УДК 343.412(477):341.171
DOI: https://doi.org/10.33216/2218-5461/2026-52-2-145-162

ЄВРОПЕЙСЬКІ СТАНДАРТИ І УКРАЇНСЬКА ПРАКТИКА ПРОТИДІЇ ЦИФРОВОМУ ДОМАШНЬОМУ НАСИЛЬСТВУ: ВЕКТОР ГАРМОНІЗАЦІЇ

Канський О.А.

EUROPEAN STANDARDS AND UKRAINIAN PRACTICE IN COUNTERING DIGITAL DOMESTIC VIOLENCE: A VECTOR OF HARMONIZATION

Kanskyi O.A.

Стрімка цифровізація повсякденного життя призводить до того, що близькі партнерські та сімейні стосунки дедалі частіше вбудовуються у цифрову інфраструктуру (смартфони, месенджери, спільні облікові записи, сімейні підписки, геолокаційні сервіси, «розумні» пристрої). Підвищуючи комфорт і безпеку, ці технології водночас створюють нові канали контролю, примусу й переслідування, які можуть використовуватися як інструменти домашнього насильства. На практиці цифрові практики домінування є поширеним і таким, що посилюється, проявом насильницької поведінки у партнерствах, але залишаються найменш «видимими» для інституцій через буденність доступу до спільних ресурсів, нормалізацію контролю, швидкоплинність цифрових слідів та брак усталених стандартів їх фіксації й оцінки.

Українське законодавство визначає домашнє насильство як фізичне, сексуальне, психологічне або економічне насильство (дію чи бездіяльність), а також погрози таких діянь. Дефініція є технологічно нейтральною, однак у цифровому середовищі потребує прикладного «перекладу» на поведінкові акти: контроль комунікацій і акаунтів, отримання доступу до сервісів без «злому», приховане відстеження (геолокація, трекери), нав'язливе онлайн-переслідування, цифрове залякування, позбавлення автономії через маніпулювання доступами та налаштуваннями пристроїв. У статті цифровість розглядається як ***модус*** *вчинення насильства, партнерський зв'язок - як кваліфікуючий контекст, а електронні сліди - як процесуальний виклик для стандартів доказування.*

Метою дослідження є формування цілісної моделі кваліфікації цифрового домашнього насильства у партнерствах та практичної моделі доказування: від збору і збереження цифрових слідів до їх оцінки в кримінальних, адміністративних і цивільних провадженнях. Актуальність для України посилюється імплементацією стандартів Ради Європи (Стамбульська конвенція), рекомендаціями GREVIO щодо цифрового виміру насильства та вектором права ЄС (Директива (ЄС) 2024/1385), а також національною дискусією щодо сталкінгу (законопроєкт № 12088). Практичну основу доказування пропонується вибудовувати з урахуванням дисципліни «ланцюга збереження» та форензичних підходів (NIST SP 800-86; NIST SP 800-101 Rev.1).

Ключові слова: *геолокаційне відстеження; домашнє насильство, залякування; кіберсталкінг; контроль акаунтів; кримінальний процес; обмежувальний припис; партнерські та сімейні стосунки; сталкінг; Стамбульська конвенція; цифрове домашнє насильство; цифровий контроль; цифрові докази; електронні докази; форми домашнього насильства.*

Постановка проблеми. В умовах стрімкої цифровізації повсякденного життя інтимні та сімейні відносини дедалі частіше «вбудовані» у цифрову інфраструктуру - смартфони, месенджери, спільні облікові записи, сімейні підписки, геолокаційні сервіси, «розумні» пристрої дому. Ці технології, підвищуючи комфорт і безпеку, водночас створюють нові канали контролю й примусу, що можуть бути використані як інструмент домашнього насильства. На практиці цифрові практики домінування є поширеним і таким, що посилюється проявом насильницької поведінки у партнерствах, але залишаються найменш помітними для інституцій - через буденність доступу до спільних ресурсів, «нормалізацію» контролю в стосунках, швидкоплинність цифрових слідів та брак усталених стандартів їх фіксації й оцінки.

Українське законодавство визначає домашнє насильство як фізичне, сексуальне, психологічне або економічне насильство (дію чи бездіяльність), вчинене в сім'ї, у місці проживання або між колишнім/теперішнім подружжям чи іншими особами, які спільно проживають (проживали) однією сім'єю, незалежно від факту спільного проживання кривдника з постраждалою особою, а також як погрозу вчинення таких діянь [1; 2]. Така дефініція є технологічно нейтральною, однак у цифровому середовищі потребує доктринального й прикладного «перекладу» на мову конкретних поведінкових актів: перехоплення або контроль комунікацій, отримання доступу до акаунтів, приховане стеження через трекери та геолокацію, нав'язливе онлайн-переслідування, цифрове залякування, позбавлення автономії шляхом маніпулювання доступами та налаштуваннями пристроїв. У цій статті цифровість розглядається як модус (спосіб) вчинення насильства, партнерський зв'язок - як кваліфікуючий контекст, а електронні сліди - як процесуальний виклик, що визначає стандарти фіксації, перевірюваності та оцінки доказів. Вирішальним стає питання правової кваліфікації цих дій і їх системного осмислення як насильства саме у контексті близьких стосунків, де доступ до цифрових ресурсів часто не потребує «злому», а забезпечується фактом довіри, спільного побуту або попередньо наданих паролів.

Актуальність теми для України посилюється євроінтеграційними зобов'язаннями та розвитком стандартів Ради Європи і Європейського Союзу. Ратифікація Стамбульської конвенції закріплює обов'язок держави забезпечити ефективне запобігання, захист, переслідування та комплексну політику у сфері домашнього насильства, що потребує адекватних відповідей і на технологічно опосередковані форми насильства [3]. На рівні ЄС ухвалення Директиви 2024/1385, яка прямо охоплює окремі прояви кібернасильства, формує новий нормативний орієнтир і задає напрям гармонізації підходів до криміналізації й протидії цифровим формам насильства [4]. Додатковим національним контекстом є дискусія щодо криміналізації сталкінгу (законопроєкт № 12088 від 02.10.2024), що актуалізує питання співвідношення «сталкінгу» як окремого складу з насильством у близьких стосунках та з наявними механізмами реагування [5].

Водночас правозастосування стикається з фрагментарністю кваліфікаційних рішень і доказовими бар'єрами. Цифрові дії кривдника можуть «розкладатися» між різними юрисдикційними площинами - кримінальною, адміністративною, цивільною - але без єдиної логіки, яка б одночасно враховувала специфіку партнерського зв'язку,

інтенсивність контролю (ефект «24/7»), тривалість і повторюваність поведінки, а також вплив на свободу, приватність і психологічну недоторканність постраждалої особи. Доказування у таких справах ускладнюється крихкістю цифрових слідів, ризиками їх втрати або спотворення, складністю підтвердження авторства/джерела даних, а також потребою збалансувати ефективний захист постраждалих із гарантіями приватного життя та справедливого провадження.

Особливої ваги у цьому контексті набуває термінологічний і правозахисний вимір «партнерств». Для цілей дослідження партнерства охоплюють як шлюбні, так і фактичні (de facto) та інші інтимні відносини без формальної реєстрації, включно з колишніми партнерами, що відповідає підходу Закону « Про запобігання та протидію домашньому насильству» (далі – Закон № 2229-VIII) до кола осіб у відносинах домашнього насильства [2]. У площині прав людини додатковим орієнтиром є позиція ЄСПЛ щодо необхідності правового визнання і захисту стійких партнерських відносин як складника приватного і сімейного життя, зокрема у справі Maymulakhin and Markiv v. Ukraine, що виступає маркером ширшого «партнерського» контексту для формулювання державних позитивних зобов'язань із захисту від насильства та забезпечення ефективних засобів юридичного захисту [6].

Мета і завдання нашого дослідження полягають у формуванні цілісної юридичної моделі кваліфікації цифрового домашнього насильства в партнерствах та «практичної» моделі доказування - від збору й збереження цифрових слідів до їх оцінки у відповідних провадженнях. Для досягнення мети необхідно: уточнити поняття і типологію цифрового домашнього насильства; показати варіативність кваліфікації цифрових практик контролю/переслідування/втручання у приватність у кримінальній, адміністративній та цивільній площинах; описати стандарти, ризики й типові помилки доказування (включно з електронними доказами, ланцюгом збереження, достовірністю та допустимістю); узгодити національні підходи з міжнародними стандартами Ради Європи та тенденціями права ЄС; сформулювати рекомендації для законодавця й правозастосування щодо мінімізації «невидимості» цифрового насильства та підвищення ефективності захисту.

Об'єктом дослідження є правовідносини у сфері запобігання та протидії домашньому насильству й гарантування приватності в умовах цифрових технологій. Предметом виступають правова кваліфікація технологічно опосередкованих дій у партнерських відносинах (зокрема цифровий сталкінг, використання трекерів, контроль месенджерів/акаунтів та інші практики примусу) і доказова база у провадженнях, пов'язаних із такими діями (процесуальні інструменти фіксації, критерії оцінки електронних доказів, співвідношення захисту від насильства та охорони приватного життя).

Термінологічна позиція полягає в тому, що під «партнерствами» у цій статті розуміються шлюбні, фактичні (de facto) співжиття, а також партнерські відносини без формальної реєстрації, які відповідають критеріям інтимного/сімейного зв'язку, включно з колишніми партнерами. Такий підхід узгоджується з тим, що Закон № 2229-VIII охоплює не лише подружжя, а й інших осіб, які спільно проживають (проживали) однією сім'єю [2]. Додатковим орієнтиром є позиція ЄСПЛ щодо необхідності правового визнання і захисту стійких партнерських

відносин як складника приватного і сімейного життя, зокрема у справі Maymulakhin and Markiv v. Ukraine, що підсилює аргументацію необхідності ефективних правових механізмів захисту від насильства у ширшому «партнерському» контексті та релевантності позитивних зобов'язань держави щодо забезпечення дієвих засобів юридичного захисту [6].

Юридичне осмислення цифрового домашнього насильства у партнерствах логічно вибудовується через поєднання двох площин: типологізації технологічно опосередкованих практик контролю/переслідування та їхньої процесуально придатної моделі кваліфікації й доказування. Для коректного руху від емпіричних проявів до правової оцінки необхідно окреслити робочі дефініції та чітко розвести рівні аналізу.

У цьому контексті для забезпечення термінологічної узгодженості доцільно розрізняти рівні опису явища. Під «цифровим домашнім насильством» у цій статті розуміється не окремий юридичний склад правопорушення, а модус (спосіб) вчинення традиційно визначених форм домашнього насильства - фізичного, психологічного, економічного або сексуального - через цифрові канали комунікації та технологічні інструменти. Відповідно, поняття «кіберсталкінг / stalkerware / цифрові трекери» використовуються як узагальнені назви типових поведінкових патернів контролю та переслідування (від нав'язливого нагляду до прихованого збору даних). Саме ці патерни у подальшому аналізі "розкладаються" за юрисдикціями (кримінально-правовою, адміністративно-деліктною та цивільно-правовою) залежно від змісту дій, наслідків і ризику повторення, що, своєю чергою, створює підґрунтя для узгодженої моделі кваліфікації та доказування.

Аналіз наукових досліджень та публікацій з проблематики цифрового домашнього насильства у партнерствах засвідчує, що сучасний дискурс перебуває на етапі переходу від загальних описів «онлайн-агресії» до юридично вимогливішої рамки, у межах якої вирішальними стають дві групи питань: як саме кваліфікувати технологічно опосередковані практики контролю, переслідування та втручання у приватність у контексті близьких стосунків; якими мають бути стандарти збору, збереження та оцінки електронних доказів, якщо ключові сліди насильства є цифровими, крихкими та швидкоплинними. У цьому полі українська доктрина, з одного боку, формує понятійний апарат і пропонує нормативні траєкторії реагування, а з іншого - дедалі чіткіше пов'язує ефективність правового захисту з інституційною спроможністю держави до цифрового документування, міжвідомчої координації та забезпечення доступності допомоги.

Провідною для українського правничого осмислення є лінія, що трактує «кібернасильство» як технологічно опосередковану форму домашнього насильства, у якій ключову роль відіграють цифрові способи контролю та переслідування. Так, О. В. Степаненко, спираючись на підходи ЄСПЛ, показує, що кібернасильство може проявлятися через неправомірний доступ до електронних акаунтів**,** перегляд електронної пошти та приватного листування, копіювання фото/відео та інші втручання у приватність, а також через відстеження (зокрема GPS)**,** онлайн-переслідування, погрози та/або залякування [7, с. 224; 226–227]. Важливо, що авторка не обмежується описом феномену, а

формулює нормативний висновок: з огляду на специфіку та поширеність таких практик доцільним є виокремлення кібернасильства в межах кримінально-правового реагування - шляхом доповнення ст. 126-1 КК України ще однією формою («кібернасильство») [7, с. 224; 227]. У висновках підкреслено, що кібернасильство є симбіозом насамперед психологічного та/або сексуального насильства, що здійснюється із застосуванням ІКТ [7, с. 227]. Окремо звертається увага, що такі дії залишають «цифровий запис», який складно видалити, що може спричиняти подальшу віктимізацію [7, с. 225].

Паралельно розвивається міждисциплінарний пласт публікацій з публічного управління, який фокусується на цифрових інструментах як умовах ефективності державної політики запобігання та протидії домашньому і гендерно зумовленому насильству. В. В. Сичова та І. М. Логовський розглядають інформаційні технології як інструмент реалізації такої політики через офіційні вебсайти, урядову «гарячу лінію 15-47», мережу Інтернет і соціальні мережі, спеціалізовані інформаційні підсистеми (зокрема «Терміновий заборонний припис стосовно кривдника»), а також освітні серіали на платформі «Дія. Цифрова освіта» [8, с. 143–144]. Водночас автори прямо констатують, що відсутність Єдиного державного реєстру випадків домашнього насильства та насильства за ознакою статі гальмує ефективність реалізації політики у цій сфері [8, с. 144; 150]. Важливо, що Реєстр концептуалізується як автоматизована інформаційно-телекомунікаційна система, яка має забезпечувати електронний документообіг і управління інформаційними потоками, а також виконувати функції обліку випадків і координації діяльності суб'єктів [8, с. 149].

Для юридичної проблематики цей напрям важливий не лише як «фон» адміністративної модернізації, а як джерело аргументів, що цифрова інфраструктура взаємодії (облік випадків, електронна координація й швидкі інформаційні контакти між суб'єктами) підвищує спроможність системи вчасно реагувати, запобігати повторюваності та організовувати належне розслідування й притягнення кривдника до відповідальності [8, с. 150].

Значущим сегментом джерельної бази є практико-орієнтовані матеріали органів виконавчої влади та профільних організацій, які «переносять» проблему в площину первинної фіксації і допомоги. Публікації МВС України щодо цифрового насильства містять рекомендації з фіксації цифрових нападів (збереження посилань, скріншотів, звернення до поліції/кіберполіції із долученням збереженої інформації), що має безпосереднє значення для побудови початкового доказового масиву й мінімізації втрати цифрових слідів [10]. Інформаційні матеріали East European Resource Centre систематизують ознаки домашнього насильства та типові патерни контролю, що корисно для правильної інтерпретації цифрових дій кривдника як психологічного насильства/примусу та для оцінки ризиків у контексті захисних механізмів [11].

Хоча ці джерела не є суто науковими, вони відіграють роль «містка» між нормативними дефініціями та реальними сценаріями поведінки, а також демонструють, що ефективність захисту часто залежить від раннього документування подій - ще до відкриття провадження.

На міжнародному рівні дослідницьке поле опирається на стандарти Ради Європи та права ЄС, у яких цифровий вимір насильства проти жінок і домашнього насильства

отримав концептуальне закріплення і практичні орієнтири. Загальна рекомендація GREVIO № 1 (2021) прямо акцентує потребу розвитку цифрової криміналістичної спроможності, адаптації інструментів захисту до онлайн-контактів та переосмислення реагування з урахуванням технологічних каналів переслідування [12]. Дослідження Ради Європи щодо застосування Стамбульської та Будапештської конвенцій до технологічно опосередкованого насильства пропонує рамку «узгодження» антинасильницьких і кіберкримінальних підходів, що є особливо релевантним для ситуацій, де цифровий контроль у партнерствах перетинається з посяганнями на приватність, дані чи комунікаційну таємницю [13]. Додатково Директива (EU) 2024/1385 формує європейський нормативний вектор, прямо охоплюючи окремі форми кібернасильства й задаючи мінімальні стандарти для криміналізації, підтримки потерпілих та процедур реагування, що є значущим орієнтиром для гармонізації українських підходів у межах євроінтеграційних зобов'язань [14]. Сукупно ці документи підтверджують: цифровий вимір насильства не може розглядатися як периферійний, а потребує інтегрованих рішень, які одночасно охоплюють матеріально-правову кваліфікацію, процесуальні гарантії та інституційну спроможність.

Окремий методологічний блок джерел становлять документи цифрової криміналістики, які задають технічні правила «форензично коректної» роботи з даними та слугують опорою для юридичної моделі доказування. До нього належать, зокрема, публікації серії NIST Special Publication 800 (SP 800) - відкриті технічні настанови з кібербезпеки й суміжних практик, які розробляє і видає Національний інститут стандартів і технологій США (NIST) (федеральна установа у складі Міністерства торгівлі США) [15]. Важливо фіксувати їхній статус: це не міжнародні «ISO-стандарти», а рекомендаційні best practices (guidelines)**,** що уніфікують підходи та забезпечують відтворюваність результатів.

У прикладному вимірі для тематики статті ключовими є два документи. NIST SP 800-86 пропонує рамку інтеграції форензичних технік у реагування на інциденти та акцентує на контрольованому збиранні, документуванні й збереженні даних для підтримання їх цілісності та перевірюваності [16]**.** NIST SP 800-101 Rev.1 деталізує цикл мобільної форензики (валідація, збереження, вилучення, дослідження, аналіз, звітування), що є особливо релевантним, коли цифрові сліди насильства зосереджені на смартфоні (месенджери, журнали подій/доступу, геолокація, налаштування, резервні копії тощо) [17]**.**

Чи застосовні ці підходи в Україні? Документи NIST не є національними стандартами (ДСТУ) і не мають прямої обов'язкової сили для українських інституцій, однак можуть використовуватися як методичні орієнтири у професійній підготовці та експертній практиці. Паралельно в Україні діє офіційна стандартизація через імплементацію ISO/IEC: зокрема, ДСТУ EN ISO/IEC 27037:2022 (настанови з ідентифікації, збирання, здобуття та збереження цифрових доказів), прийнятий у пакеті стандартів за наказом ДП «УкрНДНЦ» № 285 від 28.12.2022 і чинний з 31.12.2023 [18].

Методологічна цінність NIST SP 800-86 **і** NIST SP 800-101 Rev.1 для правового аналізу полягає в тому, що вони переводять

процесуальні вимоги до достовірності та допустимості електронних доказів у конкретні операційні кроки: фіксацію походження даних і способу їх отримання, збереження «оригіналу» без втручання, документування ланцюга збереження (chain of custody) та, за потреби, коректне вилучення даних із пристрою із залученням спеціаліста/експерта [16; 17]. У практичному вимірі це означає, що для месенджер-листування або даних зі смартфона важливо підтверджувати не лише зміст, а й контекст (час, ідентифікатор акаунта/пристрою, повнота й безперервність переписки) та прозоро відображати, хто і коли мав доступ до носія або копій.

Узагальнення наявних досліджень і публікацій дозволяє вибудувати послідовну конструкцію викладу: від доктринального розуміння цифрового домашнього насильства як інструменту влади й контролю - до вибору коректної юридичної рамки кваліфікації, окреслення суб'єктного складу, а далі - до практичної моделі доказування, здатної «перетворити» цифрові сліди на допустимі й достовірні докази. По-перше, українська доктрина переконливо показує, що цифрові практики у партнерствах не є «побічним» різновидом конфліктної комунікації: вони формують структурований механізм домінування, який здатен відтворювати офлайн-насильство, підсилювати його ефект (через безперервність контролю) та продовжувати переслідування після розриву стосунків. Звідси випливає ключове методологічне положення: юридична оцінка має виходити не з «каналу» (онлайн/офлайн), а з функції дії - контролю, примусу, залякування, позбавлення автономії та руйнування приватності як умов свободи. По-друге, дослідження уточнюють, чому навіть правильно сконструйована норма може не спрацювати: ефективні юридичні рішення потребують інституційної «підкладки» - даних, реєстрів, цифрових сервісів, протоколів взаємодії та операційної спроможності держави фіксувати, супроводжувати й оцінювати ризики повторюваності. Отже, питання кваліфікації в цифрових кейсах неминуче пов'язане з питанням видимості насильства для інституцій: без стандартизованих процедур документування цифровий контроль легко «випадає» з поля правозастосування. По-третє, міжнародні стандарти Ради Європи й право ЄС закріплюють цифровий вимір насильства як обов'язковий елемент сучасної політики й права та вимагають адаптації захисних механізмів, а також розвитку спроможності держави збирати й зберігати електронні докази. Це означає, що українська модель має бути не лише внутрішньо узгодженою, а й сумісною з європейським вектором, у якому цифрове насильство розглядається як частина континууму насильства. По-четверте, стандарти NIST дають техніко-процедурний каркас, який дозволяє перетворити загальні вимоги права щодо належності, допустимості й достовірності доказів у конкретні кроки зі збереження цілісності даних та відтворюваності результатів аналізу. У сукупності ці підходи формують необхідність узгодженої моделі кваліфікації цифрових практик контролю й переслідування у партнерствах та практичної моделі доказування, яка забезпечує ефективний захист постраждалих за одночасного дотримання гарантій приватності й справедливого провадження.

Вихідною точкою такого конструювання є чинна нормативна матриця України. Закон № 2229-VIII не містить кодифікованого визначення «цифрового домашнього

насильства» як окремої форми, натомість оперує формами насильства (фізичне/сексуальне/психологічне/економічне) та системою реагування (зокрема приписи) [2]. Звідси випливає перший висновок: цифрові дії мають бути описані як спосіб вчинення цих форм, а не як «п'ята» форма. Така формула є юридично коректною і одночасно узгоджується з доктринальним висновком про кібернасильство як «симбіоз» насильницького впливу (передусім психологічного/сексуального) та електронних комунікацій. Практичне значення цього підходу полягає в тому, що він одразу «вбудовує» цифрові фабули в діючі механізми - без очікування спеціальної криміналізації чи окремої дефініції. Саме тому другий висновок є процедурним: інструменти протидії вже нормативно охоплюють онлайн-контакти, адже терміновий заборонний припис може містити заборону контакту «в будь-який спосіб», а обмежувальний припис - заборону спілкування та контактів через засоби зв'язку. Отже, «прогалина» переміщується з рівня нормотворчості на рівень правозастосування: потрібно навчитися перекладати цифрові практики контролю на юридично значущі ознаки психологічного/економічного/сексуального насильства, а також забезпечувати їх доказовість.

Однак коректна кваліфікація неможлива без чіткого визначення суб'єктного складу, оскільки саме він перетворює насильницьку поведінку на «домашнє насильство» у юридичному сенсі. Закон № 2229-VIII прив'язує домашнє насильство не до технології, а до зв'язку між кривдником і постраждалою особою: воно може бути вчинене в сім'ї/в межах місця проживання, між родичами, між колишнім/теперішнім подружжям або між іншими особами, які спільно проживають (проживали) однією сім'єю, незалежно від факту спільного проживання на момент події. Відтак перехід до категорій «шлюб», «родина», «сім'я», «партнерство» є не суто термінологічним, а доказовим: саме через них встановлюється «домашній» контекст. Сімейний кодекс України визначає сім'ю як спільність осіб, що спільно проживають, пов'язані спільним побутом і мають взаємні права та обов'язки; сім'я створюється не лише шлюбом і спорідненням, а й іншими не забороненими законом підставами. Із цього випливає важливе обґрунтування для цифрових фабул: «сімейний» зв'язок може підтверджуватися не лише формальними документами, а й фактичними ознаками спільного життя, які у цифрову епоху часто матеріалізуються в спільних підписках, сімейних облікових записах, спільному користуванні пристроями та сервісами. Водночас шлюб як зареєстрований сімейний союз дає «простий» доказовий маркер: чинне/колишнє подружжя прямо охоплюються дефініцією домашнього насильства. Категорія «партнерства» в українському праві не кодифікована як універсальна форма, тому в науковій моделі доцільно використовувати її як робочий термін і розрізняти: шлюбне партнерство (подружжя), фактичне партнерство (проживання однією сім'єю без шлюбу) та інтимні стосунки без спільного проживання, щодо яких «домашній» контекст може бути проблемним з огляду на формулу Закону № 2229-VIII. Саме тут з'являється додаткове правозахисне підґрунтя: у конвенційній площині «партнерство» є ширшим за національно-сімейні форми, що підтверджується підходом ЄСПЛ до захисту стійких партнерських відносин у контексті приватного і сімейного життя (справа

Maymulakhin and Markiv v. Ukraine) [6]. Отже, суб'єктний блок у статті виконує подвійну функцію: забезпечує відповідність національній дефініції домашнього насильства та одночасно дає аргумент для ширшого, правозахисно орієнтованого тлумачення «партнерських» зв'язків у межах позитивних зобов'язань держави.

Після встановлення суб'єктного зв'язку природно перейти до типових сценаріїв цифрового контролю, бо саме вони показують, яким чином насильство «працює» у технологічному середовищі. Кіберсталкінг (нав'язливе переслідування), приховане відстеження (трекери, геолокація, «stalkerware») та контроль комунікацій/акаунтів є найбільш практично значущими сценаріями, оскільки вони одночасно мають високу поширеність, здатні забезпечувати режим «24/7» і залишають специфічні, але крихкі цифрові сліди. Їх юридична оцінка має фокусуватися не на «наявності повідомлень», а на сукупності ознак патерну: інтенсивність, повторюваність, контрольна мета, створення страху, обмеження автономії, емоційна залежність або погіршення якості життя - саме ці наслідки переводять поведінку в площину домашнього насильства як правового явища.

Від сценаріїв доцільно перейти до триступеневої моделі реагування, яка узгоджує швидкість захисту з вимогами доказування. На першому рівні пріоритет має превентивний контур (приписи), оскільки цифровий контроль легко ескалує і дає кривднику можливість швидко «очистити» сліди; тому припис має бути не абстрактним, а технологічно конкретизованим у мотивуванні (канали контакту, псевдоакаунти, геолокаційне відстеження тощо). На другому рівні адміністративне реагування за ст. 173-2 КУпАП є релевантним для ранніх або епізодичних ситуацій, де систематичність ще не доведена, але необхідна швидка реакція на психологічний тиск через цифрові канали [19; 20]. На третьому рівні кримінально-правова відповідь за ст. 126-1 КК України охоплює систематичні цифрові практики контролю, якщо вони доводяться як патерн домашнього насильства з відповідними наслідками; при цьому «сателітні» склади (таємниця спілкування, приватність, несанкціоноване втручання, шантаж/вимагання, погрози) виконують функцію фіксації технічного способу та об'єкта посягання, підвищуючи повноту оцінки й забезпечуючи процесуальні можливості роботи з електронними доказами [21]. У цьому ж вузлі виникає обґрунтована увага до прогалини криміналізації сталкінгу та актуальності законопроєкту № 12088: тривале нав'язливе переслідування нині часто «розкладається» між різними нормами та юрисдикціями, що ускладнює передбачуваність і єдність практики [5].

У цифрових кейсах домашнього насильства найбільш «прикладною» для негайного припинення контакту є цивільна (і частково сімейна) траєкторія захисту - провадження про обмежувальний припис. Її ефективність пояснюється функцією припису: суд не «карально» реагує на вже доведений склад правопорушення, а оцінює ризик повторення/продовження насильства та потребу у тимчасовому обмеженні дій кривдника, насамперед - контактування. Саме тому механізм припису природно «підхоплює» цифрові фабули, де ключовою шкодою є повторюваний контроль і переслідування через месенджери, соціальні мережі та інші канали зв'язку.

У провадженнях про приписи ключовим є не ретроспективне "доведення складу", а

оцінка ризику повторюваності та потреби негайного обмеження контакту, тому доказова вага цифрових матеріалів визначається їх здатністю показати патерн контролю й актуальність загрози. ЦПК України передбачає окреме провадження щодо видачі обмежувального припису у справах про домашнє насильство (статті 350^{1}–350^{8}) [22]. Важливо, що конструкція припису дозволяє трансформувати технологічно нейтральну заборону «контакту» у практично дієве обмеження саме цифрових каналів: листування, дзвінків у застосунках, повідомлень у месенджерах, контактів у соціальних мережах тощо. Тобто цивільний механізм створює юридичний «бар'єр» не лише для фізичного наближення, а й для цифрової присутності кривдника в повсякденному житті постраждалої особи, де й відбувається основна шкода (страх, виснаження, контроль, ізоляція).

Нормативна рамка приписів уже містить «цифровий місток» без потреби додавати окрему «п'яту» форму насильства. У навчально-методичних матеріалах Верховного Суду серед типового змісту обмежувального припису прямо названо заборону «вести листування, телефонні переговори з постраждалою особою або контактувати з нею через інші засоби зв'язку особисто і через третіх осіб». Отже, цифровий контакт (месенджери, дзвінки через застосунки, повідомлення в соцмережах) не є «поза правом» - він включається в предмет заборони за умови, що суд (і заявник) технологічно конкретизують, які саме канали контакту становлять ризик продовження насильства.

У цьому сенсі показовими є підходи, відображені у публічних матеріалах судів: цифрове листування (зокрема в месенджерах) може мати значення для доведення потреби в обмежувальному приписі, однак його доказова сила визначається лише після оцінки в сукупності з іншими доказами (у комунікаціях судів як ілюстрацію наводять справу № 753/10840/19 ЄДРСР № 90385050 [23]. Така логіка узгоджується із загальними правилами доказування: у справах про припис ключовою є не «формальна оболонка» повідомлень, а те, чи здатні вони підтвердити модель контролю/залякування та наявність ризику повторення насильницьких дій. Приклад № 753/10840/19 у публічному дискурсі використовується саме для демонстрації того, що Viber-повідомлення або їх роздруківки можуть враховуватися судом, якщо вони співвідносяться з іншими даними справи. Отже, цифрові повідомлення не відсіюються наперед, але й не визнаються автоматично: суд очікує встановлення зв'язку між змістом листування, контекстом близьких відносин і доказами реального ризику.

Ефективність обмежувального припису в цифрових кейсах прямо залежить від того, чи зможе заявник «процесуалізувати» електронні сліди. Процесуальна «опора» для такого підходу закріплена в інституті електронних доказів у цивільному процесі (ст. 100 ЦПК): цифрова інформація (зокрема листування, вебсторінки тощо) визнається потенційним доказовим джерелом, а питання зміщується в площину належності, допустимості та перевірюваності походження. ЦПК визначає електронні докази як інформацію в цифровій формі та встановлює правила їх подання і перевірки (ст. 100). Звідси випливає ключовий практичний наслідок: для суду вирішальним є не сам факт наявності зображення екрана, а можливість перевірити походження даних, їх контекст і зв'язок із конкретним акаунтом/особою.

Цю позицію додатково підкреслюють матеріали Верховного Суду щодо електронних доказів: до потенційно належних джерел прямо віднесено й скріншоти/роздруківки з месенджерів (зокрема Viber) за умови оцінки в сукупності з іншими даними [24]. Відтак, «доказовий пакет» у справах про цифрове насильство має будуватися як система взаємопідтверджень: (а) сам пристрій або можливість його огляду; (б) прив'язка акаунта до номера/пошти; (в) експорт чату/резервні копії; (г) повідомлення про входи/зміну пароля; (ґ) свідчення; (д) документи про наслідки психологічного насильства - залежно від фабули. Звідси випливає практичний наслідок: у цифрових справах сильнішою є не одинична «картинка-скріншот», а доказовий пакет, який дозволяє суду відтворити контекст і мінімізувати сумніви щодо автентичності (прив'язка акаунта/номера, наявність пристрою, експорт переписки, хронологія, паралельні підтвердження).

Українська практика приписів і електронних доказів розвивається в полі європейських стандартів, де цифровий вимір насильства розглядається не як «екзотика», а як обов'язкова частина сучасної політики запобігання насильству. У Загальній рекомендації GREVIO № 1 цифрове насильство прямо включено до «континууму» насильства; окремо підкреслено, що protection orders/emergency orders мають бути responsive до насильства, вчиненого онлайн або через ІКТ, а система кримінальної юстиції повинна мати спроможність збирати та зберігати електронні докази. Це, по суті, задає тест для національної практики: чи здатні приписи реально «зупинити» переслідування в цифрових каналах і чи здатна система довести порушення припису/насильницький патерн на основі електронних слідів. Додаткове обґрунтування того, чому саме приписи та доказова інфраструктура мають бути «цифрово чутливими», дає GREVIO: рекомендації щодо цифрового виміру насильства підкреслюють, що захисні/термінові обмежувальні заходи мають бути здатні реагувати на небажану комунікацію «в будь-який спосіб», включно з цифровими каналами, а інструменти захисту - бути придатними до ситуацій онлайн-переслідування [12].

Паралельно з цивільним захистом у цифрових кейсах існує ще один критично важливий відтинок - проміжок між першим зверненням і реальною ізоляцією кривдника. Цифрові кейси мають специфічний ризик: між першим зверненням і реальною ізоляцією кривдника залишається проміжок, у якому контроль може продовжуватися, а сліди - зникати. Саме тому терміновий заборонний припис (як поліцейський інструмент негайного реагування) набуває особливої ваги в ситуаціях, коли онлайн-погрози поєднані з доступом до геолокації, акаунтів або іншою технічною перевагою кривдника. Закон № 2229-VIII прямо передбачає терміновий припис і його змістові можливості, включно із заборонами, спрямованими на негайне припинення насильницької поведінки.

Цей підхід узгоджується з конвенційним стандартом позитивних зобов'язань держави. У справі Levchuk v. Ukraine ЄСПЛ, описуючи українську нормативну рамку, прямо вказав на наявність «спеціальних заходів щодо протидії домашньому насильству», серед яких - терміновий заборонний припис поліції та обмежувальний припис суду (§ 51) [25]. Для цифрових фабул це означає: держава має не лише формально мати інструменти, а й забезпечувати їх реальну дієвість щодо онлайн-контактів і технологічних каналів переслідування.

Нарешті, кваліфікаційна побудова неминуче завершується блоком доказування, бо саме він визначає, чи стане цифрове насильство «видимим» для суду. Доказова проблема має дві сторони: цифрові дії залишають сліди, але ці сліди крихкі, залежні від провайдерів і легко знищуються. Тому практична модель доказування має базуватися на принципі мінімізації втрат у перші години/дні та забезпеченні цілісності даних. Цифрові прояви насильства парадоксальні: вони можуть залишати багато даних, але юридично повноцінними стають лише за умови швидкого збереження, відтворюваності та прив'язки до конкретної особи й партнерського контексту. На «побутовому» рівні цю логіку відображають рекомендації МВС: зберігати посилання/скріншоти і звертатися до поліції/кіберполіції із долученням збереженої інформації [10]. Однак для складніших втручань (stalkerware, приховані трекери, доступ до хмарних копій) цього недостатньо - потрібна процедура, здатна витримати перевірку на автентичність.

Саме тому «пакет» взаємопідтверджень, достатній для первинної процесуалізації електронних слідів, у технічно складних випадках природно переходить у форензичні стандарти там, де ризик маніпуляцій або характер втручання вимагають експертного вилучення й перевірки даних. Євроінтеграційний вектор конкретизується також правом ЄС. Директива (ЄС) 2024/1385, закріплюючи мінімальні стандарти протидії насильству проти жінок і домашньому насильству, прямо працює з окремими цифровими формами та процедурними очікуваннями щодо підтримки потерпілих [4]. У цьому ж контексті з'являється більш прикладний нормотворчий вузол - сталкінг/переслідування: цифровий сталкінг/переслідування потребує більш упорядкованої кваліфікації, ніж «розкладання» фабули між різними складами та юрисдикціями; саме тому актуальність законопроєкту № 12088 у наведеній аргументації є функціонально обґрунтованою [5].

Чинна українська нормативна конструкція дозволяє кваліфікувати цифрові практики контролю як домашнє насильство та застосовувати приписи, що охоплюють онлайн-контакти; однак її ефективність залежить від двох взаємопов'язаних умов - послідовної кваліфікаційної побудови (цифровість як модус вчинення + за потреби сукупність із «сателітами») та процедурно коректної моделі доказування, яка забезпечує достовірність і допустимість електронних слідів у провадженні. Саме на цій підставі поєднання приписів, процесуалізації електронних доказів і форензичних підходів постає не «додатком» до правового реагування, а умовою його реальної дієвості в цифровому середовищі.

Окрему роль відіграє кримінально-правовий «місток» між захистом і доказуванням: КК України передбачає обмежувальні заходи, серед яких прямо названо заборону «листування, телефонних переговорів, інших контактів… через електронні комунікації чи інші засоби зв'язку». Це дозволяє вибудовувати наскрізну конструкцію: припис/заборона → контроль виконання → відповідальність за порушення, де цифрові канали не є винятком, а типовим середовищем реалізації заборони.

Висновки та рекомендації. З огляду на наявну нормативну базу України та європейські стандарти, раціональна стратегія розвитку полягає не у «перейменуванні» домашнього насильства на «цифрове», а у підвищенні чутливості чинних інструментів

до цифрових способів вчинення та у стандартизації доказування. Пріоритетом є впорядкування переслідування/сталкінгу (включно з цифровим виміром) як системної поведінки - з урахуванням стандартів Стамбульської конвенції та орієнтирів Директиви (ЄС) 2024/1385; у національному вимірі це кореспондує з дискусією навколо законопроєкту № 12088 і проблемою «розкладання» тривалого переслідування між різними нормами та юрисдикціями [5].

Паралельно доцільно деталізувати (нормативно або через підзаконні стандарти практики), що «заборона контакту» у приписах охоплює не лише дзвінки та листування, а й технологічні форми «контакту/контролю» (системні спроби захоплення акаунта, нав'язливі запити на відновлення пароля, зловживання «сімейними» групами, геолокаційними сервісами тощо).

У правозастосуванні центральним є стандарт первинної фіксації та сукупної оцінки: цифрові повідомлення визнаються потенційними доказами, але їх переконливість забезпечується перевірюваністю походження та контексту, що узгоджується з публічно описуваними підходами у справах про приписи (зокрема приклад № 753/10840/19) [23]. З урахуванням рамки електронних доказів (ст. 100 ЦПК) це означає пріоритет «пакета взаємопідтверджень» над одиничним скріншотом [24].

Рекомендації GREVIO щодо нарощення цифрово-форензичної спроможності вимагають практичних протоколів для поліції/слідчих: що саме фіксувати, як описувати, як мінімізувати ризик стирання даних і як документувати доступ до носіїв і копій [12]. У технічно складних фабулах такий протокол має спиратися на форензичну дисципліну й ланцюг збереження, що «перекладає» вимоги належності/допустимості/достовірності у послідовні кроки зі збереження цілісності й відтворюваності [16; 17], а також узгоджується з чинними підходами стандартизації цифрових доказів в Україні [18].

У підсумку, українське право вже має фундамент для реагування на цифрові прояви домашнього насильства: приписи як швидкий захист, процесуальні правила про електронні докази та можливість заборон, релевантних для електронних комунікацій [21]. Водночас результативність цього фундаменту залежить від двох умов, які взаємно підсилюють одна одну: технологічно конкретизованих приписів, здатних реально «закрити» цифрові канали контролю й переслідування, та стандартизованої доказової практики, що перетворює крихкі цифрові сліди на перевірювані й переконливі докази без вторинної віктимізації постраждалих - у спосіб, який відповідає сучасним стандартам Ради Європи та тенденціям права ЄС.

Література:

1. Про запобігання та протидію домашньому насильству : Закон України від 07.12.2017 № 2229-VIII (Терміни в документі) // Термінологія законодавства. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/term/2229-19 (дата звернення: 26.02.2026).

2. Про запобігання та протидію домашньому насильству : Закон України від 07.12.2017 № 2229-VIII (поточна редакція від 19.12.2024) // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2229-19 (дата звернення: 26.02.2026).

3. Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами

(Стамбульська конвенція) : Конвенція; Рада Європи від 11.05.2011 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/994_001-11 (дата звернення: 26.02.2026).

4. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence // Official Journal of the European Union. 2024. OJ L, 2024/1385, 24.05.2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1385 (дата звернення: 26.02.2026).

5. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (сталкінг) : законопроєкт № 12088 від 02.10.2024 // Верховна Рада України. Законотворчість. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/44972 (дата звернення: 26.02.2026).

6. Справа «Маймулахін і Марків проти України» (Заява № 75135/14) : Рішення; Європейський суд з прав людини від 01.06.2023 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/974_i96 (дата звернення: 26.02.2026).

7. Степаненко О. В. Кібернасильство як форма домашнього насильства. *Держава та регіони. Серія: Право.* 2022. № 4(78). С. 224–228. DOI: https://doi.org/10.32840/1813-338X-2022.4.34 (дата звернення: 26.02.2026).

8. Сичова В. В., Логовський І. М. Інформаційні технології як інструмент реалізації державної політики у сфері запобігання та протидії домашньому та гендерно зумовленому насильству. *Наукові перспективи.* 2022. № 5(23). С. 143–158. DOI: 10.52058/2708-7530-2022-5(23)-143-158 (дата звернення: 27.02.2026).

9. Danish Refugee Council. Поняття та обсяг гендерно зумовленого насильства (ГЗН): довідка № 1. 2024. 3 с. URL: https://drc.ngo/media/gkie0jt3/drc-ukraine-legal-briefing-note-scope-and-concept-of-gbv-ukr.pdf (дата звернення: 27.02.2026).

10. Міністерство внутрішніх справ України. Цифрове насильство - серйозна загроза для психічного і фізичного здоров'я людини // *Офіційний сайт МВС України.* 26.11.2024. URL: https://mvs.gov.ua/news/cifrove-nasilstvo-seriozna-zagroza-dlia-psixicnogo-i-fizicnogo-zdorovia-liudini (дата звернення: 27.02.2026).

11. EERC. Як розпізнати ознаки домашнього насильства. 30.09.2025. URL: https://eerc.org.uk/ua/iak-rozpiznati-oznaki-domasnyogo-nasilstva (дата звернення: 27.02.2026).

12. GREVIO. *GREVIO General Recommendation No. 1 on the digital dimension of violence against women* : adopted on 20 October 2021 (GREVIO(2021)20); published on 24 November 2021. Strasbourg : Council of Europe, 2021. 33 p. URL: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147 (дата звернення: 27.02.2026).

13. van der Wilk A. Protecting women and girls from violence in the digital age : The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women. Strasbourg : Council of Europe, 2021. 71 p. URL: https://edoc.coe.int/en/violence-against-women/10686-protecting-women-and-girls-from-violence-in-the-digital-age.html (дата звернення: 27.02.2026).

14. Директива (ЄС) 2024/1385 Європейського парламенту і Ради від 14.05.2024 про боротьбу з насильством стосовно жінок і домашнім насильством // *Official Journal of the European Union*. 2024. OJ L, 2024/1385, 24.05.2024. CELEX: 32024L1385. URL: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng (дата звернення: 27.02.2026).

15. National Institute of Standards and Technology. *NIST Special Publication 800-series General Information* // NIST (Information Technology Laboratory). Updated 24.06.2024. URL: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information (дата звернення: 25.02.2026).

16. Kent K., Chevalier S., Grance T., Dang H. *Guide to Integrating Forensic Techniques into Incident Response* : NIST Special Publication 800-86.

Gaithersburg, MD : National Institute of Standards and Technology, August 2006. 121 p. URL: https://csrc.nist.gov/pubs/sp/800/86/final (дата звернення: 25.02.2026).

17. Ayers R., Brothers S., Jansen W. *Guidelines on Mobile Device Forensics* : NIST Special Publication 800-101 Revision 1. Gaithersburg, MD : National Institute of Standards and Technology, May 2014. 87 p. DOI: https://doi.org/10.6028/NIST.SP.800-101r1. URL: https://csrc.nist.gov/pubs/sp/800/101/r1/final (дата звернення: 27.02.2026).

18. Про пакетне прийняття європейських нормативних документів CEN/CENELEC : Наказ ДП «УкрНДНЦ» від 28.12.2022 № 285 (ред. від 21.12.2023) // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/v0285774-22 (дата звернення: 28.02.2026).

19. Суд пояснив, коли переписка у Viber між колишнім подружжям може бути доказом у справі про домашнє насильство // Судово-юридична газета. 28.11.2022. URL: https://sud.ua/uk/news/publication/255365-sud-obyasnil-kogda-perepiska-v-viber-mezhdu-byvshimi-suprugami-mozhet-yavlyatsya-dokazatelstvom-po-delu-o-domashnem-nasilii (дата звернення: 28.02.2026).

20. Кодекс України про адміністративні правопорушення : Кодекс України; Закон, Кодекс від 07.12.1984 № 8073-X // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/8073-10 (дата звернення: 28.02.2026).

21. Кримінальний кодекс України : Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 28.02.2026).

22. Цивільний процесуальний кодекс України : Кодекс України; Кодекс, Закон від 18.03.2004 № 1618-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1618-15 (дата звернення: 28.02.2026).

23. Постанова Верховного Суду (Касаційний цивільний суд) від 13.07.2020 у справі № 753/10840/19 (провадження № 61-22727св19, ЄДРСР № 90385050). Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/90385050 (дата звернення: 28.02.2026).

24. Сакара Н. Електронні докази у цивільному процесі: презентація (Касаційний цивільний суд у складі Верховного Суду). 27.11.2025. Верховний Суд. URL: https://court.gov.ua/storage/portal/supreme/prezentacii_2025/Prezent_Elektr_dokazu_tciv_proces.pdf (дата звернення: 28.02.2026).

25. Справа «Левчук проти України» (Заява № 17496/19) : Рішення ; Європейський суд з прав людини від 03.09.2020 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/974_f92 (дата звернення: 28.02.2026).

Reference:

1. Pro zapobihannia ta protydiiu domashnomu nasylstvu : Zakon Ukrainy vid 07.12.2017 № 2229-VIII (Terminy v dokumenti) // Terminolohiia zakonodavstva. Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/laws/term/2229-19 (data zvernennya: 26.02.2026).

2. Pro zapobihannia ta protydiiu domashnomu nasylstvu : Zakon Ukrainy vid 07.12.2017 № 2229-VIII (potochna redaktsiia vid 19.12.2024) // Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/go/2229-19 (data zvernennya: 26.02.2026)..

3. Konventsiia Rady Yevropy pro zapobihannia nasylstvu stosovno zhinok i domashnomu nasylstvu ta borotbu iz tsymy yavyshchamy (Stambulska konventsiia) : Konventsiia; Rada Yevropy vid 11.05.2011 // Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/go/994_001-11 (data zvernennya: 26.02.2026).

4. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence // Official Journal of the European Union. 2024. OJ L, 2024/1385, 24.05.2024. URL: https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1385 (data zvernennya: 26.02.2026).

5. Proekt Zakonu pro vnesennia zmin do Kryminalnoho protsesualnoho kodeksu Ukrainy ta Zakonu Ukrainy «Pro zapobihannia ta protydiiu domashnomu nasylstvu» shchodo vstanovlennia vidpovidalnosti za zlochynne peresliduvannia (stalkinh) : zakonoproiekt № 12088 vid 02.10.2024 // Verkhovna Rada Ukrainy. Zakonotvorchist. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/44972 (data zvernennya: 26.02.2026).

6. Sprava «Maimulakhin i Markiv proty Ukrainy» (Zaiava № 75135/14) : Rishennia; Yevropeiskyi sud z prav liudyny vid 01.06.2023 // Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/go/974_i96 (data zvernennya: 26.02.2026).

7. Stepanenko O. V. Kibernasylstvo yak forma domashnoho nasylstva // Derzhava ta rehiony. Seriia: Pravo. 2022. № 4(78). S. 224–228. DOI: https://doi.org/10.32840/1813-338X-2022.4.34 (data zvernennya: 26.02.2026).

8. Sychova V. V., Lohovskyi I. M. Informatsiini tekhnolohii yak instrument realizatsii derzhavnoi polityky u sferi zapobihannia ta protydii domashnomu ta henderno zumovlenomu nasylstvu // Naukovi perspektyvy. 2022. № 5(23). S. 143–158. DOI: 10.52058/2708-7530-2022-5(23)-143-158 (data zvernennya: 27.02.2026).

9. Danish Refugee Council. Poniattia ta obsiah henderno zumovlenoho nasylstva (HZN): dovidka № 1. 2024. 3 s. URL: https://drc.ngo/media/gkie0jt3/drc-ukraine-legal-briefing-note-scope-and-concept-of-gbv-ukr.pdf (data zvernennya: 27.02.2026).

10. Ministerstvo vnutrishnikh sprav Ukrainy. Tsyfrove nasylstvo - seriozna zahroza dlia psykhichnoho i fizychnoho zdorovia liudyny // Ofitsiinyi sait MVS Ukrainy. 26.11.2024. URL: https://mvs.gov.ua/news/cifrove-nasilstvo-seriozna-zagroza-dlia-psixicnogo-i-fizicnogo-zdorovia-liudini (data zvernennya: 27.02.2026).

11. EERC. Yak rozpiznaty oznaky domashnoho nasylstva. 30.09.2025. URL: https://eerc.org.uk/ua/iak-rozpiznati-oznaki-domasnyogo-nasilstva (data zvernennya: 27.02.2026).

12. GREVIO. GREVIO General Recommendation No. 1 on the digital dimension of violence against women : adopted on 20 October 2021 (GREVIO(2021)20); published on 24 November 2021. Strasbourg : Council of Europe, 2021. 33 p. URL: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147 (data zvernennya: 27.02.2026).

13. van der Wilk A. Protecting women and girls from violence in the digital age : The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women. Strasbourg : Council of Europe, 2021. 71 p. URL: https://edoc.coe.int/en/violence-against-women/10686-protecting-women-and-girls-from-violence-in-the-digital-age.html (data zvernennya: 27.02.2026).

14. Dyrektyva (YeS) 2024/1385 Yevropeiskoho parlamentu i Rady vid 14.05.2024 pro borotbu z nasylstvom stosovno zhinok i domashnim nasylstvom // Official Journal of the European Union. 2024. OJ L, 2024/1385, 24.05.2024. CELEX: 32024L1385. URL: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng (data zvernennya: 27.02.2026).

15. National Institute of Standards and Technology. NIST Special Publication 800-series General Information // NIST (Information Technology Laboratory). Updated 24.06.2024. URL: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information (data zvernennya: 25.02.2026).

16. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response : NIST Special Publication 800-86. Gaithersburg, MD : National Institute of Standards and Technology, August 2006. 121 p. URL: https://csrc.nist.gov/pubs/sp/800/86/final (data zvernennya: 25.02.2026).

17. Ayers R., Brothers S., Jansen W. Guidelines on Mobile Device Forensics : NIST Special Publication 800-101 Revision 1. Gaithersburg, MD : National Institute of Standards and Technology, May 2014. 87 p. DOI: https://doi.org/10.6028/NIST.SP.800-101r1. URL:

https://csrc.nist.gov/pubs/sp/800/101/r1/final (data zvernennya: 27.02.2026).

18. Pro paketne pryiniattia yevropeiskykh normatyvnykh dokumentiv CEN/CENELEC : Nakaz DP «UkrNDNTs» vid 28.12.2022 № 285 (red. vid 21.12.2023) // Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/go/v0285774-22 (data zvernennya: 28.02.2026).

19. Sud poiasnyv, koly perepyska u Viber mizh kolyshnim podruzhzhiam mozhe buty dokazom u spravi pro domashnie nasylstvo // Sudovo-yurydychna hazeta. 28.11.2022. URL: https://sud.ua/uk/news/publication/255365-sud-obyasnil-kogda-perepiska-v-viber-mezhdu-byvshimi-suprugami-mozhet-yavlyatsya-dokazatelstvom-po-delu-o-domashnem-nasilii (data zvernennya: 28.02.2026).

20. Kodeks Ukrainy pro administratyvni pravoporushennia : Kodeks Ukrainy; Zakon, Kodeks vid 07.12.1984 № 8073-X // Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/go/8073-10 (data zvernennya: 28.02.2026).

21. Kryminalnyi kodeks Ukrainy : Kodeks Ukrainy; Kodeks, Zakon vid 05.04.2001 № 2341-III // Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/go/2341-14 (data zvernennya: 28.02.2026).

22. Tsyvilnyi protsesualnyi kodeks Ukrainy : Kodeks Ukrainy; Kodeks, Zakon vid 18.03.2004 № 1618-IV // Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/go/1618-15 (data zvernennya: 28.02.2026).

23. Postanova Verkhovnoho Sudu (Kasatsiinyi tsyvilnyi sud) vid 13.07.2020 u spravi № 753/10840/19 (provadzhennia № 61-22727sv19, YeDRSR № 90385050). Yedynyi derzhavnyi reiestr sudovykh rishen. URL: https://reyestr.court.gov.ua/Review/90385050 (data zvernennya: 28.02.2026).

24. Sakara N. Elektronni dokazy u tsyvilnomu protsesi: prezentatsiia (Kasatsiinyi tsyvilnyi sud u skladi Verkhovnoho Sudu). 27.11.2025. Verkhovnyi Sud. URL: https://court.gov.ua/storage/portal/supreme/prezentacii_2025/Prezent_Elektr_dokazu_tciv_proces.pdf (data zvernennya: 28.02.2026).

25. Sprava «Levchuk proty Ukrainy» (Zaiava № 17496/19) : Rishennia ; Yevropeiskyi sud z prav liudyny vid 03.09.2020 // Baza danykh «Zakonodavstvo Ukrainy» / Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/go/974_f92 (data zvernennya: 28.02.2026).

Kanskyi O. A. European standards and ukrainian practice in countering digital domestic violence: a vector of harmonization. – Article.

The rapid digitalization of everyday life increasingly embeds intimate partner and family relationships in digital infrastructure (smartphones, messaging apps, shared accounts, family subscriptions, geolocation services, and "smart" devices). While enhancing convenience and security, these technologies simultaneously create new channels of control, coercion, and surveillance that can be used as instruments of domestic violence. In practice, technology-facilitated dominance is a widespread and growing manifestation of abusive behavior in partnerships, yet it often remains the least "visible" to institutions due to routine access to shared resources, the normalization of controlling conduct, the volatility of digital traces, and the absence of established standards for their preservation and assessment.

Ukrainian law defines domestic violence as physical, sexual, psychological, or economic violence (acts or omissions), as well as threats of such acts. This definition is technologically neutral; however, in a digital environment it requires an applied "translation" into concrete behavioral acts: monitoring communications and accounts, gaining access to services without "hacking," covert tracking (geolocation, trackers), persistent online harassment, digital intimidation, and deprivation of autonomy through manipulation of access credentials and device settings. The article treats the "digital" dimension as a modus (means) of perpetration, the partner relationship as a qualifying context, and electronic traces as a procedural challenge for evidentiary standards.

The study aims to develop an integrated model for qualifying technology-facilitated domestic violence in partnerships and a practical evidentiary framework-from collecting and preserving digital traces to assessing them in criminal, administrative, and civil proceedings. The relevance for Ukraine is reinforced by the implementation of Council of Europe standards (the Istanbul Convention), GREVIO recommendations on the digital dimension of violence, and the EU legal vector (Directive (EU) 2024/1385), as well as the national debate on stalking (Draft Law No. 12088). The proposed evidentiary basis relies on the discipline of the chain of custody and digital forensic approaches (NIST SP 800-86; NIST SP 800-101 Rev.1).

Keywords: *geolocation tracking; intimidation; domestic violence, cyberstalking; account control; criminal procedure; restraining order; intimate partner and family relationships; stalking; Istanbul Convention; technology-facilitated domestic violence; digital control; digital evidence; electronic evidence; forms of domestic violence.*

Авторська довідка:

Канський Олександр Адольфович – здобувач третього (освітнього-наукового) рівня вищої освіти кафедри публічного та приватного права, Східноукраїнський національний університет ім. В. Даля, https://orcid.org/0009-0007-7756-3791

Науковий керівник: **Татаренко Галина Вікторівна** – к.ю.н., професор кафедри публічного та приватного права Східноукраїнського національного університету ім. Володимира Даля. ORCID ID: 0000-0001-6291-4455

Дата подачі автором 03.03.2026.
Дата прийняття після рецензування 20.03.2026.
Дата публікації 09.05.2026