

**АНАЛІЗ
ЗАКОНОДАВСТВА
У СФЕРІ ОБМЕЖЕНЬ
ПРАВА НА ПРИВАТНІСТЬ
В УМОВАХ
ВОЄННОГО СТАНУ**



Київ. 2024

Аналіз законодавства у сфері обмежень права на приватність в умовах воєнного стану.

Українська Гельсінська спілка з прав людини (УГСПЛ) – найбільша асоціація правозахисних організацій України. Спілка об'єднує 26 правозахисних недержавних організацій. Метою діяльності УГСПЛ є захист прав людини.

УГСПЛ вважає себе частиною гельсінського руху і продовжувачем традицій та діяльності Української Гельсінської групи сприяння виконанню Гельсінських угод – УГГ.

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](https://www.facebook.com/irf.ukraine)

Європейський Союз складається з 27 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності і процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їхніми народами, та з народами з-поза їхніх меж.



Зміст

МЕТОДОЛОГІЯ	4
I. Право на приватність та воєнний стан	6
1. Право на приватність: міжнародно-правове регулювання.....	6
2. Право на приватність: національне регулювання	8
3. Допустимі обмеження права на приватність в умовах воєнного стану.....	9
II. Найбільші виклики для забезпечення права на приватність в умовах воєнного стану	13
1. Воєнний стан та виклики для права на приватність: кримінальний процес та поліцейська діяльність	13
2. Розвиток системи публічного відеоспостереження, зокрема із застосуванням технологій штучного інтелекту.....	23
3. Законодавчі ініціативи щодо права на приватність: єдина система відеоспостереження та захист персональних даних.....	29
III. Реагування на незаконне втручання у реалізації права на приватність	38
1. Реагування з боку Уповноваженого Верховної Ради України з прав людини.....	38
2. Реагування органів правопорядку (кримінальний аспект).....	40
3. Судова практика.....	41
ВИСНОВКИ	43
РЕКОМЕНДАЦІЇ	44

МЕТОДОЛОГІЯ

У зв'язку із повномасштабним вторгненням військ Російської Федерації на територію України Указом Президента України від 24 лютого 2022 року №64/2022 було введено воєнний стан, який було неодноразово продовжено і триває до сьогодні з огляду на продовження збройного конфлікту.

Цим Указом визначено, що у зв'язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені ст. 30-34, 38, 39, 41-44, 53 Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені ч. 1 ст. 8 Закону України «Про правовий режим воєнного стану».

Серед прав і свобод людини, які обмежуються в умовах воєнного стану відповідно до Конституції України перебувають такі права і свободи як недоторканність житла, таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, а також гарантій на невтручання в особисте і сімейне життя (ст. 34 Конституції України). Більш загальною їх прийнято називати правом на приватність.

Здійснення цих прав може бути обмежене 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, або для підтримання авторитету і неупередженості правосуддя.

Водночас важливим є, щоб такі обмеження застосовувались виходячи із принципів законності, пропорційності і необхідності таких обмежень в демократичному суспільстві. Сутність цих принципів, зокрема визначено в практиці Європейського суду з прав людини, так само у ній є приклади правомірних застосувань цих обмежень, що в умовах дії воєнного стану в Україні могли б служити певним орієнтиром.

Відтак **предметом** цього аналізу є стан українського законодавства у сфері обмежень права на приватність разом, що включає себе огляд ключових європейських стандартів. **Метою** такого аналізу є можливість органам влади використовувати дані щодо стану дотримання права на приватність в умовах воєнного стану для більше професійного підходу до питання втручання у реалізацію цього права, а громадянському суспільству розуміти де такі обмеження виправдані і законні, а в яких їх обґрунтованість сумнівна з огляду на процеси європейської інтеграції, до якої воно активно долучене.

Аналіз включає в себе:

- **розгляд** європейських стандартів захисту права на приватність;
- **допустимі** обмеження права на приватність в умовах воєнного стану;
- **законодавчі** ініціативи у сфері обмежень права на приватність в умовах воєнного стану;
- **огляд** найбільш інвазивних практик втручання у реалізацію права на приватність в умовах воєнного стану (кримінальний процес, поліцейська діяльність, захист приватності в системі відеоспостереження та збереження персональних даних в контексті євроінтеграційних процесів);
- **реагування** на випадку порушення права на приватність (контрольні органи, органи правопорядку, судова практика).

Під час підготовки цієї аналітичної публікації застосовано загальнонаукові методи аналізу, вивчено законодавство, міжнародні стандарти, кримінальну та судову статистику, тематичні публікації (наукові, аналітичні, публіцистичні), а також законотворчу активність парламентарів. За результатами аналізу сформульовано висновки щодо тенденцій у сфері дотримання права на приватність органами влади в умовах воєнного стану та сформульовано рекомендації для покращення ситуації у цій сфері.

I. ПРАВО НА ПРИВАТНІСТЬ ТА ВОЄННИЙ СТАН

1. Право на приватність: міжнародно-правове регулювання

Стаття 8 Конвенції про захист прав і основоположних свобод людини гарантує кожній людині *право на повагу до приватного і сімейного життя* (право на приватність). Відповідно до цієї статті кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. При цьому органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Таке право може бути розглянуто з трьох позицій. По-перше, як право індивіда на власне життя, на дії щодо самого себе. Це право напряму пов'язане з індивідуальністю конкретної людини і забезпечує захист від втручання з боку інших людей. По-друге, як неприпустимість втручання у приватне життя особи з боку держави, будь-яких організацій, установ, підприємств і фізичних осіб. По-третє, як право, що суміжне з такими правами, як право на недоторканність сімейного життя, право на недоторканність житла, право на недоторканність кореспонденції

Таке право містить чотири основні складові:

- 1) *інформаційну* (що включає в себе такі аспекти, як поширення відомостей про особу, збір та обробку персональних даних);
- 2) *фізичну* (тобто захист фізичної недоторканості особи);
- 3) *комунікативну* (безпека та приватність листування, електронної пошти, телефонних розмов та інших видів приватних комунікацій);
- 4) *просторову* (яка охоплює поняття дому, робочого місця, тобто безпосереднього середовища особи)¹.

В статті 8 Конвенції немає вичерпного визначення приватності або приватного життя, оскільки це поняття дуже «широке»² з огляду на принцип «живого дерева», який застосовує ЄСПЛ під час розвитку своєї практики і розширення змісту конвенційного права. В зміст цього права можуть входити, наприклад, такі складові:

- потерпілі від насилля;
- репродуктивні права;
- примусове лікування та обов'язкові медичні процедури;
- психічні хвороби;

¹ Шевчук С. Судовий захист прав людини: Практика Європейського Суду з прав людини у контексті західної правової традиції. – Вид. 2-е, випр., доп. – К.: Реферат, 2007. – С. 362.

² «Пек проти Сполученого Королівства», п. 57; «Смірнови проти Російської Федерації», п. 95 Judgment in the Case of «Smirnova v. Russia» (Applications nos. 46133/99 and 48183/99). URL: <http://hudoc.echr.coe.int/eng?i=001-61262>; «Німіцт проти Німеччини», п. 29 Judgment in the Case of «Niemietz v. Germany» (Application no. 13710/88). URL: <http://hudoc.echr.coe.int/eng?i=001-57887>

- охорона здоров'я і лікування;
- проблеми щодо завершення життя;
- проблеми, пов'язані з інвалідністю;
- проблеми щодо поховання;
- екологічні проблеми;
- статева орієнтація та статеве життя;
- професійна і ділова діяльність;
- право на власне зображення і фотографію, оприлюднення фотографій і статей;
- захист особистої репутації; наклеп;
- захист даних;
- право на доступ до особистої інформації;
- інформація про здоров'я особи;
- збирання інформації службами безпеки або іншими державними органами;
- поліцейське стеження;
- повноваження поліції із затримання і обшуку;
- приватне життя під час ув'язнення;
- право на особистий розвиток і автономію;
- право встановити своє походження;
- релігійні і особисті переконання;
- бажана зовнішність;
- право на ім'я/посвідчення особи;
- гендерна ідентичність;
- право на етнічну ідентичність;
- апатридізм, громадянство і місце проживання;
- шлюбний і батьківський статус тощо³.

³ Право на приватність у світлі статті 8 Конвенції про захист прав людини і основоположних свобод // УГСПЛ, 26.04.2021 [Електронний ресурс] / Режим доступу: <https://www.helsinki.org.ua/articles/pravo-na-pryvatnist-u-svitli-statti-8-konventsii-pro-zakhyst-prav-liudyny-i-osnovopolozhnykh-svobod/>

В контексті предмету цього аналізу нас цікавить найбільше інформаційний та комунікативний аспекти права на приватність, адже більшість обмежень прав і свобод людини в умовах воєнного стану стосуються питання доступу до персональних даних особи, накладення обмежень на поширення інформації, розкриття таємниці комунікації під час перевірок вмісту електронних пристроїв особи тощо.

2. Право на приватність: національне регулювання

Право на приватність гарантується Конституцією України. Зокрема, захищається:

- деякі аспекти фізичної приватності (жодна людина без її вільної згоди не може бути піддана медичним, науковим чи іншим дослідом) (ст. 28);
- територіальна приватність (кожному гарантується недоторканність житла) (ст. 30);
- комунікаційна приватність (таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції) (ст. 31);
- інформаційна приватність (ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків передбачених Конституцією України, не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди) (ст. 32).

На виконання положень Конституції України було ухвалено низку законів, предмет регулювання яких повністю або частково присвячений забезпеченню права на приватність. Серед них:

- **Кримінальний процесуальний кодекс України** (Закон №4651-VI від 13.04.2012), яким врегульовано порядок найбільш тяжкого втручання у право на приватність під час реалізації кримінальної процедури;
- **Кримінальний кодекс України** (Закон №2341-III від 05.04.2001) в частині кримінально-правового захисту права на приватність (ст. 145 «Незаконне розголошення лікарської таємниці», ст. 182 «Порушення недоторканності приватного життя», ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю», ст. 232 «Розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках», ст. 232-1 «Незаконне використання інсайдерської інформації», ст. 232-2 «Приховування інформації про діяльність емітента», ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 396 «Втручання в діяльність захисника чи представника особи» Кодексу);
- **Цивільний кодекс України** (Закон №435-IV від 16.01.2003) (ст. 286 «Право на таємницю про стан здоров'я», ст. 301 «Право на особисте життя та його таємницю», ст. 306 «Право на таємницю кореспонденції», ст. 1076 «Банківська таємниця»);

- **Закон України «Про Національну поліцію»** (Закон №580-VIII від 02.07.2015) (в частині регулювання доступу до персональних даних, застосування поліцейських заходів тощо);
- **Закон України «Про контррозвідувальну діяльність»** (Закон №374-IV від 26.12.2022) та Закон України «Про оперативно-розшукову діяльність» (Закон №2135-XII від 18.02.1992) (в частині регулювання інвазивних заходів з метою забезпечення національної безпеки поза кримінальною процедурою);
- **Закон України «Про захист персональних даних»** (Закон №2297-VI від 01.06.2010), яким врегульовано правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних;
- **Закон України «Про Єдиний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»** (Закон №5492-VI від 20.11.2012);
- **Закон України «Про адвокатуру і адвокатську діяльність»** (Закон №5076-VI від 05.07.2012) (в частині захисту адвокатської таємниці);
- **Основи законодавства України про охорону здоров'я** (Закон №2801-XII від 19.11.1992) (в частині захисту лікарської таємниці);
- **Закон України «Про банки і банківську діяльність»** (Закон №2121-III від 07.12.2000) (в частині захисту банківської таємниці).

3. Допустимі обмеження права на приватність в умовах воєнного стану

Захист прав і свобод громадян є одним із ключових обов'язків держави. Однак існують ситуації, коли їх обмеження є невідворотним і здійснюється винятково у спосіб та за допомогою засобів, передбачених чинним законодавством. Стаття 64 Конституції України встановлює виключення, за яких можуть встановлюватися окремі обмеження прав і свобод людини. Такою підставою безпосередньо виступає впровадження воєнного або надзвичайного стану – як легітимна мета втручання у реалізацію прав і свобод людини.

Так, Указом Президента України від 24.02.2022 року № 64/2022⁴ в Україні введено воєнний стан із 05 години 30 хвилин 24 лютого 2022 року строком на 30 діб. Надалі строк дії воєнного стану в Україні неодноразово продовжувався у зв'язку із збереженням загрози національній безпеці – повномасштабною агресією з боку Російської Федерації, що є збройним конфліктом міжнародного характеру (війною)⁵.

⁴ Указ Президента України №64/2022 від 24 лютого 2022 року [Електронний ресурс] / Режим доступу: <https://www.president.gov.ua/documents/642022-41397>

⁵ Останнє продовження відбулось з 05 години 30 хвилин 14 лютого 2024 року строком на 90 діб. Указ Президента України від 05.02.2024 №49/2024 [Електронний ресурс] / Режим доступу: <https://www.president.gov.ua/documents/492024-49741>

Відповідно до ч. 3 Указу № 64/2022 (і подальших указів, якими воєнний стан неодноразово продовжувався) на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30 – 34, 38, 39, 41 – 44, 53 Конституції України, а саме:

- недоторканність житла;
- *таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції;*
- *невтручання в особисте і сімейне життя, крім випадків, передбачених Конституцією України;*
- свобода пересування, вільний вибір місця проживання, право вільно залишати територію України, за винятком обмежень, які встановлюються законом;
- право на свободу думки і слова, на вільне вираження своїх поглядів і переконань;
- право брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування;
- право збиратися мирно, без зброї і проводити збори, мітинги, походи і демонстрації;
- право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності;
- право на підприємницьку діяльність, яка не заборонена законом;
- право на працю;
- право на страйк для захисту своїх економічних і соціальних інтересів;
- право на освіту.

Цікавою в контексті пошуку відповіді на питання щодо необхідних меж застосування правомірного обмеження прав людини і громадянина під час дії воєнного стану є окрема думка судді Конституційного Суду України В.В. Лемака, яку він надав за результатами постановлення Рішення Конституційного Суду України від 6 квітня 2022 року № 1-р(II)/2022. Суддя зазначив таке: *«Під час війни неприпустимим є різке протиставлення публічного (державного) інтересу, відповідних конституційних цінностей, з одного боку, та поваги до індивідуальних прав людини, з іншого боку, як це нерідко бувало в мирні часи. Під час війни найбільше має виявлятися сприйняття того, що публічний інтерес (наприклад, оборона, національна безпека), в якому акумулюються індивідуальні права і свободи людини. Наприклад, обмеження пересування громадян (комендантська година, блокпости) чи навіть вилучення для потреб оборони майна громадян спрямоване на захист найбільш засадничих прав і свобод людини – права на життя, їх гідності і свободи (наприклад, захист від діяльності диверсійно-підривних груп ворога). Такий підхід підтверджується не тільки теоретично, а й суворими реаліями оборонної війни в Україні»⁶.*

⁶ Окрема думка (збіжна) судді Конституційного Суду України Лемака В.В. стосовно Рішення Конституційного Суду України (другий сенат) у справі за конституційною скаргою Поліщука Сергія Олексійовича щодо відповідності Конституції України (конституційності) пункту 4 статті 16-3 Закону України «Про соціальний і правовий захист військовослужбовців та членів їх сімей» (справа про посилені соціальний захист військовослужбовців) [Електронний ресурс] / Режим доступу: https://ccu.gov.ua/sites/default/files/docs/1_p2_2022_1.pdf

Обмеження прав людини – це звуження обсягу її прав і свобод, а також чинники, що унеможливають або ускладнюють реалізацію особою таких прав і свобод. Загалом, це певні заборони, що покликані змінити поведінку особи через обмеження суб'єктивного права. При цьому обмеження прав і свобод людини застосовуються тільки за чітко визначених умов.

Відповідно до «трискладового тесту»⁷, сформованого у практиці ЄСПЛ такі обмеження мають бути:

- 1) встановлені законом або здійснюватись згідно із законом;
- 2) переслідувати легітимну мету такого втручання;
- 3) бути необхідними в демократичному суспільстві.

Стосовно першого критерію – **відповідності закону** – Європейський суд з прав людини напрацював низку вимог, що розкривають його зміст:

- закон має бути достатньо доступним – особі має бути відомо про правові норми, що застосовуються в кожному конкретному випадку;
- норма закону має бути сформульована достатньо чітко, щоб дати особі змогу передбачити наслідки відповідних дій (правова визначеність).

Щодо другого критерію – **правомірності мети обмеження (легітимної мети втручання)** – то кожна стаття Конвенції про захист прав людини і основоположних свобод містить перелік цілей для обмеження кожного конкретного права.

Щодо третього критерію – **необхідності у демократичному суспільстві** – Європейський суд з прав людини визнає за державами певну свободу для роздумів щодо питання, що є необхідним в тому чи тому демократичному суспільстві, однак вимагає від держав дотримання пропорційності між обмеженням прав і свобод людини і громадянина та досягнутою законною метою захисту інтересів суспільства.

Обмеження прав і свобод людини в умовах надзвичайного стану викликано тим, що реалізація таких прав може призвести до збільшення соціальної напруженості та створити перешкоди для органів державної влади, уповноважених підтримувати і відновлювати конституційний правопорядок. Легітимність мети полягає якраз у збереженні конституційного правопорядку, тобто правових засобів, які сприятимуть подоланню загроз, поставлених воєнним станом. З огляду на наявність мети подолання загроз – правовий режим воєнного стану є тимчасовим заходом, тож і обмеження встановлюються тимчасово.

При цьому громадяни обов'язково мають бути проінформованими про те, що на території, де вони проживають чи перебувають, введено воєнний стан та які права і свободи у зв'язку з цим буде обмежено. Обмеження прав і свобод людини в умовах воєнного стану має здійснюватися під парламентським контролем, тобто введення воєнного стану та продовження терміну його дії обов'язково має бути схвалено парламентом (форма

⁷ 1) prescribed by law/in accordance with law / 2) legitimate aim / 3) necessary in a democratic society – в широкому сенсі мова йде про доктрину margin of appreciation.

контролю у парламентсько-президентській республіці, якою є Україна). Водночас введення надзвичайного стану не припиняє діяльності судових органів, а тому громадяни зберігають своє право на звернення до суду за захистом своїх прав і свобод, а також оскарження незаконних обмежень цих прав⁸.

Окремо слід зазначити, що Європейський суд з прав людини передбачає не лише можливість обмеження прав і свобод людини і громадянина, але й право держави відступити на певний час від своїх зобов'язань під час війни або іншої суспільної небезпеки. Стаття 15 Конвенції, регламентуючи цю процедуру, обмежила ситуації правомірного відступу від зобов'язань такими умовами: 1) відступ може мати місце тільки під час війни або іншої суспільної небезпеки, яка загрожує життю нації; 2) заходи, що вживаються у відповідь на таку війну або суспільну небезпеку, не виходять за межі, яких вимагає гострота становища; 3) заходи не повинні суперечити іншим зобов'язанням держави згідно з міжнародним правом.

Інтерпретацію критеріїв відступу від зобов'язань щодо прав людини в надзвичайних ситуаціях в межах принципу «згідно з законом» містить система показників «Rule of Law Checklist» («Мірило правовладдя»). Такими критеріями є: наявність особливих приписів національного права, що застосовуються до надзвичайних станів (воєнний стан є його різновидом в цих термінах), із відповідними відступами від зобов'язань з прав людини; встановлені підстави запровадження обмежень (обставини і критерії); заборона на відступ від зобов'язань за певними правами навіть за надзвичайних ситуацій; співмірність (пропорційність) способів відступу в контексті гостроти потреб ситуації, її тривалості, умов та обсягу; обмеженість можливостей виконавчої влади відступати від звичайного розподілу повноважень; парламентський контроль та судовий нагляд щодо дії та тривалості надзвичайного стану і щодо обсягу будь-якого відступу в його рамках⁹.

При цьому будь-яка Висока Договірна Сторона відповідно до Конвенції, використовуючи це право на відступ від своїх зобов'язань, у повному обсязі інформує Генерального секретаря Ради Європи про вжиті нею заходи і причини їх вжиття.

Після 24 лютого 2022 року у зв'язку із впровадженням правового режиму воєнного стану та введенням обмежень на реалізацію прав і свобод людини, 28 лютого Україна звернулася до Ради Європи з повідомленням про відступ (дерогацію) зобов'язань за Конвенцією¹⁰. У повідомленні йшла мова про відступ від зобов'язань за такими статтями Конвенції про захист прав і основоположних свобод людини: стаття 4 (параграф 3) (**заборона примусової праці**); стаття 8 (**право на повагу до приватного і сімейного життя**); стаття 9 (**свобода думки, совісті і релігії**); стаття 10 (**свобода вираження поглядів**); стаття 11 (**свобода зібрань та об'єднання**); стаття 14 (**заборона дискримінації**); стаття 16 (**обмеження політичної діяльності іноземців**); статті 1, 2 додаткового протоколу до Конвенції (**захист права власності та право на освіту**); стаття 2 Протоколу №4 до Конвенції (**свобода пересування**).

Отже, право на приватність (право на повагу до приватного і сімейного життя) перебуває серед тих конвенційних прав і свобод, від яких здійснила відступ Україна.

⁸ Хила І. Ю. Конституційні основи обмеження прав і свобод в умовах надзвичайного стану: досвід зарубіжних країн. Науковий вісник публічного та приватного права. 2019. Вип. 2. Том 1 – С. 43.

⁹ Мірило правовладдя: коментар, глосарій, Rule of Law Checklist. Венеційська Комісія Ради Європи / пер. С. Головатий. 2017. – С. 19.

¹⁰ Derogation contained in the Note Verbale No. 31011/32-017-3 from the Permanent Representation of Ukraine to the Council of Europe, dated 28 February 2022, registered at the Secretariat General on 1 March 2022 [Електронний ресурс] / Режим доступу: <https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=005&codeNature=0>

II. НАЙБІЛЬШІ ВИКЛИКИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРАВА НА ПРИВАТНІСТЬ В УМОВАХ ВОЄННОГО СТАНУ

1. Воєнний стан та виклики для права на приватність: кримінальний процес та поліцейська діяльність

Втручання у реалізацію права на приватність в умовах воєнного стану викликає стурбованість навіть після запровадження окремих законодавчих засобів захисту, створення в різних формах інструментів та механізмів їх захисту. Тобто досягнення певних механізмів втручання у реалізацію цього права, які б з одного боку сприяли досягнення цілей воєнного стану (захисту національної безпеки), з іншого – робили таке втручання мінімальним, а обмеження допустиме в демократичному суспільстві навіть в умовах збройного конфлікту.

Збройний конфлікт порушує значне коло питань пов'язаних із різними аспектами права на приватність, як щодо недоторканності житла, захисту персональних даних, так і щодо використання систем публічного відеоспостереження, тому важливим є як інформування населення про випадки порушення права на приватність, так і більш ретельний розгляд пропорційності такого втручання.

Серед тенденцій останніх двох років, які можна назвати найбільшimi викликами для забезпечення права на приватність, можна виокремити такі:

- 1) спрощення порядку втручання у реалізацію права на приватність в межах проведення слідчих дій в кримінальному провадженні, а саме послаблення гарантій судового контролю за таким втручанням у певних випадках (ст. 615 КПК України);
- 2) спрощення порядку реалізації органами правопорядку та безпеки повноважень з доступу до персональних даних в межах реалізації своїх повноважень (проведення перевірок телефонів, поверхневих оглядів, оглядів автомобілів на блокпостах тощо);
- 3) розширення масштабів використання камер відеофіксації та відповідного програмного забезпечення для дотримання громадської безпеки та ідентифікації осіб, які причетні до вчинення правопорушень (камери в межах програм «Безпечне місто», використання Clearview AI при ідентифікації людей, причетних до вчинення злочинів тощо).

Надалі детальніше розглянемо кожен з викликів.

1.2 Послаблення судового контролю за дотриманням права на приватність в межах кримінального провадження

Після повномасштабного вторгнення збройних сил російської федерації 24 лютого 2022 року питання здійснення правосуддя постало перед усією системою правопорядку. Неможливість фізично здійснювати правосуддя торкнулася багатьох судів, а навантаження на систему правосуддя в частині судового контролю суттєво зросло у зв'язку з потребою протидії колабораційній, диверсійній, підривній діяльності, запобігання масовому вчиненню майнових злочинів на територіях, звідки було евакуйовано / виїхало населення тощо. *Навесні-влітку 2022 року було ухвалено низку змін до кримінального та кримінального процесуального законодавства*, які детально врегулювали питання особливого режиму досудового розслідування та судового розгляду в умовах воєнного стану.

Зокрема, було ухвалено низку змін до Розділу IX-1 КПК України – Законом [№ 2111-IX](#) від 3 березня 2022 року; Законом [№ 2125-IX](#) від 15 березня 2022 року; Законом [№ 2137-IX](#) від 15 березня 2022 року; Законом [№ 2201-IX](#) від 14 квітня 2022 року; Законом [№ 2462-IX](#) від 27 липня 2022 року. Ними як суттєво розширено обсяг правового регулювання ст. 615 КПК України, так і доповнено Розділ IX-1 новими статтями, що надає йому більшої системності та права називатися справді *особливим режимом здійснення досудового розслідування, судового розгляду в умовах воєнного стану*. Деякі процесуальні гарантії для підозрюваного / обвинувачення не один раз змінювалися, наприклад збільшився граничний строк затримання, протягом якого особа має постати перед слідчим суддею / судом.

Відповідно до ухвалених змін за умови *«відсутності об'єктивної можливості виконання у встановлені законом строки слідчим суддею повноважень»* повноваження з судового контролю перебирає на себе прокурор. Так, ст. 615 КПК України дозволяє керівнику відповідного органу прокуратури, що здійснює судовий контроль, реалізовувати повноваження, передбачені статтями 140 (привід), 163, 164 (*тимчасовий доступ до речей і документів*), 170, 173 (арешт майна), 206 (загальні обов'язки щодо захисту прав людини), 219 (строки досудового розслідування), 232 (допит, впізнання у режимі відеоконференції), 233, 234, 235 (*санкціонування обшуку*), 245–248 (*санкціонування певних видів експертиз*), 250 (НСРД) і 294 (продовження строків досудового розслідування) КПК України.

Фактично, що проведення такої слідчої дії як обшук, що тимчасовий доступ до речей і документів або певні види експертиз, пов'язані із втручанням у приватне життя (наприклад відібрання біологічних зразків) є втручанням у право на приватність.

Про такі рішення прокурор за першої можливості повідомляє прокурора вищого рівня, а також суд, надаючи копії відповідних документів не пізніше ніж за 10 днів з дня повідомлення (ч. 3 ст. 615 КПК України). Оскільки ані форма, ані зміст такого повідомлення не визначені, то можна вважати, що воно здійснюється в довільній формі. Таким чином, ця норма має лише інформативний характер. Хоча насправду подібні дії мали б тягнути за собою певні юридичні наслідки, тоді необхідність такого повідомлення була б виправдана з позиції захисту прав і свобод людини. У такому випадку виникає небезпека упередженості та зловживання повноваженнями відповідним керівником органу прокуратури¹¹.

¹¹ Крапивін Є. EDITORIAL: покладення функції судового контролю на прокурора: як обґрунтовується «відсутність об'єктивної можливості» його здійснення? // Just Talk, 13.04.2023 [Електронний ресурс] / Режим доступу: <https://justtalk.com.ua/post/editorial-pokladennya-funktsii-sudovogo-kontrolyu-na-prokurora-yak-obgruntovuyetsya-vidсутnist-obektivnoi-mozhливosti-jogo-zdijsnennya>

Чинний КПК України для виконання керівником органу прокуратури функції судового контролю в межах особливого режиму досудового розслідування та судового розгляду передбачає наявність таких умов:

- 1) правовий режим воєнного стану;
- 2) відсутність об'єктивної можливості виконання слідчим суддею повноважень, передбачених відповідними статтями КПК України;
- 3) наявність клопотання прокурора або клопотання слідчого за погодженням з прокурором;
- 4) винесена керівником органу прокуратури постанова, яка має містити обґрунтування правомірності здійснення ним повноважень слідчого судді (абз. 2 п. 2 ч. 1 ст. 615 КПК України).

Поняття **«відсутність об'єктивної можливості»** є відкритим текстом норми права, тобто вона не визначена текстуально, проте визначається правозастосовником у кожному конкретному випадку залежно від обставин. Простішими словами, це оцінне (оціночне) поняття на кшталт понять «розумні строки» чи «обґрунтована підозра».

Оскільки наразі немає судової практики у вигляді правових позицій Верховного Суду чи рішень Європейського суду з прав людини з цього питання (квазіпрецедентних форм права), ніхто не може чітко відповісти, у чому саме полягає об'єктивна неможливість. Водночас очевидно, що мова йде про пристосування до надзвичайних обставин задля забезпечення можливості здійснення правосуддя в умовах, що унеможливають функціонування судів на конкретній території. Причиною цього може бути як окупація, близькість до зони бойових дій, так і фізична непридатність приміщень, неповернення суддів з евакуації після деокупації територій тощо.

Також об'єктивна неможливість виконання слідчим суддею повноважень може бути пов'язана не тільки безпосередньо з воєнними діями: вона може виникнути через організацію роботи суду, комендантську годину, місце зберігання матеріалів досудового розслідування тощо. Кожна конкретна ситуація обґрунтовується керівником відповідного органу прокуратури в постанові.

Стосовно практичних наслідків, то якість **«судового контролю» за дотриманням прав і свобод людини в кримінальному провадженні, що здійснюється прокурором, прямо впливає на забезпечення прав підозрюваного / обвинуваченого.**

За таких умов єдиною гарантією законності та обґрунтованості рішень, ухвалених у межах особливого режиму досудового розслідування, залишається судове оцінювання правомірності застосування положень ст. 615 КПК України за результатами судового розгляду кримінального провадження при оцінюванні доказів у нарадчій кімнаті під час ухвалення судового рішення.

Наслідком порушення цих прав і свобод людини (процесуальних гарантій) може бути визнання доказів недопустимими (ст. 86, 87 КПК України). Проте це не відбувається автоматично в кожному випадку необґрунтованості постанови про виконання керівником

відповідного органу прокуратури функцій слідчого судді, суду. Як зазначає Верховний Суд у своїй правовій позиції щодо допустимості доказів, «...[Суд] повинен у межах доводів сторін перевірити, чи призвів спосіб призначення експертизи до порушення тих чи інших прав і свобод людини, передбачених Конвенцією та/або Конституцією України. У разі визнання доказів недопустимими суд має вмотивувати свої висновки про істотне порушення вимог кримінального процесуального закону, зазначивши, які саме й чії права і свободи було порушено і в чому це виражалось»¹².

Але частіше це питання професійності, компетентності, неупередженості прокурора. Наприклад, Кваліфікаційно-дисциплінарна комісія прокурорів (КДКП) притягнула до відповідальності прокурора, який застосовував положення ч. 2 ст. 615 КПК України на території м. Києва у травні 2022 року, посилаючись на неможливість функціонування суду (рішення № 202дп-22)¹³. Водночас коли мова йшла про перші дні квітня 2022 року, коли м. Київ лише звільнили від оточення, то комісія вирішила, що посилання на відсутність об'єктивної можливості виправдане, і закрила провадження щодо прокурора (рішення № 41дп-23)¹⁴.

Масштабів застосування прокурорами відповідних положень ст. 615 КПК України станом на сьогодні невідомо. Хоча практика КДКП, наведена вище, а також публікації в ЗМІ дають підстави вважати, що вона була присутня лише у 2022 році – все одно, масштаби проблеми невідомі. Припускаємо, що прокурори можуть вдаватись до реалізації повноважень з судового контролю на територіях, де дійсно складно здійснювати правосуддя через постійні обстріли, відсутність електрики тощо. Проте якраз судова влада має активно реагувати на будь-які випадки безпідставного перебирання на себе таких повноважень, а сама прокуратура активніше комунікувати з суспільством випадки такого перебирання на себе судових функцій. В умовах воєнного стану ці повноваження лишаються чинними, отже можуть в будь-який момент бути застосовані прокурором, а отже гарантування права на приватність у кримінальному процесі послаблено.

1.3 Спрощення процедур проведення поліцейських заходів органами правопорядку та безпеки

В умовах воєнного стану Національна поліція отримала додаткові повноваження для реалізації покладених на неї завдань. Так, ст. 8 Закону України «Про Національну поліцію» доповнено частиною четвертою, яка передбачає, що під час дії воєнного стану поліція діє згідно з призначенням та специфікою діяльності з урахуванням тих обмежень прав і свобод громадян, а також прав і законних інтересів юридичних осіб, що визначаються відповідно до Конституції України та Закону України «Про правовий режим воєнного стану».

¹² Постанова Великої Палати Верховного Суду від 31.08.2022 (провадження № 13-Зкс22, справа № 756/10060/17) [Електронний ресурс]. – Режим доступу: <https://reyestr.court.gov.ua/Review/106141457>

¹³ Рішення Кваліфікаційно-дисциплінарної комісії прокурорів від 09.11.2022 № 202дп-22 [Електронний ресурс]. – Режим доступу: <https://kdkp.gov.ua/decision/2022/11/09/3275>

¹⁴ Рішення Кваліфікаційно-дисциплінарної комісії прокурорів від 01.03.2023 № 41дп-23 [Електронний ресурс]. – Режим доступу: <https://kdkp.gov.ua/decision/2023/03/01/3397>

Розділ 5 Закону України «Про Національну поліцію» також зазнав деяких змін, які стосуються періоду воєнного стану, а саме:

- 1) поліція отримала можливість здійснювати перевірку документів та фіксувати дані, що містяться в документах, якщо особа володіє зовнішніми ознаками, схожими на зовнішні ознаки особи, яка самовільно залишила місце для утримання військовополонених (п. 1 ч. 1 ст. 32 Закону);
- 2) поліція має право зупиняти транспортні засоби, якщо наявна інформація, яка свідчить про те, що водій або пасажир транспортного засобу є особою, яка самовільно залишила місце для утримання військовополонених.
- 3) за новою редакцією ст. 40 Закону поліція зможе використовувати у своїй діяльності такі технічні засоби, як безпілотні літальні апарати, та спеціальні технічні засоби протидії їх застосуванню; спеціалізоване програмне забезпечення для здійснення аналітичної обробки фото- й відеоінформації, у тому числі для встановлення осіб і номерних знаків транспортних засобів.

Свою фото- та відеотехніку, технічні прилади та технічні засоби з виявлення та/або фіксації правопорушень, а також з виявлення радіаційних, хімічних, біологічних та ядерних загроз, поліція має змогу закріплювати на однострої, у/на безпілотних літальних апаратах, службових транспортних засобах, суднах чи інших плавучих засобах, у тому числі тих, що не мають кольорографічних схем, розпізнавальних знаків та написів, які свідчать про належність до поліції, а також монтувати/розміщувати їх по зовнішньому периметру доріг і будівель;

- 4) за необхідності відбиття нападу, що загрожує життю чи здоров'ю поліцейського чи іншої особи, та усунення небезпеки у стані крайньої необхідності або при затриманні особи, яка вчинила правопорушення та/або чинить опір, поліцейський має право застосовувати будь-які підручні засоби, а не тільки ті спеціальні засоби, які передбачені ст. 45 Закону (ч. 5 ст. 42 Закону).
- 5) під час дії воєнного стану поліцейський має право застосовувати заходи примусу, передбачені ст. 42, стосовно осіб, які беруть участь у збройній агресії проти України, без врахування вимог та заборон, які стосуються порядку застосування заходів примусу, порядку застосування спеціальних засобів та порядку застосування вогнепальної зброї (ч. 9 ст. 42 Закону).

У разі застосування такого примусу, внаслідок чого зазначеним особам було спричинено тілесне ушкодження, каліцтво, вогнепальне поранення, поліцейський за можливості має усно або за допомогою засобів комунікації повідомити про це свого безпосереднього керівника, який у разі необхідності за можливості повідомляє центральний орган управління поліції та відповідного прокурора (ч. 10 ст. 42 Закону)¹⁵.

До того ж Закон України «Про правовий режим воєнного стану» містить перелік заходів, які можуть бути впроваджені у випадку введення воєнного стану. До них серед іншого відноситься:

¹⁵ Іщенко Ю., Марченко Н. Національна поліція в умовах воєнного стану: зміни в законодавстві // Право в умовах війни, 16.08.2022 [Електронний ресурс] / Режим доступу: <https://law-in-war.org/nacjonalna-policiya-v-umovah-voyennogo-stanu-zminy-v-zakonodavstvi/>

- «встановлення у визначеному Кабінетом Міністрів України порядку особливого режиму в'їзду і виїзду, обмеження свободи пересування громадян, іноземців та осіб без громадянства, а також руху транспортних засобів» (п. 6 ч. 1 ст. 8 Закону);
- «перевірка у визначеному Кабінетом Міністрів України документів в осіб, а за потреби проведення огляду речей, транспортних засобів, багажу та вантажів, службових приміщень і житла громадян, за винятком обмежень, встановлених Конституцією України» (п.7 ч. 1 ст. 8 Закону).

Здійснення таких поліцейських заходів покладається насамперед на Національну поліцію, а також інші органи правопорядку та безпеки (включно з військовими формуваннями), які задіяні до реалізації правових обмежень в умовах воєнного стану.

Детальніше заходи, які можуть бути охарактеризовані як перевірки на блокпостах, визначені Постановою Кабінету Міністрів України «Про затвердження Порядку встановлення особливого режиму в'їзду і виїзду, обмеження свободи пересування громадян, іноземців та осіб без громадянства, а також руху транспортних засобів в Україні або в окремих її місцевостях, де введено воєнний стан» № 1455 від 29.12.2021 р.¹⁶ з подальшими змінами (надалі – Порядок № 1455) та Постановою Кабінету Міністрів України «Про затвердження Порядку перевірки документів в осіб, огляду речей, транспортних засобів, багажу та вантажів, службових приміщень і житла громадян під час забезпечення заходів правового режиму воєнного стану» № 1456 від 29.12.2021 р. (надалі – Порядок № 1456)¹⁷.

На блокпосту правоохоронці можуть:

- 1) перевіряти документи осіб;
- 2) оглядати речі;
- 3) оглядати транспортні засоби;
- 4) оглядати багаж та вантаж.

Варто зауважити, що Порядок № 1456 визначає проїзд транспортного засобу через блокпост підставою для його зупинки уповноваженою особою. Після зупинки машини особи водія та пасажирів можуть перевірити.

Визначення підстав для встановлення блокпостів, порядку їх функціонування та комплексу заходів, які можуть бути здійснені до осіб, у законодавстві України свідчить про те, що перевірки здійснюються відповідно до закону.

Перевірка документів передбачає право вимагати уповноваженою особою їх пред'явлення за наявності визначених підстав. Право на проведення перевірки документів в осіб, огляду речей, транспортних засобів, багажу та вантажів, службових приміщень і

¹⁶ Постанова Кабінету Міністрів України від 29.12.2021 №1455 «Про затвердження Порядку встановлення особливого режиму в'їзду і виїзду, обмеження свободи пересування громадян, іноземців та осіб без громадянства, а також руху транспортних засобів в Україні або в окремих її місцевостях, де введено воєнний стан» [Електронний ресурс] / Режим доступу: <https://zakon.rada.gov.ua/laws/show/1455-2021-%D0%BF#Text>

¹⁷ Постанова Кабінету Міністрів України від 29.12.2021 №1456 «Про затвердження Порядку перевірки документів в осіб, огляду речей, транспортних засобів, багажу та вантажів, службових приміщень і житла громадян під час забезпечення заходів правового режиму воєнного стану» [Електронний ресурс] / Режим доступу: <https://zakon.rada.gov.ua/laws/show/1456-2021-%D0%BF#Text>

житла громадян надано відповідним уповноваженим особам Національної поліції, Служби безпеки України, Національної гвардії, Держприкордонслужби, Державної міграційної служби, Держмитслужби та Збройних Сил, які визначені в наказі коменданта.

Важливо, що Порядком № 1456 визначений вичерпний перелік підстав, за яких відбувається пред'явлення документів і серед них відсутня «проїзд через блокпост». Водночас очевидним є те, що у переважній більшості випадків після зупинки транспортного засобу вимога пред'явити документи буде озвучена.

Для того, щоб вимагати документи уповноважена особа повинна керуватися однією з підстав, передбачених Порядком № 1456. Особливі питання виникають щодо пункту «якщо існує достатньо підстав вважати, що особа вчинила або має намір вчинити правопорушення». Незважаючи на закріплення цієї підстави у законі, людина фактично позбавлена гарантій від зловживань, оскільки нею можна виправдати будь-яку вимогу пред'явлення документів. Це може бути як суб'єктивне уявлення уповноваженої особи, що не підкріплено жодними достатніми підставами, або втілення іншої мети – наприклад, вручити повістку.

Водночас, проаналізувавши перевірку документів на предмет пропорційності, навряд вагомим аргументом стане те, що **вимога пред'явити документи була непропорційним втручанням у право на приватність в умовах воєнного стану**. Питання про свавільне втручання можуть постати, якщо перевірки документів відбувались неуповноваженою особою, документи вилучались та не повертались їх власнику або їх фотографували чи передавали третім особам. Крім того, втручанням у право на особисту свободу є заборона залишити блокпост після пред'явлення документів без пояснення причин та за відсутності підстав. Інший аспект стосується перевірок документів, що супроводжується запитаннями. Звичайно, не кожне питання на блокпосту автоматично призводить до посягання на право на приватність. Проте, надмірна цікавість уповноважених осіб і характер питань, що не стосуються виконання уповноваженим обов'язку та дозволяють йому досягти мети вже є втручанням у право на приватність¹⁸.

Під час огляду **транспортного засобу** уповноважена особа має право проводити поверхневу перевірку¹⁹, якщо:

- 1) існує достатньо підстав вважати, що у транспортному засобі перебуває правопорушник або особа, свобода якої обмежується в незаконний спосіб;
- 2) існує достатньо підстав вважати, що у транспортному засобі перебувають речі, обіг яких заборонено чи обмежено або які становлять загрозу життю чи здоров'ю такої особи або інших осіб;
- 3) існує достатньо підстав вважати, що речі, багаж, вантажі або транспортний засіб є знаряддям вчинення правопорушення та/або вони перебувають в тому місці, де може бути скоєно кримінальне правопорушення, для запобігання якого необхідно провести поверхневу перевірку.

¹⁸ Мезенцова Н. Перевірки на блокпостах: коли порушується право на приватність? // УГСПЛ, 08.02.2024 [Електронний ресурс] / Режим доступу: <https://www.helsinki.org.ua/articles/perevirky-na-blokpostakh-koly-porushuietsia-pravo-na-privatnist/>

¹⁹ Фактично це повторює підстави для проведення поверхневої перевірки поліцейським, що передбачені ст. 34 Закону України «Про Національну поліцію».

Поверхнева перевірка передбачає право уповноваженої особи вимагати відкриття кришки багажника та/або двері салону. Вміст особистих речей чи транспортного засобу людина повинна самостійно показати уповноваженій особі.

Критерій «достатніх підстав» не розкривається у законодавстві, що дає доволі широке поле для самостійного визначення їх уповноваженою особою. Добре, якщо це спирається на об'єктивні підстави, гірше коли уповноважені особи керуються виключно власними передчуттями або суб'єктивними факторами, що відкриває поле для потенційного свавілля.

Огляд транспортного засобу, речей чи багажу за своїм змістом та способом проведення характеризується як втручання в право на приватність. Перебування особи в публічному місці та взаємодія із представниками держави не виводить повністю цю взаємодію із сфери охоплення поняттям приватне життя. Більш того, проведення певних заходів саме у публічному місці може сприяти підвищенню дискомфорту. Поверхнева перевірка може призвести до того, що певні елементи приватного життя будуть продемонстровані публічно та побачені сторонніми глядачами, що може засоромити та принизити.

Для прикладу, у справі "Gillan and Quinton v. The United Kingdom"²⁰ ЄСПЛ встановив, що при проведенні обшуків у публічному місці ст. 8 Європейської конвенції з прав людини підлягає застосуванню. Суд наголосив, що у деяких випадках *публічний обшук може навпаки посилювати серйозність втручання через присутність елемента приниження та сорому.*

Захищаючи громадську безпеку та порядок, важливо дотримуватись балансу між публічними інтересами та приватним інтересом особи не зазнавати надмірного втручання в приватне життя.

Порядок № 1456 *не передбачає окремого права уповноважених осіб перевіряти на блокпосту телефони осіб на вміст інформації, що може становити загрозу національній безпеці.* Але з початку повномасштабного вторгнення це достатньо поширена практика, завдяки якій неодноразово виявлялись особи, у чиїх діях вбачалась колабораційна діяльність чи інші кримінальні правопорушення (ст. 111, 111-1, 111-2, 114-2 або 436-2 Кримінального кодексу України).

Уповноважені особи на блокпостах обґрунтовують перевірку телефонів обов'язком особи показати вміст особистих речей. Але існують великі сумніви, що це перетворює перевірку на таку, що відбувається відповідно до закону. І навіть наявність публічної мети не може стати виправданням для такого втручання.

У телефоні може зберігатись не лише інформація інтимного характеру, але і особисті листування, чутливі дані тощо, що підпадають під захист від свавільного втручання. Доступ до такої інформації повинен відбуватись відповідно до закону та узгоджуватись із захистом персональних даних. З метою захисту особи від свавілля перевірка вмісту телефону повинна здійснюватись у межах кримінального провадження – при наявності обґрунтованої підозри щодо особи і з дотримання вимог судового контролю за втручанням у права і свободи людини.

²⁰ CASE OF GILLAN AND QUINTON v. THE UNITED KINGDOM (Application no. 4158/05). 12.01.2020 [Електронний ресурс] / Режим доступу: <https://hudoc.echr.coe.int/?i=001-96585>

Варто зауважити, що виявлена інформація на телефоні може в майбутньому бути використана як доказ на підтвердження винуватості особи. Збирання доказів у межах кримінального провадження відбувається лише за встановленою процедурою, а до відкриття кримінального провадження може бути лише здійснено огляд місця події (ст. 237 КПК України). Водночас збір доказів, що призвів до порушенням прав і свобод людини або у випадках, прямо передбачених КПК України призводить до недопустимості таких доказів (ст. 86, 87 КПК України; Постанова Верховного Суду від 16.02.2022)²¹.

При цьому важливо, щоб передбачений законом огляд із правом проведення поверхневої перевірки не перетворився в обшук. Це відбувається за таких умов:

- 1) самостійне відкриття уповноваженою особою багажнику чи салону;
- 2) самостійне відкриття особистих речей, багажу та їх перевірка;
- 3) фізичне проникнення уповноваженої особи в салон транспортного засобу;
- 4) здійснення особистого обшуку особи;
- 5) вилучення та дослідження вмісту телефону тощо.

Суттєвою відмінністю від особистого огляду (в межах КПК України, наприклад під час затримання особи) є спосіб здійснення перевірки, а саме **візуальний огляд**. Тобто тактильний контакт особи з поліцейським відсутній, за винятком окремих випадків. Поліцейський оглядає лише те, що бачить або речі, що самостійно показуються особою. Тактильний контакт може мати місце тільки у вигляді проведення по поверхні одягу рукою, спеціальним технічним приладом (засобом), наприклад металошукачем тощо. Такий спосіб значно відрізняє його особистого огляду, під час якого поліцейський самостійно знаходить речі, оглядає їх тощо. На думку законодавця, візуальний огляд є значно меншим втручанням у приватне життя особи, тому обсяг гарантій є мінімальним²².

Відтак, якщо людина не заперечує і дозволяє такі дії, йдеться про недотримання уповноваженими особами процедури та свавільне втручання. Відмова людини від своїх прав не призводить до права агентів держави їх порушувати.

Обшук – це захід, що здійснюється у межах кримінального провадження у визначених випадках, за визначеною процедурою (ст. 234 КПК України). При цьому, повинні бути обґрунтовані підстави вважати, що особа вчинила кримінальне правопорушення. Недотримання під час проведення огляду положень ст. 34 Закону України «Про національну поліцію» щодо проведення поверхневої перевірки особи як превентивного поліцейського заходу, в результаті чого фактично здійснюється обшук особи, є підставою для визнання доказів недопустимими (Постанова Верховного Суду від 26.05.2021)²³.

²¹ Постанова ККС ВС від 16.02.2022 у справі №711/9435/19 / Режим доступу: <https://lpd.court.gov.ua/adjudication/7360>

²² Крапивін С. Особистий огляд та поверхнева перевірка: експертний аналіз // УМДПЛ, 18.05.2016 [Електронний ресурс] / Режим доступу: <https://umdpl.info/police-experts.info/2016/05/18/inspection/>

²³ Постанова ККС ВС від 26.05.2021 у справі 758/13581/15-к [] / Режим доступу: <https://lpd.court.gov.ua/adjudication/4388>

Особистий огляд особи, огляд речей, їх вилучення в межах процедури згідно з Кодексом України про адміністративні правопорушення повинен відбуватись у належному порядку із відповідною фіксацією (ст. 264 Кодексу України про адміністративні правопорушення).

Фактичне здійснення обшуку замість допустимого огляду – це свавільне втручання, що може визнаватись порушенням права на приватність.

Як зазначалось вище лише факт запровадження воєнного стану та необхідність забезпечення публічного інтересу не можуть бути підставою для виправдання будь-якого втручання. Окрім мети, аналізу підлягають такі складові, як здійснення на підставі закону та пропорційність втручання.

Комплекс заходів з проведення перевірок на блокпостах має підставу в законі, проте надто розмиті, неконкретні формулювання цих підстав можуть призвести до зловживання та свавілля.

Пропорційність втручання є елементом, що підлягає оцінці в кожній окремій ситуації, та дозволяє зробити висновок про доцільність втручання в тому обсязі, що застосовувався відповідно до переслідуваної мети. Якщо виконати завдання можна було з допомогою менш інтенсивного втручання та за рахунок менш обтяжливого заходу, то це свідчить про непропорційність, що призводить до порушення гарантованого права.

У ситуаціях із оглядом транспортних засобів, речей, багажу про непропорційність може свідчити спосіб проведення такого огляду, особисті обставини особи, тривалість, контекст, присутність великої кількості сторонніх осіб, поведінка представників держави в процесі огляду тощо²⁴.

Розв'язанням цієї проблеми могли б стати:

- зміни до законодавства, які б чіткіше визначали пропорційні випадки втручання у реалізацію права на приватність;
- формування правових позицій Верховного Суду з питань проведення поліцейських заходів та інших форм обмеження права на приватність;
- впровадження Стандартних операційних процедур (СОП), єдиних алгоритмів проведення перевірок на блокпосту для всіх органів влади, які залучаються до такого процесу з подальшим притягненням до дисциплінарної або кримінальної відповідальності у разі їх недотримання з причин, що полягають у невиконанні або неналежному виконанні службових обов'язків.

²⁴ Мезенцова Н. Перевірки на блокпостах: коли порушується право на приватність? // УГСПЛ, 08.02.2024 [Електронний ресурс] / Режим доступу: <https://www.helsinki.org.ua/articles/pervirky-na-blokpostakh-koly-porushuetsia-pravo-na-privatnist/>

2. Розвиток системи публічного відеоспостереження, зокрема із застосуванням технологій штучного інтелекту

2.1 Система відеоспостереження та право право на приватність

До 2022 року в Україні працювало понад 19 тисяч відеокамер з різним функціоналом, із яких більше третини – у столиці. Найбільші після Києва системи було встановлено в Одесі, Дніпрі, Львові та Харкові. Тим часом, камери розміщували у себе й невеличкі міста і селища, навіть села. Місцеві ради регулярно звітували про зростання муніципальних систем відеоспостереження, розширення функціоналу та плани їх подальшого повсюдного поширення. Ресурси на це виділяли місцеві ради, зазвичай у рамках місцевих бюджетних програм.

Такі системи дозволяли ефективніше встановлювати обставини вчинення кримінальних правопорушень та виконували значну превентивну функцію у сфері публічного порядку. Нагромаджені великі дані були у пригоді при плануванні транспортних потоків та в містобудуванні²⁵.

Водночас правове регулювання цього питання було і залишається слабким. Усі системи створювались децентралізовано, а державний регулятор у цій сфері був відсутній. Уповноважений Верховної Ради України з прав людини надавав «Рекомендації щодо дотримання права на приватність під час встановлення і використання систем відеоспостереження у громадських місцях» (2021)²⁶, проте їх юридична сила є м'якою, а отже орієнтування на них ОМС було мінімальним. Як наслідок передбачуваних правил щодо строку зберігання інформації, порядку її збору та обробки не було, а отже питання захисту персональної інформації стояло гостро.

Поліцейський відеомоніторинг зазнав суттєвого розширення за 2022-2024 роки в кількісному вимірі. Попри ризики воєнного часу в Україні продовжує діяти як система автоматичної фіксації порушень Правил дорожнього руху, так і окремі системи відеоспостереження в межах програм «Безпечне місто»²⁷. З певною періодичністю представники правоохоронних органів звітують у медіа про чергові досягнення вже впроваджених систем відеонагляду.

Так, щодо наслідків роботи дорожніх камер ідеться про 400 млн грн²⁷ сплачених штрафів до місцевих бюджетів за 10 місяців 2023 року, зниження аварійності ділянок з камерами²⁸, а також доцільність поступового збільшення їхньої кількості²⁹. Водночас сама система автоматичної фіксації порушень ПДР обмежена встановленням лише одного виду

²⁵ (Майже) Старший Брат стежить за тобою: відеоспостереження за дотриманням публічного порядку в Україні. Звіт за результатами дослідження, проведеного в січні-жовтні 2019 року // Упор. М. Каменів та С. Золотар. – К.: Асоціація УМДПЛ, 2019. – С. 35-36.

²⁶ Рекомендації Уповноваженого Верховної Ради України з прав людини щодо дотримання права на приватність під час встановлення і використання систем відеоспостереження у громадських місцях. Київ, 2021 [Електронний ресурс] / Режим доступу: <https://ombudsman.gov.ua/storage/app/media/%D0%97%D0%9F%D0%94/%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D1%96%D1%97%20%D1%89%D0%BE%D0%B4%D0%BE%20%D0%B4%D0%BE%D1%82%D1%80%D0%B8%D0%BC%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%B0%D0%B2%D0%B0%20%D0%BD%D0%B0%20%D0%BF%D1%80%D0%B8%D0%B2%D0%B0%D1%82%D0%BD%D1%96%D1%81%D1%82%D1%8C.pdf>

²⁷ У 2023 році камери зафіксували більше 2 мільйонів порушень ПДР // Закон і Бізнес, 16.11.2023 [Електронний ресурс] / Режим доступу: <https://zib.com.ua/ua/158740.html>

²⁸ У Дніпрі запрацюють дві камери автоматичної фіксації порушень правил дорожнього руху: де розташовані та який штраф // Суспільне. Дніпро, 27.04.2023 [Електронний ресурс] / Режим доступу: <https://susplne.media/dnipro/458154-u-dnipri-zapracuut-dvi-kameri-avtomatichnoi-fiksacii-porusen-pravil-doroznogo-ruhu-de-voni/>

²⁹ В Україні з 1 січня запрацюють ще 50 камер фіксації порушень ПДР // Суспільне новини, 01.01.2024 [Електронний ресурс] / Режим доступу: <https://susplne.media/651820-v-ukraini-z-1-sicna-zapracuut-se-50-kamer-fiksacii-porusen-pdr/>

порушень: перевищення швидкості (не враховуючи декілька камер у Києві, які додатково фіксують порушників на смузі громадського транспорту). Відеокамера самостійно заміряє швидкість руху та передає фото порушника до Центру обробки даних Національної поліції, де комп'ютер підтягує інформацію про порушника та формує протокол, а вже співробітник поліції його перевіряє та підписує.

Водночас системи відеоспостереження, встановлені в межах муніципальних програм «Безпечне місто», працюють за дещо іншим принципом. Більшість камер «Безпечного міста» є оглядовими та позбавлені додаткових функцій. Такі камери в цілодобовому режимі транслюють відео до інформаційних центрів, де відбувається запис та зберігання трансляції. Зазвичай інформаційні центри створюються на базі комунальних підприємств або на певних об'єктах, що потребують підвищеного рівня охорони, а територіальні підрозділи поліції забезпечують постійний доступ до камер і збережених записів. У такому разі поліцейські можуть отримати інформацію щодо обставин порушення або особи порушника лише постфактум. Малоймовірно, що поліцейський у прямому ефірі певної муніципальної відеокамери побачить, наприклад, крадіжку з вітрини вуличного магазину³⁰.

Загальнодоступність нових технологічних рішень у питанні розпізнавання облич дозволила муніципальним органам та поліції розвивати тему відеонагляду. Логічним кроком стала презентація поліцією Київської області в травні 2023 року системи публічної безпеки, оснащеної камерами з функцією розпізнавання облич та номерних знаків, а також аналітичним програмним забезпеченням, що дозволяє ідентифікувати осіб у режимі реального часу³¹.

В 2023 році МВС України продовжило працювати над розбудовою комплексних інтеграційних платформ відеоспостереження та повідомило, що їм вдалось інтегрувати в єдину платформу більше 8 тисяч відеокамер. «У планах – долучити всі понад 50 тисяч встановлених нині. В тому числі – більше 7 тисяч інтелектуальних» – зазначив міністр внутрішніх справ І. Клименко³².

З правового погляду такі новітні системи залишаються поза межами регулювання закону, а тому централізований контроль щодо їхнього впровадження відсутній. Як наслідок, уже в січні 2024 року журналісти «Схем» опублікували розслідування³³, в якому наголошили на пов'язаних зі шпигуванням та хакерськими атаками ризиках використання «розумних» камер і програмного забезпечення китайського походження, що встановлюють муніципальні органи в межах програм «Безпечне місто».

³⁰ Зеленчук В. Неочевидні загрози єдиній системі відеомоніторингу // Інститут масової інформації, 11.03.2024 [Електронний ресурс] / Режим доступу: <https://imi.org.ua/monitorings/neochevydni-zagrozy-yedynoyi-systemy-videmonitoryngu-i59814>

³¹ Новітня система відеонагляду з функцією розпізнавання облич: Поліція Київщини продемонструвала роботу інтегрованих камер // МВС України, 23.05.2023 [Електронний ресурс] / Режим доступу: <https://mvs.gov.ua/news/policiia-kiyivshhini-prodemonstruvava-robotu-integrovanix-kamer-z-funkciji-ru-rozpiznavannia-oblic>

³² Наразі ми інтегрували в єдину платформу більше 8 тисяч відеокамер, - Ігор Клименко // Урядовий портал, 26.12.2023 [Електронний ресурс] / Режим доступу: <https://www.kmu.gov.ua/news/narazi-my-intehruvaly-v-iedynu-platformu-bilshe-8-tysyach-videokamer-ihor-klymenko>

³³ Нагляд з Китаю. Як тисячі китайських камер відеоспостереження в Україні передають інформацію і чому це небезпечно // Радіо Свобода, 25.01.2024 [Електронний ресурс] / Режим доступу: <https://www.radiosvoboda.org/a/skhemy-kytayski-kamery-sposterezheniya-v-ukrayini/32791514.html>

Подібна історія мала місце раніше із програмним забезпеченням російського походження. Так, до 2019 року широко використовувались програмні продукти від російської компанії Аххон Soft, втім, у грудні 2018 року Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ звернувся до Асоціації міст України з листом³⁴ про припинення практики розгортання систем відеоспостереження на базі російського програмного забезпечення.

Щоб зменшити загрози хаотичного та безсистемного розвитку муніципальних програм безпеки, ініціативна група депутатів за участю Міністерства внутрішніх справ подала 20 лютого 2024 року до Верховної Ради законопроект №11031 від 20.02.2024 «Про єдину систему відеомоніторингу стану публічної безпеки». Детальніше про цей проект Закону див. нижче.

Окремо варто зазначити, що системи відеоспостереження починаються використовувати технології штучного інтелекту. Насамперед, технологію розпізнавання обличчя (ТРО), що може посилити порушення прав людини з боку поліції чи інших органів правопорядку, зокрема право на недоторканість приватного життя. У сфері правоохоронної діяльності обличчя людини використовують для перевірки і ідентифікації особи. Система включає в себе масовий моніторинг, збір, зберігання, аналіз конфіденційних персональних даних (біометричних даних) і використання матеріалів без обґрунтованої підозри у вчиненні кримінального правопорушення, що можна вважати невивірковим масовим наглядом.

В 2020 році була схвалена «Концепція розвитку штучного інтелекту в Україні»³⁵, метою якої є визначення основних завдань розвитку технологій штучного інтелекту для задоволення прав та законних інтересів фізичних та юридичних осіб. Метою Концепції задекларовано визначення напрямів розвитку ШІ для задоволення прав та інтересів людей, побудову конкурентоспроможної економіки та покращення публічного управління. Концепція визначила дев'ять пріоритетних сфер реалізації державної політики розвитку галузі ШІ, а саме: освіту, науку, економіку, кібербезпеку, оборону, інформаційна безпеку, державне управління, правове регулювання та етику, правосуддя. Одним із пріоритетних напрямів реалізації Концепції є «зайняття провідних позицій в світових рейтингах (AI Readiness Index by Oxford Insights, AI Index by Stanford University) до 2030 року». Однак цей документ не створює жодних юридичних зобов'язань та не встановлює конкретної юридичної відповідальності за неправомірне використання таких технологій.

В Законі України «Про захист персональних даних» не передбачений захист таких даних, як зображення облич, автоматично зібраних камерами відеоспостереження. Встановлення камер відеоспостереження в Україні регламентується місцевими органами влади, і не створює жодних юридичних прав та обов'язків. Це призводить до порушення права особи на приватність, що передбачено ст. 8 Закону України «Про захист персональних даних», відповідно до якої *суб'єкт персональних даних має право знати про джерела їх збирання, місцезнаходження та мету їх обробки*.

³⁴ (Майже) Старший Брат стежить за тобою: відеоспостереження за дотриманням публічного порядку в Україні. Звіт за результатами дослідження, проведеного в січні-жовтні 2019 року // Упор. М. Каменев та С. Золотар. – К.: Асоціація УМДПЛ, 2019. – С. 20.

³⁵ Розпорядження Кабінету Міністрів України від 02.12.2020 №1556-р «Про схвалення Концепції розвитку штучного інтелекту в Україні» [Електронний ресурс] / Режим доступу: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>

Перевагами застосування цієї технології є безпека (пошук злочинців, запобігання крадіжкам в магазинах, тощо), зручність, економія часу, простота використання. До того ж реальне розпізнавання обличчя допоможе правоохоронцям відшукати не лише ймовірних злочинців, а й, наприклад, без вісти зниклих осіб. В умовах війни Україна почала використовувати систему розпізнавання обличчя Clearview AI, яка застосовується в контексті протидії збройної агресії Росії і ідентифікації воєнних злочинців. «Україна використовує програмне забезпечення Clearview AI для розпізнавання облич, щоб ідентифікувати тіла російських солдатів, які загинули в бою, та інформувати їхні сім'ї про їх загибель» – повідомив міністр цифрової трансформації Михайло Федоров³⁶. Станом на кінець 2022 року компанія сприяла пошуку 125 тисяч осіб на території України.

Однак, використання штучного інтелекту може привести до порушення фундаментальних прав людини, закріплених в міжнародно-правових актах. Технології штучного інтелекту, подібні Clearview AI, здійснюють збір даних особи автоматично, без її інформування про цей процес та за відсутності згоди на обробку даних³⁷.

Загалом питання штучного інтелекту, його загроз та можливостей є дискусійним сьогодні в правничому середовищі. Наприклад, компанія Clearview AI, яка надає свої послуги Україні, зазнає значної критики серед міжнародної спільноти. Національні регулятори Італії, Австрії та Франції вже наклали санкції та багатомільйонні штрафи на компанію через порушення норм Загального регламенту про захист даних (General Data Protection Regulation, GDPR). Цим було фактично заморожено її діяльність на ринках держав-членів ЄС. Тож Україна в межах театру російсько-української війни надає компанії шанс перевірити та довести ефективність своїх розробок у ході практичного застосування³⁸.

Представники громадянського суспільства в Україні зазначають³⁹, що подальше використання технологій, заборонених на території деяких держав ЄС, може загальмувати або поставити під загрозу процес вступу України до ЄС. Експерти Лабораторії законодавчих ініціатив Анна Людва і Тетяна Авдеева серед головних ризиків застосування технологій Clearview AI виділяють: залежність від алгоритму через неучасть людини у верифікації рішення про ідентифікацію, виклики конфіденційності та недостатній захист даних від зловмисного втручання в цілому⁴⁰.

Хоча законодавство про захист персональних існує на рівні Європейського Союзу (насамперед GDPR⁴¹), а також в більшості європейських країн Європи, в Україні досі немає належного регулюючого законодавства і якісного підходу до роботи з такими технологіями.

³⁶ Андрощук Г. Україна використовує систему розпізнавання облич для ідентифікації вбитих російських солдатів // Юридична газета, 24.03.2022 [Електронний ресурс] / Режим доступу: <https://jur-gazeta.com/golovna/ukrayina-vikoristovue-sistemu-rozpiznavannya-oblich-dlya-identifikaciyi-vbitih-rosiyskikh-soldativ.html>

³⁷ Войнов М. Система розпізнавання обличчя: правові аспекти використання в Україні та в ЄС // УГСПЛ, 04.10.2023 [Електронний ресурс] / Режим доступу: <https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes/>

³⁸ Бойко Д., Городиський І. Штучний інтелект у сфері оборони: виклики регулювання // Центр Дністрянського, 12.01.2024 [Електронний ресурс] / Режим доступу: <https://dc.org.ua/news/shtuchnyy-intelekt-u-sferi-oborony-vyklyky-regulyuvannya>

³⁹ Bergengruen V. Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company // Time, 14.11.2023 [Електронний ресурс] / Режим доступу: <https://time.com/6334176/ukraine-clearview-ai-russia/>

⁴⁰ How "clear" is the legality of Clearview AI in Ukraine? // Digital Security Lab, 09.10.2023 [Електронний ресурс] / Режим доступу: <https://dslua.org/publications/how-clear-is-the-legality-of-clearview-ai-in-ukraine/>

⁴¹ General Data Protection Regulation – Загальний регламент про захист даних. Regulation (EU) 2016/679 [Електронний ресурс] / Режим доступу: <https://gdpr-text.com/uk/>

За останні роки Європейський суд з прав людини ухвалив низку рішень, пов'язаних з порушенням права на недоторканність приватного життя при застосуванні урядами заходів і процедур спостереження.

Знаковим в цьому аспекті є рішення ЄСПЛ у справі *«Сабо та Віші проти Угорщини»*⁴². В цій справі двоє громадян Угорщини оскаржували сумісність заходів спостереження, запроваджених в рамках антитерористичного законодавства Угорщини, з правом на недоторканність приватного життя. Заявники скаржилися на те, що до них потенційно можуть бути застосовані невиправдані та непропорційні заходи з метою нібито забезпечення національної безпеки, тому що Антитерористичне законодавство Угорщини дозволяло Службі національної безпеки здійснювати широкомасштабні таємні заходи спостереження – таємний запис розмов, розкриття листів і посилок, а також перевірку і запис змісту електронних повідомлень без відома або згоди осіб, за якими здійснюється спостереження.

Суд погодився із заявниками, визнавши, що мало місце порушення статті 8 Конвенції. За висновками Суду, заходи спостереження були надмірно широкими, не було проведено жодної оцінки необхідності такого спостереження і не було здійснено судового нагляду за цією діяльністю. Відповідно, виконавча влада необмежено втручалася в приватне життя громадян. Рішення ЄСПЛ у цій справі значною мірою підтвердило результати, досягнуті попередніми рішеннями Суду. Зокрема, воно вкотре підтвердило фундаментальну роль судової влади в оцінці необхідності та *пропорційності заходів масового спостереження, а також визнало зображення обличчя особи чутливою біометричною інформацією*.

Інше рішення – *«Глухін проти Росії»*⁴³ від 4 липня 2023 року. Ця справа стосувалася використання владою технології розпізнавання обличчя проти заявника після проведення ним одиночної демонстрації в столичному метро. Його ідентифікували та пізніше знайшли за допомогою технології розпізнавання обличчя після поїздки з картонною фігурою іншого протестувальника в повний ріст (справа якого привернула широку увагу ЗМІ), що тримав банер із написом: *«Мені загрожує до п'яти років... за мирні протести»*. Заявник стверджував, зокрема, що притягнення його до адміністративної відповідальності та використання технології розпізнавання обличчя під час обробки його особистих даних порушило його право на повагу до приватного життя та свободу вираження поглядів.

Звертаючись до загальних принципів, напрацьованих ЄСПЛ за статтею 8 Конвенції, цей Суд відзначив, що інституції Конвенції вважають, що моніторинг дій та переміщень фізичної особи в громадському місці за допомогою камери, яка не записувала візуальних даних, сам по собі не є формою втручання у приватне життя. Однак застереження щодо приватного життя можуть виникнути, щойно з'явиться будь-який систематичний або постійний запис таких персональних даних, зокрема фотографії ідентифікованої особи.

Аналізуючи питання наявності та пропорційності втручання у право заявника, ЄСПЛ зазначив, що законодавство держави-відповідача, зокрема положення чинного на час подій Закону «Про обробку персональних даних» відповідно до якого обробка персо-

⁴² CASE OF SZABÓ AND VISSY v. HUNGARY (Application no. 37138/14). 12.01.2016 [Електронний ресурс] / Режим доступу: <https://hudoc.echr.coe.int/fre?i=001-160020>

⁴³ CASE OF GLUKHIN v. RUSSIA (Application no. 11519/20). 04.07.2023 [Електронний ресурс] / Режим доступу: <https://hudoc.echr.coe.int/?i=001-225655>

нальних біометричних даних особи без її згоди була правомірною за умови «здійснення правосуддя, а також у випадках, передбачених законодавством з питань оборони, безпеки, боротьби з тероризмом, транспортної безпеки, боротьби з корупцією та оперативно-розшукової діяльності», на які посилався уряд як на правову підставу втручання у права заявника, були сформульовані занадто широко та не містили жодних обмежень щодо характеру ситуацій, які можуть призвести до використання технології розпізнавання обличчя, передбачуваних цілей, категорій людей, які можуть стати ціллю, або щодо обробки конфіденційних персональних даних. Крім того, уряд не посилався на будь-які процедурні гарантії, механізми наглядового контролю та доступні засоби правового захисту, що мали б супроводжувати використання технології розпізнавання обличчя в росії. Тобто національне законодавство навіть не передбачало фіксації в офіційних документах/базах повідомлення особи/громадськості про використання технології розпізнавання обличчя.

ЄСПЛ вважав заходи, вжиті до заявника, «особливо нав'язливими» тому, що вони стосувалися технології розпізнавання обличчя в реальному часі. Оброблені персональні дані містили інформацію про участь заявника в мирній акції протесту, а отже розкривали його політичні погляди. Відповідно, вони належали до спеціальних категорій конфіденційних даних, які потребують підвищеного рівня захисту. ЄСПЛ зауважив, що використання такої особливо нав'язливої технології для ідентифікації та арешту учасників мирних акцій протесту може мати негативний ефект щодо прав на свободу вираження поглядів і свободу зібрань.

За таких обставин використання технології розпізнавання обличчя для ідентифікації заявника не відповідало «нагальній суспільній потребі» та є несумісним з ідеалами й цінностями демократичного суспільства, керованого верховенством права, яке Конвенція покликана забезпечувати та підтримувати. ЄСПЛ дійшов висновку, що **використання технології розпізнавання обличчя в реальному часі без застосування належних законодавчо визначених процедурних гарантій та механізмів наглядового контролю становить порушення вимог статті 8 Конвенції про захист прав людини і основоположних свобод.**

Отже, в нових умовах мова йде не лише про розширення масштабів відеоспостереження, а й програмного забезпечення, що охоплює все більш зон приватності особи та є втручанням у реалізацію нею цього права. Швидкість розвитку механізмів штучного інтелекту, а також якість реагування на них в країнах ЄС та на рівні Європейського Союзу дає підстави серйозно ставитись до необхідності якнайшвидше врегулювати це питання, а не просто спостерігати за ростом масштабів систем відеоспостереження в Україні, навіть в умовах воєнного стану.

Відтак, **хоча законодавство у сфері персональних даних і не зазнало змін в умовах воєнного стану, проте виникли додаткові ризики для національної безпеки, що полягають у витоці персональних даних та неналежному використанні камер відеоспостереження, що встановлюються органами влади або органами місцевого самоврядування. Якщо раніше зволікання з правовим та організаційним вирішенням цього питання з боку держави не було пріоритетним, то наразі розширення і масштабування систем відеоспостереження має відбуватись із чітким встановленням юридичних механізмів захисту права на приватність.**

3. Законодавчі ініціативи щодо права на приватність: єдина система відеоспостереження та захист персональних даних

Цифрова трансформація сьогодні відбувається не тільки в соціальній сфері, а й правоохоронній. Очевидно, що війна в Україні підштовхнула до розвитку нових технологічних рішень щодо контролю за населенням. Надалі ще більше будуть розвиватися міські системи відеоспостереження, програми ідентифікації осіб за допомогою штучного інтелекту та біометричної інформації, багато інших напрямів, які стосуються оборони, публічної та національної безпеки. Усі ці технології працюють на основі даних. Якщо не буде сформована правильна політика, то в майбутньому можуть виникнути протести. Технології повинні розвиватися, але з урахуванням усіх загроз і правового поля⁴⁴.

Першим кроком до формування такої політики має бути нормативне врегулювання системи відеоспостереження та використання програмного забезпечення із застосуванням технології штучного інтелекту для ефективного функціонування в діяльності органів влади з одного боку, з іншого – гарантуванню захисту права на приватність.

3.1 Проєкт Закону №11031 щодо системи відеоспостереження

20 лютого 2024 року у Верховній Раді України зареєстровано проєкт Закону №11031 «Про єдину систему відеомоніторингу стану публічної безпеки»⁴⁵, яким пропонується створити єдину систему відеомоніторингу. Законопроєкт розроблено за участі Міністерства внутрішніх справ України на виконання пункту 259 Плану законопроєктної роботи Верховної Ради України на 2024 рік, затвердженого Постановою Верховної Ради України від 6 лютого 2024 року № 3561-ІХ⁴⁶.

Проєктом Закону передбачається унормування:

- єдиних функціональних та технічних вимог до побудови та функціонування систем відеомоніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів, відомчих систем відеомоніторингу підприємств, установ організацій (незалежно від форм власності) та фізичних осіб, установлених у публічних місцях, порядок доступу до інформації, а також складу відеоданих, метаданих, аналітичних даних, відеоархівів, сигналів тривоги, що створюються ними;

- забезпечення єдиних правил інформаційного обміну на державному, регіональному та місцевому рівнях між суб'єктами єдиної системи відеомоніторингу стану публічної безпеки через єдиний інформаційний простір з урахуванням розмежування прав доступу до інформації;
- захисту інформації, у тому числі персональних даних у системах відеомоніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів та відомчих системах відеомоніторингу підприємств, установ організацій (незалежно від форм власності) та фізичних осіб, установлених у публічних місцях.

⁴⁴ Шадська У. Захист персональних даних під час війни. Списки українців. Freerights Association. Київ, 2023. – С. 62.

⁴⁵ Проєкт Закону про єдину систему відеомоніторингу стану публічної безпеки (реєст. №11031 від 20.02.2024) [Електронний ресурс] / Режим доступу: <https://itd.rada.gov.ua/billInfo/Bills/Card/43733>

⁴⁶ Постанова Верховної Ради України №3651-ІХ від 06.02.2024 «Про План законопроєктної роботи Верховної Ради України на 2024 рік» [Електронний ресурс] / Режим доступу: <https://zakon.rada.gov.ua/laws/show/3561-20#Text>

Така система буде включати в себе камери з функціями детектування обличчя, охорони периметра, керування трафіком, визначення задимлення, вибухів, несанкціонованого залишення предметів. Система ідентифікуватиме фізичних осіб на основі біометричних даних, відцифрованого образу обличчя людини та інших персональних даних. Їх зберігатимуть не більш як 15 років, а після закінчення строку зберігання вони підлягатимуть знеособленню.

Людина, дані про яку внесуть до єдиної системи відеомоніторингу, зможе ознайомитися з ними, а також вимагати поновити й виправити інформацію про себе.

Крім людей, моніторити за допомогою цієї системи зможуть:

- транспортні засоби;
- публічні місця;
- об'єкти інфраструктури, зокрема парки, рекреаційні зони, сади, сквери та майданчики;
- пам'ятки культурної та історичної спадщини;
- вулиці, дороги, провулки, пішохідні та велосипедні доріжки;
- автомобільні стоянки та майданчики для паркування транспортних засобів, інші території загального користування;
- будівлі, споруди, в яких розташовані органи державної влади або органи місцевого самоврядування;
- та інші об'єкти.

У пояснювальній записці до проекту Закону вказують, що його метою є підвищення рівня публічної безпеки та порядку, а також запобігання можливим загрозам і контроль за усуненням наслідків надзвичайних ситуацій та правопорушень. До нової системи відеомоніторингу матимуть доступ лише органи влади.

Загалом проект закону започатковує створення єдиної системи відеомоніторингу під керівництвом Міністерства внутрішніх справ шляхом об'єднання різнорівневих програм відеонагляду, як-от камер ПДР, муніципальних систем безпеки, відеоспостереження на підприємствах і навіть камер фізичних осіб, що повністю або частково здійснюють відеомоніторинг публічних місць. Передбачається створення єдиного аналітичного центру на базі МВС, впровадження стандартів технічного та програмного оснащення, запровадження спільних правил доступу до інформації із системи, параметрів ідентифікації об'єктів та централізованого контролю за дотриманням законодавства. Тобто розв'язання згаданої у попередньому підрозділі проблеми з відсутністю єдиного державного регулятора та уніфікованих правил щодо реалізації системи відеонагляду, що гарантували б дотримання права на приватність осіб, дані стосовно яких збирає система.

Разом з тим законотворець заклав у положення проекту дещо більше, ніж просто об'єднання та унормування. Очевидно, що проект закону розроблявся за участю фахівців, які усвідомлюють перспективи подальшого розвитку системи відеоспостереження, зокрема шляхом застосування можливостей штучного інтелекту⁴⁷.

⁴⁷ Зеленчук В. Неочевидні загрози єдиної системи відеомоніторингу // Інститут масової інформації, 11.03.2024 [Електронний ресурс] / Режим доступу: <https://imi.org.ua/monitorings/neochevydni-zagrozy-yedynoyi-systemy-videomonitoringu-i59814>

Законопроект використовує поняття «метадані», тобто структуровані (за певними критеріями) дані про характеристики зафіксованих об'єктів з метою обліку, пошуку, оцінювання та управління такими даними. Фактично класифікація даних дозволить здійснювати пошук за певними характеристиками будь-якого об'єкта в реальному часі, якщо він перебуває в полі зору хоча б однієї з камер. Тобто йдеться не лише про ідентифікацію об'єкта в конкретний момент і в конкретному місці, але й про цілеспрямоване **стеження за ним або пошук зв'язків з іншими об'єктами за певними критеріями**.

У контексті зазначених термінів та задекларованої в законопроекті мети запобігання правопорушенням особливого значення набувають пропозиції ринку відеоаналітичних послуг. Навіть найперше пошукове посилання пропонує придбати платформу відеоаналітики в режимі реального часу, яка «виявляє та обробляє тимчасові просторові події», «співставляє дані для побудови можливих сценаріїв», «розпізнає вік, настрій, стать та етнічну приналежність людини». Звичайно, така система будується на основі штучного інтелекту.

Це при тому, що завдання системи не обмежуються системою кримінальної юстиції, тобто доступ до таких даних мають не лише органи правопорядку, а й розпорядники відомчих систем на підприємствах, в установах, організаціях (незалежно від форм власності) та приватні системи окремих фізичних осіб, якщо вони повністю або частково моніторять публічні місця. Тобто приватні особи зможуть і далі на власний розсуд збирати інформацію з камер спостереження, самостійно встановлених у публічних місцях, за умови, якщо поліція та муніципальні органи матимуть до них постійний доступ.

Фахівці Інституту масової інформації наводять приклади неоднозначного міжнародного досвіду який треба спочатку вивчити для того, щоб впроваджувати такі масштабні ризики, що несуть загрози для приватності людини.

Так, Лондонське метро в період із 2022 до 2023 року інтегрувало⁴⁸ штучний інтелект у систему безпеки однієї зі станцій. У результаті за один рік штучний інтелект сповістив про понад 44 тисячі випадків протиправної чи агресивної поведінки. Звісно, система припустилася низки помилок, неправильно інтерпретуючи людську поведінку, що підвищує ризик упередженого ставлення⁴⁹ та навіть дискримінації щодо уявних «порушників».

З іншого боку, місцева влада Стюбенвілла (штат Огайо, США), за версією містян⁵⁰, використовує посилений відеоконтроль, щоб знайти підстави для виселення мешканців з державних будинків. У цьому разі система відеонагляду, ймовірно, стала інструментом зловживання правом з боку правоохоронців, що є неприпустимим наслідком принципу «безпека понад приватність».

⁴⁸ London Underground Is Testing Real-Time AI Surveillance Tools to Spot Crime // Wired, 08.02.2024 [Електронний ресурс] / Режим доступу: <https://www.wired.com/story/london-underground-ai-surveillance-documents/>

⁴⁹ 'Immature biometric technologies could be discriminating against people' says ICO in warning to organisations // ICO. Information Commissioner's Office, 26.10.2022 [Електронний ресурс] / Режим доступу: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations/>

⁵⁰ MacMillan D. Eyes on the poor: Cameras, facial recognition watch over public housing // The Washington Post, 16.05.2023 [Електронний ресурс] / Режим доступу: https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/?utm_campaign=wp_post_most&utm_medium=email&utm_source=newsletter&wpisrc=nl_most&carta-url=https%3A%2F%2Fs2.washingtonpost.com%2Fcar-ln-tr%2F3a07371%2F6463a6d05dfb5222c4bcf9c7%2F629f57979110416a155db9bb%2F8%2F74%2F6463a6d05dfb5222c4bcf9c7

Поки Франція цього року планує продовжити⁵¹ започатковану Японією, Бразилією та Грецією традицію використання штучного інтелекту для відеоспостереження під час Олімпійських ігор, Європейська комісія вже майже третій рік доопрацьовує проєкт закону про штучний інтелект⁵², який забороняє системи біометричної ідентифікації в реальному часі в громадських місцях.

Загострення проблеми етичності використання штучного інтелекту в системах відеомоніторингу, зрештою, дістанеться і українського суспільства.

Зазвичай, щоб не спричиняти додаткової соціальної напруги та не порушувати звичної поведінки людей у громадських місцях, у будь-якій країні світу використання з боку державних установ та органів правопорядку відеомоніторингу на основі штучного інтелекту (чи без нього) відбувається приховано.

На противагу цьому автори законопроекту №11031 запропонували цікаве рішення: інформування про використання засобів запису за допомогою розміщення повідомлення на вході до зони їхнього використання на видному місці (ч. 4 ст. 6 проєкту Закону). Але в такому разі ефективність засобів спостереження суттєво знизиться.

Загалом законопроект розширює доступний поліції механізм відеоспостереження, а також відкриває громадянам доступ до ознайомлення з персональними даними, за якими цей механізм планує їх відстежувати

Тож фахівці Інституту масової інформації роблять висновок, що складається враження, ніби значна частина положень, яких він потребує, була пропущена. Зокрема, потребують додаткового регулювання питання:

- переліку видів та категорій даних, що можуть збиратися єдиною системою відеоспостереження, крім тих, що стосуються ідентифікації осіб та транспортних засобів;
- розумних меж збирання та аналізу інформації в межах цієї системи, враховуючи всі її складові;
- **гарантій недопущення порушення меж права на приватне життя** та стандартів захисту конфіденційних відомостей.

Поки ці та інші питання очікують на своє розв'язання, використання штучного інтелекту в українських системах відеомоніторингу на всіх рівнях залишатиметься поза межами регулювання, а тому умовний «цифровий поліцейський» обмежуватиметься лише волею розпорядників та власників цих систем.

⁵¹ Paris 2024 Olympics: Concern over French plan for AI surveillance / BBC, 19.07.2023 [Електронний ресурс] / Режим доступу: <https://www.bbc.com/news/world-europe-66122743>

⁵² The EU Artificial Intelligence Act. Up-to-date developments and analyses of the EU AI Act [Електронний ресурс] / Режим доступу: <https://artificialintelligenceact.eu/>. 13 березня 2024 року Європейський парламент затвердив цей документ за № P9_TA(2024)0138. Надалі Акт також має бути офіційно схвалений Радою ЄС та буде повністю застосовний через 24 місяці після набуття ним чинності (з урахуванням певних винятків).

Комітет Верховної Ради України з питань інтеграції України до Європейського Союзу надав **негативний висновок**⁵³ щодо цього законопроєкту, зазначивши, що він **суперечить цілям** Угоди про асоціацію та міжнародно-правовим зобов'язанням України, а також праву ЄС (acquis EU).

Фахівці Комітету зазначають, що найбільші ризики, пов'язані із впровадженням системи відеомоніторингу публічної безпеки, стосуються потенційних порушень широкого переліку прав людини у зв'язку зі здійсненням системою ідентифікації фізичної особи (право на повагу до приватного і сімейного життя, свобода вираження поглядів, свобода зібрань та об'єднання, заборона дискримінації, право на справедливий суд тощо).

Так, згідно з ч. 1 ст. 10 проєкту Закону ідентифікація інформаційних об'єктів у системах відеомоніторингу стану публічної безпеки здійснюється за визначеними цим Законом параметрами, з використанням технічних та програмних засобів.

В ч. 2 цієї статті вказано, що ідентифікація інформаційного об'єкта «фізична особа» здійснюється на підставі певного набору біометричних даних та такої інформації про особу: власне ім'я, дата народження/смерті, місце народження, стать, відомості про зареєстроване або задеклароване місце проживання (перебування) особи, зняття особи з реєстрації місця проживання або про зміну місця проживання (перебування) особи, відомості про громадянство або його відсутність, відцифрований образ обличчя особи, реєстраційний номер облікової картки платника податків або серія та номер паспортного документа особи (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків відповідно до закону).

З огляду на положення ст. 10 проєкту Закону йдеться, зокрема, і про застосування технологій ШІ з метою ідентифікації інформаційних об'єктів, оскільки саме алгоритми ШІ сьогодні мають технологічні можливості ідентифікувати фізичних осіб, зокрема, шляхом аналізу біометричних даних (обличчя, голос тощо).

В законопроєкті відсутні положення, які б дозволили сформулювати повне розуміння усіх етапів ідентифікації інформаційного об'єкта, що у свою чергу суперечить вищевказаному принципу прозорості обробки персональних даних. Не є зрозумілим, як працюватиме одна з **найчутливіших** функцій системи, а саме ідентифікація осіб шляхом обробки біометричних даних (наприклад, розпізнавання обличчя)⁵⁴.

Також невизначеним є питання про те, чи система відеомоніторингу не створюватиме або розширюватиме бази даних розпізнавання облич за допомогою нецільового (невибіркового) збирання зображень облич з мережі Інтернет чи записів камер відеоспостереження, що заборонено Актом про ШІ. Крім того, слід зауважити, що технології розпізнавання обличчя можуть працювати в режимі реального часу або ретроспективно. Зі змісту положень Акту про ШІ бачимо, що ЄС особливий акцент зробив на забороні ви-

⁵³ Висновок (експертиза щодо європейської інтеграції) у картці проєкту Закону №11031 від 20.02.2024 [Електронний ресурс] / Режим доступу: <https://itd.rada.gov.ua/billInfo/Bills/Card/43733>

⁵⁴ Загалом, існує три способи роботи технології розпізнавання обличчя: 1) верифікація – технологія порівнює одне обличчя з іншим конкретним зображенням; 2) ідентифікація – технологія порівнює одне обличчя з набором інших облич (біометричних шаблонів); 3) класифікація – технологія аналізує риси обличчя однієї чи кількох осіб за певними ознаками (усмішка, сміх, насуплени брови, колір шкіри та очей, будова черепа).

користання систем дистанційної біометричної ідентифікації «в режимі реального часу» в публічних місцях для правоохоронних цілей за винятком кількох ситуацій. Понад те, в Акті зазначено, що використання такої технології «в режимі реального часу» у виняткових випадках може здійснюватись лише з дотриманням певних умов: характер ситуації та наслідки використання системи для прав і свобод усіх зацікавлених осіб.

Щодо стандартів автоматичної обробки біометричних даних в рамках Ради Європи, то в Рекомендаціях щодо розпізнавання обличчя Консультативного комітету Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (далі – Конвенція 108+)⁵⁵ зазначено, що відповідно до ст. 6 Конвенції 108+ обробка спеціальних категорій даних, таких як біометричні дані, має бути дозволена, лише якщо така обробка ґрунтується на відповідній правовій основі та якщо додаткові та відповідні гарантії закріплено в національному законодавстві.

Відповідно до цих Рекомендацій законодавцю необхідно класифікувати різні випадки використання технології розпізнавання обличчя та створити правову базу для обробки біометричних даних за допомогою розпізнавання обличчя. Ця законодавча база повинна визначити для кожного способу використання технології розпізнавання таке:

- детальне пояснення щодо конкретного способу використання технології та цільового призначення;
- мінімальна надійність і точність використовуваного алгоритму;
- термін зберігання збережених фотографій;
- можливість перевірки (аудиту) цих критеріїв;
- простежуваність процесу;
- гарантії захисту проти порушень.

Згідно з Рекомендаціями правове регулювання, застосовне до обробки біометричних даних за допомогою розпізнавання обличчя, повинно враховувати та визначати таке: різні етапи використання технологій розпізнавання обличчя, включаючи етапи створення та розміщення бази даних; сектори, в яких використовуються ці технології; нав'язливість певних типів технологій розпізнавання обличчя (технології розпізнавання обличчя наживо або в записі), надаючи водночас чіткі роз'яснення щодо їх законності.

Враховуючи нав'язливість цих технологій, на етапі застосування технологій розпізнавання обличчя в неконтрольованому середовищі закон повинен забезпечити, щоб правоохоронні органи продемонстрували, що низка факторів, у тому числі місце та час застосування цих технологій, виправдовує особливу необхідність і пропорційність використання.

Ураховуючи наведене вище, можна стверджувати, що *законопроект не містить детального пояснення щодо функціонування системи ідентифікації фізичної особи; зміст запропонованих положень не дозволяє простежити процес ідентифікації; відсутні запобіжники щодо потенційних порушень та зловживань (наприклад, відсутність положень щодо незалежного*

⁵⁵ Guidelines on Facial Recognition (2021) [Електронний ресурс] / Режим доступу: <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-onfacial-recognition.html#>

наглядového органу, який би контролював функціонування системи моніторингу; відсутні механізми захисту зібраної інформації, а саме немає положень щодо технічних стандартів, які мають стати основою для запуску системи відеомоніторингу тощо).

Схожі висновки містять у висновках Комітету Верховної Ради України з питань цифрової трансформації (пропозиція – відхилити проект Закону) та ГНЕУ Апарату Верховної Ради України.

Відтак хоча питання нагальне і потребує законодавчого врегулювання, проте з огляду на невідповідність європейським стандартам щодо захисту персональних даних та непропорційне втручання у реалізацію громадянами права на приватність, не може бути ухвалений в такі редакції.

3.2 Проект Закону №8153 та №6177 щодо захисту персональних даних

На розгляді у Верховній Раді України перебуває проект Закону України «Про захист персональних даних» (реєст. №8153)⁵⁶, спрямований на приведення законодавства України у відповідність до європейських стандартів у сфері захисту персональних даних (Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)) та Модернізованої конвенції 108+.

Проектом Закону передбачається:

- визнати таким, що втратив чинність Закон України «Про захист персональних даних»;
- визначити такі терміни, як «персональні дані», «біометричні дані», «генетичні дані», «згода на обробку персональних даних», «знеособлення персональних даних», «обробка персональних даних», «порушення безпеки персональних даних» тощо;
- закріпити на законодавчому рівні принципи обробки персональних даних (законність, добросовісність та прозорість; обмеження мети; мінімізація та точність персональних даних; обмеження зберігання; підзвітність тощо);
- встановити підстави для обробки персональних даних з деталізацією щодо форми та вимог до згоди на обробку персональних даних (може бути подана у письмовій та електронній формі; шляхом обрання відповідних технічних налаштувань в інтерфейсі веб-сайта; через іншу ствердну дію чи поведінку);
- заборонити обробку чутливих персональних даних (про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в професійних спілках, а також генетичних та біометричних даних, даних, що стосуються здоров'я, статевого життя або сексуальної орієнтації);

⁵⁶ Проект Закону про захист персональних даних 8153 від 25.10.2022 [Електронний ресурс] / Режим доступу: <https://itd.rada.gov.ua/billInfo/Bills/Card/40707>

- врегулювати особливості обробки персональних даних роботодавцем, персональних даних, пов'язаних з притягненням до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості;
- отриманих для цілей журналістської чи творчої діяльності, в результаті аудіо, відео або фото фіксації публічних заходів, а також особливості обробки персональних даних після смерті суб'єкта персональних даних;
- визначити окремі аспекти обробки біометричних даних суб'єктами владних повноважень;
- встановити, що обробка персональних даних з іншою метою, ніж та, з якою вони збирались (первинна мета), забороняється, крім випадків, якщо нова мета є сумісною з первинною;
- закріпити права суб'єктів персональних даних (на інформацію, на виправлення, на забуття, на заперечення проти їх обробки, на захист від автоматизованого прийняття рішення, відшкодування шкоди тощо), а також обов'язки контролерів та операторів;
- зобов'язати контролера та оператора персональних даних призначити відповідальну особу з питань захисту персональних даних;
- запровадити Кодекс поведінки з питань захисту персональних даних;
- передбачити нові розміри штрафів за порушення законодавства у сфері захисту персональних даних.

У травні 2023 р. Верховна Рада України отримала правовий висновок експертів Ради Європи щодо законопроєкту реєстр. №8153. Упродовж 2023 р. відбулися секторальні обговорення законопроєкту, зокрема з представниками банківської та телекомунікаційної спільноти, державних органів, громадських об'єднань з метою вироблення узгодженої позиції.

При цьому ГНЕУ Апарату Верховної Ради України у своєму висновку зазначає, що проєкт Закону містить значну кількість положень, які не відповідають принципу правової визначеності («значний обсяг персональних даних», «значна кількість суб'єктів персональних даних», «короткий та зрозумілий суб'єкту персональних даних опис технології відстеження», «серйозні транскордонні загрози» тощо). Звертає увагу на неприйнятності запропонованих у ч. 12 ст. 52 проєкту положень, згідно з якими персональні дані, що стосуються суб'єкта персональних даних, уповноваженого на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень, не є конфіденційною інформацією і можуть бути відкриті третім особам. Акцентує увагу на наявності у проєкті невідповідності й неточності щодо обробки персональних даних правоохоронними та розвідувальними органами. Зокрема, надає зауваження до визначення терміну «правоохоронний орган» та наголошує на необхідності врахувати особливості обробки таких суб'єктів персональних даних, як особи, які притягаються до адміністративної відповідальності, особи, щодо яких здійснюється оперативно-розшукова діяльність, особи, щодо яких повинен вестися профілактичний облік тощо.

Відповідно до Правового висновку, підготовленого міжнародними експертами Ради Європи в межах проєкту Ради Європи «Підтримка впровадження європейських стандартів прав людини в Україні», передбачений проєктом Закону підхід досить близький до того, який виходить з європейських стандартів. У зв'язку з цим відзначається, що деякі положення відповідають Конвенції 108+ та GDPR, а також іншим відповідним стандартам, і не потребують поправок. При цьому, деякі положення проєкту рекомендується переглянути, уточнити або внести до них правки, щоб гарантувати їх відповідність європейським стандартам і, зокрема, Конвенції 108+ і GDPR.

Наразі профільний Комітет Верховної Ради України з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій України, національних меншин і міжнародних відносин ухвалив рішення рекомендувати Верховній Раді України проєкт Закону України про захист персональних даних, реєстр. № 8153 від 25.10.2022, поданий народним депутатом України Стефанчуком Р.О. та іншими народними депутатами України, за наслідками розгляду в першому читанні прийняти за основу з урахуванням необхідності, відповідно до ч. 1 ст. 116 Регламенту Верховної Ради України, внесення пропозицій і поправок щодо виправлень, уточнень, усунення помилок та/або суперечностей у тексті законопроєкту, інших структурних частин законопроєкту та/або інших законодавчих актів, що не були предметом розгляду в першому читанні та відповідають предмету правового регулювання законопроєкту. Проєкт Закону очікує на розгляд Парламентом.

Крім того, у Верховній Раді України зареєстровано проєкт Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» (реєстр. № 6177)⁵⁷, який передбачає створення нового контролюючого органу у сфері захисту персональних даних та визначає статус, повноваження, принципи організації та порядок діяльності цього органу.

⁵⁷ Проєкт Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації №6177 від 18.10.2021 [Електронний ресурс] / Режим доступу: <https://itd.rada.gov.ua/billInfo/Bills/Card/27996>

III. РЕАГУВАННЯ НА НЕЗАКОННЕ ВТРУЧАННЯ У РЕАЛІЗАЦІЇ ПРАВА НА ПРИВАТНІСТЬ

1. Реагування з боку Уповноваженого Верховної Ради України з прав людини

1.1 Виконання контрольних функцій у сфері захисту персональних даних

Відповідно до ст. 22 Закону України «Про захист персональних даних» контроль за додержанням законодавства про захист персональних даних здійснюють такі органи як Уповноважений Верховної Ради України з прав людини та суди. З огляду на це 25 травня 2022 року Уповноважений видав Роз'яснення щодо захисту персональних даних в умовах воєнного стану⁵⁸.

Попри вживання в назві предмету роз'яснення – «в умовах воєнного стану» – в ньому радше наголошується на тих вимогах законодавства, що існували і раніше. А саме інформація щодо обмежень прав людини та правових підстав для обробки персональних даних державними органами (пункт 1); щодо обов'язків володільців та розпорядників персональних даних стосовно забезпечення захисту персональних даних (пункт 2); щодо правових підстав для обробки персональних даних підприємствами, установами і організаціями приватної форми власності, фізичними особами – підприємцями, фізичними особами, що провадять незалежну професійну діяльність з метою надання адресної благодійної допомоги громадянам, які постраждали від військової агресії (пункт 3); щодо захисту своїх персональних даних від кіберзлочинців (пункт 4) та шахрайських дій (пункт 5) та в умовах тимчасової окупації (пункт 6).

За винятком останніх п. 4,5,6, які принаймні стосуються нових викликів у сфері злочинності та загроз для безпеки даних з огляду на прямі наслідки збройної агресії, більша частина документу стосується загальних положень щодо дотримання законодавства у сфері захисту персональних даних та не містить жодних винятків чи послаблень з урахуванням умов воєнного стану.

1.2 Реагування на звернення громадян щодо порушення права на приватність

До Уповноваженого як контрольного органу у сфері захисту персональних даних також звертаються громадяни із заяви про порушення їхнього права на приватність. У 2022 році 60% таких повідомлень стосувались незаконної обробки персональних даних; 28% – права на доступ до інформації щодо себе; 12% – відсутності повідомлення щодо організації обробки персональних даних⁵⁹.

⁵⁸ Рекомендації Уповноваженого щодо захисту персональних даних в умовах воєнного стану // Уповноважений ВРУ з прав людини, 25.05.2022 [Електронний ресурс] / Режим доступу: https://ombudsman.gov.ua/news_details/rekomendaciyi-upovnovazhenogo-shchodo-zahistu-personalnih-danih-v-umovah-voyennogo-stanu

⁵⁹ Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2022 році [Електронний ресурс] / Режим доступу: <https://ombudsman.gov.ua/report-2022/>

Наприклад, до Уповноваженого Верховної Ради України з прав людини звернувся⁶⁰ заявник Р. щодо стверджуваного порушення його права на приватність посадовою особою товариства з обмеженою відповідальністю, яке займається комплексним обслуговуванням об'єктів житлових будинків в м. Львів.

Заявник повідомив, що було допущено розголошення його персональних даних (конфіденційної інформації) шляхом поширення у чаті групи месенджеру «Viber» фотокопій документів (кореспонденції), що містять персональні дані заявника.

Крім того, також було спричинено неправомірне втручання у приватне життя заявника шляхом поширення фото із його зображенням та зазначенням інформації про його місце проживання на офіційній сторінці зазначеного товариства в соціальній мережі «Facebook».

За даними фактами оприлюднення персональних даних відділом дізнання Львівського районного управління поліції № 1 ГУНП у Львівській області відкрито кримінальне провадження за ч. 1 ст. 182 Кримінального кодексу України «Порушення недоторканості приватного життя» для перевірки щодо законності зберігання, використання, поширення конфіденційної інформації про особу.

Інший приклад – до Уповноваженого Верховної Ради України з прав людини звернувся⁶¹ заявник Д. щодо стверджуваних неправомірних дій одного з працівників психоневрологічного інтернату, що призвело до порушення права на приватність інших осіб.

Заявник повідомив, що всупереч вимогам законодавства про захист персональних даних було допущено розголошення персональних даних (конфіденційної інформації) підопічних інтернату шляхом поширення у мережі Інтернет відеозапису, на якому їх зображено.

У зв'язку з тим, що відомості стосовно стверджуваних у зверненні неправомірних дій з боку службової особи інтернату містили ознаки кримінального правопорушення, до Національної поліції України було направлено відповідний лист для перевірки викладених у зверненні фактів.

За даними фактами оприлюднення персональних даних, сектором дізнання Уманського районного управління поліції ГУНП в Черкаській області відкрито кримінальне провадження за частиною першою статті 182 Кримінального кодексу України «Порушення недоторканості приватного життя» для перевірки щодо законності зберігання, використання, поширення конфіденційної інформації про особу.

З огляду на зміст таких звернень та результатів реагування за ними можна зробити висновок, що вони стосуються регулярного реагування Уповноваженого на випадки порушення права на приватність, що не пов'язано із обмеженнями прав і свобод людини, впровадженими у зв'язку із введенням в Україні правового режиму воєнного стану.

⁶⁰ Вжито заходів реагування через втручання у приватне життя особи та збір і поширення про неї персональних даних // Уповноважений ВРУ з прав людини, 08.03.2023 [Електронний ресурс] / Режим доступу: https://www.ombudsman.gov.ua/news_details/vzhito-zahodiv-reaguvannya-cherez-vtruchannjam-u-privatne-zhittya-osobi-ta-zbir-i-poshirennya-pro-neyi-personalnih-danih

⁶¹ Втручання у приватне життя осіб та збір і поширення про них персональних даних: Офісом Омбудсмена вжито заходів реагування // Уповноважений ВРУ з прав людини, 24.03.2023 [Електронний ресурс] / Режим доступу: https://www.ombudsman.gov.ua/news_details/vtruchannya-u-privatne-zhittya-osib-ta-zbir-i-poshirennya-pro-nih-personalnih-danih-ofisom-ombudsmana-vzhito-zahodiv-reaguvannya

На вебсайті Уповноваженого чи у матеріалах, до підготовки яких дотичний цей орган влади не вдалось знайти інформації про скарги чи реагування, предметом яких є обмеження, впровадженні саме у зв'язку із воєнним станом.

В Щорічній доповіді Уповноваженого ВРУ з прав людини за 2022 рік⁶² право на приватність згадується лише в контекст протиправного його обмеження у зв'язку із практикою здійснення «фільтраційних заходів» на тимчасово окупованій території (С. 34-36), викликами у сфері кіберзахисту (С. 203-204), а також неналежних умовах розміщення внутрішньо переміщених осіб або людей, які перебувають у місцях несвободи (наприклад, у системі МОЗ, МОН та Міноборони) (С. 165-168).

Аналогічна структура згадки про право на приватність у Щорічній доповіді Уповноваженого ВРУ з прав людини за 2023 рік⁶³: неналежні умови тримання в установах (місцях несвободи) (С. 169-170, С. 183); шахрайські дії з персональними даними, кібератаки (кількість яких зросла на 62,5% порівняно з попереднім 2022 роком) (С. 219) тощо.

2. Реагування органів правопорядку (кримінальний аспект)

Статтею 32 Конституції України передбачено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

За незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу передбачена кримінальна відповідальність ст. 182 КК України «Порушення недоторканності приватного життя».

Фактично це єдина підстава для кримінальної відповідальності у тих випадках, які є предметом розгляду цієї публікації (питання дотримання лікарської, банківської чи іншої таємниці ми не беремо до уваги з міркувань, вказаних у методології).

Відповідно до даних кримінальної статистики⁶⁴, розпорядником яких є Офіс Генерального прокурора, досудове розслідування випадків порушення цього права є таким:

⁶² Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2022 році [Електронний ресурс] / Режим доступу: <https://ombudsman.gov.ua/report-2022/>

⁶³ Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2023 році [Електронний ресурс] / Режим доступу: https://ombudsman.gov.ua/storage/app/media/uploaded-files/%D0%A9%D0%BE%D1%80%D1%96%D1%87%D0%BD%D0%B0%D0%B4%D0%BE%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D1%8C_%D0%A3%D0%BF%D0%BE%D0%B2%D0%BD%D0%BE%D0%B2%D0%B0%D0%B6%D0%B5%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0_2023_%D1%80%D1%96%D0%BA.pdf

⁶⁴ Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування // Офіс Генерального прокурора [Електронний ресурс] / Режим доступу: <https://gp.gov.ua/ua/posts/pro-zarejestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>

Статистичні дані щодо досудового розслідування кримінальних правопорушень за ст. 182 КК України «Порушення недоторканності приватного життя»

Рік	Кількість зареєстрованих проваджень	Кількість повідомлень про підозру	Кількість проваджень, в яких обвинувальний акт скеровано до суду
2022	164	47	23
2023	422	175	163
2024 (1 кв.)	202 (прогнозовано за рік – 808)	52 (прогнозовано за рік – 408)	43 (прогнозовано за рік – 172)

На жаль, структуру складів кримінальних правопорушень встановити неможливо. Припускаємо, що суттєвий ріст кількості кримінальних проваджень у 2023 році пов'язаний радше з нормалізацією функціонування органів влади, відсутності потреби в людей вирішувати базові безпекові потреби та більше усвідомлення функціонування юридичних механізмів захисту своїх прав.

Водночас ріст кількості кібератак, зокрема за участі держави-агресора теж вплинув на зростання кількості зареєстрованих злочинів. Водночас виокремити випадки порушення права на життя в межах кримінального процесу, застосування поліцейських заходів чи інших випадків, які є предметом цієї публікації, не видається можливим.

3. Судова практика

Відповідно до даних судової статистики⁶⁵, розпорядником якої є Державна судова адміністрація, кількісні дані щодо розгляду обвинувальних актів за ст. 182 КК України є такими: за 2022 рік до суду надійшло 19 проваджень, в 3 з яких постановлено обвинувальний вирок; за 2023 рік до суду надійшло 24 провадження, в 6 з яких постановлено обвинувальний вирок.

Невідповідність кількості скерованих обвинувальних актів до суду органами прокуратури кількості справ, що надійшли на розгляд суду пояснюється різними підходами до ведення статистичних даних в системі прокуратури (на даних ЄРДР) та судової влади. Така проблема присутня щодо всіх кримінальних правопорушень і не дає змоги об'єктивно дослідити стан справ щодо здійснення правосуддя.

Важливішим є контентний аналіз таких проваджень – вироків судів, що набрали законної сили. Так, відповідно до даних Єдиного державного реєстру судових рішень за період з 01 січня 2022 року до 05 квітня 2024 року наявні дані щодо 7 вироків, що набрали законної сили. Ще 3 вироків (за березень-квітень 2024 року) – ще не набрали законної сили.

⁶⁵ Судова статистика. Судова влада України [Електронний ресурс] / Режим доступу: https://court.gov.ua/inshe/sudova_statystyka/

Ці вироки стосуються таких випадків:

- незаконне стеження за приватним життям особи (засуджено до штрафу 10600 грн, звільнено від покарання у зв'язку із закінченням строків давності)⁶⁶;
- незаконне поширення конфіденційної інформації про особу (поширення даних паспорту з шахрайською метою) (засуджено до обмеження волі на строк 3 роки, затверджено угоду про примирення)⁶⁷;
- незаконне поширення фотографій інтимного характеру, зроблених без згоди особи (засуджено до штрафу 8500 грн)⁶⁸;
- використання персональних даних для оформлення кредитування на підставну особу (поєднане з шахрайством) (засуджено до 2 років обмеження волі)⁶⁹;
- поширення персональних даних у соціальній мережі, зокрема щодо місця проживання, публікація фотографій образливого змісту тощо (засуджено до штрафу 4250 грн)⁷⁰;
- правоохоронці під час санкціонованого обшуку отримали доступ до персональних даних, фотографій та інших предметів приватного життя, які потім поширювали у соціальних мережах та месенджерах без згоди особи (засуджено до штрафу 8500 грн)⁷¹;
- незаконне встановлення прихованої прослуховуючої апаратури для збору відомостей про приватне життя потерпілої особи (засуджено до штрафу 11050 грн)⁷².

Отже, контентний аналіз вищенаведених судових рішень дозволяє дійти висновку, що переважна більшість наведених випадків стосуються приватних стосунків між фізичними особами, а відповідальність настала за порушення їх суб'єктивних прав. Лише в одному випадку мова йде про зв'язок між представниками органів влади в кримінальному процесі та порушенні об'єктивних прав потерпілої особи. Водночас це не стосується правових обмежень, впроваджених у зв'язку із воєнним станом або умов воєнного стану як таких.

⁶⁶ Рішення Ковельського міськрайонного суду Волинської області у справі № 159/4835/19 від 07.03.2023 [Електронний ресурс] / Режим доступу: <https://reyestr.court.gov.ua/Review/102951854>

⁶⁷ Рішення Нововолинського міського суду Волинської області у справі № 165/322/22 від 27.04.2022 [Електронний ресурс] / Режим доступу: <https://reyestr.court.gov.ua/Review/104087021>

⁶⁸ Рішення Святошинського районного суду м. Києва у справі № 759/1149/23 від 24.01.2023 [Електронний ресурс] / Режим доступу: <https://reyestr.court.gov.ua/Review/108571346>

⁶⁹ Рішення Залізничного районного суду м. Львова у справі № 462/4731/23 [Електронний ресурс] / Режим доступу: <https://reyestr.court.gov.ua/Review/111810181>

⁷⁰ Рішення Шевченківського районного суду м. Чернівці у справі № 727/4263/23 [Електронний ресурс] / Режим доступу: <https://reyestr.court.gov.ua/Review/111962549>

⁷¹ Рішення Першотравневого районного суду м. Чернівці у справі № 727/2632/22 [Електронний ресурс] / Режим доступу: <https://reyestr.court.gov.ua/Review/112507141>

⁷² Рішення Хмельницького міськрайонного суду Вінницької області у справі № 149/1/22 [Електронний ресурс] / Режим доступу: <https://reyestr.court.gov.ua/Review/114007842>

ВИСНОВКИ

За результатами проведеного аналізу можна ствердно сказати, що інформації для відстеження тенденцій у сфері дотримання права на приватність особи в умовах воєнного стану недостатньо. Ймовірно масштаб таких випадків не такий значний порівняно із іншими засадничим правами і свободами людини, тому про нього на рівні медіа, позицій органів влади та статистичних даних небагато.

Водночас в умовах воєнного стану запроваджено обмеження реалізації особами прав і свобод людини; право на приватність – не виняток. Так, у сфері кримінального провадження послаблено судовий контроль за дотриманням права на приватність в окремих випадках; поліцейські та інші працівників органів правопорядку отримали більше законних можливостей до доступу до приватних даних з метою надання відсічі збройній агресії та запобігання загрозам національній безпеці, а ті тенденції, що мали місце раніше, наприклад поширення системи публічного відеоспостереження в умовах воєнного стану несуть нові ризики.

Наразі важко ствердно сказати, що рівень захисту права на приватність з боку держави знизився чи покращився у зв'язку із впровадженням воєнного стану. З одного боку очевидного погіршення у цій сфері немає, з іншого – повага до цього права та усвідомлення громадянами про необхідність його захисту як залишалась на невисокому рівні, так і залишається. Це стає проблемним в умовах євроінтеграційних процесів. Нещодавні законодавчі ініціативи щодо публічного відеоспостереження та впровадження нового Закону про захист персональних даних демонструють наскільки високими є вимоги стандартів ЄС у сфері захисту персональних даних і наскільки складно адаптувати українське законодавство для них. Це один із тих викликів про які мало говорять, але їх подолання вимагає переосмислення ставлення до «серйозності» права на приватність.

Врешті більшість загроз сьогодні пов'язані із зовнішнім чинником (кібератаками з боку держави-агресора, ростом шахрайства та кіберзлочинності серед криміналітету тощо), аніж внутрішніми (обмеження в реалізації права на приватність з боку органів влади).

РЕКОМЕНДАЦІЇ

Верховній Раді України:

- з огляду на євроінтеграційні процеси враховувати фахові висновки інституцій, що спеціалізуються на захисті права на приватність під час законодавчого процесу;
- **внести** зміни до законодавства України щодо захисту персональних даних, а саме ухвалити новий Закон України «Про захист персональних даних» з метою приведення його у відповідність до вимог Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенції 108+) та GDPR (Загальний регламент про захист даних), а також посилення механізмів захисту персональних даних як необхідних кроків щодо гармонізації українського законодавства та законодавства Європейського Союзу у цій сфері;
- **обмежити** дискрецію правоохоронних органів щодо огляду ними телефонів громадян під час дії воєнного стану задля уникнення можливих порушень щодо таких видів інформації, як адвокатська, медична таємниця чи інших видів таємниць;
- **встановити** чіткі законодавчі рамки використання технологій штучного інтелекту з попереднім аналізом їх впливу на права людини (зокрема, правила видалення персональних даних після закінчення воєнного часу, можливості оскарження рішень системи тощо).
- **врегулювати** питання застосування штучного інтелекту з метою ідентифікації осіб – розпізнавання облич, перевірки автентичності документів тощо, а також статус отриманої внаслідок застосування таких технологій інформації для обмеження прав людини (затримання чи арешту або ж доказів у судовому провадженні тощо);

Офісу Генерального прокурора:

- **публікувати** дані щодо перебирання прокурором на себе повноважень і судового контролю в порядку, встановленому ст. 615 КПК України, зокрема із зазначенням форм такого судового контролю та рішень, що приймаються;
- **реагувати** на всі випадки безпідставного перебирання прокурорів на себе повноважень слідчого судді, суду, зокрема Генеральні інспекції впровадити форми контролю за такими діями для виявлення випадків порушень кримінального процесуального законодавства;

Міністерству цифрової трансформації України:

- **розробити** технічні стандарти щодо технологій штучного інтелекту, які можна застосовувати в Україні в період воєнного стану, порядок залучення іноземних технологій для державних потреб та способів їх імплементації.
- **сприяти** поширенню інформації щодо цифрової безпеки та цифрових навичок, особливо для вразливих категорій користувачів (громадяни на окупованих територіях, військовослужбовці);

Міністерству внутрішніх справ та Національній поліції:

- **проводити** роз'яснювальні роботи з особовим складом щодо випадків, коли правоохоронці чи військовослужбовці можуть здійснювати огляд телефона на предмет зйомки заборонених об'єктів та локацій, яких саме локацій це стосується та в якому порядку такий огляд має здійснюватися (зокрема, з рук, без вилучення девайсів тощо);
- **розробити** та впровадити Стандартні операційні процедури (СОП) щодо проведення перевірок, оглядів, поверхневих перевірок та інших форм обмеження права на приватність осіб, які перетинають блокпости або до яких застосовуються поліцейські заходи з інших підстав;
- **поширити** позитивний досвід застосування цих СОП на інші правоохоронні органи та військові формування з метою дотримання єдиних стандартів гарантування права на приватність осіб, стосовно яких застосовуються поліцейські заходи в умовах воєнного стану;

Уповноваженому Верховної Ради України з прав людини:

- **розширити** підрозділ Щорічного звіту про дотримання інформаційних прав комплексного огляду права на приватність;
- **розробити** і створити окремий підрозділ розділу «воєнний стан» на вебсайті з публікацією статистичних даних про порушення прав людини у зв'язку із воєнним станом та результатами реагування на них.

