ПРАВА ЛЮДИНИ У ЦИФРОВОМУ ВИМІРІ

2024

Лабораторія цифрової безпеки

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Авторський колектив:

Тетяна Авдєєва
Віта Володовська
Максим Дворовий
Анна Людва
Сергій Савелій
Євгенія Стаднік
Каріна Левадня
Вікторія Ткаченко
Соломія Яременко
Богдана Ярута

Звіт підготовлено в рамках проєкту «Права людини у цифровому вимірі: дотримання міжнародних зобов'язань та план дій на шляху до ЄС» за підтримки Міжнародного фонду «Відродження». Звіт представляє позицію авторів і не обов'язково відображає позицію Міжнародного фонду «Відродження».

Лабораторія цифрової безпеки (Цифролаба) - українська неурядова організація, що допомагає незалежним медіа, журналістам, активістам та громадянському суспільству посилювати власну цифрову безпеку. Цифролаба також працює над впровадженням стандартів прав людини в цифровій сфері через напрацювання аналітичних матеріалів, долучення до законотворчих процесів та адвокаційних кампаній в Україні та світі.

Сайт: https://dslua.org
E-mail: dslua@dslua.org
ФБ: https://www.facebook.com/dslua

Міжнародний фонд «Відродження» – одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів на суму понад 350 мільйонів доларів США.

Сайт: www.irf.ua
Facebook: www.fb.com/irf.ukraine

ПРО ЗВІТ

Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Цей конституційний принцип є абсолютним. Будь-які обмеження, навіть ті, що запроваджені під час воєнного чи надзвичайного стану, є виправданими лише доти, доки не підважують цінність людини та утвердження її прав як головного обов'язку держави.

Цей звіт – є зрізом стану забезпечення прав людини у цифровому середовищі під впливом повномасштабного вторгнення Росії та зобов'язань України щодо гармонізації національного законодавства з правом ЄС станом на 2024 рік. Аналіз зосереджений на заходах щодо забезпечення доступу до інтернету (Розділ 1) як умови для реалізації цифрових прав, забезпеченні свободи вираження поглядів та свободи медіа онлайн (Розділ 2), захисті персональних даних та приватності у цифровому середовищі (Розділ 3). Звіт також досліджує вплив технологій штучного інтелекту на права людини та заходи, що можуть впроваджуватися для попередження можливих порушень та мінімізацію ризиків (Розділ 4). Останній розділ цього звіту досліджує вплив цифрових технологій на право на вільні вибори, зокрема крізь призму регулювання політичної реклами. У наступних щорічних звітах Лабораторія цифрової безпеки планує розширювати сферу дослідження, аналізуючи вплив цифровізації і на інші основоположні права людини.

Звіт містить детальні рекомендації щодо реформування національного законодавства та вжиття інших заходів щодо виконання вимог у сфері прав людини в онлайн середовищі, розроблені на основі проведеного аналізу та міжнародних договорах, стороною яких є Україна, рекомендаціях та резолюціях Ради Європи, практиці Європейського суду з прав людини, рекомендаціях ООН, Хартії ЄС про основоположні права та інших актах права ЄС, імплементація яких є необхідною умовою євроінтеграції України.

ЗМІСТ

ДОСТУП ДО ІНТЕРНЕТУ ЯК ОСНОВА ДЛЯ РЕАЛІЗАЦІЇ ПРАВ ЛЮДИНИ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Реформа національного законодавства у сфері електронних комунікацій, зокрема набрання чинності Законом України «Про електронні комунікації» у 2022 році, однозначно гарантували право громадян на якісний та доступний інтернет (універсальні електронні комунікаційні послуги), що є необхідною умовою для самовираження та реалізації прав людини онлайн. Гармонізація українського права з вимогами ЄС також передбачає послаблення регуляторного тиску, покращення умов для розвитку ринку, що в результаті має привести до зростання якості послуг для споживачів. Однак повноцінне впровадження законодавчих нововведень досі триває. Повномасштабне вторгнення Російської Федерації в Україну відклало ухвалення багатьох підзаконних актів, необхідних для імплементації передбачених гарантій та програм на практиці, як і їх фінансування. Крім цього, споживачі на тимчасово окупованих територіях залишаються переважно повністю відключеними від українських мереж.

Пошкодження інтернет-інфраструктури, пов'язані з воєнними діями, є серйозною загрозою для реалізації права на доступ до інтернету. Спільні зусилля держави та бізнесу дозволяють відносно швидко відновлювати доступ до послуг, де це можливо. Проте окремі рішення уряду, наприклад впровадження вимог щодо забезпечення безперебійності доступу до мережі під час аварійних відключень електроенергії, критикували через надмірне навантаження на постачальників електронних послуг. Невеликі інтернет-провайдери також скаржилися на податковий тиск через зміну режимів оподаткування, що наразі є предметом розгляду у кількох судових справах.

Попри впровадження правового режиму воєнного стану, в Україні не застосовувались загальні тимчасові обмеження доступу до інтернету. Водночас, діяльність Національного центру оперативно-технічного управління електронними комунікаційними мережами України (НЦУ), що на цей період може видавати обов'язкові для виконання постачальниками розпорядження, потребує більшої правової визначеності та прозорості.

1.1. Забезпечення загального доступу до мережі Інтернет

Право на доступ до інтернету в Україні передбачене Законом України «Про електронні комунікації», який з 2022 року гарантує споживачам отримання універсальної електронної комунікаційної послуги, зокрема послуги широкосмугового доступу до мережі Інтернет у фіксованому місці. Закон також закріплює певні вимоги до такої послуги - а саме її швидкості, що має бути достатньою для підтримки доступу споживачів до низки сервісів - від електронної пошти і медіа до соціальних мереж, месенджерів та відеоз'єднань.

Стандарти щодо якості універсальної послуги встановлюються центральним органом виконавчої влади у сфері електронних комунікацій (з 1 вересня 2023 року ним є Міністерство цифрової трансформації України, до цього - Адміністрація Державної служби спеціального зв'язку та захисту інформації). З 2023 року швидкість передачі даних у кінцевому пункті, тобто для кінцевого споживача, має становити не менше 30 Мбіт/с.

Держава не встановлює вартості універсальної електронної комунікаційної послуги, а тому ціна на її отримання залежить від конкретного постачальника. Закон зобов'язує постачальників надавати універсальні послуги за економічно обґрунтованими, прозорими та недискримінаційними цінами та інформувати споживачів про зміни цін на універсальні послуги не пізніше ніж за 20 календарних днів до їх застосування. Стаття 100 Закону України «Про електронні комунікації» також передбачає проведення державного моніторингу рівня тарифів (цін), однак відповідний проект постанови Кабінету Міністрів України «Про затвердження Порядку здійснення моніторингу рівня тарифів (цін) на універсальні електронні комунікаційні послуги» Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (НКЕК), як відповідальний регуляторний орган опублікувала для обговорення лише у грудні 2024 року.

За декількома рейтингами Україна належить до країн з найдешевшим інтернетом у світі. Дослідження Picodi за 2023 рік зазначає, що середня ціна необмеженого пакету на швидкості 100 Мбіт/с в України становить 6,1$, що є другим показником у світі. Cable.co.uk вимірює вартість 1 ГБ мобільних даних у світі в рамках дослідження Worldwide Data Pricing, і за його інформацією станом на 2023 рік Україна перебувала на шістнадцятій позиції у світі, з середньою вартістю 0,27$. Водночас, в аналітичних матеріалах до Проекту Стратегії розвитку сфери електронних комунікацій України на період до 2030 року зазначається, що у порівнянні з країнами Європи, відносна вартість для населення є найвищою (1,36% від доходу населення).

З даних, поданих Міністерством цифрової трансформації у згаданих аналітичних матеріалах, рівень покриття (частки населення, що має технічну можливість користуватися інтернетом) мобільним широкосмуговим доступом до мережі Інтернет в Україні становить 91% населення, а фіксованого доступу до мережі Інтернет - 88,4% населення. Обидва показники є меншими за аналогічні показники в Європейському Союзі, а тому розглядаються як поле для покращення авторами Стратегії. Цей документ ще не був затверджений, але може слугувати дороговказом для покращення ситуації з забезпеченням права на доступ до інтернету в Україні. Одним з його пріоритетів є розвиток технології 5G, тестовий запуск якої було анонсовано Віце-прем'єр-міністром Михайлом Федоровим у листопаді 2024 році, а також забезпечення 98% населення України мобільним широкосмуговим доступом до мережі Інтернет на середній швидкості не меншій за 90 Мбіт/с.

Загалом, українське законодавство у сфері забезпечення доступу до інтернету відповідає вимогам ЄС та Ради Європи. Втім, державі слід сфокусуватися на його імплементації та практичному досягненні закріплених показників, а також розвивати нові технології доступу до мережі. Для цього слід:

- Схвалити Стратегію розвитку сфери електронних комунікацій України на період до 2030 року та затвердити операційний план її реалізації, із залученням зацікавлених сторін та громадянського суспільства;
- Впровадити систему моніторингу рівня тарифів (цін) на універсальні електронні комунікаційні послуги для оцінки їх доступності та вжиття заходів для реалізації права на отримання універсальної електронної комунікаційної послуги.

1.2. Спеціальні заходи гарантування доступу до мережі Інтернет для вразливих соціальних груп

Українське законодавство передбачає гарантії доступу до інтернету для вразливих соціальних груп. Зокрема, стаття 101 Закону України «Про електронні комунікації»

фактично закріплює право вразливих споживачів на цільову адресну соціальну допомогу, у разі якщо ціни на універсальні електронні комунікаційні послуги не є доступними. Порядок отримання та розмір такої допомоги має встановлюватися Кабінетом Міністрів України. Втім, підзаконних актів на урядовому рівні щодо втілення цієї норми в життя на сьогодні не прийнято; на публічному обговоренні знаходиться лише проект Критеріїв та їх значень для визначення цінової доступності універсальних електронних комунікаційних послуг. Варто зазначити, що дія цієї норми була призупинена на 2024 рік. Закон України «Про Державний бюджет України на 2025 рік» продовжив зупинку ще на рік.

Іншою гарантією є механізми забезпечення права на доступ до мережі Інтернет у географічно віддалених місцевостях. Згадане положення Закону України «Про електронні комунікації» передбачає, що в разі встановлення географічними оглядами розгортання мереж відсутності на певній території універсальної послуги, регуляторний орган (НКЕК) визначає цю територію такою, що потребує забезпечення доступу до універсальних електронних комунікаційних послуг. Для забезпечення доступу до інтернету на таких територіях може бути проведений конкурс з частковим відшкодуванням постачальникам коштів, витрачених на розбудову інфраструктури, або примусове зобов'язання певного постачальника побудувати мережу, знову ж таки, з подальшим відшкодуванням відповідних витрат. НКЕК затвердив таку методологію, і на початку 2024 року вона була зареєстрована у Міністерстві юстиції України, але оглядів за нею ще не проводилося.

Окремо стаття 100 Закону України «Про електронні комунікації» гарантує і сприяння отриманню універсальних електронних комунікаційних послуг споживачами з інвалідністю та вжиття заходів із сприяння забезпеченню їх відповідним термінальним обладнанням та спеціальними засобами, що покращують рівноцінний доступ, включаючи, за необхідності, розпізнавання та синтез мови. Втім, підзаконного урядового акту, який би встановлював механізми реалізації цього права, на сьогодні не ухвалено.

На проблеми з практичною реалізацією позитивних обов'язків держави у цій сфері звертають увагу і в Проекті Стратегії розвитку сфери електронних комунікацій України на період до 2030 року. Однією з основних проблем у сфері автори проекту вважають забезпечення географічної і цінової доступності універсальних послуг, зокрема механізмів надання споживачам з вразливих соціальних груп цільової адресної допомоги на отримання таких послуг та механізмів компенсації постачальникам послуг збитків, завданих виконанням обов'язку з надання універсальних послуг, та відсутність розроблених актів у цій сфері.

Для досягнення цілі в мінімум 75% українських домогосподарств, які мають можливість користуватися фіксованим широкосмуговим доступом до мережі Інтернет зі швидкістю до 1 Гбіт/с, Стратегія передбачає, серед іншого, необхідність забезпечення надавачами послуг інклюзивності доступу до інтернету для осіб з інвалідністю (пільги під час придбання технічних засобів доступу до інтернету та спеціального програмного забезпечення; механізм забезпечення постачальниками електронних комунікаційних послуг доступності для осіб з інвалідністю електронних комунікаційних послуг) та реалізацію універсальної електронної комунікаційної послуги (механізм забезпечення географічної та фінансової доступності універсальної електронної комунікаційної послуги для вразливих соціальних груп споживачів). Проект Стратегії тут перегукується з Національною стратегією із створення безбар'єрного простору в Україні на період до 2030 року. У ній завданнями, спрямованими на досягнення цифрової безбар'єрності, також визначені забезпечення технічної можливості підключення домогосподарств у сільській місцевості до фіксованого широкосмугового

доступу до інтернету, надання пільг для осіб з інвалідністю, а також забезпечення конкурентного середовища операторів та провайдерів фіксованого широкосмугового доступу до інтернету в населених пунктах.

Загалом, українське законодавство у сфері забезпечення доступу до інтернету для вразливих соціальних груп на нормативному рівні є адекватним, але, на жаль, декларативним. Тому державі слід передусім сфокусуватися на його імплементації та практичному досягненні задекларованих завдань. Для цього слід:

- Ухвалити Стратегію розвитку сфери електронних комунікацій України на період до 2030 року;
- Розробити та затвердити на основі її положень, а також положень Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року нормативні акти Кабінету Міністрів України та відповідальних державних органів, що передбачатимуть конкретні заходи, які сприятимуть поліпшенню доступу до інтернету для вразливих категорій населення.

1.3. Гарантування умов для вільного доступу до якісних послуг інтернету

Закон України «Про електронні комунікації» гарантує кінцевим користувачам право на вільний вибір постачальника електронних комунікаційних послуг, а також своєчасне і якісне одержання таких послуг. Це право забезпечується, серед іншого, свободою підприємницької діяльності щодо надання послуг інтернету та зобов'язанням держави забезпечити конкурентне середовище, зокрема через аналіз ринків електронних комунікацій та подальше застосування антимонопольних заходів. Такі заходи можуть застосовуватися регулятором - Національною комісією, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (НКЕК) - у порядку, закріпленому законодавством.

У розрізі надання доступу до інтернету, слід сконцентруватися на роздрібних ринках надання доступу до мобільного зв'язку, що також дозволяє забезпечувати доступ до інтернету, та широкосмугового фіксованого доступу до мережі. Перший з них був визначений у 2023 році НКЕК як такий, що може потребувати запровадження заходів з забезпечення конкуренції, адже 99% ринку займає три оператори. Другий з них є конкурентним: в Україні діє понад 4000 провайдерів, і частка найбільшого з них - ПАТ «Київстар» - не перевищує 16% ринку. У 2024 році НКЕК почав процедуру аналізу ринку мобільного зв'язку на предмет потреби застосовувати до цього ринку конкурентні заходи та визнав його конкурентним.

Водночас, у 2024 році склалася ситуація податкового тиску на постачальників електронних комунікаційних послуг, що може зменшити пропозицію на ринку доступу до інтернету. З кінця вересня 2024 року Державна податкова служба де-факто зобов'язала всіх постачальників переходити зі спрощеної на звичайну систему оподаткування, користуючись двозначністю тлумачення норм Податкового кодексу України. Це призвело до шквалу заяв до НКЕК про призупинення діяльності малими постачальниками, петиції до Кабінету Міністрів, на яку була надана негативна відповідь, а також опозиції зі сторони громадянського суспільства та профільних бізнес-асоціацій. Серед озвучених загроз - погіршення якості послуг доступу до мережі Інтернет та їх доступності, зокрема, під час аварійних відключеннях електроенергії, а також подорожчання послуг для споживачів внаслідок зростання їх собівартості та монополізації ринку. Понад 100 постачальників оскаржили до суду рішення Державної податкової служби про скасування їхньої реєстрації як платників єдиного

податку. Водночас, у парламенті станом на кінець 2024 року не було зареєстровано пропозицій, спрямованих на усунення неоднозначного тлумачення норм податкового законодавства.

Для захисту плюралізму ринку надання послуг з доступу до інтернету необхідно:

- Внести зміни до Податкового кодексу України та Закону України «Про електронні комунікації» задля забезпечення чіткості правового регулювання статусу та вимог (зокрема, у податковій сфері) до постачальників електронних комунікаційних послуг;

1.4. Законність та обґрунтованість обмежень надання послуг доступу до мережі Інтернет

Обмеження надання послуг доступу до мережі Інтернет слід розглядати у загальному та індивідуальному аспектах. У першому з них йтиметься про так звані шатдауни – повне або часткове вимкнення можливості надавати доступ до інтернету на території всієї країни або ж її частини. Другий з них стосується обмеження індивідуальних прав на доступ до інтернету певним категоріям осіб, зокрема засудженим.

Існує декілька норм, що дозволяють шатдауни в Україні поза контекстом воєнного стану. Перш за все, Закон України «Про правовий режим надзвичайного стану» та його стаття 18 дозволяють запроваджувати особливі правила користування зв'язком та передачі інформації через комп'ютерні мережі у разі введення надзвичайного стану у зв'язку з масовими порушеннями громадського порядку. Межі цього обмеження мають встановлюватися відповідним Указом Президента з подальшим затвердженням зі сторони Верховної Ради України.

Також важливою є норма Закону України «Про електронні комунікації». Його стаття 115 передбачає, що для припинення терористичної діяльності може здійснюватися тимчасове обмеження надання електронних комунікаційних послуг споживачам, що перебувають у визначеному районі проведення антитерористичної операції. Також тимчасові обмеження можуть вводитися місцевими органами виконавчої влади та органами місцевого самоврядування за погодженням з Міністерством цифрової трансформації у відповідних регіонах, однак з метою оповіщення та забезпечення електронними комунікаційними послугами учасників ліквідації наслідків надзвичайних ситуацій та відбудовних робіт. На практиці, щоправда, такі обмеження не вводилися жодного разу.

На індивідуальному рівні обмеження доступу до інтернету варто згадати Кримінально-виконавчий кодекс України. Він передбачає право засуджених до позбавлення волі на користування інтернетом під контролем адміністрації у вільний від роботи час їх власним коштом або коштом інших осіб шляхом внесення таких коштів на електронний гаманець. Таким чином, у разі наявності фінансової спроможності, обмеження права на доступ до інтернету в пенітенціарних закладах для ув'язнених не передбачається.

Доступ до інтернету надається за заявою до адміністрації установи та відповідно до графіку роботи інтернет-класу. Відомості про надання засудженим права користуватися інтернетом обліковуються та заносяться до спеціального журналу, як і використання ними IP-телефонії та відеозв'язку. Передбачається, що під час доступу до мережі засудженим дозволяється відвідувати певний перелік сайтів, визначений адміністрацією установи, який формується відповідно до категорій, затверджених порядком Міністерства юстиції. Засуджені можуть отримати доступ до сайтів

органів державної влади та місцевого самоврядування, міжнародних організацій, Європейського суду з прав людини, творчих, освітніх, спортивних, культурних, юридичних та довідкових сайтів, а також до сайтів зареєстрованих медіа; на запит засудженого адміністрація закладу може надати доступ і до інших сайтів.

Водночас, засудженим може бути заборонено вчиняти певні дії в мережі. Так, засудженим заборонено використовувати соцмережі, відвідувати порнографічні сайти, а їх дзвінки можуть перериватися внаслідок використання засудженими агресивної лексики чи нецензурної лайки щодо осіб, з якими вони спілкуються. Крім того, їх листування може переглядатися, за винятком листування з судами, міжнародними організаціями, прокурором та захисником. Таке листування здійснюється винятково через електронну скриньку, зареєстровану під контролем адміністрації пенітенціарної установи. Оскарження в наданні цього права відбувається за загальними правилами, передбаченими для публічно-правових спорів, а саме в рамках адміністративного судочинства.

Попри те, що законодавство України не накладає надмірного простору для шатдаунів та обґрунтовано обмежує право на індивідуальний доступ до інтернету для засуджених, у разі запровадження будь-яких заходів з загального обмеження права на доступ до інтернету, для відповідності вимогам міжнародного права слід:

- Дотримуватися процедур, пов'язаних з належним повідомленням Генерального секретаря ООН та Ради Європи про запровадження правового режиму надзвичайного стану;
- Застосовувати найменш обмежувальний захід для досягнення визначеної мети при надзвичайному стані чи антитерористичній операції;
- Регулярно переглядати запроваджені заходи на предмет їх необхідності та пропорційності.

1.5. Доступ до інтернету в умовах воєнного стану

Закон України «Про правовий режим воєнного стану» дозволяє запроваджувати такі заходи, як регулювання роботи постачальників електронних комунікаційних мереж та/або послуг, а також заборона передачі інформації через комп'ютерні мережі. Повноваженнями щодо такого регулювання наділяється Національний центр оперативно-технічного управління електронними комунікаційними мережами України (НЦУ), що утворюється Адміністрацією Державної служби спеціального зв'язку та захисту інформації (Держспецзв'язку) та є надзвичайним регулятором у сфері електронних комунікацій під час воєнного стану. Законодавчі зміни, що були прийняті у 2022 році невдовзі після повномасштабного вторгнення, формалізували його повноваження щодо видачі розпоряджень, які є обов'язковими для виконання постачальниками під час правового режиму воєнного стану. До його компетенції відноситься введення тимчасових обмежень у наданні послуг користувачам, що закріплене Постановою Кабінету Міністрів України від 29 червня 2004 року № 812, яка регулює діяльність НЦУ. У окремих розпорядженнях НЦУ також міститься посилання на Положення про НЦУ, затверджене наказом Адміністрації Держспецзв'яку № 209 від 11 квітня 2019 року зі змінами, однак його тексту у вільному доступі немає.

В Україні не запроваджувалися шатдауни у класичному розумінні цього слова, навіть попри воєнний стан. Обмеження у наданні послуг, були найчастіше викликані обстрілами зі сторони російських військ та супутніми вимкненнями електроенергії. Втім, у лютому 2024 року НЦУ видав Розпорядження про забезпечення сталості

електронних комунікаційних мереж в умовах воєнного стану та декілька разів вносив до нього зміни. Цей документ передбачав обов'язок постачальників електронних комунікаційних мереж та/або послуг забезпечити безперервну роботу мереж протягом визначених періодів часу (10 годин у випадках вимкнень для 100% базових станцій мобільного зв'язку до 1 лютого 2025 року, 72 години для провайдерів локальних мереж інтернету до 1 грудня 2024 року). Він спричинив серйозні виклики для провайдерів, хоча за оцінками голови Держспецзв'язку, частина вимог була в цілому виконана.

27 лютого 2022 року НЦУ видав розпорядження про блокування автономних систем (AS), пов'язаних з Росією. Автономні системи є кластерами IP-адрес, асоційованими з російськими постачальниками інтернету. Сукупно цим, а також ще двома розпорядженнями НЦУ було заблоковано понад 600 автономних систем з понад 48 мільйонами IP-адрес, тобто майже весь російський сегмент мережі. Ці розпорядження діятимуть до кінця воєнного стану, хоча інформації про стан їх виконання постачальниками немає.

Запроваджені обмеження можуть бути виправданими потребою захисту українських користувачів від кібератак та загроз, а також від шкідливого контенту, що розповсюджується у російському сегменті інтернету. Втім, компетенція НЦУ видавати рішення про блокування автономних систем є недостатньо чітко передбаченою у законодавстві. Застосування таких заходів на хиткому законодавчому ґрунті могло бути виправданим на початку повномасштабного вторгнення, коли оперативне реагування на загрози потребувало гнучкості та дискреції для надзвичайного регулятора. Наприкінці третього року великої війни держава мала б забезпечити чіткіший порядок роботи такого органу, передбачивши його компетенції у онлайн-сфері, а також забезпечивши додаткову прозорість його функціонування, зокрема щодо централізованої публікації його рішень та визначення того, які рішення можуть чи не можуть оприлюднюватися на сайті Держспецзв'язку, як це відбувається зараз.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- Ухвалити зміни до постанови Кабінету Міністрів України від 29 червня 2004 року № 812, уточнивши сфери повноважень НЦУ щодо блокування автономних систем, а також впровадивши чіткі вимоги щодо оприлюднення розпоряджень НЦУ, що не містять інформації з обмеженим доступом;
- Провести аналіз ефективності та переглянути відповідно вимоги, пов'язані із забезпеченням безперебійного доступу до інтернету, особливо з урахуванням можливостей представників малого бізнесу;
- Після закінчення правового режиму воєнного стану забезпечити перегляд рішень НЦУ про обмеження доступу до інтернет-ресурсів та інших запроваджених обмежень.

СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Попри продовження повномасштабної війни, у сфері свободи вираження поглядів українська влада поки що не вдавалась до масових обмежень та навіть продовжує активно гармонізувати національне законодавство з правом ЄС у сфері медіа та прав журналістів. Значну роль в підтриманні балансу відіграють правозахисні та медійні організації, які вчасно відстежують потенційні ризики та долучаються з конструктивною критикою та пропозиціями щодо вдосконалення регулювання.

Водночас, актуальними залишаються проблеми, пов'язані із безкарністю злочинів проти журналістів та використанням дифамаційних позовів як спроб цензурувати медіа, браком правової визначеності в процедурах та підставах застосування санкцій у онлайн сфері, необґрунтованим обмеженням доступу до суспільно важливої інформації та браком належних ресурсів для посилення інституцій, відповідальних за повноцінне впровадження європейських стандартів у сфері свободи вираження поглядів та медіа.

2.1. Свобода отримувати та поширювати інформацію онлайн

2.1.1. Законодавчі гарантії свободи отримувати та поширювати інформацію онлайн

Конституція України у статті 34 гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, що відображається у праві кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір. Цією ж нормою передбачені і обмеження свободи вираження поглядів. Вони мають бути встановлені законом:

- в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам;
- для охорони здоров'я населення;
- для захисту репутації або прав інших людей;
- для запобігання розголошенню інформації, одержаної конфіденційно;
- для підтримання авторитету і неупередженості правосуддя.

Ця норма є основною у чинній національній системі захисту свободи вираження поглядів. Хоча вона не повною мірою відтворює положення статті 10 Конвенції про захист прав людини та основоположних свобод (Конвенції) та статті 19 Міжнародного пакту про громадянські та політичні права, випускаючи вимогу необхідності обмеження в демократичному суспільстві, загалом вона створює належну законодавчу рамку на національному рівні. Крім того, врахування практики Європейського суду з прав людини, який тлумачить статтю 10 Конвенції, передбачене вимогами статті 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини».

Положення Конвенції та Пакту також враховані у спеціальних законах, які врегульовують відносини, пов'язані з поширенням та отриманням інформації. Стаття 5 Закону України «Про інформацію» постулює право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної

для реалізації своїх прав, свобод і законних інтересів - у разі, якщо здійснення такого права не порушує прав інших осіб та не становить зловживання інформацією відповідно до статті 28 того ж Закону. Стаття 6 Закону відтворює конституційні принципи обмеження цього права. Своєрідним продовженням цього законодавства є корпус норм щодо права на доступ до публічної інформації, закріплений в однойменному законі. Його положення гарантують відкритість інформації, що створюється суб'єктами владних повноважень та іншими розпорядниками, а також передбачають відповідний регуляторний механізм щодо оскарження порушень права на доступ до інформації.

Стаття 4 Закону України «Про медіа» також закріплює свободу діяльності у сфері медіа, що спирається на свободу вираження поглядів і переконань, свободу поширення, обміну та отримання інформації. Також у цьому Законі наголошується на потребі дотримання трискладового тесту обмеження прав людини при втручанні у діяльність медіа, включно з критерієм необхідності в демократичному суспільстві, наявним у Конвенції та відсутнім у Конституції.

Право на судове оскарження будь-якого рішення, дій чи бездіяльності органів державної влади та органів місцевого самоврядування, а також на звернення до Уповноваженого Верховної Ради України з прав людини за захистом власних прав, гарантоване статтею 55 Конституції України. Ця норма поширюється і на порушення права свободи вираження поглядів зі сторони представників держави в загальних рамках адміністративного судочинства.

2.1.2. Законні та обґрунтовані підстави блокування Інтернет-ресурсів та фільтрування онлайн-контенту

Блокування Інтернет-ресурсів. На кінець 2024 року в Україні існувало п'ять механізмів блокування веб-сайтів (не рахуючи механізми, пов'язані із запровадженням правового режиму воєнного стану). Два з них можуть використовуватися за рішенням суду, для двох необхідним є рішення регуляторного органу, яке може бути оскаржене до суду, а ще один є наслідком застосування політико-правового інструменту санкцій. Згаданими механізмами є:

- Блокування ресурсів, через які здійснюється розповсюдження дитячої порнографії, на підставі рішення суду постачальниками електронних комунікаційних послуг за частиною третьою статті 18 Закону України «Про електронні комунікації»;
- Блокування ресурсів, через які надається доступ до проведення азартних ігор без належної ліцензії, на підставі рішення Комісії з регулювання азартних ігор та лотерей (КРАІЛ) власником такого ресурсу або постачальником послуг хостингу за статтею 25 Закону України «Про державне регулювання діяльності щодо організації та проведення азартних ігор»;
- Заборона поширення анонімних онлайн-медіа у разі вчинення протягом одного місяця 3 незначних або значних або 2 грубих порушень, а також тимчасова заборона поширення незареєстрованих онлайн-медіа строком на 14 днів у разі вчинення ними протягом одного місяця 5 значних порушень, за які було накладено штрафи, на підставі рішення Національної ради України з питань телебачення і радіомовлення за частинами шістнадцятою та тринадцятою статті 116 Закону України «Про медіа»;
- Заборона поширення зареєстрованих онлайн-медіа у разі вчинення впродовж одного місяця 4 грубих порушень, а також заборона поширення незареєстрованих онлайн-медіа у разі вчинення впродовж одного місяця

3 грубих порушень на підставі рішення суду за частинами чотирнадцятою-п'ятнадцятою статті 116 Закону України «Про медіа»;

- Блокування доступу до інформаційних ресурсів, які використовуються для демонстрації та використання символіки терористичних організацій і груп, пропагування ідей та програмних цілей таких організацій (груп) на підставі рішення Ради національної безпеки та оборони України (РНБО), затвердженого Указом Президента України за статтями 4-5 Закону України «Про санкції».

Перші чотири механізми стосуються протиправного контенту та або гарантують судову процедуру винесення рішення про обмеження доступу до сайту, або ж накладаються незалежним регулятором після досить довгої комунікації з суб'єктами щодо постійної протиправності вчинюваних ними дій. Лише один з них застосовувався у 2024 році: КРАІЛ прийняв рішення про блокування 105 сайтів. Національна рада отримала відповідні повноваження наприкінці березня 2024 року і не користувалася ними, а в Єдиному державному реєстрі судових рішень відсутні рішення прийняті відповідно до норм Закону України «Про електронні комунікації».

Більш проблемним є механізм блокувань, передбачений Законом України «Про санкції». Новий санкційний захід - блокування доступу до інформаційних ресурсів, які використовуються для демонстрації та використання символіки терористичних організацій і груп, пропагування ідей та програмних цілей таких організацій (груп) - був доданий до законодавства у 2023 році. Чинне формулювання не містить виключень щодо використання забороненої символіки із освітньою, новинною чи іншою легітимною метою. Крім того, практика її застосування викликає питання щодо правової визначеності текстів самих указів про накладення санкцій. У 2024 році цю санкцію було застосовано у трьох указах (щодо російських медіа, медіа Ігоря Гужви та Анатолія Шарія та громадянина України Олексія Селіванова), причому жодного разу без вказівки на те, які безпосередньо ресурси мають бути заблоковані.

Також продовжується практика застосування Закону України «Про санкції» для блокування сайтів іншим чином, а саме через використання пункту про можливість накладення «інших санкцій, що відповідають принципам застосування, встановленим цим Законом». Ця практика склалася ще з 2017 року, і на її невідповідності міжнародним стандартам у сфері захисту прав людини неодноразово наголошували фахівці. Основними проблемами застосування цього механізму були використання неоднакових формулювань щодо блокувань, практика блокування сайтів накладанням санкцій на фізичних осіб, включно з громадянами України та померлими та неузгодженість строковості накладення санкцій. Також фахівці наголошували і на потребі наводити належну інформацію, що дала б зрозуміти підстави застосування відповідної санкції до певного суб'єкта. У 2024 році цей пункт Закону використовувався для блокування сайтів у 6 указах Президента, почасти - поруч з попереднім видом санкцій. Крім того, заблокованими на підставі застосування цієї норми залишаються понад 800 сайтів. У 2024 році українському урядові була комунікована перша справа щодо відповідності цього механізму Європейській конвенції з прав людини, що стосується блокування російських соцмереж у 2017 році.

У 2024 році також пропонувалися окремі зміни до законодавства у санкційній сфері, що можуть вплинути на систему блокувань. Зокрема, урядовий Проект Закону № 11492 про внесення змін до Закону України «Про санкції» щодо заборони використання програмних продуктів та доступу до електронних інформаційних ресурсів пропонує запровадити таку санкцію як «заборона доступу до електронних інформаційних ресурсів в Інтернеті (веб-сторінки, веб-сайти, інші веб-ресурси), електронних комунікаційних мережах, електронних комунікаційних системах, інформаційних

системах, інформаційно-комунікаційних системах». Наразі цей законопроект перебуває на розгляді у Комітеті Верховної Ради України з питань національної безпеки, оборони та розвідки. Хоча він частково вирішує проблему з відсутністю чіткої норми, яка б дозволяла блокувати сайти в Інтернеті на підставі санкцій, його положення не надають чіткості щодо порядку втілення цієї санкції в життя. Інший Проект Закону № 12102 про внесення змін до деяких законів України щодо формування та ведення переліку терористичних організацій (груп), прийнятий у грудні 2024 року, але підписаний Президентом вже у 2025 році, передбачає процедуру формування переліку терористичних організацій. Її запровадження, а також формування відповідного переліку, додасть чіткості у можливому застосуванні так званого «терористичного блокування», вже передбаченого санкційним законодавством.

Фільтрування та видалення онлайн-контенту. Чинне законодавство не містить положень щодо фільтрування онлайн-контенту. Втім, два законодавчих акти, а саме Закон України «Про медіа» та Закон України «Про авторське право і суміжні права», містять положення, що потенційно дозволяють вимагати обмежувати доступ до конкретного контенту в мережі.

Частина третя статті 99 Закону України «Про медіа» надає Національній раді право звертатися до провайдерів онлайн-платформ та уповноважених представників пошукових систем з вимогами обмежити доступ до інформації та/або виключити з результатів пошуку, що видаються за запитами користувачів, посилання на інформацію, яка порушує вимоги законодавства України у разі, якщо за її поширення до суб'єкта у сфері медіа було застосовано будь-яку санкцію, окрім припису. Втім, з огляду на описану в 2.3.1 цього Звіту юрисдикційну проблему, на практиці реалізація цієї норми буде ускладнена. Національна рада у 2024 році не зверталася до цієї процедури.

Стаття 56 Закону України «Про авторське право і суміжні права» встановлює процедуру припинення порушень авторського права в Інтернеті. Її норми передбачають, що обмеження доступу можливе лише до цифрового контенту, і у крайньому випадку - до веб-сторінки, що містить контенту, який порушує авторське право. Процедура такого обмеження є позасудовою, а суб'єктами, що мають обмежувати доступ до контенту - власник веб-сайту або постачальник послуг хостингу.

Для гармонізації українського законодавства та його імплементації у цій сфері з вимогами ЄС та Ради Європи, варто:

- Внести зміни до Закону України «Про санкції» з метою уточнення підстав та порядку блокування веб-сайтів та унеможливлення його застосування для обмеження діяльності національних медіа, а також забезпечення оприлюднення підстав їх застосування до відповідних суб'єктів у Державному реєстрі санкцій;
- Ухвалити законодавство, яке дозволить належно застосовувати обмеження терористичного контенту онлайн, з урахуванням винятків для легальних можливостей використання терористичної символіки на веб-сайтах в новинних, освітніх, історичних та інших законних цілях, та у відповідності з підходами ЄС;
- У разі запровадження законодавчих змін, окреслених вище, переглянути попередні рішення про блокування сайтів на підставі санкцій на предмет їх необхідності, пропорційності та відповідності законодавству.

2.1.3. Обмеження свободи вираження поглядів, запроваджені в інтересах національної безпеки, територіальної цілісності, громадської безпеки, для запобігання заворушенням чи злочинам

Норми, що в широкому сенсі спрямовані на забезпечення національної безпеки шляхом обмеження протиправних висловлювань, містяться у різних законодавчих актах, що охоплюють різних суб'єктів залежно від сфери дії такої норми. Основними сферами, на які слід звернути увагу, є кримінальне, адміністративно-деліктне та медійне законодавство, позаяк норми статті 28 Закону України «Про інформацію», що передбачає види зловживання інформацією, на практиці втілюються в життя через реалізацію цих норм. Також варто окремо згадати і законодавство, що забороняє пропаганду певної символіки, адже воно залишається несинхронізованим з кримінальним, адміністративно-деліктним та медійним законодавством щодо застосування заходів відповідальності.

Кримінальне та адміністративно-деліктне законодавство. Кримінальний кодекс України передбачає низку норм, які криміналізують певні типи висловлювань незалежно від медіуму їх висловлювання, тобто і в Інтернеті. Частина з них є нічим іншим, як обмеженням свободи вираження поглядів задля забезпечення інтересів національної безпеки, територіальної цілісності, громадської безпеки, а також запобігання заворушенням чи злочинам. У цьому контексті слід згадати такі норми:

- стаття 109 (публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади – до 3 років позбавлення волі, а у разі використання засобів масової інформації – до 5 років; у обох випадках можливою є конфіскація майна);
- стаття 110 (публічні заклики чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України – до 5 років позбавлення волі, а у разі, якщо вони призвели до загибелі людей чи інших тяжких наслідків – аж до довічного позбавлення волі; у обох випадках можливою є конфіскація майна);
- стаття 111-1 (публічне заперечення здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України – позбавлення права займатися певною діяльністю чи займати певні посади на строк від 10 до 15 років; здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України – позбавлення волі від 10 до 12 років з позбавленням права займатися певною діяльністю чи займати певні посади на строк від 10 до 15 років та можливою конфіскацією майна, а якщо ця діяльність призвела до загибелі людей чи інших тяжких наслідків – 15 років позбавлення волі або довічне позбавлення волі з усіма перерахованими додатковими покараннями);
- стаття 258-2 (публічні заклики до вчинення терористичного акту – до 3 років позбавлення волі, а у разі використання засобів масової інформації – до 5 років

з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років; у обох випадках можливою є конфіскація майна);

- стаття 295 (публічні заклики до погромів, підпалів, знищення майна, захоплення будівель чи споруд, насильницького виселення громадян, що загрожують громадському порядку - до 3 років обмеження волі);
- стаття 436 (публічні заклики до агресивної війни або до розв'язування воєнного конфлікту та виготовлення матеріалів, що їх містять - до 3 років позбавлення волі);
- стаття 436-1 (публічне використання символіки комуністичного, націонал-соціалістичного (нацистського) тоталітарних режимів - до 5 років позбавлення волі, а у разі використання засобів масової інформації - до 10 років позбавлення волі; в обох випадках можливою є конфіскація майна; стаття також окремо передбачає винятки легітимного використання такої символіки);
- стаття 436-2 (виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, розпочатої у 2014 році, у тому числі шляхом представлення збройної агресії Російської Федерації проти України як внутрішнього громадянського конфлікту, виправдовування, визнання правомірною, заперечення тимчасової окупації частини території України, а також глорифікація осіб, які здійснювали збройну агресію Російської Федерації проти України, розпочату у 2014 році - до 3 років позбавлення волі, у разі виготовлення матеріалів з такими закликами - від 3 до 5 років позбавлення волі, а у разі використання для цього засобів масової інформації - від 5 до 8 років позбавлення волі; в останніх двох випадках можливою є конфіскація майна);
- стаття 442 (прямі та публічні заклики до геноциду, а також виготовлення та розповсюдження матеріалів, що їх містять - від 3 до 7 років позбавлення волі).

У 2024 році у цій сфері було прийнято лише один закон, що змінював положення Кримінального кодексу у зв'язку з ратифікацією Римського статуту. Його положення змінили статтю 442 щодо закликів до геноциду, таким чином забезпечивши відповідність диспозиції норми статті 25 Статуту.

Водночас, змін потребують і інші положення кримінального законодавства, зокрема положення статті 436-1 Кримінального кодексу, прийняті в рамках декомунізаційного законодавства, та низка норм (статті 111-1 та 436-2 Кримінального кодексу), що були ухвалені Верховною Радою у березні 2022 року на початку вторгнення. Надмірність санкцій, передбачених статтею 436-1 Кодексу, була фактором, на який звернула увагу Венеціанська комісія у своєму висновку ще у 2015 році, і ці положення не були виправлені, попри спроби подати відповідний законопроект ще у парламенті попереднього скликання. В той же час, диспозиції норм частини першої статті 111-1 та частини першої статті 436-2 Кодексу створюють ситуацію, коли особу можуть двічі покарати за одне і те ж діяння відповідно до різних норм Кримінального кодексу. Відсутність гармонізації цих норм може призводити до надмірних негативних наслідків для тих, хто вчиняє правопорушення, та має бути виправлена.

Окремо слід зупинитися і на практиці застосування цих норм. Дослідження Платформи прав людини у 2023 році, вказує на задавнені проблеми судової влади щодо розгляду справ за відповідними статтями Кримінального кодексу. Національні суди не проводять самостійного аналізу тексту та змісту висловлювань, які стали підставою для обвинувачень у порушенні, покладаючись на висновки експертизи без додаткової їх оцінки. Більшість вироків не містять цитат та опису висловлювань, які

стали підставою для притягнення до відповідальності, та не містять аналізу аудиторії, яка могла ознайомитися з тим чи іншим дописом, а в окремих випадках зустрічаються випадки притягнення до відповідальності за лайки та репости контенту. Також суди продовжують розглядати соцмережі як «засоби масової інформації» всупереч оновленому медійному законодавству, яке виділяє онлайн-платформи в окрему категорію суб'єктів. Така класифікація має наслідком застосування норми, яка містить більшу санкцію.

Кодекс України про адміністративні правопорушення також містить дві норми, що мають легітимною метою обмеження, пов'язані з національною безпекою та публічним порядком. Стаття 173-3 Кодексу передбачає відповідальність за публічне використання, демонстрацію або носіння георгіївської (гвардійської) стрічки. У 2024 році Європейський суд з прав людини у рішенні щодо прийнятності у справі Borzykh v Ukraine визнав правомірність такого обмеження та його відповідність статті 10 Європейської конвенції про права людини. Стаття 173-1 Кодексу також забороняє поширювати неправдиві чутки, що можуть викликати паніку серед населення або порушення громадського порядку.

Медійне законодавство. Стаття 36 Закону України «Про медіа» також містить низку обмежень, які спрямовані на забезпечення цих законних інтересів. Її положення забороняють медіа публікувати:

- заклики до насильницької зміни, повалення конституційного ладу, розв'язування або ведення агресивної війни або воєнного конфлікту, порушення територіальної цілісності України, ліквідації незалежності України, інформацію, яка виправдовує чи пропагує такі дії;
- пропаганду або заклики до тероризму та терористичних актів, інформацію, що виправдовує чи схвалює такі дії;
- інформацію, що заперечує або виправдовує злочинний характер комуністичного тоталітарного режиму 1917-1991 років в Україні, злочинний характер націонал-соціалістичного (нацистського) тоталітарного режиму, створює позитивний образ осіб, які обіймали керівні посади у комуністичній партії (посаду секретаря районного комітету і вище), вищих органах влади та управління СРСР, УРСР (УСРР), інших союзних та автономних радянських республік (крім випадків, пов'язаних з розвитком української науки та культури), працівників радянських органів державної безпеки, виправдовує діяльність радянських органів державної безпеки, встановлення радянської влади на території України або в окремих адміністративно-територіальних одиницях, переслідування учасників боротьби за незалежність України у XX столітті;
- інформацію, що містить символіку комуністичного або націонал-соціалістичного (нацистського) тоталітарного режиму, крім випадків, передбачених Законом України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки»;
- інформацію, що містить пропаганду російського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, а також символіку воєнного вторгнення російського тоталітарного режиму, крім випадків, передбачених Законом України «Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну»;

- інформацію, що принижує або зневажає державну мову;
- інформацію, що заперечує або ставить під сумнів існування українського народу (нації) та/або української державності та/або української мови.

Детальніше стандарти застосування передбачених законом обмежень мають розробити органи спільного регулювання, що розпочали свою діяльність у 2024 році. Один з них – у сфері аудіовізуальних медіа – визначив питання, пов'язані з національною безпекою пріоритетними для власної діяльності у 2025 році. Санкцій за порушення цих норм до онлайн-медіа та VOD-сервісів у 2024 році Національна рада України з питань телебачення і радіомовлення не застосовувала.

Законодавство щодо заборони символіки. Після повномасштабного вторгнення, Україна посилила політику пам'яті та закріпила у законодавстві додаткові обмеження щодо пропаганди певних режимів та їх символіки. Було прийнято два закони: «Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну» та «Про засудження та заборону пропаганди російської імперської політики в Україні і деколонізацію топонімії». Обидва з них містять визначення забороненого контенту та символіки, а також винятки для їх правомірного використання. Втім, у законодавстві, що спрямоване на протидію російській імперській політиці, виняток, залишений для медіа, може бути незастосовним до інших типів медіа, окрім аудіовізуальних, оскільки передбачає звільнення від відповідальності лише в інформаційних, інформаційно-аналітичних програмах та документальних фільмах. Аналогічна хиба збережена і в Законі України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки».

Законопроект № 12062 пропонує внести зміни до Кодексу України про адміністративні правопорушення та Кримінального кодексу України щодо встановлення відповідальності за пропаганду символіки російської імперської політики в Україні, визначеної відповідним законом: адміністративні штрафи у розмірі 1700-3400 гривень для фізичних осіб та 3400-5100 гривень для посадових осіб. Кримінальна відповідальність передбачена для випадків, коли така символіка використовується в органах державної влади і місцевого самоврядування та на підприємствах державної і комунальної власності. Також пропоновані норми містять посилання на винятки щодо правомірних випадків використання такої символіки. Втім, при внесенні подібних змін до законодавства слід зважати на уже існуючу потребу узгодження норм кримінального права щодо розмежування різних правопорушень, суспільну небезпечність поширення певного висловлювання та пропорційність покарання.

Для гармонізації українського законодавства та його імплементації у цій сфері з вимогами ЄС, Ради Європи та рекомендаційними документами на рівні ООН, варто:

- Переглянути та змінити норми Кримінального кодексу України, що встановлюють відповідальність за протиправні висловлювання з метою захисту національної безпеки, задля уникнення конкуренції норм та гарантування пропорційності санкції через додавання альтернативних видів покарання;

- Уніфікувати підходи до обмеження демонстрації символіки та її пропаганди, зокрема розширивши винятки правомірного використання такої символіки для медіа;

- Сприяти розробці кодексів спільного регулювання для медіа щодо визначення критеріїв віднесення інформації до такої, яку заборонено поширювати на території України відповідно до пунктів 1, 4, 10-14 частини першої статті 36 Закону України «Про медіа»;

- Сприяти підвищенню кваліфікації суддів у сфері розгляду справ, пов'язаних з поширенням протиправного контенту в Інтернеті, для кращого врахування стандартів практики Європейського суду з прав людини.

2.1.4. Обмеження свободи вираження поглядів, пов'язані з захистом репутації і прав інших осіб

Стаття 34 Конституції України гарантує кожному право на свободу думки і слова та на вільне вираження своїх поглядів і переконань. Проте також передбачає, що ці права можуть бути обмежені за законом для захисту репутації або прав інших людей. Балансування свободи вираження поглядів та права на повагу до приватного життя та репутації особи неодноразово здійснював Європейський суд з прав людини у справах щодо України по статті 10 Конвенції про захист прав людини та основоположних свобод, завдяки чому національне законодавство оновлювалось із врахуванням європейських стандартів.

Закон України "Про інформацію" у статті 30 розмежовує факти та оціночні судження. Ніхто не може бути притягнений до відповідальності за висловлювання оціночних суджень. Оціночні судження не містять фактичних даних, які можна було б спростувати, але можуть бути висловленими за допомогою певних мовностилістичних засобів, як от сатира, гіперболи, алегорії. Якщо особа вважає, що оціночні судження або думки принижують її гідність, честь чи ділову репутацію, а також інші особисті немайнові права, вона вправі скористатися наданим їй законодавством правом на відповідь, а також на власне тлумачення справи у тому самому медіа з метою обґрунтування безпідставності поширених суджень, надавши їм іншу оцінку. Якщо суб'єктивну думку висловлено в брутальній, принизливій чи непристойній формі, що принижує гідність, честь чи ділову репутацію, на особу, яка таким чином та у такий спосіб висловила думку або оцінку, може бути покладено обов'язок відшкодувати завдану моральну шкоду. Водночас, така думка спростуванню не підлягає, оскільки не є фактичною інформацією.

Національне законодавство враховує статус «публічних осіб», визнаючи ширші межі критики та втручання у їх приватне життя, а також забороняє обмежувати доступ до інформації, що є предметом суспільного інтересу: свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, інформація про шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо. Для журналістів Закон України «Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста», передбачає додатковий захист та звільняє їх від відповідальності за поширення інформації, що не відповідає дійсності, якщо суд встановить, що журналіст діяв добросовісно та здійснював її перевірку.

Водночас, на практиці суди не завжди коректно імплементують законодавчі гарантії. Так, наприклад, у 2024 році Верховний суд своєю постановою скасував рішення судів першої та апеляційної інстанцій та вказав на помилковість їх висновків про спростування недостовірної інформації шляхом розміщення на сторінці групи у фейсбуці публічних вибачень. Верховний суд узгодив свою позицію із рішенням ЄСПЛ у справі "Редакція

газети “Правовоє дєло” та Штекель проти України”, відповідно до якого вибачення не є засобом захисту честі, гідності та репутації, оскільки не передбачене чинним цивільним законодавством. У інших справах Верховний суд також відзначав неправильне застосування норм щодо розмежування фактів та оцінок.

На сьогодні наявного рівня імплементації європейських стандартів щодо балансування свободи вираження поглядів та захисту репутації і приватності вже недостатньо. Одним із поширених інструментів тиску на журналістів та медіа залишаються так звані «стратегічні позови проти участі громадськості» (СППУГ, або англ. SLAPPs - “strategic litigation against public participation”), особливістю яких є, зокрема, мета зупинити суспільне обговорення, легітимну критику чи протести, та стримати журналістів чи інших представників активної громадськості від подібного висвітлення у майбутньому.

У грудні 2024 року працівник ДБР та колишній прокурор Олександр Говорущак подав на Слідство.Інфо» та журналістку Яніну Корнієнко до суду через розслідування про придбання йогоріднею майна, яке могло коштувати 35 мільйонів гривень. Посадовець вимагає спростувати та видалити всю опубліковану інформацію, пов’язану з ним та йогоріднею, а також відшкодувати по 40 тис. гривень моральної шкоди з кожного відповідача. Раніше, у 2023 році український бізнесмен Сергій Семенюк подав позов про захист честі, гідності та ділової репутації, у зв’язку з публікацією розслідування про зв’язки його клінінгових компаній із росією, проти редакції «Слідства.Інфо» та авторки матеріалу Яніни Корнієнко. При цьому його адвокати намагалися маніпулювати процедурою електронного розподілу суддів, яка автоматично визначає, хто буде розглядати справу, та навіть обрали додаткового відповідача для того, щоб обґрунтувати подання позову саме до відповідного районного суду.

Колишня суддя Донецького окружного адміністративного суду Людмила Арестова у грудні 2024 року подала позов про захист честі, гідності та ділової репутації проти української служби Радіо Свобода та журналіста “Схем” Георгія Шабаєва. Екс-суддя у своєму позові просить визнати інформацію з розслідування “Схем” про її російське громадянство недостовірною та такою, що порочить честь, гідність та ділову репутацію, видалити з публікації її фотографії, які “Схеми” знайшли у відкритих джерелах, а також стягнути 180 тис. гривень компенсації за моральну шкоду.

Яскравим прикладом СППУГ є численні позови колишнього посадовця часів Віктора Януковича Андрія Портнова, які явно спрямовані на те, щоб журналісти менше висвітлювали інформацію про його діяльність через загрозу судових справ. У 2020 році Андрій Портнов позивався до програми журналістських розслідувань “Схеми” та їх головної редакторки Наталки Седлецької з вимогами визнати недостовірною інформацію про його причетність до підпалу автомобіля водія знімальної групи та його погрози редакції. Печерський районний суд задовольнив позов Портнова. У вересні 2024 року це рішення підтримав Київський апеляційний суд. Журналісти подали касаційну скаргу. У іншій справі за позовом Портнова, у грудні 2024 року Київський апеляційний суд підтримав рішення Печерського районного суду та зобов’язав hromadske видалити розслідування про його можливу причетність до процесів, пов’язаних із окупацією Криму у 2014 році, а також стягнув суму компенсації за правничу допомогу у розмірі 56 тисяч гривень та 15 тисяч гривень за послуги адвоката. Редакція готує скаргу до Верховного суду.

На місцевому рівні подібні позови теж є поширеними і можуть мати ще більш «охолоджувальний ефект». У 2023 році головна редакторка інтернет-видання “Волинь Online” Мар’яна Метельська повідомила, що група компаній “Технторг” подала судовий позов проти неї через її розслідування про можливий зв’язок їх діяльності

з Росією та Білоруссю. Позивачі вимагають спростування інформації та стягнути з редакторки 750 тис. грн компенсації моральної шкоди. Справа розглядається у суді першої інстанції.

У грудні 2024 року Рада Європи представила попередні законодавчі та політичні пропозиції для впровадження стандартів Ради Європи та ЄС щодо протидії використанню стратегічних позовів проти участі громадськості в Україні. Документ містить слушні рекомендації щодо оновлення процесуальних кодексів, Закону України «Про судовий збір», а також розглядає можливість ухвалення окремого закону, який визначатиме поняття СППУГ, його характеристики та додаткові заходи для захисту, наприклад, механізми підтримки осіб, постраждалих від СППУГ. Пропозиції розроблені на основі Рекомендації CM/Rec(2024)2 Комітету міністрів державам-членам щодо протидії використанню стратегічних позовів проти участі громадськості від 5 квітня 2024 року. При внесенні змін до законодавства важливо також брати до уваги положення Директиви Європейського Союзу (ЄС) 2024/1069 Європейського парламенту та Ради від 11 квітня 2024 року «Про захист осіб, які беруть участь у громадських дискусіях, від очевидно необґрунтованих позовів або неправомірних судових розглядів (стратегічні позови проти участі громадськості)».

Для гармонізації українського законодавства з вимогами ЄС, рекомендаціями Ради Європи та ООН, необхідно:

- розробити та запровадити зміни до законодавства щодо протидії СППУГ, яке включатиме визначення та основні характеристики СППУГ, необхідні процесуальні гарантії та запобіжники від зловживань, захист та підтримку постраждалих, відповідно до Рекомендацій Комітету міністрів Ради Європи Rec(2024)2 та Директиви Європейського Союзу (ЄС) 2024/1069;
- створити механізми для моніторингу та підвищення обізнаності про шкоду від СППУГ, включно з тренінгами для суддів, прокурорів та адвокатів;
- ініціювати професійні обговорення змін до Правил адвокатської етики щодо неетичності СППУГ та їх розмежування із обґрунтованими позовами щодо захисту честі, гідності чи ділової репутації особи.

2.1.5. Обмеження свободи вираження поглядів для захисту моралі та охорони здоров'я

Конституція України не вказує «захист моралі» як окрему підставу для обмеження свободи слова, тож будь-які «моральні» застереження допустимі, лише якщо належно обґрунтовані необхідністю захисту інтересів національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, охорони здоров'я населення, захисту репутації або прав інших людей, запобігання розголошенню інформації, одержаної конфіденційно, або підтримання авторитету і неупередженості правосуддя.

Контраверсійний Закон України «Про захист суспільної моралі», який встановлював «правові основи захисту суспільства від розповсюдження продукції, що негативно впливає на суспільну мораль» втратив чинність у 2023 році, у зв'язку з ухваленням Закону України «Про медіа». Останній у статті 36 забороняє поширювати у медіа та на платформах спільного доступу до відео порнографічні матеріали, пропаганду вживання наркотичних засобів, психотропних речовин, пропаганду жорстокого поводження з тваринами. За порушення передбачено застосування припису або штраф (для онлайн медіа - до 10 мінімальних заробітних плат, якщо не виконано

припис або це повторне значне порушення за один місяць). Поширення матеріалів, що заохочують сексуальну експлуатацію та насильство над дітьми, демонструють статеві відносини дітей, використовують образ дітей (візуальний запис образу дітей) у видовищних заходах сексуального чи еротичного характеру є грубим порушенням, за яке до суб'єктів у сфері онлайн-медіа застосовується штраф до 15 мінімальних заробітних плат (якщо одноразове порушення). Стаття 42 Закону «Про медіа» також регулює правила поширення окремих видів контенту для уникнення заподіяння шкоди дітям. Детальніше про це у наступному розділі.

У 2024 році тривала дискусія щодо декриміналізації порнографії (крім дитячої). Чинна стаття 301 Кримінального кодексу України встановлює відповідальність за розповсюдження творів, зображень, кіно- та відеопродукції порнографічного характеру з можливим максимальним покаранням до 5 років позбавлення волі. Ще у 2022 році петиція щодо декриміналізації порнографії набрала 25 тисяч голосів. Пізніше того ж року Коаліція громадських організацій закликала декриміналізувати поширення порнографічного контенту. 18 вересня 2023 був зареєстрованим Проєкт Закону №9623 про внесення змін до Кримінального кодексу України щодо забезпечення свободи від втручання в приватне життя. Пропонувалось змінити статтю 301 Кримінального кодексу, нова редакція якої передбачала б покарання лише за поширення порнографічних матеріалів без згоди людини, яка на них зображена («порнопомста»), або серед неповнолітніх осіб. Водночас, автори законопроєкту пропонували залишити кримінальну відповідальність за поширення чи виробництво дитячої порнографії та екстремальної порнографії (як от зоо- та некрофілії чи зображення насильницьких дій). Тоді прогресу щодо розгляду законопроєкту не відбулося.

11 листопада 2024 року народні депутати зареєстрували новий Проєкт Закону №12191 про внесення змін до Кримінального кодексу України щодо вдосконалення його окремих положень про кримінальні правопорушення проти громадського порядку та моральності, який є переглянутою та більш «компромісною» версією попередніх ініціатив. Новий законопроєкт пропонує залишити кримінальну відповідальність за розповсюдження творів, зображень або інших предметів порнографічного характеру, кіно- та відеопродукції, комп'ютерних програм порнографічного характеру малолітнім та неповнолітнім особам, а також за примушування дітей до створення порнографічних матеріалів. Комітет Верховної Ради України з питань правоохоронної діяльності на засіданні 23 грудня 2024 року, розглянув Проєкт закону № 12191 та рекомендував парламенту ухвалити проєкт за основу із встановленням продовженого строку на подання та розгляд правок та пропозицій.

Про необхідність декриміналізації порнографії для повнолітніх осіб свідчить і судова практика. Часто дії, за які винесені вироки за статтею 301 ККУ, очевидно не є суспільно небезпечними і лише обтяжують національну судову систему. Офіс ефективного регулювання BRDO у рамках проєкту "Порнобарометр" проаналізував, що за 9 місяців 2024 року до судів надійшло 1104 обвинувальних актів, що на 75% більше за аналогічний період 2023 року. При цьому, за два роки судовими вироками завершились лише 7% справ. Протягом 9 місяців 2024 року українські суди винесли 43 обвинувальних вироки, серед яких типовими прикладами порушень є справа №367/4183/24, у якій жінка отримала випробувальний термін та позбавлення права займатися діяльністю у сфері фото- та відеозйомки за продаж самостійно відзнятих відео в месенджері Telegram; справа №176/573/24, у якій чоловіка засудили за розміщення власних фотографій на сайті знайомств або справа №542/1052/23, в якій суд оштрафував особу майже на $1,000 за відправку двох еротичних відео своєму партнеру.

Закон України «Про рекламу» містить низку обмежень, спрямованих на захист моралі та охорону здоров'я. Зміни, що були внесені до закону, у зв'язку із необхідністю

імплементації окремих положень acquis ЄС у сфері аудіовізуальної реклами у 2023 році, розширили заборону вміщувати в рекламі твердження та/або зображення, які є дискримінаційними та/або розпалюють ненависть, ворожнечу чи жорстокість до окремих осіб чи груп осіб за ознаками, зокрема, віку, етнічної належності, сексуальної орієнтації, інвалідності, за іншими ознаками. Посилено та уточнено заборону реклами, спонсорства та продакт-плейсменту тютюнових виробів, пристроїв для споживання тютюнових виробів без їх згоряння, предметів, пов'язаних з їх вживанням, трав'яних виробів для куріння, електронних сигарет, заправних контейнерів, рідин, що використовуються в електронних сигаретах, тютюновмісних виробів для електричного нагрівання (ТВЕН) за допомогою підігрівача з електронним управлінням. Також прямо передбачається саморегулювання та співрегулювання у сфері реклами шляхом прийняття кодексів (правил) створення та розповсюдження реклами, зокрема щодо реклами алкогольних напоїв - з метою зменшення впливу на дітей такої реклами; реклами, яка включена у дитячі програми аудіальних чи аудіовізуальних медіа, а також розповсюджується на платформах спільного доступу до відео щодо харчових продуктів та напоїв, які містять жири, транс-жирні кислоти, сіль, соду або цукор, надмірне споживання яких у загальній дієті не рекомендується. Проєкт закону №12253, пропонує подальше приведення Закону України «Про рекламу» у відповідність з вимогами ЄС, зокрема в частині визначення дискримінаційної реклами, обмеження реклами, спонсорства та продакт-плейсменту алкогольних напоїв, обмеження реклами та телепродажу медичних виробів та ін.

Для приведення українського законодавства та його імплементації у відповідність з вимогами ЄС та Ради Європи, варто:

- Внести зміни до Кримінального кодексу України, виключивши загальну заборону на зберігання та розповсюдження порнографії, крім дій, що спрямовані на або залучають малолітніх та неповнолітніх дітей;
- Розробити та ухвалити зміни до законодавства щодо ефективних гарантій захисту особи від поширення її інтимних зображень без згоди («порнопомста»);
- Привести норми національного законодавства про рекламу у відповідність з вимогами Директиви ЄС про аудіовізуальні медіапослуги, зокрема в частині обмеження реклами, спонсорства та продакт-плейсменту товарів та послуг, шкідливих для здоров'я.

2.1.6. Обмеження свободи вираження поглядів, пов'язані з захистом дітей

Закон України «Про медіа» у статті 42 встановлює вимоги щодо поширення контенту, який може завдати шкоди фізичному, психічному або моральному розвитку дітей. До нього належать:

- надмірне зосередження уваги на насильстві, а саме поширення висловлювань або зображень насильства, які не є обґрунтованими або є надмірними в контексті відповідної програми чи публікації;
- позитивна оцінка нанесення, заподіяння самому собі каліцтва або вчинення самогубства, підбурювання до таких дій, надмірна і необґрунтована деталізація засобів і обставин самогубства;
- демонстрування жорстокого поводження з тваринами, методів умертвіння тварин, демонстрація великим планом такої, що вмирає, або жорстоко понівеченої тварини, крім випадків, якщо така демонстрація необхідна для популяризації гуманного ставлення до тварин, за умови попередження глядачів про сцени жорстокості;

- позитивна оцінка вандалізму;
- позитивна оцінка злочинного діяння або ідеалізація злочинця, надмірно деталізовані моделювання злочинних дій та/або демонстрація дій, відтворення яких дітьми може бути небезпечним для їхнього здоров'я і життя;
- позитивна оцінка залежності від наркотичних, токсичних, психотропних речовин, тютюну чи алкоголю, а також від інших речовин, які використовуються або можуть використовуватися з метою одурманення, заохочення їх вживання, виробництва, розповсюдження чи придбання, крім творів мистецтва;
- нецензурні висловлювання, слова, непристойні жести, крім випадків використання у творах мистецтва або відтворення у повідомленнях про новини дня або поточні події, що мають характер звичайної прес-інформації;
- заклики грати в азартні ігри, спонукання до участі в азартних іграх, крім випадків, передбачених законами України;
- демонстрація великим планом тіла померлої, такої, що вмирає, або жорстоко понівеченої людини, крім випадків, якщо така демонстрація необхідна для ідентифікації особи, за умови попередження глядачів про сцени жорстокості.

В Інтернеті показ такого контенту VOD-сервісами допускається лише за умови застосування системи умовного доступу, попередження про наявність цього контенту, а також маркування спеціальними позначеннями у каталозі. Онлайн-медіа можуть поширювати згадану вище інформацію також винятково за умови забезпечення належного попередження про потенційну шкідливість такої інформації для дітей.

Обмеження, встановлені цією нормою, є пропорційними і ненадмірними, і були визнані такими, що відповідають вимогам Директиви ЄС про аудіовізуальні медіапослуги. Крім того, законодавство передбачає, що критерії тлумачення цих обмежень будуть встановлюватися органами спільного регулювання, які у 2024 році лише були зареєстрованими, і більш активно працюватимуть над розробкою відповідних кодексів спільного регулювання вже у 2025 році. Притягнення суб'єктів, що діють в онлайні, до відповідальності за це порушення, що є значним, у 2024 році Національна рада здійснила у одній справі. Незареєстроване криворізьке онлайн-медіа «Свої» отримало припис за поширення фото неповнолітньої у матеріалі без належної на те потреби. Онлайн-медіа видалило відповідне фото після накладення медійним регулятором санкції.

Стаття 36 Закону «Про медіа» також забороняє поширювати на території України матеріали, що заохочують сексуальну експлуатацію та насильство над дітьми, демонструють статеві відносини дітей, використовують образ дітей (візуальний запис образу дітей) у видовищних заходах сексуального чи еротичного характеру. Таке порушення за законодавчою термінологією належить до грубих, а тому медіа, що його здійснить, може одразу отримати санкцію у виглядів штрафу. Втім, у 2024 році Національна рада не фіксувала таких порушень зі сторони медіа.

Окремо варто згадати про індустрійну нормотворчість - спільні акти узгодження, що розробляються представниками аудіовізуальних медіа при медійному регуляторі з 2016 року та прямо стосуються захисту прав дітей у медіа. У січні 2024 року було оголошено про погодження тексту шостого з таких актів, що мав би стосуватися висвітлення в медіа фактичних обставин досудового розслідування за участі дітей. Втім, після цього текст акту не було оприлюднено, що може свідчити над продовження роботи над ним або відкладення процесу його фіналізації до запуску органів спільного регулювання за законом «Про медіа». Ці органи матимуть зважати на спільні акти узгодження при створенні власних кодексів у 2025 році.

Кримінальний кодекс у статтях 301-1 та 301-2 встановлює відповідальність за дії, пов'язані з отриманням доступу до, ввезенням, виготовленням та розповсюдженням дитячої порнографії, зокрема за допомогою інформаційно-комунікаційних технологій, та з проведенням і переглядом видовищних заходів сексуального характеру за участі неповнолітніх. Ці норми були запроваджені у 2021 році для імплементації Ланцаротської конвенції про захист дітей від сексуальної експлуатації та сексуального насильства та відповідають її статтям 20-21, які передбачають криміналізацію відповідних видів діянь. У 2024 році не було винесено жодного вироку за статтею 301-2 Кримінального кодексу та 84 вироки за статтею 301-1 Кримінального кодексу.

Для гармонізації українського законодавства та його імплементації у цій сфері з вимогами ЄС, Ради Європи та рекомендаціями ООН, варто:

- Сприяти розробці кодексів спільного регулювання для медіа щодо визначення критеріїв віднесення інформації до такої, що може заподіяти шкоду фізичному, психічному або моральному розвитку дітей.

2.1.7. Обмеження свободи вираження поглядів, пов'язані з підтриманням авторитету і безсторонності суду

Стаття 34 Конституції України встановлює можливість обмеження права на свободу думки і слова, на вільне вираження своїх поглядів і переконань відповідно до закону для підтримання авторитету і неупередженості правосуддя. Частина 3 статті 6 Закону України «Про судоустрій та захист суддів» забороняє втручання у здійснення правосуддя, вплив на суд чи суддів у будь-який спосіб, неповагу до суду, а також збирання, зберігання, використання чи поширення інформації з метою дискредитації суду або впливу на його безсторонність. Зокрема, стаття 376 Кримінального кодексу України встановлює кримінальну відповідальність за втручання в будь-якій формі в діяльність судді з метою перешкодити виконанню ним службових обов'язків або добитися винесення неправосудного рішення. Відповідно до частини 4 статті 48 Закону України «Про судоустрій і статус суддів» - суддя зобов'язаний звернутися з повідомленням про втручання в його діяльність як судді щодо здійснення правосуддя до Вищої ради правосуддя та до Генерального прокурора.

У 2023 році публікація голови Центру протидії корупції Віталія Шабуніна, яка критикувала здатність окремих суддів Вищого антикорупційного суду виконувати свої обов'язки, стала підставою для звернення до Вищої ради правосуддя. ВРП розцінила допис як можливе втручання у правосуддя відповідно до статті 376 ККУ. Такий підхід до трактування критики може мати негативні наслідки для громадянського суспільства, журналістів та активістів, які здійснюють контроль за судовою системою, оскільки будь-яка критика суддів може трактуватися як втручання, що створює ризик кримінального переслідування.

За даними Реєстру повідомлень суддів про втручання в діяльність (Реєстр) за 2024 рік 73 повідомлення стосувалися критики суддів, підозри в корумпованості тощо, висловленої під час судових засідань, в публікаціях та розслідуваннях медіа, в публікаціях в соціальних мережах та в заявах сторін процесу до суду. Щодо 11 повідомлень наразі рішення ВРП відсутні. 11 повідомлень стосувалися розслідувань та публікацій медіа (в 10 випадках ВРП не встановила втручання в діяльність суддів). У 52 з 73 випадків повідомлень про втручання в діяльність суддів ВРП не встановила обставин існування ризиків втручання в діяльність суддів. Водночас переважно повідомлення, статті, дописи в соціальних мережах про корумпованість суддів, погрози суддям ставали підставою для надсилання відповідних звернень ВРП до прокуратури для перевірки обставин.

У 2024 році продовжились тенденції обмеження доступу до інформації про судову діяльність, що підважує принцип відкритості судових рішень, засідань та інформації про судові справи (частина 1 статті 11 Закону України «Про судоустрій та захист суддів»). Через повномасштабне вторгнення доступ до Єдиного державного реєстру судових рішень у 2022 році було обмежено для забезпечення безпеки суддів і учасників процесу, а також інформаційної безпеки. Попри часткове відновлення доступу після тиску громадянського суспільства, доступ до певних рішень залишається обмеженим і у 2024 році (приклад з матеріалу Фундації DEJURE). Крім того, 23 травня 2024 року за основу з доопрацюванням прийнято законопроєкт №7033-д, який непропорційно обмежує доступ до окремих категорій судових рішень, зокрема тих, що стосуються злочинів проти національної безпеки, інформація про які може становити суспільний інтерес.

З 2023 року доступ до інформації про суд продовжує суттєво обмежуватися, що відображає регрес прозорості судової системи. Зокрема, рішення Верховного Суду та дії органів суддівського самоврядування, таких як ВККС і ВРП, часто необгрунтовано обмежували публічний доступ до важливої інформації, пов'язаної із діяльністю суддів, аргументуючи це захистом конфіденційності або національної безпеки. Така закритість підриває довіру до судової системи та потребує змін для забезпечення балансу між конфіденційністю та громадським контролем.

Для гармонізації українського законодавства з вимогами Ради Європи, ЄС та рекомендаційними документами ООН, варто:

- забезпечити прозорість роботи судової системи шляхом розширення доступу до Єдиного державного реєстру судових рішень із відповідними заходами безпеки із врахуванням суспільного інтересу та чітким контролем правових підстав обмежень доступу до судових рішень;
- гармонізувати обмеження доступу до інформації та визначити чіткі обґрунтування та критерії, що забезпечують баланс між безпекою, конфіденційністю та правом на інформацію.

2.2. Свобода медіа

2.2.1. Свобода діяльності медіа, плюралізм та редакційна незалежність

Закон України «Про медіа» визначає своєю метою забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, забезпечення плюралізму думок і вільного поширення інформації, захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа. Закон, у відповідності до Конституції України та Директиви ЄС про аудіовізуальні медіапослуги, забороняє цензуру та незаконне втручання у діяльність суб'єктів у сфері медіа з боку державних органів, органів місцевого самоврядування, громадських об'єднань, політичних партій, власників відповідних суб'єктів, будь-яких інших фізичних та юридичних осіб.

Водночас, Директива - не єдиний акт ЄС, що вимагає плюралізму медіа та гарантій свободи їх діяльності, а просте закріплення принципів у законі не означає їх справжнього виконання на практиці. Європейський акт про свободу медіа (EMFA) — регламент, ухвалений ЄС у квітні 2024 року, спрямований на захист плюралізму та незалежності медіа в ЄС в умовах цифрової трансформації медіапростору. Документ є актом

прямої дії для Держав-членів ЄС, але водночас вимагає від них запровадити низку законодавчих гарантій у внутрішньому законодавстві для того, аби надати нормам EMFA змісту через конкретні механізми. У 2024 році він був включений до переліку актів ЄС для скринінгу на предмет відповідності національного законодавства України праву ЄС, тож його впровадження є важливим кроком на шляху до євроінтеграції, особливо з огляду на підвищену увагу ЄС до медіа реформи.

Загальні принципи щодо доступу користувачів до різноманітного редакційно незалежного медіа контенту, забезпечення редакційної та функціональної незалежності суспільного мовлення, належне обґрунтування та пропорційність заходів, що застосовуються до медіа державними регуляторами, прозорість медіа власності, вже передбачені чинним Законом «Про медіа». Ці норми, однак, не можуть повноцінно захистити від заходів тиску чи цензури, які безпосередньо не пов'язані із реалізацією повноважень регуляторним органом. Так, наприклад, у жовтні 2024 року «Українська правда» заявила про тривалий та системний тиск, який Офіс президента здійснює на редакцію та окремих журналістів онлайн-медіа, зокрема, шляхом блокування спікерів від влади щодо спілкування з журналістами «Української правди» та участі в заходах, а також тиску на бізнес з метою зупинити рекламну співпрацю з виданням. Такі ситуації потребують висвітлення та загального перегляду системи відповідальності за перешкоджання журналістській діяльності (див. Розділ 2.2.3.)

Європейський акт про свободу медіа передбачає доповнення національного законодавства вимогами щодо проведення оцінки впливу концентрації на медійному ринку на медійний плюралізм та редакційну незалежність, окремо від оцінки відповідно до Закону України «Про захист економічної конкуренції». Така оцінка має враховувати вплив на вибір медіапослуг на ринку, запобіжники для редакційної незалежності, економічну стійкість медіа без концентрації, а також взяті на себе зобов`язання сторін концентрації щодо забезпечення медійного плюралізму та редакційної незалежності. Активну роль в проведенні такої оцінки має здійснювати медійний регулятор, тож повноваження Національної ради мають бути розширені з одночасним посиленням експертизи для проведення такого аналізу.

Багато уваги у EMFA приділено і питанню прозорості та недискримінаційних підходів до державного фінансування медіа: державні кошти або будь-які переваги, надані, прямо чи опосередковано, державними органами чи їх юридичними особами медіа або онлайн-платформам для державної реклами чи контракти на надання послуг повинні виконуватися прозоро, об'єктивно, пропорційно і недискримінаційно, заздалегідь оприлюднюватися за допомогою електронних і зручних засобів. Конкурси на фінансування мають бути відкритими. При цьому, суб'єкти у сфері медіа, які отримують державну підтримку зобов'язані оприлюднювати про це інформацію. До Закону України "Про медіа" також потрібно буде додати загальний обов'язок для медіа, що надають новинний контент та матеріали про поточні події, щодо гарантування внутрішньої редакційної свободи та розкриття будь-яких можливих конфліктів інтересів, що можуть вплинути на висвітлення ними новин.

Впровадження цих норм, серед іншого, вимагатиме перегляду існуючих зараз підходів фінансування з державного бюджету та усунути можливі зловживання.

Для гармонізації українського законодавства та його імплементації з вимогами ЄС та Ради Європи, необхідно:

- Підготувати комплексний план щодо імплементації вимог Європейського акту про свободу медіа в національне законодавство, із залученням представників медіа, громадськості, експертів ЄС та Ради Європи;

- Посилити фінансову та експертну спроможність Національної Ради України з питань телебачення і радіомовлення впроваджувати запропоновані зміни, особливо щодо оцінки впливу концентрації медіа на плюралізм та редакційну незалежність.

2.2.2. Захист журналістських джерел та конфіденційність комунікацій

Стаття 25 Закону України «Про інформацію» передбачає право журналіста не розкривати джерело інформації або інформацію, яка дозволяє встановити джерела інформації, крім випадків, коли його зобов'язано до цього рішенням суду на основі закону. Кримінальний процесуальний кодекс України у статті 65 встановлює, що не можуть бути допитані як свідки журналісти — про відомості, які містять конфіденційну інформацію професійного характеру, надану за умови нерозголошення авторства або джерела інформації. А інформація, що знаходиться у володінні засобу масової інформації або журналіста і надана їм за умови нерозголошення авторства або джерела інформації належить до охоронюваної законом таємниці (стаття 162), доступ до якої має надаватися лише за умови неможливості іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів.

На перший погляд може здатися, що національне законодавство гарантує захист журналістських джерел та конфіденційність їх комунікацій, але чинні норми насправді не відповідають мінімальному стандарту, який встановлює Європейський акт про свободу медіа ЄС. Ба більше, навіть ці гарантії на практиці не виконуються.

У 2021 році Європейський суд з прав людини виніс рішення у справі журналістки Наталки Седлецької щодо порушення Україною статті 10 Конвенції про захист прав людини та основоположних свобод. Заявниця скаржилася на те, що ухвали суду, якими Генеральній прокуратурі України було надано дозвіл на доступ до інформації щодо вхідних і вихідних з'єднань з її мобільного телефону, становили невиправдане втручання у її право на захист журналістських джерел інформації. ЄСПЛ звернув увагу на низку порушень, що призвели до неправомірного втручання у право журналістки: необґрунтований розгляд клопотання про дозвіл отримати доступ до інформації без її участі та повідомлення про застосування таких заходів, наведені національними судовими органами підстави для збору великої кількості захищеної інформації щодо вхідних і вихідних з'єднань стосовно особистих та професійних контактів заявниці за шістнадцятимісячний період не були достатніми, обмеження можливостей заявниці оскаржити ухвалу та ін.

Водночас, якщо спеціальні гарантії щодо захисту журналістських джерел принаймні передбачені законом щодо застосування заходів тимчасового доступу до речей та документів, такі гарантії відсутні щодо заходів тимчасового вилучення майна, арешту майна, обшуку, проведення негласних слідчих (розшукових) дій. При санкціонуванні таких дій не передбачено балансування інтересів розслідування із захистом журналістських джерел чи їх конфіденційних комунікацій.

Ухвалений у квітні 2024 року в ЄС Європейський акт про свободу медіа має на меті уніфікувати підходи до захисту журналістських джерел та комунікацій у ЄС, встановивши мінімальні гарантії. Для України приведення національного законодавства у відповідність із цим актом є одним із завдань в рамках переговорів про вступ до ЄС. Серед ключових змін, які необхідно впровадити - поширення гарантій захисту не лише на журналістів, але і на інших працівників медіа, осіб, які через свої регулярні або професійні відносини з провайдером медіапослуг або його редакцією можуть володіти такою інформацією, розкривати її.

Національне законодавство передбачає, що доступ до конфіденційних комунікацій в рамках кримінального провадження може відбуватись лише з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, що відповідає підходу ЄС. Водночас, розслідування, яке дає підстави отримувати доступ до конфіденційних комунікацій (у т.ч. через використання шпигунського програмного забезпечення), має також здійснюватися безпосередньо щодо особи, на яку поширюються гарантії захисту цієї статті, а не в рамках будь-якого кримінального провадження.

Чинне національне законодавство встановлює вимоги щодо повідомлення особи про застосування до неї заходів, які мали наслідком отримання доступу до її конфіденційних персональних даних, в рамках кримінального розслідування. Особа також може звернутися про отримання такої інформації на підставі законодавства у сфері захисту персональних даних. Водночас, виконання цих гарантій на практиці потребує посилення, зокрема в частині належного контролю від зловживань. Повноваження з такого контролю можуть, зокрема, здійснюватися незалежним регуляторним органом у сфері захисту персональних даних (див. Розділ 3.4.1.)

Українське законодавство на сьогодні також не регулює використання технологій стеження, у тому числі шпигунського програмного забезпечення, що не виключає їх застосування на практиці. Загальні гарантії щодо захисту журналістських джерел та конфіденційних комунікацій в цілому поширюються і на випадки стеження за допомогою спеціального програмного забезпечення. Проте з огляду на інвазивність таких технологій, складність їх виявлення та контролю, законодавство має містити належні спеціальні гарантії законності їх використання, зокрема виняткові підстави та прозорі механізми застосування і контролю. Таким чином, національне законодавство, зокрема в частині повноважень органів безпеки, правоохоронних органів та інших державних органів має бути доповнене відповідними гарантіями від свавільного застосування таких інтрузивних засобів стеження.

У 2024 році не було напрацьовано змін до законодавства щодо посилення захисту журналістських джерел. Навпаки, наприкінці 2023 року у парламенті був зареєстрований Проєкту закону №10242 про внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що обробляється в публічних електронних реєстрах, та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем. Медійні та правозахисні організації закликали Верховну Раду не підтримувати законопроєкт, оскільки він несе суттєві загрози для свободи слова, роботи журналістів, захисту журналістських джерел та викривачів корупції в Україні. Під прикриттям боротьби із «зловживанням даними» створюється інструмент, який може бути використаний для переслідування журналістів, що висвітлюють корупційні схеми або зловживання владою. Посилення відповідальності також відкриває можливість для застосування негласних слідчих дій проти журналістів, зокрема прослуховування та стеження, що суттєво порушує стандарти захисту джерел інформації.

Для гармонізації українського законодавства та його імплементації з вимогами ЄС та Ради Європи, необхідно:

- Розширити коло осіб, яким надається захист щодо нерозголошення інформації про журналістські джерела чи конфіденційність комунікацій — інші працівники медіа, інші особи, які через свої регулярні або професійні відносини з провайдером медіапослуг або його редакцією можуть володіти такою інформацією, розкривати її.

- Внести зміни до національного законодавства щодо гарантування ефективного судового нагляду в усіх випадках отримання доступу до інформації про журналістські джерела чи конфіденційних комунікацій, а також впровадження інших стандартів, передбачених Європейським актом про свободу медіа.
- Врегулювати використання спеціального шпигунського програмного забезпечення відповідно до вимог та умов ЄС (лише за умови недостатності альтернативних заходів, лише при розслідуванні тяжких або особливо злочинів, вчинених відповідною особою з обов'язковим судовим наглядом, регулярним переглядом та подальшим інформуванням про застосовані обмеження) чи встановити заборону на використання таких засобів.

2.2.3. Захист від перешкоджання журналістській діяльності у цифровому середовищі

Українські медіа та журналісти часто стають жертвами кібератак та погроз онлайн. Розслідування таких випадків переважно затягнуті та неефективні, що створює атмосферу безкарності та сприяє вчиненню нових порушень. За 2024 рік IMI зафіксували 58 випадків кібератак проти журналістів та медіа. ГО "Жінки в медіа" у 2024 році оприлюднили 29 верифікованих випадків онлайн-атак на журналісток, серед яких доксинг, мова ворожнечі, дифамація та навіть погрози зґвалтуванням, смертю та фізичним насильством.

За даними Інституту масової інформації, у 2024 році росіяни продовжили залякувати журналістів та бути найчастішим джерелом погроз (45 випадків) та кібератак (35 з 58 зафіксованих випадків). Зокрема, IMI зафіксував три хвилі (у жовтні, листопаді та грудні) анонімних погроз про мінування низки редакцій та установ у різних областях України: ідентичні електронні листи отримала низка медіа та журналістів. Російські хакери протягом 2024 року ламали ефіри українських телеканалів та запускали свою пропаганду на них, атакували сайти як національних, так і регіональних медіа, які висвітлюють воєнні злочини РФ.

Водночас, джерелом погроз та інших спроб тиску на незалежні медіа була не лише держава-агресор: IMI зафіксували 21 випадок перешкоджання та 19 випадків непрямого тиску на журналістів з боку України.

Онлайн-видання «Українська правда» повідомляла про погрози на адресу журналіста-розслідувача Михайла Ткача у травні 2024 року, ще один випадок, пов'язаний з іншим розслідуванням трапився у жовтні, однак теж залишився без належної реакції з боку правоохоронних органів. Комісія з журналістської етики закликала органи влади піддавати належному розгляду повідомлення будь-яких журналістів, медіа й професійних організацій, які привертають увагу до таких інцидентів та вживати всіх відповідних подальших заходів реагування.

Представники українського громадянського суспільства також виступили із заявою проти переслідування органами правопорядку антикорупційних активістів та журналістів-розслідувачів в Україні. Так, у квітні 2024 року редакція «Слідство. Інфо» повідомила про те, що працівник Служби безпеки України міг давати вказівки представникам військкомату щодо вручення повістки журналісту «Слідства. Інфо», який проводив розслідування щодо елітного майна керівника департаменту кібербезпеки СБУ. Агенція подала до правоохоронних органів заяву про переслідування та перешкоджання журналістській діяльності. Державне бюро розслідувань відкрило кримінальне провадження, проте досудове розслідування затягується, що створює сумніви в його ефективності.

У 2024 році суди винесли 10 обвинувальних вироків за злочини проти журналістів. Усі з них стосуються випадків фізичного перешкоджання, знищення майна, погроз, висловлених безпосередньо під час здійснення журналістської діяльності.

Для належного захисту журналістів від перешкоджання їх діяльності у цифровому середовищі необхідно:

- Посилити міжвідомчу координацію щодо розслідування злочинів проти журналістів, у тому числі, тих, що здійснюються у цифровому середовищі;
- Посилити ефективність контролю щодо ефективного розслідування випадків перешкоджання журналістам та співпраці органів розслідування з правозахисними та медійними організаціями.

2.2.4. Незалежний та ефективний регуляторний орган у сфері медіа

Національна рада України з питань телебачення і радіомовлення (Національна рада) - є незалежним постійно діючим колегіальним державним органом, що здійснює державне регулювання, нагляд та контроль у сфері медіа на підставі Конституції України, Закону «Про медіа» та інших законів України. Статус, повноваження, процедура призначення членів регуляторного органу в цілому відповідають вимогам ЄС - Директиві про аудіовізуальні медіа послуги та Європейському акту про свободу медіа. Експерти Ради Європи оцінюючи новели Закону України «Про медіа» також відзначили позитивні зміни, зокрема посилення гарантій незалежності через вдосконалення процедури відбору кандидатів на посади членів Національної ради, створення механізмів спільного регулювання, закріплення вимог щодо обґрунтованості та об'єктивності рішень. У аналітичному висновку також наголошують на важливості проведення незалежного і прозорого конкурсу та залучення громадськості до номінування кандидатів та нагляду за процесом проведення такого конкурсу. Наразі це передбачено статтями 76 та 77 Закону України "Про медіа".

Водночас, для реального забезпечення незалежності та ефективності регулятора важливою є реалізація законодавчих гарантій на практиці. З моменту набрання чинності медійним законом у 2023 році, Національна рада не отримала фінансування у встановлених законом обсягах. Закон «Про Державний бюджет України на 2024 рік» також зупинив норми статті 78 Закону України "Про медіа" щодо гарантування розмірів заробітних плат членів медійного регулятора та посадових осіб апарату регулятора. Аналогічні обмеження були застосовані і бюджетом на 2025 рік. З огляду на суттєве розширення компетенції Національної ради, відсутність належних ресурсів є суттєвою загрозою для імплементації медійної реформи. У своєму звіті про політику розширення ЄС щодо України у 2024 році, Європейська Комісія наголосила на необхідності гарантування достатнього фінансування та людських ресурсів для виконання Національною комісією своїх функцій.

Іншим аспектом, що може підважити незалежність регулятора та його здатність ефективно виконувати повноваження, є повернення обов'язкової процедури державної реєстрації регуляторних актів Національної ради в Міністерстві юстиції України. Чинні норми Закону України «Про медіа» передбачають, що такі акти не підлягають державній реєстрації, адже Національна рада є окремим конституційним органом і не входить в систему органів виконавчої влади, що підпорядковуються чи підзвітні Кабінету Міністрів України. Втім, ухвалений у серпні 2023 року Закон України «Про правотворчу діяльність», що набуде чинності через рік після закінчення правового режиму воєнного стану, повертає процедуру так званого юстування. Вирішити цю проблему пропонують в рамках Проєкту Закону №12111 про внесення змін до деяких законів України щодо

діяльності медіа. Цей законопроєкт, ухвалений в першому читанні у грудні 2024 року, виключає обов'язок юстування актів Національної ради.

Відкритим залишається питання щодо необхідності внесення змін до Конституції України для вдосконалення процедури формування складу Національної ради. Конституція України розділяє між парламентом та Президентом України призначення однакової кількості (половини) членів регуляторного органу. На практиці затягування одним із суб'єктів призначення рішень щодо кандидатів може призводити до блокування роботи всього регулятора. Крім цього, повна назва Національної ради не повністю відображає усю сферу, що належить до її контролю - тепер це не лише телебачення та радіо, але і інші форми медіа та онлайн-платформ.

Для гармонізації українського законодавства та практики його імплементації з вимогами ЄС та Ради Європи, необхідно:

- Забезпечити належне фінансування Національної ради України з питань телебачення і радіомовлення у повній відповідності з вимогами Закону України «Про медіа»;
- Скасувати застосування процедури юстування до нормативно-правових актів, що приймаються Національною радою як незалежним регуляторним органом у сфері медіа;
- Після завершення правового режиму воєнного стану, розглянути необхідність змін до Конституції України щодо посилення незалежності Національної ради та приведення її статусу та гарантій діяльності у відповідність з вимогами права ЄС.

2.3. Свобода вираження поглядів та онлайн-платформи

2.3.1. Зобов'язання держави щодо захисту прав користувачів онлайн-платформ

На сьогодні українське законодавство містить обмежені норми щодо регулювання онлайн-платформ та захисту користувачів від їх можливих зловживань. Навіть наявні норми переважно не мають практичного застосування в Україні, з огляду на відсутність юрисдикції щодо найпопулярніших компаній.

На діяльність онлайн-платформ під українською юрисдикцією поширюються вимоги Закону України «Про електронну комерцію» та Закону України «Про захист прав споживачів», але їх чинні редакції містять лише загальні положення про захист прав державою та не містять зобов'язань для будь-якого типу платформ. Лише нова редакція Закону України «Про захист прав споживачів», що була прийнята у 2023 році та набуде чинності після закінчення воєнного стану, запровадить певні гарантії для користувачів маркетплейсів, зокрема, щодо доступу до інформації.

Така специфічна категорія платформ як платформи спільного доступу до відео має додаткове регулювання в рамках Закону України «Про медіа» відповідно до вимог статті 28b оновленої Директиви ЄС про аудіовізуальні медіапослуги. Стаття 23 Закону «Про медіа» передбачає такі обов'язки провайдерів платформ спільного доступу до відео:

- розмістити умови користування сервісом та ознайомити з ними користувачів;
- передбачити в умовах користування сервісом заборону на поширення програм, рекламної та користувацької інформації, що містять протиправний контент, а також порушують вимоги законодавства про авторське право та суміжні права;

- забезпечити перевірку віку користувача перед отриманням ним доступу до інформації, що може завдати шкоди фізичному, психічному або моральному розвитку дітей, забезпечити можливість використання системи батьківського контролю з метою захисту дітей від такої інформації;
- впровадити прозорі та зрозумілі механізми оцінки та направлення провайдерам звернень користувачів щодо інформації, розміщеної на такій платформі, що може порушувати вимоги законодавства та умови користування, механізми ефективного розгляду звернень та повідомлення користувачам про результати такого розгляду, а також забезпечити прозорий, простий та ефективний механізм оскарження дій провайдера щодо розгляду звернень користувачів;
- передбачити в умовах користування сервісом порядок реалізації права на відповідь або спростування недостовірної інформації та забезпечити інформування користувачів про факт і зміст спростування або відповіді в описовій інформації до відповідного користувацького відео, а також шляхом повідомлення користувачів перед отриманням доступу до відповідної програми;
- включати та впроваджувати в умовах користування сервісом вимоги щодо поширення рекламної інформації, встановлені законодавством, а також забезпечувати користувачам можливість зазначати, чи містить їхнє користувацьке відео рекламну інформацію;
- впроваджувати ефективні заходи та інструменти медіаграмотності, підвищувати обізнаність користувачів щодо таких заходів.

Директива, як і норми Закону «Про медіа», заохочує вдаватися до спільного регулювання щодо напрацювання механізмів втілення цих обов'язків у життя. Також Закон відтворює положення Директиви щодо надання користувачам платформ доступу до суду для захисту своїх прав. Станом на кінець 2024 року, Національна рада України з питань телебачення і радіомовлення не зареєструвала жодного провайдера платформ спільного доступу до відео в Україні.

Стосовно регулювання платформ, які перебувають під юрисдикцією іноземних держав, то чинне законодавство визнає неможливість прямо впливати на їх діяльність та пропонує підхід співпраці щодо захисту прав користувачів. Вже згаданий Закон «Про медіа» ввів категорію «платформа спільного доступу до інформації», яка має покривати такі платформи як Facebook, Instagram, X (Twitter) та інші. Національна рада наділена правом укладати з такими платформами договори або меморандуми. Предмет таких меморандумів чітко визначається лише у контексті законодавства про всеукраїнський референдум і включає вимоги та обмеження щодо інформації, що поширюється на платформах та доступна на території України, механізми співрегулювання, співпраця у сфері протидії поширенню дезінформації під час підготовки та проведення референдуму, забезпечення прозорості агітації на платформах та впровадження відкритих бібліотек агітації. Станом на кінець 2024 року, жодного такого меморандуму з платформами не укладено.

На фоні цього та росту впливу такої платформи як Telegram як основного джерела отримання інформації для більшості громадян України, у 2024 році посилилися голоси щодо запровадження більш суворої рамки регулювання для онлайн-платформ. Основна регуляторна робота відбувається під егідою Міністерства цифрової трансформації, що відповідає за запровадження в Україні Акту ЄС про цифрові послуги (Digital Services Act або ж DSA). У серпні 2024 року стало відомо, що проєкт законодавчих змін для імплементації основних положень DSA, готовий та очікує на оцінку зі сторони Європейської комісії на предмет відповідності тексту Акту. Ним запроваджуватимуться

вимоги щодо побудови державами та платформами інфраструктури для захисту прав користувачів, зокрема запровадження механізмів notice-and-action, створення позасудових органів з вирішення спорів щодо протиправного контенту, підвищення прозорості рекомендаційних систем тощо.

У березні 2024 року народні депутати зареєстрували Проект Закону № 11115 про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація. Він пропонує запровадити аналогічні до згаданих вище щодо платформ спільного доступу до відео обов'язки на ширшу категорію суб'єктів, які законопроектом визначаються як «платформи спільного доступу до інформації, через які поширюється масова інформація». Такий підхід частково забезпечує відповідність DSA, адже в загальних рисах враховує вимоги щодо notice-and-action та відповідності умов користування сервісами стандартам у сфері захисту прав людини. Він також частково бере до уваги положення Акту щодо номінування локальних юридичних представників у разі, якщо платформа не перебуває під юрисдикцією України чи держави-члена Європейського Союзу. Втім, прийняття цих норм не дозволить говорити про впровадження DSA та потребуватиме подальшого доопрацювання.

Для гармонізації українського законодавства та його імплементації у цій сфері з вимогами ЄС, Ради Європи та рекомендаціями ООН, варто:

- Доопрацювати законопроєкт, що запроваджуватиме норми Акту ЄС про цифрові послуги в Україні у відповідності з висновками Європейської комісії та із залученням громадськості;
- Напрацювати підхід щодо встановлення юрисдикції над іноземними онлайн-платформами, який не запроваджуватиме надмірних обмежень для їх діяльності в Україні та водночас краще забезпечуватиме права українських користувачів і відповідатиме Актові ЄС про цифрові послуги;
- Відправити на доопрацювання Проект Закону № 11115 про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація та забезпечити подальшу координацію будь-яких ініціатив, пов'язаних з регулюванням онлайн-платформ, з діяльністю Міністерства з питань цифрової трансформації, з метою забезпечення їх відповідності стандартам ЄС у сфері цифрового врядування.

2.3.2. Статус та вимоги до онлайн-платформ щодо дотримання принципів свободи вираження поглядів

Закон України «Про електронну комерцію» врегульовує статус інтернет-посередників та їх імунітет від відповідальності. У частині четвертій статті 9 Закону, фактично, відтворюється норма Директиви ЄС про електронну комерцію щодо імунітету провайдерів послуг хостингу, яка надалі перенесена до Акту ЄС про цифрові послуги. Вони не нестимуть відповідальності за поширення інформації третіми особами у разі, якщо у них відсутні відомості про незаконну діяльність або факти чи обставини, які вказують на те, що діяльність має ознаки незаконної, а після отримання таких відомостей вдаються до швидких дій з метою усунення можливості доступу чи припинення доступу до інформації. Це положення може застосуватися до платформ, що перебувають під українською юрисдикцією, та відповідає вимогам DSA. Втім, лише Закон України «Про авторське право і суміжні права» у статтях 56-58 деталізує порядок втілення її норм в життя щодо такого суб'єкта як провайдери послуг обміну контентом. Цей підхід відповідає DSA та Директиві ЄС про авторське право на єдиному цифровому

ринку. Водночас, законодавство України не закріплює заборону держави покладати на платформи загальний обов'язок з моніторингу протиправної активності у власних мережах.

У випадках, коли онлайн-медіа діють як посередники - наприклад, коли вони надають можливість коментувати матеріали або ж мають частину сайту, що наповнюється сторонніми користувачами (колонки чи блоги), - вони також можуть скористатися імунітетом, передбаченим Законом «Про медіа». Частина п'ята статті 117 Закону звільняє онлайн-медіа від відповідальності за інформацію, що була поширена користувачами у розділах для коментування чи розміщення користувацьких публікацій на веб-сайті чи веб-сторінці такого медіа та доступ до якої був обмежений медіа протягом 3 робочих днів з моменту отримання скарги від споживачів чи припису Національної ради.

Закон «Про медіа» окремо передбачив і можливість Національної ради звертатися до провайдерів платформ спільного доступу до інформації та провайдерів пошукових систем щодо обмеження поширення на території України програм або користувацької інформації, що порушує контентні обмеження. Такі повноваження можуть надавати належну правову підставу положенням про накази щодо вчинення дій протиправного контенту, які згадані у статті 9 DSA та адресуються онлайн-платформам. Втім, невиконання цих обов'язків не нестиме практичних наслідків для платформ з огляду на описані вище юрисдикційні перепони.

Згаданий у попередньому підрозділі Проект Закону № 11115 про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація, пропонував додати до обов'язків таких платформ видалення протиправного контенту за рішенням Національної ради. Цей обов'язок має забезпечуватися відповідальністю платформ - у розмірі від 5 до 25 мінімальних заробітних плат на день здійснення порушення (на кінець 2024 року - від 40,000 до 200,000 гривень) - в разі невидалення одиниці контенту. Втім, такий підхід не відповідає DSA, що хоч і передбачає великі розміри штрафів за порушення його вимог, але концентрується на регулюванні процесів та процедур, які має започаткувати та підтримувати в належному стані платформа. Притягнення до значної відповідальності за невидалення одного допису чи однієї одиниці контенту буде непропорційним втручанням.

Для гармонізації українського законодавства та його імплементації у цій сфері з вимогами ЄС, Ради Європи та рекомендаціями ООН, варто:

- Доопрацювати законопроєкт, що запроваджуватиме норми Акту ЄС про цифрові послуги в Україні у відповідності з висновками Європейської комісії та із залученням громадськості
- Відправити на доопрацювання Проект Закону № 11115 про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація та забезпечити подальшу координацію будь-яких ініціатив, пов'язаних з регулюванням онлайн-платформ, з діяльністю Міністерства з питань цифрової трансформації, з метою забезпечення їх відповідності стандартам ЄС у сфері цифрового врядування;

2.3.3. Незалежний та ефективний регуляторний орган у сфері онлайн-платформ

У своєму звіті щодо України у рамках політики розширення у 2024 році, Єврокомісія звернула окрему увагу на важливість розбудови «незалежної регуляторної спроможності» у сфері цифрових послуг та створення дорожньої карти з детальними

кроками щодо приведення регулювання у відповідність з Актом ЄС про цифрові послуги. Ці кроки, серед іншого, мають включати визначення компетентних органів, що відповідатимуть за впровадження регулювання для онлайн-платформ. Акт ЄС про цифрові послуги передбачає можливість призначення декількох компетентних органів влади для розподілу обов'язків щодо впровадження акту. Зокрема, ними можуть бути регулятори у сферах захисту персональних даних, захисту споживачів, електронних комунікацій чи медіа. Втім, кожна країна ЄС, навіть у разі надання кільком органам повноважень щодо впровадження акту, зобов'язана призначити один орган державної влади, який буде відповідальний за нагляд та координацію - Координатора цифрових послуг.

Вибір компетентних органів та Координатора буде наріжним для побудови ефективної системи регулювання діяльності онлайн-платформ в Україні. Міністерство з питань цифрової трансформації поки що не представило публічно своє бачення щодо такої інституційної системи. Серед можливих варіантів – як створення окремої інституції, так і наділення додатковими повноваженнями існуючі державні органи, що відповідають вимогам Акту ЄС про цифрові послуги, зокрема, є незалежними.

Так, Національна рада України з питань телебачення і радіомовлення вже має окремі повноваження щодо платформ спільного доступу до відео відповідно до Закону «Про медіа». У відповідності з Директивою ЄС про аудіовізуальні медіапослуги, Національна рада може притягувати до відповідальності платформи за, наприклад, незастосування системи верифікації віку користувачів щодо контенту, який може завдавати шкоди дітям, або ж відсутність механізмів направлення користувачами скарг на поширення протиправного контенту.

Інший кандидат – Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (НКЕК) – має досвід у сфері регулювання однієї з категорій Інтернет-посередників, а саме постачальників електронних комунікаційних послуг, які кваліфікуються за Актом ЄС про цифрові послуги як mere conduit. Чинний Закон України «Про електронні комунікації» не передбачає вимог, що встановлюються до таких суб'єктів за Актом ЄС про цифрові послуги. Попри це, НКЕК має досвід роботи з великою кількістю суб'єктів, на які поширюватимуться положення нового законодавства у сфері цифрових послуг. Водночас, НКЕК, як і Національна рада, наразі не має достатніх фінансових та людських ресурсів для виконання додаткових повноважень, з огляду на призупинення гарантій фінансування.

Варто зауважити, що створення нового регуляторного органу необхідне і у сфері захисту персональних даних відповідно до Загального регламенту про захист даних ЄС, а також у майбутньому у сфері штучного інтелекту при імплементації Акту ЄС про штучний інтелект. Це свідчить про необхідність комплексного підходу до формування нової інституційної системи регуляторних органів у сферах медіа, технологій та прав людини.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто:

- Розробити єдиний та узгоджений підхід до створення/призначення нових регуляторних органів у сферах цифрових послуг, захисту персональних даних та штучного інтелекту, узгодження їх статусу та повноважень, порядку співпраці з іншими компетентними органами;
- Гарантувати законом і на практиці належне фінансове забезпечення та ресурси для ефективного виконання компетентними органами їх повноважень відповідно до Акту ЄС про цифрові послуги;

- Після припинення правового режиму воєнного стану, розглянути зміни до Конституції України щодо посилення незалежності Національної ради з питань телебачення та радіомовлення та загального унормування діяльності незалежних регуляторних органів.

2.4. Свобода вираження поглядів в умовах воєнного стану

2.4.1. Обмеження свободи вираження поглядів під час воєнного стану

Україна 4 квітня 2024 року оновила свою декларацію про відступ від зобов'язань за Міжнародним пактом про громадянські та політичні права і Європейською конвенцією про права людини. У ній і надалі містяться положення про можливість України додатково обмежувати права, гарантовані статтями 19 та 10 відповідних міжнародних договорів, що гарантують право на свободу вираження поглядів. Текст декларації є достатньо загальним і не вказує на конкретні заходи, що можуть бути запроваджені для обмеження свободи слова на період воєнного стану.

Закон України «Про правовий режим воєнного стану» дозволяє регулювати в порядку, встановленому Кабінетом Міністрів, діяльність медіа зі сторони військового командування та військових адміністрацій. Втім, такого нормативного порядку урядом не прийнято. У 2022 році було прийнято Наказ Головнокомандувача ЗСУ № 73 «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками медіа на час дії правового режиму воєнного стану», останні зміни до якого були запроваджені у лютому 2024 року. Ці зміни, за оцінками фахівців, лібералізували доступ до безпосередніх зон конфлікту (так званої «червоної зони») та уможливили діяльність без нагляду зі сторони прес-офіцерів у «жовтій зоні», а також дозволили отримувати акредитацію окремим блогерам, що є позитивним зрушенням для роботи онлайн-медіа.

Закон України «Про медіа» містить Розділ IX, пов'язаний з обмеженнями, спрямованими на зменшення впливу держави-агресора в інформаційному просторі України. Вони запроваджуються на час агресії та застосовуватимуться протягом перехідного періоду строком у 5 років (зі щорічним переглядом) з моменту скасування Верховною Радою статусу держави-агресора. Стаття 119 Закону забороняє поширювати чотири типи протиправного контенту під час збройної агресії:

- інформацію, що висвітлює збройну агресію проти України як внутрішній конфлікт, громадянський конфлікт чи громадянську війну, якщо наслідком цього є розпалювання ворожнечі чи ненависті або заклики до насильницької зміни, повалення конституційного ладу чи порушення територіальної цілісності;
- недостовірні матеріали щодо збройної агресії та діянь держави-агресора, її посадових осіб, осіб та організацій, що контролюються державою-агресором, у разі, якщо наслідком цього є розпалювання ворожнечі чи ненависті або заклики до насильницької зміни, повалення конституційного ладу чи порушення територіальної цілісності;
- програми та матеріали (крім інформаційних та інформаційно-аналітичних програм), одним з учасників яких є особа, внесена до Переліку осіб, які створюють загрозу національній безпеці;
- музичні фонограми, відеограми, музичні кліпи, здійснені співаком (співачкою), який є або був у будь-який період після 1991 року громадянином держави-агресора, та/або вироблені фізичною особою та/або юридичною особою, яка була громадянином держави-агресора або зареєстрована в державі-агресорі.

Також висвітлення діяльності органів влади держави-агресора в інформаційних та інформаційно-аналітичних програмах або матеріалах має супроводжуватися повідомленням про статус держави-агресора. Перші дві категорії контенту, згадані вище, є грубими порушеннями для онлайн-медіа, і можуть призводити до відповідних санкцій. Решта згаданих порушень є значними, що тягне за собою більш помірний режим відповідальності. Протягом 2024 року, Національна рада України з питань телебачення і радіомовлення не притягувала до відповідальності онлайн-медіа за порушення відповідних вимог законодавства. Також Закон України «Про медіа» передбачає можливість розробки кодексів (правил) створення та поширення інформації щодо повідомлення про статус держави-агресора та перші два типи контенту, згадані в попередньому абзаці. Прийняття перших кодексів очікується у 2025 році.

Втім, до законодавчої якості цих обмежень залишається низка питань. Зокрема, підстави для включення до Переліку осіб, які створюють загрозу національній безпеці, у законі залишаються нечіткими, хоча у 8 рішеннях про включення до нього протягом 2024 року 22 осіб Міністерство культури і стратегічних комунікацій зазначало відповідні підстави (наприклад, у наказі від 22 жовтня 2024 року). Крім того, особи, внесені туди до прийняття Закону «Про медіа» без розкриття відповідних підстав залишатимуться в ньому без належного перегляду. Схожі проблеми з правовою визначеністю норм обговорювалися фахівцями і стосовно обмежень на трансляцію російських пісень та формування так званих білих списків російських артистів.

Інша категорія обмежень, що стосуються медіа, випливають з принципу країни заснування та походження такого суб'єкта. Стаття 120 Закону забороняє бути суб'єктом у сфері медіа в Україні низці осіб. Практичне застосування цієї норми означає, що російські громадяни чи юридичні особи, а також українські компанії, якими безпосередньо або часткою від 2% у яких володіють росіяни чи російські юридичні особи, або які фінансуються ними, не зможуть отримати ліцензію або зареєструватися як суб'єкт у сфері медіа. Ця заборона фактично діє з 2015 року і послідовно продовжує застосовуватися донині з розширенням у 2023 році кола суб'єктів та включенням до нього онлайн-медіа.

Серед загальних обмежень свободи отримувати та поширювати інформацію на час воєнного стану - зміни до Кримінального кодексу України. Стаття 114-2 у 2022 році запровадила кримінальну відповідальність за поширення в умовах воєнного чи надзвичайного стану інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, у тому числі про їх переміщення територією України (санкція - від 3 до 5 років позбавлення волі), а також інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань, за можливості їх ідентифікації на місцевості (санкція - від 5 до 8 років позбавлення волі). Відповідальність за ці дії наставатиме лише у разі, якщо відповідна інформація до цього не була поширена військовими органами, спецслужбами або уповноваженими органами державної влади. У разі наявності обтяжуючих обставин, відповідальність може сягати 8-12 років позбавлення волі. У 2022-2023 році було ухвалено 112 обвинувальних вироків, у 2024 - 85 вироків. Соціальні мережі, зокрема Telegram найчастіше стають засобом поширення несанкціонованої інформації. Огляд судової практики свідчить про труднощі в розмежуванні відповідальності за цією статтею та статтею 111 Кримінального кодексу, яка встановлює відповідальність за державну зраду. Верховний суд відносить до державної зради пошук, збирання та передавання представникам іноземної держави-агресора відомостей про розташування військової техніки, особового складу ЗСУ та інших військових формувань, залучених до надання відсічі збройній агресії російської федерації, оскільки це сприяє можливим чи дійсним зусиллям іноземної

держави, іноземної організації або їх представникам заподіяти шкоду національній безпеці України.

Окремо варто згадати про спроби обмежити користування месенджером Telegram, що пов'язують з Росією. 19 вересня 2024 року Національний координаційний центр кібербезпеки (НКЦК), що діє при Раді національної безпеки та оборони, прийняв рекомендаційне рішення обмежити використання Telegram на службових пристроях в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури. У подальшому, подібний шлях обрали щонайменше декілька освітніх інституцій.

Для обгрунтованого та пропорційного обмеження свободи вираження поглядів під час воєнного стану у відповідності з міжнародними стандартами прав людини, необхідно:

- У разі тривалого продовження правового режиму воєнного стану чіткіше окреслити обсяг відступів від зобов'язань у сфері свободи вираження поглядів та оновити відповідну декларацію;
- Забезпечити належне виконання оновленого Наказу № 73 з метою полегшення доступу представників зареєстрованих онлайн-медіа до зон ведення бойових дій та поліпшення умов для надання об'єктивної інформації про війну;
- Оновити законодавство у сфері формування Переліку осіб, які створюють загрозу національній безпеці та білих списків артистів держави-агресора для забезпечення принципів правової визначеності;
- Сприяти розробці кодексів спільного регулювання для медіа щодо визначення критеріїв віднесення інформації до такої, яку заборонено поширювати на території України відповідно до пунктів 1-2 частини першої та частини другої статті 119 Закону України «Про медіа»;
- Після закінчення правового режиму воєнного стану забезпечити належний перехід до повноцінного гарантування свободи вираження поглядів та свободи медіа, з урахуванням обмежень, встановлених Законом України «Про медіа»;
- Переглянути зміни до Кримінального кодексу України задля усунення конкуренції статей кодексу, що встановлюють відповідальність за несанкціоноване поширення інформації про розташування та переміщення військової техніки, особового складу ЗСУ та ін.

2.4.2. Правові підстави та порядок блокування Інтернет-ресурсів під час війни

Серед процедур блокування сайтів, які існують в Україні, дві є застосовними під час правового режиму воєнного стану. Ці процедури пов'язані з діяльністю Національної ради України з питань телебачення і радіомовлення та Національного центру оперативно-технічного управління електронними комунікаційними мережами України (НЦУ) та передбачені Законами України «Про медіа» та «Про електронні комунікації» відповідно.

Стаття 123 Закону «Про медіа» дозволяє блокувати за рішенням Національної ради сайти винятково аудіовізуальних медіа-сервісів на замовлення (так званих VOD-сервісів) та провайдерів аудіовізуальних сервісів держави-агресора (фактично сайтів, що надають доступ до пакетів телеканалів) у разі, якщо вони відповідають низці законодавчих критеріїв (мають у структурі власності представника держави-агресора чи фінансуються ним, або ж спрямовані на територію і аудиторію цієї держави). Серед критеріїв спрямування такого сервісу, зокрема, є надання доступу до медіа чи контенту, поширення яких є обмеженим на території України. Після встановлення

одного з цих критеріїв у рамках належної процедури, сервіс вноситься до Переліку аудіовізуальних медіа-сервісів на замовлення та сервісів провайдерів аудіовізуальних сервісів держави-агресора. Рішення про включення до Переліку може бути оскаржене до суду.

У рішенні про включення до Переліку медійний регулятор має зазначити як підставу внесення до нього, так і перелік дій щодо обмеження доступу до такого сервісу. Однією з таких дій є повідомлення Регулятора комунікаційних послуг (НКЕК) про перелік веб-сайтів, що використовуються для надання сервісів, доступ до яких на території України підлягає обмеженню постачальниками електронних комунікаційних послуг. Це повідомлення надсилається протягом 3 робочих днів з дня прийняття рішення, після чого ще 3 робочі дні дається НКЕК на направлення його операторам, які мають обмежити доступ до сайтів протягом наступних 3 робочих днів. Практичне застосування цієї норми у 2024 році обмежилося внесенням 5 сервісів до Переліку. Рішення були належно опубліковані регулятором, і Перелік містить посилання на відповідні рішення. Таким чином, було заблоковано 15 сайтів, що надавали доступ до цих сервісів, переважно спрямованих на державу-агресора.

Більш проблематичними з точки зору міжнародних стандартів є обмеження, що накладаються НЦУ, про що вже частково згадувалось в Розділі 1.1.5 цього Звіту. Дані Платформи прав людини вказують на 11 754 заблокованих сайти станом на серпень 2023 року. Ці блокування продовжилися і у 2024 році: на сайті Держспецзв'язку можна віднайти 131 розпорядження НЦУ про блокування доменних імен та IP-адрес протягом року. У попередні періоди фіксувалося застосування такого порядку блокувань до сайтів з продажу алкоголю та тютюнових виробів, а також сайтів з доступом до азартних ігор, що не пов'язане з забезпеченням інтересів національної безпеки, якого першочергово має стосуватися така процедура. Також НЦУ запровадило систему фільтрації фішингових доменів, критика якої лунала від Інтернет-асоціації України щодо наявності належних для цього повноважень та ризиків використання системи для блокування сайтів, які не використовуються для шахрайства.

Для гармонізації українського законодавства та його імплементації у цій сфері з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- Ухвалити зміни до постанови Кабінету Міністрів України від 29 червня 2004 року № 812, уточнивши сфери повноважень НЦУ щодо блокування автономних систем, а також впровадивши чіткі вимоги щодо оприлюднення розпоряджень НЦУ, що не містять інформації з обмеженим доступом;
- Після закінчення правового режиму воєнного стану забезпечити перегляд рішень НЦУ про обмеження доступу до інтернет-ресурсів та інших запроваджених обмежень.

ПРАВО НА ПОВАГУ ДО ПРИВАТНОГО ЖИТТЯ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Чинне законодавство про захист персональних даних не відображає багатьох процедурних та технічних новел, які вже впроваджені на рівні ЄС. Наприклад, Закону України «Про захист персональних даних» бракує концепції права на забуття, інституту відповідальної за захист даних особи, процедури проведення оцінки впливу на захист даних тощо. Для гармонізації з європейськими стандартами варто імплементувати стандарти Загального регламенту про захист даних, а також створити незалежного регулятора у сфері захисту даних, який зможе забезпечити виконання законодавства.

Крім того, Україна має впровадити і ряд інших європейських актів, таких як Акт про дані, Акт про штучний інтелект, Акт про управління даними тощо. Їх належна імплементація передбачає комплексне оновлення національного законодавства, включно з передбаченням переліку заборонених практик у сфері захисту даних. Україна також має забезпечити належні гарантії у сфері державного стеження, а також запровадити заборону на використання шпигунського та шкідливого програмного забезпечення щодо вразливих груп, таких як журналісти, активісти та правозахисники. Особливо актуальними такі заходи є на тлі додаткових обмежень, впроваджених на час дії правового режиму воєнного стану.

3.1. Захист персональних даних

3.1.1. Законодавчі гарантії захисту персональних даних

Основні засади регулювання сфери захисту персональних даних передбачені Законом України “Про захист персональних даних”. Закон в цілому відображає гарантії, які вимагаються Загальним регламентом про захист даних ЄС (GDPR): передбачає принципи та підстави обробки персональних даних, перелічує права суб’єкта даних, забороняє обробку чутливих категорій даних із відповідними винятками, та ін. Водночас, положення закону сформульовані у загальних та нечітких термінах, які відкривають поле для правової невизначеності. У законі також відсутній концепт “контролера” та “процесора” у формальному розумінні Загального регламенту про захист даних - натомість передбачено “володільця” та “розпорядника” даних, які лише частково відображають функції згаданих суб’єктів.

Визначення “контролера” в українському законі залишається неоднозначним. Згідно зі статтею 2 закону, володільцем персональних даних є “фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом”. Українська дефініція вимагає від володільця визначати виключно “мету обробки”, в той час як Загальний регламент про захист даних наголошує на визначенні мети та “засобів”. На практиці це означає, що володілець не перевіряє, як та за допомогою яких інструментів досягається відповідна мета. Оскільки робота контролера повинна відбуватися з кумулятивним урахуванням як мети, так і засобів обробки даних, відсутність одного з елементів у цьому випадку прямо суперечить європейським керівництвам щодо захисту персональних даних (п. 36).

Закон також не передбачає концепції “спільних контролерів” та механізму регулювання їх спільної обробки даних. Відсутність законодавчих орієнтирів у даному випадку призводить до незрозумілого поділу обов’язків щодо дотримання прав суб’єкта даних.

Наприклад, існує ризик невиконання функцій контролера щодо запитів суб'єкта даних (про видалення або виправлення інформації та ін.), оскільки невідомо, чи був наділений відповідний контролер функціями щодо обробки відповідних даних у першу чергу.

Чинний закон не встановлює принципи захисту даних за проектуванням та за замовчуванням, передбачені Загальним регламентом про захист даних, тому українські контролери наразі не зобов'язані вживати превентивні заходи, які могли б усунути потенційні порушення. Закон також не встановлює належних механізмів реагування на порушення, повідомлення особи про неправомірні дії з її даними або забезпечення ефективних засобів її правового захисту.

Проєкт Закону №8153 про захист персональних даних, зареєстрований у жовтні 2022 року, спрямований на гармонізацію українського законодавства з європейськими стандартами в сфері захисту персональних даних. На відміну від чинного закону, Розділ V проєкту цілком присвячений контролеру та оператору ("процесору") - він віддзеркалює положення Загального регламенту про захист даних та описує функції відповідних суб'єктів, включаючи концепції спільних контролерів, проектування за дизайном та замовчуванням, а також механізм реагування на правопорушення у сфері захисту даних. Головний комітет ВРУ прийняв проєкт за основу у листопаді 2024 року, документ готується до другого читання.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто:

- вдосконалити закон у сфері захисту персональних даних із урахуванням стандартів Загального регламенту про захист даних;
- передбачити в окремому розділі закону механізм роботи контролера та процесора відповідно до стандартів Загального регламенту про захист даних, а саме:
  - узгодити визначення "контролера" з дефініцією, передбаченою у Загальному регламенті про захист даних;
  - встановити відповідні функції та повноваження контролера та процесора;
  - передбачити концепцію "спільних контролерів";
  - встановити зобов'язання щодо розробки технічних та організаційних заходів для реагування на порушення у сфері захисту персональних даних (як превентивних, так і проактивних).

3.1.2. Дотримання загальних принципів та підстав обробки персональних даних

Стаття 6 Закону України "Про захист персональних даних" встановлює загальні вимоги до обробки персональних даних, які відображають основоположні принципи, закріплені Загальним регламентом про захист даних. Незважаючи на те, що принципи становлять фундамент правомірної обробки даних, закон не акцентує на них увагу, дотично зазначаючи їх в окремих положеннях. Наприклад, принцип "мінімізації даних" випливає із частини 3 статті 6 закону, за яким "склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки". У свою чергу, принцип "обмеження мети" відображається у частині 5 та третьому абзаці частини 1 статті 6 закону. У цій же статті закон у загальних рисах передбачає принципи законності, добросовісності та прозорості, точності персональних даних та конфіденційності. Примітно, що закон не містить чіткого переліку таких принципів - вони фрагментарно розкидані окремими положеннями

статті без структуризації та узгодження між собою, що ускладнює сприйняття та розуміння механізму їх реалізації.

Чинний закон не передбачає принципу "обмеження зберігання", за яким персональні дані повинні зберігатися не довше, ніж це необхідно для цілей, в яких вони обробляються, за винятком випадків, встановлених законом. Закон також не містить посилання на принципи "цілісності" (обробка даних із вжиттям належних технічних та організаційних заходів) та "підзвітності" (відповідальність контролера за дотримання принципів). Це пояснюється відсутністю в українському законі концепцій "контролера" та "процесора" і, як наслідок, недосконалим механізмом їх роботи.

У свою чергу, посилання на підстави для обробки персональних даних міститься у статті 11 закону та фактично відображає вимоги Загального регламенту про захист даних. Говорячи про підставу щодо необхідності виконання завдання контролером, український закон посилається лише на "необхідність виконання обов'язку володільця персональних даних, який передбачений законом" (п. 5 ч. 1 стаття 11), не адресуючи необхідності виконання завдання в суспільних інтересах як додаткової підстави, передбаченої Загальним регламентом про захист даних. Аналогічна проблема міститься і у статті 7 закону, яка містить вимоги до обробки чутливих персональних даних та встановлює випадки, за яких така обробка буде правомірною. Закон здебільшого відображає всі підстави, що містяться у регламенті, проте випускає обробку чутливих даних, необхідну в цілях "значного суспільного інтересу" та "архівування в суспільних інтересах, для цілей наукового чи історичного дослідження або статистичних цілей".

Відсутність концепції "суспільного інтересу" у даному випадку слугує обмежуючим фактором щодо обробки даних приватними інституціями та громадськими організаціями, залученими у суспільно важливу діяльність, зокрема, у контексті дослідницьких проєктів, ініціатив у сфері охорони здоров'я та програм соціальної допомоги.

На відміну від чинного закону, Проєкт Закону №8153 про захист персональних даних окреслює принципи та підстави обробки персональних даних у більш розширеному форматі. Віддзеркалюючи положення Загального регламенту про захист даних, проєкт передбачає перелік принципів обробки персональних даних та пояснює їх значення, а також деталізує підстави такої обробки, фактично закриваючи всі прогалини, які містять діючі положення.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто:

- передбачити перелік основоположних принципів обробки персональних даних та механізм їх реалізації, доповнивши ряд принципами щодо обмеження зберігання, цілісності та підзвітності;
- передбачити необхідність обробки персональних даних в цілях суспільного інтересу як додаткову підставу для обробки персональних даних;
- передбачити необхідність захисту значного суспільного інтересу та архівування в суспільних інтересах, для цілей наукового чи історичного дослідження або статистичних цілей як додаткові підстави для обробки чутливих категорій даних.

3.1.3. Дотримання прав суб'єктів персональних даних

Стаття 8 Закону України "Про захист персональних даних" в цілому наділяє суб'єкта даних широким обсягом прав, серед яких право на інформацію, право на доступ до даних, право на зміну або видалення даних, право на заперечення щодо обробки

персональних даних, відшкодування шкоди тощо. Втім, законодавчим положенням бракує деталізації – окрім переліку наданих прав, закон не містить індикаторів щодо механізму їх реалізації, що, у свою чергу, ускладнює розуміння власних гарантій суб'єктами даних.

У контексті права на доступ до персональних даних закон не уточнює інформацію, яка обов'язково повинна надаватися суб'єкту даних для забезпечення цього права відповідно до умов Загального регламенту про захист даних і яка включає мету обробки даних, період зберігання даних, джерела збору даних тощо. Наразі інформаційні зобов'язання контролера не є суттєвими та наділяють його можливістю на власний розсуд вирішувати, який обсяг інформації буде отримано суб'єктом даних.

Крім того, окремі положення не конкретизують обсягу прав суб'єктів даних відповідно до стандартів Загального регламенту про захист даних. Закон наділяє особу правом заперечувати проти обробки своїх персональних даних (п. 5 ч. 2 стаття 8), але конкретизує реалізацію такого права при здійсненні обробки даних для цілей прямого маркетингу або профайлингу. Закон також не поширює права заперечення на обробку даних в наукових або дослідницьких цілях. Аналогічна деталізація відсутня і у положенні, що передбачає право суб'єкта даних на обмеження обробки даних: особа може здійснити відповідне застереження виключно "під час надання згоди" (п. 10 ч. 2 стаття 8). Закон не уточнює обставин, за яких особа потребуватиме від контролера збереження її даних після здійснення обробки: йдеться, наприклад, про оскарження точності персональних даних або їх неправомірну обробку. Нарешті, у контексті права на захист від автоматизованого прийняття рішення, закон не включає захист від профайлингу, а також легітимні випадки, на які такий захист не поширюватиметься.

Український закон не наділяє суб'єкта даних ні «правом бути забутим», ані правом на мобільність персональних даних (надання суб'єкту даних копії будь-яких його персональних даних), які передбачені Загальним регламентом про захист даних. Найбільш наближеним до «права бути забутим» можна вважати п. 4 ч. 2 статті 15 Закону України "Про захист персональних даних", за яким персональні дані підлягають видаленню або знищенню в разі набрання законної сили рішенням суду щодо видалення або знищення персональних даних. Втім, за законом, вимога щодо знищення персональних може бути пред'явлена тільки якщо ці дані обробляються незаконно чи є недостовірними (п. 6 ч. 2 стаття 8), тому і судова практика обмежується виключно відповідними скаргами. Водночас стаття 21 Проєкту Закону №8153 про захист персональних даних передбачає право на забуття та механізм його реалізації за європейськими стандартами.

Ситуацію недосконалості законодавчих положень значним чином вирішує Проєкт Закону №8153 про захист персональних даних. Запозичуючи структуризацію Загального регламенту про захист даних, проєкт присвячує Розділ IV правам суб'єктів персональних даних, описує механізм їх реалізації в окремих положеннях, розширює обсяг таких прав та інкорпорує регуляторні аспекти, яких бракує у чинному законі.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, у оновленому законі варто:

- імплементувати право бути забутим та право на мобільність персональних даних;
- конкретизувати обсяг існуючих прав, а саме:
  - посилити інформаційні зобов'язання у праві на доступ до персональних даних, уточнивши перелік інформації, яку повинен надавати контролер;

- поширити обсяг права на заперечення проти обробки персональних даних на обробку даних в цілях профайлингу, прямого маркетингу, а також науково-дослідницьких цілях (включаючи архівування та статистику);
- передбачити додаткові обставини, за яких буде реалізовано право на обмеження обробки персональних даних (наприклад, оскарження точності даних або неправомірна обробка даних);
- розширити обсяг права на захист від автоматизованого прийняття рішення, включивши захист від профайлингу.

3.1.4. Внутрішні інструменти дотримання стандартів захисту персональних даних

Чинний Закон України "Про захист персональних даних" не передбачає внутрішніх інструментів захисту персональних даних, а отже, не відповідає вимогами статей 35-43 Загального регламенту про захист даних. Зміни пропонується внести Законопроєктом №8153. Зокрема, статті 39-40 передбачають вимогу щодо проведення оцінки впливу обробки персональних даних і, в цілому, є реплікою положень регламенту ЄС. Аналогічно законопроєкт передбачає механізм призначення відповідальної за захист даних особи, а також процедуру для проведення кваліфікаційного іспиту для такої особи. Стаття 43 також містить положення щодо Кодексу поведінки. Втім, положення щодо моніторингу дотримання добровільно взятих зобов'язань відсутні, тож процедура впровадження і виконання вимог таких кодексів залишається незрозумілою. Щонайменше в цій частині Законопроєкт потребує уточнень - або ці зобов'язання покладатимуться на наглядовий орган, або слід призначати окремий саморегулівний орган, який слідкуватиме за дотриманням вимог Кодексу. Крім того, будь-які положення про процедури сертифікації, печаток чи маркування відсутні, тож законопроєкт не відповідає вимогам Загального регламенту про захист даних в цій частині, а саме статтям 42-43.

На практиці подібні інструменти використовують нечасто. Так, в Україні немає практик призначати відповідальних осіб із захисту даних у компаніях, які не орієнтуються на європейський ринок. Подібна проблема існує і в державних органах, особливо тих, які на практиці обробляють персональні дані - наприклад, адмініструють державні додатки "Дія", "ДійВдома", "Резерв+", "Мрія" тощо. Аналогічного підходу притримуються і щодо оцінки впливу на захист даних – її переважно проводять у випадку, коли необхідно довести відповідність вимогами Загального регламенту про захист даних. Методології для проведення такої оцінки немає, проте на її необхідності наголошував Уповноважений ВРУ з прав людини. В Україні наразі відсутні і кодекси поведінки. Модельний кодекс поведінки ще у 2019 році був оприлюднений Київським ЦНАПом, втім ані процедури приєднання до нього, ані списку підписантів у публічному доступі немає. З цього можна зробити висновок, що більшість приватних і публічних акторів наразі керуються винятково законодавчими вимогами та внутрішніми політиками, не маючи додаткових зобов'язань відповідно до Кодексів поведінки. Жодних практик сертифікації, накладання печаток чи маркування наразі немає.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто:

- внести у законодавство вимоги щодо проведення оцінки впливу процесів обробки на захист даних та вимоги до такої обробки;
- розробити підзаконні нормативно-правові акти щодо випадків, коли оцінка впливу є обов'язковою, а також типових алгоритмів проведення такої оцінки;

- доповнити законодавство про захист персональних даних вимогами щодо призначення відповідальної особи за захист даних, вимогами щодо призначення осіб на такі посади та мінімального обсягу їх повноважень;
- сприяти розробці та підписанню добровільних кодексів поведінки у сфері захисту персональних даних;
- розробити механізм сертифікації/акредитації органу, що здійснює моніторинг дотримання добровільно взятих в рамках кодексів поведінки обов'язків відповідними контролерами та операторами даних;
- розробити типові сертифікати, печатки і маркування, які використовуватимуться для посвідчення відповідності практик обробки даних законодавчим вимогами;
- розробити механізм сертифікації/акредитації органу, що здійснює сертифікацію, надає печатки та маркування.

3.1.5. Вільний обіг даних

Чинний Закон України "Про захист персональних даних" у статті 29 частково регулює питання транскордонної передачі даних (з посиланням на правила, передбачені Конвенцією 108+). Водночас, він не відповідає вимогам Загального регламенту про захист даних в частині права на мобільність даних, вимог щодо перевірки рівня захисту даних корпоративними правилами або державним регулюванням при їх транскордонній передачі. Також закон не містить положень щодо діяльності інтернет-посередників та онлайн-платформ, що ускладнює його застосування в сучасних реаліях. В цілому, як зазначалося раніше, чинне законодавство потребує щонайменше гармонізації із Загальним регламентом про захист даних.

Ключові зміни в цій сфері пропонує Законопроєкт №8153, який у статті 23 закріплює право на мобільність даних, а також має окремий Розділ VI, присвячений транскордонній передачі даних і встановленню вимог до суб'єктів, що отримуватимуть до них доступ. В тому числі, такі правила стосуються мінімальних вимог до корпоративних правил (стаття 47). Водночас, законопроєкту все ще бракує положень щодо права на альтруїзм даних та супутніх вимог до організацій, які допомагають його реалізувати, можливості повторного використання даних та інтероперабельності сервісів, які обробляють персональні дані (зокрема, як передбачено Актом про управління даними на рівні ЄС). Також немає вимог щодо обов'язків посередників і постачальників послуг онлайн-пошуковиків для товарів і послуг у сфері захисту персональних даних, особливостей обробки і варіантів, як вона може здійснюватися. Оскільки законодавство у сфері захисту персональних даних перебуває в процесі оновлення, доречно було б поєднати усі вимоги та новели, впроваджені за останні кілька років на рівні ЄС та об'єднати їх в одному регуляторному акті.

Регулювання обігу інформації у публічному секторі здійснюється Законом України "Про доступ до публічної інформації", а також Постановою 835 Кабінету Міністрів України «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних». В цілому, стаття 10-1 Закону регулює відкриті дані і формат в якому вони мають надаватися (безоплатно, вільно, з можливістю автоматизованої обробки). Водночас, він не містить згадок про динамічні дані, а також немає належних санкцій за несвоєчасне оновлення відкритих даних чи незабезпечення доступу з технічних чи юридичних причин. Також немає вимог щодо заборони локалізації даних (з відповідними безпековими винятками). Також немає регулювання, що уможливлює повторе використання даних (не захищених правом інтелектуальної

власності чи законодавством про захист персональних даних) на підставі договорів, яке передбачене Актом про управління даними.

Окремі аспекти обігу даних регулюються Законом України «Про електронні комунікації», зокрема щодо даних трафіка і даних про місцезнаходження користувачів. Стаття 119 вказує на те, що така інформація має захищатися постачальниками електронних комунікаційних послуг. Водночас, відсутня пряма норма про заборону зберігання та доступу до вмісту комунікацій (паралельно зі зберіганням даних трафіка). Стаття 120 передбачає захист від спаму і небажаних повідомлень. Крім того, в Законі України «Про захист інформації в інформаційно-комунікаційних системах» та Порядку передачі, зберігання, функціонування та доступу до державних інформаційних ресурсів та їх резервних копій є певні вимоги щодо умов зберігання даних, в тому числі тих, що належать до державного сектору. Окремих вимог щодо заборони локалізації даних чи винятків немає.

Окрім цього, Закон України "Про електронну комерцію" дуже побіжно згадує посередників і постачальників послуг онлайн-пошуковиків для товарів і послуг, узагальнюючи їх єдиним поняттям "інтернет-магазин". На жаль, цей регуляторний акт не містить жодних вимог до порядку організації роботи таких суб'єктів з даними, в тому числі персональними, можливості та умов доступу до даних та їх передачі третім особам. Відсутні також і вимоги щодо прозорості таких процесів обробки даних. В цілому українське законодавство жодним чином не регулює питання доступу до даних генерованих продуктами інтернету речей, структури таких даних і режимів доступу користувачів.

На практиці, наразі відсутні механізми сертифікації рівня захисту персональних даних в інших країнах, а конкретні обмеження щодо незастосування положень Конвенції 108+ до країни-агресора належно не прописані. Також, за рахунок відсутності належного нагляду на національному рівні корпоративні правила захисту даних часто не виконуються і є декларативними. Більше того, існують проблеми з оновленням відкритих даних, особливо тієї категорії, що є динамічною. Якість даних на Порталі відкритих даних (що регулюється окремою Постановою 867) часто є відносно низькою, тож зацікавленим у отриманні потрібної інформації особам доводиться користуватися механізмами, передбаченими Законом України "Про доступ до публічної інформації". Це робить процес отримання необхідних даних значно складнішим. З огляду на воєнний стан і супутні обмеження, запитувачі часто отримують відмови на запит про доступ до публічної інформації. Наразі дієвих механізмів отримання інформації немає і спори у цій сфері часто вирішуються у судовому порядку.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто:

- внести зміни до Закону України "Про захист персональних даних" щодо посилення захисту персональних даних при транскордонній передачі шляхом гармонізації з вимогами Загального регламенту про корпоративні правила та оцінку адекватності рівня захисту даних;
- уточнити вимоги щодо заборони локалізації даних та забезпечення вільного обігу даних з державами-членкинями ЄС та (потенційно) державами-учасницями Конвенції 108+ з відповідними застереженнями щодо країни-агресора на час дії воєнного стану;
- розробити і впровадити в національне законодавство (зокрема, Закон України "Про захист персональних даних") концепцію "альтруїзму даних", а також організацій, які можуть використовувати такі дані, обмеженого переліку цілей їх використання та процедур поводження з даними, які більше не є потрібними;

- внести зміни до Закону України "Про електронні комунікації" щодо спеціальних вимог до обробки даних про місцезнаходження, а також період зберігання даних трафіка і метаданих;
- оновити законодавство щодо локалізації даних (в тому числі Закон України "Про електронні комунікації"), чіткіше прописавши винятки, коли локалізація даних є необхідною з питань національної безпеки чи захисту публічного порядку, а також встановити механізми контролю і співпраці щодо обміну даними, зокрема з країнами ЄС, в рамках загальної заборони на локалізацію даних;
- законодавчо закріпити право на мобільність даних і доступ до даних генерованих продуктами інтернету речей, включно з тим, як дані структуровані, на якій підставі доступ отримується та які існують винятки (невідкладні обставини, обґрунтовані запити державних органів);
- врегулювати діяльність посередників і постачальників послуг онлайн-пошуковиків для пропонування товарів і послуг, встановити вимоги до їх діяльності та режими їх роботи з персональними даними;
- оновити Закон України "Про доступ до публічної інформації" і внести зміни щодо регулювання відкритих даних, обов'язків забезпечувати їх доступність і адекватний формат, процедурних вимог щодо отримання даних від розпорядників (в тому числі щодо динамічних даних);
- на рівні підзаконних нормативно-правових актів розробити стандарти інтероперабельності, доступу до динамічних даних і API-специфікацій шляхом оновлення Постанови 835, оновити перелік наборів даних, що оприлюднюються у форматі відкритих даних (гармонізувавши його з Директивою про відкриті дані на рівні ЄС);
- на рівні підзаконних нормативно-правових актів розробити моніторингові механізми дотримання правил транскордонної передачі даних, типові договірні положення для передачі даних, типові безпекові протоколи захисту даних (зокрема для державних органів);
- в рамках освітніх програм розробити тренінги для офіцерів захисту даних та рекомендації для бізнесу щодо обігу даних та застосовних правових стандартів у цій сфері, включно з вимогами до захисту персональних даних.

3.1.6. Заборонені практики у сфері захисту даних

Чинний Закон України "Про захист персональних даних" не встановлює заборону на прийняття рішень, які мають правові наслідки для особи чи іншим чином істотно впливають на неї, виключно на підставі автоматизованої обробки персональних даних, у тому числі профайлінгу. Частина 13 статті 8 закону, що закріплює право суб'єкта персональних даних "на захист від автоматизованого рішення, яке має для нього правові наслідки" потребує оновлень. Детальніше про це йдеться у частині 5.4.2 цього Звіту. Крім того, у чинному українському законодавстві про захист персональних даних відсутня дефініція поняття "профайлінг". Законопроєкт №8153 пропонує заповнити ці прогалини шляхом додавання визначення "профайлінгу" та виділення деталізованих положень щодо автоматизованого прийняття рішень в окрему статтю (стаття 25).

Регулювання систем ШІ поки відсутнє на рівні національного законодавства. Відповідно, в Україні не передбачено категоризації систем ШІ за рівнем ризику та встановлення законодавчої заборони на системи ШІ, які становлять неприйнятний ризик для безпеки і прав людини. Це не узгоджується із вимогами Акту ЄС про ШІ (AI Act), у статті 5 якого наведено перелік таких заборонених систем: соціального ранкування, категоризації

осіб на основі біометричних даних та ін. Відомо, що в майбутньому планується імплементація Акту ЄС про штучний інтелект до національного законодавства, у тому числі й положень щодо заборонених систем ШІ, проте процес впровадження буде тривалим.

На практиці, в Україні широко використовуються системи ШІ, у зв'язку з чим відсутність чітких нормативних заборон чи принаймні обмежень щодо найбільш небезпечних систем призводить до серйозної загрози для захисту персональних даних. Наприклад, у ЄС Clearview AI було визнано винним у нецільовому скрейпінгу зображень облич з інтернету для розширення бази даних розпізнавання облич, що є несумісним із вимогами Загального регламенту про захист даних. У той же час український уряд активно співпрацює із Clearview AI, зокрема з метою ідентифікації загиблих осіб, посилення безпеки на контрольно-пропускних пунктах та ідентифікації російських воєнних злочинців. Тобто, з одного боку, використання цієї системи істотно допомагає Україні в умовах війни, але з іншого – нецільовий скрейпінг зображень облич становить значні ризики для суб'єктів даних. Цей приклад демонструє потребу впровадження в Україні регулювання щодо систем ШІ, які здійснюють обробку біометричних та інших чутливих персональних даних, із встановленням меж для їхнього використання.

У чинній редакції Закону України "Про захист персональних даних" відсутні положення щодо заборони обробки персональних даних неповнолітніх осіб у комерційних цілях. Законопроєкт № 8153 теж не містить заборони такої обробки. Водночас, у статтях 13 (частина 10) та 14-2 (частина 6) чинного Закону України "Про рекламу" встановлено заборону для суб'єктів у сфері аудіальних та аудіовізуальних медіа, а також провайдерів платформ спільного доступу до відео та платформ спільного доступу до інформації, обробляти зібрані чи в інший спосіб отримані персональні дані дітей з такою комерційною метою, як прямий маркетинг та профайлінг, включно із поведінково орієнтованою рекламою. Ці положення відповідають вимогам Директиви ЄС про аудіовізуальні медіапослуги та стандартам Ради Європи. Проте серед кола суб'єктів, на яких спрямована ця заборона в національному законодавстві, не зазначено про провайдерів онлайн-платформ у більш широкому розумінні, що не узгоджується із положеннями Акту ЄС про цифрові послуги.

Акт про цифрові послуги поширює захист від заборонених форм профайлінгу у сфері маркетингу не лише на неповнолітніх осіб. Адже він передбачає загальну заборону для провайдерів онлайн-платформ демонструвати рекламу на основі профайлінгу із використанням чутливих персональних даних. Тобто ця заборона стосується захисту персональних даних усіх осіб, без диференціації за віком. Закон України "Про рекламу" поки що не містить аналогічної заборони.

На практиці, виявлено випадки реклами на основі профайлінгу із використанням чутливих персональних даних. Так, зокрема, Cambridge Analytica використовувала персональні дані користувачів Facebook без їхньої згоди (у тому числі дані, що розкривають політичні погляди) для профайлінгу виборців у цілях таргетованої політичної реклами. Такі приклади підкреслюють важливість встановлення законодавчої заборони на застосування профайлінгу на основі чутливих персональних даних у маркетинговій сфері для захисту прав суб'єктів даних і справедливих демократичних процесів.

Для гармонізації українського законодавства з вимогами ЄС, варто:

- внести до Закону України "Про захист персональних даних" поняття профайлінгу, що узгоджуватиметься із визначенням у Загальному регламенті про захист даних;

- уточнити в законодавстві, що профайлінг не повинен призводити до дискримінації осіб на основі чутливих персональних даних;
- розширити перелік суб'єктів, яким на підставі Закону України "Про рекламу" забороняється здійснювати обробку персональних даних неповнолітніх осіб у комерційних цілях, шляхом поширення цієї заборони на провайдерів онлайн-платформ;
- на законодавчому рівні заборонити провайдерам онлайн-платформ демонструвати рекламу на основі профайлінгу із використанням чутливих персональних даних;
- врегулювати використання державними органами систем ШІ, які обробляють біометричні дані, зокрема для баз даних розпізнавання облич, із встановленням належних гарантій захисту даних від нецільового скрейпінгу;
- встановити пропорційні санкції за порушення норм щодо заборонених практик у сфері захисту персональних даних.

3.2. Приватність та безпека у цифровому середовищі

3.2.1. Захист честі, гідності та ділової репутації

Національне законодавство гарантує кожному право на захист честі, гідності або ділової репутації від шкоди, заподіяної внаслідок поширення про особу та (або) членів її сім'ї недостовірної інформації. Особа може самостійно обрати належний спосіб захисту: відшкодування майнової та/або моральної (немайнової) шкоди (пп. 8-9 ч. 2 статті 16 Цивільного кодексу України), право на відповідь або спростування недостовірної інформації (ч. 1 статті 277 ЦК України); встановлення факту недостовірності поширеної інформації та її спростування, коли неможливо встановити поширювача (ч. 4 статті 277 ЦК України); заборона поширення інформації, якою порушуються особисті немайнові права (стаття 278 ЦК України).

Варто зауважити, що Цивільний кодекс у статті 280 встановлює виняток щодо відшкодування шкоди, майнової та (або) моральної, у разі неумисного повідомлення викривачем недостовірної інформації про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону України "Про запобігання корупції". У такому випадку фізична особа, особисті немайнові права якої порушено внаслідок такого повідомлення, має право на відповідь.

Закон України «Про медіа», що набрав чинності 31 березня 2023 року, у статті 43 уніфікував процедуру та правила позасудової реалізації права на відповідь та спростування, якщо недостовірна інформація була поширена у медіа, гармонізувавши національні норми з вимогами Директиви про аудіовізуальні медіапослуги (стаття 28). Закон встановлює строки на подання заяви, вимоги до зазначеної в ній інформації, строки розгляду та вичерпний перелік підстав для відмови, порядок поширення спростування або відповіді та ін. Відмова поширити спростування або відповідь, дії суб'єкта у сфері аудіовізуальних, друкованих або онлайн-медіа з поширення спростування або відповіді, які не відповідають вимогам закону, можуть бути оскаржені до суду. При цьому, подання особою заяви про спростування або реалізацію права на відповідь до суб'єктів у сфері медів, не є обов'язковою умовою (чи перешкодою) для звернення до суду з відповідним позовом.

Оскільки зареєстровані суб'єкти у сфері медіа зобов'язані оприлюднювати свої вихідні дані (стаття 37 Закону України «Про медіа»), зокрема дані реєстрації та контакти,

це полегшує можливість ідентифікувати поширювачів інформації для подання заяви до суду. Водночас, поширення недостовірної інформації анонімними каналами у соціальних мережах створює суттєві перешкоди в реалізації права на ефективний захист через неможливість ідентифікувати належного відповідача у дифамаційній справі.

Важливо, що захист честі, гідності та ділової репутації особи завжди вимагатиме зважування реалізації цього права з правом на свободу вираження поглядів. Детальніше стандарти такого балансування розглянуті у Розділі 2.1.4.

У 2022 році Кримінальний кодекс України був доповнений статтею 435-1, яка передбачила кримінальну відповідальність за образу честі і гідності військовослужбовця, його близьких родичів чи членів сім'ї, виготовлення та поширення матеріалів з такими повідомленнями, з покаранням у формі обмеження волі на строк від трьох до п'яти років або позбавленням волі на той самий строк. Державний реєстр судових рішень дозволяє ознайомитись із двома вироками про визнання винними у вчиненні кримінального порушення, які стосувались дописів у соціальних мережах, що ображали військовослужбовців. У справі №712/4108/22 порушниці призначили покарання у виді позбавлення волі на три роки та звільнили від його відбування з випробуванням. У справі №718/418/23 суд затвердив угоду між прокурором та обвинуваченим, зобов'язавши порушника сплатити штраф у розмірі 17 тис. грн.

Встановлення кримінальної відповідальності за образу честі та гідності саме по собі не є одразу порушенням міжнародних стандартів у сфері прав людини, проте на практиці у конкретних справах державам рідко вдається довести наявність нагальної суспільної потреби та пропорційність застосованих заходів, адже саме по собі притягнення до кримінальної відповідальності, навіть якщо призначене покарання буде незначним або умовним, вже є серйозним втручанням в права людини. Варто згадати, що у 2001 році при прийнятті нового Кримінального кодексу України до нього свідомо не були перенесені статті, що криміналізували наклеп та образу, зокрема з огляду на низьку суспільну небезпечність. Крім цього, поняття «образа», «честь» та «гідність» мають суб'єктивний характер, а тому цивільний процес тут більше пристосований для пошуку адекватного способу захисту прав особи.

Застосування статті 435-1 до цивільних осіб також викликає питання законності, адже стаття 401 відповідного розділу Кримінального кодексу чітко визначає, що військовими кримінальними правопорушеннями визнаються передбачені цим розділом кримінальні правопорушення проти встановленого законодавством порядку несення або проходження військової служби, вчинені військовослужбовцями, а також військовозобов'язаними та резервістами під час проходження зборів. Тобто, йдеться про спеціального суб'єкта. Науковці вказують і на низку інших колізій та недоліків, пов'язаних із застосуванням нових норм.

З огляду на це, для гармонізації українського законодавства та правозастосування з вимогами ЄС та Ради Європи, варто:

- переглянути доцільність статті 435-1 Кримінального кодексу України в її чинній редакції, з огляду на проаналізовані теоретичні колізії та практику застосування, та внести необхідні зміни до Кримінального кодексу України, у т.ч. виключивши з переліку кримінальних правопорушень «образу честі і гідності».

3.2.2. Право на зображення

В українській правовій системі право особи на захист її зображення закріплюється різними законами. Так, стаття 308 Цивільного кодексу України встановлює загальну заборону на публічний показ, відтворення та розповсюдження фотографій особи без її згоди, за винятком необхідності захисту її інтересів або інтересів інших осіб. Аналогічне положення міститься і у п. 9 частини 1 статті 8 Закону України "Про рекламу", який забороняє використовувати зображення особи без її згоди, наданої в письмовій або електронній формі. Крім того, фотографічний твір є об'єктом авторського права, на який поширюються вимоги Закону України "Про авторське право і суміжні права" (п. 9 частина 1 стаття 6).

Стаття 10 Закону України "Про охорону дитинства" встановлює гарантії для захисту права на зображення неповнолітніх осіб, забороняючи публікацію будь-якої інформації про дитину, що може спричинити їй шкоду, без згоди законного представника дитини. Водночас рекламне законодавство забороняє використовувати зображення дитини у небезпечних ситуаціях або обставинах, що можуть завдати їй шкоди (частина 2 статті 20).

У контексті ступеня публічності особи в громадському житті як фактору, що враховується ЄСПЛ при балансі приватності та свободи вираження поглядів, українське законодавство окреслює певні категорії осіб, інформація про яких може бути поширена на законних підставах. Наприклад, закон не відносить до інформації з обмеженим доступом інформацію про керівників або членів наглядової ради державного чи комунального підприємства, членів виконавчого органу або наглядової ради господарського товариства. Аналогічно, до цієї категорії не входять і відомості про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб. Тобто журналістські розслідування залишаються захищеними, включно з візуальними матеріалами.

Українські закони не передбачають адміністративної чи кримінальної відповідальності за неправомірне поширення або публікацію зображень особи. Наразі Кримінальний кодекс України передбачає санкції лише за незаконне відтворення, використання та розповсюдження фотографічних творів як порушення авторського права і суміжних прав (стаття 176), а також ввезення, виготовлення, збут і розповсюдження зображень порнографічного характеру (стаття 301).

У контексті практичного застосування статті 308 ЦК українські суди притримуються здебільшого єдиного підходу – публікація зображень особи без її згоди забороняється за винятком необхідності досягнення легітимного інтересу. При цьому чіткого тлумачення щодо концепту "легітимного інтересу" судами надано не було. Якщо ж особа самостійно опублікувала фотографії, наприклад, у соцмережах, необмеженому колу осіб, подальше використання вже публічних та відкритих фото третіми особами вважається правомірним. Втім, з огляду на відсутність в українській системі концепції "права на зображення", суди залишаються небагатослівними щодо правомірності використання зображень з боку медіа, дотримуючись відносно формального та обмеженого тлумачення закону.

Натомість ясність у законодавство намагаються вносити на рівні саморегулювання – експерти з незалежних агентств оцінюють та аналізують справи, виокремлюють проблемні аспекти та надають рекомендації щодо етичного висвітлення журналістами матеріалів справи. Примітно, що на практиці особи, чиї фотографії були поширені без їх згоди у медіа, зазвичай не оскаржують правомірність публікацій – скарги стосуються здебільшого дифамації, коли фотографії особи опубліковані із супроводжуючим

текстом про неї, який не відповідає дійсності. Втім, загальним правилом залишається те, що медіа не повинні публікувати разом із матеріалом супроводжуючу фотографію особи, якщо зображення не несе жодної цінності до публічної дискусії, а лише посилює/провокує інтерес громадськості до відповідних новин.

На потребі щодо належного балансування права на приватність із правом громадськості на отримання інформації неодноразово наголошували і органи саморегулювання у своїх окремих рішеннях. Такі рішення стосувалися здебільшого публікації медіа "резонансних справ", які викликали великий інтерес громадськості та в яких часто фігурували посадові особи та державні діячі. Наприклад, у справі, де було опубліковано матеріали про доходи керівниці Аудиторської палати, Комісія журналістської етики визнала, що опубліковані фотографії керівниці як публічної особи були виправдані суспільним інтересом. Водночас у справі, яка стосувалася допису в Телеграм-каналі журналіста про новорічну вечірку з оголеними танцівницями, Комісія визнала, що навіть сенсаційні новини повинні відповідати стандартам журналістської етики щодо дотримання особами права на приватність, особливо якщо в них не фігурують відомі особи.

Незалежна медійна рада (НМР) наголосила, що при публікації зображень та висвітлення матеріалів справи (особливо щодо кримінальних правопорушень) медіа передовсім повинні дотримуватися "принципу гуманізму, а не сенсаціоналізму", який пов'язаний із уникненням голосних заголовків та неупередженим форматом подачі інформації. Це яскраво виражається у рішеннях НМР щодо матеріалів ТОВ «Телерадіокомпанія "Студія "1+1"» та інтернет-порталу «Vesti.ua», які висвітлювали інформацію щодо злочинів проти статевої свободи, додатково опубліковуючи фотографії потерпілих та резонансні заголовки.

Українська правова система не містить також і правил щодо маркування зображень, згенерованих системами ШІ, не дивлячись на активну залученість України у розробку та використання ШІ-технологій. Втім, потреба у регулюванні вже була окреслена у окремих державних політиках для мінімізації ризиків правам людини. Наприклад, добровільне маркування систем ШІ слугує одним із інструментів мінімізації ризиків правам людини у Білій книзі з регулювання ШІ в Україні. Крім того, для підвищення прозорості у сферах маркетингу, Мінцифри рекомендує маркувати ШІ-контент та інформувати користувачів про використання ШІ в рекламі. Детальніше про це йдеться у розділі 4.3.2. цього Звіту.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами на рівні ООН, в українське законодавство варто:

- імплементувати концепцію "права на зображення", уточнивши гарантії захисту особи від неправомірного втручання у її право на приватність;
- запровадити національні правила/вимоги щодо маркування контенту, згенерованого системами ШІ.

3.2.3. Гарантування анонімності та безпеки онлайн

Закон України «Про захист персональних даних» містить загальні норми щодо безпеки та анонімності, які поширюються і на обробку персональних даних онлайн. Зокрема, стаття 6 визначає, що обробка персональних даних здійснюється за згодою особи для законних цілей. У той же час цей закон не містить деталізації щодо безпеки та анонімності, а лише надає загальні гарантії захисту персональних даних, чого недостатньо для відповідності міжнародним стандартам. Загальні положення містять

і Закон України «Про рекламу» - заборона розповсюджувати рекламу у формі спаму без попередньої згоди споживача – і Закон України «Про інформацію» - заборона збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом. Але вони все ще не відображають особливості гарантування безпеки й анонімності в онлайн просторі.

Закони України «Про електронну комерцію» і «Про електронні комунікації» встановлюють зобов'язання із захисту персональних даних на суб'єктів електронної комерції та постачальників мереж або послуг електронних комунікацій відповідно, але не містять конкретних зобов'язань чи алгоритмів дій для захисту персональних даних. В цьому питанні, ситуацію частково виправляє Законопроєкт № 8153, який деталізує зобов'язання щодо заходів захисту відповідних до рівню ризиків, зокрема щоб доступ до персональних даних мали лише особи, які мають на це дозвіл, в передбачених законом цілях, захист персональних даних від знищення, втрати або зміни, неправомірного зберігання, обробки, доступу або оприлюднення, та впровадження заходів дотримання безпеки обробки персональних даних. Також законопроєкт пропонує повідомляти споживачів про ризик для безпеки електронних комунікаційних мереж або послуг та містить окрему статтю щодо охорони таємниці приватного спілкування. Ще одним позитивним елементом є пряма заборона втручання у приватне спілкування у формі прослуховування, записування, зберігання та передачі інформації, без згоди учасників спілкування. Проте запропонована стаття 119-4 до ЗУ «Про електронні комунікації» фактично надає абоненту право подати запит щодо відстеження викликів, які він вважає зловмисними чи небажаними, при цьому немає ніяких гарантій чи вимог для такого запиту. Також Законопроєкт не уточнює, чи постачальник електронних комунікаційних мереж чи послуг зобов'язаний реагувати на кожне звернення чи це залишається його дискрецією – нечіткість, що відкриває можливості для зловживань.

У той же час Законопроєкт № 8153 пропонує надати постачальнику електронних комунікаційних мереж або послуг можливість отримувати, використовувати та передавати іншим інформацію про приватне спілкування, якщо це необхідно для надання електронних комунікаційних послуг (попередньо повідомивши про це споживача). Тим не менше, тут відсутнє регулювання захисту наскрізного шифрування чи інших засобів забезпечення анонімності та безпеки персональних даних користувачів, як це вимагається міжнародними стандартами. Це, у свою чергу, відкриває можливості для обходу заходів безпеки онлайн, включаючи «backdoors» чи надання ключів шифрування. Наприклад, державний портал «Дія», який використовується великою кількістю українців та містить їхню конфіденційну інформацію, не повністю відповідає стандартам захисту персональних даних і містить ризик передання інформації третім особам.

Окремий аспект захисту персональних даних – збирання і використання інформації правозахисними органами. Закон України «Про національну поліцію» визначає, що поліція має доступ до інформаційних ресурсів інших органів влади із обов'язковим дотриманням Закону України «Про захист персональних даних». Як вже було зазначено вище, цей закон не містить конкретизованих норм щодо онлайн-сфери, що, фактично, означає відсутність регулювання доступу поліції до персональних даних онлайн. У той же час стаття 159 Кримінального процесуального кодексу надає слідчим та прокурорам можливість тимчасового доступу до інформації в електронних інформаційних системах, та її копіювання «у разі необхідності». Також вони можуть здійснити пошук, виявлення та фіксацію комп'ютерних даних без дозволу на проведення обшуку, якщо «є достатні підстави вважати», що ця інформація «має значення для встановлення обставин у кримінальному провадженні» (стаття 236). Таким чином, правоохоронні та слідчі органи мають дуже широку дискрецію у сфері

доступу та використання персональних даних онлайн без конкретизації обсягу повноважень та способу їхнього застосування, як це вимагається практикою ЄСПЛ.

Законодавство України наразі не містить заборон псевдонімізації чи анонімності онлайн, але так само відсутнє і їхнє гарантування. У той же час, Законопроєкт №9223 фактично пропонує заборонити використання анонімних або псевдонімізованих облікових записів для поширення недостовірної інформації чи втручання в діяльність державних органів влади та інших осіб на шкоду суверенітету. Також Законопроєкт №11115, хоч і не містить прямого зобов'язання розкривати персональні дані володільців облікових записів (тільки дані провайдера про себе, володільців платформи), має положення щодо впровадження механізму оцінки та направлення володільцям сторінок звернень користувачів щодо розміщеної інформації і оскарження дій володільців, але не деталізує, які саме механізми маються на увазі і чи не розкриваються при цьому персональні дані володільця користувачу.

Міжнародні стандарти також вимагають існування окремого органу щодо кібербезпеки та нагляду за безпекою та анонімністю онлайн. Наразі Закон України «Про основні засади забезпечення кібербезпеки України» визначає, що контроль за дотриманням захисту персональних даних здійснюється Уповноваженим Верховної Ради з прав людини, але він діє у всіх сферах, не обмежуючись лише онлайн безпекою та анонімністю, тобто його не можна вважати спеціалізованим органом. Законопроєкт № 6177 пропонує створення Національної комісії з питань захисту персональних даних та доступу до публічної інформації, одним із завдань якої буде реалізація державної політики у сфері кібербезпеки в частині захисту персональних даних, у тому числі шляхом співпраці з суб'єктами кібербезпеки при запобіганні кіберінциденту. Тобто, загалом такі повноваження відповідають міжнародним вимогам, але необхідна подальша деталізація в частині повноважень цього органу у сфері захисту персональних даних онлайн.

Так само держава має запровадити ефективні засоби захисту у сфері безпеки та анонімності онлайн. Наразі Кримінальний кодекс встановлює відповідальність за порушення таємниці листування через комп'ютер (стаття 163), несанкціоноване втручання в роботу електронних комунікаційних систем і мереж (стаття 361), несанкціоновані дії з інформацією, яка зберігається на них, особою, що має доступ до неї (стаття 362). КУпАП передбачає штраф за недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних (стаття 188-39).

Як вже зазначалося, Омбудсман контролює захист персональних даних, через Департамент у сфері захисту персональних даних Секретаріату Омбудсмана. Відповідно до Закону «Про захист персональних даних», особи можуть звертатися до нього зі скаргами на неправомірну обробку своїх персональних даних, Омбудсман також може за власною ініціативою проводити перевірки дотримання законодавства у цій сфері. Уповноважений є скоріше медіатором, проте до його повноважень за Законом належать видавати обов'язкові вимоги щодо усунення порушень, складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду. Те саме стосується і департаменту кіберполіції: відповідно до Закону «Про національну поліцію» – особа має змогу написати скаргу до кіберполіції, але притягати до відповідальності і накладати санкції за порушення законодавства у сфері захисту персональних даних онлайн буде суд.

Також існує Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового

зв'язку (НКЕК), яка має повноваження розгляду справ щодо порушення законодавства у сфері електронних комунікацій (включаючи захист персональних даних в електронних комунікаційних мережах, як це передбачено Законом «Про електронні комунікації»). Проте наразі діяльність Комісії сфокусована на переоформленні ліцензій та інших питаннях радіочастотного спектра чи поштового зв'язку, а практика захисту персональних даних в електронних комунікаційних мережах відсутня. Цей орган має дуже широку сферу діяльності і не може здійснювати ефективний захист персональних даних онлайн.

Для гармонізації українського законодавства зі стандартами ЄС та Ради Європи варто:

- деталізувати законодавство із захисту персональних даних щодо гарантування безпеки та анонімності онлайн, включаючи внесення конкретизованих зобов'язань постачальників мереж чи послуг щодо захисту персональних даних користувачів у Закон «Про електронні комунікації».
- доповнити законодавство положеннями, які б регулювали захист використання засобів шифрування, анонімізації та псевдонімізації;
- включити в законодавство заборону «backdoors» та інших засобів для послаблення чи обходу заходів безпеки або використання їхніх існуючих недоліків;
- внести до кримінального процесуального та профільного правоохоронного законодавства конкретизовані норми щодо механізмів, обсягу повноважень та випадків доступу прокурорів, слідчих та поліції до персональних даних онлайн таким чином, щоб обмеження відповідали міжнародним стандартам визначеності, прозорості та ефективного зовнішнього нагляду;
- створити профільний орган відповідальний за управління ризиками у сфері кібербезпеки та профільний орган нагляду за дотриманням принципів щодо безпеки та анонімності онлайн

3.2.4. Протидія кібербулінгу, порнопомсті, гендерно зумовленому насильству

Онлайн-цькування (кібербулінг). Кримінальний кодекс України не містить жодних спеціальних положень, пов'язаних з кібербулінгом чи кібернасиллям, що ускладнює ефективне розслідування таких справ та притягнення винуватих до відповідальності. Водночас, Кодекс України про адміністративні правопорушення (КУпАП) у статті 173-4 встановлює відповідальність за булінг учасника освітнього процесу, у тому числі за кібербулінг - психологічне, фізичне, економічне, сексуальне насильство із застосуванням засобів електронних комунікацій, внаслідок якого могла бути чи була заподіяна шкода психічному або фізичному здоров'ю потерпілого. Склад правопорушення обмежений лише неповнолітніми особами та освітнім процесом. У окремих випадках до відповідальності притягують батьків «булерів» на підставі статті 184 КУпАП через невиконання обов'язків щодо виховання дітей. Інша норма - стаття 173-5 КУпАП - стосується цькування на робочому місці. На відміну від булінгу учасників освітнього процесу, склад цього правопорушення не охоплює онлайн-простір напряму. Тож тлумачення залишається за українськими судами, які часто напрацьовують досить неоднорідну практику.

Власне, за словами адвокатів, судовий захист на сьогодні не є ефективним, адже об'єктивно тяжкі наслідки, до яких призводить кібербулінг дітей майже ніколи не тягне за собою кримінальної відповідальності. Максимальні адміністративні санкції 1700-3400 гривень адміністративного штрафу. Дослідження DocuDays 2020 року (поки

що єдине в Україні на цю тему) вказує на те, що незважаючи на кількість складених протоколів, через невдалі законодавчі формулювання (зокрема, термін "електронні комунікації") притягнення до відповідальності є складним процесом. Проблема часто полягає і в тому, що постраждалі не знають, до кого звернутися у випадку кібербулінгу. Профільні юридичні видання публікують гарячі лінії Національної поліції та служб підтримки, проте ця інформація не є загально відомою і часто оминається в матеріалах медіа на цю тему. Іншою проблемою, про яку згадують правозахисники, є відсутність законодавства про кібернасильство, а отже, - неможливість зібрати і належно оформити докази для органів правопорядку, довести вину конкретної особи (особливо, з огляду на анонімність в мережі). Тож навіть за наявності декількох профільних статей КУпАП, їх застосування є надзвичайно складним з практичної точки зору.

Окреме регулювання пропонує стаття 42 Закону України «Про медіа», яка забороняє поширювати інформацію, що зосереджує надмірну увагу на насильстві, сприяє самокаліцтву чи суїцидальним думкам у дітей, пропагує нецензурні висловлювання та жести. Більш детальні критерії того, який контент підпадатиме під ці заборони, мають розробити органи спільного регулювання в рамках кодексів створення і поширення інформації. Такий орган у сфері онлайн-медіа вже створено і невдовзі він почне роботу над напрацюванням кодексів. Цей підхід цілком відповідає Директиві про аудіовізуальні медіапослуги, гармонізацію з якою Україна мала здійснити в рамках євроінтеграційних процесів.

Поширення інтимних зображень без згоди ("порнопомста"). Чинний Закон України "Про захист персональних даних" не містить жодних додаткових регулювань, окрім загальної заборони поширення персональних даних особи без наявності правових підстав. Законопроєкт №8153, яким планують замінити чинну редакцію закону, теж не має додаткових уточнень з цього приводу. Єдиним корисним інструментом, який пропонує законопроєкт є впровадження права на забуття, що потенційно уможливить швидке видалення інтимних зображень чи відео з мережі чи з пошукових систем.

Більш спеціальні норми містяться у Кримінальному кодексі України (ККУ). Так, чинне кримінальне законодавство містить дві норми, які захищають приватність особи: статтю 163 ("Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер") та статтю 182 ("Порушення недоторканності приватного життя"). Обидві в теорії можуть поширюватися на випадки поширення інтимних зображень без згоди особи. На практиці, українські суди застосували статтю 163 ККУ до ситуації, в якій засуджена вирвала з рук мобільний телефон потерпілої для того, аби ознайомитися з її СМС-листуванням з чоловіком засудженої. Справ щодо порнопомсти та публікації змісту переписок на платформах спільного доступу до інформації, втім, поки що немає. Але потенційно, в ситуаціях публікації відповідного листування, можливою є кваліфікація діяння за статтею 163 ККУ. Стаття 182 ККУ забороняє незаконне зберігання та поширення конфіденційної інформації про особу. Максимальною санкцією є обмеження волі на строк до трьох років, а за наявності обтяжуючих обставин – позбавлення волі на строк до п'яти років (при повторності вчинення злочину або ж завданні істотної шкоди). Закон України "Про інформацію", а також Закони України «Про доступ до публічної інформації» та «Про захист персональних даних» визнають фото і відео особи конфіденційною інформацією, що може поширюватися без згоди особи лише у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини.

А от на практиці, найчастіше притягають до відповідальності не за поширення інтимних зображень без згоди особи, а за поширення порнографії. З одного боку, санкція статті 301 ККУ є вищою за згадані статті, а отже, краще може виконувати

превентивну функцію. Офіс ефективного регулювання (BRDO) в рамках проєкту «Порнобарометр» з'ясував, що за 9 місяців 2024 року до судів надійшло 1104 обвинувальних акти у справах щодо порнографії (стаття 301 ККУ), що на 75% більше, ніж у попередньому році. Вироки були винесені лише у 7% випадків. З іншого боку, на практиці справи часто завершуються накладенням штрафу, найчастіше - досить незначного. До того ж, неправильна кваліфікація злочинів сприяє тому, що оцінка завданої шкоди здійснюється хибно, адже не враховується індивідуальний ефект таких дій для потерпілих осіб. Потенційно ситуацію може змінити декриміналізація порнографії в Україні. Така ініціатива вже обговорювалася у 2023 році, а цьогоріч знову зареєстрували пропозицію нормативно-правового акту. Так, Законопроєкт 12191 пропонує скасувати кримінальну відповідальність за зйомку і поширення відео інтимного характеру між дорослими особами, водночас залишивши її за: порнографію без згоди (порнопомста, порнофейки); екстремальну порнографію (насилля, зоофілія тощо); дитячу порнографію. Такі зміни в цілому відповідають європейським підходам і стандартам. Водночас, все ще бракує повноцінного регулювання платформ спільного доступу до інформації, адже все більше такого контенту поширюється на майданчиках, чиї умови користування і модераційні політики не відповідають міжнародним стандартам.

Гендерно зумовлене насильство онлайн. Україна ратифікувала Стамбульську конвенцію лише влітку 2022 року, а свій перший звіт з базовою оцінкою законодавства на предмет відповідності конвенції держава надала у 2023 році. Урядовці, які готували звіт, відзначили лише кілька загальних норм КУпАП та ККУ, що стосуються кібернасильства. Так, стаття 173-2 КУпАП охоплює такі діяння як образи, погрози та переслідування за ознакою статі, внаслідок яких могла бути чи була завдана шкода фізичному або психічному здоров'ю. Максимальна санкція за вчинення такого правопорушення складає адміністративний арешт на строк до 10 діб, а у разі вчинення повторно протягом року – до 15 діб. Втім, ця норма прямо нічого не говорить про онлайн-вимір насильства і навряд буде застосовуватися таким чином. Так само не говорять про нього і вже згадані статті 163 та 182 ККУ. Втім, практика за статтею 182 вказує на можливість притягнути порушника до відповідальності за певні форми кібернасильства, зокрема порнопомсту та кіберфлешинг, а також сталкінг. Такі дії якраз і передбачені Директивою про подолання насилля щодо жінок і домашнього насилля як основні приклади гендерно зумовленого насилля онлайн. Іншою нормою, яка може захистити від онлайн-насильства є стаття 126-1 ККУ, що забороняє вчинення домашнього насильства, а отже, теоретично мала б застосовуватися і до погроз та психологічного насилля, яке переходить у онлайн-формат. Проте говорити про успішний системний підхід складно, адже на думку правозахисників кіберполіція часто не має достатньо ресурсів та залученості у цій сфері, віддаючи пріоритет іншим галузям (як-от поширення діпфейків, що підривають національну безпеку). І хоча оновлений Закон України "Про запобігання і протидію домашньому насильству" містить інструменти для повідомлення, в тому числі, про гендерно зумовлене насильство онлайн, брак ресурсів у наглядових і виконавчих органів фактично зводить законодавчий порив нанівець.

Окремі категорії контенту, що становить гендерно зумовлене насильство, заборонені до публікації в медіа, а за порушення заборони медіа нестимуть відповідальність в рамках санкційних процедур за рішеннями Національної ради України з питань телебачення і радіомовлення. Стаття 36 Закону України «Про медіа» забороняє розповсюджувати висловлювання, що (1) розпалюють ненависть, ворожнечу чи жорстокість або ж (2) підбурюють до дискримінації чи утисків стосовно окремих осіб за ознакою статі, сексуальної орієнтації або ґендерної ідентичності. Більш детальні

критерії того, який контент підпадатиме під цю заборону, мають розробити органи спільного регулювання в рамках кодексів створення та поширення інформації.

Інших механізмів щодо видалення контенту, який становить гендерно зумовлене насильство, в Україні немає, як і консолідованого законодавства щодо регулювання контенту в Інтернеті, навіть попри заявлений у 2021 році в Стратегії інформаційної безпеки пріоритет цього напрямку державної політики. Відсутнє і регулювання діяльності онлайн-платформ, хоча законодавство-аналог згаданого Акту про цифрові послуги, нині готується Міністерством цифрової трансформації. На практичному рівні, Міністерство також робило низку кроків для захисту дітей від шкідливого контенту і онлайн-насильства, але ці ініціативи не мали профільного гендерного спрямування та поки що не були втілені в життя. Тож значну частину вимог до технічних платформ держава має зробити частиною загальної регуляторної рамки.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи у сфері протидії кібербулінгу, порнопомсті та гендерно зумовленому насильству, державі варто:

- вдосконалити законодавчі норми щодо кримінальної та адміністративної відповідальності за кібербулінг та кібернасильство;
- сприяти розробці кодексів спільного регулювання у сфері медіа із врахуванням питань протидії кібербулінгу, порнопості та гендерно зумовленому насильству онлайн;
- впровадити концепцію права на забуття з можливістю її застосування до випадків кібербулінгу, порнопости та гендерно зумовленого насильства онлайн;
- в рамках регулювання платформ спільного доступу до інформації забезпечити включення питань кібербулінгу, порнопости та гендерно зумовленого насильства до переліку контенту, що має видалятися системами оцінки контенту та на запит користувача, а також який не має інституційно толеруватися платформами (на рівні політик та дизайну систем управління контентом);
- створити законодавчі механізми обмеження доступу до контенту, що містить кібербулінг, порнопосту та гендерно зумовлене насильство, за рішенням суду чи незалежного регулятора, що враховуватимуть гарантії належного процесу і ролі Інтернет-посередників щодо розміщення такого контенту;
- проводити тренінги для державних службовців щодо виявлення та належного реагування на випадки кібербулінгу, порнопости та гендерно зумовленого насильства онлайн для створення адекватної системи моніторингу у цих сферах;
- збільшити ресурси департаментів органів правопорядку, що відповідають за реєстрацію та розслідування порушень у сфері кібербулінгу, порнопости та гендерно зумовленого насильства онлайн, проводити навчання щодо особливостей розслідування таких порушень та спілкування з потерпілими, залучати до співпраці профільні громадські організації;
- розробити адекватну комунікаційну стратегію для поширення обізнаності про гарячі лінії з підтримки постраждалих від кібербулінгу, порнопости та гендерно зумовленого насильства, а також правової допомоги таким особам;
- впровадити систему підтримки та реабілітації постраждалих від таких порушень.

3.3. Стеження

3.3.1. Встановлення та дотримання гарантій прав людини під час застосування заходів стеження

Україна активно залучена до використання технологій стеження (часто оснащених технологіями ШІ), проте все ще не має уніфікованої правової бази у цій сфері. Наразі посилання на використання таких технологій міститься в окремих спеціальних законах, які окреслюють дискрецію уповноважених органів у сфері правопорядку. При цьому загальні гарантії суб'єктів даних, над якими можливе стеження, обмежуються вимогами Закону України "Про захист персональних даних".

В Україні заходи стеження обумовлюються здебільшого захистом національної безпеки та дотриманням правопорядку - тому на використання таких технологій уповноважені відповідні суб'єкти. Закон України "Про Національну поліцію" дозволяє поліції використовувати "фото - і відеотехніку, у тому числі техніку, що працює в автоматичному режимі", а також "спеціалізоване програмне забезпечення для здійснення аналітичної обробки фото - та відеоінформації" (пп. 1, 5 ч. 1 статті 40). У цьому випадку на правоохоронні органи не накладається жодних обмежень, окрім зобов'язання використовувати спостереження для чітко визначеної мети. Відповідно до Кримінального процесуального кодексу, слідчий або прокурор мають доступ до інформаційно-комунікаційних систем досудового розслідування, які містять дані, зібрані з технічних пристроїв, в тому числі з фото- або відеокамер стеження, які функціонують у публічних місцях (стаття 300). Крім того, кодекс уповноважує правоохоронні органи вдаватися до негласних розшукових дій (наприклад, аудіо- та відеоконтроль особи, арешт, огляд і виїмка кореспонденції), але лише у випадку підозри вчинення тяжких або особливо тяжких злочинів та якщо переслідувана мета не може бути досягнута за допомогою інших заходів (статті 260, 262). Згідно із Законом України "Про оперативно-розшукову діяльність", уповноважені органи мають право здійснювати відео- та аудіоконтроль за особою, знімати інформацію з електронно-комунікаційних мереж та здійснювати спостереження за особою, але виключно для досягнення легітимної цілі, вичерпний перелік яких передбачено у законі (пп. 9, 11 ч. 1 стаття 8). Аналогічно, за Законом України "Про контррозвідувальну діяльність", органи та підрозділи СБУ уповноважені здійснювати спостереження за особою, але лише в цілях національної безпеки (п. 2 ч. 2 стаття 7).

Регулювання на сьогодні є фрагментарним та складається з розмитих формулювань, що у свою чергу піднімає ряд проблем. Однією з них є надмірний обсяг дискреції: хоча закони деталізують функції правоохоронних органів, вони не містять жодних індикаторів щодо обмеження їх повноважень в певних випадках та чітких підстав, за яких вони можуть вдаватися до засобів стеження. Проблема надмірних повноважень є особливо вираженою, враховуючи відсутність ефективного контрольного механізму - українське законодавство наразі не встановлює окремого інституційно незалежного органу для ефективного дотримання законодавства у сфері стеження. Деякі із законів, як-от Закон України "Про оперативно-розшукову діяльність", дозволяють вдаватися до заходів стеження лише за наявності попереднього судового дозволу, який на практиці є частіше формальністю.

Нарешті, закон не містить мінімальних гарантій для суб'єктів даних, які піддаються стеженню. Повідомлення особи про здійснення над нею заходів стеження, здійснюється лише у контексті кримінальних розслідувань, виключаючи попередження про здійснення аудіо- або відео нагляду в інших випадках (наприклад, в публічних місцях). Втім, і тут особа позбавлена можливості оскаржити такі дії. Це зумовлено

також і відсутністю судового перегляду заходів на їх правомірність, не дивлячись на те, що першочергова авторизація надається саме судом.

Відсутність законодавчих запобіжників відображається і на законодавчих ініціативах, які реєструються в парламенті. Однією з таких ініціатив є Проєкт Закону №11228-1, який, шляхом внесення змін до Закону України "Про контррозвідувальну діяльність", уповноважує органи Служби безпеки України (СБУ) на здійснення нових функцій, а саме проведення спеціальних операцій у кіберпросторі. Проєкт наділяє СБУ повноваженнями щодо фактично необмеженого доступу до персональних даних, які містяться у державних базах даних, не передбачаючи ні гарантій для суб'єктів даних, ані запобіжників проти зловживань. Наразі проєкт очікує на друге читання Комітетом Верховної Ради України з питань правоохоронної діяльності.

Крім того, наслідки відсутності законодавчого регулювання у сфері стеження стали особливо помітними після скандалу щодо стеження за журналістами медіа Bihus.info – камери стеження було секретно встановлено у готельних номерах журналістів, а пізніше в мережі оприлюднили відео про нібито вживання журналістами заборонених речовин. Як з'ясувалося при подальшому розслідуванні, незаконне прослуховування медійників здійснювалося протягом року.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами на рівні ООН, варто:

- розробити уніфіковані правила щодо загального механізму використання засобів стеження на законодавчому рівні;
- доповнити статті Кримінального процесуального кодексу щодо негласних слідчих розшукових дій положеннями, які встановлюють легітимну мету та підстави для використання засобів стеження;
- внести відповідні зміни до профільних законів органів, уповноважених на стеження, передбачивши обсяг їх дискреції, основні завдання та функції, а також потенційні "червоні лінії" як запобіжники зловживанням;
- передбачити ряд прав та гарантій для суб'єктів даних, які стають об'єктом стеження, які включають обов'язкове повідомлення особи про здійснення стеження (після здійснених заходів, якщо стеження необхідне для запобігання злочину), роз'яснення суб'єкту даних його прав (включаючи право на інформацію про зібрані дані або доступ до його персональних даних), а також право особи на оскарження здійснених заходів стеження у судовому порядку;
- передбачити ефективний контрольний механізм у сфері масового стеження, створивши інституційно незалежний орган, який здійснюватиме моніторинг заходів стеження, починаючи від винесення судового дозволу і закінчуючи наглядом за обробкою та зберіганням отриманих даних.

3.3.2. Обмеження масового стеження

Як зазначалося в попередньому розділі, Україна не містить єдиної правової системи щодо регулювання механізму стеження. Незважаючи на це, держава часто вдається до використання засобів масового стеження для підтримання правопорядку на місцевому рівні. Починаючи з 2019 року, в рамках програми "Безпечне місто" в Києві було встановлено 4 тисячі відеокамер, а деякі з них — оснащено технологією розпізнавання обличчя. Система розпізнавання обличчя є біометричною технологією, яка ідентифікує або верифікує особу за її цифровим зображенням. На відміну від систем звичайного стеження, вищезгадані системи є більш інтрузивними та піддаються більш

жорстокому регулюванню з огляду на посилене втручання у приватність суб'єктів даних. Наразі в Україні вже функціонує приблизно 50 тисяч камер відеоспостереження, які можуть долучити до єдиної системи, створення якої планувалося з початку 2024 року. Примітно, що спроби впровадження регуляторних інструментів передбачали надання муніципальним органам повноважень щодо використання засобів стеження. Однак профільний Закон України "Про місцеве самоврядування в Україні" не містить жодних індикаторів щодо таких функцій, і відповідних змін також внесено не було. Жодних вимог у площині регулювання публічних закупівель – ні технічних вимог, ані обмежень на те, як оголошувати відповідні тендери – наразі також немає.

Наразі в Україні фактично самовільно використовуються системи масового стеження, які не обмежені рамками ні на законодавчому, ані на підзаконному рівнях. Мінімальні гарантії та функції уповноважених органів, встановлені відповідно законами "Про захист персональних даних" та "Про Національну поліцію" (де доречно), не є достатніми та ефективними для належного захисту приватності суб'єктів даних.

Втім, Україна продовжує впроваджувати ініціативи у сфері стеження, незважаючи не лише на відносно низький захист персональних даних, а й технічну несумісність використовуваних систем із європейськими стандартами. Так, у 2021 році було оголошено про створення та розвиток програмно-апаратного комплексу "Безпечна країна" – ініціативи, спрямованої, зокрема, на підвищення рівня громадської безпеки, забезпечення безпеки дорожнього руху та зменшення загрози вчинення терористичних актів. Пізніше в рамках цієї програми держава отримала обладнання і програмне забезпечення для створення відповідного комплексу на суму 197 мільйонів гривень. До обладнання входять системи розпізнавання облич, поведінкової аналітики, аналітики розслідувань, керування інформацією та безпекою – тобто прилади, якими були оснащені більшість відеокамер, встановлених в рамках вже відомої програми "Безпечне місто". Проте у 2023 році розслідування "Схем" продемонструвало, що тисячі відеокамер, які функціонували на українських вулицях, були обладнані російським програмним забезпеченням TRASSIR, що означало передачу фактично всіх зібраних даних серверам держави-агресора. Існуючий стан речей демонструє не лише серйозні технічні проблеми використовуваних систем, а й вкотре підкреслює необхідність термінової розробки чітких нормативних вимог для безпеки персональних даних з українських інформаційних систем.

Проєкт Закону №11031, спрямований на запровадження єдиної системи відеомоніторингу стану публічної безпеки є однією з формальних спроб врегулювати застосування засобів стеження. Розроблений з метою підтримання правопорядку, проєкт має на меті уніфікувати правила щодо використання механізму стеження, а також врегулювати єдину платформу відеоспостереження в Україні. Втім, у своїй першочерговій редакції проект вже суперечить ряду міжнародних стандартів та потребує перегляду з огляду на такі проблеми: посягання на приватність, надмірно широка дискреція державних і муніципальних органів, відсутність контролю за дотриманням законодавства, небезпека захоплення даних та технічні проблеми власне системи відеомоніторингу.

Крім того, вже відомий Проєкт Закону №8153 про захист персональних даних в окремій статті 10 передбачає механізм здійснення відеоспостереження. Згідно з проєктом, державне стеження у публічних місцях може здійснюватися виключно "з метою запобігання, виявлення або фіксування правопорушень та забезпечення громадської безпеки і порядку". При здійсненні стеження проєкт вимагає наявності обов'язкового попередження про такі заходи, а також обробки отриманих даних виключно в спосіб, сумісний з цілями, задля яких вони були першочергово зібрані. У цьому контексті у статті 8 проєкт також передбачає особливості обробки персональних

даних, пов'язаних з притягненням до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості. Втім, ця стаття є здебільшого формальною, без відображення ключових положень Європейської Директиви 2016/680: стаття не передбачає переліку злочинів, при підозрі або вчиненні яких органи можуть вдаватися до заходів стеження, а також не розрізняє між категоріями осіб, над якими здійснюється стеження (наприклад, обвинувачений, потерпілий тощо).

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- розробити законодавство щодо відеоспостереження, з урахуванням міжнародних стандартів прав людини та регулювання ЄС;
- розробити законодавче визначення "масового стеження", включаючи стеження з використанням інтрузивних засобів (як-от систем розпізнавання обличчя), врешклюванти технології розпізнавання обличчя, механізм їх роботи, вичерпний перелік підстав для їх використання, а також правила подальшої обробки біометричних даних;
- розмежувати звичайне спостереження та спостереження, кероване штучним інтелектом, системи "високого ризику" та "низького ризику" (за прикладом Акту ЄС про штучний інтелект), біометричне та небіометричне спостереження;
- розробити механізм обробки персональних даних у правоохоронних цілях за прикладом Директиви 2016/680;
- передбачити додаткові гарантії для суб'єкта даних якщо стеження відбувається із використанням інтрузивних технологій (наприклад, обмеження періоду зберігання біометричних даних або встановлення механізм видалення даних у випадку, якщо спостереження досягло своєї мети і дані більше не є релевантними).

3.3.3. Обмеження застосування шпигунського програмного забезпечення

Чинний Закон України "Про захист персональних даних" не містить конкретних вимог щодо можливості та умов використання заходів стеження. Також, як зазначалося раніше, в правовому полі існує проблема щодо ефективності наглядового органу та його можливості належним чином відстежувати діяльність безпекових органів та перевіряти наявність правових підстав для застосування шпигунського програмного забезпечення. Водночас, Закон України "Про Службу безпеки України" досить широко визначає повноваження СБУ у статті 24. Так, можливість "здійснювати контррозвідувальні заходи з метою попередження, виявлення, припинення і розкриття будь-яких форм розвідувально-підривної діяльності проти України" може передбачати в тому числі використання шкідливого і шпигунського програмного забезпечення. Контроль і нагляд за діяльністю СБУ здійснює Президент України (який має право видавати розпорядження та накази СБУ, а отже, - не може здійснювати незалежний нагляд). Закон України "Про контррозвідувальну діяльність" уповноважує відповідні органи на здійснення в тому числі і заходів стеження, втім їх порядок визначається Законом України "Про оперативно-розшукову діяльність" і вимагає ухвали слідчого судді у випадку, якщо йдеться про дуже інтрузивні інструменти, як-от відеостеження, перехоплення електронних комунікацій тощо.

Закон України "Про Національну поліцію" не має переліку конкретних заходів, проте містить відсилки на згаданий закон про оперативно-розшукову діяльність, а також ґрунтується на вимогах Кримінального процесуального кодексу України. Останній

містить ряд статей, які уможливлюють збір інформації, втім будь-який захід такого характеру має здійснюватися на підставі ухвали слідчого судді. Тобто вимоги щодо належного судового нагляду у випадку з діяльністю поліції виконані, на відміну від браку аналогічних застережень і гарантій у законодавстві щодо безпекових органів (СБУ, контррозвідувальних органів тощо).

Загальні зміни пропонується внести Законопроєктом №8153, що замінить закон про захист персональних даних та гармонізує національні стандарти з вимогами Загального регламенту про захист даних. Утім, оскільки сам Загальний регламент не має детального регулювання технологій стеження, законопроєкт на цю тему також залишається лаконічним. Так, у статті 17 вказується, що використання спеціального програмного забезпечення чи технологій стеження (контекстуально зрозуміло, що йдеться саме про шпигунське програмне забезпечення) забороняється за винятком випадків, коли суб'єкт надав згоду, таке відстеження необхідне для функціонування застосунків чи мобільних програм, обробка необхідна для захисту від шахрайства чи надання послуги суб'єкту даних. Очевидно, що у пропонованій статті 17 йдеться саме про приватну сферу. Водночас, жодних уточнень щодо таких заходів в контексті діяльності органів правопорядку законопроєкт наразі не містить, а отже, правових гарантій недостатньо. Аналогічно уточнень не містить і стаття 31-2, яка захищає таємницю приватного спілкування. Законопроєкт №6177 щодо створення Національної комісії з захисту персональних даних та доступу до публічної інформації серед повноважень наглядового органу передбачає можливість здійснювати нагляд за обробкою персональних даних іншими державними органами. Детальніше про це йдеться у розділі щодо ефективності та незалежності регулятора у сфері захисту персональних даних.

Крім того, тривалий час точаться дискусії довкола Законопроєкту №11228-1 щодо врегулювання питань протидії розвідувально-підривній діяльності спеціальних служб іноземних держав. Поміж іншого, він має на меті дозволити СБУ мати прямий і автоматизований доступ до систем та баз даних, які адмініструються державними та муніципальними органами. Проєкт закону значно розширює існуючу дискрецію органів безпеки без внесення змін до профільних законів, надаючи необмежений доступ до персональних даних навіть за відсутності легітимних підстав. Наразі законопроєкт очікує на друге читання, проте навіть чинна доопрацьована редакція потребує суттєвих правок. На додачу, цей законопроєкт неодноразово критикували громадські організації, основною причиною була саме надміру широка дискреція.

Українська практика щодо використання шкідливого програмного забезпечення та заходів стеження за останні декілька років не дуже масштабна. Оскільки в країні вже три роки триває повномасштабна війна, більшість зусиль спрямовані на протидію російській агресії. Серед ключових інструментів, спрямованих "всередину" країни можна виокремити ініціативи Бюро економічної безпеки щодо використання засобів моніторингу фінансових та економічних активностей, а також прогнозування ризиків в економічній сфері. Наразі з описів достеменно не відомо, чи планується в рамках таких проєктів будь-яке втручання у роботу пристроїв осіб (наприклад посадовців, що здійснюють розпорядження державними коштами). Втім, ризик надмірного втручання залишається, в той час як жодних законодавчих гарантій, в тому числі і для приватності осіб, щодо яких планують здійснювати такий моніторинг, наразі немає.

Значно різноманітнішою (і небезпечнішою для українців) є практика використання шкідливого програмного забезпечення та шпигунських програм росіянами. Лабораторія цифрової безпеки вже оприлюднювала декілька досліджень щодо російських атак: наприклад, щодо фішингових схем, які містили файли зі шкідливим програмним забезпеченням. У 2023 році Державна служба спеціального зв'язку

також повідомила про автоматичне виявлення близько 1,500,000 файлів зі шкідливим програмним забезпеченням. Серед них найбільш поширеними були SmokeLoader, Agent Tesla, Snake Keylogger, Remcos та Formbook. Також були неодноразові спроби імперсоналізації державних органів, зокрема і СБУ, для отримання доступу до пристроїв користувачів та завантаження шпигунського програмного забезпечення. Про масштабність атак, що містять шкідливе програмне забезпечення або шпигунські програми, говорять і міжнародні дослідники. При цьому, важливо усвідомлювати, що націлюють такі атаки не лише на державні органи чи підприємства, а і на приватних осіб: зокрема, українські медіа, журналістів, громадські організації та бізнес.

На додачу до посилення загальних законодавчих і практичних гарантій у сфері стеження, для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаціями ООН, варто:

- посилити національне законодавство у сфері стеження нормами, що забороняють використання шкідливого програмного забезпечення, яке має нецільове призначення і здатне невибірково збирати інформацію з пристроїв;
- встановити незалежний нагляд за використанням шкідливого і шпигунського програмного забезпечення безпековими органами;
- створити протоколи обробки і документування доказів, отриманих внаслідок використання програм стеження, врегулювати законодавчо статус таких доказів;
- розробляти програми підвищення цифрової безпеки, зокрема серед працівників державних органів, підприємств критичної інфраструктури для попередження російських атак, що містять шкідливе програмне забезпечення;
- розробити законодавчі та практичні механізми захисту викривачів, які повідомляють про зловживання;
- розробити законодавче регулювання у сфері технологій подвійного призначення, які в тому числі охоплюють заходи кіберстеження, а також розробити підзаконні нормативно-правові акти щодо авторизації розробників та дозвільної системи імпорту/експорту технологій.

3.4. Наглядовий орган та заходи захисту права на повагу до приватного життя

3.4.1. Незалежність та ефективність наглядового органу у сфері захисту персональних даних

Закон України «Про захист персональних даних» визначає, що контроль за додержанням законодавства про захист персональних даних у межах своїх повноважень здійснюють суди та Уповноважений Верховної Ради України з прав людини (далі - Уповноважений). Саме Уповноважений на сьогодні фактично виконує функції, що відповідають ролі наглядового органу відповідно до Загального регламенту про захист даних, хоч і частково та без дотримання усіх вимог до такого органу.

Оцінюючи стан чинного законодавства на відповідність гарантіям незалежності та ефективності наглядового органу у сфері персональних даних, як передбачено Загальним регламентом про захист даних, варто проаналізувати норми Закону України "Про Уповноваженого Верховної Ради України з прав людини" та Закону України "Про захист персональних даних".

Законом України "Про Уповноваженого Верховної Ради України з прав людини", зокрема, статтями 4-9 закріплені основні гарантії незалежності Уповноваженого. Так, визначено строк його повноважень та умови їх припинення, встановлено чіткі правила щодо конфлікту інтересів, несумісності з посадою Уповноваженого. Також варто зазначити про відокремленість інституту Уповноваженого від загальної системи органів держави та наявність лише необхідного контролю його діяльності (статті 4, 9, 18). Водночас, процедура призначення Уповноваженого повністю залежить від Верховної Ради України, кандидати подаються членами парламенту, а процедура голосування є таємною. Це не узгоджується з вимогами щодо незалежного призначення та звільнення наглядового органу відповідно до Загального регламенту про захист даних.

Власне, звільнення Уповноваженої з прав людини у 2022 році супроводжувалось значною критикою з боку правозахисників, через порушення передбачених законом гарантій та внесення змін до Закону України «Про правовий режим воєнного стану» (ч. 4 статті 12), що дозволяють Верховній Раді України звільняти посадових осіб, що призначаються парламентом, через висловлення їм недовіри. Таке питання розглядається на пленарному засіданні Верховної Ради України невідкладно та без урахування процедур, передбачених спеціальними законами, що визначають правовий статус відповідних посадових осіб.

Уповноважений ВРУ з прав людини має необхідні повноваження розглядати звернення з питань захисту персональних даних та приймати рішення за результатами їх розгляду, проводити необхідні перевірки, отримувати доступ до будь-якої інформації, яка необхідна для здійснення контролю за забезпеченням захисту персональних даних, видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом та ін. Водночас, закон не регулює процедурні аспекти розгляду скарг Уповноваженим та процесуальні права скаржників.

Окремою проблемою є заходи впливу, які може застосовувати уповноважений. Безпосередній вплив на правопорушників важливий для припинення та попередження порушень у майбутньому. Хоча санкції й не визначені як обов'язковий елемент наглядового органу в Конвенції 108+, проте Загальний регламент про захист даних виносить їх на один рівень із мінімальними необхідними повноваженнями для забезпечення ефективності наглядового органу. Нині ж у законі визначено, що можуть вживатися заходи для попередження чи усунення правопорушення (пункт 5 частини першої статті 23), але це жодним чином не передбачає накладення санкцій за порушення - наприклад, штрафи накладаються лише у судовому порядку.

На противагу чинному законодавству Законопроєкт №6177 пропонує створити новий наглядовий орган - Національну комісію з питань захисту персональних даних та доступу до публічної інформації (далі - Нацкомісія). У поєднанні із Законопроєктом №8153, який 20 листопада 2024 року було прийнято за основу Верховною Радою України, вони зможуть доповнити та покращити чинне законодавство.

У своєму висновку стосовно Законопроєкту №8153 (з урахуванням Законопроєкту №6177) Рада Європи в основному робить зауваження щодо нечіткості формулювання окремих положень законопроєкту. Із більш суттєвих рекомендацій це: для дотримання принципу правової визначеності та встановлення ефективних і належних санкцій, чітко виписати "інші заходи", що наглядовий орган може застосувати (чи може бути щось окрім штрафів) (частина 2 статті 58), статтю 59 доповнити конкретними факторами для накладення штрафів (характер, тяжкість і тривалість порушення

та його наслідки, дії, вжиті для виконання вимог закону, а також будь-які дії, спрямовані на запобігання негативним наслідкам, що виникли внаслідок порушення, або на зменшення їх впливу), строк давності для застосування відповідальності збільшити для забезпечення можливості ефективного втручання з боку наглядового органу (стаття 60,) пропонується передати санкційні повноваження наглядовому органу щодо порушень окремих положень Закону України «Про електронні комунікації», визначених пунктом 5.6 Перехідних та прикінцевих положень (зокрема щодо таємниці приватного спілкування), а також додатково переглянути законопроєкти №8153 та №6177 в сукупності й проаналізувати їх на відповідність Загальному регламенту про захист даних та Конвенції 108+.

Законопроєкт №6177 загалом імплементує підходи до незалежності та ефективності наглядового органу, як це перебачено Загальним регламентом про захист даних. Водночас, залишається питання щодо можливості гарантувати належне фінансове забезпечення для якісного виконання повноважень. Інше питання - актуальне для будь-яких нових регуляторних органів - статус Національної комісії. Європейські стандарти вимагають відокремленості наглядового органу у сфері персональних даних від інших державних органів. У Законопроєкті №6177 пропонується зробити Нацкомісію центральним органом виконавчої влади зі спеціальним статусом. Попри задекларовану незалежність порядок утворення Національної комісії та обрання її членів свідчать про вирішальний вплив Кабінету Міністрів України, а отже не забезпечують достатнього рівня «відокремленості» інституції. Правозахисники та експерти також відзначали низку інших проблем законопроєкту №6177, що в цілому вказує на потребу в його суттєвому доопрацюванні до ухвалення.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто:

- забезпечити процес ґрунтовного та інклюзивного перегляду та доопрацювання законопроєкту №6177 та законопроєкту №8153 задля створення та впровадження ефективної та незалежної системи нагляду за дотриманням законодавства у сфері захисту персональних даних;
- розмежувати функції Уповноваженого Верховної Ради України з прав людини та новоствореного органу у частині захисту права на повагу до приватного життя.

3.4.2. Ефективні засоби правового захисту

Чинний Закон України "Про захист персональних даних" містить декілька статей, що передбачають механізми оскарження дій володільця і розпорядника персональних даних. Стаття 18 уможливлює оскарження відмови у доступі до даних до Уповноваженого ВРУ з прав людини. Стаття 22 вказує, що загальний контроль за дотриманням Закону здійснює Уповноважений ВРУ з прав людини та суди, в той час як стаття 28 наголошує на тому, що порушники будуть нести відповідальність, встановлену законом. Водночас, чіткої процедури оскарження чи відповідальності Закон не передбачає. Наприклад, стаття 23 серед повноважень Уповноваженого ВРУ з прав людини перелічує можливість отримувати скарги щодо порушень, проводити перевірки та направляти протоколи про притягнення до адміністративної відповідальності до суду. Закон України "Про Уповноваженого Верховної Ради України з прав людини" не містить жодних додаткових обов'язків чи тлумачень того, яким чином розглядаються звернення. Водночас, цей Закон передбачає можливість оскаржити рішення чи бездіяльність Уповноваженого ВРУ з прав людини у судовий спосіб.

Стаття 182 Кримінального кодексу України передбачає відповідальність за незаконну обробку конфіденційної інформації про особу або незаконну зміну такої інформації, крім випадків, передбачених іншими статтями Кодексу, а також посилену відповідальність за такі дії, якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи або були вчинені повторно. Важливо відзначити, що ця стаття не оперує термінологією законодавства про захист персональних даних, послуговуючись більш всеохопним та розмитим терміном "конфіденційна інформація". На практиці, вже були інциденти щодо ймовірного порушення статті 182, а також звернення до Уповноваженого ВРУ з прав людини з відповідними скаргами. Втім, наразі бракує достатньої судової практики та роз'яснень Верховного Суду з приводу застосування статті 182 Кримінального кодексу України.

Стаття 188-39 Кодексу України про адміністративні правопорушення також містить перелік заборонених практик у сфері захисту персональних даних, вчинення яких призводить до накладення адміністративних штрафів. Серед складів правопорушень наразі виокремлюють:

- неповідомлення або несвоєчасне повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню, повідомлення неповних чи недостовірних відомостей;
- невиконання приписів Уповноваженого ВРУ з прав людини або визначених ним посадових осіб щодо запобігання або усунення порушень законодавства про захист персональних даних;
- недодержання порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта;
- повторні вчинення згаданих правопорушень (що тягне за собою відповідальність з вищою мірою покарання).

Правозастосовча практика в цих питаннях є неоднозначною. Наприклад, звернення до Уповноваженого ВРУ з прав людини щодо порушення статті 188-39 часто завершуються оскарженням бездіяльності офісу Уповноваженого та визнання строку розгляду скарг надмірним, а дій Уповноваженого ВРУ з прав людини - недостатніми. В інших справах, суди визнають порушення з боку органів місцевого самоврядування, проте накладають санкції у мінімальному розмірі (5100 гривень). Аналогічні штрафи суди застосовують і до приватних суб'єктів, які порушують законодавство та не виконують приписів Уповноваженого ВРУ з прав людини з вимогою усунути порушення. Тобто фактично, в багатьох випадках штраф є номінальним і не заважає бізнесу надалі здійснювати неправомірну діяльність у сфері персональних даних. У мотивувальній частині суди нечасто належним чином обґрунтовують розмір санкції, накладений на порушника, а уніфікованих критеріїв для визначення розміру санкції немає.

Зміни до законодавства пропонується внести Законопроєктом №8153, Розділ X якого передбачає механізм відповідальності за порушення у сфері захисту персональних даних. Стаття 58 прямо передбачає, що притягнення до адміністративної та кримінальної відповідальності не звільняє суб'єктів, чиї права порушені, від права на компенсацію моральної та матеріальної шкоди. Стаття 59 також свідчить про збільшення розміру санкцій за порушення у сфері захисту даних. Втім, мінімальні санкції все ще є занадто низьким: в той час як Загальний регламент про захист даних пропонує штрафи до 2% річного обороту, Законопроєкт №8153 послуговується лише штрафами від 0,05% до 0,1%. Для багатьох бізнесів ця сума буде зовсім незначною. В іншому, положення статті 59 також не передбачають факторів, які слід враховувати при накладенні адміністративних санкцій, що не відповідає статті 83 Загального регламенту про захист даних.

Законопроєкт №6177 пропонує врегулювати діяльність Національної комісії про захист персональних даних та доступ до публічної інформації - тобто створити наглядовий орган у цій сфері. Значною новелою, порівняно з чинною системою, є збільшення повноважень органу, який здійснює наглядові функції. Стаття 4(ч. 4), зокрема, передбачає повноваження щодо притягнення до відповідальності суб'єктів, що порушують Закон України "Про захист персональних даних". Стаття 22 передбачає, що будь-яка особа або об'єднання може направляти до Національної комісії звернення, на підставі яких орган має відкрити провадження. Результатом провадження може стати накладення Національною комісією штрафу на порушника. Стаття 40 уможливлює оскарження рішень наглядового органу у судовому порядку.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- внести зміни до статті 182 Кримінального кодексу України, уніфікувавши термінологію кримінальної норми з масивом законодавства у сфері захисту персональних даних і передбачивши належну санкцію за порушення правил обробки персональних даних, що призводить до тяжких наслідків для особи;
- уповноважити новий наглядовий орган у сфері захисту персональних даних накладати адміністративний штраф за порушення у сфері захисту персональних даних (з можливістю його подальшого оскарження в судовому порядку);
- встановити законодавчі вимоги щодо порядку визначення розміру санкції залежно від тяжкості порушення та супутніх факторів, що впливають на наслідки вчиненого правопорушення у відповідності зі статтею 83 Загального регламенту про захист даних;
- при реформуванні системи відповідальності за порушення законодавства про захист персональних даних враховувати необхідність запровадження механізмів моральної компенсації за шкоду, спричинену незаконною діяльністю.

3.5. Обмеження права на повагу до приватного життя під час воєнного стану

3.5.1. Захист персональних даних під час війни

24 лютого 2022 року Президент України підписав указ про введення воєнного стану в Україні. Згідно з указом, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи, серед яких, зокрема, таємниця листування та кореспонденції, право на особисте та сімейне життя. З моменту оголошення воєнний стан було неодноразово продовжено - згідно з останніми змінами, воєнний стан триватиме до 9 травня 2025 року.

У 2015 році, у зв'язку з окупацією Донецької та Луганської областей державою-агресором, Україна на міжнародній арені оголосила про відступ від окремих зобов'язань, визначених Міжнародним пактом про громадянські і політичні права та Конвенцією про захист прав людини і основоположних свобод. Після початку повномасштабного вторгнення 2022 року Україна повідомила про відступ від окремих зобов'язань, передбачених Конвенцією. Навесні 2024 року обсяг відступу було переглянуто та зменшено, що демонструє готовність України відновлювати власні зобов'язання та гарантувати громадянам права та свободи.

Згідно зі ст. 25 Закону України "Про захист персональних даних", обмеження прав може здійснюватися в інтересах національної безпеки, економічного добробуту або захисту

прав і свобод суб'єктів персональних даних чи інших осіб. Положення сформульоване у загальних термінах та не передбачає механізму обмеження прав у сфері захисту даних - це здійснюється окремими спеціальними законами. Закон України "Про правовий режим воєнного стану" прямо не адресує питання персональних даних, проте передбачає втручання у право на приватність та контроль за комунікаціями у контексті заходів правового режиму воєнного стану. Згідно зі статтею 8 закону, військове командування та уповноважені органи можуть проводити огляд речей, службових приміщень та житла громадян. Вони також можуть регулювати роботу постачальників електронних комунікаційних мереж та забороняти передачу інформації через комп'ютерні мережі. Аналогічні заходи передбачаються і у ст. 18 Закону України "Про правовий режим надзвичайного стану".

У свою чергу, механізм запровадження відповідних заходів під час воєнного стану встановлюється на підзаконному рівні - наразі це регулюється Розпорядженням КМУ від 24 лютого 2022 року. Розпорядження містить План дій, у якому деталізуються заходи, описані в спеціальному законі, встановлюється строк виконання таких заходів, а також призначаються органи, відповідальні або які можуть бути залученими до здійснення заходів.

Чинний механізм правового регулювання впровадження воєнного стану є дієвим та базується на законних підставах. Втім, на законодавчому рівні його реалізація призвела не лише до посилення втручання у приватність, а й до значного розширення повноважень державних органів через відповідні зміни, виправдані необхідністю захисту публічної та національної безпеки.

У березні 2022 року було внесено зміни до ст. 25 Закону України "Про Національну поліцію", згідно з якими поліція уповноважена керувати реєстром та базами даних, які містять дані про підозрюваних злочинців, обвинувачених, підсудних, осіб, які переховуються від правосуддя, тощо. Примітно, що така база даних також містить біометричні дані осіб (включаючи цифрове зображення обличчя людини), які поліція зобов'язана збирати у осіб. Крім того, було внесено зміни до статті 615 Кримінального процесуального кодексу, згідно з якими прокурор був уповноважений санкціонувати тимчасовий доступ до інформації, яка зберігається в особи або в базі персональних даних володільця даних. Такі дії можуть бути вчинені без авторизації слідчого судді. Того ж місяця до кодексу було внесено зміни, які мали вплив на приватність громадян. Зокрема, при здійсненні обшуку житла чи іншого володіння особи, закон уповноважив слідчого мати доступ до комп'ютерних систем чи мобільних терміналів та фіксувати їх дані навіть за відсутності дозволу на обшук таких систем за умови, що інформація на них може мати значення для кримінального провадження. Закон також розширив перелік слідчих розшукових дій, додавши нову статтю 245-1 щодо "зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису". У цьому випадку слідчий або прокурор отримують копії фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі. Оскільки стаття не обмежує масив інформації, який підлягає збору, презюмується, що правоохоронні органи можуть мати доступ і до біометричних даних. Наразі основною проблемою, яка об'єднує відповідні положення, є відсутність індикаторів між обмеженнями прав під час воєнного стану та мирного часу, а також вказівки, за якої норми щодо розширеної дискреції втрачатимуть силу при закінченні періоду воєнного стану.

У 2024 році були також запроваджені зміни до законів, пов'язаних із організацією проходження військової служби та військовим обліком, а саме: Закону України "Про військовий обов'язок і військову службу" та Закону України "Про мобілізаційну підготовку та мобілізацію". Оскільки чинні закони не оперували поняттями "персональні дані"

та “конфіденційні дані”, Парламент ухвалив нову законодавчу базу, яка регламентує збір та обробку персональних даних військовослужбовців та військовозобов’язаних осіб.

Відповідно до нововведень в Україні було створено державний реєстр “Оберіг”, робота над яким тривала з часів прийняття спеціального Закону України “Про Єдиний державний реєстр призовників, військовозобов’язаних та резервістів” у 2017 році. Згідно з законом, доступ до реєстру мають лише уповноважені структури, які гарантують захист даних від несанкціонованого доступу або зловживання. Внесені до реєстру персональні та службові дані є конфіденційною інформацією (ч. 2 ст. 6). Стаття 7 закону передбачає досить розширений перелік персональних даних, які включаються до реєстру, а ч. 3 статті 14 містить невичерпний перелік державних органів, які володіють відповідними даними та надають їх для актуалізації реєстру. У цьому випадку Головне науково-експертне управління Апарату ВРУ ще на стадії затвердження змін висловило занепокоєння, що персональні дані, зібрані від суб’єктів даних для законних цілей, будуть оброблятися іншими державними органами для реалізації інших цілей, що несумісні з першочерговою метою. А це, у свою чергу, призведе до обробки невизначеного обсягу даних для невизначених цілей, що суперечить ключовим принципам Загального регламенту про захист даних.

Пізніше в Україні запрацював застосунок “Резерв+” – електронний кабінет призовника, військовозобов’язаного чи резервіста, де громадяни, які перебувають на військовому обліку, добровільно можуть зареєструвати та оновити свої військово-облікові дані. Інформація з “Оберіг” автоматично підтягується до застосунку. Після встановлення додатку вимагається авторизація за допомогою BankID, підтвердження своїх персональних даних, а також задання паролю чи налаштування FaceID або відбитку пальця для входу. Користувачі критикують додаток за технічні збої: неможливість увійти, некоректно відображені чи не оновлені дані. Експерти висловлювали застереження щодо безпекової інфраструктури – наразі не оприлюднено жодної інформації щодо заходів безпеки та захисту застосунку.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- при розширенні повноважень органів у профільних законах передбачати чіткий індикатор щодо дії положення виключно на період воєнного стану;
- здійснювати регулярний перегляд заходів, запроваджених під час воєнного стану, на їх необхідність та пропорційність;
- підвищити прозорість у контексті доступу користувачів до їх військово-облікових даних шляхом надання інформації щодо розпорядників даних, обсягу та категорій персональних даних тощо.

3.5.2. Застосування технологій стеження під час війни

Залученість України до цифрових технологій демонструється використанням на воєнному полі передових інструментів, які включають, зокрема, системи стеження, оснащені технологіями ШІ.

З початком повномасштабного вторгнення Україна активно почала використовувати Clearview AI – американську систему розпізнавання обличчя. Система застосовувалася для пошуку зниклих, спростування неправдивих дописів у соцмережах, підвищення безпеки у пунктах пропуску (ідентифікація осіб на блокпостах), ідентифікації загиблих солдатів та виявлення російських шпигунів. Хоча Clearview дійсно продемонстрував

ефективність для пошуку та ідентифікації осіб, використання системи супроводжується численними порушеннями приватності та застосуванням інтрузивних технологій, які йдуть в розріз з європейськими стандартами. З огляду на це на компанію було подано декілька юридичних позовів та скарг регулюючим органам Франції, Австрії, Італії, Греції та Великобританії. Система Clearview критикувалася, зокрема, за нелегальний збір персональних даних, неправомірну обробку біометричних даних, а також відсутність прозорості технічних принципів щодо роботи системи.

Паралельно з Clearview в Україні також використовували FindClone – схожий за цільовим призначенням додаток, який розпізнає обличчя за допомогою зображень. До застосунку зверталися здебільшого для ідентифікації російських солдатів, оскільки система здійснює пошук не лише серед соціальних мереж (як-от Вконтакте, Facebook), але і загальнодоступних фотографій, які були випадково завантажені третіми особами. Примітно, що як Clearview, так і FindClone відносяться до систем високого ризику, використання яких є забороненим відповідно до Акту ЄС про штучний інтелект, що прямо суперечить європейським стандартам.

Суперечливим залишається питання і щодо функціонування єдиної системи відеостеження в контексті програми "Безпечне місто". Як відомо, тисячі встановлених відеокамер перебували на російському програмному забезпеченні TRASSIR, а отримані дані опинялися на серверах в Москві, які н3алежать компаніям, що мають зв'язки з ФСБ (див. Розділ 3.3.2.). Пізніше в Україні почали використовувати камери та програмне забезпечення китайського виробництва Hikvision та Dahua з додатковим наголосом, що "закрита мережа убезпечує від відправки інформації з пристроїв до серверів виробника". Втім, і таких заходів безпеки виявилося недостатньо: 2 січня 2024 року держава-агресор здійснила масовану атаку на Київ та область. Пізніше органи СБУ підтвердили, що російські спецслужби зламали відеокамери, які перебували на застарілому програмному забезпеченні та транслювали локації атакованої критичної інфраструктури. При цьому, згідно з даними СБУ, від початку повномасштабної війни було заблоковано понад 10 тисяч IP-камер, за допомогою яких держава-агресор могла коригувати свої ракетні атаки. З огляду на те, що тисячі інших відеокамер все ще знаходяться під загрозою кібератак держави-агресора, наразі проблему щодо українських відеокамер важко назвати вирішеною.

Вищезгадані практичні проблеми набувають особливого значення в сукупності з фактом відсутності законодавчого регулювання стеження в Україні: під час тривалої роботи інтрузивних технологій не було впроваджено жодних регуляторних положень, які передбачають механізм роботи відповідної системи, підстави для її використання, категорії органів, які мають доступ до системи та належні гарантії проти зловживань.

Втім, для зменшення ризиків приватності та несанкціонованого доступу до захищених даних, Україна почала брати активну участь у розробці локальних інструментів для захисту національної безпеки. Наприклад, Центр інновацій Міністерства оборони України розробив платформу ШІ Avengers, яка допомагає силам оборони (шляхом отримання відеоданих) щотижня автоматично виявляти 12 тисяч одиниць ворожої техніки. Крім того, з липня 2023 року в Україні запущено Кластер оборонних технологій Brave1, спрямований на підтримку розробників технологій ШІ у воєнній сфері. У контексті Кластеру було розроблено Mantis Analytics - ШІ-платформу, яка здійснює моніторинг та аналіз інформаційного простору, виявляє загрози (як-от маніпуляції або фейки) та реагує на них. Mantis в режимі реального часу обробляє тисячі повідомлень та гігабайти даних із медіа та соцмереж, розміщуючи інформацію на інтерактивній мапі: отримані дані у подальшому допомагають ефективніше боротися із російською пропагандою та дезінформацією.

Серед ключових проблем, з якими стикається Україна при використанні вищезгаданих технологій під час війни, варто виокремити неврегульованість відповідних систем на законодавчому рівні та відсутність стратегії виходу для використання таких технологій після скасування воєнного стану. Немає навіть підзаконних актів чи інструкцій щодо окремих інструментів. Така проблема пов'язана як зі стрімким розвитком цифрових технологій, які значно переганяють чинне законодавство, так і відсутністю європейських орієнтирів з огляду на те, що національна оборона не входить до обсягу регулювання основних документів ЄС. Відповідна сфера залишена на дискрецію окремих держав, що лише підкреслює потребу у належній законодавчій базі.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто:

- уточнити на підзаконному рівні види та обсяг додаткових заходів і технологій, дозволених до застосування виключно у воєнний час;
- уточнити на підзаконному рівні, до яких інтрузивних технологій (таких як автоматизовані системи прийняття рішень, системи, керовані ШІ) можуть вдаватися органи влади, вказавши, що такі цифрові інструменти можуть використовуватися таким чином лише у воєнний час;
- передбачити механізм співпраці між правоохоронними органами та Clearview AI (і подібними компаніями), перерахувавши цілі, для яких використовується система, функції, які має виконувати Clearview, та обмеження на її використання з урахуванням приватності суб'єктів даних;
- розробити законодавчі стратегії виходу щодо використання технологій стеження після скасування воєнного стану.

ВПЛИВ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Україна активно інвестує у створення сприятливого правового та технологічного середовища для розробки і запуску численних ШІ проєктів. Наразі вже створено регуляторну пісочницю для тестування ШІ-проєктів, що мають значну суспільну цінність, запущено AI Center of Excellence, розроблено Білу книгу з регулювання ШІ в Україні. Ці ініціативи є важливим першим кроком для виведення сфери ШІ у правову площину. На додачу, Мінцифри активно сприяє напрацюванню секторальних рекомендацій – документів м'якого права, які містять ключові стандарти щодо розробки і використання систем ШІ у різних галузях (медіа, реклама, освіта, захист інтелектуальної власності тощо).

Водночас, слід усвідомлювати, що повноцінне регулювання є неможливим без впровадження комплексного законодавства, яке визначає права і обов'язки суб'єктів у сфері ШІ – розробників та постачальників систем, користувачів, аудиторів тощо. Крім того, важливим є і створення (або розширення повноважень вже існуючого) контролюючого органу, що зможе незалежно, ефективно і фахово здійснювати нагляд за дотриманням законодавчих вимог у сфері ШІ.

Напрацювання такого законодавства є необхідним як з огляду на швидкий розвиток галузі в Україні, так і зважаючи на євроінтеграційні зусилля держави, адже одним із завдань у середньостроковій перспективі є напрацювати і запустити механізми, що є своєрідними аналогами Акту про штучний інтелект на рівні ЄС. Для своєчасного запуску таких процесів обговорення та пропозиції мають з'явитися вже незабаром.

4.1. Загальні засади

4.1.1. Загальні принципи регулювання у сфері ШІ

Регулювання ШІ в Україні почалося з прийняття Концепції розвитку штучного інтелекту в Україні - документу, що визначив пріоритетні галузі для розвитку новітніх технологій, втім фактично відтермінував правове регулювання цієї сфери на невизначений строк. Примітно, що Концепція з'явилася ще задовго до появи перших напрацювань Акту про штучний інтелект на рівні ЄС, а тому жодних стандартів тоді не розглядали і в Україні. Згодом, у 2023 році з'явилася Дорожня карта регулювання ШІ - напрацювання Міністерства цифрової трансформації України, які коротко і стисло виклали план щодо регулювання галузі до 2027 року. Згодом розширена версія такого плану була оприлюднена у Білій книзі з регулювання ШІ. Хоча цей документ пропонує алгоритм регулювання ШІ у форматі "bottom-up" (від «м'якого регулювання» до законодавчих стандартів), Біла книга не встановлює жодних жорстких вимог. Важливо, що вона пропонує орієнтуватися на Акт ЄС про штучний інтелект, який Україні доведеться інкорпорувати в рамках євроінтеграції.

Початком виконання плану, закладеного у Білу книгу, стали розвиток саморегулівних ініціатив та напрацювання рекомендацій щодо розробки і використання систем ШІ в різних сферах. Рівень саморегулювання наразі відзначився підписанням Декларації про саморегулювання у сфері ШІ, яка містить загальні орієнтири для компаній-підписанток. Серед них є і принцип прозорості, значну увагу якому приділяють у Акті про штучний інтелект. Крім того, Міністерство цифрової трансформації за участі багатьох різних стейкхолдерів почало активно напрацьовувати рекомендації

з відповідального використання ШІ в різних сферах (медіа, реклами та маркетингових комунікацій, захисту персональних даних, освіти, інтелектуальної власності). Також очікуються детальні рекомендації для розробників систем ШІ, які враховуватимуть численні положення Акту про штучний інтелект, зокрема і щодо певних обов'язків розробників залежно від рівня ризиковості системи. Для гармонізації термінології у сфері ШІ експерти також напрацювали Словник термінів у сфері ШІ, який поєднує і технічні, і юридичні дефініції та допомагає уніфікувати використання різних понять у нормотворчості і на практиці.

Крім того, Міністерство цифрової трансформації в середині грудня 2024 року представило візію розвитку ШІ в Україні. Серед цікавих ініціатив варто виокремити AI Center of Excellence - ідею щодо створення хабу для побудови партнерств, сприяння розробкам, а також консолідації усіх регуляторних та приватних ініціатив на одному ресурсі.

Розробити ефективне регулювання наразі є важливим з кількох причин: по-перше, Україна має намір ратифікувати Рамкову конвенцію про штучний інтелект, права людини, демократію, та верховенство права. Оскільки Рамкова конвенція передбачає механізми звітування щодо проведення оцінки ризиків та дотримання інших норм, Україна потребуватиме регуляторної рамки, яка визначатиме, що таке системи ШІ та хто зобов'язаний здійснювати оцінку ризиків. По-друге, наразі існує значна кількість систем ШІ, які застосовуються у публічному секторі, тож надзвичайно важливо забезпечити, щоб такі системи належним чином перевірялися. Для цього необхідним є базове регулювання систем ШІ, а також впровадження моделі ЄС щодо ризик-орієнтованого підходу. Інші стандарти, зокрема і вимога щодо прозорості, також є необхідними для того, щоб уможливити оцінку впроваджених у публічному секторі технологій ШІ незалежними експертами.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- напрацювати законодавство, що впроваджує ризик-орієнтований підхід до регулювання систем ШІ, а також встановити вимоги до суб'єктів, які взаємодіють з системами ШІ на різних етапах їх життєвого циклу;
- розробити базові вимоги щодо кібербезпеки високоризикових систем ШІ;
- розробити підзаконні нормативно-правові акти, що регулюватимуть питання стандартизації систем ШІ та процедури оцінки їх відповідності національному законодавству (процедура комплаєнсу).

4.1.2. Оцінка впливу на права людини та управління ризиками

Повноцінна імплементація у законодавство методології оцінки впливу ШІ на права людини стане можливою лише після прийняття комплексного регулювання. Впровадження відповідних систем оцінки, а також інших дотичних інструментів передбачене Білою книгою з регулювання ШІ (регуляторна пісочниця, методологія оцінки впливу ШІ на права людини, добровільні кодекси поведінки та загальні і секторальні рекомендації). Крім того, Міністерство цифрової трансформації України вже видало ряд рекомендацій щодо відповідального використання систем ШІ у сфері медіа, сфері реклами та маркетингових комунікацій, сфері захисту персональних даних, освітній сфері, сфері інтелектуальної власності, на основі яких можна провести базову оцінку відповідності стандартам у сфері прав людини.

В межах регуляторного процесу для України одним із важливих кроків є ратифікація Рамкової конвенції про штучний інтелект і права людини, демократію та верховенство права, яка кристалізує мінімальні стандарти у сфері відповідального використання ШІ - одним з ключових є саме оцінка впливу систем ШІ на права людини. Методологія HUDERIA, напрацьована як один з варіантів впровадження вимог Рамкової конвенції, може бути корисним інструментом для виконання таких зобов'язань, а також сприяти відповідальному та безпечному використанню систем ШІ в різних сферах. Оскільки на Україну очікує гармонізація національного законодавства з вимогами Акту ЄС про штучний інтелект, очевидно держава муситиме встановити жорсткіші вимоги і для приватного сектору. Отже, ратифікація Рамкової конвенції має включати поширення її дії і на приватний сектор, адже це допоможе українському бізнесу підготуватися до більш вимогливих стандартів ЄС та покращити якість технологій.

Оскільки Україна була однією з п'яти країн, які брали участь у тестуванні Методології HUDERIA - так званій, пілотній версії проєкту, український бізнес вже побіжно знайомий з механізмом оцінки впливу. Наприклад, юридична компанія Juscutum вже проводила вебінари щодо адаптування та правильно застосування Методології. Окрім того, з прийняттям Законопроєкту №8153 щодо захисту персональних даних, щонайменше одна складова оцінки впливу на права людини - оцінка впливу на захист даних - стане обов'язковою для всіх суб'єктів.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто доповнити національне законодавство:

- вимогами щодо проведення оцінки впливу на права людини для високоризикових систем ШІ перед їх впровадженням;
- вимогами щодо проведення оцінки ризиків протягом усього життєвого циклу високоризикових систем ШІ;
- підзаконними нормативно-правовими актами, що містять відповідні методології оцінки впливу на права людини та оцінки ризиків, які були розроблені із залученням до процесу всіх зацікавлених сторін, включно з громадянським суспільством та академічною спільнотою;
- формами звітності щодо імплементації таких методологій публічними та приватними суб'єктами.

4.1.3. Фаховий людський нагляд за системами ШІ

Наразі в Україні відсутнє регулювання систем ШІ і, як наслідок, немає вимог щодо фахового людського нагляду відносно усіх високоризикових систем. Водночас, в статті 8 (частина 13) Закону України "Про захист персональних даних" є вимога щодо впровадження захисту від автоматизованого прийняття рішень, що має для людини правові наслідки. На практиці, це передбачає обов'язок встановити альтернативні способи отримання послуг та забезпечити можливість перегляду рішень системи ШІ людиною. Рекомендації Міністерства цифрової трансформації України щодо відповідального використання систем ШІ у сфері медіа, сфері реклами та маркетингових комунікацій, сфері захисту персональних даних, освітній сфері, сфері інтелектуальної власності наголошують на необхідності встановлення фахового людського нагляду за діяльністю систем ШІ. Інструменти для впровадження людського нагляду також передбачені в рамках заходів Білої книги з регулювання ШІ (регуляторні пісочниці, впровадження наглядового органу тощо). Крім того, принцип людського нагляду згадується у Декларації про саморегулювання у сфері ШІ, підписаній представниками української ШІ-індустрії, що стане підґрунтям для подальшої розробки добровільних кодексів поведінки.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто доповнити національне законодавство:

- вимогами щодо встановлення людського нагляду за діяльністю високоризикових систем ШІ, формату такого нагляду;
- підзаконними нормативно-правовими актами щодо нагляду за високоризиковими системами ШІ, процедурою здійснення такого нагляду, типовими формами звітів та протоколів;
- підзаконними нормативно-правовими актами щодо нагляду за системами ШІ, які розробляються і впроваджуються у публічному секторі (державними органами, органами місцевого самоврядування, відповідними КП та ДП) з деталізованими вимогами до фахівців, які здійснюватимуть такий нагляд.

4.1.4. Кодекси практики та кодекси поведінки

Розробка кодексів практики - документів, що містять тлумачення законодавчих вимог та порядок їх застосування залежно від сфери чи типу систем ШІ, - стане можливою лише після впровадження комплексного регулювання у сфері ШІ. Розробка та підписання кодексів поведінки - документів, що передбачають додаткові зобов'язання, які беруть на себе провайдери систем ШІ поруч із законодавчими вимогами, - а також інших інструментів саморегулювання вже передбачена Білою книгою з регулювання ШІ. Першим кроком стало підписання Декларації про саморегулювання у сфері ШІ, до якої долучилися представники української ШІ-індустрії. Ця декларація є підґрунтям для подальшої розробки добровільних кодексів поведінки у різних сферах. Зокрема, у середині грудня 2024 року низка технологічних компаній підписала перший Кодекс поведінки, який закріплює основоположні принципи для роботи з системами ШІ. Цей документ підписали 14 компаній, втім він відкритий до підписання й іншими членами індустрії. Також кодекси поведінки можуть розроблятися в рамках механізмів співрегулювання, передбачених Законом України "Про медіа". Такі кодекси, в тому числі, стосуватимуться питань використання ШІ у медійній та рекламній сферах.

Для гармонізації українського законодавства з вимогами ЄС та Ради Європи, варто доповнити національне законодавство:

- положеннями щодо впровадження механізмів спів- та саморегулювання у сфері ШІ, а також тематик, які охоплюватимуть документи, розроблені в рамках таких механізмів;
- розробляти кодекси поведінки та кодекси практики із залученням всіх зацікавлених сторін, включно з громадянським суспільством та академічною спільнотою;
- вимогами щодо дотримання добровільно взятих на себе зобов'язань представниками індустрії, а також урахуванням (не)дотримання таких зобов'язань при накладанні санкцій за порушення у сфері ШІ.

4.1.5. Регуляторні пісочниці і тестування в умовах реального світу

У березні 2023 року Міністерство цифрової трансформації України оголосило про запуск першої регуляторної пісочниці. Регуляторна пісочниця має бути спрямована на тестування ШІ-проєктів, WEB-3, блокчейн або інших інноваційних продуктів, що дозволить вдосконалити бізнес-модель, зрозуміти, які регуляторні норми застосовні до продуктів, а також ефективніше залучати інвестиції. Згодом плани щодо

запуску регуляторної пісочниці підтвердили в Дорожній карті регулювання ШІ, а також у Білій книзі з регулювання ШІ. Остання пропонує перейняти формат регуляторної пісочниці з Акту про ШІ, що також спростить подальшу євроінтеграцію та адаптацію бізнесу до вимог ЄС. Зважаючи на обмежений ресурс, до участі у регуляторній пісочниці планується допускати систем ШІ, що мають середній та високий рівень впливу на права людини. Іншим критерієм для відбору планується визнати соціальну значущість проєктів. Привілеї планується зробити для середнього та малого бізнесу, а також стартапів - це цілком відповідає вимогам статті 58 Акту ЄС про ШІ. Наприкінці жовтня 2024 року український уряд ухвалив Постанову про регуляторну пісочницю, що визначає Порядок реалізації експериментального проєкту. Відповідно до короткого викладу документу, пісочниця працюватиме таким чином:

- через веб-портал Фонду розвитку інновацій компанія подає заявку на участь, надаючи дані про себе;
- заявку опрацьовує адміністратор;
- якщо компанія відповідає встановленим вимогам, заявник матиме можливість додати опис про сам продукт;
- експерти готують план дослідження продукту та погоджують його з компанією;
- після цього розпочинається процес роботи різних фахівців із цим продуктом.

Оскільки Акт про штучний інтелект залишає варіанти і формати імплементації вимог статей 57-58 на розсуд національних урядів, алгоритм роботи регуляторної пісочниці, запропонований Міністерством цифрової трансформації відповідає європейським вимогам. Водночас, принциповим буде питання щодо фінальної версії критеріїв для доступу до пісочниці, адже вони мають бути недискримінаційними.

Наразі, втім, ключовою проблемою є відсутність наглядового органу, який може здійснювати контроль за дотриманням правил, процедур і регламентів щодо діяльності в межах регуляторної пісочниці. Також варто пам'ятати, що статті 57 та 59 Акту ЄС про ШІ встановлюють спеціальний режим обробки персональних даних в межах регуляторних пісочниць. Таким чином, у випадку орієнтування на європейські стандарти, слід буде вносити зміни і до Закону України «Про захист персональних даних». Інакше, обробка персональних даних в рамках регуляторної пісочниці буде надзвичайно складною з юридичної точки зору - доведеться щоразу отримувати згоду особи або доводити наявність легітимного інтересу.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами на рівні ООН, варто доповнити національне законодавство, а саме:

- ввести в національне законодавство поняття регуляторної пісочниці;
- розробити регламенти, інструкції та інші підзаконні нормативно-правові акти, спрямовані на регулювання доступу до пісочниці (в тому числі гарантій рівного доступу), умов та вимог до участі, припинення участі, звітування та нагляду за діяльністю в межах регуляторної пісочниці;
- розробити інструментарій (методологію) для оцінки ризиків і відповідності національному законодавству в межах регуляторної пісочниці;
- впровадити вимоги до тестування систем ШІ в умовах реального світу, уповноважити наглядовий орган здійснювати контроль такої діяльності.

4.2. Інституції в сфері ШІ

4.2.1. Нотифікуючий орган

Наразі в Україні відсутнє регулювання систем ШІ і, як наслідок, немає вимог щодо призначення окремих нотифікуючих органів. Хоч створення регуляторного органу з питань ШІ передбачене в рамках заходів Білої книги з регулювання ШІ, воно стосується скоріше органів ринкового нагляду (описаних у пункті 5.2.2 цього документу), а не нотифікуючих органів, які відповідно до вимог Акту ЄС про штучний інтелект, мають відповідати за розробку та виконання процедур для оцінювання, призначення та повідомлення органів з оцінки відповідності та моніторингу їх діяльності. Останні є недержавними установами, які мають здійснювати оцінку відповідності стандартам у сфері ШІ, при цьому будучи незалежними від постачальників систем ШІ (по суті, своєрідний зовнішній незалежний аудит).

Оскільки сфера ШІ залишається відносно неврегульованою, окремих вимог до сертифікації органів з оцінки відповідності немає. Втім, такі повноваження найімовірніше буде покладено на Національне агентство з акредитації України, ключовим завданням якого і є посвідчення спроможності організацій та установ діяти відповідно до законодавства та здійснювати перевірки.

Водночас, оскільки діяльність Національного агентства з акредитації регулюється Положенням Міністерства економіки України, можуть виникнути питання щодо дотримання принципів незалежності та неупередженості при формуванні такого органу. Тож потенційні зміни мають стосуватися не лише розширення обсягу повноважень і охоплення сфери ШІ, а і порядку формування Національного агентства. Важливо, що такі повноваження не можуть покладатися на орган ринкового нагляду.

Для гармонізації українського законодавства з вимогами ЄС, варто доповнити національне законодавство:

- вимогами щодо розширення повноважень Національного агентства з акредитації України;
- змінами щодо порядку формування та гарантій незалежності Національного агентства з акредитації України;
- підзаконними нормативно-правовими актами щодо порядку здійснення акредитації органів, що здійснюють оцінку відповідності систем ШІ національному законодавству.

4.2.2. Нагляд за діяльністю ринку

Необхідність призначення окремого органу ринкового нагляду у сфері ШІ окреслена в рамках заходів Білої книги з регулювання ШІ, втім конкретних пропозицій щодо того, кому передавати повноваження чи яким чином варто створювати нового регулятора в документі висловлено не було.

В межах ЄС практика є досить неоднорідною, залежно від особливостей правової системи та вже наявних органів з тематично наближеними повноваженнями. Серед прикладів запровадження нових органів для дотримання вимог ЄС щодо систем ШІ, Ірландія призначила дев'ять комісій для контролю за відповідністю вимогам Акту ЄС про штучний інтелект. Кожна з комісій відповідає за окремий сектор вимог законодавства ЄС, такі як захист даних, медіа, права людини, довкілля, тощо. Призначення цих органів контролю стало прецедентом для національного

регулювання ШІ серед країн ЄС. На противагу, Франція запроваджує зміни в чинне законодавство з розширенням повноважень наявних органів контролю, що відповідають за конкретні сектори, для дотримання вимог ЄС у сфері регулювання систем ШІ. Тобто жодних нових регуляторів не створюється.

Наразі більшість координаційної та регуляторної роботи в Україні виконується на міністерському рівні. Наприклад, Постанова про регуляторну пісочницю, ухвалена у жовтні 2024 року, визначає Міністерство цифрової трансформації координатором експериментального проєкту. І якщо в питаннях тестових середовищ чи розробки загальнодержавних політик це питання може належати до повноважень Міністерства, то вирішення суперечливих ситуацій та спорів має здійснюватися за участі незалежного регулятора, а не центральних органів виконавчої влади. Оскільки в Україні розгортається значна кількість ШІ-проєктів, створення органу ринкового нагляду або наділення існуючих регуляторів такими повноваженнями стає все актуальнішим питанням.

Створення нового органу потребує значних фінансових та адміністративних ресурсів, для України наразі це може стати складнішою опцією. Водночас, євроінтеграційні процеси вимагають трансформації системи державних органів не лише в сфері ШІ. Йдеться і про призначення координатора з цифрових послуг в рамках імплементації Акту про цифрові послуги, і про створення Національної комісії з питань захисту персональних даних.

Одним із варіантів може стати і розширення повноваження Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (НКЕК), яка має технічну експертизу та опікується сферою електронних комунікацій. Недоліком цього варіанту є те, що НКЕК менш заточена під захист прав людини, який є фокусом діяльності органу ринкового нагляду відповідно до Акту ЄС про штучний інтелект. На противагу, Національна рада з питань телебачення та радіомовлення, повноваження якої були розширені Законом України "Про медіа", вже займається питаннями онлайн-технологій та платформ, а також на практиці стикається з питаннями регулювання ШІ в рамках своєї роботи у сфері свободи вираження. Водночас, цей регулятор наразі і так має значне навантаження. Оскільки змінити це до кінця дії воєнного стану неможливо, покладати ще одну, абсолютно іншу сферу на нього теж є суперечливим питанням. На додачу, в Україні планується створити окремий контролюючий орган з питань захисту персональних даних та доступу до публічної інформації. Втім, тут питання полягає у фінальному варіанті повноважень такого органу і порядку його формування, адже чинна редакція законопроєкту є недосконалою, про що детальніше йдеться у пунктах 3.4.1 та 3.4.2 цього звіту. Отже, ідеальних варіантів немає і при виборі органу, на який варто покладати додаткові повноваження щодо нагляду за сферою ШІ, варто буде зважувати усі переваги та ризики.

Зрештою, спеціалізовані повноваження можуть бути покладені на профільні органи. Наприклад, нагляд за ринковою конкуренцією у сфері ШІ природно може стати частиною повноважень Антимонопольного комітету України (АМКУ). Відповідно, навіть за умови призначення окремого наглядового органу, що візьме на себе моніторинг дотримання спеціальних вимог у сфері ШІ, для уникнення дублювання повноважень все ще необхідно буде оновити секторальне законодавство і визначити відповідальні компетентні органи. При цьому, таке оновлення законодавства буде потрібним незалежно від того, чи буде створено нового регулятора, чи його повноваження перекладуть на один з уже існуючих органів.

Для гармонізації українського законодавства з вимогами ЄС, варто здійснити такі кроки:

- визначитися з оптимальною моделлю для органу ринкового нагляду і створити такий регуляторний орган або покласти додаткові повноваження на вже існуючі контролюючі органи з урахуванням фокусу на правах людини;
- забезпечити, щоб усі повноваження, які мають бути віднесені до сфери відання незалежного регулятора, перейшли до нього від центральних органів виконавчої влади, які наразі тимчасово реалізують такі повноваження;
- доповнити законодавство підзаконними нормативно-правовими актами щодо процедури звітування до наглядових органів в разі виявлення порушень.

4.2.3. Засоби правового захисту

Наразі в Україні відсутні спеціальні процедури щодо оскарження порушень прав людини у зв'язку із застосуванням технологій ШІ, зокрема, в рамках роботи наглядових органів або судів, а також профільних регуляторів. Існує загальне право подання пропозицій, скарг і заяв згідно з Законом України "Про звернення громадян". Закон надає можливості звернення до державних органів, які розробляють і використовують системи ШІ, здатні порушити права людини. Потенційно це уможливлює подання скарг щодо систем відеоспостереження, обладнаних функцією розпізнавання облич, додатків на кшталт «держава-в-смартфоні» та інших технологій, використовуваних у публічному секторі. Крім того, він дозволяє звертатися до підприємств, установ та організацій на території України - що охоплює і українських розробників систем ШІ. Складнішою є історії з іноземними компаніями - якщо їх представництва в Україні немає, то доведеться шукати інші шляхи для відновлення порушених прав.

Стаття 212-3 Кодексу України про адміністративні правопорушення встановлює відповідальність за незаконну відмову у прийнятті та розгляді звернень, надісланих відповідно до профільного Закону про звернення громадян. Втім, практики в контексті неповної відповіді на звернення щодо систем ШІ або ж ігнорування звернень їх розробниками немає. З цього можна зробити висновок, що або звернення розглядаються своєчасно і належно, або заявники не користуються статтею 212-3 КуПАП для оскарження порушень до Уповноваженого ВРУ з прав людини або у судовому порядку.

Крім того, відповідальність може наставати за порушення профільного законодавства - наприклад, Закону України "Про захист персональних даних", який містить загальні положення щодо захисту даних, застосовні незалежно від сфери, а отже, - і до систем ШІ. Також відповідальність може наставати у разі порушення Закону України "Про авторське право і суміжні права", який безпосередньо регулює об'єкти, створені комп'ютерними програмами, захищаючи їх правом особливого роду (sui generis). Порушення законодавства щодо заборони дискримінаційного ставлення також є актуальним, втім, більшість справ розглядатимуться або Уповноваженим ВРУ з прав людини, або в судовому порядку - тобто поза наглядовими повноваженнями регуляторів. Винятком є лише медійна сфера, де Закон України "Про медіа" уповноважує Національну раду з питань телебачення і радіомовлення розглядати випадки поширення упереджень та мови ворожнечі у медіа, що потенційно охоплює і використання медіа систем ШІ.

Проте жоден з описаних механізмів не заточений під розв'язання проблем, пов'язаних з системами ШІ та відповідальністю за порушення у цій сфері, а також не гарантує постраждалим можливість отримати від розробника чи користувача систем

ШІ інформацію про порядок їх функціонування в повному обсязі, необхідному для подання позову чи скарги.

Для гармонізації українського законодавства з вимогами ЄС, варто доповнити національне законодавство:

- повноваженнями наглядових органів розглядати скарги у позасудовому порядку (на зразок механізму, що наразі діє у сфері медіа);
- підзаконними нормативно-правовими актами щодо процедури подання звернень до відповідних органів в разі виявлення порушень;
- підзаконними нормативно-правовими актами щодо вимог повідомлення користувачів про порушення та засоби реагування на ці порушення;
- встановити законодавчі вимоги щодо порядку визначення розміру санкції залежно від тяжкості порушення та супутніх факторів, що впливають на наслідки вчиненого правопорушення.

4.3. Контент та ШІ

4.3.1. Вимоги щодо маркування контенту

Наразі в Україні відсутні законодавчі вимоги щодо маркування ШІ-модифікованого контенту. Міністерство цифрової трансформації України вже видало ряд рекомендацій щодо відповідального використання систем ШІ. Серед них прямі вимоги щодо маркування містять документи, які стосуються сфери медіа, сфери реклами та маркетингових комунікацій, та сфери інтелектуальної власності. Рекомендації в сфері медіа, зокрема, наголошують на проактивному сприянню поінформованості аудиторії про використання систем ШІ та про природу поширеного контенту. Ці рекомендації прямо вказують на необхідність маркування контенту для чіткого розмежування автентичного та ШІ-модифікованого контенту. Розробка інструментів для маркування ШІ-модифікованого контенту також передбачена в рамках заходів Білої книги з регулювання ШІ. Цей документ передбачає встановлення добровільного маркування для розробників систем для забезпечення відповідності поточним та майбутнім законодавчим вимогам ЄС та України.

Вимога щодо прозорості міститься у Кодексі поведінки, підписаному в рамках становлення механізмів саморегулювання у сфері ШІ. Також, оскільки найактуальнішими питання маркування генерованого контенту є для медійної сфери, Комісія журналістської етики видала Рекомендації щодо використання ШІ в медіа, які наголошують на необхідності позначати згенерований контент, а також перелічують випадки, коли таке генерування є недоречним або шкідливим.

На практиці різного роду маркування при використанні генерованого контенту вже використовуються в державному секторі. Наприклад, проєкт Міністерства закордонних справ “Вікторія ШІ” - цифрова представниця з консульських питань, має різні попередження та позначки, що вказують на те, що створений контент є штучно згенерованим. Втім, генерований контент далеко не завжди позначається у комунікаціях державних органів. У приватному секторі ситуація з маркуванням є неоднозначною: було багато випадків, коли медіа з необачності поширювали непромаркований контент або погано його перевіряли. Оскільки відповідальності за такі порушення немає, часто медіа не виносять уроків з неприємних ситуацій і продовжують поширювати немаркований контент, незважаючи на репутаційні ризики.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами на рівні ООН, варто доповнити національне законодавство:

- вимогами маркування ШІ-модифікованого контенту для розробників систем ШІ;
- підзаконними нормативно-правовими актами, що містять процедурні вимоги до формату та способів маркування залежно від типу контенту, суб'єкта та рівня ризиковості системи ШІ;
- вимогами маркування ШІ-модифікованого контенту для користувачів систем ШІ та відповідальністю у разі відсутності такого маркування для певних суб'єктів (наприклад, для медіа, рекламної сфери тощо).

4.3.2. Протидія дезінформації

Закон України "Про інформацію" визначає достовірність і цілісність інформації як один із принципів інформаційних відносин. Водночас, конкретні заходи щодо попередження дезінформації чи притягнення до відповідальності за таку діяльність не передбачені. Закон України "Про медіа" також послуговується загальними заборонами: як стаття 36, так і стаття 119 обмежують поширення нелегальних закликів та контенту, пов'язаного з російською агресією без оцінки його достовірності. Єдина мінімально дотична норма передбачена статтею 302 Цивільного кодексу України. Втім, зобов'язуючи осіб поширювати лише достовірну інформацію, вона стосується лише позовів щодо порушення честі, гідності та ділової репутації, адже в спорах, які зачіпають публічний інтерес, пересічна особа навряд буде визнана належним позивачем.

Міністерство цифрової трансформації України вже видало ряд рекомендацій щодо відповідального використання систем ШІ, серед яких документи у сфері медіа та сфері реклами і маркетингових комунікацій прямо чи побічно охоплюють питання поширення неправдивого контенту. Зокрема, рекомендації для сфери медіа наголошують на проактивному сприянню поінформованості аудиторії про використання систем ШІ та про природу поширеного контенту. Вони також наголошують на необхідності уникати перепоширення контенту, який згенерований з використанням систем ШІ з метою введення в оману, поширення дезінформації чи нелегального контенту. Медіа мають обачно ставитися і до контекстів, в яких вони поширюють згенерований контент - наприклад, генеровані зображення не варто поширювати при повідомленні інформації на чутливі теми, на кшталт війни, політичних чи соціальних питань.

Якщо в більшості європейських країн проблема генерованого контенту і дезінформації пов'язана з виборчими процесами, то в Україні найбільшої шкоди може завдати дезінформація, поширювана Росією в контексті збройної агресії. Неодноразово поширювалися діпфейки Зеленського, Залужного, Сирського, Кличка та інших посадовців, активні кампанії координованої неавтентичної поведінки організовуються на платформах Meta. Так само, зображення українських ведучих та популярних блогерів використовуються для поширення дезінформації на чутливі теми, як-от мобілізація, у TikTok. Оскільки діяльність платформ, як і діяльність користувачів на платформах, в Україні залишається неврегульованою, єдиним механізмом для протидії залишаються або заходи з медіаграмотності, або співпраця з платформами на горизонтальному рівні (як з боку державних органів, так і з боку громадських організацій).

З березня 2021 року в Україні діє Центр з протидії дезінформації як робочий орган при Раді національної безпеки і оборони. Центр працює на попередження прогнозованих загроз національній безпеці та національним інтересам України в інформаційній сфері.

Також при Міністерстві культури та стратегічних комунікації діє Центр стратегічних комунікацій та інформаційної безпеки - ще один орган, який відслідковує шкідливі наративи в інформаційному просторі та вживає відповідних заходів для їх подолання з боку виконавчої влади. У Міністерстві функціонує і просвітницький проєкт Фільтр, який передусім опікується питаннями медіаграмотності. Багато заходів в рамках діяльності згаданих органів та проєкту присвячені саме протидії дезінформації, зокрема, пов'язаній з російською агресією. Моніторинг шкідливих наративів у воєнній сфері також здійснюють в рамках Brave1 - там існує окрема платформа Mantis Analytics, за допомогою якої моніторять небезпечні повідомлення та канали їх поширення. Важливо, що цей проєкт передбачає застосування ШІ для верифікації інформації та аналізу великих масивів даних.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто доповнити національне законодавство:

- положенням щодо чіткого розподілу обов'язків Центру протидії дезінформації та Центру стратегічних комунікацій та інформаційної безпеки, зокрема щодо моніторингу генерованої ШІ дезінформації та співпраці з ключовими стейкхолдерами за цим напрямком;
- нормами щодо заборони використання систем ШІ, що маніпулюють свідомістю людей або вводять їх в оману для прийняття людьми нетипових рішень, в тому числі за допомогою діпфейків;
- вимогами щодо сприяння державними органами у створенні спів- та саморегулівних інструментів для подолання дезінформації та підвищення рівня цифрової та медіаграмотності.

4.3.3. Вимоги до систем управління контентом

Наразі національне законодавство не містить вимог до систем пріоритезації, рекомендації чи модерації контенту, здійснюваного онлайн-платформами. І хоча Закон України "Про інформацію" встановлює загальний обов'язок забезпечувати рівний доступ до інформації, а також постулює інформаційний плюралізм та свободу обміну ідеями, ця норма є занадто загальною, а отже, порядок її застосування до технічних платформ є незрозумілим і неоднозначним. Закон України "Про медіа" обмежується регулюванням платформ спільного доступу до відео. Втім, стаття 25 не передбачає окремих зобов'язань щодо систем рекомендацій для таких суб'єктів, послуговуючись загальною вимогою щодо оприлюднення прозорих і зрозумілих умов користування. Водночас, провайдерам таких послуг прямо забороняється збирати і обробляти персональні дані дітей з комерційною метою.

Серед законодавчих ініціатив відповіді на те, як регулювати системи рекомендації контенту також немає. Наприклад, Законопроєкт №11115, який спрямований передусім на регулювання Телеграму, не містить пропозицій, як саме регулювати системи управління контентом і не відповідає європейським вимогам у цій площині (оскільки пропонує карати платформи за невидалення окремих одиниць контенту, а не невжиття системних заходів). Інших ініціатив, які комплексно регулюють провайдерів онлайн-платформ у парламенті зареєстровано не було, втім активно обговорюється необхідність прийняття закону-аналогу Акта ЄС про цифрові послуги.

Водночас, Міністерство цифрової трансформації України видало ряд рекомендацій щодо відповідального використання систем ШІ у сфері медіа, сфері інтелектуальної власності а також сфері реклами та маркетингових комунікацій. Ці три документи

наголошують на тому, що системи персоналізації контенту мають бути прозорими та ґрунтуватися на принципах плюралізму та цілісності інформації, а також поваги до персональних даних. Вони підкреслюють, що інформація має бути правдивою і надійною, а користувачі мають наділятися правом персоналізувати рекламні і комерційні повідомлення та системи видачі контенту. Жоден з документів, втім, не говорить про заборону систем, що маніпулюють користувацькою поведінкою.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- встановити заборону на системи ШІ, що використовують методи впливу на підсвідомість або є умисно маніпулятивними чи оманливими і мають на меті вплив на поведінку людини, в тому числі маніпулятивні системи рекомендації контенту;
- встановити вимоги до платформ спільного доступу до інформації, а саме щодо прозорості та механізму функціонування систем рекомендації контенту, а також заборони на використання таких систем з маніпулятивною чи оманливою метою;
- заборонити рекламу, що використовує персональні дані дітей з комерційною метою, для всіх типів Інтернет-посередників, наприклад, шляхом внесення відповідних змін до Закону України "Про захист персональних даних";
- встановити обов'язок для платформ впровадити можливість налаштовувати медіа пропозицію користувачами;
- внести зміни до законодавства, що визначатимуть обов'язки суб'єктів, які є виробниками пристроїв чи надають користувацький інтерфейс, щодо застосування технологій ШІ.

4.4. ШІ та приватність

4.4.1. Порядок збору даних для розробки систем ШІ

Наразі в Україні відсутнє належне законодавче регулювання щодо збору навчальних даних для тестування та валідації ШІ-продуктів. Законодавчим орієнтиром для розробників систем ШІ слугує Закон України "Про захист персональних даних", який встановлює здебільшого загальні гарантії, не фокусуючись на положеннях автоматизованого збору даних або алгоритмах машинного навчання. Зокрема, закон передбачає загальні підстави щодо обробки персональних даних, а також забороняє збір біометричних даних, за винятком ряду легітимних випадків, включаючи дії з даними, "які були явно оприлюднені суб'єктом персональних даних" (п. 8 ч. 2 статті 7).

У контексті доступу до даних, які охороняються авторським правом, Закон України "Про авторське право і суміжні права" відносить до об'єктів авторського права бази даних (компіляції даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності. При цьому закон не містить механізму авторизації щодо доступу та збору відповідних даних. Водночас стаття 33 закону встановлює право особливого роду (*sui generis*) на неоригінальні об'єкти, згенеровані комп'ютерною програмою. У цьому контексті синтетичні дані, створені алгоритмами ШІ, можуть підпадати під цю категорію, оскільки вони не є результатом творчої діяльності особи. При цьому право на такі дані належатиме розробнику відповідної системи ШІ, а не автору початкових даних, що фактично уможливлює його на використання згенерованих даних для тренування машинних моделей. Втім, таке право залишається обмеженим, якщо йдеться про використання даних третіми особами (ч. 8 статті 33).

У цьому випадку важливо дотримуватися принципу справедливого використання даних як одного із європейських стандартів роботи з даними.

З українського законодавства також випливає, що розробники можуть користуватися даними, які перебувають у відкритому доступі. Ст. 10-1 Закону України "Про доступ до публічної інформації" вказує, що публічна інформація у формі відкритих даних є дозволеною для її подальшого вільного використання та поширення. Сюди входить копіювання, публікація та використання даних (в тому числі в комерційних цілях), проте з обов'язковим посиланням на джерело отримання такої інформації (ч. 2 статті 10-1). У свою чергу, Постанова КМУ №835 затверджує набір відкритих даних, які підлягають оприлюдненню, а також розпорядників відповідної інформації.

Жодних спроб регулювання механізму тестування систем ШІ не було здійснено і на рівні законопроєктів. Проєкт Закону №8153 про захист персональних даних, покликаний гармонізувати українське та європейське законодавство, хоча і акцентує увагу на автоматизованому прийнятті рішень, проте дуже побічно зачіпає питання ШІ. Примітно, що регулювання біометричних даних на рівні проєкту залишається досить жорстким, але розробники потенційно можуть користуватися положенням щодо легітимних випадків обробки біометричних даних, як-от "в цілях архівування в суспільних інтересах, для цілей наукового чи історичного дослідження або статистичних цілей" (стаття 7). У цьому випадку проєкт фактично дозволяє збір навчальних даних, здійснений без мети прибутку.

Втім, спроби регулювання збору даних для розробки систем ШІ можна спостерігати на рівні державних політик. Зокрема, у Білій книзі з регулювання ШІ в Україні Міністерство цифрової трансформації висловило намір про створення регуляторної пісочниці для можливості розробки та тестування ШІ-продуктів під наглядом та із залученням експертів. Крім того, в березні 2023 року було анонсовано запуск регуляторної пісочниці для розробників ШІ, а вже через рік уряд ухвалив Постанову КМУ №1238 про запуск інструменту для допомоги українським стартапам у сфері ШІ та блокчейн. Згідно з Постановою, за допомогою регуляторної пісочниці компанії, які планують запускати високотехнологічні продукти, можуть проводити дослідження для їх повноцінного використання. Постанова не вказує, які дані будуть використані для тренування відповідних систем, проте оперує поняттям "розподілена база даних", що передбачає децентралізовану базу даних із постійно оновлюваною та синхронізованою інформацією.

Належним орієнтиром слугують і рекомендації Мінцифри, розроблені урядом разом із юридичними та технічними експертами, які роз'яснюють чинне законодавство та надають поради щодо відповідального та етичного використання систем ШІ. Зокрема, у Рекомендаціях щодо ШІ та інтелектуальної власності наголошено на можливості правомірного використання об'єктів права особливого роду (*sui generis*) за умови дотримання таких вимог: (1) отримання дозволу на використання відповідного об'єкту, зокрема, шляхом укладення договору; (2) впровадження механізмів захисту прав на охоронювані об'єкти, зокрема, вилучення об'єктів із системи ШІ; (3) заохочення щодо відкритості даних, на яких тренуються системи ШІ. Рекомендації щодо ШІ та прав людини наголошують на належному захисті персональних даних, які можуть підлягати збору, а також заохочують розробників за потреби анонімізувати використовувані дані та здійснювати оцінку ризиків під час дослідження відповідної системи.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами на рівні ООН, варто:

- у оновленому Законі України "Про захист персональних даних" передбачити механізм обміну даних для цілей тренування та валідації систем ШІ (за моделлю Акту ЄС про дані та Акту ЄС про управління даними), а саме:
  - встановити явну згоду користувачів на збір та обробку їх біометричних даних, а також їх попереднього повідомлення про те, як ці дані будуть використовуватися, як обов'язкові вимоги для збору розробниками навчальних даних для цілей ШІ;
  - встановити механізм видалення навчальних даних після закінчення тренування системи ШІ на вимогу суб'єкта даних;
- розробити стандарти етичного використання даних для тренування систем ШІ, які можуть включати анонімізацію або ліцензування даних;
- передбачити створення державних баз даних (з попередньо отриманою згодою від суб'єктів даних та авторів матеріалів) для надання в користування розробникам ШІ відкритих навчальних даних для цілей тренування машинних моделей;
- дозволити розробникам ШІ повторно використовувати дані державного сектору, які не можуть бути доступні як відкриті дані (за моделлю Акту ЄС про управління даними), передбачивши категорії таких даних, механізм їх анонімізації або модифікації перед використанням, а також захист авторського права користувачів та їх персональних даних.

4.4.2. Захист від автоматизованого прийняття рішень

Національне законодавство передбачає право на захист від автоматизованого прийняття рішень. Наприклад, частина 13 статті 8 Закону України "Про захист персональних даних" наводить його у переліку прав суб'єкта даних. Втім, жодної деталізації цього права закон не містить, так само як і переліку винятків, передбачених Загальним регламентом про захист даних (GDPR). Наприклад, щодо прямої згоди особи або укладення правочину. Стаття 8 (частина 12) також передбачає право знати механізм автоматичної обробки даних, але формулювання є досить розмитим і незрозуміло, чи це право охоплює можливість отримати пояснення в кожному індивідуальному випадку, чи лише загальну інформацію про порядок функціонування тієї чи іншої автоматизованої системи. В контексті систем ШІ це питання є особливо актуальним, адже для розробників важливим є усвідомлювати обсяг своїх зобов'язань щодо суб'єктів даних.

Зміни пропонується внести Законопроєктом №8153 - фактично новою редакцією закону про захист персональних даних, покликаною гармонізувати регулювання з європейськими стандартами. Наприклад, статті 18 та 19 законопроєкту пропонують розширити право на інформацію про персональні дані уточненням щодо повідомлення про "наявність механізму автоматизованого прийняття рішень, у тому числі профілювання та необхідну інформацію про алгоритми (логіку), що використовуються у таких механізмах, а також значимість та передбачувані наслідки такої обробки". Це є своєрідною комбінацією вимог Акту ЄС про штучний інтелект та Загального регламенту про захист даних. Також Законопроєкт пропонує окрему статтю 25, що стосується захисту від автоматизованого прийняття рішень. Стаття є повною реплікою вимог Загального регламенту про захист даних.

Судова практика з питань реалізації права на захист від автоматизованої обробки даних та прийняття рішень на цій підставі є відносно чіткою, але невеликою. Одним з досить масштабних за своїм впливом стало рішення у справі №127/13877/19, що стосувалася автоматизованої обробки персональних даних АТ "Укрпошта", де позивачі скаржилися на самовільну обробку даних поштовим сервісом, автоматичним заповненням розрахункових квитанцій і вимогою повідомляти номер мобільного телефону для здійснення відправлень, мотивованих вимогою автоматизованої комп'ютерної програми. Суд вказав, що, з огляду на частину 13 статті 8 Закону України "Про захист персональних даних", позивачі мають право на отримання послуг без застосування автоматизованої системи обробки даних, а неможливість/небажання забезпечити такий формат надання послуг є порушенням закону. І хоча ця справа є досить ілюстративною з точки зору правозастосування, вона є радше поодиноким випадком, в той час як в багатьох ситуаціях автоматизовану обробку даних здійснюють без надання альтернативи отримати послуги, надані людиною.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- доповнити національне законодавство винятками до права на захист від автоматизованого прийняття рішень (аналогом статті 22 Загального регламенту про захист даних);
- чітко передбачити в національному законодавстві право на обґрунтування рішень прийнятих автоматизованими системами в кожному індивідуальному випадку (на додачу до права на повідомлення про механізм функціонування таких систем);
- розробити ефективні програми з медіа- та цифрової грамотності, а також ШІ-грамотності;
- регулятору у сфері захисту персональних даних варто здійснити огляд практик автоматизованої обробки даних, на підставі якої приймаються рішення, що мають суттєвий вплив на особу, та перевірити, чи такі практики є правомірними і чи право на захист від такої автоматизованої обробки належно забезпечене.

4.4.3. Системи біометричної ідентифікації

В Україні використання систем біометричної ідентифікації набуває все більших обертів – починаючи від біометричних паспортів та закінчуючи системами розпізнавання облич. Наразі основною метою звернення до відповідних заходів слугує реалізація безпекових ініціатив та надання публічних послуг.

Одним із найвідоміших порталів цієї сфери є "Дія" – платформа, яка надає державні послуги онлайн, допомагає бізнесу та підтримує IT-індустрію. Дія також містить відповідний застосунок, через який можна отримати доступ до електронних документів громадян та їх даних з державних реєстрів: вхід до додатку здійснюється через FaceID. Через застосунок особа також може підписувати документи в електронному форматі, проте за умови попередньої ідентифікації обличчя через камеру. Загалом в Україні є широко поширеною практика електронних документів – наприклад, у 2015 році було впроваджено біометричні паспорти, які містять інформацію про біометричні дані власника (зокрема, відбитки пальців). Крім того, великою популярністю користується і онлайн-банкінг, тобто мобільні застосунки відповідних банків, вхід до яких може здійснюватися через біометричну аутентифікацію. У свою чергу, BankID може використовуватися для входу в Дію або інші аналогічні застосунки.

На початку повномасштабного вторгнення Україна активно використовувала Clearview AI та FindClone – іноземні системи розпізнавання обличчя, які ідентифікували загиблих солдатів держави-агресора. Крім того, в Україні діє Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Система моніторить осіб, котрі в'їжджають та виїжджають з України, а також здійснює контроль за додержанням ними правил перебування на території України. Положення містить перелік органів, уповноважених на доступ до біометричних даних, проте оцінити відповідність такої системи вимогам GDPR важко з огляду на загальні формулювання положень. Відповідно до п. 4, "обробка персональних даних у національній системі, у тому числі їх зберігання, здійснюється з дотриманням вимог Закону України "Про захист персональних даних". Крім того, положення не деталізує гарантії поінформованості суб'єктів даних щодо їх прав, пов'язаних з такою обробкою.

Системи біометричної ідентифікації спостерігаються і на локальному рівні. Так, в рамках проєкту "Безпечне місто", безліч українських міст було оснащено камерами стеження, обладнаних системами розпізнавання облич. Встановлення відеокамер переслідувало такі легітимні цілі: ідентифікація осіб, що розшукуються, а також фіксація порушень правопорядку та моніторинг громадських місць. За допомогою спеціального аналітичного модуля розпізнавання, одночасно система може обробляти 450 потоків, 1100 облич на секунду. Відповідна інформація зберігається у аналітичних базах даних розшукуваних осіб. Наразі регулювання механізму таких інтрузивних систем відбувається на локальному рівні органами місцевого самоврядування, приклад - Положенням про комплексну систему відеоспостереження міста Києва. Спроба регулювання на законодавчому рівні запропонована у Проєкті Закону №11031, який має на меті запровадження єдиної системи відеомоніторингу та уніфікацію правил щодо механізму використання камер відеостеження. Чинна редакція проєкту містить положення і щодо збору біометричних даних, які порушують основоположне право суб'єктів даних на приватність. Згідно з проєктом, ідентифікація особи здійснюється за допомогою біометричних даних та інформації, яка включає, зокрема, дату народження/смерті, місце народження, стать та відомості про громадянство. Така практика має чіткі ознаки профайлингу, використання якого має супроводжуватися виключним дотриманням принципів захисту персональних даних та пояснюватися необхідністю втручання у приватність особи. У свою чергу, положення проєкту не обґрунтовують потребу у зборі такої великої кількості даних, що йде врозріз з вимогами Загального регламенту про захист даних.

Проєкт Закону №8153 про захист персональних даних у статті 7 встановлює загальні вимоги щодо обробки чутливих категорій даних (які включають біометричні дані), додатково виокремлюючи вимоги щодо обробки біометричних даних у конкретних випадках. Так, стаття 9 проєкту передбачає обробку біометричних даних суб'єктами владних повноважень та визначає вичерпний перелік випадків, за яких така обробка буде вважатися правомірною. У свою чергу, стаття 11 проєкту регулює обробку персональних даних в результаті аудіо, відео або фото фіксації публічних заходів.

Серед суттєвих проблем, з якими стикається держава у контексті використання систем біометричної ідентифікації, залишається відсутність належного законодавчого регулювання. Наразі в Україні немає уніфікованих та єдиних правил, які слугували б орієнтиром як для суб'єктів даних, так і уповноважених суб'єктів – регулювання здійснюється виключно на підзаконному рівні. Це, у свою чергу, призводить до фрагментарності положень, прогалин у законодавстві та відсутності узгодженості з ЄС стандартами. Навіть враховуючи наявність Закону України "Про захист персональних даних", передбачені ним гарантії відстають від європейських стандартів, які більш чітко регулюють збір, обробку та зберігання біометричної інформації.

З огляду на це, існують реальні ризики приватності громадян, чиї біометричні дані підлягають збору: вони можуть бути як технічними (як-от несанкціонований доступ, витік даних або недосконалість самої системи), так і етичними (як-от використання даних без згоди особи або питання дискримінації при розпізнаванні особи за її біометричними складовими).

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- розробити на рівні закону правила щодо використання систем біометричної ідентифікації державними органами (а саме підстави та умови використання, коло уповноважених суб'єктів та обмеження), які відповідатимуть вимогам Акту ЄС про штучний інтелект;
- заборонити на рівні закону використання систем біометричної категоризації;
- удосконалити правила щодо обробки та зберігання біометричних даних у Законі України "Про захист персональних даних", передбачивши додаткові гарантії для суб'єктів даних, які можуть включати:
  - розробку механізму, що дозволить суб'єктам даних повністю видаляти їх біометричні дані у випадку досягнення мети обробки або неправомірності такої обробки;
  - зберігання біометричних даних у зашифрованому вигляді як захід безпеки;
  - встановлення обмеженого доступу до біометричних даних виключного переліку уповноважених осіб;
  - механізм оскарження суб'єктами даних незаконної обробки їх даних та ін.

4.4.4. Приватність за проєктуванням і приватність за замовчуванням

Національне законодавство наразі не містить жодних згадок концепції приватності за проєктуванням чи приватності за замовчуванням. Відповідні зміни пропонується внести Законопроєктом №8153, що у статті 29 повністю реплікує статтю 25 Загального регламенту про захист даних. Втім, до прийняття законопроєкту вимоги посиленого фокусу на захист приватності при розробці технічних систем відсутні. Водночас, Міністерство цифрової трансформації України видало ряд рекомендацій щодо відповідального використання систем ШІ у сфері медіа, сфері реклами та маркетингових комунікацій, сфері захисту персональних даних, освітній сфері, сфері інтелектуальної власності. Кожен з документів наголошує на необхідності імплементувати практики захисту приватності при розробці та використанні ШІ, в той час як цільові рекомендації у сфері приватності розкривають варіанти інкорпорування згаданих концепцій у процес створення систем ШІ. Крім того, у середині грудня 2024 року низка технологічних компаній підписала Кодекс поведінки - саморегулівний інструмент у сфері ШІ, який закріплює основоположні принципи для роботи з системами ШІ та стане основою для створення органу саморегулювання. Одним з таких принципів є обов'язок захищати приватність користувачів на всіх етапах життєвого циклу систем ШІ.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- інкорпорувати в Закон України "Про захист персональних даних" вимоги щодо приватності за проєктуванням та приватності за замовчуванням;

- розробити підзаконні нормативно-правові акти щодо впровадження згаданих концепцій при розробці систем ШІ;
- здійснити аудит державних цифрових продуктів (“Дія”, “Мрія”, “Резерв+” тощо) на предмет відповідності згаданим підходам.

4.5. ШІ та заборона дискримінації

4.5.1. Збалансованість наборів даних

Національне законодавство у сфері забезпечення рівного ставлення та протидії дискримінації є загальним. Так, Закон України “Про засади запобігання та протидії дискримінації в Україні” містить положення, що забороняють будь-які форми дискримінаційного ставлення за будь-якою ознакою. Це, з одного боку, стосується і розробників, провайдерів та користувачів систем ШІ, а з іншого - не деталізує, яким саме чином ці норми застосовні до таких технологій, на якому саме етапі слід вживати додаткових заходів, якої форми вони мають набувати і хто здійснює контроль за їх дотриманням. Інші нормативні акти у сфері забезпечення рівності, включно з Законом України «Про забезпечення рівних прав та можливості жінок та чоловіків», Законом України «Про основи соціальної захищеності осіб з інвалідністю в Україні», Законом України «Про забезпечення прав і свобод внутрішньо переміщених осіб», Законом України «Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ» та Кримінальним кодексом України, також не визначають особливостей щодо протидії дискримінації у сфері ШІ чи хоча б новітніх технологій. Водночас, законодавство про захист персональних даних, детально проаналізоване в попередньому розділі, містить спеціальне регулювання щодо чутливих даних.

Про необхідність запроваджувати заходи протидії дискримінації говорить Біла книга з регулювання ШІ - своєрідний план та перелік інструментів, які можна використовувати для побудови відповідального ШІ-середовища в Україні. Втім, конкретних пропозицій щодо формування наборів даних і цей документ не містить. З ініціатив, які можуть спробувати покращити ситуацію щодо збалансованості наборів даних можна виокремити вже згадані регуляторні пісочниці, де розробники зможуть тестувати системи ШІ. Крім того, рекомендації з відповідального використання ШІ в різних сферах (медіа, реклами та маркетингових комунікацій, захисту персональних даних, освіти, інтелектуальної власності) наголошують на необхідності забезпечувати рівність при створенні і використанні систем ШІ. Також у 2025 році очікуються детальні рекомендації для розробників систем, які ймовірно враховуватимуть відповідні положення статті 10 Акту ЄС про штучний інтелект.

Оскільки наразі існує значна кількість систем ШІ, які застосовуються у публічному секторі, важливо забезпечити збалансованість наборів даних у таких системах, а також залишати інформацію про те, які дані використовувалися для розробки і тестування системи, публічно доступною для оцінки незалежних експертів.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- встановити вимоги щодо протидії дискримінації та забезпеченню рівності у сфері ШІ на всіх етапах життєвого циклу систем ШІ;

- законодавчо закріпити вимоги до наборів даних, що використовуються для тренування, тестування або валідації систем ШІ, а також відповідні заборони та винятки щодо використання чутливих даних у цих процесах;
- розробити методологію для здійснення аудиту наборів даних на предмет упереджень чи порушень;
- розробити механізми відновлення порушених прав та забезпечення рівності у сфері ШІ, в тому числі позасудові інструменти;
- здійснити аудит наборів даних, які використовувалися і наразі використовуються для тренування, тестування та функціонування систем ШІ у публічному секторі;
- розробити еталонний набір даних для тренування, тестування і валідації систем ШІ, призначених для використання у публічному секторі.

4.5.2. Системи предиктивної аналітики

Національне законодавство не містить ні заборони на використання деяких видів предиктивних систем ШІ, ні порядку використання таких технологій у судовій та правоохоронній сферах. Наприклад, Кримінальний процесуальний кодекс України у статті 314-1, що стосується змісту досудової доповіді представників органу пробації, не містить жодних посилань на автоматизовані системи чи вимог до них. Дотичні закони щодо діяльності поліції, антикорупційних органів, служби безпеки чи контррозвідувальних органів також не передбачають спеціальних повноважень, пов'язаних з використанням подібних систем. Регулювання відсутнє і на рівні підзаконних нормативно-правових актів конкретних міністерств та відомств.

На практиці, Міністерство юстиції України у тестовому режимі почало використовувати програмне забезпечення на базі ШІ "Касандра" - систему, яка на основі анкети з 97 питань визначатиме схильність особи до повторного вчинення злочинів (рецидив), що згодом інтегруватиметься у досудову доповідь. Ще у 2020 році Міністр юстиції Денис Малюська підкреслив, що за кілька років внаслідок машинного навчання буде достатньо даних, щоб "Кассандра" навчилася "аналізувати відповіді не тільки на перелік простих запитань, а й аналізувати всі інші дані, які є про злочинця". Актуальних даних щодо ефективності системи наразі немає. Це може як свідчити про те, що переходу на другий етап проєкту, коли ШІ виходить за межі відповідей і аналізує масиви даних комплексно, не відбулося, так і про використання системи без публічного висвітлення. Українські активісти та правозахисники б'ють на сполох, коли мова заходить про "Касандру", адже ризики від неправильних результатів системи можуть бути дуже значними. Підзаконних нормативно-правових актів, що регулюють використання цієї чи інших подібних систем в Україні наразі немає.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- встановити заборону на системи ШІ, метою яких є оцінка або класифікація осіб на основі їхньої соціальної поведінки або відомої, припущеної чи передбаченої характеристики особистості, якщо така оцінка спричиняє шкідливі наслідки, а також систем ШІ для оцінки або прогнозування ризику вчинення особою злочину виключно на основі профілювання особи або оцінки її особистісних якостей та характеристик (з винятком описаним далі);
- запровадити законодавчі зміни, що регулюють порядок використання систем предиктивної аналітики в правоохоронній та судовій сферах, включно з правовими гарантіями, як-от невикористання таких систем до осіб, щодо яких відсутня обґрунтована підозра в участі у вчиненні злочину;

- розробити підзаконні нормативно-правові акти, що встановлюють технічні і юридичні вимоги до систем предиктивної аналітики, порядок їх використання та механізм відповідальності за можливі порушення.

4.5.3. Портали для зворотного зв'язку

Національне законодавство наразі не регулює ані діяльності розробників систем ШІ, ані провайдерів онлайн-платформ, тож конкретних вимог щодо порталів для зворотного зв'язку чи скарг наразі немає. Чинний Закон України "Про захист прав споживачів" не пристосований до порядку функціонування онлайн-сервісів, в тому числі тих, які мають системи ШІ, а отже, немає жодних положень про внутрішні механізми розгляду скарг та вимоги до них. Нова редакція Закону України "Про захист прав споживачів", яка набере чинності після завершення воєнного стану, має статтю 39, що чітко встановлює право споживача на розгляд його скарг суб'єктом господарювання, який здійснив ймовірне порушення. Законодавство передбачає обов'язок своєчасно та обґрунтовано реагувати на такі скарги. Втім, застосовність таких норм до користувачів систем ШІ є сумнівною. Так само сумнів виникає щодо доречності надмірної деталізації статті 39 в контексті роботи провайдерів онлайн-платформ та розробників або постачальників систем ШІ. Тож, окремі норми все ще необхідно внести у профільне законодавство.

Водночас, ряд рекомендацій щодо відповідального використання систем ШІ від Міністерства цифрової трансформації України підкреслює необхідність створення можливості зворотного зв'язку при використанні систем ШІ (наразі такі рекомендації охоплюють сферу медіа, сферу реклами та маркетингових комунікацій, сферу захисту персональних даних, освітню сферу, та сферу інтелектуальної власності). Біла книга з регулювання ШІ також пропонує розробити типові механізми та інструменти, що дозволять покращувати практики комунікації провайдерів та розробників систем ШІ з користувачами з приводу прогалин у роботі їх продуктів.

Для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами ООН, варто:

- передбачити у законодавстві щодо онлайн-платформ вимоги до порталів для скарг в межах сервісів таких платформ, які також адресуватимуть питання використання систем ШІ;
- передбачити у регулюванні сфери ШІ вимоги до порталів для скарг та зворотного зв'язку;
- передбачити право на оскарження бездіяльності розробників/провайдерів систем ШІ до наглядових органів.

ПРАВО НА ВІЛЬНІ ВИБОРИ: ПОЛІТИЧНА РЕКЛАМА В ЦИФРОВОМУ СЕРЕДОВИЩІ

На сьогодні Україна не готова до подальшого зростання ролі онлайн політичної реклами на законодавчому рівні. Чинне регулювання є фрагментарним і застарілим, а комплексний підхід до питання відсутній. На ці проблемні питання у своїх звітах, зокрема, вказували й спостерігачі Обмеженої місії БДІПЛ зі спостереження за виборами на місцевих виборах 2020 року. Так, окремі їхні співрозмовники наголошували на тому, що «політичні партії та кандидати часто віддавали перевагу рекламі у соціальних мережах, з метою обходження вимог щодо фінансування кампаній, оскільки розміщення політичної онлайн-реклами не врегульовано законодавством». Відтак, однією з рекомендацій Обмеженої місії було те, що «виборче законодавство та нормативно-правова база, що регулює діяльність ЗМІ, повинні містити конкретні положення про фінансову звітність щодо політичної реклами в соціальних мережах та онлайн-ЗМІ». З цією метою, на думку, спостерігачів, закон повинен визначати політичну агітацію як таку, що також включає агітацію в соціальних мережах.

Використання онлайн політичної реклами під час виборчого процесу регулюється загальними положеннями розділу VIII Виборчого кодексу про передвиборну агітацію. Відповідно до ч.1 статті 51 Кодексу, передвиборна агітація може здійснюватися шляхом «оприлюднення в друкованих та аудіовізуальних (електронних) засобах масової інформації політичної реклами, виступів, інтерв'ю, нарисів, відеофільмів, аудіо- та відеокліпів, інших публікацій та повідомлень». Водночас ч.4 цієї статті наголошує, що агітація здійснюється за рахунок коштів виборчих фондів кандидатів, партій або їх організацій. Це означає, що витрати на агітацію в інтернеті мають бути відображені у фінансових звітах виборчих фондів.

Згідно з ч.5 статті 54 Кодексу, у передвиборній агітації заборонена прихована реклама та матеріали, які не позначені належним чином. Проте відсутність чіткого визначення «прихованої агітації» ускладнює запобігання таким порушенням в онлайн-середовищі. Крім того, ст.52 Кодексу встановлює загальну норму щодо припинення агітації о 24:00 у п'ятницю перед днем голосування. Хоча стаття 55 деталізує порядок використання електронних медіа, ці правила стосуються лінійних аудіовізуальних медіа, як-от телебачення та радіо. Спеціальних норм для інтернет-агітації Кодекс не містить.

Для врегулювання цих прогалин у березні 2021 року було створено робочу групу при парламентському Комітеті з питань державної влади, місцевого самоврядування та регіонального розвитку. До групи увійшли представники громадських організацій, медіаексперти, бізнес та народні депутати. Одним із завдань стало узгодження правил для медіа у виборчому процесі із законопроєктом «Про медіа». 30 серпня 2022 року Верховна Рада у першому читанні прийняла Закон України «Про медіа». Попри заклики громадськості положення щодо агітації у Виборчому кодексі було вилучено у другому читанні. Водночас зміни до Закону «Про всеукраїнський референдум» ухвалили.

Для того, щоб вказані положення таки були відображені у законодавстві, 27 грудня 2022 року було зареєстровано проєкт Закону № 8310 «Про внесення змін до Виборчого кодексу України». Цей документ передбачає низку новел щодо регулювання агітації в інтернеті та на платформах спільного доступу. Зокрема:

- Розміщення агітаційних матеріалів лише на підставі договору з виборчим фондом;

- Надання інформації про умови розміщення та копій договорів на запит НАЗК, ЦВК або Нацради;
- Обов'язкове маркування агітаційних матеріалів онлайн;
- Відповідальність розповсюджувачів банерної реклами;
- Співпраця Нацради з провайдерами платформ спільного доступу для виконання вимог;
- Покладення на користувачів Інтернет та платформ спільного доступу обов'язку дотримання вимог та обмежень щодо здійснення передвиборної агітації.

Втім, реалізація цих норм може бути проблематичною. Так, для укладення договору медіа має бути зареєстроване в Україні, але реєстрація є добровільною (стаття 63 Закону «Про медіа»). Оплата агітації онлайн через виборчі фонди є складною через банківські обмеження. На виборах 2020 року ці послуги оплачували фізичні особи, що дозволяло обходити законодавство. Законопроєкт не передбачає ефективних механізмів моніторингу, а також санкцій за порушення.

Варто також, зазначити, що згідно з законопроєктом, вимоги щодо маркування стосуються лише виборчого процесу, а поза ним політична реклама не регулюється. Це підкреслює концептуальну проблему українського законодавства, котра полягає у відсутності чіткого визначення «політичної реклами». Виборчий кодекс регулює лише передвиборну агітацію під час виборів, тоді як інформація, яка є агітацією в міжвиборчий період, взагалі не охоплена законодавством. Крім того, законодавець використовує поняття «передвиборна агітація» і «політична реклама» паралельно, що створює плутанину і дозволяє обходити вимоги щодо фінансування та порядку агітації.

Щодо фінансування онлайн політичної реклами, згідно з Виборчим кодексом, на президентських і парламентських виборах розмір виборчого фонду кандидата на пост Президента України та, відповідно, партії на виборах народних депутатів становить 90 000 розмірів мінімальної заробітної плати. При цьому розмір виборчого фонду для кожного кандидата у народні депутати, включеного до регіонального партійного списку, обмежується 4000 розмірів мінімальної заробітної плати. Водночас ці ліміти жодним чином не адаптовані до сучасного цифрового середовища і не враховують особливості його моделей функціонування.

Окремо слід уточнити також, що українське законодавство не містить спеціального регулювання питання таргетингу політичної реклами в Інтернеті. Опосередковано таке регулювання здійснюється рамковим законом «Про захист персональних даних». Так, згідно зі статтею 11 Закону, ключовою передумовою для обробки персональних даних є згода суб'єкта персональних даних на обробку його персональних даних. Подібний підхід використовується й у Законі України «Про електронну комерцію», згідно зі статтею 10 якого «комерційні електронні повідомлення поширюються лише на підставі згоди на отримання таких повідомлень, наданої особою, якій такі повідомлення адресовані». Водночас, комерційне електронне повідомлення може надсилатися особі без її згоди лише за умови, що вона може відмовитися від подальшого отримання таких повідомлень.

На практиці користувачі часто надають згоду на обробку персональних даних, не маючи повної та доступної інформації про її використання. Це призводить до проблеми, яка полягає у втраті контролю над особистою інформацією, коли суб'єкт персональних даних, тобто будь-який користувач онлайн-сервісів, має право відкликати згоду на обробку персональних даних (ст. 8 ЗУ «Про захист персональних даних»). Крім того, зазначений вище Закон «Про електронну комерцію» застосовується до «комерційних електронних повідомлень», метою яких, за визначенням, є пряме чи опосередковане

просування товарів, робіт чи послуг або ділової репутації особи, яка провадить господарську або незалежну професійну діяльність. Відтак, вказані норми не можуть бути застосовані до онлайн політичної реклами у міжвиборчий період та до матеріалів передвиборної агітації у мережі Інтернет.

Відтак, для гармонізації українського законодавства з вимогами ЄС, Ради Європи та рекомендаційними документами на рівні ООН, варто задовго до початку виборчого процесу перших повоєнних виборів внести комплексні зміни до Закону України «Про рекламу» або ухвалити окремий Закон «Про політичну рекламу». Цей закон має привести регулювання політичної реклами у відповідність до вимог Регламенту ЄС № 2024/900, зокрема - передбачати врегулювання порядку виготовлення, розміщення та фінансування політичної реклами не лише у зв'язку з виборами, але й у міжвиборчий період.

Крім того, такий законодавчий акт повинен:

- гарантувати належний рівень прозорості онлайн політичної реклами, зокрема шляхом надання інформації про замовників таких матеріалів на сервісах, де вона розміщується, а також містити вимоги до маркування онлайн політичної реклами, завдяки якому у чіткий, виразний та недвозначний спосіб громадяни можуть відділити політичну рекламу від іншої реклами, дізнатися про її замовників, отримати інформацію про те, чи застосовувалися інструменти таргетингу, а також, у разі якщо ця політична реклама є елементом передвиборної агітації чи агітації на референдумі – інформацію про той виборчий чи референдумний процес, якого вона стосується;
- містити зобов'язання для провайдерів політичної реклами щодо збереження архівів онлайн політичної реклами протягом достатнього часу у машиночитному форматі для забезпечення належного аналізу матеріалів державними інституціями та дослідниками; також доцільно у майбутньому передбачити можливість створення національного репозиторію онлайн політичної реклами;
- передбачити обов'язок платформ періодично звітувати про суму доходів отриманих частково або повністю в обмін на надані послуги онлайн політичної реклами;
- зобов'язати платформи та сайти, на яких розміщуються матеріали онлайн політичної реклами мати механізми, які дозволять фізичним або юридичним особам повідомляти їх, якщо конкретна політична реклама опублікована ними порушує права та свободи людини, а також суперечить Конституції України та іншим законодавчим актам;
- забезпечити, за допомогою засобів спільного регулювання, щоб онлайн-платформи надавали доступ до політичної реклами у справедливий і недискримінаційний спосіб і встановлювали для усіх однакові ціни за однакові послуги;
- передбачити можливість компетентних державних інституцій витребувати у провайдерів онлайн політичної реклами будь-яку необхідну інформацію – така інформація має бути повною, точною та достовірною та надаватися у чіткому, послідовному, зведеному та зрозумілому форматі;
- унормувати питання таргетингу онлайн політичної реклами;
- передбачити належні санкції за порушення у сфері онлайн політичної реклами.

Прикінцеві та перехідні положення цього Закону мають передбачати внесення змін до Виборчого кодексу, спрямованих на їхню гармонізацію, зокрема й у частині обмеження витрат на передвиборну агітацію в Інтернеті.

Лабораторія
цифрової
безпеки

МІЖНАРОДНИЙ
ФОНД
ВІДРОДЖЕННЯ