DOI: https://doi.org/10.32353/acfs.13.2026.09
УДК 343.1

Михайло Роганін,
аспірант Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса»,
м. Харків, Україна,
ORCID: https://orcid.org/0009-0003-9198-3208,
e-mail: mykh_roh@ukr.net

Огляд персональної інформації в мобільних телефонах під час проведення обшуку: підходи de facto, de jure та de lege ferenda

Михайло Роганін

Стаття присвячена розкриттю питання про правову природу та необхідні процесуальні гарантії доступу до персональної інформації в мобільних телефонах під час проведення обшуку, її огляду та подальшого використання в кримінальному провадженні з позиції de jure, de facto та de lege ferenda у світлі практики Європейського суду з прав людини. З'ясовано, що чинне нормативно-правове регулювання з цього питання не відповідає вимогам повноти та передбачуваності, оскільки насамперед не закріплює необхідних процесуальних гарантій, здатних обмежити дискреційні повноваження сторони обвинувачення при пошуку, копіюванні та вилученні цифрової інформації з мобільних телефонів. Водночас констатовано, що актуальна правозастосовна практика з цього аспекту є суперечливою, оскільки допускає застосування різних заходів для легалізації отриманої інформації, жоден з яких не задовольняє достатньою мірою стандарти забезпечення права особи на приватність, сформульовані в практиці Європейського суду з прав людини. Це дало підстави як підтримати деякі пропозиції, сформульовані в науковій літературі щодо розширення переліку слідчих (розшукових) дій, так і висловити авторські пропозиції щодо вдосконалення чинного кримінального процесуального законодавства.

Ключові слова: кримінальне провадження, досудове розслідування, права людини, обшук, цифрові докази, Європейський суд з прав людини.

Постановка наукової проблеми. Поряд із тим, що проведення обшуку в житлі чи іншому володінні особи саме по собі належить до тих заходів, що спричиняють суттєве втручання в основоположні права людини, передусім регламентовані у ст. 8 Європейської конвенції з прав людини (далі – ЄКПЛ або Конвенція), по суті обшук може виходити далеко за межі того приміщення, де він безпосередньо проводиться. Це, насамперед, обумовлено тим, що переважно кожне проведення обшуку супроводжується оглядом інформації на мобільних телефонах, її копіюванням, а за певних обставин – навіть їх безпосереднім вилученням з подальшим призначенням комп'ютерно-технічної експертизи. Водночас слід наголосити, що наразі доступ до такої інформації у більшості сучасних смартфонів означає не лише втручання у приватне та сімейне життя (наприклад, через ознайомлення з фотогалереєю, списком контактів, нотатками, історією браузерів, геолокаційними даними тощо), а й обмеження права на повагу до таємниці спілкування (у термінології ЄКПЛ – таємниці кореспонденції), оскільки на цих цифрових носіях міститься суттєвий масив комунікативних даних – наприклад, збережене листування в різноманітних месенджерах, голосові повідомлення, СМС-повідомлення тощо.

Наведена проблематика ще більше актуалізується з огляду на технічні можливості сучасних мобільних телефонів, що дозволяють отримати доступ до віддалених джерел інформації – наприклад, електронних поштових скриньок, банківських додатків з інформацією про рахунки та операції на них, хмарних сховищ та ін. Ця обставина, без сумніву, максимально розширює межі втручання як у приватне життя, так і в таємницю корес-

ФІНАНСУВАННЯ

Це дослідження не отримувало жодних спеціальних грантів від фінансуючих організацій у державному, комерційному чи некомерційному секторах.

ЗАСТЕРЕЖЕННЯ

Фінансуюча сторона не брала участі в розробці дизайну дослідження, зборі та аналізі даних, прийнятті рішення про публікацію або підготовці рукопису.

УЧАСНИКИ

Автор брав участь виключно в інтелектуальній дискусії, що лежить в основі цієї статті, дослідженні прецедентного права, написанні та редагуванні, і несе відповідальність за зміст та інтерпретацію.

ДЕКЛАРАЦІЯ ПРО КОНФЛІКТ ІНТЕРЕСІВ

Автор заявляє, що у нього немає конфлікту інтересів.

Mykhailo Roganin,

NSPECTION OF PERSONAL DATA ON MOBILE PHONES DURING A SEARCH: DE FACTO, DE JURE AND DE LEGE FERENDA APPROACHES

The article is devoted to revealing the legal nature of access to personal data stored on mobile phones during searches, inspections and its subsequent use in criminal proceedings, as well as the necessary procedural safeguards, from the perspectives of de jure, de facto and de lege ferenda, in the light of the case law of the European Court of Human Rights.

The relevance of this research is indicated by the fact that the vast amount of information – including communications data – stored on modern mobile phones, the relatively easy access to it, and the ability to identify and retrieve information stored remotely (for example, in cloud storage) via access to the relevant programmes and applications on the mobile phone, significantly broadens the scope of potential interference with the right to respect for privacy (including the secrecy of correspondence). This necessitates a shift in perspective regarding the standards and procedural safeguards that must be ensured when accessing information on mobile phones seized during a search of a person's home or other premises.

The systematic analysis of the current provisions of criminal procedural law carried out in this study has revealed a lack of a sufficient and precise legal framework on this issue, one that would take into account both the nature of the procedural actions being carried out and the necessary safeguards against arbitrariness – above all, deliberate judicial control over interference with the relevant fundamental right. Indeed, the inspection of computer data introduced in 2022 does not require separate judicial authorisation and, moreover, does not cover actions involving the search for and copying of information from computer systems.

The article also notes that current judicial practice on this matter remains equally unsatisfactory, as the existing procedural measures (primarily the seizure of property, temporary access to items and documents, or the extraction of information from electronic information systems) applied to such situations involving the handling of information on mobile phones do not take into account the specific

понденції під час проведення відповідних процесуальних дій. Тим більше, що у разі обмеження права на таємницю спілкування шляхом ознайомлення з відповідним листуванням втручання відбувається в комунікацію не лише особи, якій належить відповідний мобільний пристрій, а й тих суб'єктів, з якими вона спілкується. Додатково підкреслимо, що серед них можуть бути також, наприклад, адвокати, що вимагає дотримання особливих підвищених гарантій захисту інформації, коли йдеться про охоронювану законом адвокатську таємницю. Ще один важливий аспект, що може свідчити про актуальність розглядуваної проблематики, пов'язаний із тим, що під час проведення обшуку в певному приміщенні можуть бути присутні і сторонні особи, які не є власниками/володільцями житла чи іншого володіння. При цьому, з огляду на положення ст. 236 Кримінального процесуального кодексу України (далі – КПК), зважаючи на суттєву дискрецію слідчого, прокурора, який проводить обшук, визначати, які саме об'єкти можуть мати значення для кримінального провадження або містити відповідну інформацію, мобільні телефони таких осіб так само можуть стати предметом ретельного аналізу.

Усе вищенаведене підкреслює особливу важливість дослідження питання про те, в якому саме процесуальному порядку має відбуватися доступ до інформації, що міститься в мобільних телефонах, під час проведення обшуку в житлі чи іншому володінні особи, її вивчення та якими процесуальними гарантіями це має супроводжуватися, насамперед у світлі європейських стандартів захисту права людини на приватність. При цьому, з огляду на те, що законодавчий підхід не відповідає достатньою мірою вимогам точності, визначеності та передбачуваності, що викликає як розбіжності у правозастосовній практиці, так і полеміку в науковій літературі, спробуємо розглянути окреслені аспекти з погляду de jure, de facto та de lege ferenda.

Аналіз основних досліджень і публікацій. Проблематика цифровізації кримінального провадження, зокрема і в контексті формування та використання цифрових (електронних) доказів, уже багато років залишається перманентно актуальною. Серед досліджень, які безпосередньо присвячені аналізу правової природи тих процесуальних дій, що здійснюються з метою пошуку, виявлення та вилучення інформації, що може мати доказове значення, з цифрових носіїв, зокрема і мобільних телефонів, а також процесуальним гарантіям, які мають супроводжувати такі дії, можна згадати науковий доробок В. В. Вапнярчука, М. І. Демури, Д. І. Клепки, І. О. Крицької, О. П. Метелева, А. В. Скрипника, І. А. Смаль та багатьох інших.

До того ж, це питання привертає увагу і зарубіжних науковців. Наприклад, L. Bernardini та F. Sanvitale аналізують близькі за змістом до проблематики статті аспекти в розрізі італійського кримінального процесуального законодавства (що містить майже ідентичні з українським недоліки в правовій регламентації) та документів Європейського Союзу[1].

Метою статті є розкриття питання про правову природу та необхідні процесуальні гарантії огляду персональної інформації в мобільних телефонах під час проведення обшуку з позиції de jure, de facto та de lege ferenda у світлі практики Європейського суду з прав людини (далі – ЄСПЛ або Суд).

Викладення основного матеріалу дослідження. Зважаючи на те, що будь-яке втручання у фундаментальні права особи повинно, передусім, відповідати вимозі законності, спробуємо проаналізувати наявні правові рамки та з'ясувати, чи достатнім, передбачуваним і якісним є чинне нормативне забезпечення процесуального порядку отримання доступу до інформації, що міститься в мобільних телефонах, за результатами проведення обшуку в житлі чи іншому володінні особи, ознайомлення з нею, її копіювання та вилучення.

Можемо зауважити, що тривалий час це питання взагалі залишалося в певному правовому вакуумі, оскільки, окрім низки норм, що стосувалися особливостей застосування деяких заходів забезпечення кримінального провадження до електронних носіїв інформації (наприклад, абз. 2 ч. 1 ст.

[1] Bernardini L., Sanvitale F. Searches and seizures of electronic devices in European criminal proceedings:a new pattern for independent review? Revista Ítalo-Española de Derecho Procesal. 2023.Num. 1. Pp. 73-119. DOI: 10.37417/rivitsproc/1475

159 КПК, абз. 2–3 ч. 2 ст. 168 КПК), а також доказового значення як оригіналів документів копій інформації, зокрема комп'ютерних даних, що містяться в інформаційних (автоматизованих) системах, електронних комунікаційних системах тощо, виготовлених слідчим, прокурором із залученням спеціаліста (ч. 4 ст. 99 КПК), інші дотичні правові приписи були відсутні.

Проте Законом України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за «гарячими слідами» та протидії кібератакам» № 2137-IX від 15 березня 2022 р. кримінальне процесуальне законодавство було доповнено низкою новел. Їх частина, зокрема, стосувалася і зазначених вище норм, деталізуючи порядок виготовлення копій інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів, та застосування щодо неї тимчасового вилучення та арешту майна (насамперед, абз. 4–5 ч. 2 ст. 168, абз. 2 ч. 3 ст. 170 КПК). Водночас було також запроваджено новий вид огляду – комп'ютерних даних (абз. 2 ч. 2 ст. 237 КПК), а також регламентовано можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, здійснення на них пошуку, виявлення та фіксації комп'ютерних даних, що на них містяться, на місці проведення обшуку (ч. 6 ст. 236 КПК)[2].

Зміст нового різновиду огляду було розкрито законодавцем у згаданій вище ч. 2 ст. 237 КПК – зокрема, він полягає у «відображенні у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їхнього змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі)». При цьому зазначимо, що навіть побіжний аналіз наведеної норми може свідчити про її певну термінологічну недосконалість з певних причин. По-перше, все ж таки поняття «огляд» не досить точно відображає характер пошукових дій представників сторони обвинувачення. Адже перед тим як оглянути певну цифрову інформацію на смартфоні чи ноутбуці, переважно потрібно провести активні дії з її відшукання на носії інформації. До речі, саме такі дії і згадуються у ч. 6 ст. 236 КПК – «пошук, виявлення та фіксація комп'ютерних даних», що містяться на певних цифрових носіях. По-друге, використаний законодавцем термін «комп'ютерні дані» може бути помилково сприйнятий правозастосовниками як такий, що охоплює інформацію, яка зберігається виключно на комп'ютерах.

Проте заради справедливості варто зазначити, що саме це поняття використано у Конвенції про кіберзлочинність, де у ст. 1 наведена його дефініція[3]. Їх вивчення дозволяє зробити висновок, що ця категорія охоплює також і мобільні телефони та інформацію, що на них зберігається. Однак необхідність такої ускладненої інтерпретації поняття «комп'ютерні дані» через відсилання до міжнародно-правового договору навряд чи свідчить про доступність для сприйняття цього нормативного положення та передбачуваність його застосування.

У світлі цього можемо відмітити, що до запровадження відповідних новел у березні 2022 р. відповідні дії з пошуку, виявлення інформації на цифровому носії та ознайомлення з нею так само переважно здійснювалися в межах огляду. Однак тоді йшлося про огляд предмета (наприклад, мобільного телефону), що викликало певні дискусії в наукових розробках, оскільки вести мову в такому разі виключно про огляд певного матеріального об'єкта (як-от телефону) навряд чи було коректно. У контексті тогочасної нормативної регламентації досить слушно зауважувалося, що за описаних обставин слідчий, дізнавач або прокурор не обмежується суто візуальним спостереженням зовнішніх ознак відповідного

[2] Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за «гарячими слідами» та протидії кібератакам [On Amendments to the Criminal Procedure Code of Ukraine to Improve the Effectiveness of Pre-Trial Investigations Conducted in Real Time and to Counter Cyberattacks]: Закон України № 2137-IX від 15 березня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2137-20#n12

[3] Конвенція про кіберзлочинність [Convention on Cybercrime] (підписана 23 листопада 2001 р., ратифікована із застереженнями і заявами Законом № 2824-IV від 7 вересня 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

Mykhailo Roganin,

DIE EINSICHTNAHME IN PERSONENBEZOGENE DATEN IN MOBILTELEFONEN IM RAHMEN EINER DURCHSUCHUNG: DE-FACTO-, DE-JURE- UND DE-LEGE-FERENDA-ANSÄTZE

Der Artikel befasst sich mit der Frage nach der rechtlichen Natur und den erforderlichen Verfahrensgarantien für den Zugriff auf personenbezogene Daten in Mobiltelefonen während einer Durchsuchung, deren Einsichtnahme und der anschließenden Verwendung im Strafverfahren aus der Perspektive von de jure, de facto und de lege ferenda im Lichte der Praxis des Europäischen Gerichtshofs für Menschenrechte. Es wird festgestellt, dass die geltenden Rechtsvorschriften zu diesem Thema nicht den Anforderungen an Vollständigkeit und Vorhersehbarkeit entsprechen, da sie vor allem keine notwendigen Verfahrensgarantien vorsehen, die die Ermessensbefugnisse der Anklage bei der Suche, dem Kopieren und der Beschlagnahme digitaler Informationen aus Mobiltelefonen einschränken könnten. Gleichzeitig wird festgestellt, dass die aktuelle Rechtspraxis in diesem Bereich widersprüchlich ist, da sie die Anwendung verschiedener Maßnahmen zur Legalisierung der erhaltenen Informationen zulässt, von denen keine den in der Praxis des Europäischen Gerichtshofs für Menschenrechte formulierten Standards zur Gewährleistung des Rechts auf Privatsphäre ausreichend erfüllt. Dies gab Anlass, sowohl einige in der wissenschaftlichen Literatur formulierte Vorschläge zur Erweiterung des Katalogs der Ermittlungsmaßnahmen zu unterstützen als auch eigene Vorschläge zur Verbesserung der geltenden Strafprozessordnung zu unterbreiten.

Schlüsselwörter: Strafverfahren, Ermittlungsverfahren, Menschenrechte, Hausdurchsuchung, digitale Beweismittel, Europäischer Gerichtshof für Menschenrechte.

Mykhailo Rohanin,

EXAMEN DES INFORMATIONS PERSONNELLES DANS LES TÉLÉPHONES PORTABLES LORS D'UNE RECHERCHE : APPROCHES DE FACTO, DE JURE TA DE LEGE FERENDA

L'article examine la question de la nature juridique et des garanties procédurales nécessaires à l'accès aux données personnelles contenues dans les téléphones mobiles lors d'une perquisition, leur examen et leur utilisation ultérieure dans le cadre de poursuites pénales, du point de vue de jure, de facto et de lege ferenda, à la lumière de la jurisprudence de la Cour européenne des droits de l'homme. Il apparaît que la réglementation et la législation actuelles en la matière ne répondent pas aux exigences d'exhaustivité et de prévisibilité, car elles n'établissent pas, en premier lieu, les garanties procédurales nécessaires pour limiter le pouvoir discrétionnaire du ministère public lors de la perquisition, de la copie et de l'effacement des données numériques contenues dans les téléphones mobiles. Par ailleurs, il est constaté que la pratique actuelle des forces de l'ordre en la matière est contradictoire, puisqu'elle autorise le recours à diverses mesures pour légaliser les informations obtenues, sans qu'aucune ne réponde pleinement aux normes garantissant le droit au respect de la vie privée telles que formulées par la jurisprudence de la Cour européenne des droits de l'homme. Cela a permis à la fois de soutenir certaines propositions formulées dans la littérature scientifique concernant l'élargissement de la liste des actions d'enquête (de recherche), et d'exprimer les propositions de l'auteur concernant l'amélioration de la législation procédurale pénale actuelle.

Mots clés: procédure pénale, enquête préliminaire, droits d l'homme, recherche, preuves numériques, Cour européenne des droits de l'homme.

гаджета, а отримує доступ до збереженої на ньому цифрової інформації, чим насамперед втручається у приватне спілкування особи без окремого судового дозволу [4].

Порівнюючи чинну редакцію КПК у світлі цього питання з попереднім нормативним підходом, безумовно, можемо відмітити більшу законодавчу точність у назві відповідної процесуальної дії, оскільки перенесення акценту з огляду предмета на огляд інформації, що на ньому міститься («комп'ютерних даних»), на наш погляд, є доцільним та слушним уточненням. Попри це, навіть після новел 2022 р., у науковій літературі все ще висловлюються думки щодо неточності та неповноти відповідної назви.

Так, О.П. Метєлєв на прикладі огляду персонального комп'ютера, що загалом може бути екстрапольовано також і на огляд мобільного телефону, підкреслює, що під оглядом доцільно розуміти лише «візуальне обстеження місцевості, приміщення або речі, які знаходяться у вільному доступі, без активного пошукового впливу на них». Проте, як зауважує науковець, органами, які проводять слідчі дії у формі огляду цифрового носія, в межах цього заходу проводяться операції з відкриття папок із файлами та самих файлів, вивчення їх вмісту та властивостей, які за своєю суттю є цілеспрямованим пошуком інформації, тобто обшуком – примусовою дією. При цьому О.П. Метєлєв також вказує на можливість виокремлення кількох етапів під час огляду цифрового (електронного) носія інформації, засобів стільникового зв'язку (мобільних телефонів, модемів і т. ін.) (йдеться, по-перше, про зовнішній огляд матеріального носія (найменування пристрою, зовнішні ознаки); по-друге, про конструктивний огляд (наявність елементів живлення, карт пам'яті, SIM-карт і т. ін.); по-третє, про огляд інформаційного середовища (огляд і фіксація відомостей, які містяться на цифровому носії інформації)))[5].

Критично ставиться до чинної нормативної регламентації розглядуваного питання також А. В. Скрипник, підкреслюючи, що попри появу у 2022 р. норми, яка легалізувала процесуальну дію, що є віддаленим аналогом цифрового обшуку, все ж повноцінної слідчої (розшукової) дії, яка б регламентувала пошукові дії сторони обвинувачення у цифровому просторі та межі допустимого втручання у сферу прав і свобод людини, процесуальний закон все ще не передбачає. Зважаючи на це, науковець резюмує потребу нормативного врегулювання етапу проведення цифрового обшуку[6].

На продовження аналізу з погляду de jure можемо погодитися з наведеним вище висновком щодо недосконалості чинної правової регламентації не лише в аспекті назви процесуальної дії та повноти охоплення цією назвою всіх етапів пошуку та дослідження цифрової інформації на носії, а й стосовно точності та достатності врегулювання процесуального порядку та процесуальних гарантій роботи з інформацією на мобільному телефоні, доступ до якого був отриманий під час проведення обшуку в житлі чи іншому володінні особи.

Отже, виходячи зі змісту ч. 6 ст. 236 КПК, можна виокремити такі процесуальні правила: (1) під час здійснення обшуку особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть вказати на це слідчому, прокурору, а також надати до них доступ – така інформація має бути відображена в протоколі обшуку; (2) у разі здійснення обшуку за відсутності вказаних вище осіб або якщо така особа хоча і присутня, однак відмовляється зняти (деактивувати) систему логічного захисту, слідчий, прокурор може робити це самостійно (зокрема, в примусовому порядку); (3) доступ до відповідних комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку може бути отриманий навіть у разі, якщо вони безпосередньо не

[4] Демура М., Крицька І., Клепка Д. Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження [Safeguarding the rights and legitimate interests of individuals in the context of the 'digitalisation' of criminal proceedings]. *Часопис Київського університету права*. 2020/1. С. 297. DOI: 10.36695/2219-5521.1.2020.60

[5] Метелев, О. П. Щодо способів збирання і формування цифрових доказів у кримінальному провадженні [On Methods for Collecting and Compiling Digital Evidence in Criminal Proceedings]. 2024. *Вісник кримінального судочинства,* Вип. 3-4. С. 52, 54. DOI: https://doi.org/10.17721/2413-5372.2023.3-4/47-58

[6] Скрипник А.В. Цифровий обшук: бути чи не бути? [Digital searches: to be or not to be?] Цифровізація кримінального провадження: стан та перспективи : матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В. Глинська (голов. ред.), Д. І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 148-149.

зазначені в ухвалі про дозвіл на обшук, однак, на переконання слідчого, прокурора, є достатні підстави вважати, що інформація, яка на них міститься, має значення для встановлення обставин у кримінальному провадженні.

Додаткові правила встановлені також у деяких нормах, присвячених застосуванню таких заходів забезпечення кримінального провадження, як тимчасове вилучення майна та арешт майна. А саме, поряд із загальною забороною тимчасового вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, якщо вони безпосередньо не були зазначені в ухвалі слідчого судді, суду, все ж допускаються винятки з цього правила. Йдеться про ситуації, коли надання таких пристроїв є необхідним для проведення експертного дослідження, а також коли сам носій інформації був предметом кримінального правопорушення або засобом чи знаряддям його вчинення, або «якщо такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення». Крім того, що важливо в контексті положень ч. 6 ст. 236 КПК, тимчасове вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку є допустимим також, якщо доступ до них був обмежений власником, володільцем, утримувачем чи пов'язаний з подоланням системи логічного захисту.

Отже, окреслені вище правові приписи по суті стосуються передусім контролю за втручанням у право на мирне володіння майном. У світлі цього можна навести позицію В. В. Вапнярчука, який, розмежовуючи огляд комп'ютерних даних під час обшуку на місці його проведення та вже після нього (поза місцем проведення обшуку – зокрема, коли подолання систем логічного захисту і отримання доступу вимагає застосування спеціального технічного обладнання та/або програмного забезпечення), вказує на таке. Так, на думку вченого, у першій ситуації, особливо коли йдеться про випадки незазначення в ухвалі слідчого судді, суду дозволу на відшукання певних цифрових носіїв інформації, огляд комп'ютерних даних перебуває поза судовим контролем. Водночас у другій ситуації, як вказує В. В. Вапнярчук, такий судовий контроль наявний у формі вирішення питання про арешт тимчасово вилученого майна[7].

Що ж до обмеження права на повагу до приватності, можемо резюмувати, що доступ до інформації на цифрових носіях може бути отриманий незалежно від того, чи захищені вони логічним захистом, а також попри заперечення з боку власників, володільців, утримувачів. При цьому відповідні процесуальні дії з пошуку, виявлення та копіювання інформації з цифрових носіїв не потребують отримання окремої ухвали слідчого судді, суду. Вивчення нормативного змісту абз. 1 ч. 6 ст. 236 КПК може вказувати на те, що по суті цифрові носії інформації в такому разі прирівнюються до закритих приміщень, шухляд чи шаф. Проте, вочевидь, законодавець у такому разі залишив поза увагою ті суттєві особливості технічних пристроїв (наприклад, мобільних телефонів), про які ми зазначали на початку нашої роботи. А отже, доступ до значних масивів інформації приватного характеру, зокрема і щодо приватного спілкування осіб, залишається поза цілеспрямованим судовим контролем, тобто відсутні належні процесуальні гарантії та запобіжники від свавілля з боку представників сторони обвинувачення.

У світлі цього підкреслимо, що подібний підхід у нормативній регламентації не відповідає європейським стандартам забезпечення права особи на приватність[8]. Зокрема, враховуючи триступеневий тест аналізу, що застосовується при втручанні в права, гарантовані ст. 8 ЄКПЛ, і охоплює необхідність оцінки відповідності закону, наявності легітимної мети та необхідності в демократичному суспільстві, можемо резюмувати наявність проблем вже на першому етапі. Зокрема, чинне кримінальне

[7] Вапнярчук В. В. Щодо дослідження змісту електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку під час кримінального провадження [Regarding the examination of the contents of electronic information systems, computer systems or parts thereof, and mobile terminals of communication systems during criminal proceedings]. *Аналітично-порівняльне правознавство*. 2025. Вип. 2. С. 970. URL: https://app-journal.in.ua/wp-content/uploads/2025/04/146.pdf

[8] Рішення ЄСПЛ у справі «Roman Zakharov проти Росії» [ECHR Judgment in the Case of Roman Zakharov v. Russia] [ВП] (заява № 47143/06) від 4 грудня 2015 р. URL: https://hudoc.echr.coe.int/eng?i=001-159324; Рішення ЄСПЛ у справі «Potoczka і Adamco проти Словаччини» [ECHR Judgment in the Case of Potoczka and Adamco v. Slovakia] (заява №7286/16) від 12 січня 2023 р. URL: https://hudoc.echr.coe.int/eng?i=001-222143 та інші.

Michaił Roganin,

PRZEGLĄD DANYCH OSOBOWYCH W TELEFONACH KOMÓRKOWYCH PODCZAS PRZEPROWADZANIA PRZESZUKANIA: PODEJŚCIA DE FACTO, DE JURE I DE LEGE FERENDA

Artykuł poświęcony jest omówieniu kwestii natury prawnej oraz niezbędnych gwarancji proceduralnych dotyczących dostępu do danych osobowych w telefonach komórkowych podczas przeszukania, ich przeglądu oraz dalszego wykorzystania w postępowaniu karnym z perspektywy de jure, de facto oraz de lege ferenda w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka. Ustalono, że obowiązujące regulacje prawne w tej kwestii nie spełniają wymogów kompletności i przewidywalności, ponieważ przede wszystkim nie zapewniają niezbędnych gwarancji proceduralnych, które mogłyby ograniczyć uprawnienia dyskrecjonalne strony oskarżenia podczas wyszukiwania, kopiowania i zabezpieczania informacji cyfrowych z telefonów komórkowych. Jednocześnie stwierdzono, że aktualna praktyka stosowania prawa w tym zakresie jest sprzeczna, ponieważ dopuszcza stosowanie różnych środków w celu legalizacji uzyskanych informacji, z których żaden nie spełnia w wystarczającym stopniu standardów zapewnienia prawa do prywatności sformułowanych w praktyce Europejskiego Trybunału Praw Człowieka. Dało to podstawy zarówno do poparcia niektórych propozycji sformułowanych w literaturze naukowej dotyczących rozszerzenia wykazu czynności śledczych (operatywnych), jak i do przedstawienia autorskich propozycji dotyczących udoskonalenia obowiązującego prawa karnego procesowego.

Słowa kluczowe: postępowanie karne, dochodzenie przedprocesowe, prawa człowieka, przeszukanie, dowody cyfrowe, Europejski Trybunał Praw Człowieka.

процесуальне законодавство в питанні регулювання проведення процесуальних дій із пошуку доказової інформації на цифрових пристроях не відповідає вимогам повноти, точності та передбачуваності в застосуванні.

Ще більше дискусійних питань викликає аспект пропорційності втручання в право на повагу до приватного спілкування (або в таємницю кореспонденції в термінології ЄКПЛ) у разі отримання під час проведення обшуку в житлі чи іншому володінні особи доступу до інформації, яка зберігається на мобільних телефонах. У такому разі в рамках аналізу увага може бути звернена на низку критеріїв, якот: характер та інтенсивність втручання (огляд інформації, її копіювання, вилучення мобільного телефону тощо), наслідки для самої особи та третіх осіб, тривалість втручання, наявність процесуальних гарантій, спрямованих на недопущення зловживань та свавілля під час проведення процесуальної дії з боку агентів держави та ін.

Стосовно останнього критерію, вочевидь, ключове значення може мати наявність ефективного судового контролю, оскільки саме слідчий суддя здатний забезпечити незалежну та об'єктивну оцінку доцільності втручання у таємницю спілкування за розглядуваних обставин. Проте, як було зазначено вище, цілеспрямований судовий контроль за втручанням у таємницю спілкування в такому разі відсутній. Більш детально про те, як саме нормативна регламентація цього питання може бути вдосконалена, відзначимо в останній частині нашої роботи.

Переходячи до аналізу окресленої проблематики з погляду de facto, можемо відмітити таке.

Щодо того, в якому саме порядку може бути здійснено судовий контроль на практиці, то акумулювання теоретичних і прикладних підходів дозволяє виокремити такі варіанти:

1) накладення арешту на майно. Зокрема, у своїй постанові від 4 червня 2025 р. (справа №686/20198/22) колегія суддів Третьої судової палати Касаційного кримінального суду Верховного Суду вказала на відсутність потреби додаткового звернення органу досудового розслідування за судовим дозволом (а саме ухвалою про тимчасовий доступ) у разі, якщо телефон, законно вилучений під час обшуку, надалі був визнаний речовим доказом та згідно з ухвалою слідчого судді на нього був накладений арешт[9]. Однак такий підхід, на наш погляд, не можна визнати повністю досконалим, оскільки в такому разі спрямованість судового контролю скерована на забезпечення пропорційності втручання в інше право – право власності, передусім щодо самого матеріального носія, а не інформації, яка на ньому міститься. А отже, питання про те, до якої цифрової інформації може бути отриманий доступ, чи може вона бути скопійована тощо, залишається поза межами контролю з боку слідчого судді, суду;

2) отримання тимчасового доступу до інформації, яка міститься на цифровому носії, навіть у разі, коли відповідні цифрові носії вже перебувають у володінні сторони обвинувачення, оскільки були вилучені під час проведення огляду чи обшуку[10]. Водночас, у судовій практиці може бути віднайдено й інший підхід, мотивований саме тим, що відповідні носії інформації вже і так утримуються стороною обвинувачення[11];

3) зняття інформації з електронних інформаційних систем[12]. Наведений підхід хоча дійсно і може найбільш точно відображати характер тих дій, що вчиняються, проте не враховує ту обставину, що відповідне дослідження інформації нерідко вже є відомим для особи, яка є володільцем відповідного цифрового пристрою, а отже, не відповідає ознаці негласності, безумовно властивій цій негласній слідчій (розшуковій) дії.

Проте, як ми зауважили вище у своїх коментарях до кожного із окреслених підходів, жоден із них не забезпечує в належний спосіб одночасно і відповідність правовій природі процесуальної дії, і спрямованість судового контролю за втручанням у фундаментальне право особи на повагу до приватного життя та таємницю спілкування. Зважаючи на це, стає очевидною потреба аналізу окресленої проблематики і з позиції de lege ferenda.

Для цього, насамперед, ще раз доцільно окреслити вихідні європейські стандарти, які мають бути взяті до уваги в такому разі. Отже, по-перше, нормативне врегулювання, зокрема і питанні правового характеру відповідної процесуальної дії, в межах якої відбувається доступ до інформації, що міститься на мобільному телефоні, вилученому під час проведення обшуку в житлі чи іншому володінні особи, має бути доступним і точним, а наслідки його застосування — передбачуваними; по-друге, з метою запобігання свавіллю під час проведення пошуку, виявлення та огляду інформації на мобільному телефоні такі дії мають супроводжуватися цілеспрямованим судовим контролем; по-третє, ухвала слідчого судді, суду стосовно цього питання повинна бути належним чином вмотивована та точна (конкре-

---

[9] Постанова колегії суддів Третьої судової палати Касаційного кримінального суду Верховного Суду [Decision of the Panel of Judges of the Third Judicial Chamber of the Cassation Criminal Court of the Supreme Court] від 4 червня 2025 р. (справа №686/20198/22). URL: https://protocol.ua/ua/postanova_kks_vp_vid_04_06_2025_roku_u_spravi_686_20198_22_1/

[10] Ухвала Луцького міськрайонного суду Волинської області [Order of the Lutsk City and District Court of Volyn Oblast] від 16 вересня 2022 р. (справа №161/12140/22). URL: https://reyestr.court.gov.ua/Review/106281527; Ухвала Кам'янець-Подільського міськрайонного суду Хмельницької області [Order of the Kamianets-Podilskyi City and District Court of Khmelnytskyi Oblast] від 6 грудня 2021 р. (676/7097/21). URL: https://reyestr.court.gov.ua/Review/101840315; Ухвала Індустріального районного суду м. Дніпропетровська [Order of the Industrial District Court of Dnipropetrovsk] від 2 вересня 2024 р. (справа №202/9526/24). URL: https://reyestr.court.gov.ua/Review/121311481.

[11] Ухвала Центрально-Міського районного суду м. Кривого Рогу Дніпропетровської області [Order of the Central City District Court of Kryvyi Rih, Dnipropetrovsk Oblast] від 10 листопада 2022 р. (справа № 216/2987/22). URL: https://reyestr.court.gov.ua/Review/107233029; Постанова колегії суддів Першої судової палати Касаційного кримінального суду Верховного Суду [Decision of the Panel of Judges of the First Judicial Chamber of the Cassation Criminal Court of the Supreme Court] від 11 вересня 2025 р (справа №601/1913/18). URL: https://reyestr.court.gov.ua/Review/130271025

[12] Ухвала Вінницького міського суду Вінницької області [Order of the Vinnytsia City Court, Vinnytsia Region] від 1 вересня 2022 р. (справа №127/17774/22). URL: https://reyestr.court.gov.ua/Review/106103464

тизована), щоб не допускати занадто широких дискреційних повноважень сторони обвинувачення вже на етапі пошуку та вилучення цифрової інформації; по-четверте, у випадку роботи з цифровою інформацією на мобільному телефоні така конкретизація повинна, серед іншого, уточнювати ті програми та додатки, які можуть бути відкриті та досліджені під час пошуку на мобільному телефоні відомостей, що можуть мати доказове значення; по-п'яте, за відсутності попереднього судового контролю має бути забезпечено інший ефективний засіб захисту – наприклад, процесуальну можливість оскарження дій сторони обвинувачення з виявлення, копіювання, дослідження інформації на мобільних телефонах, що в разі задоволення скарги могла б мати наслідком рішення про припинення подальших дій та зобов'язання знищити знайдену/ скопійовану/ вилучену інформацію.

У світлі наведеного відмітимо, що в останні роки було висловлено досить багато ідей про те, як саме відповідний судовий контроль може бути забезпечений. Загальний концепт, на наш погляд, може бути побудований на висловленій А. В. Скрипником пропозиції адаптації досвіду окремих країн до вітчизняного кримінального процесуального законодавства щодо запровадження правила «закритого контейнера», яким би передбачався двоступеневий судовий контроль за обмеженням права особи на таємницю спілкування[13].

Ця ідея отримала досить детальну наукову розробку в монографічному дослідженні І. А. Смаль, яка пропонує низку істотних оновлень до кримінального процесуального законодавства, серед яких, зокрема, і пропозиція доповнення КПК новою статтею 236-1 «Обшук комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку». На думку авторки, ця норма повинна містити як вимоги до клопотання сторони обвинувачення щодо форми і змісту, процесуального порядку його розгляду, так і підстави для задоволення такого клопотання, включно з локальним предметом доказування в цьому разі[14].

З огляду на окреслені вище стандарти і проблеми в чинній нормативній регламентації, убачаємо за можливе концептуально підтримати пропозицію І. А. Смаль як таку, що може кардинально змінити законодавчі підходи і вирішити переважну кількість описаних у попередній частині роботи прикладних проблем. Поряд із цим, на нашу думку, можуть бути запропоновані ще два допустимі шляхи оновлення кримінального процесуального законодавства: по-перше, шляхом уточнення релевантних положень ч. 3 ст. 234, ч. 2 ст. 235 КПК посиланням на необхідність зазначення як у клопотанні сторони обвинувачення, так і в ухвалі слідчого судді, суду того, яка саме інформація може бути відшукана на мобільних телефонах та які програми чи додатки можуть бути для цього відкриті; по-друге, шляхом розширення предмета оскарження, що встановлений у ч. 1 ст. 303 КПК, а саме його доповнення діями слідчого, дізнавача, прокурора з виявлення, копіювання, дослідження інформації на мобільних телефонах, одночасно із уточненням у ч. 2 ст. 307 КПК вказівкою на припинення подальших дій та зобов'язання знищити знайдену, скопійовану, вилучену інформацію.

Висновки. Значний масив інформації, зокрема і комунікативного характеру, що міститься на сучасних мобільних телефонах, відносна легкість доступу до неї, а також можливість виявлення та вилучення інформації, що зберігається віддалено (наприклад, у хмарних сховищах) через вхід до відповідних програм і додатків на мобільному телефоні, істотно розширює межі можливого втручання у право на повагу до приватності (зокрема, і таємницю кореспонденції). Це змушує інакше поглянути на ті стандарти та процесуальні гарантії, що мають бути забезпечені під час отримання доступу до інформації на мобільних телефонах, що вилучаються під час проведення обшуку в житлі чи іншому володінні особи.

Водночас системний аналіз чинних положень кримінального процесуального законодавства засвідчив відсутність достатньої та точної нормативно-правової основи з цього питання, що враховувала б одночасно і характер вчинюваних процесуальних дій, і необхідні запобіжники проти свавілля – насамперед цілеспрямований судовий контроль за втручанням у відповідне фундаментальне право. Адже наразі запроваджений у 2022 р. огляд комп'ютерних даних не вимагає отримання окремого судового дозволу і до того ж не охоплює дії з пошуку та копіювання інформації з комп'ютерних систем.

Так само недосконалою залишається і сучасна судова практика з цього питання, оскільки наявні процесуальні дії (передусім накладення арешту на майно, тимчасовий доступ до речей і документів або зняття інформації з електронних інформаційних систем), що застосовуються для подібних ситуацій роботи з інформацією на мобільних телефонах, не враховують специфічних ознак цифрових даних і тих процесуальних вимог, що доцільно забезпечити при їх використанні в кримінальному провадженні з огляду на практику ЄСПЛ.

З огляду на це у роботі підтримується висловлена в науковій літературі ідея запровадження нової слідчої (розшукової) дії – т. зв. «цифрового обшуку». Поряд із цим також пропонуються зміни до чинного кримінального процесуального законодавства стосовно розширення переліку інформації, що має бути зазначена в клопотанні та ухвалі про дозвіл на обшук, а також передбачення можливості оскарження у порядку, регламентованому ст. ст. 303–307 КПК, дій сторони обвинувачення з виявлення, копіювання та вилучення інформації з мобільних телефонів.

References

Bernardini L., Sanvitale F. Searches and seizures of electronic devices in European criminal proceedings:a new pattern for independent review? Revista Ítalo-Española de Derecho Procesal. 2023.Num. 1. Pp. 73-119. DOI: 10.37417/rivitsproc/1475

[13] Скрипник А. Правило «закритого контейнеру» в українських правових реаліях [The 'closed container' rule in the Ukrainian legal context] . Кримінальний процес: сучасний вимір та проспективні тенденції : ІІ Харк. кримінал. процесуал. полілог : присвяч. актуал. питанням застосування заходів забезпечення кримінал. провадження (м. Харків, 12 груд. 2019 р.) / редкол. О. В. Капліна, В. І. Маринів, О. Г. Шило. Харків : Право, 2020. С. 29–31.

[14] Смаль І. А. Теоретичні та практичні аспекти використання електронних доказів у кримінальному процесі України [Theoretical and practical aspects of the use of electronic evidence in criminal proceedings in Ukraine] : монографія / І. А. Смаль. Київ : Прес, 2025. С. 271-273.

Vapniarchuk V. V. Shchodo doslidzhennia zmistu elektronnykh informatsiinykh system, kompiuternykh system abo yikh chastyn, mobilnykh terminaliv system zviazku pid chas kryminalnoho provadzhennia [Regarding the examination of the contents of electronic information systems, computer systems or parts thereof, and mobile terminals of communication systems during criminal proceedings]. Analitychno-porivnialne pravoznavstvo. 2025. Vyp. 2. S. 970. URL: https://app-journal.in.ua/wp-content/uploads/2025/04/146.pdf .

Demura M., Krytska I., Klepka D. Zabezpechennia prav ta zakonnykh interesiv osoby v umovakh «didzhytalizatsii» kryminalnoho provadzhennia [Safeguarding the rights and legitimate interests of individuals in the context of the 'digitalisation of criminal proceedings]. Chasopys Kyivskoho universytetu prava. 2020/1. S. 297. DOI: 10.36695/2219-5521.1.2020.60

Konventsiia pro kiberzlochynnist [Convention on Cybercrime] (pidpysana 23 lystopada 2001 r., ratyfikovana iz zasterezhenniamy i zaiavamy Zakonom № 2824-IV vid 7 veresnia 2005 r. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text .

Metelev, O. P. Shchodo sposobiv zbyrannia i formuvannia tsyfrovykh dokaziv u kryminalnomu provadzhenni [On Methods for Collecting and Compiling Digital Evidence in Criminal Proceedings]. 2024. Visnyk kryminalnoho sudochynstva, Vyp. 3-4. S. 52, 54. https://doi.org/10.17721/2413-5372.2023.3-4/47-58

Postanova kolehii suddiv Pershoi sudovoi palaty Kasatsiinoho kryminalnoho sudu Verkhovnoho Sudu [Decision of the Panel of Judges of the First Judicial Chamber of the Cassation Criminal Court of the Supreme Court] vid 11 veresnia 2025 r (sprava №601/1913/18). URL: https://reyestr.court.gov.ua/Review/130271025

Postanova kolehii suddiv Tretoi sudovoi palaty Kasatsiinoho kryminalnoho sudu Verkhovnoho Sudu [Decision of the Panel of Judges of the Third Judicial Chamber of the Cassation Criminal Court of the Supreme Court] vid 4 chervnia 2025 r. (sprava №686/20198/22). URL: https://protocol.ua/ua/postanova_kks_vp_vid_04_06_2025_roku_u_spravi_686_20198_22_1/

Pro vnesennia zmin do Kryminalnoho protsesualnoho kodeksu Ukrainy shchodo pidvyshchennia efektyvnosti dosudovoho rozsliduvannia za «hariachymy slidamy» ta protydii kiberatakam [On Amendments to the Criminal Procedure Code of Ukraine to Improve the Effectiveness of Pre-Trial Investigations Conducted in Real Time and to Counter Cyberattacks]: Zakon Ukrainy № 2137-IX vid 15 bereznia 2022 r. URL: https://zakon.rada.gov.ua/laws/show/2137-20#n12.

Rishennia YeSPL u spravi «Potoczka i Adamco proty Slovachchyny» [ECHR Judgment in the Case of Potoczka and Adamco v. Slovakia] (zaiava №7286/16) vid 12 sichnia 2023 r. URL: https://hudoc.echr.coe.int/eng?i=001-222143

Rishennia YeSPL u spravi «Roman Zakharov proty Rosii» [ECHR Judgment in the Case of Roman Zakharov v. Russia] [VP] (zaiava № 47143/06) vid 4 hrudnia 2015 r. URL: https://hudoc.echr.coe.int/eng?i=001-159324

Skrypnyk A. Pravylo «zakrytoho konteineru» v ukrainskykh pravovykh realiiakh [The 'closed container rule in the Ukrainian legal context] . Kryminalnyi protses: suchasnyi vymir ta prospektyvni tendentsii : II Khark. kryminal. protsesual. poliloh : prysviach. aktual. pytanniam zastosuvannia zakhodiv zabezpechennia kryminal. provadzhennia (m. Kharkiv, 12 hrud. 2019 r.) / redkol. O.V. Kaplina, V.I. Maryniv, O.H. Shylo. Kharkiv : Pravo, 2020. S. 29–31.

Skrypnyk A.V. Tsyfrovyi obshuk: buty chy ne buty? [Digital searches: to be or not to be?] Tsyfrovizatsiia kryminalnoho provadzhennia: stan ta perspektyvy : materialy nauk.-prakt. kruhloho stolu, m. Kharkiv, 19 veres. 2024 r. / [redkol.: N. V. Hlynska (holov. red.), D. I. Klepka, A. A. Barabash] ; NDI vyvch. problem zlochynnosti im. akad. V. V. Stashysa NAPrN Ukrainy ; Vid. doslidzh. problem krymin. protsesu ta sudoustroiu. Kharkiv : Pravo, 2024. S. 148-149.

Smal I. A. Teoretychni ta praktychni aspekty vykorystannia elektronnykh dokaziv u kryminalnomu protsesi Ukrainy [Theoretical and practical aspects of the use of electronic evidence in criminal proceedings in Ukraine] : monohrafiia / I.A. Smal. Kyiv: Pres, 2025. S. 271-273.

Ukhvala Vinnytskoho miskoho sudu Vinnytskoi oblasti [Order of the Vinnytsia City Court, Vinnytsia Region] vid 1 veresnia 2022 r. (sprava №127/17774/22). URL: https://reyestr.court.gov.ua/Review/106103464

Ukhvala Industrialnoho raionnoho sudu m. Dnipropetrovska [Order of the Industrial District Court of Dnipropetrovsk] vid 2 veresnia 2024 r. (sprava №202/9526/24). URL: https://reyestr.court.gov.ua/Review/121311481

Ukhvala Kamianets-Podilskoho miskraionnoho sudu Khmelnytskoi oblasti [Order of the Kamianets-Podilskyi City and District Court of Khmelnytskyi Oblast] vid 6 hrudnia 2021 r. (676/7097/21). URL: https://reyestr.court.gov.ua/Review/101840315

Ukhvala Lutskoho miskraionnoho sudu Volynskoi oblasti [Order of the Lutsk City and District Court of Volyn Oblast] vid 16 veresnia 2022 r. (sprava №161/12140/22). URL: https://reyestr.court.gov.ua/Review/106281527

Ukhvala Tsentralno-Miskoho raionnoho sudu m. Kryvoho Rohu Dnipropetrovskoi oblasti [Order of the Central City District Court of Kryvyi Rih, Dnipropetrovsk Oblast] vid 10 lystopada 2022 r. (sprava № 216/2987/22). URL: https://reyestr.court.gov.ua/Review/107233029

Надійшла до редколегії: 02.02.2026 / Рецензовано 17.03.2026 / Прийнято до друку 29.04.2026 / Доступно онлайн 30.05.2026

Приклад цитування:

Роганін, М. (2026). Огляд персональної інформації в мобільних телефонах під час проведення обшуку: підходи de facto, de jure та de lege ferenda. *Архів кримінології та судових наук.* 1 (13).115-122. DOI: https://doi.org/10.32353/acfs.13.2026.09