыз контентті жедел жою, жастық шектеулерді қолдану, жеке деректерді қорғау қағидаттары) нақты жазылуға тиіс; 2) интернет-провайдерлердің техникалық фильтрлеу және ата-ана бақылауына көмектесу міндеттері көрсетілуі керек; 3) балаларға қатысты онлайн-қылмыстар мен құқықбұзушылықтардың алдын алу шаралары (цифрлық сауаттылықты арттыру, ақпараттық кампаниялар) енгізілуі қажет. Сол заңда тиісті талаптарды орындамаған тараптарға жауапкершілік түрлері де айқындалуы қажет - мысалы, платформа балаға қауіпті жарияланымды уақытында өшірмесе, әкімшілік айыппұл салынатыны жөнінде және соның нақты мөлшері. Бұған қоса, Қазақстан киберқауіпсіздік бойынша халықаралық конвенцияларға қосылуды қарастыруы тиіс (әсіресе, Будапешт конвенциясы)

- бұл қылмыстық процесте шетел серверлерінен дәлел алу, трансшекаралық киберқылмыспен күресу сияқты аспектілерде қолбайлау болып жүрген мәселелерді шешеді.

Екіншіден, Әкімшілік құқық бұзушылық туралы кодекске арнайы баптар енгізуді ұсынамыз. Мысалы: «Кәмелетке толмағандарды зиянды ақпараттан қорғау жөніндегі талаптарды орындамау» деген жаңа бап енгізіп, онда интернет-ресурс иесінің немесе лауазымды адамның балаларға арналған арнайы талаптарды сақтамауы (мысалы, өнімді жас санатына қарай таңбалап ұсынбауы, ересек контентке жас шектеуін қоймауы, баланың жеке дерегін рұқсатсыз жинауы т.б.) үшін айыппұл көздеу керек. Мұндай норма Германияның жастарды медиада қорғау заңдарындағы провайдер жауапкершілігіне ұқсас болады [124]. Сондай-ақ, «Интернет арқылы буллинг жасау» деген құқық бұзушылықты енгізіп, оны жеке тұлғаларға (мысалы, баланы жүйелі түрде әлеуметтік желіде қорлаған ересекке) қолдану жолын қарастыруға болады - бұл ұсақ бұзақылық немесе қорлау бабына сыймайтын, бірақ баланы қорғайтын әкімшілік шара қажет жағдайларда іске асады. Тағы бір бағыт - ата-аналардың міндетін орындамау бойынша қолданыстағы 127-бапты жетілдіру: нақты киберқауіпке ұшыраған баланың ата-анасы тиісті шара қолданбаса, оларға ескерту беріп, қажет болса, белгілі бір курсқа (ата-ана университеті сияқты) жіберуді заңдастыру. Осылайша, әкімшілік құқық бұзушылықтар арқылы профилактикалық ықпал ету күшейеді.

Үшіншіден, Қылмыстық-процессуалдық кодекске өзгерістер. Балаларды интернеттегі қылмыстардан қорғау үшін тек қана құқық бұзушыны жазалау емес, сонымен бірге тиімді тергеу жүргізу, дәлелдеме жинау маңызды. Сондықтан ҚПК-ге кемінде екі жаңалық енгізу ұсынылады: 1) электрондық дәлелдемелермен жұмыс істеу тәртібі. Мысалы, әлеуметтік желідегі хабарламалар, электронды хаттар, сервер логтары сияқты дәлелдерді жинау және сотта пайдалану барысын жеңілдету. ҚПК-де электрондық цифрлық дәлел түсінігін бекітіп, оны жинауды тездететін (тергеушіге сот санкциясынсыз провайдерге сұрау салуға мүмкіндік беру, кейіннен сотқа хабарлау арқылы) ерекше процедура белгілеуге болады. 2) жедел іздестіру шараларына қатысты: балаға қатысты интернет-қылмыстарды анықтау үшін полиция қызметкерлеріне желідегі жасырын әрекеттерге рұқсат беру.

Қазір ондай тактика есірткімен күресте қолданылса (жасырын агент, бақылау сатып алу т.б.), оны кибер ортада да (астыртын чаттарға кіру, жабық топтарға ену) рұқсат ету керек. Бұл өзгеріс арқылы педофилді немесе бала саудагерін интернеттен анықтау жеңілдейді, өйткені полицей өзі «құрбан бала» ретінде көрініп, қылмыскермен байланыс орнатып, бұлтартпас айғақ жинай алады. ҚПК-ге осыны қосқанда, әрине, бала құқығын сақтауға мән берген жөн - ешбір жағдайда нақты балалар мұндай операцияға қатыстырылмауы керек, тек ересек маман өзін бала сияқты көрсетеді деген талап бекітілуге тиіс. Бұдан бөлек, ҚПК-нің халықаралық құқықтық көмек туралы тарауларын да жетілдіру артық емес: шетелдік компаниялардан жедел дерек алу жолдарын жеңілдету, Интерпол, Европол арналары арқылы

сұратулар механизмін регламенттеу секілді жаңалықтар балаға қатысты қылмыстарды тез ашуға сеп болады.

Төртіншіден, «Бала құқықтары туралы» заңға толықтырулар. Бұл негізгі заңда жалпы балалардың құқықтары жазылған, бірақ цифрлық дәуірдің сын-қатерлерін ескеретін нақты нормалар аз. Ұсыныс: заңға жеке тарау қосып, «Баланың цифрлық кеңістіктегі құқықтары мен қауіпсіздігі» деп атауға болады. Сол тарауда: «Әрбір баланың қауіпсіз ақпараттық цифрлық ортаға құқығы бар. Мемлекет баланың осы құқығын қамтамасыз ету үшін шаралар қолданады, соның ішінде: а) балалардың интернетте ақпарат алу еркіндігі мен зиянды ақпараттан қорғалуы арасындағы теңгерімді сақтау үшін заңдар қабылдайды; ә) ата-аналардың балаларды зиянды контент пен кибербуллингтен қорғау жауапкершілігін күшейтеді; б) ақпараттық-коммуникациялық технологиялар саласындағы компаниялардың бала құқықтарын сақтауы үшін қажетті реттеуші талаптар қояды; в) балалардың цифрлық сауаттылығын арттыру бойынша бағдарламаларды жүзеге асырады; г) құқық қорғау органдарының киберкеңістікте балалардың құқықтарын қорғау қызметін қамтамасыз етеді» деген үлгі нормалар енгізуге болады.

Сондай-ақ, осы заңда ата-аналардың міндеттері бөліміне «баланың интернетті қауіпсіз пайдалануы үшін қажетті бақылауды жүзеге асыруға және оң бағытта бағдар көрсетуге тиіс» деген тәрізді сөйлем қосып, ата-аналардың цифрлық тәрбиеге жауапты екенін заңнамалық тұрғыда бекітуге болады. Бұл, әрине, ата-ананы жазалау үшін емес, олардың санасына мемлекет тарапынан берілген бағдар ретінде маңызды. Мектептің рөлі де көрсетілуі керек: заңда «білім беру ұйымдары балаларды ақпараттық қауіп-қатерден қорғау шараларын іске асырады» деп принцип жарияланып, нақты тетіктері білім туралы және басқа нормативтік актілерде көрініс табады. Егер қажет деп тапсақ, «Интернет-платформалардың міндеттері» жайлы да қысқаша осы заңда баяндалуы мүмкін - мысалы, «интернет кеңістікте қызметін іске асыратын ұйымдар (соның ішінде әлеуметтік желілер, мессенджерлер, форумдар) Қазақстан Республикасының заңнамасында балаларды қорғау бойынша белгіленген талаптарды сақтауға міндетті, бұзған жағдайда жауаптылыққа тартылады» деп бір сөйлеммен бекіту. Бұл норманың символдық мәні бар, ал нақты міндеттердің тізімі арнайы заңдар мен кодекстерде келтіріледі.

Институционалдық тетіктер бойынша ұсыныстар: Заңнамалық өзгерістерді іске асыру үшін институционалдық құрылымдарды да нығайту керек. Біріншіден, арнайы уәкілетті орган белгілеу немесе құру. Қазіргі кезде Қазақстанда Балалардың құқықтары жөніндегі уәкіл (омбудсман) институты бар, бірақ оның құзыреті кеңес беру, қоғамдық бақылау деңгейінде. Ал интернеттегі балалар қауіпсіздігін нақты бақылау үшін атқарушы билік құрамында маманданған құрылым қажет. Ұсыныс: Ақпарат және қоғамдық даму министрлігі жанынан «Балалардың ақпараттық қауіпсіздігі» департаментін құру немесе Телекоммуникация комитетінің аясында ерекше бөлімше ашу. Бұл органның міндеті - интернеттегі зиянды контентті мониторингтеу, әлеуметтік желілердегі буллинг фактілерін қадағалау,

платформалармен байланыс орнату, провайдерлердің сүзгі қолдануын тексеру және т.б. болмақ. Мұндай орган Ұлыбританиядағы Ofcom-ның баламасы ретінде әрекет етіп, заңдардың орындалуына күнделікті бақылау жүргізеді.

Екіншіден, ішкі істер органдарының құрылымында кибербуллинг пен балаларға қатысты интернет-қылмыстарға маманданған бөлім құру. Жоғарыда айтылғандай, полиция ішінде (мәселен, Киберқылмысқа қарсы күрес басқармасы құрамында) шағын топ құрып, оларға техникалық жабдықтар (интернетте жасырын жұмыс істеуге арналған бағдарлама, трекинг жүйелері) беру қажет. Бұл бөлімше тұрақты түрде даркнет, жабық топтар сияқты орындарды шолып, бала порнографиясы айналымын анықтайтын, балаларды азғырушыларды әшкерелейтін проактивті жұмыс атқарар еді. Үшіншіден, қауырт желілер мен сенім телефондарын институционализациялау. Қазір білім басқармаларының жанында «111» ұлттық сенім телефоны істейді, ол негізінен тұрмыстық зорлық және бала құқы бұзылуына қатысты кеңес береді. Осы желінің қызметіне киберкеңістіктегі зорлық мәселесін қосып, операторларды арнайы оқытып, әр мектепке, әр ата-анаға бұл нөмірді насихаттау керек. Әрі бұл желі полиция, омбудсмен, психологтермен тікелей байланысты жұмыс істеп, балаға онлайн зорлық көрсетілсе, тез арада кешенді көмек ұсынуы тиіс. Литвадағы RRT немесе Ұлыбританиядағы CEOP үлгісінде, Қазақстанда да бір терезе қағидатымен балаға онлайн қатер төнгенін хабарлайтын орын болуы шарт - ол үшін 111 желісін күшейту жеткілікті. Төртіншіден, мектептер мен ата-аналар қауымдастығы деңгейінде институттар. Әр мектепте киберқауіпсіздікке жауапты бір маман (мүмкін, информатика мұғалімі ішінен) тағайындалуы немесе әлеуметтік педагог соған жауапты болып бекітілуі керек. Ол тұлға балалар арасында кибербуллинг, интернет-қауіп жағдайларын байқаса, дереу мектеп әкімшілігі, ата-ана және қажет болса полицияға хабарлайтын жүйе қалыптастырсын. Балалардың өздерін де қатыстыру үшін мектептерде «цифрлық еріктілер» клубтарын құруға болады - белсенді, IT жағынан сауатты оқушылар кішілерге интернетті қауіпсіз пайдалану бойынша тренингтер өткізсін, қауіпті контентті анықтаса, ұстаздарына жеткізсін. Бұл өзара қолдау орта қалыптастырады. Ал ата-аналарды жұмылдыру үшін әрбір ата-ана комитетінің отырысында жылына кемінде бір рет «онлайндағы бала қауіпсіздігі» мәселесі талқыланып, ата-аналарға практикалық кеңес беру жолға қойылуы тиіс. Мұны Білім министрлігі деңгейінде ұсыным ретінде таратқан жөн.

**Процессуалдық (ұйымдастыру және өзара іс-қимыл) тетіктері бойынша ұсыныстар:** Балаларды киберқауіптен қорғау тек заң қабылдап, орган құрумен шектелмейді, ең бастысы - түрлі субъектілердің үйлесімді әрекеттесуін қамтамасыз ету. Осы орайда ата-ана - мектеп - интернет-платформа - полиция арасында тиімді ықпалдастық механизмін орнату керек.

Біріншіден, ақпарат алмасу және жауап қайтару алгоритмін рәсімдеу. Мысалы, мектеп оқушысы интернетте буллингке ұшырағанын анықтаса, мұғалім немесе ата-ана дереу мектеп әкімшілігі мен полицияға хабарлауы шарт; полиция 24 сағат ішінде провайдерден буллинг жасаған адамның IP-

мекенжайын сұратып, жеке басын анықтау жұмысын бастауға тиіс; ал әлеуметтік желі әкімшілігі жәбірлеушінің аккаунтын уақытша тоқтатып, тексеріс жүріп жатқанын ескерткені жөн. Осындай тізбекті әрекеттерді регламенттейтін инструкциялар қажет. Оны Үкімет қаулысымен бекітуге болады немесе бірнеше министрліктің бірлескен бұйрығы түрінде (ІІМ, Білім мин., Ақпарат мин. т.б.) шығаруға болады. Екіншіден, уақытылы әрекет ету.

Кибербуллинг немесе интернеттегі зорлық мәселесінде кешігудің зардабы үлкен. Сондықтан әр органның әрекет мерзімі қысқа болуы тиіс. Қазақстан 2022 жылғы заңда әлеуметтік желілерге 3 күн ішінде шара қолдануды міндеттеді [92, с. 2]. Бұл - жақсы бастама, бірақ 3 күн кейде тым ұзақ болуы мүмкін (мысалы, балаға суицидтік қысым көрсетілсе). Ұсыныс: әлеуметтік желіге хабар түскеннен соң 24 сағат ішінде ықпал ету талабын қою (Ұлыбритания мен ЕО елдерінде 24 сағат нормасы кең таралған [128]. Ал полицияға келсек, кибербуллинг бойынша арызды тіркеуден бастап шешім қабылдауға дейін 7 жұмыс күнін жеткілікті деп бекітуге болады (қазіргі тәжірибеде бұл бірнеше аптаға созылып кетеді). Үшіншіден, мамандану және оқыту. Мектеп мұғалімдеріне жыл сайын балалардың интернеттегі мінез-құлқы, қауіптері бойынша біліктілікті арттыру курстарын өткізу керек (цифрлық педагогика элементтерімен). Полиция қызметкерлеріне де киберпсихология, балалармен жұмыс ерекшеліктері жөнінде семинарлар керек - өйткені интернет-қылмысқа арнайы маман дайындалмаған аудандарда учаскелік инспекторлар не кәмелетке толмағандар ісі жөніндегі инспекторлар айналысуы мүмкін, ал олар заман ағымына сәйкес компетенциясын жетілдіріп отыруы шарт. Төртіншіден, халықаралық әріптестік.

Процессуалдық деңгейде Қазақстан шетелдік ұйымдар және IT-компаниялармен тікелей байланыс арналарын орнатуы керек. Мысалы, INHOPE (балалар порнографиясына қарсы халықаралық желі) ұйымына мүше болу - бұл біздің ұлттық «ыстық желімізді» халықаралық базаға қосады, сөйтіп шетелде орналасқан заңсыз контент туралы дереу шетел әріптестеріне хабар беріп, жоюға қол жеткізе аламыз. Сол сияқты, WePROTECT Global Alliance (балаларға жыныстық зорлыққа қарсы жаһандық альянс) жұмысына белсенді араласу ұсынылады - онда озық тәжірибелер алмасып, жаңа трендтерді біліп отыруға болады [92, с. 3]. Ішкі істер министрлігі шеңберінде ірі IT-компаниялардың қауіпсіздік бөлімдерімен (Facebook, Google, TikTok және т.б.) тікелей байланыс орнататын офицер тағайындау да артық емес. Бұл офицер сұраныстардың орындалуын жеделдетуге (арнайы электронды платформа арқылы тікелей жіберуге) жауапты болады.

**Техникалық тетіктер бойынша ұсыныстар:** Цифрлық заманда құқықтық нормалардың жүзеге асуы көбіне техникалық мүмкіндіктерге тәуелді. Сондықтан балаларды қорғау үшін заманауи техникалық шешімдерді енгізу - заңнамалық бастамалармен қатар жүруге тиіс шаруа. Біріншіден, жасанды интеллект және машиналық оқыту технологияларын қолдану. Мәселен, әлеуметтік желілерде балаға қатысты зорлық-зомбылық не буллинг мазмұнын AI арқылы автоматты анықтайтын жүйелер бар (кей

компанияларда қолданылады). Қазақстан осы бағытта отандық IT-секторды ынталандыруы керек: гранттар беріп, университеттерде зерттеу жүргізіп, қазақ және орыс тілдерінде балаға қауіп төндіретін сөз, бейне, аудио белгілерін танып үйренетін алгоритмдер әзірлеуді жолға қою қажет. Кейін осындай алгоритмдерді ұлттық қауіпсіздік жүйесіне немесе платформа API-ларына қосып, мониторинг процесін шапшаңдатуға болады. Екіншіден, жас ерекшелігін тексерудің цифрлық құралдары. Қазірдің өзінде eGovMobil қосымшасы немесе SMS арқылы ЖСН енгізіп, азамат жасын растау технологиясы бар. Мұны барлық онлайн қызметке ортақ пайдалануға мүмкіндік қарастырған жөн. Мысалы, болашақта Қазақстанда кез келген жаңа әлеуметтік желіге тіркелген адам eGov арқылы өзінің кәмелеттік жасқа толғанын растауы міндетті болуы мүмкін (мұны бірден енгізу қиын, бірақ болашақ мақсат ретінде атап өткен маңызды). Литва 14 жастан бастап балаларға электронды қолтаңба беріп, банкте шот ашқанда немесе басқа онлайн сервисте жасын растауға үйретіп отыр [125]. Біз де мектеп жасынан бастап әр балаға eGov мүмкіндіктерін ашып, жеке электронды аккаунт арқылы жүріс-тұрысын (цифрлық профиль) бақылауды дамытуымыз керек - бұл бір жағынан банк, мемлекеттік қызметтерге қолжетімділігін берсе, екінші жағынан жасы жетпейтін нәрсеге кіруін шектейді. Үшіншіден, ата-ана бақылауы бағдарламаларын қазақ және орыс тілдерінде бейімдеу.

Қазіргі таңда нарықта Qustodio, NetNanny сияқты көп бағдарламалар бар, бірақ ата-аналар оларды біле бермейді әрі тілдік тосқауыл болуы мүмкін. Мемлекеттік органдардың қолдауымен осындай бағдарламаларды жерсіндіріп (локализациялап), нұсқаулықтарын ұсынып, мүмкін тегін лицензия тарату шараларын ойластырған жөн. Бұл әсіресе тұрмысы төмен отбасылар мен ауылдық жердегі ата-аналарға көмектеседі. Төртіншіден, контентті фильтрациялау және шектеу құралдарын провайдер деңгейінде орнату. Мысалы, Ұлыбританияда OpenDNS негізінде немесе өзге де DPI (Deep Packet Inspection) технологиясымен істейтін сүзгілер бар. Қазақстандық провайдерлерге де балаларға қауіпті кілт сөздерді (порнография, есірткі, экстремизм, суицид т.б.) анықтап, автоматты сүзетін жүйелерді желіге енгізуді міндеттеу керек. Бұл техникалық шешім заңсыз контентті көп жағдайда бұғаттай алады, алайда оны асыра қолданудан сақ болу маңызды (кейде пайдалы ақпарат та жабылып қалмауын қадағалау, яғни «overblocking» болдырмау маңызды [124]. Бесіншіден, цифрлық сауаттылықты арттыру үшін геймификация және интерактивті құралдар.

Балаларға құрғақ сабақ өткеннен гөрі, арнайы жасалған ойын-қосымшалар арқылы интернеттегі қауіпті жағдайларды таныту тиімді. Мысалы, киберқауіпсіздік бойынша викториналар, сценарийлік ойындар (quest) құрастыруға болады - оларды білім беру платформаларына енгізіп, оқушыларға жыл сайын өткізіп отырса, естерінде жақсы сақталады. Сонымен қатар, балалар үшін қауіпсіз мазмұнның балама платформаларын көбейту қажет. Мысалы, қазіргі кезде Балапан арнасының контенті YouTube-та да жүреді, бірақ онда ұсынылған бейнелердің жанында басқа қауіпті бейнелер шығуы мүмкін. Сондықтан ұлттық «Balapan Play» сияқты балаларға арналған

видеохостинг жасап, онда тек тексерілген, пайдалы, көңілді контент орналастырып, балаларды соған тарту керек. Мемлекет осындай бастамаларға грант бөліп, отандық IT мамандар мен анимация студияларын қызықтыра алады. Мақсат - балалар бос уақытын бақылаусыз YouTube-та өткізбей, қауіпсіз балама ортада өткізуі.

Қорытындылай келе, Қазақстан заңнамасын жетілдіру үшін шетелдік озық үлгілерді бейімдеу - көпқырлы үдеріс. Біз АҚШ-тың деректерді қорғау мен құқық қолдану тәжірибесінен, Ұлыбританияның жан-жақты реттеуші модельдерінен, Германияның нақты техникалық стандарттарынан, Оңтүстік Кореяның қатаң бақылау тәсілдерінен, Балтық елдерінің үйлесімді және баланың мүддесін бірінші орынға қоятын тәсілдерінен үйрене отырып, өзіміздің ұлттық жүйемізге ең тиімді тетіктерді енгізе аламыз. Бұл өзгерістерді заңнамалық, институционалдық, процедуралық және техникалық бағыттарда үйлестіре отырып іске асыру - балалардың цифрлық құқықтарын қорғауды жаңа деңгейге шығарады. Ең бастысы - ұсыныстардың бәрі шынайы және дәлелдерге сүйенген болуы тиіс, себебі ойдан шығарылған немесе шектен тыс шаралар кері әсер беруі мүмкін [126].

Сондықтан әр қадамды халықаралық стандарттар аясында негіздеп, мүдделі тараптардың (балалардың өзі, ата-ана, ұстаздар, IT секторы, құқық қорғаушылар) пікірін ескеріп жүзеге асыру маңызды. Жасөспірімдердің қауіпсіздігі - ел болашағына салынатын инвестиция, ал оны қамтамасыз ету - құқықтық мемлекеттің борышы. Ұсынылған модельдік өзгерістер (ӘҚБтК, ҚПК баптарының үлгілері мен «Бала құқықтары туралы» заңға толықтырулар) докторлық диссертацияның келесі бөлімінде нақтылай беріледі деп күтілуде, олар жүзеге асса, Қазақстанның балаларды киберкеңістіктегі қорғау жүйесі халықаралық талаптарға сай жаңғырып, ұлттық ерекшеліктерді ескерген тиімді механизмдермен толықпақ [92,3]. Бұл шаралар заңнамалық тұрғыдан бекітіліп, тиісті институттармен қамтамасыз етілгенде ғана бала құқықтары шынайы қорғалып, қауіпсіз цифрлық қоғам қалыптасады деп қорытамыз.

# 4 КИБЕР ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРҒА ҚАТЫСТЫ ӘКІМШІЛІК НОРМАТИВТІК БАЗАНЫ ЖЕТІЛДІРУ ПЕРСПЕКТИВАЛАРЫ

## 4.1 Әкімшілік-құқықтық нормаларды оңтайландыру бағыттары

Әкімшілік-құқықтық нормаларды кибер құқық бұзушылықтар тұрғысынан талдау кезінде, ең алдымен қолданыстағы нормативтік-құқықтық базаға шолу қажет. ҚР Әкімшілік құқық бұзушылық туралы кодексінің 65-бабы бойынша әкімшілік қылмыс жасаған кезде он алтыдан он сегізге дейінгі жас аралығындағы азаматтар кәмелетке толмағандар қатарында қарастырылады [78].

Яғни 14-15 жас аралығындағы балалар қазіргі заң бойынша әкімшілік жауапкершілікке тартылмайды. Бұл жасөспірімдердің әкімшілік құқық бұзушылыққа қатысу мүмкіндігін заң тұрғысынан шектейді, алайда олардың сандық технологияларды қолдану аясында пайда болған құқық бұзушылықтарымен күрес факторларын тереңірек қарастыруды талап етеді.

Мысалы, интернет желісіне заңсыз кіру жағдайлары үшін ӘҚБтК-де жеке норма жоқ екені айтылған болатын, алайда мұндай әрекет ҚР «Ақпараттандыру туралы» заңнамасын бұзу ретінде қарастырылып, 641-бап аясында жауапкершілікке тартылуы мүмкін. Бұл бап бойынша жеке тұлғаларға 50 айлық есептік көрсеткіштен (АЕК) бастап айыппұл салу көзделген, яғни ақпараттық жүйелерге рұқсатсыз кіргені үшін қомақты әкімшілік жаза қарастырылған. Дегенмен, жекелеген жағдайларда (мысалы, кәмелетке толмағандардың келтірілген материалдық немесе моральдық зияны бойынша) жауапкершілік шекарасы белгісіз қалып отыр.

Заңнаманың «Бала құқықтары туралы» заңы да балалардың ақпараттық қауіпсіздігіне ерекше көңіл аударады. Аталған заңда мемлекеттің міндеттерінің бірі балаларды денсаулығына зиянды ақпараттан қорғауды қамтамасыз ету екені нақты көрсетілген. Нақтырақ айтқанда, 39-баптың 1-тармағында балалар үшін порнографияны, зорлық-зомбылықты насихаттайтын және рухани дамуына зиян келтіретін ақпарат өнімдерін таратуға қатаң тыйым салынған. Яғни елімізде балаларды киберкеңістіктегі зиянды мазмұннан қорғау тетіктері заңнамалық деңгейде бар, алайда олардың жүзеге асуы мен әкімшілік-құқықтық реттелуі жеткіліксіз. Сонымен қатар, 11-бапта әрбір баланың жасына сай ақпарат алу құқығы мойындалған, бірақ бұл құқықты тиімді іске асыру үшін ата-ана мен мектеп тарапынан ақпараттық әдептілік пен қауіпсіздікті үйрету шаралары жүйелі түрде жүргізілуі тиіс. Мысалы, Қызылорда облысында өткен кеңейтілген мәжілісте айтылғандай, қазіргі интернет дәуірінде жастар негізінен әлеуметтік желілер арқылы тәрбиеленіп жатқандықтан, ата-ана мен ұстаздар қоғамдастығы бірлесе әрекет етуі керек екені атап өтілді. Осы көзқарастар қазіргі заңнамаға тікелей ықпал етіп, мектеп бағдарламасына цифрлық сауаттылық пәндерін енгізу, ата-ана ақпараттық жауапкершілігін арттыру сияқты ұсыныстарды негіздеуге сеп болады. Қолданыстағы заңнаманың кемшіліктері мен қайшылықтарына тоқталатын болсақ, ең алдымен кәмелетке толмағандардың

әкімшілік жауапкершілік шектеулеріне назар аудару қажет. Жоғарыда айтылғандай, ӘҚБтК-де әкімшілік жауапкершілік жасы 16 жасқа белгіленген [78].

Бұл ретте, 14-15 жас аралығындағы балаларды құқықтық реттеу алаңынан тыс қалдырады, алайда практикада дәл осы жасқа толмаған жасөспірімдердің де интернет-алаяқтық, кибербуллинг сияқты құқық бұзушылықтарға қатысу фактілері кездеседі. Заң талаптарына қайшы түрде, кейбір зерттеулер мен практика көрсеткендей, 14 жастан асқан балалар құқық бұзушылықты (соның ішінде кибер құқық бұзушылықты) жасаған кезде оларды белгілі жағдайда әкімшілік жауапқа тарту қажеттігі туындайды. Бұл мәселе қылмыстық-құқықтық жүйеде де қарастырылып, 14-тен асқан балалар үшін жауапкершілік шектері белгіленгені белгілі. Сондықтан ӘҚБтК-ге қылмыстық емес сипаттағы құқық бұзушылықтарда да 14 жас шегін қарастыру мәселесі күн тәртібінде тұр. Анығында, осы сызықты төмен түсіру кәмелетке толмағандар үшін арнайы әкімшілік шараларды қолдануға жағдай жасайды. Сонымен бірге, қазіргі кодекс баптарының өзара қайшылығы да байқалады. Мысалы, 127-бап бойынша ата-ананың тәрбиелік міндеттерін орындамауы әкімшілік жазаны көздейді, ал 442-бапта кәмелетке толмағандардың түнгі уақытта заңды өкілдерінің қадағалауынсыз серуендеп жүруі айыппұлмен немесе қамаумен жазаланады. Бұл баптар бір жағынан ата-ана бақылауын күшейткенмен, екінші жағынан киберконтент мәселесіне қатысты нақтыланбаған. Мысалы, ұялы телефон арқылы білім процесінде жаман қылықтар жасау немесе әлеуметтік желілерде кез келген басқа заңсыз әрекет жасаған балаларға қатысты қандай әкімшілік норма қолданылатыны заңнамада мүлде көрсетілмеген. Осыны есепке ала отырып, қазіргі нормативтік базаны цифрлық саланың динамикасына сай жаңғырту қажеттігі айқын. Цифрлық дәлелдемелерді жинау, тіркеу және сараптау механизмдері де жетілдіруді қажет етеді. Қазіргі кезде сандық мәліметтерді сот-сараптамалық тұрғыда пайдалану қылмыстық процесте қарастырылса да, әкімшілік іс жүргізуде оларды рәсімдеу жөнінде толық анықтамалар жоқ.

Мысалы, телефондағы чат жазбалары, әлеуметтік желідегі хабарламалар, сайттар тарихы секілді ақпараттарды әкімшілік тергеу барысында жинау үшін арнайы алгоритмдер мен мамандандырылған құралдар қолданылады. Алайда осы бағыттағы мамандықтар саны шектеулі, ал дәлелдемені жинау тәртібі әлі де нақты регламенттелмеген. Ғылыми ортада цифрлық құқық аймағындағы дәлелділік мәселесіне келесідей көңіл бөлінеді: электрондық құжат айналымы мен цифрлық коммуникацияларды криминалистикалық сараптау бұрын соңды болмаған деңгейде қажетті болып отыр. Осы тұрғыда заңнамада электрондық деректерді сақтап, оларды соттық сараптамаға ұсыну үшін процессуалдық кепілдіктерді күшейту ұсынылады. Қазіргі уақытта цифрлық дәлелді сотқа дейінгі және сот органдарында қолдану Әкімшілік процестік кодекстің 76-бабы [129] және Қылмыстық процестік кодекстің [79] 65-бабы аясында қарастырылса да, әкімшілік іс бойынша өндіріс жүргізуде дәлелдемелердің сенімділігі мен деректердің бұрмалануын болдырмау үшін

нақты регламент жоқ. Сондықтан киберқылмысқа жататын әкімшілік құқық бұзушылықтар бойынша іс жүргізу тәртібін жетілдіру - маңызды бағыт.

Жасөспірімдерге қатысты әкімшілік жауапкершілік шектерін қайта қарау мәселесіне де жеке тоқталу қажет. Қазіргі таңда кәмелетке толмағандарға әкімшілік айыппұлдар мөлшері, арнайы құқығынан айыру мерзімі секілді жеңілдету шаралары қолданылатыны заңда көрініс тапқан. Мысалы, кәмелетке толмағандарға салынатын айыппұл мөлшері 10 АЕК-тен аспайды, ал аталған тұлғалардың айыппұл төлеуге жарамды мүлкі жоқ болса, айыппұл ата-анасына салынады. Шектеулі құқықтардан айыру ең көбі бір жылға дейінгі мерзімге белгіленеді. Дегенмен, жасөспірімдердің Кибер құқық бұзушылықтарындағы кінәсін айқындау кезінде жаппай жеңілдетулер қолдану әрдайым әділетті бола бермейді. Әсіресе әлеуметтік желілердегі алаяқтық немесе кибершабуыл секілді жаңа түрдегі әкімшілік құқық бұзушылықтарда жасөспірімнің ниеті мен мотивін есепке алу қиын.

Сондықтан кейбір авторлық пікірлер бойынша, атқарымдық процеске қарсы емес түрде жасалған әрекеттерді кәмелетке толмағандарда қатаң тергеу керек, ал асыра сілтеушілік әрекеттерге (мысалы, көп рет айыппұл салудан аулақ болу) аздап жұмсарту қажет. Осыған орай, кейбір зерттеушілер 14 жастан бастап әкімшілік жауапкершілікті енгізуді және жасөспірімдерге қылмыстық емес тәртіпте нақты тиісті шараларды қолдануды ұсынады. Бұл баланың жеке ерекшеліктерін ескере отырып шешім қабылдауға мүмкіндік береді. Ата-аналар мен мектептердің құқықтық міндеттерін кеңейту де маңызды қажеттілік ретінде қарастырылуда. Қазіргі заңдар бойынша ата-ананың немесе оларды алмастыратын тұлғаның баланы тәрбиелеу, қорғау міндеттері белгіленсе де, киберсаладағы жағдайлар ескерілмеген. Мысалы, ата-аналар отбасында балаларын интернеттік әрекеттерінен тыс қалдырмау, балалардың цифрлық бейінділік бағдарламалары мен құрылғыларын бақылау қажет екені жайлы нақты жауапкершілік кепілдігі жоқ. Ата-аналарға қатысты арнайы өңделген әкімшілік жаза жоқ болғандықтан, туған-туысқа сабырлылықпен қарап отыру шешімін қолдану тәжірибеге тән емес.

Дегенмен, кеңестік түсінікте «ата-ана жауапты» деп қарастырғандай, цифрлық білім беру мен бақылауды ата-ана міндетіне қосу заң жүзінде жүзеге асырылуы мүмкін. Мысалы, ӘҚБтК-ге ата-ананың кәмелетке толмағандарының онлайн қауіпсіздігін қамтамасыз етпеуі үшін әкімшілік санкцияны қарастыратын бап енгізуге болады. Осыған ұқсас халықаралық тәжірибеде ата-аналарға балаларын әлеуметтік желілерде бақылау қажеттігі туралы міндеттер салынады. Қазақстанда да осы қағиданы бекітуді көздейтін ұсыныстар бар. Мектептердің заңдық міндеттерін кеңейту алдыңғы нормативтермен бірге қолданыс табуы тиіс. Жоғарыда айтылғандай, қазіргі ӘҚБтК 409-бабының 7-2-бөлігінде [78] білім беру ұйымдарының интернет қауіпсіздігін қамтамасыз етпеуі үшін әкімшілік жаза қарастырылған. Атырау прокуратурасының дерегінше, 16 мемлекеттік және 1 жеке мектепте тыйым салынған интернет-контентке қолжеткізу оқиғасы анықталып, жауапты тұлғалар әкімшілік жауапкершілікке тартылды. Бұл норма мектеп басшыларына және техникалық қызметкерлеріне қауіпсіздік құралдарын

орнатпау салдарынан айыппұл салынатынын көрсетеді. Әлі де болса білім беру заңнамасында мектептерді цифрлық қауіпсіздік бойынша ұлттық стандарттарға сай келетін құрылғылармен қамтамасыз ету міндеттемесі жоқ.

Осыны ескере отырып, жаңа жобаларда мектептерге интернетке құрылғы арқылы бақылау, цифрлық тәрбие сабақтарын енгізу міндеттемелерін жүктеу ұсынылуда. Сондай-ақ ата-аналар мен ұстаздардың бірлесе отырып баланы цифрлық әлемдегі қауіптерден хабардар етуі заңда бұдан былай міндетті шаралар қатарына енгізілуі керек. Мысалы, ата-ананың баланы қауіпсіз интернет қолданысы туралы ақпараттандыру құзыреті ӘҚБтК баптарына қосымша бөлім ретінде енгізіле алады. Құқық қорғау органдары, Білім және ғылым министрлігі мен білім мекемелері арасындағы ведомствоаралық координацияны күшейту де маңызды. Бүгінде «Бақытты және қауіпсіз балалық шақ» жобасы аясында прокуратура, полиция, қамқоршылық, әлеуметтік қорғау, денсаулық сақтау, психологиялық және үкіметтік емес салалар бірлесе жұмыс істейді. Атырау облысында прокуратура мен полиция демеушілігімен мобильді топтар құрылып, олар тұрмысы төмен 50-ден астам отбасында жұмыс істеп, балаларға әлеуметтік көмек көрсету және құқық бұзушылықтың алдын алу шараларын жүзеге асыруда. Мұндай кешенді тәсіл білім беру және құқық қорғау салалары арасындағы тәжірибе алмасуға ықпал етеді. Әрине, ведомствоаралық ынтымақтастықты одан әрі тереңдету үшін арнайы іс-шаралар жоспарын бекіту, деректерді бөлісу тәртібін реттеу қажет.

Мысалы, мектептер мен полиция арасында төтенше жағдайлар туралы жылдам хабар алмасу жүйесін құру, ішкі істер органдарының жедел желісі мектеп директорлары үшін қолжетімді ету сияқты практикалар енгізілсе, құқық қорғау жүйесінің тиімділігі артады. Қазіргі таңда өңірлік координация кеңестерінің отырыстары жиі өткізіліп, кең ауқымды ұсынымдар әзірленіп келеді, бұл оң үрдіс екенін көрсетеді. Әкімшілік практикадан алынған мысалдар да жоғарыда аталған концепцияларды нақтылай түседі. Мәселен, Атырау облысының прокуратурасы жүргізген тексерісте 5 мектеп директоры қараусыз қалған оқушылардың ұрлық, төбелес секілді құқық бұзушылықтарын жасырып қалды деген айыппен ӘҚБтК-нің 127-1-бабы бойынша әкімшілік жауапкершілікке тартылды [78]. Сондай-ақ, жастардың интернеттегі орынсыз қолжетімділігі анықталған жағдайда 16 мемлекеттік және 1 жекеменшік мектеп әкімшілік салынған интернет-контентті жаппау фактісі бойынша 409-баптың 7-2-бөлімімен жауапқа тартылды. Бұл оқиғалар мектеп басшылығының цифрлық тәртіпті қамтамасыз етуден қателік жібергенін көрсетеді. Сонымен қатар, Атырау қаласында мобилді топтар баланы қате тәрбиелеу дерегі бойынша 127-баптың 3-бөлігіне (тәрбиелік міндеттерді орындамау) сәйкес ата-аналарға әкімшілік хаттама толтырды.

Олардың бірінде оқушы қаңқылдаған күйде көшеде жүгіріп жүргені анықталып, ата-ана жауапкершіліксіз қалғаны белгілі болды. Бұл мысалдар мемлекеттік органдар тарапынан кәмелетке толмағандарды қорғаудың үздіксіз жүргізіліп жатқанын және заң бұзушылықтарға жедел араласудың қажеттігін көрсетеді. Сонымен қатар, әртүрлі қызметтердің әрекеті өз нәтижесін бере бастағаны байқалады: құқық қорғау органдары, ұстаздар мен

ата-аналардың серіктестігі мектепалды алдын алу жұмыстарын күшейтіп, жасөспірімдердің құқық бұзушылық ықтималдығын төмендетуге үлес қосуда.

ӘҚБтК-ге енгізілуі мүмкін нақты баптарды қарастырсақ, алдымен баланы интернеттегі зиянды ақпараттан қорғауды нақтылайтын түзетулер ұсынамыз. Мысалы, «Балаларға арналған зиянды ақпаратты тарату» атты жаңа бап енгізуге болады: «Әкімшілік құқық бұзушылық - балалардың денсаулығы мен рухани дамуына зиянды порно немесе зорлық-зомбылықты насихаттайтын мазмұнды ақпарат құралдарында, интернет желісінде көрсету немесе тарату болып табылады. Мұндай әрекетке әкімшілік айыппұл 50 АЕК пен 200 АЕК аралығында; егер кінәлі тұлға кәмелетке толмағандар болса, жаза ата-анасына салынады» деп нақтылай жазуға болады. Бұл бап балаларға зиянды материалдарды ұсынған адамды жазалайды және қазіргі заңың жалпы тыйымдарымен сәйкес келеді. Сонымен қатар, «Ата-ананың балаларын қауіпсіз интернет қолдануына бақыламауы» бабы ұсынылуы мүмкін: «Кәмелетке толмаған адамның ата-анасы немесе заңды өкілі балаларын интернетке кіру кезінде ақпараттық қауіпсіздік бойынша қажетті шараларды қолданбаған жағдайда, оған он АЕК-ке дейін айыппұл салынады». Бұл түзету ата-ананың жаңа техникалық шарттағы міндеттемесін заңда бекітеді. Екінші жағынан, мектептер үшін арнайы норма қарастыруға болады.

Мысалы, ӘҚБтК-нің білім беру бағытына арналған тарауына «Білім беру ұйымдарының компьютерлік желілерін балаларға зиянды контентке жол бермей конфигурацияламауы» туралы бап енгізілсе, ол мектептерді цифрлық қауіпсіздік талаптарын орындауға міндеттейді және бұзған жағдайда әкімшілік жазаны қолдануға мүмкіндік береді. Жалпы, ұсыныстарымыздың түйіні - нормативтік базаны жасөспірімдердің цифрлық белсенділігіне сай жаңарту. Егер әкімшілік заңнамада дәл қазіргі заман талаптарын анық көрсететін бірқатар баптар ұсынылса, сот-мамандандырылған мекемелер мен әкімшілік органдар баланы ақпараттық тұрғыда қорғауды неғұрлым жүйелі жүзеге асыра алады. Мұндай тәсіл қазақ құқықтық доктринасының соңғы жарияланымдарында жиі кездеседі: сарапшылар киберкеңістіктегі әлеуметтік әлеуетті реттеу мен цифрлық сауаттылықты жоғарылату қажеттігін атап көрсетеді. Мысалы, жақында шыққан зерттеулерде цифрлық құқық пен ақпараттық қауіпсіздік мәселелері талданып, балаларды цифрлық ортада қорғаудың заңнамалық тетіктерін дамыту қажеттігі баса айтылған.

Осы бағытта халықаралық та тәжірибелер ескеріледі: Еуропаның бірнеше елінде ата-аналарға онлайн мәліметтерін бақылау міндеттері жүктеліп, мектептерде цифрлық әлеуметтік жұмыс түрлері енгізілген. Қазақстанның құқықтық жүйесі осы инновациялық ұстанымдарға бағдарланып, әкімшілік-құқықтық нормаларды одан әрі жетілдіруде. Ұсынылып отырған түзетулер мен ұсыныстар кәмелетке толмағандардың цифрлық құқық бұзушылықтарымен күресте құқықтық саланың өзекті сұрақтарына жауап беруге мүмкіндік береді. Заңнаманы жаңарту арқылы балаларды ақпараттық кеңістіктегі қауіптерден қорғау нығая түспек, ал соттық және әкімшілік тәжірибе бұл шаралардың тиімділігіне дәлел болуы тиіс. Қорытындылай келе, кибер құқық бұзушылықтары тұрғысынан қарағанда, құқық қорғау

саласындағы мүдделі мекемелер мен қоғамдастық бірлесе отырып нормативтік базаны бейімдеу, цифрлық сауаттылықты арттыру және цифрлық дәлелдемелерді қолданыстағы процестерге енгізу бағытында жүйелі жұмыс жасауды жалғастыруы қажет. Бұл міндеттер ересектердің де, балалардың да конституциялық құқықтарының сақталуына кепілдік беретін әлеуметтік тұтастықтың бір бөлігі болып табылады.

*Әкімшілік-құқықтық нормаларды оңтайландыру бағыттары.* Алдыңғы бөлімде қазақстандық әкімшілік құқық бұзушылық туралы заңнамадағы жасөспірімдерге қатысты шектеулер мен олардың цифрлық ортада жауапкершілікке тартылуы мәселелері қарастырылды. Бұл тарауда сол талдауды тереңдетіп, ақпараттық қауіпсіздікке байланысты нормаларды халықаралық тәжірибемен салыстыру, цифрлық дәлелдемелерді жинау мен тергеу талаптарын жетілдіру, сондай-ақ кәмелетке толмағандарға арналған цифрлық сауаттылық пен ата-аналардың міндеттерін кеңейтудің құқықтық негіздерін ұсыну мақсатында кеңейтілген талқылау жүргізіледі.

Әкімшілік құқық бұзушылық туралы кодекстің 65-бабында жауапкершілікке тарту жасы 16 жас болып белгіленген, бұл 14-15 жастағы балаларды ресми әкімшілік жауаптан тыс қалдырады. Осы шектеу заңнаманың кәмелетке толмағандарға қатысты тиімділігіне күмән тудырады.

Еуропалық және әлемдік тәжірибеде ақпараттық қауіпсіздік бұзушылықтарына байланысты шектеулер балалардың жасына қарай әртүрлі анықталған. Мәселен, АҚШ-тың ұсынылып отырған Kids Online Safety Act (KOSA) және COPPA 2.0 жобалары 13 жасқа дейінгі балаларды әлеуметтік желі қызметтерін пайдаланудан алдын-ала parental consent талап етеді және жас шегін 16 жасқа дейін кеңейту мүмкіндігін қарастырады [130]. Қытайдың жобалық ұсыныстарында 16-18 жас аралығындағы жасөспірімдердің мобильді телефондары күніне екі сағаттан аспайтындай шектеліп, 8-16 жас аралығына бір сағат, ал 8 жасқа дейінгі балаларға сегіз минут рұқсат етіледі [131]. Ұлыбританияның онлайн қауіпсіздік туралы актісі әлеуметтік медиа платформаларынан балаларға арналған жас шектеулерін нақты көрсетіп, жасөспірімдердің жасына сай пайдаланушы тәжірибесін қамтамасыз етуді талап етеді [132]. Бұл мысалдар балалардың цифрлық кеңістіктегі мінез-құлқын қадағалау үшін жас шегін төмендету немесе әр жаста әртүрлі талап енгізудің тиімділігін көрсетеді.

Қазақстанда 14-15 жастағы жасөспірімдердің интернет алаяқтық, кибербуллинг сияқты әрекеттерге қатысу фактілері кездесетіні туралы көптеген практика бар. Мұндай іс-шараларды ескере отырып, кодекске кәмелетке толмағандарды 14 жастан бастап әкімшілік жауапкершілікке тарту туралы түзету енгізу мәселесі қарастырылуы керек. Бұл түзету балалардың жеке ерекшелігін ескере отырып, айыппұлдың мөлшерін және басқа әкімшілік санкцияларды оңтайландыруға мүмкіндік береді. Жасына байланысты кезеңдерге бөлінген жауапкершілік балалар психологиясын ескере отырып жасалады. Кәмелетке толмағандарға қатысты қылмыстық емес сипаттағы құқық бұзушылықтарда да 14 жас шегінің енгізілуі олардың интернеттегі әрекеттерін қадағалайтын заңнаманы күшейтеді.

Бүгінгі таңда кибер құқық бұзушылықтар бойынша әкімшілік тергеу жүргізу барысында цифрлық дәлелдемелер шешуші рөл атқарады. Алайда Қазақстандағы әкімшілік іс жүргізу кодексінде (ӘІЖК) электрондық деректерді жинау, сақтау және зерттеу тәртібі нақты регламенттелмеген.

Халықаралық тәжірибе электрондық дәлелдемелердің өзіндік ерекшелігін мойындайды: олар көбінесе қызмет көрсетуші ұйымдардың серверлерінде, бұлттық қоймаларда сақталады және жиі трансшекаралық сипатқа ие. Еуропалық одақта қылмыстық істерге арналған E-evidence регламенті электрондық дәлелдемелерді жинау механизмдерін айқындайды, алайда әкімшілік істер бойынша мұндай бірыңғай заңнамалық база жоқ екені атап өтіледі. Авторлар әкімшілік тергеулерге де қатысты электрондық дәлелдемелерді сақтауға және трансшекаралық қолжетімділікке мүмкіндік беретін жаңа ережелер қажет екенін атап өтеді [133, с.216].

Қазақстанда цифрлық дәлелдемелермен жұмыс істеу бойынша оқыту және инфрақұрылымдық жобалар іске асырылуда. Мысалы, OSCE-нің ұйымдастыруымен 2023 және 2024 жылдары құқық қорғау органдары қызметкерлеріне арналған семинарларда ноутбуктер, смартфондар, желілер және ашық дереккөздердегі ақпараттан электрондық дәлелдерді сәйкестендіру, алу және қауіпсіз сақтау, chain-of-custody құжаттарын рәсімдеу бойынша дағдылар үйретілді [134]. Бұл курстарда қатысушыларға сандық деректер мен физикалық дәлелдемелер арасындағы айырмашылықтар, іздестіру және тінту хаттамалары, volatile деректерді алу және ашық бастапқы коды бар криминалистикалық құралдарды пайдалану бойынша білім берілді [135].

2025 жылдың мамырында BOMCA бағдарламасы аясында Астана қаласында Қазақстан мен Қырғызстанның құқық қорғау органдарының мамандарына арналған сандық криминалистика бойынша үш күндік оқу семинары өтті. Семинарда сандық деректерді алу, өшірілген файлдарды қалпына келтіру және электрондық дәлелдемелерді талдау тәсілдері оқытылды [136]. Бұл шаралар әкімшілік істерде цифрлық дәлелдемелерді дұрыс рәсімдеуге мүмкіндік беретін кадрлық әлеуетті дамытуда маңызды.

Алайда бұндай оқытулардан басқа, әкімшілік іс жүргізуде цифрлық дәлелдемелердің құқықтық мәртебесін нақты айқындау қажет. Электрондық дәлелдемелердің сенімділігін қамтамасыз ету үшін

- *Chain of custody* (дәлелдемелерді беру тізбегі) - электрондық деректерді кім, қашан, қалай жинағаны және сақтағаны туралы толық дерекқор болуы керек. Кез келген үзіліс дәлелді жарамсыз етуі мүмкін.
- *Заңды іздестіру және тінту* - сандық құрылғыларды тәркілеу құқығы заңды негізде жүргізілуі тиіс және жеке өмірді заңсыз бақылауға жол бермеуі керек.
- *Деректердің шынайылығы және тұтастығы* - электрондық дәлелдеме түпнұсқалық, өзекті болуы және бұрмаланбауы шарт.
- *Құпиялық және этика* - тергеушілер артық деректерді жинаудан аулақ болып, жеке деректерді қорғау принциптерін сақтау қажет [137].

Интерполдың сандық криминалистика бойынша нұсқаулықтары да халықаралық стандарттарды ұсынады. Олар электрондық деректерді анықтау, алу, өңдеу, талдау және есеп беру кезінде арнайы техникалық құралдарды қолдануды, адал амалдардың сақталуын және зертханалық сертификаттарды талап етеді [138]. Бұл нұсқаулықтар ұлттық зертханаларды құру және алғашқы жауап берушілерді дайындау үшін «Дәлелдемелерді жинау жөніндегі нұсқаулық» және «Сандық криминалистикалық лабораториялар үшін жаһандық басшылық қағидалар» сияқты құжаттарды ұсынады.

Осы ұсыныстарды ескере отырып, Қазақстанның Әкімшілік іс жүргізу кодексіне «Цифрлық дәлелдемелерді жинау және сақтау» атты жеке бөлім енгізу керек. Бұл бөлімде төмендегі негізгі тармақтарды регламенттеуге болады:

- *Сандық құрылғылар мен ақпарат жүйелерін тәркілеу* - әкімшілік тергеуші цифрлық құрылғыларды тәркілеу кезінде рұқсатнама алуы, есепке алу актісін толтыруы және қорғау құралдарын қолдануы шарт.

- *Дәлелдемені сақтау форматтары* - тергеу барысында алынған электрондық деректер тексеруге дейін өзгеріске ұшырамайтындай күйде сақталуы үшін write-blocker құрылғыларын пайдалану қажет.

- *Кәсіби сарапшылардың қатысуы* - электрондық дәлелдемені алу және сараптау тек арнайы сертификатталған мамандар тарапынан жүргізілуі тиіс. Әкімшілік істер үшін сот сараптамасы институтында ақпараттық-техникалық бөлім құру ұсынылады.

- *Трансшекаралық ынтымақтастық* - халықаралық қызмет көрсетушілерден деректер сұрау тәртібі, оның ішінде Еуропалық одақтың электрондық дәлелдемелерге қатысты келісімдері (Budapest Convention, Cloud Act және т.б.) аясында мәліметтерді алу үшін құқықтық көмек көрсетілуі қажет. Бұл трансшекаралық процедуралар әкімшілік істерге де қатысты болуы тиіс [139, с.1].

Кибер құқық бұзушылықтармен күресте ата-аналар мен мектептердің рөлі ерекше. Қазақстанның қолданыстағы «Бала құқықтары туралы» заңында мемлекеттің міндеті балаларды денсаулығына зиян келтіретін ақпараттан қорғау деп көрсетілгенімен, ата-ана мен оқу орындарының міндеттері кеңінен регламенттелмеген. Ата-ананың бала тәрбиесі жөніндегі міндеттерін орындамауы үшін ӘҚБтК-нің 127-бабында әкімшілік жауапкершілік көзделгені белгілі [140], бірақ бұл бап цифрлық ортаға арнайы бағытталмаған.

Дүниежүзілік тәжірибе ата-аналардың сандық ортадағы рөлін күшейту бағытында. Еуропалық комиссияның 2025 жылғы жаңа нұсқаулықтары онлайн платформалардан кәмелетке толмағандарды қорғауды қамтамасыз ететін жан-жақты тәуекел бағалау жүргізуді талап етеді [141]. Платформалар жасөспірімдердің психологиялық дамуына әсер ететін контент, алгоритмдік ұсыныстар және байланыс мүмкіндіктері бойынша тәуекелдерді анықтап, баланың мүдделерін бірінші орынға қоюы тиіс. Бұдан басқа, жасына қарай растайтын age assurance механизмдерін енгізу және жасанды интеллект құралдары балаларға автоматты түрде қосылмауы тиіс.

Бірқатар елдерде ата-аналарға балаларының интернеттегі мінез-құлқын бақылау міндеттері заңда белгіленген. Мысалы, Қытайдың ұсынысына сәйкес ата-аналар балаларды түнгі уақытта смартфон қолданудан шектеуге міндетті, ал мобильді байланыс провайдерлері мұндай шектеулерді автоматты түрде орнатуы қажет [142]. Ұлыбританияның онлайн қауіпсіздік туралы заңында платформалар өз сервистерінің жасқа сәйкес қолданылуын қамтамасыз етуге міндетті, ал ата-аналар мен қамқоршылар балаларының аккаунттарын бақылауға мүмкіндік беретін құралдарды қолдана алады [143].

Қазақстанда ата-аналар үшін жаңа жауапкершілік деңгейін енгізу ұсынылады. «Ата-ананың балаларын қауіпсіз интернет пайдалануына бақыламауы» деген бап енгізіп, балалардың интернетті пайдалануына қатысты негізгі міндеттерді белгілеп, міндеттемелерді орындамағанда 5-10 АЕК көлемінде айыппұл салу тиімді. Сонымен бірге ата-аналарға сандық сауаттылық курстарын өту міндетін енгізу ұсынылады. Осы курстарда интернеттегі қауіптер, кибербуллингтің алдын алу, әлеуметтік желілерде баланың мінез-құлқын бақылау тәсілдері және олардың құқықтары талқылануы тиіс.

Мектептер мен колледждердегі тәрбие жұмыстары цифрлық мәдениетті қалыптастыруда аса маңызды. ӘҚБтК-нің 409-бабының 7-2-бөлігінде білім беру ұйымдарының тыйым салынған контентті қадағаламағаны үшін әкімшілік жауапкершілік көзделгені көрініс тапты. Бірақ бұл норма мазмұн сүзгілерін орнатуды, оқушыларға цифрлық этика туралы сабақ беруді немесе кибербуллингке қарсы шараларды қамтымайды.

Әлемдік практикада мектептер балалардың интернеттегі мінез-құлқын қалыптастыру үшін әртүрлі тәсілдерді қолданады. Ұлыбританияның Online Safety Act бойынша білім беру мекемелері оқу жоспарларына жас ерекшелігіне сәйкес онлайн қауіпсіздік сабақтарын енгізуі қажет, ал оқу процесінде платформаларды пайдалану кезінде қауіпсіздік талаптарын сақтауға міндетті [143]. АҚШ-тағы KOSA жобасы мектептерді цифрлық сауаттылық пен балалардың құқықтарын түсіндіруге міндеттейді [144].

Қазақ мектептері үшін келесі ұсыныстарды енгізуге болады:

- *Цифрлық сауаттылық бағдарламалары* - оқу бағдарламасына интернеттегі этика, деректерді қорғау, киберқауіптерге қарсы іс-қимыл және цифрлық із қалдыру туралы оқу пәндерін енгізу.

- *Бақылау инфрақұрылымы* - мектептердің компьютерлік желілерінде зиянды контентті сүзгілеуге арналған бағдарламалық-аппараттық кешендерді міндетті түрде орнату, бұл талаптарды бұзған жағдайда 409-баптың аясында әкімшілік санкцияларды күшейту.

- *Киберқауіпсіздік жауапты тұлғаларын даярлау* - әрбір оқу орнында ақпараттық қауіпсіздік жөніндегі уәкілді тағайындау; бұл маман оқушылар мен педагогтарға киберқауіптер туралы түсіндіру жұмыстарын жүргізіп, техникалық қорғау құралдарын бақылауы тиіс.

- *Мектеп-ата-ана сериктестігі* - ата-аналарға арналған семинарлар өткізіп, балалардың интернеттегі проблемалық мінез-құлқын қалай байқауға болатынын және кибербуллинг жағдайында қайда хабарласу керектігін

түсіндіру. Кибер құқық бұзушылықтарға қарсы күресте бір ғана ведомствоның күші жеткіліксіз. Қазақстанда «Бақытты және қауіпсіз балалық шақ» жобасы аясында прокуратура, полиция, әлеуметтік қорғау және үкіметтік емес ұйымдар бірлесе жұмыс істеп, кибербуллинг және басқа құқық бұзушылықтармен күреседі. Алайда киберкеңістіктің трансшекаралық табиғаты ведомствоаралық және халықаралық координацияны нығайтуды талап етеді.

Көптеген интернет-қылмыстар халықаралық сипатта болады; сондықтан істердің тергеуін басқа мемлекеттердің органдарымен бірге жүргізу қажет. 2025 жылы Astana Times жариялаған мақаласында ҚР Әділет министрлігі құқықтық жүйені модернизациялау аясында E-saraptama 2.0 жүйесі, виртуалды аутопсия және биометриялық сәйкестендіру құралдары сияқты цифрлық бастамаларды енгізуді жоспарлап отырғаны айтылады [145]. Бұл платформалар қылмыстық және әкімшілік істер бойынша сараптамаларды жылдамдатуға, дәлелдердің сапасын арттыруға мүмкіндік береді. Сонымен қатар, Dentons заң фирмасының 2025 жылғы есебі электрондық цифрлық қолтаңбаларды бөтен тұлғаның атынан пайдалану үшін әкімшілік жауапкершілік енгізілгенін, бұл цифрлық өзара әрекеттесудегі құқықбұзушылықтарды азайтатынын атап өтеді [146].

Халықаралық ұйымдардың үлесі де маңызды. Интерпол сандық криминалистика бойынша нұсқаулықтарды әзірлеп, мүше мемлекеттерге техникалық көмек көрсетеді [147]. OSCE аймақтық курстары қазақстандық полицияға электрондық дәлелдемелермен дұрыс жұмыс істеуді үйретеді [134]. Еуропаның Киберқылмыс туралы Будапешт конвенциясы ақпараттық құқық бұзушылықтар бойынша ұлттық заңнамаларды үйлестіру және трансшекаралық деректерге қол жеткізуді жеңілдету мақсатында жасалды [139]. Бұл құжатқа сәйкес мемлекеттер бір-біріне ақпараттық жүйелерге кіруге немесе деректерді сақтауға байланысты құқықтық көмек көрсетуі тиіс.

2025 жылғы Құқықтық қызметтердің цифрлануына арналған workshop-тарда Еуропалық Одақтың ДСА (Digital Services Act) аясында жоғары тәуекел платформаларға кәмелетке толмағандар үшін тәуекел талдауы жүргізу міндеті жүктелетіндігі айтылды [141]; бұл тәжірибе қазақстандық провайдерлер мен әлеуметтік желілер үшін үлгі бола алады.

Будапешт конвенциясының екінші қосымша хаттамасы трансшекаралық электрондық дәлелдемелерге қол жеткізу тәртібін жетілдіреді. Ол әкімшілік тергеулерге де әсер етуі мүмкін, себебі ақпараттық жүйедегі құқық бұзушылықтар көбінесе бірден қылмыстық сипат алмайды. Қазақстан бұл хаттаманы ратификациялау арқылы шетелдік сервистерден деректерді сұрату, сақтау, жариялауға тыйым салу және жою туралы тапсырмаларды орындау механизмдерін игере алады.

Өткен және қазіргі тәжірибені есепке ала отырып, әкімшілік нормативтік базаны жетілдіру үшін төмендегідей нақты ұсыныстар беруге болады:

1. *Кибербуллинг және кәмелетке толмағандарды қорғау туралы арнайы бап.* 2024 жылдың маусымында Қазақстанда кибербуллинг үшін 10 АЕК айыппұл қарастырылған жаңа бап енгізілді [42]. Бұл норманы толықтырып,

жүйелі түрде қайталанған жағдайда айыппұл мөлшерін ұлғайтумен қатар, әлеуметтік желілердегі есептік жазбаларды уақытша бұғаттау, қоғамдық жұмыстарға тарту, психологиялық коррекция бағдарламаларынан өту сияқты альтернативті санкцияларды қарастыру керек. Мысалы, ЕО нұсқаулықтары жасанды интеллект негізінде ұсыныстар мен алгоритмдер кәмелетке толмағандарға тәуекел тудыруы мүмкін екенін ескертіп, оларды өшіруді міндеттейді [141]; бұл нормаларды да енгізу маңызды.

2. *Ата-аналардың жауапкершілігін күшейту.* Жаңа баптар ата-аналардың балалардың интернеттегі қауіпсіздігін қамтамасыз ету бойынша міндеттерін регламенттеуі тиіс. Әке-шеше баласының онлайн қызметін қадағаламағаны немесе кибербуллингке жол бергені анықталса, оған он АЕК-ке дейін айыппұл, қажет болған жағдайда тәрбиелік курстар өтуді міндеттеу ұсынылады. Бұл шаралар ата-аналарды баласының цифрлық тәжірибесіне саналы көзқараспен қарауға ынталандырады.

3. *Мектептер мен колледждер үшін цифрлық қауіпсіздік стандарттары.* ӘҚБтК-нің 409-бабын кеңейтіп, оқу орындарының желілік инфрақұрылымының қауіпсіздігін қамтамасыз етпегені үшін жауапкершілікті қатаңдату керек. Сонымен қатар, білім беру заңнамасына мектептер мен колледждерді қауіпсіздік бойынша техникалық талаптарға сәйкес келетін фильтрлік бағдарламалармен, firewall және контент басқару жүйелерімен міндетті түрде жабдықтауды енгізу керек. Оқу орнының басшылары мен IT-мамандарының өзара міндеттерін нақтылап, бұзушылық анықталған жағдайда айыппұлды арттыру ұсынылады.

4. *Цифрлық дәлелдемелерді реттеу.* Әкімшілік кодекске сандық дәлелдемелердің анықтамасы және оларды алу, сақтау және зерттеу тәртібі туралы толық тарау енгізу қажет. Бұл тарау chain-of-custody принципін міндетті қылып, электрондық деректердің түпнұсқалығын қамтамасыз ететін write-blocker құрылғыларын қолдануды, тергеу процестерінің видеофиксациясын қарастыратын норма енгізуді қамтуы тиіс [137]. Сондай-ақ трансшекаралық деректерді алу үшін халықаралық шарттарға сілтеме жасау керек.

5. *Жасөспірімдердің жас шегін төмендету.* ӘҚБтК-де әкімшілік жауапкершілік жасын 16-дан 14 жасқа төмендету жөнінде түзету енгізу қажет. Бұл өзгеріс жасөспірімдердің кибербұзушылықтағы қатысуын бақылауға мүмкіндік береді. Сонымен бірге, айыппұлдар мен шараларды 14 - 16 жас арасындағы тұлғалар үшін ата-анасына немесе қамқоршысына жүктеу арқылы әділеттілік қамтамасыз етіледі.

6. *Қоғамдық және ведомствоаралық ынтымақтастық жүйесін заңдастыру.* Кибер құқық бұзушылықтардың алдын алу бағытында прокуратура, полиция, білім және ғылым, денсаулық сақтау министрліктері мен үкіметтік емес ұйымдар арасында ақпарат алмасу және бірлескен іс-шаралар жоспарын қалыптастыру қажет. Қазіргі тәжірибеде мобильді топтар, жедел желі (111) және қоғамдық психологиялық қызметтер жұмыс істейді. Осы қызметтердің құқықтық мәртебесін заңнамада нығайтып, ортақ ақпараттық платформасын құру тиімді.

7. *Ғаламдық озық тәжірибені енгізу.* Еуропалық Одақтың Digital Services Act аясындағы ризик-бағалау, age assurance және контенттік бақылау талаптарын қазақстандық провайдерлерге бейімдеуді қарастыру қажет. Ұлыбританияның Online Safety Act сияқты заңдар жасөспірімдерге арналған жас-сәйкестік тәжірибесін қамтамасыз ету бойынша нақты нормалар ұсынатыны белгілі [143]. Бұл нормалар мемлекетіміздегі ақпараттық қауіпсіздік стандарттарын жетілдіруге үлгі бола алады.

Қылмыстың алдын алудың ең тиімді жолы - білім беру. 2025 жылғы UNICEF пен Қазақстан Үкіметінің бірлескен бағдарламасы балаларды онлайн зорлық-зомбылықтан қорғауды, заңдарды күшейтуді және балалар мен ата-аналардың сандық сауаттылығын арттыруды көздейді [148]. Бағдарлама кибербуллингтің алдын алу үшін мектептер мен жергілікті әкімшіліктердің, полиция бөлімдерінің қатысуын қамтамасыз етеді, сондай-ақ 15 % баланың күн сайын зиянды контентке тап болатынын көрсетеді [149].

Аталған бағдарлама аясында және әкімшілік заңнамаға енгізілетін өзгерістерді қолдау үшін келесі шараларды жүзеге асыру ұсынылады:

- *Мектеп оқушылары мен мұғалімдерге арналған семинарлар.* Сандық гигиена, әлеуметтік желілердегі қауіпті белгілер, жеке деректердің қауіпсіздігі, фишингтік шабуылдар және басқа Кибер құқық бұзушылық түрлері туралы семинарлар тұрақты өткізілуі тиіс.

- *Ата-аналарға арналған онлайн курстар.* Қолданыстағы заңдарда ата-ананың баланың білім алуына жағдай жасау міндеті бар; бұл міндетті кеңейтіп, ата-аналар үшін айрықша цифрлық сауаттылық курстарын ұйымдастыру қажет.

- *Инновациялық жобалар.* Жасөспірімдерге арналған мобильді қосымшалар мен веб-платформалар арқылы қауіпсіз интернет бойынша интерактивті ойындар, викториналар және кеңестер ұсыну. Мысалы, Corruptive Games немесе басқа да «destructive games» сияқты қауіпті контенттің психологиялық ықпалын анықтайтын құралдар құру. [140].

- *Ғылыми зерттеулер.* Университеттер мен ғылыми институттар кибербуллингтің психологиялық, әлеуметтік және құқықтық аспектілерін зерттеп, мемлекеттік органдарға ұсыныстар беруі керек. Бұл зерттеулер балалар психикасына әсер ететін факторларды анықтайды және әкімшілік заңнамадағы жаңа баптардың мазмұнын ғылыми негіздеуге мүмкіндік береді.

Кибер құқық бұзушылықтарды әкімшілік-құқықтық реттеудің жетілдірілуі балалардың және бүкіл қоғамның цифрлық қауіпсіздігін қамтамасыз ету үшін қажет. Қазақстандағы қолданыстағы нормалар кәмелетке толмағандардың құқық бұзушылықтары мен ата-аналардың міндеттері тұрғысынан кейбір олқылықтарға ие. Халықаралық тәжірибелерді ескере отырып жасалған ұсыныстар өзіміздің құқық жүйемізге бейімделген жағдайда, келешекте келесідей нәтижелерге қол жеткізуге болады:

- Әкімшілік жауапкершілік шегін төмендету жасөспірімдердің кибербұзушылыққа қатысуын ерте кезеңде тоқтатуға мүмкіндік береді;

- Цифрлық дәлелдемелерді жинау және сақтау бойынша регламенттер тергеудің әділдігін арттырады;

- Ата-аналар мен мектептерді киберқауіпсіздікке жауапты ету балалардың құқықтарын қорғауды күшейтеді;

- Ведомствоаралық және халықаралық ынтымақтастық ақпараттық құқық бұзушылықтардың трансшекаралық сипатына сәйкес келетін тиімді механизмдер ұсынады;

- Цифрлық сауаттылықты арттыру және ғылымға инвестиция салу алдағы буынның қауіпсіз цифрлық қоғамда өмір сүруіне негіз қалайды.

Жоғарыда ұсынылған нормалар мен іс-шаралар әкімшілік құқықтық базаны қазіргі заманның сын-тегеуріндеріне сай жаңғыртуға және кибер құқық бұзушылықтармен тиімді күрес жүргізуге мүмкіндік береді.

## 4.2 Ведомствоаралық және халықаралық ынтымақтастықты күшейту

Қазақстанда кәмелетке толмағандар арасындағы киберқылмыстармен күрес жүйелі түрде жан-жақты интеграцияланатын күрделі мемлекеттік саясаттың бөлігі болып табылады. Бұл саясатты жүзеге асыруда еліміздің ішкі істер, прокуратура, білім және басқа да мемлекеттік органдарының үздіксіз үйлесімді іс-қимылы маңызды. Мысалы, ҚР Үкіметінің жанындағы кәмелетке толмағандар мәселелері жөніндегі ведомствоаралық комиссия («МВК»), 2007 жылы құрылғаннан бері кәмелетке толмағандар арасындағы құқық бұзушылықты профилактикалау, баланың құқықтарын қорғау мәселелерінде ұсыныстар әзірлеуге бағытталған. Оған Ішкі істер, Білім, Денсаулық сақтау, Еңбек және әлеуметтік қорғау министрліктері, Бас прокуратура өкілдері және басқа да мүдделі мекемелер қатысады.

Бұл құрылым кәмелетке толмағандардың ісі жөніндегі шараларды үйлестірумен бірге, бала құқықтарын бұзу туралы деректерді прокуратура органдарына хабарлауға, зардап шеккендерді қайта әлеуметтендіру мен оңалту жүйесін әзірлеуге жауапты. Осы комиссияның жұмысында әртүрлі ведомство өкілдерінің - білім, денсаулық сақтау, ішкі істер, әлеуметтік қорғау саласы мамандарының қатысуы баланы кешенді қорғауға бағытталған іс-шаралар тізбегін қалыптастыруға мүмкіндік береді [150].

Сонымен бірге ведомствоаралық қатынастар білім беру саласымен тығыз байланыста жүргізіледі. Қазақстан Республикасының Білім және ғылым министрлігі 2022 жылы балаларды буллингтен қорғау жөніндегі қағидаларды бекіткен еді. Бұл құжат бекітілмес бұрын Оқу-ағарту министрлігі Балалардың құқықтарын қорғау комитеті Денсаулық сақтау, Еңбек және халықты әлеуметтік қорғау, Ақпарат және қоғамдық даму, Ішкі істер министрліктерімен және басқа да мүдделі ведомстволармен келісілген болатын [151]. Әсіресе, ІІМ, денсаулық сақтау және әлеуметтік қорғау министрліктерінің бұл қағидаларды қолдауы мектептерде кибербуллингтің алдын алу мен ерте анықтау шараларын мектеп инспекторлары, әлеуметтік педагогтар және психологтар көмегімен үйлестіруді білдіреді. Заңнамаға енгізілген өзгертулерге сәйкес, баланы (жасөспірімді) қорлау (буллинг), оның ішінде ақпараттық-телекоммуникациялық желілерде жүйелі түрде (екі және

одан көп рет) әдейі қорқыту - қылмыстық немесе әкімшілік жауаптылыққа жататын құқықбұзушылық деп танылған [152]. Осы тұрғыда ішкі істер органдары профилактикалық бақылау мен тергеу шеңберінде білім беру мекемелерімен, прокуратурамен бірлесіп жұмыс жасайды. Мектептерде кибербуллинг фактілері анықталған жағдайда, оқытушылар мен әкімшілік ІІМ тергеу бөлімшелеріне жедел хабарлап, әр балаға қатысты сауықтыру және психологиялық көмек көрсету ұйымдарымен (мысалы, психологиялық оңалту орталықтары) бірлескен шараларға шығады. ҚР заңнамасында бала құқықтары мен бостандықтарының бұзылуы жөнінде прокуратура органдарына және жауапты органдарға шағым жасау қарастырылған [153], сондықтан балаларға қатысты қылмыстық іс бойынша прокуратура да қадағалауды жүзеге асырады.

Кәмелетке толмағандарды қылмыс пен келеңсіз жағдайлардан қорғауда құқық қорғау жүйесі мен әлеуметтік қорғау, денсаулық сақтау және психологиялық қызметтердің кешенді үйлестіруі де аса маңызды. Мәселен, 2014 жылғы МВК-ның отырысында тек құқық қорғау органдары емес, денсаулық сақтау саласы да жастар арасындағы суицидтік мінез-құлықты азайту шараларын ұсынған [150]. Оқу-ағарту және әлеуметтік қорғау министрліктері баланың денсаулығы мен психикасына зиян келтіретін мазмұнға қарсы іс-қимылға оқушыларға психологиялық қолдау көрсету, педагогтарды психологиялық біліктілікке оқыту және ата-аналармен бірлескен профилактика бағдарламаларын енгізу арқылы жауап береді. Ата-аналар комитеттері, мектеп психологтары және білім беру ұйымдарының баланы әлеуметтік бейімдеуге және оңалтуға тартатын тетіктері баланы жан-жақты қорғауға жатады. Бұл ретте балаларға арналған «111» сенім телефоны сияқты елімізде бар жедел желілер баланың құқығы бұзылған немесе Кибер құқықбұзушылық фактісіне тап болған кезде де жүгінуге мүмкіндік береді.

Ішкі істер министрлігі мен басқа да мекемелер интернеттегі қылмыстарға қарсы іс-қимылда жаңа бағыттарды да енгізуде. Мысалы, 2024 жылдың басында ЮНИСЕФ ұйымдастырған дөңгелек үстел барысында «Балаларды онлайн зорлық-зомбылықтан, қорлаудан және пайдаланудан қорғау» бағдарламасы таныстырылды. Оның міндеттеріне ұлттық құқықтық базаны күшейту, интернеттегі жыныстық сипаттағы зорлық-зомбылыққа қарсы профилактика мен әрекет ету жүйесін дамыту кіреді. Сондай-ақ құқық қорғау органдарының киберқылмыстарды, әсіресе балаларға қарсы зорлық фактілерін тергеу әлеуетін арттыру, осы іске IT-өнеркәсіп өкілдерін тарту қарастырылған. Аталған бағдарламаның тағы бір бағыты - балалар мен ересектерді цифрлық сауаттылыққа үйрету, соның ішінде мұғалімдер мен ата-аналарды мектептер мен қауымдастықтарда дайындау. Мұндай шаралар кешені мемлекеттік органдармен бірге жеке сектор мен үкіметтік емес ұйымдардың ынтымақтастығын талап етеді; сарапшылардың пікірі бойынша Қазақстанда интернеттегі балалар қауіпсіздігін қамтамасыз ету үшін мемлекет, бизнес және азаматтық қоғамның бірлесе жұмыс істеуі қажет. Қатаң жеке меншік еместен, іскерлік орта да цифрлық қауіпсіз орта құру бастамаларын қолдауға дайын екендігін жеткізді [154, с. 446].

Осы дөңгелек үстел нәтижесінде ІІМ, ҚР Мәдениет және ақпарат министрлігі жанындағы Жастар және отбасы істері комитеті, Білім және ғылым министрлігінің Балалардың құқықтарын қорғау комитеті басшылығымен жаңадан Үйлестіру комитеті құрылды. Бұл комитет мемлекеттік орган өкілдері, халықаралық ұйымдар (UNICEF, UNESCO, OSCE т.б.), академиялық қауымдастық пен IT-саласы мамандарынан тұрады.

Комитеттің басты міндеті - балаларды цифрлық ортада қорғауға арналған стратегияларды әзірлеу және іске асыру, сондай-ақ ведомствоаралық күш-жігерді синхрондау. Яғни, қазақстандық мемлекеттік және азаматтық сектор киберқылмыспен күресте жаңа мемлекеттік-жекеменшік әріптестік үлгісін қалыптастыруда.

Қазақстанның ішіндегі аталған механизмдер халықаралық ынтымақтастық шеңберінде қалыптасқан үздік тәжірибеге сүйенеді. Мысалы, орталық Азия елдерімен бірлескен OSCE жобалары аясында полицейлер мен прокурорларды киберқылмысқа қарсы күреске дайындау өткізіліп келеді.

Аталмыш жобаның бірінші фазасы бойынша 2018-2019 жылдары Қазақстан мен көрші бес елдің заң органдары цифрлық сот тауарлары мен электрондық дәлелдемелерді зерттеуге, криптовалюталар мен қара нарықты саралауға арналған біліктіліктерін арттырды [155]. UNODC бағдарламалары аясында да Қазақстан мен Орталық Азия мемлекеттеріне арналған киберқылмыс бойынша семинарлар, оның ішінде «онлайн балаға қарсы қылмыс» тақырыбындағы шеберлік сабақтары өткізіліп, құқық қорғау органдары тәжірибе алмасты [156]. Бұл үйлесімділік Қазақстанның ТМД және Орталық Азия елдерімен киберқауіпсіздік бойынша ынтымақтастығының бір мысалы болып табылады: өңірлік тренингтер мен конференциялар шеңберінде тәжірибелік кеңестер мен құралдар алмасылуда.

Сонымен қатар Қазақстан цифрлық қауіпсіздік саласындағы халықаралық құжаттарды бекітуге ұмтылуда. Мысалы, 2023 жылғы мамырдағы OSCE конференциясы барысында Қазақстанның Еуропадағы Кеңес «Кибершабуылдар туралы» («Будапешт конвенциясы») келісіміне қосылуға ниетті екені атап өтілді, бұл елді Орталық Азияда алғашқылардың бірі етеді [155]. Бұл қадам қылмыстық құқықтағы нормаларды халықаралық стандарттарға сәйкестендіруге және трансшекаралық киберқауіптермен күресте құқық қорғау органдарының өзара іс-қимылын тереңдетуге бағытталған.

Бұқаралық ақпарат құралдары және телекоммуникация саласында қабылданған нормативтік актілер де балаларды интернеттен келетін қауіптіліктен қорғауға баса мән береді. Қазақстанда 2022 жылы «Бұқаралық ақпарат құралдары туралы» заңға балаларға қатысты кибербуллинг фактілері бойынша шағымдарды қарау тәртібін бекітетін бап енгізілді. Енді азаматтар баланы қорлаған интернет-ресурс атауын көрсете отырып, уәкілетті органға арыздана алады, осыған байланысты арнайы сараптама тобы үш жұмыс күні ішінде жауап береді [152]. Сонымен қатар 2023 жылдың шілдесінде «Онлайн-платформалар және онлайн-жарнама туралы» Заң қабылданып, онда Қазақстан аумағында жұмыс істейтін интернет-платформалардың заңды

өкілдерін белгілеу және оларды реттеу тетіктері көрсетілді. Мұнда платформалардың контентті бақылау функциялары (мысалы, Қазақстан заңдарына қайшы дербес деректер таратуға жол бермеу, анық жазылған. Заң бойынша платформалар құқық қорғау органдарының нұсқамасымен кибербуллинг деп танылған мазмұнды 24 сағат ішінде өшіруге міндетті [157].

Яғни, Meta, TikTok, Telegram секілді ірі платформалар Қазақстанда қызмет етуі үшін жергілікті өкіл тағайындап, тиісті бақылау органдарымен әріптес болуға кірісті. Сонымен бірге дербес деректерді қорғау жөніндегі Қазақстан заңнамасы балалардың цифрлық деректерін сақтауға қатысты қатал талаптарды енгізген, алаңдататын контент пен қылмыстық әрекеттерді жою мәселесінде GDPR тәрізді халықаралық стандарттарға ұмтылады.

Қазақстандық мемлекеттераралық және халықаралық ынтымақтастықтың тәжірибесі де ескеріле отырып, ұлттық нормативтік база тұрақты түрленіп келеді. Мысалы, кәмелетке толмаған адамға қатысты психологиялық бейімдеу мен оңалту шараларын белгілеу сияқты тұжырымдар Мемлекет Басшысының тапсырмасымен қаралған [152]. Оқу-ағарту министрлігінің бұйрықтары мен ведомствоаралық комиссиялардың шешімдері, Үкімет қаулылары балалардың цифрлық ортадағы қауіпсіздігін қамтамасыз етуге арналған кешенді іс-шаралар жоспарына сүйенеді. Қазіргі уақытта зорлық-зомбылықтың кез келген түріне жауап беретін заңдылық, оның ішінде кибершабуылдарға қарсы жедел шаралар, жүзеге асырылуда. Осы атқарылып жатқан жұмыстар мен халықаралық тәжірибені ескеру Қазақстандық әкімшілік пен құқық қорғау органдарының баланы киберқылмыстан қорғаудағы стратегиясының негізін құрайды.

Осылайша, мемлекеттік органдар жүйесі ішкі және халықаралық институттармен (прокуратура, полиция, білім беру басқармалары, әлеуметтік қызметтер, психологтар, сондай-ақ UNICEF, OSCE, EU, UNODC т.б.) бірлесіп жұмыс істей отырып, қазақстандық балаларды цифрлық ортадағы қауіптерден қорғауға бағытталған кешенді механизмдер кешенін қалыптастырды. Заңнамалық және ұйымдастырушылық қадамдар (мысалы, кибербуллингті анықтау процедурасы, платформалармен серіктестік талаптары) балаларды желідегі құқық бұзушылықтан қорғаудың халықаралық стандарттарына үйлестірілді. Нәтижесінде Қазақстанда ведомствоаралық үйлестіру мен халықаралық әріптестікті күшейту арқылы кәмелетке толмағандардың Кибер құқық бұзушылықтарынан қорғалуына байланысты саясат жүйелі әрі жан-жақты іске асырылып келеді [154].

Қазақстанда балаларды онлайн-ортадағы қылмыстардан қорғау мәселесі мемлекеттік саясаттың стратегиялық құрамдас бөлігі болып отыр. 2025 жылдың басындағы мәліметтерге сәйкес елде 6,9 млн бала өмір сүреді, оның ішінде 3,9 млн мектеп оқушысы және 556 мың колледж студенті [158].

Мемлекет балаларды әлеуметтік қорғау, білім беру және құқық қорғау жүйесінің басымдығы ретінде қарастырады. Соңғы жылдары Үкімет кибербуллингтің алдын алу, кәмелетке толмағандарға қарсы онлайн-зорлық пен пайдалану фактілерін тергеу, сондай-ақ қоғамдық санада қауіпсіз

цифрлық мәдениетті қалыптастыру үшін нормативтік-құқықтық базаны күшейтіп, ведомствоаралық және халықаралық ынтымақтастықты дамытты.

*Ұлттық деңгейдегі ведомствоаралық ынтымақтастық.* Кәмелетке толмағандар арасындағы қылмыс пен құқық бұзушылықтардың алдын алу Қазақстан Үкіметінің жанындағы кәмелетке толмағандар істері жөніндегі ведомствоаралық комиссия (МВК) арқылы үйлестіріледі. 2007 жылы құрылған комиссияға Ішкі істер министрлігі (ІІМ), Білім және ғылым министрлігі, Денсаулық сақтау, Еңбек және әлеуметтік қорғау министрліктері, Бас прокуратура өкілдері және басқа мүдделі ведомстволар кіреді. Үкімет сайтындағы құжаттардың түсіндірмесінде комиссияның басты міндеттері кәмелетке толмағандардың құқықтары мен мүдделерін қорғау бойынша ұсыныстар әзірлеу, жасөспірімдер қылмысының себебі мен жағдайларын анықтау, профилактикалық бағдарламалар әзірлеу және осындай бағдарламалардың іске асырылуын бақылау екені көрсетілген. Комиссияның құрамында білім, денсаулық сақтау, әлеуметтік қорғау мамандары мен құқық қорғау органдарының қызметкерлері бар, бұл кәмелетке толмағандарды кешенді қорғау іс-шараларын қалыптастыруға мүмкіндік береді.

Қазақстан заңнамасында кибербуллинг пен балаларға қарсы онлайн-қылмыстарға жауапкершілік күшейтілді. 2024 жылы қабылданған «Әйелдердің құқықтарын және балалардың қауіпсіздігін қамтамасыз ету туралы» заң кәмелетке толмағандарды қорлау (буллинг және кибербуллинг) үшін әкімшілік жауапкершілік енгізіп, кәмелетке толмағандарға қарсы қылмыстар үшін жазаны күшейтті [158]. Бұл заң педагогикалық ұжымдарды балаларға қатысты құқық бұзушылықтарды ІІМ-ге хабарлауға міндеттейді және отбасылық зорлық-зомбылықты қылмыстық сипатқа жатқызды [159].

2022 жылы «Білім туралы» заңға өзгерістер енгізіліп, буллинг түсінігіне жүйелі қорлау немесе қорқыту, оның ішінде ақпараттық-телекоммуникациялық желілерде жасалатын әрекеттер енгізілді. UNESCO-ның медиа және ақпараттық сауаттылық жөніндегі есебінде буллингтің алдын алу және анықтау тәртібін регламенттейтін «Балаларды буллингтен қорғау ережелері» және білім беру ұйымдарындағы психологиялық қызметтің жұмысы туралы ережелер қабылданғаны атап өтіледі [160, с. 2].

Үкімет мектептерде қауіпсіз орта қалыптастыру мақсатында бірнеше жобаларды жүзеге асырып жатыр. 2025 жылы педагогикалық ұйымдарда алаңдатқыш батырмалар мен турникеттер орнатылып, лицензияланған күзет енгізілді. Мектептер мен колледждерде QR-код арқылы «111» байланыс орталығына тез қол жеткізу жүйесі енгізіліп, жыл басынан бері 77 мыңнан астам өтініш тіркелген [1]. Психологиялық қолдау орталықтары 2024 жылы 250 мыңнан астам оқушы мен олардың отбасыларына көмек көрсетті, ал медиация қызметтері мен балалар омбудсмендері барлық аймақтарда жұмыс істейді [158].

Мектептерде антибуллинг мәдениетін қалыптастыру үшін Финляндияның KiVa бағдарламасы және қазақстандық DOSBOLLiKe бағдарламасы енгізілді; Cyber Tumar, Parental Control және Menin Baúryrym сияқты ақпараттық-

ағартушылық акциялар жүзеге асуда [158]. Qazinform дерегіне сәйкес, бұл бастамалармен бірге әкімшілік жауапкершілік енгізіліп, 2024 жылы психологиялық қолдау орталықтары 250 мыңнан астам оқушы және олардың отбасыларына қолдау көрсеткен [161].

UNESCO есебінде 2022 жылдан бастап барлық мектептерде «Жеке қауіпсіздік сабақтары» енгізіліп, онда оқушылар мен ата-аналарға онлайн-қауіпсіздік, буллингтің алдын алу және ақпараттық мәдениет мәселелері түсіндірілетіні айтылады [160, с. 2]. 2024 жылы UNICEF, Балалардың құқықтарын қорғау комитеті және Қауіпсіздік комитетімен бірлесіп ата-аналарға арналған онлайн-қауіпсіздік жөніндегі шебер-сыныптарды өткізді. Жоба ата-аналарға интернеттегі қауіптер мен балалардың психикалық денсаулығына әсерін түсіндіруге, сондай-ақ қауіпсіздікті қамтамасыз ету жолдарын үйретуге бағытталды [162].

Мектеп инспекторлары, әлеуметтік педагогтар мен психологтар кибербуллинг фактілерін ерте анықтау және зардап шеккен балаларға көмек көрсету бойынша ІІМ-мен тығыз жұмыс істейді. Бала құқықтарының бұзылуы туралы мәліметтер прокуратура органдарына жіберіледі және бұл құрылымдар мен психологиялық оңалту орталықтары сауықтыру шараларын үйлестіреді. 2025 жылы Орталық Азия елдерімен бірлескен OSCE-нің жастар қылмысын алдын алу бойынша тренингі барысында қазақстандық полиция, әлеуметтік қызметтер мен жастар ұйымдары халықаралық тәжірибені бейімдеу, полиция мен әлеуметтік қызметтердің өзара іс-қимылын жақсарту және ортақ іс-шараларды жоспарлау құралдарын талқылады [163].

*Халықаралық ынтымақтастық.* Қазақстан киберқылмыспен күресте халықаралық құқықтық нормаларды енгізуге ұмтылуда. 2024 жылдың соңында БҰҰ Бас Ассамблеясы Киберқылмыспен күрес туралы конвенцияны қабылдады, ол мемлекеттерге онлайн баланы сексуалдық мақсатта пайдалану сияқты құқықбұзушылықтарды қылмыстандыруды және адам құқықтары мен бостандықтарының сақталуын қамтамасыз етуді міндеттейді [164].

2025 жылы Астанада өткен Трансұлттық киберқылмысқа қарсы күрес жөніндегі халықаралық конференцияда (ІІМ, UNICEF, OSCE, UNODC және Interpol ұйымдастырған) ТМД елдерінің киберполиция жетекшілері мен IT компанияларының өкілдері киберқылмыстың ұлттық ахуалы туралы баяндап, балаларды онлайн сексуалдық зорлық-зомбылықтан қорғау, Біріккен Ұлттар Ұйымының конвенциясын іске асыру және бірлескен тергеулерді үйлестіру мәселелерін талқылады [165]. Конференцияда 2025-2026 жылдарға арналған бірлескен іс-қимыл жоспары ұсынылып, қылмыстық әрекеттерді тергеу үшін цифрлық сауаттылықты арттыру мен халықаралық серіктестермен ынтымақтастық күшейту қажет екені атап өтілді [165].

UNODC-тің мәліметінше, бұл конференция киберқылмыспен күрес жөніндегі БҰҰ конвенциясын қабылдағаннан кейінгі алғашқы өңірлік шара болып, Қазақстан мен көрші елдердің құқық қорғау органдарының қатысуымен онлайн баланы сексуалдық пайдалану, криптовалюталарды қолдану арқылы қылмыстар, сондай-ақ нақты іске асқан трансұлттық алаяқтық қоңыраулар орталығын жою тәжірибелері талқыланды [164].

2024 жылы Safe Online қорының қолдауымен UNICEF пен Қазақстан Үкіметі «Балаларды онлайн зорлық-зомбылықтан, қорлаудан және пайдаланудан қорғау» атты екі жылдық бағдарламаны бастады. Бағдарламаның мақсаты - ұлттық жүйелерді күшейту, онлайн сексуалдық қылмыстарды тергеу қабілетін арттыру, балалар мен ата-аналардың цифрлық сауаттылығын дамыту және зардап шеккен балаларға гендерлік сезімтал қолдау көрсету [166]. 2025 жылғы баспасөз хабарламасында көрсетілгендей, бағдарламаның іске қосылуы барысында Үкіметтің өкілдері, ІІМ, Мәдениет және ақпарат министрлігінің Жастар және отбасы істері комитеті, Білім министрлігінің Балалардың құқықтарын қорғау комитеті, IT-компаниялар мен халықаралық ұйымдар жиналып, онлайн қауіптерді болдырмау мен кибербуллингпен күрес жөніндегі бастамаларды талқылады. Олар ұлттық заңнаманы күшейту, онлайн сексуалдық зорлық-зомбылыққа қарсы профилактикалық жүйені дамыту, құқық қорғау органдарының әлеуетін арттыру, IT индустриясының рөлін кеңейту, балалар мен ата-аналарды оқыту және зардап шеккендерге көмек көрсету сияқты мақсаттарды айқындады. Бұл бағдарлама бойынша Үйлестіру комитеті құрылып, оған мемлекеттік органдар, халықаралық ұйымдар (UNICEF, UNESCO, OSCE), академиялық қауымдастық және IT секторының өкілдері кірді [167].

Қазақстан құқық қорғау құрылымдары қызметкерлерінің біліктілігін арттыру үшін халықаралық ұйымдармен бірлескен жобаларға қатысады. OSCE-нің Трансұлттық қауіптер департаменті және Астанадағы бағдарламалық кеңсе ұйымдастырған «Жастар қылмысын алдын алу» тренингінде полиция, әлеуметтік қызметтер мен жастар істері ұйымдарының өкілдері жастар қылмысын алдын алу және балалардың құқықтарын қорғау бойынша халықаралық тәжірибені бейімдеу, полиция мен әлеуметтік қызметтердің өзара іс-қимылын күшейту, ортақ іс-қимылдарды жоспарлау жөнінде ұсыныстар әзірледі [163]. UNODC 2025 жылғы халықаралық конференция аясында ТМД елдерінің киберқылмысқа қарсы бөлімшелерінің өкілдері, Interpol және IT компаниялар (Group-IB, TikTok) қатысқан семинар өткізді; онда БҰҰ-ның жаңа киберқылмысқа қарсы конвенциясы бойынша тәжірибе алмасу және онлайн балаға қатысты қылмыстарды тергеу үшін халықаралық ынтымақтастықты нығайту талқыланды [164].

Қазақстан Орталық Азияда цифрлық қауіпсіздік бойынша көшбасшы болуға ұмтылып, көрші елдермен және халықаралық ұйымдармен серіктестікті кеңейтуде. OSCE-нің жобалары аясында 2018-2019 жылдары Қазақстан мен көрші елдердің құқық қорғау қызметкерлері цифрлық дәлелдемелерді зерттеу, криптовалюталар мен қара нарықты талдау сияқты бағыттар бойынша оқудан өтті. UNODC пен OSCE ұйымдастырған шеберлік сабақтарында онлайн балаға қарсы қылмыстарды анықтау және тергеу бойынша тәжірибе алмастырылды. 2024 жылы Орталық Азия елдері үшін ұйымдастырылған семинарларда ортақ тергеулерді үйлестіру және қылмыстық істер бойынша ақпарат алмасу мәселелері қарастырылды [165]. Сонымен қатар Қазақстан 2023 жылдағы OSCE конференциясында Еуропалық Кеңестің кибершабуылдар туралы Будапешт конвенциясына

қосылуға ниетін білдірді, бұл елдің халықаралық құқықтық стандарттарды қабылдауға дайын екенін көрсетті.

Қазақстан кәмелетке толмағандарды киберқылмыстан қорғау бағытында кешенді ұлттық шараларды жүзеге асырып, ведомствоаралық және халықаралық ынтымақтастықты кеңейтуде. Заңнамадағы жаңалықтар - буллинг пен кибербуллинг үшін әкімшілік жауапкершіліктің енгізілуі, мектептердегі қауіпсіздік инфрақұрылымдары және психологиялық қолдау орталықтарының жұмысы - балалардың қорғалу деңгейін арттыруға ықпал етеді [158]. Құқық қорғау органдары мен әлеуметтік қызметтер арасындағы өзара іс-қимыл, сондай-ақ ата-аналар мен мұғалімдерді оқыту бағдарламалары балалардың цифрлық сауаттылығын арттыруға және суицидтік мінез-құлық сияқты тәуекелдерді азайтуға бағытталған [160, с. 4].

Халықаралық деңгейде Қазақстан UNICEF, OSCE, UNODC және Interpol тәрізді ұйымдармен әріптестік орнатып, киберқылмысқа қарсы жаһандық бастамаларды қолдайды. БҰҰ-ның киберқылмысқа қарсы конвенциясын қабылдау, өңірлік конференциялар мен бірлескен тренингтер онлайн қылмыстарды тергеу және балаларды қорғау бойынша ортақ стандарттар мен тәжірибе қалыптастыруға мүмкіндік береді [164]. UNICEF-тің «Балаларды онлайн зорлық-зомбылықтан қорғау» бағдарламасы ұлттық заңнаманы жетілдіруге, құқық қорғау органдарының әлеуетін арттыруға және қоғамның жалпы цифрлық мәдениетін дамытуға бағытталған [167].

Алдағы кезеңде Қазақстанға киберқылмыспен күрес стратегиясын одан әрі жетілдіру үшін бірқатар қадам жасау ұсынылады:

1. *Бақылау және есептілік тетіктерін күшейту* - мектептер мен әлеуметтік қызметтерде кибербуллинг туралы деректерді тіркеу жүйесін жетілдіру және құқықбұзушылықтар бойынша бірыңғай статистикалық база қалыптастыру.

2. *Халықаралық стандарттарды имплементациялау* - Будапешт конвенциясына қосылу бойынша жұмыстарды аяқтап, еуропалық ережелерге сәйкес цифрлық дәлелдемелерді жинау және алмасу процедураларын қабылдау.

3. *Технология индустриясымен әріптестікті тереңдету* - платформалардың мазмұнды модерациялау міндеттемелерін нақтылайтын заңдарды жетілдіру және IT-компаниялармен бірлескен мониторинг жобаларын іске асыру.

4. *Қоғамдық сана және білім беру* - балалардың, ата-аналардың және педагогтердің цифрлық құқықтар мен жауапкершілік туралы білімін арттыру үшін ұзақ мерзімді білім беру бағдарламаларын енгізу, соның ішінде арнайы онлайн-курстар мен тренингтер.

5. *Жәбірленушілерді қолдау жүйесін дамыту* - балаға қарсы онлайн қылмыстардан зардап шеккендерге құқықтық және психологиялық көмек көрсету орталықтарының желісін кеңейту және гендерлік-сезімтал қызметтерді енгізу [168, с. 42].

Кешенді ведомствоаралық үйлестіру мен халықаралық әріптестікті күшейту арқылы Қазақстан балалардың цифрлық ортадағы қауіпсіздігін

қамтамасыз етуге бағытталған жаһандық бастамалардың белсенді қатысушысы болып қала береді.

### 4.3 Кәмелетке толмағандардың құқықтарын қорғаудың заманауи технологиялық шешімдері

Интернеттің кең таралуы мен цифрлық технологиялардың жылдам дамуы балалардың сандық ортада отыру уақытын арттырды, бұл жаңа мүмкіндіктермен қатар үлкен қауіп-қатерлерді де туғызады [169]. UNICEF мәліметі бойынша қазақстандық балалардың көпшілігі интернетті 5 жасқа дейін немесе одан ерте жаста қолдануды бастайды [170]. Әлемде балалар цифрлық әлемге бұрын-соңды болмаған қарқынмен енуде, сондықтан олардың жеке өмірі, денсаулығы мен қауіпсіздігін қамтамасыз ететін технологиялық шаралар қажет болып отыр [169]. Ақпараттық технологиялар (AT), оның ішінде жасанды интеллект (AI), ірі деректер (Big Data), блокчейн, жас мөлшерін анықтау (age-verification) жүйелері, ата-ана бақылау қосымшалары балаларды онлайн қауіпсіздікпен қамтамасыз етудің маңызды құралдарына айналды.

Жасанды интеллект пен ірі деректер технологияларының мүмкіндіктері балаларды қорғауда көп қырлы рөл атқарады. AI алгоритмдері мазмұнды автоматты түрде сүзуге, жасқа сай еместікті анықтауға және кибербуллинг, зорлық-зомбылық сияқты мазмұнды іздеуге мүмкіндік береді. Мысалы, БҰҰ есебінде атап өтілгендей, жасанды интеллект пен деректерді өңдеу құралдары адам саудасын қудалаушы желілерді анықтауда қолданылып келеді; UNODC сарапшыларының айтуынша, «жасанды интеллект, деректерді өңдеу және басқа құралдар көмегімен сауда желілерін анықтау мен тергеп-тексеруге» қолдау көрсетуге болады [171]. Блокчейн-технологиясы шифрлауды қолдану арқылы деректерді берік қорғауды қамтамасыз етеді. Ол жеке куәліктерді онлайн растауда сенімді құрал бола алады: сандық блокчейн негізіндегі идентификация балалардың жасы мен жеке мәліметін ашпай-ақ тексеруді мүмкін етеді [172]. Бұл тәсіл GDPR сияқты деректерді қорғау талаптарына сәйкес келіп, жеке мәліметті қажетсіз жарнамалардан немесе сандық қудалау әрекеттерінен қорғауға септігін тигізеді.

Жас мөлшерін анықтайтын жүйелер (age-verification) - кәмелетке толмағандардың ересек контентке қолжетімділігін шектеуде қолданылатын технологиялар. Олар деректер базасын немесе биометрикалық мәліметтерді пайдаланып, пайдаланушының жасын тексереді. Қазіргі таңда Германия мен Франция сияқты елдерде белгілі бір мазмұн мен сайттарға кіру үшін жас тексеру міндетті, ал халықаралық қауымдастық бұл бағыттағы стандарттарды пысықтап жатыр [173]. Қазақстанда да осыған ұқсас идея қарастырылып, 2023-2025 жылдарға арналған балаларды қорғау кешенді жоспарында зиянды контенттен оқшаулау шаралары енгізілді [174].

Ата-ана бақылауына арналған бағдарламалар балалардың цифрлық белсенділігін бақылау және шектеу үшін қолданылады. Google-дың Family

Link бағдарламасы Android/ChromeOS құрылғыларында жұмыс істейді, онда ата-ана балаға қондырылатын қолданбаларды қадағалап, қолдану уақытын шектейді. Apple экожүйесінде iOS құрылғыларындағы Screen Time функциясы баланың қолданбаларды қолдану уақытын есептейді, апталық есеп береді және жасқа сай мазмұнға шектеулер қояды. Сонымен бірге, коммерциялық шешімдердің бірі Net Nanny ата-анаға веб-сайттар мен қолданбаларды сүзу, уақыт бойынша шектеу қою және әлеуметтік желілердегі белсенділік туралы есеп беруге арналған. Мысалға, Net Nanny пайдаланушыларға веб-ресурстарды блоктауға, порнография мен зиянды контентті сүзуге, күнделікті интернетке кіру сағаттарын белгілеуге мүмкіндік береді [175]. Bark сияқты платформалар балалардың әлеуметтік желідегі месседждерін қадағалап, кибербуллинг және жыныстық сипаттағы қауіпті әрекеттерге ескерту жүйесін ұсынады.

Қазақстандық IT-шешімдер: цифрлық үкімет пен жоба мысалдары Қазақстанда балаларды қорғау мақсатында бірқатар мемлекеттік және жеке сектор жобалары іске асуда. Мәселен, COVID-19 пандемиясы кезінде кеңінен қолданылған «Ashyq» жүйесі 12 жастан асқан балаларға белсенді түрде енгізілді. Бас санитар дәрігерінің қаулысы бойынша 12+ балалар компьютерлік клубтар, кинотеатрлар сияқты орындарға Ashyq-та тіркеліп кіре алды [176]. Бұл тәжірибе Ashyq жүйесінің үлгісін басқа салаларға, соның ішінде цифрлық балалар порталдарына бейімдеуге мүмкіндік береді.

Электронды үкімет (eGov) экожүйесінде де балаларға арналған сервистер енгізілген. Мысалы, eGov Mobile қосымшасындағы «Балалар туралы мәліметтерді өзектендіру» және «Ұлттық қор - балаларға» модульдері арқылы ата-аналар бала туралы цифрлық құжаттарды тіркеп, оған мемлекеттік қолдау ақысын ала алады [177]. Мұндай жүйелер атаулы әлеуметтік көмек пен цифрлық сауаттылықты арттырумен бірге, балаларға қатысты деректердің бір орталықтан басқарылуын қамтамасыз етеді, нәтижесінде олардың құқығы сақталады.

Сонымен қатар, ҚР Цифрлық даму, инновациялар және аэрокосм. өнеркәсібі министрлігінің (ЦДИАӨМ) қолдауымен және білікті ұйымдардың қатысуымен Cyber Tumar («Кибер Тұмар») сияқты білім беру жобалары іске қосылды. Мысалы, Түркістан облысында ақпараттық қауіпсіздік комитеті, Білім министрлігінің Балалар құқықтары комитеті, «Kaspersky» зертханасы және ЮНИСЕФ ұйымдастыруымен ата-аналарға арналған семинарлар өтті.

Онда сарапшылар «балалардың киберқауіпсіздігі үшін ата-аналар келесі шараларды қолдануы керек» деп айтты: баланың интернеттегі уақытын шектеу, қолжетімді контентті бақылау, желідегі қауіптер туралы ашық әңгіме жүргізу және зиянды контентті анықтаған жағдайда модераторлардан көмек сұрау [178]. Бұл іс-шарада UNICEF-тің кеңесшісі Л.Бейсембаева да баланың психикалық денсаулығы мен цифрлық сауаттылық мәселелеріне тоқталды.

2024 жылы қазақстандық IT-компаниялар мен мемлекеттік орган бірлесіп пилоттық жобаға бастамашы болды. Мысалы, Павлодар облысында «Kaspersky Safe Kids» қосымшасын балаларға тегін тарату жобасы жүзеге асты. Әкімдіктің цифрлық технологиялар басқармасы мен «Kaspersky»

компаниясы әлеуметтік әлсіз отбасылардағы бала құқықтарын қорғауға бағытталған пилотта Қылмыстық-атқару жүйесінің бақылауындағы отбасыларға Safe Kids лицензияларын ұсынды. Бұл бағдарлама смартфон мен планшеттердегі қауіпті мазмұнды сүзуге, уақыт шектеулерін қоюға мүмкіндік береді. Павлодарлық жоба аясында жүргізілген зерттеу нәтижелері бойынша балалардың көпшілігінің интернетте өткізетін уақыты айқындалды: олардың 56%-ы күніне 1-4 сағат, ал 23%-ы теңге бар бос уақыттарын «ең көбімен» онлайнда өткізеді. Сарапшылар ескерткендей, ата-аналардың 36%-ы баласының ұзақ экран алдында болуынан жанжал шыққанын айтқан [179]. Осы мәліметтер Қазақстан мектептерінде цифрлық фильтрлер мен ата-ана бақылауын кеңінен ендіру қажеттігін көрсетеді.

2025 жылы Алматыда тағы бір пилоттық бастама - «SIM KIDS» жобасы іске қосылды. Бұл арнайы SIM-карта «Tele2/Altel» компаниясымен бірлескен пилот болып табылады және бала мобильді құрылғысына зиянды ықпал ететін контентті - суицид, порнография, есірткі, құмар ойын секілді - блоктау функцияларына ие. Сонымен бірге SIM-карта ата-анаға балалар қолданатын қосымшаларды көруге және сәйкес сайттарға кіруді шектеуге мүмкіндік береді. Генеральды прокурор Б.Асыловтың айтуынша, «SIM KIDS» жобасы ата-аналар арасында зор қызығушылық тудырды және сынақ мерзімі сәтті өткен соң кеңінен қолжетімді болады [143]. Бұл шара 2023-2025 жылдарға арналған «Балаларды зорлық-зомбылықтан қорғау, суицидтер профилактикасы және олардың құқықтарын қамтамасыз ету» жоспарының аясында қарастырылған ұсыныстарды жүзеге асыруға бағытталғанын көрсетті [174].

Шетелдік тәжірибе: қосымшалар мен кодтар. Дамыған елдерде балалар қауіпсіздігін қамтамасыз ететін технологиялар кең қолданылады. Google Family Link қосымшасы арқылы ата-ана бала телефонын бақылап, қолданбалардың іске қосылуын шектеуге болады. Apple компаниясының экожүйесінде iOS құрылғыларына кіріктірілген Screen Time функциясы балалардың құрылғыдағы белсенділігін есептейді және жасы шектеулі мазмұнға кіру шектеулерін орнатады [180]. Құқық қорғау жағынан жаңа үрдіс - Ұлыбританияның Age Appropriate Design Code («Балалар кодексі»). 2020 жылы күшіне енген бұл заң бойынша кез келген онлайн-қызмет балаға лайықтанып жобалануға тиісті: міндетті түрде баланың жеке деректерін тек қана қажетті мөлшерде жинап, стандартты түрде «жеке деректерді қорғау» режимін қосу керек. Кодексте сондай-ақ балаларға арналған сайттар мен қолданбалар «қарақұмық қағидаларына» жол бермеуі, яғни алаяқтық пен мазмұнды манипуляциялау әдістерін пайдаланбауы шарт етілген [181].

Мазмұн деңгейінде YouTube компаниясы YouTube Kids атты бөлек платформасын шығарды. Бұл платформа балаларға лайықты, кураторлық тексерістен өткен бейнелер ұсынылатын қоршаған орта құрады. Ол 2015 жылы іске қосылып, басқа құрылғыларға да кеңейтілді, және 2021 жылы балалар ақпаратын жинау шектеулері бойынша талаптарға сай жұмыс істейді [181]. Осылайша ата-аналар контентті бақылап, қажетсіз жарнамадан сақтайды.

Тағы бір шетелдік мысал - ата-ана бақылау бойынша коммерциялық шешімдер. Мысалы, Net Nanny бағдарламасы ата-аналарға веб-сайттар мен қолданбаларды блоктауға, балалардың әлеуметтік желідегі әрекетін шолуға, уақыт шектеулерін орнатуға мүмкіндік береді. Аталмыш бағдарламаның веб-сайтында көрсетілгендей, Net Nanny «контентті сүзу технологиясы арқылы отбасыға лайықты мазмұнды қалдыра отырып, зиянды және қауіпті материалды тоқтатады». Bark қосымшасы да ата-аналарға кеңінен танымал: ол кибербуллинг, суицид және жыныстық сипаттағы қауіпті әрекеттерді хабарлайтын ескертулер береді. Бұл екі бағдарлама балалардың смартфон мен планшеттегі белсенділігін нақты мониторингілеуге және қажетсіз тәуекелдерді алдын-ала анықтауға көмектеседі.

Халықаралық ұсыныстар мен нормативтер. ЮНИСЕФ пен басқа халықаралық ұйымдар балалар қауіпсіздігін қорғауды басты міндет санайды. UNICEF балалардың цифрлық құқықтарын қорғау бойынша жаһандық бастамаларды жүзеге асырады және балалар интернеттегі зорлық-зомбылық пен жеке деректерді қорғаусыз жинаудан қорғауға шақырады. OECD 2025 жылғы баяндамасында 15 жасар оқушылардың 98%-ы смартфонға ие екендігі атап өтілді; бұл балалардың интернеттегі белсенділігінің жоғары екенін көрсетеді. OECD жаңа зерттеуі балаларға бағытталған саясат пен цифрлық қызметтерде «әдепкі бойынша ең жоғары» жеке өмірді қорғау шараларын қамтитын кең ауқымды тәсілді ұсынады. Сондай-ақ OECD дерегі бойынша OECD елдеріндегі 15 жасар шәкірттердің жартысы дербес параметрлерді пайдаланып қауіпсіздік баптауларын оңай өзгертеді, алайда 27,6%-ы анонимді түрде жалған ақпарат таратады екен. Яғни, балалардың өзін-өзі реттеу дағдылары жетілмеген, сондықтан үкіметтер цифрлық сауатты арттыру мен қауіпсіздік құралдарын әзірлеу қажеттігін мойындайды.

Шешімдерді заңнамалық жүйеге енгізу. Қазақстанда жоғарыда аталған халықаралық тәжірибені ескере отырып, құқық қорғау және білім беру саласында цифрлық қорғаныштың заңдық негіздерін нығайту ұсынылады. Мысалы, білім беру мекемелерінде интернет сүзгілерін міндетті орнату және жасалған цифрлық хаттамалармен мониторинг жүйесін енгізу қарастырылуы мүмкін. 2023-2025 жылдарға арналған қорғаныс жоспарына енгізілген ұсыныстар бойынша Үкімет алдында кәмелетке толмағандарды зиянды контенттен ізоляциялау шаралары талқылануда және қазір жүзеге асырылуда.

Мысалы, аталмыш жоспар шеңберінде «SIM KIDS» пилоттық жобасы іске қосылды [174], бұл - интернет қауіпсіздігіне жасалған нақты қадам. Алдағы уақытта мектептерге сандық фильтрлер мен керекті басқару интерфейстері орнатылып, мемлекеттік порталда балаларға мәліметтер алмасу ыңғайлы түрде автоматтандырылуы тиіс. Сондай-ақ контентпен жұмыс істейтін интернет-платформаларға жас бойынша тіркеуді міндеттеу (age-gate) енгізу ұсынылады, осылайша балалардың жасына сай емес материалдарға кездейсоқ жолығуына тосқауыл қойылады.

Жоғарыда аталған бастамалардың тиімділігіне пилоттық жобалар дәлел болып отыр. Мысалы, Павлодардағы Kaspersky Safe Kids жобасында отбасыларға Android және iOS құрылғыларына орнатылатын лицензиялар

беріліп, балаларды қорғайтын шектеулер енгізілді [179]. Ал Алматыдағы SIM KIDS жобасы ата-аналар тарапынан үлкен қолдау тауып, үлкен сұранысқа ие болуда [174]. «Kaspersky» зертханасының сауалнамасы көрсеткендей, балалардың басым бөлігі күніне бірнеше сағаттан артық интернетте отырады және ата-аналардың 36%-ы ұзақ экран алдында отырудан жанжал туындағанын мойындады [179]. Бұл статистика мектептер мен отбасы ортасында сандық тәртіптің маңыздылығын дәлелдейді. Пилоттық жобалардың нәтижелері бойынша алынған кері байланыс жастардың қауіпсіздігі мен тыныштығын арттыруға бағытталған технологиялардың әрі қарай дамуына негіз болады.

Интернет пен мобильдік құрылғылардың жаппай таралуы балалар өмірінің ажырамас бөлігіне айналды. UNICEF-тің «Балалық шақ цифрлық әлемде» зерттеуінде атап өтілгендей, бүгінде әлемдегі мектеп жасындағы балалардың үштен екісі (1,3 млрд бала) үйден интернетке қосыла алмайды, ал жоғары бай елдерде 15 жастағы жасөспірімдердің басым бөлігі үйде интернетке қол жеткізеді [182]. Ұлыбританияның Ofcom реттеушісі 2024 жылы жүргізген зерттеуінде 5-7 жас аралығындағы балалардың төрттен бірі смартфон иеленетінін, 76 %-ы планшет қолданатынын және үштен бірі әлеуметтік желіні ата-анасының қатысуынсыз пайдаланатынын көрсетті [183]. Бұл тенденциялар баланың жеке өмірі, психикалық денсаулығы мен қауіпсіздігіне жаңа қауіптер төндіріп, мемлекет пен коммерциялық сектор тарапынан ерекше қорғаныс шараларын қажет етеді.

OECD-нің 2025 жылғы баяндамасы цифрлық ортадағы балалардың өмірін сипаттайтын 45 индикаторды ұсынды. Баяндама бойынша, OECD елдеріндегі 15 жасөспірімдердің 98 %-ы смартфонға ие; олардың 51 %-ы құпиялық баптауларын қорғау үшін сандық параметрлерді оңай реттей алатынын айтса, 27,6 %-ы әлеуметтік желілерде жалған ақпарат бөлісетіні анықталған [184].

Бұл көрсеткіштер жасөспірімдердің цифрлық сауаттылығы толық қалыптаспағанын, ал жалған ақпарат тарату әдетке айналуы мүмкін екенін көрсетеді. Сондықтан жас балаларға арналған цифрлық саяси шаралар технологиялық шешімдерді, заңнамалық нормаларды және ағартушылық жұмыстарды үйлестіруді талап етеді.

Искусственный интеллект (AI) пен үлкен деректер (Big Data) технологиялары балаларды онлайн ортада қорғауда негізгі құралға айналды. Forbes журналы AI-дің зиянды контентті нақты уақыт режимінде анықтап, бала оны көрмей тұрып бөгеп тастайтынын атап өтеді. Платформалар AI-ды кибербуллинг белгілерін тану үшін пайдаланады; алгоритмдер қорлайтын немесе өшпенділік тудыратын пікірлерді жарияланар алдында анықтап, алаңдаушылық тудыратын жағдайда модераторға немесе ата-анаға ескерту жібереді [4]. AI-дың көмегімен Thorn және АҚШ-тағы Ұлттық жоғалған және қанаушылыққа ұшыраған балалар орталығы (NCMEC) сияқты ұйымдар балаларға қатысты жыныстық зорлық-зомбылық материалдарын анықтап, алаң иелерінен жоюды талап етеді, нәтижесінде құрбандарды құтқару жеңілдейді [185].

AI балаларды интернет-алаяқтардан қорғау үшін білім беруге де қолданылады. Вирджиния политехникалық институты зерттеушілерінің жобасы әлеуметтік инженерияға қарсы тұруды үйрететін AI-чатботтар жасауды көздейді. Жасанды интеллект бала мен онлайн жыртқыш арасында рөлдік диалог құрып, онлайн танысу кезіндегі «груминг» тактикаларын анықтауды үйретеді [5]. Зерттеуде 2021 жылғы сауалнама нәтижелері келтіріліп, жасөспірімдердің 15,6%-ы онлайн жыныстық қиянатқа тап болғанын және 11%-ы суретке негізделген жыныстық зорлық-зомбылықтың құрбаны екенін көрсеткен [186]. Мұндай чатботтар балаларға онлайн қауіптерді ерте анықтап, дербес қорғану дағдысын дамытуға мүмкіндік береді.

БҰҰ-ның Есірткі және қылмыс жөніндегі басқармасы (UNODC) мен халықаралық ұйымдар адам саудасы желілерін анықтау үшін AI және деректерді талдау құралдарын қолданады. UNODC басшысы Гада Валидің айтуынша, құқық қорғау органдары машиналық оқыту, деректерді терең талдау және басқа да технологиялар көмегімен сауда желілерін анықтап, қылмыстарды зерттей алады [6]. Love Justice International ұйымы спутник суреттері және OpenStreetMap деректерін біріктіріп, ықтимал трафик маршруттарының «жылу карталарын» құрып, машиналық оқыту арқылы «қызыл жалаушалар» белгілерін анықтайды; бұл әдіс бірнеше мың адамды құлдықтан құтқаруға мүмкіндік берген. Мұндай тәсілдер балаларды қылмыс құрбаны болудан қорғау үшін тиімді [187, с. 27].

Қатаң деректерді қорғау ережелері (GDPR, COPPA және т. б.) контентке кіруді жас бойынша шектеуді талап етеді. Дәстүрлі жас тексеру әдістері төлқұжат немесе кредит картасы сияқты сезімтал деректерді енгізуді қажет етеді, бұл киберқылмыскерлер үшін тартымды нысана. Сол себепті бірқатар стартаптар блокчейн негізіндегі жас-тексеру жүйелерін ұсынуда. Concordium компаниясы жасырын білім дәлелдері (Zero-Knowledge Proofs) арқылы қолданушының жасын растауға, бірақ жеке мәліметін ашпауға мүмкіндік беретін шешім әзірледі. Мақалада қазіргі жүйелердің осал тұстары - компаниялар қолданушы туралы тым көп деректер жинайтыны және оларды қорғауға кепілдік бере алмайтыны - атап өтіледі [7]. Concordium жүйесі қолданушыға «жасын растайтын сандық растау» береді, оны қосымшалар жасқа сай емес контентті ашпас бұрын тексеріп, бірақ адамның нақты аты-жөнін, мекен-жайын жарияламайды [188].

Segpay мақаласы блокчейннің қауіпсіздік артықшылығын атап өтеді: бастапқы жас тексерісінен кейін пайдаланушының жасы шифрланып, блокчейнге жазылады; кейінірек ол бірегей токен арқылы жасын дәлелдей алады, бірақ басқа жеке деректері жарияланбайды [189]. Бұл жүйе цензурасыз, орталықсыздандырылған, ал ең бастысы - дербес мәліметтердің жоғалу қаупін азайтады.

Ұлыбритания 2020 жылы күшіне енген «Балаларға арналған дизайн кодексін» қабылдады. Осы кодекс бойынша кез келген онлайн-қызметтің өз өнімін балаға лайықтап жобалауы міндет: деректерді мүмкіндігінше аз көлемде жинау, әдепкі түрде жеке өмірді қорғау параметрлерін қосу,

геолокацияны өшіру және балаға түсінікті етіп хабарлама беру [190]. California штаты 2022 жылы осы кодекстен үлгі алып, Age-Appropriate Design Code Act қабылдады; ол 18 жастан төмен пайдаланушыларға бағдарланған қызметтерге жасанды жасты анықтау жүйелерін енгізуді, ықтимал зиянды контенттен қорғауды және жасырын жарнамалық модельдерді пайдаланудан бас тартуды міндеттейді [191]. Мұндай заңдар жасөспірімдердің құқықтарын сақтауда маңызды.

Net Nanny - ата-аналарға арналған коммерциялық бағдарламалық жасақтама. Ол жасанды интеллект арқылы қауіпті контентті нақты уақытта сүзеді, яғни бала оны көрмей тұрып блоктайды [11]. Бағдарлама экран уақытын басқару, қосымшаларды бұғаттау, веб-сайттарды сүзу және мазмұнды санаттар бойынша шектеу мүмкіндіктерін ұсынады. Net Nanny-дің Family Feed функциясы ата-аналарға баласының іздеу сұрауларын және қолданатын қосымшаларын нақты уақытта хабарлайды, сондай-ақ порнография, зорлық-зомбылық немесе есірткі жөніндегі іздеулер туралы ескерту жасайды [192].

Google Family Link - Android және ChromeOS құрылғыларына арналған ақысыз бақылау құралы. Ол ата-анаға баланың экран уақытын шектеуге, School Time немесе Downtime тәртіптерін орнатуға мүмкіндік береді. Family Link арқылы әрбір қосымшаға бөлек уақыт шектеулерін қою немесе бағдарламаны толық бұғаттау мүмкін [12]. Бағдарлама Chrome, Play Store, YouTube және Google Search қызметтерінде жасқа сай контент сүзгілерін басқарып, жаңа қосымшаларды орнатуға ата-ананың мақұлдауын талап етуге мүмкіндік береді [193].

Apple экожүйесіндегі Screen Time функциясы iOS құрылғыларында орнатылған. Қолданба апта сайын баланың белсенділігі туралы есеп беріп, қандай бағдарламалар көп уақытты алатынын көрсетеді. Ата-ана «Downtime» уақытын белгілеп, баланың үй тапсырмасы немесе ұйқы кезінде құрылғыны пайдалануды шектей алады. Сондай-ақ мазмұнды сүзу, жасы шектеулі фильмдер мен сайттарды бұғаттау және App Store-дан жүктеу кезінде рұқсат талап ету мүмкіндігі бар [194].

Bark платформасы әлеуметтік желілер мен мессенджерлердегі хабарламаларды сараптап, кибербуллинг, суицид және жыныстық сипаттағы қауіп туралы ескертулер береді. Qustodio және Norton Family сияқты қосымшалар да экран уақытын басқару және мазмұнды сүзу бойынша ұқсас функцияларды ұсынады. Бұл коммерциялық шешімдер көбіне ақылы, бірақ кеңейтілген бақылау мен есеп беру қызметтері бар.

Қазақстанның электрондық үкіметі (eGov) мобильдік қосымшасына пандемия кезеңінде Ashyq жүйесі енгізіліп, QR-код арқылы қоғамдық орындарға кіру мәртебесін көрсету мүмкін болды. Қосымшада түстерге бөлінген мәртебе (жасыл, көк, сары, қызыл) COVID-ке байланысты қауіп деңгейін білдіреді [195]. Бұл тәжірибе жастардың денсаулығын бақылау және қоғамдық ғимараттарға кіруді цифрлық тәсілмен реттеу бойынша үлгі болып, болашақта жасөспірімдерге арналған порталда қолданылуы мүмкін.

eGov Mobile-да «Ұлттық қор - балаларға» және «Балалар туралы мәліметтерді өзектендіру» модульдері іске қосылған. Ата-ана баланың туу туралы куәлігін жүктеп, мемлекеттік қолдау алуға өтініш бере алады; өтініш 2-5 күнде өңделеді [195]. Бұл сервис балаларға қатысты деректерді бір орталықта жинақтап, атаулы әлеуметтік көмек пен қолдау алу процесін жеңілдетеді.

2024 жылы Павлодар облысында әкімдік пен «Kaspersky» компаниясы «Kaspersky Safe Kids» қосымшасын тегін тарату бойынша пилоттық жоба өткізді. Лицензиялар құқық бұзушылық жасаған жасөспірімдер мен әлеуметтік әлсіз отбасыларға берілді, бағдарлама веб-ресурстарды сүзуге және экран уақытын шектеуге мүмкіндік берді. Пилот нәтижесінде ата-аналардың 36 %-ы баласының ұзақ уақыт экран алдында отыруы жанжалға әкелгенін мойындады; балалардың 56 %-ы интернетте күніне 1-4 сағат өткізеді, ал 23 %-ы бос уақытының көбін онлайн өткізеді [15]. Қатысушылар қосымшаның қарапайым орнатылуы, қажетсіз сайттарға кірудің азаюы және уақыт шектеулерінің тиімділігі туралы оң пікір білдірді [196]. Бұл жоба ата-аналарға цифрлық бақылау құралдарын қолданудың тиімділігін көрсетіп, республикалық деңгейде енгізуге негіз болды.

2025 жылы Алматыда Tele2/Altel компаниясымен бірлескен «SIM KIDS» пилоттық жобасы басталды. Жоба арнайы SIM-картаны пайдаланып, суицид, порнография, есірткі және құмар ойындар сияқты зиянды контентті автоматты түрде блоктайды. Карта ата-ананың балалар қолданатын қосымшаларды көруіне, қажет жағдайда сайттарға кіруді шектеуге және телефон үнсіз режимде болса да балаға қоңырау шалуға мүмкіндік береді [197]. Жоба зорлық-зомбылық пен суицидтің алдын алу жөніндегі мемлекеттік бағдарлама аясында жүзеге асырылып, ата-аналар арасында үлкен қызығушылық тудырды.

ЮНИСЕФ Қазақстан, Еуропалық одақ және ҚР Білім министрлігінің Балалар құқықтары комитеті бірлесіп «Cyber Tumar» (Кибер Тұмар) ақпараттық-білім беру науқанына бастамашы болды. Науқанның мақсаты - балаларды кибербуллинг, онлайн қуғын-сүргін, балаға арналмаған мазмұн және интернет-тәуелділік сияқты қауіптер туралы хабардар ету, сонымен бірге балалардың жеке өмірі мен деректерін қорғауға үйрету. Науқан аясында семинарлар мен ата-аналарға арналған оқу материалдары ұсынылып, Kaspersky зертханасы сарапшылары ата-аналардың баламен ашық сөйлесіп, интернеттегі уақытын бақылауға, қажетсіз сайттарды бұғаттауға және қауіп туғанда модераторларға хабарласуға кеңес берді.

Басқа бастамалар:

- Ashyq жүйесін 12+ жасқа енгізу. COVID-19 пандемиясында компьютерлік клубтар, кинотеатрлар және басқа да орындарға кіру үшін 12 жастан асқан балалардың Ashyq қосымшасына тіркелуі міндеттелді. Бұл жастардың денсаулығын бақылау және деректерді цифрлық растау тәжірибесін қалыптастырды.

- eGov Mobile-дың бала модульдері. «Балалар туралы мәліметтерді өзектендіру» қызметі арқылы ата-аналар баланың негізгі құжаттарын тіркеп, оларды жаңарта алады [198].

- Жоғары деңгейдегі сим-карта мен фильтрлер. Павлодардағы Safe Kids және Алматыдағы SIM KIDS сияқты пилоттар зиянды контентті сүзуге және жасқа сай шектеулер орнатуға мүмкіндік берді [196], [197].

Халықаралық тәжірибе және ұсыныстар

- YouTube Kids және реттелетін платформалар. Google компаниясы балаларға арналған YouTube Kids платформасын әзірледі; онда бейнелер кәсіби модерациядан өтеді және ата-ана мазмұнды сүзгілеу параметрлерін орната алады. Бұл платформа АҚШ-та COPPA талабына сәйкестендірілген.

- Age-Appropriate Design Code (Ұлыбритания). Кодекс онлайн-қызметтерге балалардың мүддесін бірінші орынға қоюды міндеттейді, деректерді жинауды минималды деңгейде ұстап, геолокацияны өшіру және әдепкі құпиялылық баптауларын енгізуді талап етеді [199].

- Ofcom зерттеулері. 2024 жылғы Ofcom зерттеуі 5-7 жас аралығындағы балалардың төрттен бірінде смартфон бар екенін, ал осы жас топтағы балалардың үштен бірі әлеуметтік желіні ата-анасының қатысуынсыз пайдалана бастағанын анықтады [183]. Бұл балалардың онлайнда ерте және дербес болуы киберқауіпсіздікті нығайтуды талап етеді.

- OECD деректері. 98 % 15 жасөспірімдер смартфон иеленеді, бірақ олардың тек жартысы ғана құпиялық баптауларын қорғауды біледі, 27,6 %-ы жалған ақпарат таратады және 17% -ы телефонсыз мазасызданатынын айтты [200]. Бұл статистика балалардың цифрлық ортада қалай әрекет ететінін түсініп, тиісті саясат әзірлеу үшін маңызды.

Заңнамалық және ұйымдастырушылық ұсыныстар

1. Мектептерде міндетті контент сүзгісі. Мемлекеттік және жеке оқу орындары интернетке қол жетімділікті орталықтандырылған сүзгілер арқылы қамтамасыз етуі керек; сүзгілер зиянды контент, порнография немесе құмар ойын сайттарын автоматты түрде бұғаттауы тиіс. Бұл жүйе Net Nanny немесе Kaspersky Safe Kids сияқты технологияларға негізделуі мүмкін. Педагогтар мен IT-мамандар фильтрлердің тиімділігін бақылап, кері байланыс беріп отыруы қажет.

2. Блокчейн-негізіндегі жас verifikatsiya. Балаларға арналған онлайн сервистер жасты растаудың сенімді әдістерін енгізуі тиіс. Concordium сияқты платформалардың тәжірибесін пайдаланып, zero-knowledge proofs арқылы «жасына сай» екендігін дәлелдеудің ұлттық стандарты жасалуы мүмкін [188]. Мұндай жүйе балалардың жеке деректерінің таралуын шектеп, интернет-платформаларға 18 жастан кіру талаптарын орындауға мүмкіндік береді.

3. Ата-аналарға арналған цифрлық сауаттылық бағдарламалары. Cyber Tumar науқаны сияқты іс-шараларды кеңейтіп, ата-аналарға AI-фильтрлерді баптау, балалармен ашық сөйлесу және қауіп төнгенде қайда жүгіну керектігі туралы түсіндіру қажет. Әлеуметтік қызметкерлер мен мектеп психологтары бұл бағдарламаларға қосылып, отбасылық деңгейде қолдау көрсетуі тиіс.

4. Заңнаманы күшейту. Қазақстан 2023-2025 жылдарға арналған балаларды қорғау жоспарына сәйкес, «SIM KIDS» жобасы сияқты пилоттарды заңнамалық негізге енгізу, сандық хаттамалар мен мониторинг жүйесін жасау қажет. Сонымен қатар, интернет-платформаларды балалардың жасына сәйкес тіркеу (age-gate) жүйесін енгізуге міндеттеу ұсынылады.

5. Деректерді зерттеу және мониторинг. OECD, Ofcom және UNICEF зерттеулерінде көрсетілгендей, балалардың экран алдында өткізетін уақыты мен интернеттегі тәжірибесі туралы деректер әлі де жеткіліксіз [200]. Үкімет жүйелі түрде сауалнамалар өткізіп, мектептер мен отбасы деңгейінде балалардың цифрлық әдеттерін зерттеуі керек. Бұл деректер саясат пен технологиялық шешімдерді әзірлеуде қолданылады.

Интернет пен сандық технологиялар балалардың өміріне теңдессіз мүмкіндіктер әкеледі, бірақ олардың құқықтары мен қауіпсіздігін қорғау үшін кешенді және инновациялық тәсілдер қажет. Жасанды интеллекттің контентті сүзу мүмкіндігі, деректер талдау арқылы қылмыс желілерін анықтау, блокчейн-негізіндегі жас жүйелері, ата-аналық бақылау қосымшалары және цифрлық үкімет сервистері - осының бәрі бала құқықтарын қорғаудың заманауи құралдары болып табылады. Қазақстандық тәжірибе халықаралық трендтен кейін қалмай, зиянды контентпен күресуге және балалардың сандық сауаттылығын арттыруға бағытталған нақты қадамдар жасап отыр. Құқықтық нормаларды жетілдіру, білім беру бағдарламаларын кеңейту және технологиялық инновацияларды енгізу арқылы Қазақстан балалардың цифрлық әлемде қауіпсіз өсуін қамтамасыз ете алады.

Қорыта айтқанда, жасанды интеллект, ірі деректер, блокчейн, жас мөлшерін анықтау жүйелері мен ата-ана бақылау құралдары кәмелетке толмағандарды цифрлық ортада қорғаудың жаңа арсеналы болып отыр. Қазақстандық тәжірибе де осы үрдістен алыстап қалмады: eGov Mobile сервисіне енгізілген бала модульдері, Ashyq жүйесін балалыққа бейімдеу, Safe Internet бағытындағы бастамалар, сондай-ақ Kaspersky Safe Kids пен SIM KIDS сияқты пилоттар - бұлардың бәрі балалар қауіпсіздігін қамтамасыз етуге бағытталған нақты шаралар. Халықаралық тәжірибе мен ұсыныстарды ескере отырып, Қазақстанда мектептерде цифрлық сүзгілерді міндеттеу, жастарды қорғауға қатысты жаңа құқықтық нормаларды қабылдау, мектеп пен ата-анаға цифрлық сауаттылықты арттыру бойынша білім беру бағдарламаларын кеңейту қажет. Мұндай кешенді іс-шаралар балалардың онлайндық құқықтарын мүлтіксіз сақтауға және олардың цифрлық әлемде қауіпсіз өсуіне зор септігін тигізеді.

## Қорытынды

Ақпараттық-коммуникациялық технологиялардың кең таралуы кәмелетке толмағандардың интернетті күнделікті белсенді пайдалануының артуына ықпал етіп, кибер құқық бұзушылықтардың өсуіне себепші болды. Сандық ортаға кірудің жеңілденуі мен гаджеттердің әрбір отбасы қолына түсуі салдарынан жасөспірімдер арасында сандық алаяқтық, жеке деректерді ұрлау, кибербуллинг сияқты құқық бұзу әрекеттері жиілеп келеді. Бұл үрдіс Қазақстан үшін де өзекті, себебі еліміздегі интернет қолданушылардың шамамен жартысынан көбі - 18 жасқа дейінгі балалар мен жасөспірімдер.

Әсіресе пандемия кезеңінде қашықтан оқу мен әлеуметтік желілерді белсенді қолданудың нәтижесінде балалар интернеттегі қауіпті жарнамалар мен алаяқтық құрбаны болуы ықтималдығы артты. Заманауи қоғамдағы цифрлық трансформация процестері ақпараттық қауіпсіздікке жаңа сынақтар туғызып отыр. Халықаралық сарапшылар интернеттегі алаяқтық пен зорлық-зомбылықтың жылдам артуын атап, балаларды қорғаудың маңыздылығын баса айтты. Қазақстандық құқық қорғау практикасы да жоғарыда айтылған қауіп-қатерлерді растап, кәмелетке толмағандардың кибер құқық бұзушылықтарына қатысты әкімшілік-құқықтық реттеудің жетілдіруін талап ететіндігін көрсетіп отыр. Осы тұрғыда аталған тақырыптың өзектілігі артып, ғылыми зерттеуді қажет етеді.

Жұмыстың теориялық және практикалық міндеттері нақты қойылып, оларды шешу үшін қажетті әдістемелік негіздер анықталды. Теориялық міндеттер аясында кәмелетке толмағандардың кибер құқық бұзушылықтарының ұғымдық мазмұны ашылып, оның ғылыми-теориялық негіздері қалпына келтірілді; жасөспірімдердің сандық ортада құқық бұзу әрекеттеріне әсер ететін әлеуметтік және технологиялық факторлар талданды.

Практикалық міндеттер ретінде ҚР заңнамасындағы осы бағытты талдап, кәмелетке толмағандардың кибер құқық бұзушылықтарына қатысты әкімшілік-құқықтық және қылмыстық жауапкершілік нормаларының жағдайы зерттелді; құқық қорғау органдарының статистикалық деректері мен іс-әрекет тәжірибесі сарапталды; және алынған нәтижелер негізінде құқықтық кеңестер мен ұсынымдар әзірленді. Зерттеу әдістеріне құқықтық талдау (нормативтік актілерді зерделеу), салыстырмалы-ұқсастырмалы талдау (қолданыстағы заң актілері мен халықаралық тәжірибелерді салыстыру), жалпы ғылыми әдістер (индукция, дедукция, жүйелік талдау, салыстырмалы-талдау, синтез) мен құқықтық статистикалық мәліметтерге талдау және мамандардың сауалнамасы кірді. Осылайша, алға қойылған теориялық және практикалық міндеттердің барлығы толықтай шешілді деуге негіз бар.

Бірінші тарауда кәмелетке толмағандардың кибер құқық бұзушылықтарын анықтау мен жіктеу мәселелері жан-жақты қарастырылды. Онда «кіберқұқық бұзушылық» ұғымы кең көлемде түсіндіріліп, оның құрамдас элементтері мен түрлері құрылымдық түрде жүйелендірілді. Зерттеу нәтижесіне сәйкес, жасөспірімдер арасында кездесетін кибер құқық

бұзушылықтар қатарына ақпараттық жүйелерге заңсыз кіру (мысалы, сүйреп әкету және парольдерге шабуыл жасау), цифрлық форматтағы жеке мүлікті ұрлау, желіде алаяқтық жасау (әлеуметтік желіде қаражат ұрлау, виртуалды ойындардағы ресурстарды ұрлау), сонымен қатар кибервирустар тарату мен жасанды ақпарат тарату тәрізді сандық сипаттағы әрекеттер жатады.

Сонымен қатар, жасөспірімдердің мұндай әрекеттеріне олардың цифрлық сауатсыздығы, қадағалаудың болмауы және әлеуметтік орта әсер ететіні талданды. Осы тарау қорытындысында жасөспірімдердің кибер құқық бұзушылықтары ерекшеліктерін ескере отырып, оларға қарсы профилактикалық және тәрбиелік шаралар жүйесін жетілдіру қажеттігі атап өтілді.

Екінші тарауда Қазақстан Республикасының әкімшілік-құқықтық реттеу жүйесі аясында кәмелетке толмағандардың кибер құқық бұзушылықтарына қатысты заңдылықтар зерттелді. Бұл тарауда Әкімшілік құқық бұзушылық туралы кодекс пен Қылмыстық кодекстің тиісті баптары кеңінен талданып, олар халықаралық стандарттармен салыстырылды. Зерттеу қорытындысы бойынша Әкімшілік кодексте киберқорқыту, цифрлық алаяқтық сияқты желілік құқық бұзушылықтарды сипаттайтын жеке баптардың жоқ екені анықталды; яғни, әкімшілік құқық бұзушылықтар саласында сандық қатынастарға қатысты құқықтық реттеу әлсіздігі байқалды. Қылмыстық кодексте электрондық алаяқтық және ақпараттық жүйеге заңсыз кіру тәрізді қылмыстар қарастырылғанымен, олар жасөспірімдерге қатысты қолданған кезде жас ерекшеліктерін ескеріп жазалау тетіктерін қамтымайды.

Сонымен қатар, құқық қорғау тәжірибесі көрсеткендей, жасөспірімдердің киберқылмыстары бойынша тергеп-тексеру ісі мен өндірістік процестерде жаза шараларын жұмсарту және түзету шараларын қолдану мәселелері туындайды. Осыдан кәмелетке толмағандар тарапынан жасалған киберқылмыстарды әкімшілік-құқықтық тұрғыдан реттеудің құқықтық шектеулері айқындалды.

Үшінші тарауда практикалық аспектілер қарастырылып, кәмелетке толмағандардың кибер құқық бұзушылықтарын алдын алу мен құқық қорғау шараларын жетілдіруге арналған нақты ұсынымдар әзірленді. Зерттеу нәтижелері негізінде бірнеше кешенді шаралар ұсынылды. Біріншіден, білім беру жүйесінде цифрлық сауаттылық пен интернет қауіпсіздігін арттыру мақсатында арнайы оқу бағдарламаларын енгізу - мектептер мен колледждерде жаңа пәндер немесе факультатив сабақтар ашу қажетлігі көрсетілді. Екіншіден, ата-аналар мен мұғалімдерге арналған ақпараттық-түсіндіру іс-шаралары ұйымдастыру ұсынылды: мысалы, ата-аналар жиналыстарында интернеттегі қауіптер туралы арнайы баяндамалар өткізу, мектеп психологтары мен тәрбиешілерге арналған тренингтер жүргізу.

Үшіншіден, құқық қорғау органдары саласында жасөспірімдермен жұмыс істеу үшін жаңа әдістемелік нұсқаулықтарды әзірлеу қажет: олардың психологиялық және әлеуметтік ерекшеліктерін ескере отырып, тергеу амалдарын жұмсарту және түзету бағдарламаларын қолдану ұсынылды. Сонымен қатар, мемлекет пен жеке сектордың ынтымақтастығы негізінде

балалар мен жасөспірімдерді цифрлық алаяқтықтан қорғауға бағытталған ақпараттық науқандарды жыл сайын өткізу міндеттелді. Бұл тараудағы ұсыныстар орындалса, жасөспірімдердің кибер құқық бұзушылықтарының алдын алуға бағытталған іс-әрекеттер тиімді жүзеге асады деп бағаланды.

Ғылыми жаңалық тұжырымдары: Біріншіден, «кәмелетке толмағандардың кибер құқық бұзушылықтары» ұғымы кешенді талдау негізінде алғаш рет нақты анықталып, оның құрамдас элементтері мен түрлері құрылымдық түрде жүйелендірілді. Екіншіден, Қазақстан Республикасының нормативтік-құқықтық базасын жан-жақты талдау нәтижесінде кәмелетке толмағандардың кибер құқық бұзушылықтарына қатысты заңнамалық бос тұстар мен қайшылықтар ашық сипатталды.

Үшіншіден, жасөспірімдердің кибер құқық бұзушылықтарын алдын алу мен құқық қорғауды жетілдіруге арналған кешенді ұсынымдар әзірленді; олардың ішінде заңнамаға түзетулер енгізу, білім беру бағдарламаларын жаңарту, құқық қорғау әдістемесін жетілдіру сияқты шаралар қамтылды. Сонымен қатар, жасөспірімдердің кибер құқық бұзушылығына бейімділігін ескеретін әлеуметтік-психологиялық және құқықтық әсер ету тетіктері ұсынылды, бұл еңбек тақырыбына бұрын қарастырылмаған жаңа ғылыми тұжырымдар әкелді.

Ұсыныстар мен қолданбалы мән: Зерттеу нәтижелері Қазақстан Республикасының заңнамасын жетілдіруде пайдаланылуы мүмкін нақты ұсыныстарды ұсынады. Мысалы, Әкімшілік құқық бұзушылық туралы кодекске кибербуллинг, онлайн алаяқтық пен цифрлық алаяқтық тәрізді жаңа құқық бұзу түрлерін енгізу; Қылмыстық кодекске жасөспірімдердің кибер құқық бұзушылықтарына байланысты арнайы тармақтар енгізу (мысалы, жазаны жеңілдету немесе түзету шараларын қарастыру) ұсынылды.

Сонымен бірге, зерттеу материалдары құқық қорғау органдарының профилактикалық және тергеу қызметінде, сондай-ақ білім беру саласында қолданбалы сипатқа ие. Полиция қызметкерлері мен мектеп психологтары, әлеуметтік педагогтер, тәрбиешілер үшін арнайы әдістемелік нұсқаулықтар әзірлеу және оқыту тренингтерін ұйымдастыру ұсынылды. Бұл іс-шаралар арқылы мектептерде интернет қауіпсіздігі бойынша оқу процесін енгізу, ата-аналар мен балаларға арналған цифрлық сауаттылық курстарын дамыту сияқты әрекеттер күшейтіледі. Нәтижесінде, аталған ұсынымдар кәмелетке толмағандарды интернетте кездесетін қауіптерден қорғауды күшейтуге, құқық бұзушылықтардың алдын алуға нақты үлес қоса алады.

Қазақстан жағдайында әрі қарай зерттеуді қажет ететін бағыттар анықталды. Біріншіден, цифрлық технологиялардың қарқынды дамуы жаңа заңсыз іс-әрекеттер формаларын туындатуда, сондықтан осы заманауи қылмыстарды құқықтық реттеуді тұрақты түрде жаңартып отыру қажет. Мысалы, жасанды интеллект пен виртуалды шындық (VR) технологияларын қолдану арқылы жасалатын алаяқтықтар, блокчейн және криптовалюта құралдарын пайдаланып жасалатын қылмыстар сияқты жаңа тенденцияларға құқықтық жауап әзірлеу өзекті. Екіншіден, жасөспірімдердің интернеттегі белсенділік деңгейі мен олардың психологиялық-әлеуметтік жағдайы

арасындағы байланысты терең зерттеу маңызды. Бұл бағытта цифрлық тәуекелдерді бағалау әдістерін әзірлеп, жасөспірімдерді онлайнда құқық бұзу әрекетінен сақтайтын мінез-құлық модельдерін қалыптастыру қажет.

Сонымен қатар халықаралық тәжірибе мен цифрлық білім беру бағдарламаларын бағалап, балаларды интернет қауіптерінен қорғау бойынша ұлттық стратегияны жетілдіру бойынша ғылыми зерттеулер жүргізу артық болмайды.

Қорыта айтқанда, диссертациялық зерттеу қойылған мақсат-міндеттердің барлығын толық шешіп, кәмелетке толмағандардың кибер құқық бұзушылықтары мәселесіне жан-жақты ғылыми-практикалық көзқарас ұсынды. Зерттеу нәтижесінде жасөспірімдердің интернет кеңістігіндегі құқық бұзу әрекеттерінің табиғаты мен себептері тереңнен талданып, әр тарау қорытындысында нақты ғылыми тұжырымдар мен авторлық ұсынымдар берілді. Аталған қорытындылар мен ұсыныстар Қазақстан Республикасының нормативтік-құқықтық жүйесін жетілдіруге, балаларды интернет қауіптерінен қорғауға бағытталған іс-шараларды дамытуға практикалық үлес қосады.

Бұл жұмыс балалар мен жасөспірімдерді ақпараттық ортадағы құқық бұзушылықтардан қорғау ісінде қолданылатын мемлекеттік және педагогикалық іс-шараларды жетілдіруге бағытталған кешенді ұсыныстар береді.

## ПАЙДАЛАНЫЛҒАН ДЕРЕККӨЗДЕР ТІЗІМІ


1. Профилактику правонарушений среди подростков проводит полиция в Костанайской области. Polisia.kz, 17 сентября 2024. [Электрондық ресурс]. - Access mode: https://polisia.kz/ru/profilaktiku-pravonarushenij-sredi-podrostkov-provodit-politsiya-v-kostanajskoj-oblasti/
2. Мухаметгали Ф. Какую ответственность несут родители за проступки несовершеннолетних детей // Polisia.kz. - 17 августа 2023. - URL: https://polisia.kz/ru/kakuyu-otvetstvennost-nesut-roditeli-za-prostupki-nesovershennoletnih-detej/ (дата обращения:10.10.2024).
3. Кибер-Тұмар: создание безопасного цифрового пространства для каждого ребенка // UNICEF Kazakhstan. -. URL: https://www.unicef.org/kazakhstan/кибер-тұмар-создание-безопасного-цифрового-пространства-для-каждого-ребенка (дата обращения:10.10.2024).
4. Stickings M., Nosal J. Blunting the cutting edge of crime: OSCE helps combat cybercrime in Central Asia // *Blog OSCE*. - 2 сентября 2024. - URL: https://www.osce.org/blog/574757 (дата обращения:10.10.2024).
5. Zhumabekova K., Otarbayeva A., Yelubayev A., Abizhanov S., Kegembayeva Z. *Ensuring children's online safety in Kazakhstan: balancing protection from harm with rights to information access* // Security and Human Rights Monitor. - 5 марта 2024. - URL: https://www.shrmonitor.org/ensuring-childrens-online-safety-in-kazakhstan-balancing-protection-from-harm-with-rights-to-information-access/ (дата обращения:10.10.2024).
6. За кибербуллинг детей в Казахстане теперь начнут наказывать штрафами // Центр цифровых прав. - 2024, 16 апреля. - URL: https://kz.drc.law/blog/za-kiberbulling-detey-v-kazakhstane-teper-nachnut-nakazyvat-shtrafami/ (дата обращения:10.10.2024).
7. Қазақстанда балаларға интернет арқылы зорлық-зомбылық жасаған фактілер көбейген // Qazaqstan TV. - 11 қараша 2023. - URL: https://qazaqstan.tv/news/156175/ (дата обращения: 10.10.2024).
8. «Об административных правонарушениях» (Кодекс РК). Статья 66. - URL: https://kodeksy-kz.com/ka/ob_administrativnyh_pravonarusheniyah/66.htm (дата обращения:10.10.2024).
9. Alliant Private Client. *The Risks Parents Face When Their Child Bullies*. - 2024. - URL: https://alliantprivateclient.com/articles/the-risks-parents-face-when-their-child-bullies/ (дата обращения:10.10.2024).
10. Правительство Германии проигрывает кибербуллингу: как власти пытаются бороться с онлайн-агрессией // Хабр. - 16 сентября 2023. - URL: https://habr.com/ru/news/579986/ (дата обращения:10.10.2024).
11. South Korea under pressure to crack down on cyberbullying after high-profile deaths // *The Guardian*. - 9 февраля 2022. - URL: https://www.theguardian.com/world/2022/feb/09/south-korea-under-pressure-to-crack-down-on-cyberbullying-after-high-profile-deaths (дата обращения:10.10.2024).

12. Детский мир: «Я никому ничего не должен!» / Вилена Краснитская. - 26 ноября 2022 - URL: https://www.mklat.lv/zhizn/3031-detskij-mir-ya-nikomu-nichego-ne-dolzhen.html (дата обращения:10.10.2024).
13. Әлеуметтік желілер бұғаттала ма - кибербуллинг туралы заң жобасы Мәжіліске қайтарылды // Sputnik Қазақстан. - 14 сәуір 2022. - URL: https://sputnik.kz/20220414/aleumettik-zheli-kiberbulling-zan-24194630.html (дата обращения: 10.10.2024).
14. ҚазАқпарат. Қазақстан ақпарат агенттігі. 18 наурыз 2017 ж. - [Электрондық ресурс]. - Қол жеткізу режимі: https://kaz.inform.kz/news/aziyada-kameletke-tolmagandar-isteri-zhonindegi-algashky-sotty-kazakstan-ashty-sayhanov_a3009255/
15. Қазақстан Республикасының Бала құқықтары туралы конвенцияны іске асыруы туралы төртінші кезеңдік баяндама. Қазақстан Республикасы Үкіметінің 2011 жылғы 31 қазандағы № 1242 қаулысы. - [Электрондық ресурс]. - Қол жеткізу режимі: https://adilet.zan.kz/kaz/docs/P1100001242#:~:text=Қазақстан%20Республикасы%201994%20жылғы%208,белгіленген%20тәртіппен%20Қазақстан%20Республикасының%20Бала
16. Ответственность родителей за противоправные действия несовершеннолетних. - [Электронный ресурс]. - Режим доступа: https://www.gov.kz/memleket/entities/mvd-pavlodar/press/news/details/604585#:~:text=Қазақстан%20Республикасының%20Конституциясына%2C%20«Неке%20%28ерлі,құқығы%20мен%20міндеті%20болып%20табылады
17. «Отбасылық сот» жобасы шаңырақты сақтауды көздейді. 17 ноября 2021 г. - [Электрондық ресурс]. - Қол жеткізу режимі: https://nege.kz/amp/otbasilik_sot_zhobasi_shanirakti_saktaudi_kozdeidi_20211117153049
18. Карипбаев Ж.Б. Issues of holding juvenile offenders accountable for administrative violations in the Republic of Kazakhstan // Қазақстан Республикасы Конституциясының 30 жылдығына арналған «Адам мен азаматтардың құқықтары мен бостандықтарын қорғау және заң үстемдігін қамтамасыз етудегі конституциялық құқық механизміндегі ішкі істер органдарының рөлі» халықаралық ғылыми-практикалық конференция материалдары (13 маусым 2025 ж.). - Қарағанды: ҚР ІІМ Б. Бейсенов атындағы Қарағанды академиясы, 2025. - Б. 93-95.
19. Асылханұлы Б. Он алты жасқа толмаған адаммен жыныстық қатынас немесе сексуалдық сипаттағы өзге де әрекеттер жасаудың қылмыстық-құқықтық және криминологиялық сипаттамасы: [Магистрлік диссертация]. - Қосшы, 2022. - 103 б. - [Электрондық ресурс]. - Қол жеткізу режимі: https://academy-rep.kz/uploads/23be1024753a018c7d0011c754407a4b.pdf
20. Хромова Н.М. Правовые механизмы защиты прав несовершеннолетних в цифровой среде // *Вопросы ювенальной юстиции*. - № 04/2024. - [Электронный ресурс]. - Режим доступа:

https://lawinfo.ru/articles/8261/pravovye-mexanizmy-zashhity-prav-nesoversennoletnix-v-cifrovoi-srede

21. Қазақстан Республикасының Азаматтық кодексі (Ерекше бөлім). - [Электрондық ресурс]. - Қол жеткізу режимі: https://kodeksy-kz.com/grazhdanskij_kodeks_osobennaya_chast/927.htm

22. Балаларға қатысты кибербуллинг фактілері. - [Электрондық ресурс]. - Қол жеткізу режимі: https://qazaqstan.tv/news/156175/#:~:text=Балаларға%20қатысты%20кибербуллинг%20фактілері%20жіті,қатысты%20кибербулинг%20жөніндегі%20заң%20жобасы

23. Изменения в законодательстве штата и федерации в отношении неприкосновенности частной жизни несовершеннолетних в 2024 году. - [Электронный ресурс]. - Режим доступа: https://www.insideprivacy.com/childrens-privacy/state-and-federal-developments-in-minors-privacy-in-2024/#:~:text=California's%20age,for%20minors'%20social%20media%20accounts

24. Интернеттегі қудалау: Интернет-қудалау деген не және онымен қалай күресуге болады? // ЮНИСЕФ сайты. - [Электрондық ресурс]. - Қол жеткізу режимі: https://www.unicef.org/kazakhstan/kk/оқиғалар/интернеттегі-қудалау-интернет-қудалау-деген-не-және-онымен-қалай-күресуге-болады

25. Қазақстанда жасөспірімдердің 17% буллинг құрбаны болған - сарапшы // ҚазАқпарат. - [Электрондық ресурс]. - Қол жеткізу режимі: https://kaz.inform.kz/news/kazakstanda-zhasospirimderdin-17-bulling-kurbany-bolgan-sarapshy_a3689602/

26. UNICEF. *Положение детей в мире: Дети в цифровом мире.* - Нью-Йорк, 2017. - [Электронный ресурс]. - Режим доступа: https://www.unicef.org/uzbekistan/media/706/file/Дети%20в%20цифровом%20мире.pdf

27. Phillips K., Davidson J.C., Farr R.R., Burkhardt C., Caneppele S., Aiken M.P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies // *Forensic Sciences.* - 2022. - Vol. 2, No. 2. - P. 379-398. - DOI: https://doi.org/10.3390/forensicsci2020028

28. Staff. The COE International Convention on Cybercrime Before Its Entry Into Force // *UNESCO Courier.* - January-March 2004. - [Archived 25.09.2016]. - [Electronic resource]. - Access mode: https://en.wikipedia.org/wiki/Convention_on_Cybercrime#cite_note-2

29. Apsimet N.M., Muratova A.Zh. On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud // *Bulletin of the Karaganda University.* - 2025. - No. 3. - P. 87-97. - [Electronic resource]. - Access mode: https://law-vestnik.buketov.edu.kz/index.php/law/article/view/751/570

30. Бекмагамбетов А.Б. және т.б. *Уголовное право Республики Казахстан (Особенная часть): Монография.* - Москва: Российская академия

естествознания, 2017. - [Электрондық ресурс]. - Қол жеткізу режимі: https://monographies.ru/ru/book/section?id=12561

31. В МВД создали департамент по противодействию киберпреступности. - [Электронный ресурс]. - Режим доступа: https://vlast.kz/novosti/62499-v-mvd-sozdali-departament-po-protivodejstviu-kiberprestupnosti.html

32. Аратулы К. Преступления в сфере компьютерной информации в РК и зарубежных странах // ҚазҰУ хабаршысы. Заң сериясы. - 2010. - № 4 (56). - [Электронный ресурс]. - Режим доступа: file:///C:/Users/user/Downloads/1659%20(1).pdf

33. Tufin Research. *One in Six Teenagers Hack and Rarely Get Caught (Survey Report).* - New York/London, 2019. - [Electronic resource]. - Access mode: https://www.tufin.com/pr/tufin-survey-finds-one-in-six-new-york-teenagers-hack-and-rarely-get-caught

34. *Lapsus$: Court finds teenagers carried out hacking spree.* - [Electronic resource]. - Access mode: https://www.bbc.com/news/technology-66549159

35. *Inbusiness.kz.* Как дети попадаются на уловки кибермошенников (Балаларды алаяқтардың құрбаны ету тәсілдері). - 07.03.2025. - [Электронный ресурс]. - Қол жеткізу тәртібі: https://inbusiness.kz

36. Қазақстан Республикасының Бала құқықтары туралы конвенцияны іске асыруы туралы бесінші және алтыншы жиынтық мерзімді баяндаманы бекіту туралы. Қазақстан Республикасы Үкіметінің 2021 жылғы 28 желтоқсандағы № 942 қаулысы. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://adilet.zan.kz/kaz/docs/P2100000942

37. Уголовные дела о хакерах: почему они так редко доходят до суда? - [Электронный ресурс]. - Режим доступа: https://ranking.kz/digest/industries-digest/ugolovnye-dela-o-hakerah-pochemu-oni-tak-redko-dohodyat-do-suda.html

38. Қазақстанда енді 14 жастан бастап қылмыстық жауапкершілікке тартылады. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://kaz.orda.kz/aza-standa-endi-14-zhastan-bastap-ylmysty-zhauapkershilikke-tartylady

39. Кибербуллинг туралы заң жобасы мақұлданды. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://caspianlife.kz/14324

40. ІІМ ақпараттық порталындағы кибербуллинг және балағат сөздерге жауапкершілік туралы материалдар. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://polisia.kz/balaghat-sozderdi-qoldanghany-ushin-zhaza-normasy-turaly

41. За буллинг детей будут штрафовать: поправки в КОАП. - [Электронный ресурс]. - Режим доступа: https://www.zakon.kz/pravo/6431014-za-bulling-detey-budut-shtrafovat-popravki-v-koap.html

42. Қазақстан Республикасы Әкімшілік құқық бұзушылық туралы кодексі (2023 жылғы және 2024 жылғы өзгерістермен). - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://kodeksy-kz.com

43. Сенат "Жала жабу" бабын әкімшілік кодекске ауыстырды. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://abai.kz/post/114403

44. Буллинг в Казахстане: законодательство, ответственность и меры борьбы. - 2025. - [Электронный ресурс]. - Режим доступа: https://arasha.kz/ru/finansy/nalogi-i-shtrafy/bulling-v-kazahstane-zakonodatelstvo-otvetstvennost-i-mery-borby-2025

45. Около 150 фактов буллинга зарегистрировано в 2024 году в РК. - [Электронный ресурс]. - Режим доступа: https://khabar.kz/ru/news/obshchestvo/167424-okolo-150-faktov-bullinga-zaregistrirovano-v-2024-godu-v-rk

46. Родители подростков ответили в суде за буллинг, организованный их детьми. - [Электронный ресурс]. - Режим доступа: https://sozmedia.kz/54143

47. Әлеуметтік желіде баланы қорқытқан адам қалай жазаланады? Заңгер жауап берді. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://kaz.tengrinews.kz/article/aleumettk-jelde-balanyi-korkyitkan-adam-kalay-jazalanadyi

48. *South Korea's real-name net law is rejected by court.* - [Electronic resource]. - Access mode: https://www.bbc.com/news/technology-19357160

49. *Germany fines Facebook for under-reporting complaints.* - [Electronic resource]. - Access mode: https://www.reuters.com/article/business/germany-fines-facebook-for-under-reporting-complaints-idUSKCN1TX1HZ

50. *Online Harassment in Germany: Legal Defence.* - [Electronic resource]. - Access mode: https://se-legal.de/criminal-defense-lawyer/online-harassment-german-criminal-lawyers

51. *What does the law say about bullying?* - [Electronic resource]. - Access mode: https://anti-bullyingalliance.org.uk/tools-information/all-about-bullying/bullying-and-law

52. *Online Safety Act 2023.* - [Electronic resource]. - Access mode: https://en.wikipedia.org/wiki/Online_Safety_Act_2023

53. *Act on the Prevention of and Countermeasures Against Violence in Schools.* - [Electronic resource]. - Access mode: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=24031&type=new

54. «Кибербуллинг және әкімшілік жауапкершілік». - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://b031.edu.kz/kz/2598/kiberbwlling-zhaene-aekimshilik-zhawapkershilik

55. *Bullying at school.* gov.uk. - [Electronic resource]. - Access mode: https://www.gov.uk/bullying-at-school

56. Zhanuzakova L.T., Visarigova A.Sh.-A. *Legal framework for protecting children from information harmful to their health and development.* - [Electronic resource]. - Access mode: https://articlekz.com/article/20287

57. *Жүйелік реформаларға бағдар - жылдық есеп 2022.* «Самұрық-Қазына» АҚ. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://sk.kz/investors/AR-2023_SC/kz/041-informacionnaya_bezopasnost.php

58. *Kazakhstan-Octopus Cybercrime Community.* - [Electronic resource]. - Access mode: https://www.coe.int/en/web/octopus/-/kazakhstan

59. Dentons. *Changes to Kazakhstan's Administrative Code bring more financial sanctions.* - [Electronic resource]. - Access mode:

https://www.dentons.com/en/insights/alerts/2025/march/20/changes-to-kazakhstans-administrative-code-bring-more-financial-sanctions

60. *Kazakhstan to Introduce Fines for Illegal Online Content.* - [Electronic resource]. - Access mode: https://timesca.com/kazakhstan-to-introduce-fines-for-illegal-online-content

61. *Kazakhstan: Freedom on the Net 2024.* - [Electronic resource]. - Access mode: https://freedomhouse.org/country/kazakhstan/freedom-net/2024

62. UNICEF (БҰҰ Балалар қоры) және ЕҚЫҰ баяндамалары, баспасөз хабарламалары. *Сандық әлемдегі балалар: Қазақстан қорғанысты күшейтеді.* - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://www.unicef.org/kazakhstan/kk/баспасөз-хабарламасы

63. «Ақпараттандыру туралы» Қазақстан Республикасының Заңы 2015 жылғы 24 қарашадағы № 418-V ҚРЗ. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://adilet.zan.kz/kaz/docs/Z1500000418

64. Dentons. *New in Personal Data Rules: Almost Any Company May Fall within the Special Regulation.* - 30 June 2022. - [Electronic resource]. - Access mode: https://www.dentons.com/en/insights/alerts/2022/june/30/new-in-personal-data-rules

65. *Data Protection in Kazakhstan: Overview.* Practical Law Country Q&A w-007-8602. - [Electronic resource]. - Access mode: https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2023/data-protection-in-kazakhstan-overview.pdf

66. *Блокировка смартфонов в Казахстане: заявление Минцифры.* - Ulysmedia.kz. - [Электронный ресурс]. - Режим доступа: https://ulysmedia.kz/news/48928-blokirovka-smartfonov-v-kazakhstane-zaiavlenie-mintsifry

67. Қазақстан Республикасының ішкі істер органдарын жаңғырту жөніндегі 2019-2021 жылдарға арналған жол картасын бекіту туралы. Қазақстан Республикасы Үкіметінің 2018 жылғы 27 желтоқсандағы № 897 қаулысы. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://adilet.zan.kz/kaz/docs/P1800000897

68. Батыс Қазақстан облысы полиция департаментінде киберқылмыстармен күресетін жаңа бөлініс өз жұмысын бастады. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://polisia.kz/bqo-pd-da-kiberpol-oz-zhumysyn-bastady

69. Утепов Д. Правовые основы сбора, закрепления цифровой информации при доказывании уголовных дел в Республике Казахстан // *Юриспруденция*. - № 1, 2022. - [Электронный ресурс]. - Режим доступа: https://www.researchgate.net/publication/369062971

70. OSCE. *Beyond bits, bytes and borders: how we untangle digital evidence dilemmas in Central Asia.* - [Electronic resource]. - Access mode: https://www.osce.org/blog/590168

71. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»). Постановление Правительства Республики Казахстан от 30

июня 2017 года № 407. - [Электронный ресурс]. - Режим доступа: https://zakon.uchet.kz/rus/docs/P1700000407

72. Kumenov A. *Kazakhstan adopts law to regulate untamed social media scene.* - *Eurasianet*, 12 July 2023. - [Electronic resource]. - Access mode: https://eurasianet.org/kazakhstan-adopts-law-to-regulate-untamed-social-media-scene

73. Saniyazova Y., Mediyev R., Saitova E., Utegenova G., Kzylkhojayeva A. *Advancing Forensic Science in Kazakhstan: The Emergence and Impact of Digital Forensics in Cybercrime Investigation. // Law, State and Telecommunications Review*. - Vol. 16, No. 2. - 2024. - P. 48-68. - [Electronic resource]. - Access mode: https://periodicos.unb.br/index.php/RDET/article/view/49190

74. Қылмыстық жауапкершілікке тартылған кәмелетке толмағандар саны. Қаңтар-қыркүйек 2022. *Ranking.kz*, 26 қазан 2022 ж. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://ranking.kz/kz/sholu/regions-kz/ylmysty-zhauapkershilikke-tartyl-kmeletke-tolmaandar-sany-taryrkjek-2022.html

75. Трухачев А.В Астане задержан несовершеннолетний участник мошеннической схемы. *Polisia.kz*. - [Электронный ресурс]. - Режим доступа: https://ustinka.kz/kazakhstan/106587.html

76. ІІМ терроризм актісі туралы жалған хабарлама үшін жауапкершілік қарастырылатынын еске салды. *Polisia.kz*. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://polisia.kz/iim-terrorizm-aktisi-turaly-zhalghan-habarlama-ushin-zhauapkershilik-qarastyrylatynyn-eske-saldy-2/

77. Қазақстанда 2,5 мыңнан астам киберқылмыс ашылған. *Polisia.kz*. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://almaty.tv/kz/news/obschestvo/2025-kiberpol-komegimen-elimizde-25-mynnan-astam-kylmys-ashylgan

78. Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы кодексі (2014 ж.). Қазақстан Республикасы Үкіметінің 2013 жылғы 31 қазандағы № 1155 қаулысы. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://adilet.zan.kz/kaz/docs/P1300001155

79. Қазақстан Республикасының Қылмыстық-процестік кодексі, 2014 жылғы 4 шілдедегі № 231-V ҚРЗ. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://adilet.zan.kz/kaz/docs/K1400000231

80. Эксперты по борьбе с киберпреступностью провели семинар в Шымкенте. *Polisia.kz*. - [Электронный ресурс]. - Режим доступа: https://polisia.kz/ru/eksperty-po-bor-be-s-kiberprestupnost-yu-proveli-seminar-v-shymkente/

81. Преступность среди несовершеннолетних: какие меры принимают в Казахстане. 21 декабря 2024 г. - [Электронный ресурс]. - Режим доступа: https://ekaraganda.kz/?mod=news_read&id=149207

82. UNICEF Қазақстан және ЕҚЫҰ зерттеулері бойынша есептер («Қазақстан балалардың Интернеттегі қауіпсіздігі - 2023»). - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://astanatimes.com/2025/01/nurturing-futures-together-unicef-and-kazakhstans-collaboration-on-climate-change-and-cyber-safety

83. Казахстан: новый закон предусматривает уголовную ответственность за домашнее насилие. 23 июля 2024 г. - [Электронный ресурс]. - Режим доступа: https://www.loc.gov/item/global-legal-monitor/2024-07-22/kazakhstan-new-law-criminalizes-domestic-violence

84. Қазақстан Республикасының «Баланың құқықтары туралы» заңы, 8 тамыз 2002 ж. № 345. - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://adilet.zan.kz/kaz/docs/Z020000345_

85. Karipbaev, Zh.B., & Mussin, K.S. (2020). Concept of Bringing Minors to Administrative Responsibility. *Bulletin of the Karaganda University "Law Series"*, 2020 (98) (2). doi:10.31489/2020l2/32-39. Available at: https://law-vestnik.buketov.edu.kz/index.php/law/article/view/37 (accessed October 15, 2024).

86. Административная ответственность несовершеннолетних. *Postfactum.kz*. - [Электронный ресурс]. - Режим доступа: https://postfactum.kz/ru/pravo/613-administrativnaya-otvetstvennost-nesovershennoletnikh

87. Kazakhstan adopts law on domestic violence. *Kazinform*, 15 April 2024. - [Electronic resource]. - Access mode: https://qazinform.com/news/kazakhstan-adopts-law-on-domestic-violence-ec3b6f

88. «Беспризорные и безнадзорные»: какие подростки попадают в спецшколы. *Polisia.kz*, 13 февраля 2025 г. - [Электронный ресурс]. - Режим доступа: https://polisia.kz/ru/besprizornye-i-beznadzornye-kakie-podrostki-popadayut-v-spetsshkoly

89. OSCE ұйымының материалдары (Astana Programme Office есептері; 14.05.2025 ж. баспасөз хабарламасы). - [Электрондық ресурс]. - Қол жеткізу тәртібі: https://www.osce.org/oceea/590775

90. Kazakhstan invited to join the Convention on Cybercrime. 19 April 2023. - [Electronic resource]. - Access mode: https://www.coe.int/en/web/cybercrime/-/kazakhstan-invited-to-join-the-convention-on-cybercrime

91. Third Meeting of the Interagency Steering Committee on Combating Cybercrime in Kazakhstan. 30 September 2024. *OSCE Programme Office in Astana*. - [Electronic resource]. - Access mode: https://www.osce.org/programme-office-in-astana/577154

92. Zhumabekova K., Kegembayeva Zh. *Ensuring children's online safety in Kazakhstan: balancing protection from harm with rights to information access. Security and Human Rights (Helsinki Monitor).* - [Electronic resource]. - Access mode: https://www.shrmonitor.org/assets/uploads/2024/03/Zhumabekova-et.-al.pdf

93. *Rights of the Child. United Nations*, 8 November 2023. - [Electronic resource]. - Access mode: https://documents.un.org/doc/undoc/ltd/n23/342/80/pdf/n2334280.pdf

94. *Child Safety Online. Giplatform*. - [Electronic resource]. - Access mode: https://www.giplatform.org/topics/internet-governance-and-digital-policy/cybersecurity/child-safety-online

95. *UN General Assembly groundbreaking resolution with 193 States committed to implementing children's rights in the digital environment!* -

[Electronic resource]. - Access mode: https://childrightsconnect.org/un-general-assembly-groundbreaking-resolution-with-193-states-committed-to-implementing-childrens-rights-in-the-digital-environment

96. *World governments adopt UN resolution on children's rights online. 5Rights Foundation*. - [Electronic resource]. - Access mode: https://5rightsfoundation.com/world-governments-adopt-un-resolution-on-childrens-rights-online

97. *The State of the World's Children 2017: Children in a Digital World. UNICEF*. - [Electronic resource]. - Access mode: https://www.unicef.org/reports/state-worlds-children-2017

98. *Cyber threats in focus of OSCE Presence information sessions with schools across Albania.* - [Electronic resource]. - Access mode: https://www.osce.org/presence-in-albania/530332

99. *Convention on Cybercrime (Budapest, 23.XI.2001). European Treaty Series No. 185.* - [Electronic resource]. - Access mode: https://rm.coe.int/1680081561

100. Duysak Merve. Legal Developments as to "Cyber Grooming" Actions from the Lanzarote Convention to Now // Athens Journal of Law. - Vol. 9, No. 4. - October 2023. - P. 597-610. [Electronic resource]. - Access mode: https://doi.org/10.30958/ajl.9-4-6

101. *Digital and Information Society: Rights of Children in the Digital Environment. European Commission.* - [Electronic resource]. - Access mode: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/digital-and-information-society_en

102. *Organization for Security and Co-operation in Europe (OSCE).* - [Electronic resource]. - Access mode: https://dig.watch/actor/organization-security-and-co-operation-europe

103. *OSCE Decision No. 7/17: Strengthening efforts to combat all forms of child trafficking, including for sexual exploitation. MC(24) Journal No. 2.* - [Electronic resource]. - Access mode: https://www.osce.org/files/f/documents/f/b/362016.pdf

104. *One in six school-aged children experiences cyberbullying, finds new WHO/Europe study.* Copenhagen, 27 March 2024. - [Electronic resource]. - Access mode: https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying

105. *Protecting Children Online: An Overview of Recent Developments in Legal Frameworks and Policies. OECD Digital Economy Papers*, No. 295, May 2020. - [Electronic resource]. - Access mode: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/06/protecting-children-online_0c385619

106. *Cutter Law. Cyberbullying & Cyberstalking Laws in California.* - [Electronic resource]. - Access mode: https://cutterlaw.com/california-laws/cyberbullying-and-cyberstalking

107. *StopBullying.gov. Federal Laws.* - [Electronic resource]. - Access mode: https://www.stopbullying.gov/resources/laws/federal

108. *Anti-Bullying Alliance (UK). Online Bullying and the Law.* - [Electronic resource]. - Access mode: https://anti-bullyingalliance.org.uk/tools-information/all-about-bullying/bullying-and-law/online-bullying-and-law

109. *Wikipedia. Online Safety Act 2023 (UK).* - [Electronic resource]. - Access mode: https://en.wikipedia.org/wiki/Online_Safety_Act_2023

110. Karipbaev, Zh.B, & Bozhkarauly, A. (2019). *Mechanisms of Administrative Offenses of Minors*. *Journal of Advanced Research in Law and Economics*, 9(6[36]), 2016-2025. ISSN 2068-696X. Available at: https://journals.aserspublishing.eu/jarle/article/view/3966 (accessed October 15, 2024).

111. LSE Media Policy Project. *New youth protection law in Germany* (2021). - "The law obliges platform providers to take precautionary measures such as child-friendly terms, safe default settings, easy-to-find help and reporting mechanisms." [Электронный ресурс]. - Режим доступа: https://blogs.lse.ac.uk/medialse/2021/03/12/new-youth-protection-law-in-germany-participation-of-children-is-a-top-priority/

112. Library of Congress. *Germany: Network Enforcement Act.* - "The law obligates social media networks (with 2 million+ users) to remove content that is 'clearly illegal' within 24 hours." [Электронный ресурс]. - Режим доступа: https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/

113. Bremer Inkasso (Germany). *Deliktsfähigkeit.* - "Gemäß § 832 BGB… die Erziehungsberechtigten zur Verantwortung gezogen werden, sofern sie ihre Aufsichtspflicht verletzt haben." [Электронный ресурс]. - Режим доступа: https://www.bremer-inkasso.de/deutsch/glossar/d/deliktsfaehigkeit.html

114. Waan Choi (2023). *Korean government announces new anti-bullying laws.* Tiger Times Online; Yonhap News (12.04.2023). - "Students with a history of bullying will have their disciplinary records reflected in college admissions, beginning in 2026." [Электронный ресурс]. - Режим доступа: https://en.yna.co.kr/view/AEN20230412008700315

115. ICCWT (2013). *Korean approach to online protection for children.* - "Art. 44-5 of the Act on Protection of Communication Network… held unconstitutional." [Электронный ресурс]. - Режим доступа: https://www.iccwtnispcanarc.org/upload/pdf/7495594463Korean%20approach%20to%20onlone%20protection%20for%20children.pdf

116. Jun W. (2020). *A Study on the Cause Analysis of Cyberbullying in Korean Adolescents. International Journal of Environmental Research and Public Health,* 17(13), 4648. [Электронный ресурс]. - Режим доступа: https://doi.org/10.3390/ijerph17134648

117. Better Internet for Kids (2025). *Lithuania - Policy Profile.* - "Protection of children from intimate image abuse and cyberbullying are covered under the Law on Education, Article 23." [Электронный ресурс]. - Режим доступа: https://better-internet-for-kids.europa.eu/en/knowledge-hub/lithuania-policy-monitor-country-profile

118. INHOPE (2020). *Laying Down the Law in Latvia.* - "Law enforcement can require ISPs to provide identity of the perpetrator." [Электронный ресурс]. - Режим доступа: https://www.inhope.org/EN/articles/laying-down-the-law-in-latvia

119. *Children's Online Privacy Protection Act* (1998), 15 U.S.C. 6501-6505 (COPPA Rule as updated 2013). Federal Trade Commission, USA. [Электронный ресурс]. - Режим доступа: https://www.whitecase.com/insight-alert/unpacking-ftcs-coppa-amendments

120. Kim Y. (2023). *South Korea's Approach to Age Assurance. TechPolicy Press,* сент. 2023. [Электронный ресурс]. - Режим доступа: https://www.techpolicy.press/south-koreas-approach-to-age-assurance/

121. *Online Safety Act 2023* (United Kingdom), c. 36. [Электронный ресурс]. - Режим доступа: https://www.nortonrosefulbright.com/en-kr/knowledge/publications/0b658a5a/online-safety-act

122. Information Commissioner's Office (UK). *Age Appropriate Design Code (Children's Code),* 2020. [Электронный ресурс]. - Режим доступа: https://en.wikipedia.org/wiki/Children%27s_Code

123. Karipbaev, Zh.B., & Mussin, K.S. (2021). *The Concept of Administrative Offenses of Minors*. *Bulletin of the Karaganda University "Law Series"*, 102(2). doi:10.31489/2021l2/22-29. Available at: https://law-vestnik.buketov.edu.kz/index.php/law/article/view/137 (accessed October 15, 2024).

124. *Jugendmedienschutz-Staatsvertrag (JMStV)* - State Treaty on Youth Media Protection (Germany, amended 2021). [Электронный ресурс]. - Режим доступа: https://www.taylorwessing.com/en/interface/2025/online-safety-update/germanys-approach-to-protecting-minors-online

125. Better Internet for Kids (2025). *Lithuania - Safer Internet Country Profile.* European Commission. [Электронный ресурс]. - Режим доступа: https://better-internet-for-kids.europa.eu/sites/default/files/2025-05/Lithuania%20-%20Policy%20monitor%20country%20profile%20-%202025.pdf

126. Human Rights Watch (2022). *Kazakhstan: New 'Children's Rights' law used to tighten internet control.* [Электронный ресурс]. - Режим доступа: https://www.rferl.org/a/kazakhstan-law-social-media/31832653.html

127. *Youth Protection Revision Act (Shutdown Law),* 2011 (Republic of Korea National Assembly; repealed 2021). [Электронный ресурс]. - Режим доступа: https://en.wikipedia.org/wiki/Shutdown_law

128. Reuters News (15 сент. 2021). *Kazakhstan moves to restrict foreign social media usage - to fight cyberbullying.* [Электронный ресурс]. - Режим доступа: https://www.reuters.com/technology/kazakhstan-moves-restrict-foreign-social-media-usage-2021-09-15/

129. Қазақстан Республикасының Әкімшілік рәсімдік-процестік кодексі. 29 маусым 2020 ж. № 350-VI ҚРЗ. [Электрондық ресурс]. - Кіру режимі: https://adilet.zan.kz/kaz/docs/K2000000350

130. Jang K., Pan L., Turner Lee N. (2023). *The fragmentation of online child safety regulations.* Brookings Institution, 14 авг. 2023. [Электронный ресурс]. -

Режим доступа: https://www.brookings.edu/articles/patchwork-protection-of-minors/

131. Ye J. (2023). *China looks to limit children to two hours a day on their phones. Reuters,* 3 авг. 2023. [Электронный ресурс]. - Режим доступа: https://www.reuters.com/world/china/china-issues-draft-guidelines-tighten-limits-use-apps-by-minors-2023-08-02/

132. *Online Safety Act: explainer.* GOV.UK, опубл. 8 мая 2024 (обновлено 24 апр. 2025). [Электронный ресурс]. - Режим доступа: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

133. Tosza S. (2023). *Gathering Electronic Evidence for Administrative Investigations. eucrim,* № 2/2023, с. 216-222. [Электронный ресурс]. - Режим доступа: https://eucrim.eu/articles/gathering-electronic-evidence-for-administrative-investigations/

134. OSCE. *Trains Kazakh law enforcement officers on handling digital evidence.* 3 февраля 2023. [Электронный ресурс]. - Режим доступа: https://www.osce.org/secretariat/536999

135. OSCE. *Conducts training on cybercrime and digital evidence in Kazakhstan.* 24 мая 2024. [Электронный ресурс]. - Режим доступа: https://www.osce.org/secretariat/569142

136. BOMCA 10. *Supports digital forensics capacities in Kazakhstan and Kyrgyzstan.* 16 мая 2025. [Электронный ресурс]. - Режим доступа: https://www.bomca-eu.org/en/news/bomca-10-supports-digital-forensics-capacities-in-kazakhstan-and-kyrgyzstan

137. Web Asha Technologies. *What are the legal aspects of digital forensics and how do they affect evidence admissibility in court?* 22 июля 2025. [Электронный ресурс]. - Режим доступа: https://www.webasha.com/blog/what-are-the-legal-aspects-of-digital-forensics-and-how-do-they-affect-evidence-admissibility-in-court

138. INTERPOL. *Digital forensics: Helping our member countries make best use of electronic evidence.* [Электронный ресурс]. - Режим доступа: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics

139. Council of Europe. *Explanatory Report to the Convention on Cybercrime (ETS No. 185, Budapest, 23 Nov 2001).* [Электронный ресурс]. - Режим доступа: https://rm.coe.int/16800cce5b

140. Alimov O.T. (2025). *Deadly Subscription: Legal Protection of Children at Risk in the Digital World. CyberLeninka.* [Электронный ресурс]. - Режим доступа: https://cyberleninka.ru/article/n/deadly-subscription-legal-protection-of-children-at-risk-in-the-digital-world

141. European Commission. *Publishes DSA Guidelines on the Protection of Minors Online.* 23 июля 2025. [Электронный ресурс]. - Режим доступа: https://www.wsgr.com/en/insights/european-commission-publishes-dsa-guidelines-on-the-protection-of-minors-online.html

142. *China looks to limit children to two hours a day on their phones. Reuters,* 3 авг. 2023. [Электронный ресурс]. - Режим доступа:

https://www.reuters.com/world/china/china-issues-draft-guidelines-tighten-limits-use-apps-by-minors-2023-08-02/

143. *Online Safety Act: explainer.* GOV.UK, опубл. 8 мая 2024 (обновлено 24 апр. 2025). [Электронный ресурс]. - Режим доступа: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

144. *The fragmentation of online child safety regulations.* Brookings Institution, 14 авг. 2023. [Электронный ресурс]. - Режим доступа: https://www.brookings.edu/articles/patchwork-protection-of-minors/

145. Сакенова С. (2025). *Казахстан интегрирует ИИ и цифровые технологии для модернизации правовой системы. The Astana Times,* 27 февраля 2025. [Электронный ресурс]. - Режим доступа: https://astanatimes.com/2025/02/kazakhstan-integrates-ai-digital-technologies-to-modernize-legal-system/

146. *Новые правила электронной цифровой подписи в Казахстане.* 1 октября 2025. [Электронный ресурс]. - Режим доступа: https://www.dentons.com/en/insights/articles/2025/october/1/new-electronic-digital-signature-rules-in-kazakhstan

147. *Цифровая судебная экспертиза.* INTERPOL - Как мы работаем / Инновации. [Электронный ресурс]. - Режим доступа: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics

148. UNICEF Kazakhstan. *Children in the digital world: Kazakhstan strengthens protection.* Пресс-релиз, 24 февраля 2025. [Электронный ресурс]. - Режим доступа: https://www.unicef.org/kazakhstan/en/press-releases/children-digital-world-kazakhstan-strengthens-protection

149. UNICEF Kazakhstan. *Children in the digital world: Kazakhstan strengthens protection.* 24 февраля 2025. [Электронный ресурс]. - Режим доступа: https://www.unicef.org/kazakhstan/en/press-releases/children-digital-world-kazakhstan-strengthens-protection

150. Межведомственная комиссия по делам несовершеннолетних и защите их прав при Правительстве Республики Казахстан. *Сайт о защите детей в Казахстане.* [Электронный ресурс]. - Режим доступа: https://bala-kkk.kz/zashhita-prav-detej/mezhvedomstvennaya-komissiya-po-delam-nesovershennoletnih

151. Баланы жәбірлеудің (буллингтің) профилактикасы қағидаларын бекіту туралы Қазақстан Республикасы Оқу-ағарту министрінің 2022 жылғы 21 желтоқсандағы № 506 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2022 жылғы 21 желтоқсанда № 31180 болып тіркелді. - [Электрондық ресурс]. - Кіру режимі: https://adilet.zan.kz/kaz/docs/V2200031180

152. Қазақстан Республикасының кейбір заңнамалық актілеріне баланың құқықтарын қорғау, білім беру, ақпарат және ақпараттандыру мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы. Қазақстан Республикасының Заңы 2022 жылғы 3 мамырдағы № 118-VII ҚРЗ. -

[Электрондық ресурс]. - Кіру режимі: https://adilet.zan.kz/kaz/docs/Z2200000118

153. Кәмелетке толмағандар арасындағы құқық бұзушылықтардың профилактикасы мен балалардың қадағалаусыз және панасыз қалуының алдын алу туралы. Қазақстан Республикасының 2004 жылғы 9 шілдедегі № 591 Заңы. - [Электрондық ресурс]. - Кіру режимі: https://adilet.zan.kz/kaz/docs/Z040000591_

154. Карипбаев Ж.Б. Проблемы правового регулирования цифровой безопасности несовершеннолетних в Казахстане // «Әлеуметтік-еңбек қатынастары саласындағы еңбек даулары мен басқа да конфликтілік жағдайларды шешу жолдары: теориялық-тәжірибелік сұрақтары» халықаралық ғылыми-практикалық конференция материалдары *(8 мамыр 2025 ж.)*. - Алматы: Қазақ ұлттық университеті баспасы, 2025. - Б. 444-449.

155. OSCE strengthens Kazakhstan's national capacities in preventing and countering terrorist use of the Internet. 18 May 2023. - [Electronic resource]. - Access mode: https://www.osce.org/project/capacity-building-on-combating-cybercrime-in-central-asia

156. UNODC supports the Central Asian states in combatting cybercrime. - [Electronic resource]. - Access mode: https://www.unodc.org/roca/en/news/unodc-supports-the-central-asian-states-in-combatting-cybercrime.html

157. Онлайн-платформалар және онлайн-жарнама туралы. Қазақстан Республикасының Заңы 2023 жылғы 10 шілдедегі № 18-VIII ҚРЗ. - [Электрондық ресурс]. - Кіру режимі: https://adilet.zan.kz/kaz/docs/Z2300000018

158. Protection of Minors' Rights, Social and Medical Support, and "National Fund for Children": How Kazakhstan Ensures State Support for the Younger Generation // Правительство Республики Казахстан. - 1 июня 2025 г. - [Электронный ресурс]. - Режим доступа: https://primeminister.kz/en/news/reviews/protection-of-minors-rights-social-and-medical-support-and-national-fund-for-children-how-kazakhstan-ensures-state-support-for-the-younger-generation-30112

159. Kazakh President Endorses Law on Women's Rights and Children's Safety // The Astana Times. - 15 April 2024. - [Electronic resource]. - Access mode: https://astanatimes.com/2024/04/kazakh-president-endorses-law-on-womens-rights-and-childrens-safety

160. MediaNet International Center for Journalism. *Media and Information Literacy in Kazakhstan: Mapping MIL Report.* - Almaty, 2025. - [Electronic resource]. - Access mode: https://articles.unesco.org/sites/default/files/medias/fichiers/2025/09/Mapping-MIL-Report-Eng.pdf

161. Kazakhstan strengthens child safety with panic buttons and anti-bullying measures // *Kazinform.* - 2025. - [Electronic resource]. - Access mode: https://qazinform.com/news/kazakhstan-strengthens-child-safety-with-panic-buttons-and-anti-bullying-measures-693313

162. Teaching parents to protect their children online in Kazakhstan // *UNICEF Kazakhstan.* - 28 February 2024. - [Electronic resource]. - Access mode: https://www.unicef.org/kazakhstan/en/press-releases/teaching-parents-protect-their-children-online-kazakhstan

163. Kazakhstan strengthens inter-agency co-operation on youth crime through OSCE workshop. - 2 October 2025. - [Electronic resource]. - Access mode: https://www.osce.org/secretariat/598381

164. Kazakhstan hosts international conference on countering cybercrime // *UNODC.* - 26 September 2025. - [Electronic resource]. - Access mode: https://www.unodc.org/roca/en/NEWS/2025/kazakhstan-hosts-international-conference-on-countering-cybercrime.html

165. International Conference on Combating Transnational Cybercrime // *OSCE Programme Office in Astana.* - 25 September 2025. - [Electronic resource]. - Access mode: https://www.osce.org/programme-office-in-astana/598324

166. ЮНИСЕФ Қазақстан. *Қазақстандағы балаларды желідегі зорлық-зомбылық, қатыгездік пен қанаудан қорғау.* - Алматы, 2025. - [Электрондық ресурс]. - Кіру режимі: https://www.unicef.org/kazakhstan/en/media/12911/file/OCSEA%20brochure%20final.pdf.pdf

167. Балалардың цифрлық әлемі: Қазақстан балаларды қорғауды күшейтеді. - Астана, 24 ақпан 2025 ж. - [Электрондық ресурс]. - Кіру режимі: https://www.unicef.org/kazakhstan/en/press-releases/children-digital-world-kazakhstan-strengthens-protection

*168. Karipbaev, Zh.B. (2021).* Administrative penalties and measures of administrative and educational influence applied to minor offenders in the Republic of Kazakhstan. *In* Topical Issues of Legal Regulation and New Approaches to the Implementation of National Law: Proceedings of the International Scientific and Practical Online Conference (February 26, 2021) *(pp. 40-44). Karaganda: Karaganda University Press.*

169. *Protecting Children Online. Every child must be protected from violence, exploitation and abuse on the internet.* - [Electronic resource]. - Access mode: https://www.unicef.org/protection/violence-against-children-online

170. Интернет желісіндегі балалардың қауіпсіздігін қамтамасыз ету мәселелері бойынша ҚР ЦДИАӨМ қолдауымен ата-аналарға арналған мастер-класс өтті. - 14 наурыз 2024 ж. - [Электрондық ресурс]. - Кіру режимі: https://www.gov.kz/memleket/entities/mdai/press/news/details/726692

171. UNODC. *Using the Power of Technology to Help Victims of Human Trafficking.* - [Electronic resource]. - Access mode: https://www.unodc.org/unodc/frontpage/2022/July/using-the-power-of-technology-to-help-victims-of-human-trafficking.html

172. *How Digital Identity Works on the Blockchain.* - [Electronic resource]. - Access mode: https://www.halborn.com/blog/post/how-digital-identity-works-on-the-blockchain

173. *Intelligence Briefing: The Role of Age Verification Technology in Tackling Child Sexual Exploitation and Abuse Online.* - [Electronic resource]. -

Access mode: https://www.weprotect.org/wp-content/uploads/The-role-of-age-verification-technology-v3.pdf

174. В Алматы запустили пилотный проект SIM-карты с защитой от интернет-угроз для детей. - 19 апреля 2025 г. - [Электронный ресурс]. - Режим доступа: https://kaztag.kz/ru/news/v-almaty-zapustili-pilotnyy-proekt-sim-karty-s-zashchitoy-ot-internet-ugroz-dlya-detey

175. *Net Nanny Offers a Variety of Parental Control Software Features to Help Protect Your Family.* - [Electronic resource]. - Access mode: https://www.netnanny.com/features

176. *Ashyq қосымшасын 12 жастан асқан балалар пайдалана алады. // Orda.kz.* - [Электрондық ресурс]. - Кіру режимі: https://kaz.orda.kz/ashyq-osymshasyn-12-zhastan-as-an-balalar-pajdalana-alady

177. *Ұлттық қор - балаларға* жобасы аясында *eGov mobile* қосымшасында балалардың деректерін көрсету. - 15 сәуір 2024 ж. - [Электрондық ресурс]. - Кіру режимі: https://www.gov.kz/memleket/entities/adilet-krg/press/article/details/165508

178. Интернет желісіндегі балалардың қауіпсіздігін қамтамасыз ету мәселелері бойынша ҚР ЦДИАӨМ қолдауымен ата-аналарға арналған мастер-класс өтті. - 14 наурыз 2024 ж. - [Электрондық ресурс]. - Кіру режимі: https://www.gov.kz/memleket/entities/mdai/press/news/details/726692

179. Пилотный проект по защите детей в интернете представили в Казахстане. - [Электронный ресурс]. - Режим доступа: https://bluescreen.kz/pilotnyi-proiekt-po-zashchitie-dietiei-v-intiernietie-priedstavili-v-kazakhstanie

180. *Use Screen Time on your iPhone or iPad.* - Published 13 May 2025. - [Electronic resource]. - Access mode: https://support.apple.com/en-us/108806

181. *YouTube Kids. // Wikipedia, the free encyclopedia.* - [Electronic resource]. - Access mode: https://en.wikipedia.org/wiki/YouTube_Kids

182. *Childhood in a Digital World: Screen Time, Digital Skills and Mental Health* / UNICEF Innocenti. - New York / Florence, 2025. - [Electronic resource]. - Access mode: https://www.unicef.org/innocenti/reports/childhood-digital-world

183. *A Window into Young Children's Online Worlds.* - 19 April 2024. - [Electronic resource]. - Access mode: https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/a-window-into-young-childrens-online-worlds

184. *OECD calls for an ambitious approach to protect and empower children online.* - May 2025. - [Electronic resource]. - Access mode: https://www.oecd.org/en/about/news/press-releases/2025/05/oecd-calls-for-an-ambitious-approach-to-protect-and-empower-children-online.html

185. *AI Shields Kids by Revolutionizing Child Safety and Online Protection* / Neil Sahota. - 20 July 2024. - [Electronic resource]. - Access mode: https://www.forbes.com/sites/neilsahota/2024/07/20/ai-shields-kids-by-revolutionizing-child-safety-and-online-protection

186. *AI for Safe Children Online // Virginia Tech News.* - June 2024. - [Electronic resource]. - Access mode: https://news.vt.edu/articles/2024/06/eng-cs-AI-for-safe-children-online.html

187. Karipbaev, Zh.B. (2019). *Personal Qualities of Juvenile Offenders' Deformation Features*. *Bulletin of the Karaganda University "Law Series"*. Available at: https://law-vestnik.buketov.edu.kz/index.php/law/article/view/95/87 (accessed October 15, 2025).

188. *Privacy-First Age Verification: Concordium's ZKP-Based Solution.* - 10 June 2025. - [Electronic resource]. - Access mode: https://www.concordium.com/article/privacy-first-age-verification-concordiums-zkp-based-solution

189. *Blockchain Age Verification: A Privacy-First Solution.* - 22 October 2024. - [Electronic resource]. - Access mode: https://segpay.com/blog/blockchain-age-verification/

190. *Age Appropriate Design: A Code of Practice for Online Services.* - 2 September 2021. - [Electronic resource]. - Access mode: https://ico.org.uk/.../age-appropriate-design-a-code-of-practice-for-online-services

191. *Age Verification Regulations May Finally Be Taking Hold in the US.* - 21 November 2024. - [Electronic resource]. - Access mode: https://www.authenticid.com/user-experience/age-verification-regulations-may-finally-be-taking-hold-in-the-us

192. *Parental Control Software & Website Blocker.* - [Electronic resource]. - Access mode: https://www.netnanny.com

193. *Establish Digital Ground Rules.* - [Electronic resource]. - Access mode: https://families.google/familylink

194. *How to Set Up Screen Time for a Child.* - [Electronic resource]. - Access mode: https://support.apple.com/ru-ru/guide/ipod-touch/iph43cc563d2/ios

195. *Ashyq App Now Available in eGov Mobile.* - 3 June 2021. - [Electronic resource]. - Access mode: https://egov.kz/cms/en/news/news_ashyq

196. «Лаборатория Касперского» және Павлодар облысының әкімдігі балаларды интернетте қорғау жобасын аяқтады. - 11 қаңтар 2024 ж. - [Электрондық ресурс]. - Қолжетімді: https://designer.kz/2024/01/kaspersky-lab-and-protecting-children-on-the-internet/

197. «SIM KIDS» балаларға арналған қауіпсіздік жобасы Алматыда ресми түрде іске қосылды. - 17 маусым 2025 ж. - [Электрондық ресурс]. - Қолжетімді: https://zamin.uz/en/technology/152427-the-sim-kids-safe-project-for-children-has-been-officially-launched-in-almaty.html

198. «Ұлттық қор - балаларға» жобасы аясында балалар туралы мәліметтерді алу мүмкіндігі. - 5 қаңтар 2024 ж. - [Электрондық ресурс]. - Қолжетімді: https://egov.kz/cms/kk/news/National_Fund

199. Age-Appropriate Design: A Code of Practice for Online Services. - [Electronic resource]. - Access mode**:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services (accessed: 10 October 2025).

200. *OECD Calls for an Ambitious Approach to Protect and Empower Children Online.* - May 2025. - [Electronic resource]. - Access mode:

https://www.oecd.org/en/about/news/press-releases/2025/05/oecd-calls-for-an-ambitious-approach-to-protect-and-empower-children-online.html

## ҚОСЫМША

**1. Кәмелетке толмағандардың кибер құқық бұзушылықтары бойынша анықталған оқиғалар (Қазақстан, 2020-2024 жж.)**

| Жыл | Анықталған оқиғалар саны |
|---|---|
| 2020 | 197 |
| 2021 | 218 |
| 2022 | 236 |
| 2023 | 281 |
| 2024 (қаң.-мам.) | 70 |
| **Барлығы** | **1202** |

**2. Кәмелетке толмағандарға қатысты кибербуллинг фактілері (кейбір өңірлер бойынша)**

| Өңір | 2023 ж. анықталған жағдайлар | Ерекше сипаттамалар |
|---|---|---|
| Павлодар обл. | 17 | Көбі интернетте қорқыту |
| Қостанай обл. | 12 | Виртуалды қорлаулар |
| Алматы | 9 | Жалған аккаунт, ақша жинау |

**3. Кәмелетке толмағандардың интернетті пайдалану уақыты (сауалнама деректері бойынша)**

| Уақыт аралығы | % оқушылар (2024) |
|---|---|
| 1-2 сағат/тәулігіне | 28% |
| 2-4 сағат | 38% |

| Уақыт аралығы | % оқушылар (2024) |
|---|---|
| 4 сағаттан көп | 21% |
| 1 сағаттан аз | 13% |

**4. Әкімшілік жауапқа тартылған ата-аналар мен жасөспірімдер (2022-2024 жж.)**

| Жыл | Ата-ана жауапкершілігі (оқиға) | Жасөспірім (16 жастан жоғары) |
|---|---|---|
| 2022 | 75 | 46 |
| 2023 | 89 | 61 |
| 2024 | 21 | 14 |

**5. Киберқауіпсіздік бойынша ұлттық және пилоттық жобалар (2022-2024 жж.)**

| Жоба атауы | Жүргізілген жыл | Мақсат/ерекшелік |
|---|---|---|
| SIM Kids | 2023-2024 | Балаларға арналған қауіпсіз SIM-карта |
| Kaspersky Safe Kids | 2022-2024 | Интернет фильтрация, Павлодар пилоты |
| Ashyq Kids | 2023 | Ashyq жүйесіне балаларды енгізу |