УДК 342.721:351.74:004.9
DOI https://doi.org/10.32782/2709-9261-2026-2-18-19



Ріжняк Ренат Ярославович,
доктор історичних наук, професор,
завідувач кафедри загальноправових дисциплін
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0002-1977-9048



Коссе Валерій Валерійович,
доктор філософії в галузі 08 «Право», майор поліції,
декан факультету підготовки фахівців
для органів досудового розслідування Національної поліції України
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0002-6576-0620



Пронін Юрій Олександрович,
адвокат
ORCID: https://orcid.org/0009-0004-6363-0824

КОНСТИТУЦІЙНІ ГАРАНТІЇ ПРАВА НА ПРИВАТНІСТЬ ПІД ЧАС ВИКОРИСТАННЯ ПОЛІЦІЄЮ ЦИФРОВИХ ТЕХНОЛОГІЙ В УМОВАХ ВОЄННОГО СТАНУ: МЕХАНІЗМИ КОНТРОЛЮ

Статтю присвячено дослідженню конституційних гарантій права на приватність під час використання Національною поліцією України цифрових технологій в умовах воєнного стану. Проаналізовано національні та міжнародні стандарти захисту приватності, особливості застосування інформаційних систем, відеоспостереження, біометричних технологій і електронних реєстрів. Обґрунтовано необхідність забезпечення балансу між інтересами національної безпеки та правами людини. Запропоновано напрями вдосконалення механізмів конституційного, судового, парламентського, громадського й внутрішньовідомчого контролю за використанням цифрових технологій у діяльності поліції.

Ключові слова: *право на приватність, цифрові технології, Національна поліція України, воєнний стан, персональні дані, конституційні гарантії, механізми контролю.*

© Ріжняк Р. Я., Коссе В. В., Пронін Ю. О., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Постановка проблеми. Стрімкий розвиток цифрових технологій суттєво трансформує сучасну діяльність правоохоронних органів. Інформаційно-комунікаційні системи, електронні реєстри, засоби відеоспостереження, системи відеоаналітики, технології розпізнавання облич, мобільні додатки та інші цифрові інструменти дедалі активніше використовуються Національною поліцією України для забезпечення публічної безпеки, протидії злочинності та підтримання правопорядку. Особливого значення такі технології набули після запровадження правового режиму воєнного стану, коли перед державою постала необхідність оперативного реагування на безпекові загрози, виявлення диверсійних груп, документування воєнних злочинів, здійснення контролю за дотриманням спеціальних режимних обмежень та захисту критичної інфраструктури.

Разом із тим розширення цифрових можливостей правоохоронних органів актуалізує питання забезпечення конституційних прав і свобод людини, насамперед права на приватність. Відповідно до статті 32 Конституції України ніхто не може зазнавати втручання в особисте і сімейне життя, крім випадків, передбачених Конституцією України. Також гарантується захист конфіденційної інформації про особу та встановлюються конституційні обмеження щодо збирання, зберігання, використання і поширення персональних даних. В умовах цифровізації правоохоронної діяльності зазначені гарантії набувають нового змісту, оскільки значна частина інформації про особу існує саме в електронній формі та може оброблятися автоматизованими інформаційними системами.

Проблематика захисту права на приватність особливо загострюється в умовах воєнного стану. З одного боку, держава об'єктивно потребує додаткових інструментів забезпечення національної безпеки, які передбачають використання цифрових технологій для моніторингу ситуації, збору інформації та оперативного реагування на загрози. З іншого боку, розширення повноважень правоохоронних органів не повинно призводити до необґрунтованого обмеження конституційних прав людини або формування практики надмірного державного контролю. Саме тому особливого значення набуває пошук балансу між потребами безпеки держави та необхідністю збереження фундаментальних прав і свобод особи.

Важливим елементом такого балансу виступають механізми контролю за діяльністю правоохоронних органів. У демократичній правовій державі використання поліцією цифрових технологій повинно супроводжуватися ефективною системою конституційного, судового, парламентського, громадського та внутрішньовідомчого контролю. Саме ці механізми покликані забезпечити відповідність діяльності правоохоронних органів принципам верховенства права, законності, пропорційності та поваги до людської гідності.

Аналіз останніх досліджень та публікацій. Питання захисту права на приватність, персональних даних та цифрових прав людини досліджувалися у працях українських і зарубіжних учених. Значний внесок у розроблення теоретичних засад права на приватність зробили автори колективної монографії за ред. К. В. Єфремової [1], а також автори статей: Т. Ю. Дашо [2], В. А. Світличний [3], В. М. Брижко [4], Ф. П. Шульженко, О. М. Гришко [5], І. М. Шопіна [6] та інші науковці. Аналіз наведених праць дає підстави стверджувати, що, незважаючи на значну увагу науковців до проблем цифровізації, захисту персональних даних, інформаційної безпеки та цифрових прав людини, комплексне дослідження конституційних гарантій права на приватність саме під час використання поліцією цифрових технологій в умовах воєнного стану наразі відсутнє. Не досить дослідженими залишаються:

– конституційні межі використання Національною поліцією цифрових технологій;

– правові підстави застосування біометричних технологій, систем відеоаналітики, автоматичного розпізнавання облич і технологій штучного інтелекту;

– механізми судового, парламентського, прокурорського та громадського контролю за використанням поліцією цифрових засобів спостереження;

– критерії пропорційності обмеження права на приватність під час воєнного стану;

– стандарти Європейського суду з прав людини щодо допустимості цифрового втручання у приватне життя та їх імплементація в діяльність правоохоронних органів України;

– напрями вдосконалення законодавства України з урахуванням вимог права Європейського Союзу, зокрема положень GDPR, Директиви (ЄС) 2016/680 та Акта ЄС про штучний інтелект (AI Act).

Значну увагу проблемам цифрової приватності та правового регулювання інформаційних відносин приділяє зарубіжна юридична наука. Так, Гелен Ніссенбаум обґрунтувала концепцію «контекстуальної цілісності» як основу оцінки допустимості обробки персональних даних [7], Деніел Солов розробив сучасну таксономію порушень права на приватність у цифровому середовищі [8], а Джулі Коен дослідила взаємозв'язок між цифровими технологіями, особистою автономією та конституційними гарантіями прав людини [9]. Водночас у зазначених працях практично не розглядаються особливості забезпечення права на приватність під час використання цифрових технологій правоохоронними органами в умовах воєнного стану, що зумовлює актуальність дослідження цієї проблематики.

Тому **метою статті** є комплексне дослідження конституційних гарантій права на приватність під час використання Національною поліцією цифрових технологій в умовах воєнного стану, визначення основних ризиків порушення прав людини та аналіз механізмів контролю за дотриманням конституційних стандартів у правоохоронній діяльності.

Виклад основного матеріалу. Право на приватність належить до фундаментальних прав людини та становить одну з основних цінностей сучасного конституціоналізму. Його значення зумовлене тим, що саме приватна сфера забезпечує автономію особистості, свободу самореалізації та захист від свавільного втручання держави. В умовах цифровізації суспільства та активного використання правоохоронними органами інформаційно-комунікаційних технологій право на приватність набуває особливого змісту, оскільки значна частина відомостей про особу існує та обробляється в електронній формі. Тому питання забезпечення належного балансу між потребами державної безпеки та захистом приватного життя стає одним із ключових завдань конституційно-правового регулювання.

Конституційні засади захисту права на приватність в Україні закріплені насамперед у статтях 3, 8, 32 та 34 Конституції України. Відповідно до статті 3 Основного Закону людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Це положення визначає антропоцентричний характер конституційного ладу та зумовлює необхідність підпорядкування діяльності державних органів, у тому числі правоохоронних, завданню

забезпечення прав і свобод людини. Стаття 32 Конституції України безпосередньо гарантує право особи на невтручання в особисте і сімейне життя та встановлює заборону на збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди, за винятком випадків, визначених законом і необхідних в інтересах національної безпеки, економічного добробуту та прав людини [10].

Важливу роль у формуванні національних стандартів захисту приватності відіграє практика Конституційного Суду України. У Рішенні від 20 січня 2012 року № 2-рп/2012 Суд зазначив, що особисте життя фізичної особи є невід'ємною складовою частиною її свободи, а інформація про особу, яка дає змогу її ідентифікувати, належить до сфери приватності та підлягає особливому правовому захисту [11]. Суд також підкреслив, що втручання держави у сферу приватного життя повинно відповідати принципам законності, необхідності та пропорційності.

Особливе значення для діяльності правоохоронних органів має принцип верховенства права, закріплений у статті 8 Конституції України [10]. Верховенство права передбачає не лише формальну відповідність діяльності органів влади законодавству, а й необхідність дотримання вимог справедливості, правової визначеності та пропорційності втручання у права людини. У контексті використання поліцією цифрових технологій це означає, що будь-які заходи, пов'язані зі збиранням персональних даних, відеоспостереженням чи використанням інформаційних систем, повинні мати чітку правову основу та відповідати легітимній меті.

Конституційно-правовий зміст права на приватність значною мірою формується під впливом міжнародних стандартів прав людини. Насамперед ідеться про статтю 8 Конвенції про захист прав людини і основоположних свобод, яка гарантує кожному право на повагу до його приватного і сімейного життя, житла та кореспонденції [12]. Європейський суд з прав людини у своїй практиці неодноразово наголошував, що поняття «приватне життя» має широкий зміст і охоплює не лише особисту та сімейну сферу, а й інформацію про особу, її цифрову активність, біометричні дані та електронні комунікації.

Особливе значення для правоохоронної діяльності мають рішення ЄСПЛ у справах *S. and Marper v. the United Kingdom* та *Big Brother Watch and Others v. the United Kingdom*. У першій справі Суд визнав порушення статті 8 Конвенції у зв'язку з тривалим зберіганням поліцією біометричних даних осіб, які не були засуджені за вчинення злочинів [13]. У другій справі Суд сформулював важливі стандарти щодо допустимості використання державою технологій масового цифрового спостереження та наголосив на необхідності ефективного судового контролю за такими заходами [14]. Зазначені правові позиції мають безпосереднє значення для діяльності Національної поліції України в умовах використання сучасних цифрових технологій.

У контексті воєнного стану проблема забезпечення права на приватність набуває особливої актуальності. Відповідно до статті 64 Конституції України окремі права і свободи можуть бути обмежені в умовах воєнного або надзвичайного стану, однак такі обмеження повинні бути передбачені законом і відповідати вимогам необхідності та пропорційності [10]. Це означає, що навіть за наявності підвищених безпекових ризиків правоохоронні органи не можуть здійснювати необмежене втручання у приватне життя громадян. Використання систем відеоспостереження, бодікамер, електронних реєстрів, технологій розпізнавання облич та інших цифрових інструментів повинно супроводжуватися належними гарантіями захисту персональних даних і механізмами контролю за діяльністю органів влади.

Таким чином, в умовах цифровізації поліцейської діяльності та функціонування правового режиму воєнного стану особливого значення набуває забезпечення балансу між інтересами державної безпеки та необхідністю збереження приватної сфери особи. Саме цей баланс визначає межі допустимого використання цифрових технологій правоохоронними органами та виступає критерієм оцінки *законності їхньої діяльності*.

Сучасний етап розвитку правоохоронної діяльності характеризується активним впровадженням цифрових технологій у процес забезпечення публічної безпеки та правопорядку. Цифровізація діяльності Національної поліції України стала одним із ключових напрямів реформування сектору безпеки та оборони. В умовах воєнного стану використання інформаційно-комунікаційних технологій дозволяє правоохоронним органам оперативно реагувати на загрози, здійснювати пошук осіб, документувати воєнні злочини, забезпечувати охорону громадського порядку та координувати взаємодію між державними органами [15]. Одним із найважливіших напрямів цифровізації діяльності Національної поліції є функціонування інформаційно-аналітичних систем та електронних реєстрів, що забезпечують обробку даних про правопорушення, осіб, транспортні засоби, документи та інші об'єкти правоохоронного інтересу.

В умовах воєнного стану особливого значення набули цифрові інструменти ідентифікації осіб та перевірки інформації. Працівники поліції активно використовують доступ до інтегрованих державних реєстрів для перевірки документів, встановлення особи громадян, виявлення осіб, які перебувають у розшуку, а також осіб, причетних до диверсійної чи колабораційної діяльності. Важливим елементом цифрової трансформації правоохоронної діяльності є використання систем відеоспостереження та відеоаналітики. Протягом останніх років в Україні активно розвиваються комплекси «Безпечне місто», які об'єднують мережі камер відеоспостереження, центри обробки інформації та програмні засоби аналізу відеоданих. Сучасні системи відеоспостереження дедалі частіше поєднуються з технологіями штучного інтелекту та автоматизованого аналізу даних. Зокрема, програмні комплекси можуть здійснювати автоматичне розпізнавання номерних знаків транспортних засобів, аналіз поведінкових моделей, пошук осіб за зовнішніми ознаками та інші види цифрової аналітики. Окремого значення набуває використання нагрудних відеореєстраторів (бодікамер) працівниками Національної поліції. Відеофіксація службової діяльності поліцейських сприяє забезпеченню принципів законності, відкритості та підзвітності правоохоронних органів. Записи з бодікамер використовуються як джерело доказів у кримінальному, адміністративному та дисциплінарному провадженні, а також виступають засобом захисту прав як громадян, так і самих поліцейських [16]. Суттєвим напрямом цифровізації є також використання геоінформаційних технологій та цифрових картографічних систем. Такі інструменти дозволяють аналізувати криміногенну ситуацію, планувати маршрути патрулювання, координувати дії підрозділів під час надзвичайних ситуацій та здійснювати моніторинг безпекових ризиків у режимі реального часу. Важливою складовою частиною сучасної правоохоронної діяльності стало використання

цифрових платформ взаємодії з громадянами. Мобільні застосунки, електронні сервіси та онлайн-комунікація дозволяють оперативно отримувати повідомлення про правопорушення, фіксувати факти воєнних злочинів, здійснювати інформування населення про загрози та координувати взаємодію між громадянами і поліцією.

Разом із тим активне впровадження цифрових технологій у діяльність Національної поліції породжує низку правових проблем. Насамперед це стосується захисту персональних даних, забезпечення конфіденційності інформації, визначення строків її зберігання, порядку доступу до баз даних та гарантій недопущення незаконного використання цифрових ресурсів. Особливого значення набуває питання забезпечення належного балансу між потребами державної безпеки та конституційним правом людини на приватність. Саме тому використання цифрових технологій правоохоронними органами повинно супроводжуватися ефективними механізмами правового контролю, що гарантуватимуть дотримання принципів верховенства права, законності та *пропорційності втручання у права людини* [12].

Забезпечення права на приватність під час використання Національною поліцією цифрових технологій неможливе без функціонування ефективної системи контролю за діяльністю правоохоронних органів. В умовах воєнного стану така система набуває особливого значення, оскільки розширення повноважень державних органів та активне застосування цифрових засобів моніторингу створюють додаткові ризики порушення конституційних прав людини. У демократичній правовій державі контроль за діяльністю поліції має здійснюватися на кількох взаємопов'язаних рівнях: конституційному, судовому, парламентському, громадському та внутрішньовідомчому. Центральне місце у системі гарантій права на приватність посідає судовий контроль. Судовий контроль забезпечує перевірку законності дій правоохоронних органів, пов'язаних зі збиранням, використанням та зберіганням персональних даних, застосуванням засобів відеоспостереження, здійсненням негласних слідчих (розшукових) дій та використанням цифрових технологій. Особливого значення судовий контроль набуває під час надання дозволів на тимчасовий доступ до електронної інформації, проведення обшуків електронних пристроїв, отримання даних операторів телекомунікацій та використання результатів цифрового моніторингу як доказів у кримінальному провадженні. Практика Верховного Суду свідчить про послідовне застосування стандартів Європейського суду з прав людини щодо захисту приватності.

Важливим елементом системи захисту права на приватність виступає конституційний контроль. Конституційний Суд України забезпечує верховенство Конституції та здійснює офіційне тлумачення її положень, які стосуються прав і свобод людини. Особливе значення має Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012, в якому Суд визначив, що інформація про особисте та сімейне життя особи належить до сфери приватності та підлягає особливому конституційному захисту [11]. У цьому рішенні було сформульовано фундаментальний висновок, що збір, зберігання, використання та поширення конфіденційної інформації без згоди особи допускаються лише у виняткових випадках і за умови дотримання вимог законності та пропорційності. Саме Конституційний Суд України забезпечує узгодженість законодавства про цифрові технології з конституційними гарантіями права на приватність та захист персональних даних.

Важливим механізмом контролю за діяльністю поліції є парламентський контроль. Відповідно до статті 101 Конституції України парламентський контроль за додержанням конституційних прав і свобод людини здійснює Уповноважений Верховної Ради України з прав людини [10]. У сфері захисту персональних даних Омбудсман виконує функції незалежного наглядового органу. До його повноважень належать здійснення перевірок діяльності державних органів щодо обробки персональних даних, розгляд звернень громадян, внесення подань про усунення порушень законодавства та підготовка рекомендацій щодо вдосконалення практики захисту права на приватність [17]. У контексті діяльності Національної поліції особливого значення набувають перевірки законності використання інформаційних систем, електронних реєстрів та засобів відеоспостереження.

Однією з характерних ознак демократичного суспільства є наявність механізмів громадського контролю за діяльністю правоохоронних органів. Закон України «Про Національну поліцію» передбачає принцип відкритості та прозорості діяльності поліції, що створює передумови для участі громадськості у здійсненні контролю за дотриманням прав людини [18]. Громадський контроль реалізується через діяльність правозахисних організацій, громадських рад, засобів масової інформації, наукових установ та експертного середовища. В умовах цифровізації суттєво зростає роль журналістських розслідувань та громадських ініціатив, спрямованих на виявлення випадків незаконного використання інформаційних ресурсів або надмірного цифрового контролю з боку держави.

Внутрішній контроль є невід'ємним елементом забезпечення законності діяльності поліції. У структурі Національної поліції функціонують підрозділи внутрішнього контролю та підрозділи забезпечення дотримання прав людини, які здійснюють перевірку законності дій поліцейських та дотримання ними службової дисципліни [19]. Використання цифрових журналів доступу, автоматизованого аудиту дій користувачів та систем кібербезпеки дозволяє виявляти випадки несанкціонованого використання інформації та притягати винних осіб до відповідальності. Важливим інструментом внутрішнього контролю є застосування бодікамер. Відеофіксація службової діяльності поліцейських забезпечує можливість перевірки правомірності їхніх дій та виступає додатковою гарантією захисту прав громадян.

Проведений аналіз дає підстави стверджувати, що ефективне забезпечення права на приватність у діяльності поліції в умовах воєнного стану можливе лише за умови функціонування комплексної системи контролю – конституційного, судового, інституційного, відомчого і громадського контролю. Саме поєднання цих механізмів створює належні правові гарантії захисту приватності та дозволяє мінімізувати ризики порушення конституційних прав громадян під час використання правоохоронними органами *сучасних цифрових технологій*.

Загалом, стрімкий розвиток цифрових технологій та розширення їх використання у діяльності правоохоронних органів зумовлюють необхідність постійного вдосконалення механізмів захисту права на приватність. В умовах воєнного стану ця проблема набуває особливої актуальності, оскільки потреба у забезпеченні національної безпеки об'єктивно призводить до збільшення обсягів обробки персональних даних, використання систем відеоспостереження, цифрового моніторингу та інших технологічних засобів контролю. За таких умов одним із головних завдань держави стає формування ефективної системи правових, організаційних і технічних гарантій,

які забезпечуватимуть належний баланс між інтересами безпеки та конституційними правами людини.

Першочерговим напрямом удосконалення механізмів захисту права на приватність є подальший розвиток нормативно-правового регулювання обробки персональних даних у діяльності правоохоронних органів. Чинне законодавство України загалом визначає правові засади захисту персональних даних, однак значна частина його положень була сформована ще до широкого впровадження технологій штучного інтелекту, автоматизованого аналізу даних та цифрової відеоаналітики. У зв'язку з цим доцільним є оновлення законодавства з урахуванням сучасних технологічних реалій та вимог права Європейського Союзу, насамперед положень Загального регламенту про захист даних (GDPR). Особливої уваги потребують питання правових підстав використання біометричних даних, алгоритмів автоматизованого прийняття рішень та технологій розпізнавання облич. Важливим напрямом удосконалення правового механізму є законодавче закріплення спеціальних гарантій під час використання поліцією систем штучного інтелекту та автоматизованих аналітичних платформ. Сучасні цифрові системи здатні здійснювати обробку значних обсягів персональної інформації та формувати рекомендації для прийняття управлінських рішень. Водночас використання таких технологій може супроводжуватися ризиками дискримінації, алгоритмічної упередженості та непрозорості процесів прийняття рішень.

Другим важливим напрямом удосконалення є посилення судового контролю за використанням цифрових технологій у правоохоронній діяльності. В умовах зростання обсягів цифрового моніторингу саме судова влада повинна залишатися ключовим гарантом захисту конституційних прав громадян. Доцільним видається розширення судового контролю за доступом правоохоронних органів до електронних комунікацій, геолокаційних даних, інформації з цифрових пристроїв та результатів функціонування систем відеоспостереження. Важливу роль у цьому процесі має відігравати подальше впровадження стандартів Європейського суду з прав людини щодо оцінки законності та пропорційності втручання у приватне життя особи.

Окремим напрямом вдосконалення механізмів захисту права на приватність є розвиток інституційного контролю за діяльністю правоохоронних органів. У цьому контексті доцільним є розширення повноважень Уповноваженого Верховної Ради України з прав людини щодо здійснення моніторингу використання поліцією цифрових технологій. Важливим кроком може стати запровадження регулярних перевірок інформаційних систем правоохоронних органів на предмет дотримання вимог законодавства про захист персональних даних, а також підготовка щорічних звітів про стан забезпечення цифрових прав людини у діяльності органів сектору безпеки.

Суттєвого вдосконалення потребують внутрішньовідомчі механізми контролю у системі Національної поліції. Насамперед ідеться про створення ефективних процедур аудиту доступу до електронних реєстрів та інформаційних систем. Кожна операція з персональними даними повинна фіксуватися у спеціальних журналах обліку із можливістю подальшої перевірки законності таких дій. Важливим інструментом забезпечення прозорості можуть стати автоматизовані системи контролю доступу до інформаційних ресурсів, які дозволятимуть оперативно виявляти випадки несанкціонованого використання персональних даних.

Особливої уваги потребує питання професійної підготовки працівників поліції. Ефективність правового захисту приватності значною мірою залежить від рівня правової культури та цифрової компетентності працівників правоохоронних органів. У зв'язку з цим доцільно запровадити систематичне навчання поліцейських з питань захисту персональних даних, цифрових прав людини, кібербезпеки та етичних аспектів використання сучасних інформаційних технологій. Відповідні навчальні модулі мають стати невід'ємним складником професійної підготовки та підвищення кваліфікації поліцейських.

Важливим напрямом удосконалення системи захисту права на приватність є розвиток технічних механізмів безпеки. Зокрема, необхідним є впровадження сучасних засобів криптографічного захисту інформації, багаторівневої автентифікації користувачів, систем виявлення несанкціонованого доступу та технологій анонімізації персональних даних. Такі заходи дозволять мінімізувати ризики витоку інформації та підвищити рівень захищеності державних інформаційних ресурсів в умовах зростання кіберзагроз.

Не менш важливим є розширення можливостей громадського контролю за використанням цифрових технологій правоохоронними органами. У сучасних демократичних державах важливу роль відіграють механізми громадського моніторингу, незалежні експертні оцінки та публічне обговорення нових цифрових інструментів, які можуть впливати на права людини. Запровадження практики проведення громадських консультацій щодо використання нових технологій відеоспостереження, біометричної ідентифікації або автоматизованого аналізу даних сприятиме підвищенню довіри суспільства до діяльності поліції.

Висновки. Підсумовуючи викладене, слід зазначити, що вдосконалення механізмів захисту права на приватність у діяльності поліції повинно здійснюватися комплексно та охоплювати правові, інституційні, організаційні, технічні й освітні заходи. Пріоритетними напрямами такого вдосконалення мають стати гармонізація національного законодавства з європейськими стандартами захисту персональних даних, посилення судового та громадського контролю, розвиток внутрішньовідомчих механізмів аудиту, впровадження сучасних засобів кібербезпеки та підвищення рівня цифрової компетентності працівників поліції. Запропонована у статті модель чотирирівневого контролю, яка поєднує конституційний, судовий, інституційний та відомчо-громадський компоненти, може бути використана як теоретична та практична основа для подальшого вдосконалення системи забезпечення права на приватність у діяльності Національної поліції України в умовах воєнного стану та післявоєнного відновлення держави. Лише за умови реалізації зазначених заходів можна забезпечити ефективне функціонування правоохоронної системи в умовах воєнного стану та одночасно гарантувати належний рівень захисту конституційного права людини на приватність.

Список використаних джерел

1. Базові аспекти цифровізації та їх правове забезпечення : монографія. / К. В. Єфремова, Д. І. Шматков, В. П. Кохан та ін. ; за ред. К. В. Єфремової. Харків : НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. 180 с. ISBN 978-617-7806-21-8

2. Дашо Т. Ю. Інформаційно-правові гарантії права на приватність у процесі цифрової ідентифікації особи. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2026. № 1(3). С. 369–375. DOI: https://doi.org/10.24144/2788-6018.2026.01.3.55

3. Світличний В. А. Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека*. 2023. № 3(90). С. 226–236. DOI: https://doi.org/10.32631/pb.2023.3.19

4. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. 2016. № 3(18). С. 45–57. DOI: https://doi.org/10.37750/2616-6798.2016.3(18).272967

5. Шульженко Ф. П., Гришко О. М. Права людини в умовах цифрової трансформації суспільства: теоретико-правовий аналіз. *Київський часопис права*. 2021. № 1. С. 5–10. DOI: https://doi.org/10.32782/klj/2021.1.1

6. Шопіна І. М. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 1. С. 28–35. DOI: https://doi.org/10.32782/2311-8040/2023-1-4

7. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, 2009. 22 p. URL: https://crypto.stanford.edu/portia/papers/privacy_in_context.pdf

8. Solove D. J. Understanding Privacy. Harvard University Press, 2008. 24 p. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

9. Cohen J. E. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press, 2012. URL: https://scholarship.law.georgetown.edu/facpub/804/

10. Конституція України : Закон України від 28 червня 1996 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

11. Рішення Конституційного Суду України від 20 січня 2012 р. № 2-рп/2012 у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32 Конституції України. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

12. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) від 4 листопада 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

13. CASE OF S. AND MARPER v. THE UNITED KINGDOM. Judgment of the European Court of Human Rights of 4 December 2008. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}

14. CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM. Judgment of the European Court of Human Rights of 25 May 2021. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}

15. Указ Президента України від 26 серпня 2021 р. № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"». URL: https://www.president.gov.ua/documents/4472021-40013

16. Наказ МВС України від 18 грудня 2018 р. № 1026 «Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису». URL: https://zakon.rada.gov.ua/laws/show/z0028-19#Text

17. Закон України «Про захист персональних даних» від 1 червня 2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

18. Закон України «Про Національну поліцію» від 2 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

19. Закон України «Про дисциплінарний статут Національної поліції України» від 15 березня 2018 р. № 2337-VIII. URL: https://zakon.rada.gov.ua/laws/show/2337-19#Text

References

1. Yefremova, K. V. (red.)., Shmatkov D. I., Kokhan V. P. ta in. (2021). Bazovi aspekty tsyfrovizatsii ta yikh pravove zabezpechennia: monohrafiia [Basic Aspects of Digitalization and Their Legal Framework: Monograph]. Kharkiv, Research Institute of Legal Support for Innovative Development of the National Academy of Legal Sciences of Ukraine, 180 p. ISBN 978-617-7806-21-8 [in Ukrainian].

2. Dasho, T. Iu. (2026). Informatsiino-pravovi harantii prava na pryvatnist u protsesi tsyfrovoi identyfikatsii osoby [Information and Legal Guarantees of the Right to Privacy in the Process of Digital Identity Verification]. *Elektronne naukove vydannia «Analitychno-porivnialne pravoznavstvo» – Analytical and Comparative Jurisprudence (Electronic Scientific Publication)*, 1(3), 369–375. https://doi.org/10.24144/2788-6018.2026.01.3.55 [in Ukrainian].

3. Svitlychnyi, V. A. (2023). Zakhyst personalnykh danykh v umovakh voiennoho stanu v Ukraini [Personal Data Protection under Martial Law in Ukraine]. *Pravo i bezpeka – Law and Security*, 3(90), 226–236. https://doi.org/10.32631/pb.2023.3.19 [in Ukrainian].

4. Bryzhko, V. M. (2016). Suchasni osnovy zakhystu personalnykh danykh v yevropeiskykh pravovykh aktakh [Modern Foundations of Personal Data Protection in European Legal Acts]. *Informatsiia i pravo – Information and Law,* 3(18), 45–57. https://doi.org/10.37750/2616-6798.2016.3(18).272967 [in Ukrainian].

5. Shulzhenko, F. P., Hryshko, O. M. (2021). Prava liudyny v umovakh tsyfrovoi transformatsii suspilstva: teoretyko-pravovyi analiz [Human Rights in the Context of the Digital Transformation of Society: A Theoretical and Legal Analysis]. *Kyivskyi chasopys prava – Kyiv Law Journal*, 1, 5–10. https://doi.org/10.32782/klj/2021.1.1 [in Ukrainian].

6. Shopina, I. M. (2023). Informatsiina bezpeka tsyfrovoi transformatsii [Information Security of Digital Transformation]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav. Seriia yurydychna – Scientific Bulletin of Lviv State University of Internal Affairs. Series: Law*, 1, 28–35. https://doi.org/10.32782/2311-8040/2023-1-4 [in Ukrainian].

7. Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, 22 p. Retrieved from https://crypto.stanford.edu/portia/papers/privacy_in_context.pdf [in English].

8. Solove, D. J. (2008). Understanding Privacy. Harvard University Press, 24 p. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888 [in English].

9. Cohen, J. E. (2012). Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press. Retrieved from https://scholarship.law.georgetown.edu/facpub/804/ [in English].

10. Konstytutsiia Ukrainy: Zakon Ukrainy vid 28 chervnia 1996 r. [Constitution of Ukraine: Law of Ukraine of June 28, 1996]. Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text [in Ukrainian].

11. Rishennia Konstytutsiinoho Sudu Ukrainy vid 20 sichnia 2012 r. № 2-rp/2012 u spravi za konstytutsiinym podanniam Zhashkivskoi raionnoi rady Cherkaskoi oblasti shchodo ofitsiinoho tlumachennia polozhen chastyn pershoi, druhoi statti 32 Konstytutsii Ukrainy [Decision of the Constitutional Court of Ukraine No. 2-rp/2012 of January 20, 2012, in the Case upon the Constitutional Petition of the Zhashkiv District Council of Cherkasy Region concerning the Official Interpretation of the Provisions of Parts One and Two of Article 32 of the Constitution of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/v002p710-12#Text [in Ukrainian].

12. Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod (z protokolamy) (Ievropeiska konventsiia z prav liudyny) vid 4 lystopada 1950 r. [Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by the Protocols) (European Convention on Human Rights), November 4, 1950]. Retrieved from https://zakon.rada.gov.ua/laws/show/995_004#Text [in Ukrainian].

13. CASE OF S. AND MARPER v. THE UNITED KINGDOM. Judgment of the European Court of Human Rights of 4 December 2008. Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]} [in English].

14. CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM. Judgment of the European Court of Human Rights of 25 May 2021. Retrieved from https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]} [in English].

15. Ukaz Prezydenta Ukrainy vid 26 serpnia 2021 r. № 447/2021 «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy"» [Decree of the President of Ukraine No. 447/2021 of August 26, 2021 "On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 'On the Cybersecurity Strategy of Ukraine'"]. Retrieved from https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].

16. Nakaz MVS Ukrainy vid 18 hrudnia 2018 r. № 1026 «Pro zatverdzhennia Instruktsii iz zastosuvannia orhanamy ta pidrozdilamy politsii tekhnichnykh pryladiv i tekhnichnykh zasobiv, shcho maiut funktsii foto- i kinoziomky, videozapysu, zasobiv foto- i kinoziomky, videozapysu» [Order of the Ministry of Internal Affairs of Ukraine No. 1026 of December 18, 2018, "On Approval of the Instruction on the Use by Police Bodies and Units of Technical Devices and Equipment with Photo, Motion Picture, and Video Recording Functions, as well as Photo, Motion Picture, and Video Recording Equipment"]. Retrieved from https://zakon.rada.gov.ua/laws/show/z0028-19#Text [in Ukrainian].

17. Zakon Ukrainy «Pro zakhyst personalnykh danykh» vid 1 chervnia 2010 r. № 2297-VI [Law of Ukraine "On Personal Data Protection" of June 1, 2010 No. 2297-VI]. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].

18. Zakon Ukrainy «Pro Natsionalnu politsiiu» vid 2 lypnia 2015 r. № 580-VIII [Law of Ukraine "On the National Police" of July 2, 2015 No. 580-VIII]. Retrieved from https://zakon.rada.gov.ua/laws/show/580-19#Text [in Ukrainian].

19. Zakon Ukrainy «Pro dystsyplinarnyi statut Natsionalnoi politsii Ukrainy» vid 15 bereznia 2018 r. № 2337-VIII [Law of Ukraine On the Disciplinary Statute of the National Police of Ukraine, No. 2337-VIII, March 15, 2018]. Retrieved from https://zakon.rada.gov.ua/laws/show/2337-19#Text [in Ukrainian].

Rizhniak Renat,
Doctor of Historical Sciences, Professor,
Head of the Department of General Legal Disciplines
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0002-1977-9048

Kosse Valerii,
Doctor of Philosophy in Law, Police Major,
Dean of the Faculty for the Training of Specialists for the Pre-Trial Investigation Bodies
of the National Police of Ukraine
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0002-6576-0620

Pronin Yurii,
Attorney at Law
ORCID: https://orcid.org/0009-0004-6363-0824

CONSTITUTIONAL GUARANTEES OF THE RIGHT TO PRIVACY IN THE USE OF DIGITAL TECHNOLOGIES BY THE POLICE UNDER MARTIAL LAW: CONTROL MECHANISMS

The article presents a comprehensive study of the constitutional guarantees of the right to privacy in the use of digital technologies by the National Police of Ukraine under martial law. It analyzes national and international legal standards for the protection of privacy, including the provisions of the Constitution of Ukraine, the Convention for the Protection of Human Rights and Fundamental Freedoms, the case law of the Constitutional Court of Ukraine, and the European Court of Human Rights. The study identifies the specific features of applying modern digital technologies in law enforcement, including information and analytical systems, electronic registers, video surveillance systems, facial recognition technologies, body-worn cameras, geographic information systems, and digital communication tools. It substantiates the necessity of maintaining a balance between national security needs and the constitutional right to privacy in the context of expanding digital powers of law enforcement authorities. Particular attention is paid to the analysis of constitutional, judicial, parliamentary, public, and internal departmental oversight mechanisms as the principal safeguards ensuring the lawful use

of digital technologies by the police. The article proposes directions for improving legal regulation, harmonizing Ukrainian legislation with European personal data protection standards, strengthening institutional oversight, introducing advanced cybersecurity measures, and enhancing the digital competence of police officers. It also develops an original model of a comprehensive oversight system governing the use of digital technologies by law enforcement agencies, aimed at ensuring effective protection of the right to privacy and adherence to the rule of law under martial law and during Ukraine's post-war recovery.

Key words: *right to privacy, digital technologies, National Police of Ukraine, martial law, personal data, constitutional guarantees, control mechanisms.*

Дата першого надходження статті до видання: 06.07.2026
Дата прийняття статті до друку після рецензування: 29.07.2026
Дата публікації (оприлюднення) статті: 14.10.2026