УДК 343.1:343.98:004.056(4)«2020»
DOI https://doi.org/10.32782/2524-0374/2025-8/46

ВИКОРИСТАННЯ ДАНИХ ENCROCHAT[1] У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПОРІВНЯЛЬНО-ПРАВОВИЙ ТА ПРОЦЕСУАЛЬНИЙ АНАЛІЗ

USE OF ENCROCHAT[2] DATA IN CRIMINAL PROCEEDINGS: A COMPARATIVE LEGAL AND PROCEDURAL ANALYSIS

Погорецький М.А., д.ю.н., професор, член-кореспондент
Національної академії правових наук України, заслужений діяч науки і техніки України,
проректор з науково-педагогічної роботи
Київський національний університет імені Тараса Шевченка

У статті проведено комплексний порівняльно-правовий та процесуальний аналіз використання даних платформи зашифрованих комунікацій ***EncroChat*** у кримінальному провадженні. Досліджено техніко-процесуальні механізми отримання, збереження, передачі й верифікації цифрових доказів; окремо розмежовано підходи до контенту повідомлень і телекомунікаційних метаданих, а також вимоги до їх цільового та пропорційного збирання. Розкрито правову рамку Європейського наказу про розслідування (EIO) відповідно до Директиви 2014/41/ЄС, практику Суду Європейського Союзу щодо транскордонного використання цифрових доказів, а також стандарти Європейського суду з прав людини стосовно пропорційності, необхідності, процесуальних гарантій, мінімізації даних і охорони «ядра приватного життя». Особливу увагу приділено досвіду Франції, Нідерландів і Німеччини: висвітлено принцип «внутрішньої еквівалентності» щодо допустимості доказів, обмеження на використання результатів негласних слідчих (розшукових) дій, процесуальні наслідки для «похідних» доказів, а також концепцію презумпції законності дій іноземних органів за умови подальшого ефективного судового контролю у державі використання.

На цій основі сформульовано пропозиції щодо вдосконалення Кримінального процесуального кодексу України для гармонізації з європейськими стандартами. Пропонується: уніфікувати підстави й межі втручання у приватне життя при доступі до зашифрованих комунікацій; запровадити чіткі процесуальні інструкції щодо ланцюга збереження (chain of custody), хеш-ідентифікації, протоколювання та незалежної технічної валідації; передбачити спеціальні правила для «онлайн-обшуку» й віддаленого проникнення, включно з судовим дозволом, постконтролем і доктриною мінімізації; деталізувати критерії достатності підстав і конкретизації об'єкта втручання; визначити допустимі межі використання «похідних» доказів і процесуальні фільтри для їх оцінки судом; кодифікувати презумпцію належності іноземних доказів із можливістю її спростування стороною захисту. Зазначені зміни спрямовані на підвищення передбачуваності правозастосування, зміцнення змагальності та ефективності судового контролю, збільшення доказової надійності цифрових матеріалів і, водночас, на посилення гарантій прав людини у справах, що ґрунтуються на даних ***EncroChat*** та аналогічних платформ.

Ключові слова: EncroChat; цифрові докази, Європейський наказ про розслідування (EIO), Директива 2014/41/ЄС, Суд ЄС, ЄСПЛ, пропорційність, мінімізація даних, «ядро приватного життя», внутрішня еквівалентність, негласні слідчі (розшукові) дії, ланцюг збереження доказів, онлайн-обшук, транскордонне провадження, допустимість доказів, КПК України.

The article offers a comprehensive comparative-legal and procedural analysis of the use of data from the ***EncroChat*** encrypted communications platform in criminal proceedings. It examines the technical and procedural mechanisms for obtaining, preserving, transferring, and verifying digital evidence; distinguishes the treatment of message content and telecommunications metadata; and sets out the requirements for their targeted and proportionate collection. The legal framework of the European Investigation Order (EIO) under Directive 2014/41/EU is unpacked alongside the case law of the Court of Justice of the European Union (CJEU) on cross-border use of digital evidence and the standards of the European Court of Human Rights (ECtHR) concerning proportionality, necessity, procedural safeguards, data minimisation, and protection of the "inner core of private life." Particular attention is paid to the experiences of France, the Netherlands, and Germany, including the "internal equivalence" principle for evidence admissibility, restrictions on the use of results from covert investigative (search) actions, the procedural consequences for "derivative" evidence, and the presumption of lawfulness of foreign authorities' actions subject to effective ex post judicial control in the state of use.

On this basis, the paper formulates proposals to refine the Criminal Procedure Code of Ukraine in order to harmonise with European standards. It is proposed to standardise the grounds and limits of intrusions into private life when accessing encrypted communications; introduce clear procedural instructions on chain of custody, hash-based identification, logging, and independent technical validation; provide special rules for "online search" and remote intrusion, including prior judicial authorisation, ex post review, and a minimisation doctrine; detail the criteria for sufficiency of grounds and specificity of the object of intrusion; define permissible limits on the use of "derivative" evidence together with procedural filters for its judicial assessment; and codify a rebuttable presumption of regularity for foreign-obtained evidence. These changes aim to increase the predictability of law-application, strengthen adversarial principles and the effectiveness of judicial oversight, enhance the evidentiary reliability of digital materials, and, at the same time, reinforce human-rights safeguards in cases that rely on ***EncroChat*** data and analogous platforms.

Key words: EncroChat; digital evidence, European Investigation Order (EIO), Directive 2014/41/EU, CJEU, ECtHR, proportionality, data minimisation, "inner core of private life", internal equivalence, covert investigative (search) actions, chain of custody, online search, cross-border proceedings, admissibility of evidence, Criminal Procedure Code of Ukraine.

[1] EncroChat («ЕнкроЧат») – платформа зашифрованих комунікацій. EncroChat EncroChat був спеціальним зашифрованим сервісом обміну повідомленнями, популярним серед кримінальних угруповань, бо обіцяв анонімність і захист від перехоплення. Телефони EncroChat продавалися з модифікованою операційною системою, без GPS і камери, з кнопкою «панічного видалення» всіх даних. У 2020 році французька поліція разом з нідерландською, за підтримки Європолу, зламала EncroChat і таємно встановила програмне забезпечення, яке передавало всі повідомлення користувачів у режимі реального часу. У результаті були отримані сотні мільйонів повідомлень, з яких значна частина стосувалася кримінальних злочинів (наркоторгівля, зброя, відмивання грошей тощо).

[2] EncroChat – Encrypted communications platform. EncroChat was a specialized encrypted messaging service popular among criminal groups because it promised anonymity and protection against interception. EncroChat phones were sold with a modified operating system, without GPS and a camera, and featured a «panic wipe» button to erase all data instantly. In 2020, the French police, together with the Dutch police and with the support of Europol, hacked EncroChat and covertly installed software that transmitted all users' messages in real time. As a result, hundreds of millions of messages were obtained, a significant portion of which concerned criminal offenses (drug trafficking, firearms, money laundering, etc.).

Постановка проблеми. Сучасні виклики у сфері кримінальної юстиції, зумовлені цифровізацією комунікацій та поширенням зашифрованих сервісів обміну повідомленнями, істотно ускладнюють процес виявлення, фіксації та використання доказів у кримінальному провадженні. Одним із найрезонансніших прикладів стала операція з інфільтрації платформи зашифрованих комунікацій ***EncroChat*** *(«ЕнкроЧат»)* (далі – ***EncroCha***t), проведена у 2020 році правоохоронними органами Франції та Нідерландів за координації Агентства Європейського Союзу з питань правоохоронної співпраці (Європолу). Ця операція продемонструвала безпрецедентний масштаб транскордонного збору цифрових доказів і актуалізувала комплекс проблем, пов'язаних із правовою допустимістю, пропорційністю та міжнародною передачею таких даних.

Особливу складність становить правова оцінка цифрових доказів, отриманих унаслідок спеціальних технічних операцій за межами національної юрисдикції, та їх подальше використання в кримінальному процесі іншої держави. Недостатня деталізація національних процедур і відсутність єдиного підходу до перевірки «внутрішньої еквівалентності» (*internal equivalence test*) створюють ризик визнання таких доказів недопустимими, що може призвести до порушення прав людини, гарантованих статтями 8 і 10 Конвенції про захист прав людини і основоположних свобод [1].

Проблематика ускладнюється відсутністю у кримінальному процесуальному законодавстві України чіткої регламентації порядку отримання, перевірки та використання цифрових доказів, здобутих у результаті міжнародного співробітництва, зокрема за механізмом Європейського наказу про розслідування (*European Investigation Order, EIO*) відповідно до Директиви 2014/41/ЄС Європейського парламенту та Ради від 3 квітня 2014 р. щодо Європейського наказу про розслідування у кримінальних справах [2]. У цьому контексті досвід держав – членів ЄС, які вже виробили процесуальні фільтри та правові запобіжники, набуває особливого значення для удосконалення національної правової системи.

Аналіз останніх досліджень і публікацій. У зарубіжній літературі сформувалася низка підходів до оцінки правомірності масштабних технічних операцій з інфільтрації зашифрованих сервісів і використання добутих цифрових доказів.

Оглядово-порівняльний аналіз, проведений Й.Й. Оерлемансом (J.J. Oerlemans) та Т. ван Тоором (T. van Toor), висвітлює правові аспекти операції ***EncroChat*** крізь призму прав людини, акцентуючи на процесуальних гарантіях, стандартах необхідності та пропорційності, а також на викликах для механізму взаємного визнання рішень у ЄС. Автори пропонують критерії для оцінки допустимості великих масивів перехоплених даних у транскордонних кримінальних провадженнях. Спираючись на практичний досвід Нідерландів у проведенні «розслідувань, заснованих на даних» (*data-driven investigations*) у справах ***EncroChat***, вони детально описують технікопроцесуальну архітектуру збирання й відбору даних, роль національних та європейських інструментів співпраці, а також пропонують конкретні підходи, як у процесі обробки перехопленої інформації автоматично відсівати дані, що не стосуються предмета кримінального провадження, та мінімізувати обсяг інформації про приватне життя осіб, не причетних до правопорушень [3, 4].

У контексті права на справедливий судовий розгляд і визначення допустимості цифрових доказів, отриманих у результаті масштабних перехоплень, Радіна Стойкова (Radina Stoykova) досліджує концепцію так званого «*хакера з ордером*» – ситуації, коли державні органи отримують судовий дозвіл на злам захищених комунікаційних систем. Авторка розглядає, де проходить межа між законним отриманням інформації та порушенням принципів справедливого процесу, аналізує ризики, пов'язані з масовим збором приватних комунікацій, та наголошує на важливості дотримання чітких стандартів доведення, щоб такі докази були визнані судом допустимими [5].

У широко відомій колективній монографії під редакцією С. Мейсона (S. Mason) та Д. Сенга (D. Seng) систематизовано міжнародні підходи до забезпечення автентичності та цілісності цифрових доказів, підтримання безперервного «ланцюга збереження» (*chain of custody*) і застосування належних стандартів доказування під час їх використання у кримінальному провадженні [6].

Український науковий сегмент, присвячений безпосередньо дослідженню феномену ***EncroChat***, на момент підготовки цієї статті не виявлений (джерела не знайдені). Водночас у суміжній тематиці – електронні та цифрові докази, розслідування злочинів у кіберпросторі, міжнародна правова допомога у сфері отримання та використання цифрової інформації – накопичено певний масив академічних напрацювань.

До прийняття КПК України 2012 р. проблемні питання електронних доказів у контексті проведення окремих оперативно-розшукових заходів, спрямованих на зняття інформації з телекомунікаційних систем та інших каналів зв'язку, здебільшого висвітлювалися у виданнях з обмеженим доступом (К. Антонов, О. Долженков, І. Козаченко, Д. Нікіфорчук, Ю. Орлов, М. Шумило та ін.).

Однією з перших відкритих монографій, присвячених зняттю інформації з каналів зв'язку за КПК України 1960 року, де комплексно проаналізовано проблемні питання кримінального процесу та криміналістики, була праця Д. Сергєєвої. Ця робота заклала концептуальні засади для подальшого унормування відповідних положень у КПК України 2012 року та стала підґрунтям для нових досліджень у зазначеній сфері [7].

Із прийняттям КПК України 2012 року кількість наукових досліджень, присвячених проблемам кіберзлочинності та електронних доказів, істотно зросла. Цю тенденцію зумовили як зміни у кримінальному процесуальному законодавстві, так і зростання практичних потреб у протидії злочинності у кіберпросторі, необхідність її належного документування та широкого використання цифрових доказів у кримінальному провадженні. Помітний внесок у розвиток теоретичних і прикладних аспектів цієї проблематики зробили, зокрема, О. Метелєв, Ю. Орлов, А. Скрипник, В. Шеломенцев, С. Чернявський, Д. Цехан та інші дослідники [8-11].

Питання, пов'язані з особливостями розслідування та доказування злочинів у сфері використання інформаційних технологій, а також документуванням різних видів кримінальних правопорушень із застосуванням електронних засобів у межах оперативно-розшукових заходів та негласних слідчих (розшукових) дій, стали предметом цілого ряду авторських досліджень [12-24]. Зазначені напрацювання становлять методологічну основу для підготовки цієї статті.

Мета дослідження – виробити на основі аналізу операції з інфільтрації платформи зашифрованих комунікацій ***EncroChat*** та порівняльно-правового дослідження європейських і національних підходів комплекс пропозицій щодо удосконалення кримінального процесуального законодавства України, який забезпечить допустимість цифрових доказів, отриманих унаслідок транскордонних операцій, із дотриманням стандартів пропорційності, необхідності та захисту прав людини.

Виклад основного матеріалу дослідження. Операція з інфільтрації зашифрованого комунікаційного сервісу *EncroChat*, здійснена у 2020 році французькими правоохоронними органами у співпраці з нідерландськими колегами та за координації Агентства Європейського Союзу з питань правоохоронної співпраці (далі – Європол), стала

безпрецедентним прикладом масштабного транскордонного збору цифрових доказів і фактично задала стандарт подальшої практики їх використання в Європейському Союзі (далі – ЄС) [25]. У ході цієї операції на пристрої користувачів було інстальовано спеціальне програмне забезпечення, що забезпечило перехоплення повідомлень у режимі реального часу; отримані дані фіксували факти незаконного обігу наркотиків, зброї, відмивання коштів та інших тяжких злочинів. Надалі вони були передані компетентним органам інших держав-членів через механізм Європейського наказу про розслідування (далі – ЕІО) відповідно до Директиви 2014/41/ЄС [2]. Водночас широкомасштабне використання цих доказів у національних провадженнях зумовило значний масив спорів – насамперед щодо приватності, пропорційності та критеріїв допустимості транскордонних цифрових доказів.

З огляду на зазначене, подальший аналіз проводиться крізь призму трьох взаємопов'язаних рівнів: (а) технікопроцесуального – механізми одержання і передачі даних, судовий контроль у державі-джерелі та межі їх подальшого використання; (б) наднаціонального – Європейський наказ про розслідування (ЕІО) за Директивою 2014/41/ЄС і критерії, сформульовані Судом Європейського Союзу (Суд ЄС) *у справі C-670/22*; (в) прав людини – стандарти Європейського суду з прав людини (ЄСПЛ) щодо необхідності та пропорційності втручання, а також охорони «ядра приватного життя» [26; 27; 28].

У цьому контексті терміни вживаються так: *«онлайн-обшук»* – негласне проникнення до інформаційних систем або пристроїв із віддаленим доступом до контенту та/або метаданих, що здійснюється виключно за судовою санкцією для розслідування тяжких злочинів і супроводжується процесуальними обмеженнями подальшого використання результатів. Такий підхід відповідає німецькій судовій практиці, де, наприклад, Федеральний суд Німеччини (*Bundesgerichtshof*) визначає суворі критерії допустимості використання даних, отриманих шляхом віддаленого доступу, вимагаючи чіткого обґрунтування необхідності та пропорційності втручання [28].

«Тест внутрішньої еквівалентності» – вимога, за якою передача чи використання «вже наявних» у держави-виконавця доказів у порядку Європейського ордера на розслідування (ЕІО) допускається лише тоді, коли аналогічний захід міг би бути застосований у внутрішній ситуації цієї держави за дотримання її власних правових стандартів. Це охоплює вимоги щодо наявності судової санкції, чіткого визначення обсягу втручання, строків виконання та перевірки пропорційності. Суд ЄС у справі *C-670/22* підкреслив, що під час виконання ЕІО необхідно забезпечувати такий рівень процесуальних гарантій, який відповідає національним конституційним вимогам, а також принципам права ЄС [26].

«Дані електронних комунікацій» – відомості, що виникають у процесі надання чи використання електронних комунікаційних послуг (зокрема, зміст повідомлень, трафік/метадані, системні журнали доступу тощо) та можуть бути предметом одержання, передачі і використання як доказів. При цьому застосовуються вимоги, визначені правом ЄС та релевантною національною практикою: наприклад, німецьке законодавство (§ 100e(6) StPO) та відповідні судові рішення встановлюють детальні процесуальні умови доступу до таких даних і контролю за їх використанням [2; 29; 30].

Директива 2014/41/ЄС Європейського парламенту та Ради від 3 квітня 2014 року визначає *Європейський ордер на розслідування* (*EIO, European Investigation Order*) як судове чи інше компетентне процесуальне рішення, видане органом однієї держави-члена ЄС з метою виконання одного або кількох конкретних процесуальних дій в іншій державі-члені для отримання доказів, а також передачі вже наявних у держави-виконавця доказів [2].

Європейський ордер на розслідування ґрунтується на принципі взаємного визнання рішень у кримінальних справах між державами-членами, поширюється на будь-які види доказів та вимагає дотримання національних гарантій у державі-виконавці, зокрема щодо необхідності, пропорційності, судового контролю, строків і обсягу втручання. Нормативна рамка передбачає, що перед виданням ЕІО компетентний орган держави-видавця зобов'язаний провести два базові тести, визначені статтею 6(1) Директиви: *необхідності та пропорційності*, а також перевірку релевантності заходу умовам «порівнюваної внутрішньої справи» цієї держави.

У статті 1(1) Директиви закріплено, що ЕІО може використовуватися на будь-якій стадії кримінального провадження, включно з досудовим, судовим та апеляційним, а також у провадженнях, які можуть призвести до розгляду справи судом про вчинення кримінального правопорушення. Директива замінює низку фрагментарних механізмів правової допомоги (зокрема, Конвенцію 2000 року [31]. та Рамкове рішення 2003/577/ПВП) [32] єдиною уніфікованою процедурою.

Окремі положення Директиви (статті 30–31) регламентують спеціальні правила для перехоплення телекомунікацій, включно з режимом повідомлення та можливістю заборони або обмеження використання протягом 96 годин у випадках перехоплення без технічної допомоги «повідомленої» держави [2].

У контексті ***EncroChat*** ці приписи фактично «перехопили» і спрямували подальший рух доказів: виконання ЕІО має відбуватися «як у внутрішній справі» із повагою до формальностей, зазначених у наказі, тоді як у випадку «вже наявних» у держави-виконавця доказів ключовою стає оцінка відповідності заходу внутрішньому стандарту цієї держави.

Процесуальну «точку законності» сформовано ухвалою суду першої інстанції м. Лілль (*tribunal correctionnel de Lille*), якою, зокрема, дозволено інсталяцію спеціального програмного забезпечення (ПЗ) типу «троян» на сервер/пристрої ***EncroChat*** та подальше використання й передачу даних у провадження інших держав-членів [33]; ці обставини відтворені у мотивувальній частині рішення Суду Європейського Союзу (СЄС, Court of Justice of the European Union, CJEU) (далі – (Суд ЄС) *у справі C-670/22* (пп. 20, 27) [26].

Французька procedural anchor: tribunal correctionnel de Lille надав судовий дозвіл на впровадження спеціального програмного забезпечення («трояна») в операційні системи пристроїв ***EncroChat,*** створивши процесуальну базу («*anchor decision*»)[3] для подальшої передачі матеріалів у транскордонному порядку. Слід акцентувати увагу на тому, що французьке кримінальне процесуальне право допускає такі заходи за суворого судового контролю, що посилило презумпцію їх законності поза межами Франції [33].

Нідерландський підхід спирався на принцип міждержавної довіри («*interstatelijk vertrouwensbeginsel*»): за відсутності явних порушень виходять із законності дій іноземних органів та достовірності їх результатів. 13.06.2023 Верховний суд Нідерландів (Hoge Raad) у порядку преюдиційного запитання[4] (запит на попереднє тлумачення) (*prejudiciële vragen*) підтвердив релевантність цього принципу для ***EncroChat/SkyeECC*** та окреслив процесуальні запобіжники щодо відбору даних із великих масивів [4].

Федеральний суд Німеччини (Bundesgerichtshof, далі – BGH) у рішенні від *02.03.2022 (5 StR 457/21*) визнав

[3] У контексті справи EncroChat цей термін означає первинне судове рішення (ухвалу), яке створює законну підставу для проведення слідчих дій і подальшої транскордонної передачі зібраних даних.

[4] У нідерландському та праві ЄС це означає питання, які національний суд ставить Суду Європейського Союзу для отримання офіційного тлумачення норм права ЄС перед ухваленням рішення у справі.

можливість використання даних ***EncroChat*** у справах про тяжкі злочини за умови дотримання національних процесуальних гарантій. Отримання таких даних суд кваліфікував за функцією як аналог «онлайн-обшуку» (§ 100b Кримінально-процесуального кодексу Німеччини [30] (далі – StPO)), поширив на них жорсткі обмеження використання за аналогією (§ 100e(6) StPO) та застосував принцип вільної оцінки доказів (§ 261 StPO). При цьому BGH наголосив на необхідності проведення тесту допустимості індивідуально для кожної справи (*case-by-case*) з урахуванням вимог пропорційності та процесуальних гарантій [26, 35]. Такий підхід відображає не ізольовану оцінку технічної операції, а вбудовування її результатів у звичні національні процесуальні «фільтри».

Федеральний конституційний суд Німеччини (BVerfG) (*2 BvR 684/22, 01.11.2024*) відхилив скаргу щодо ***EncroChat*** як неприйнятну, вказавши, що використання не торкнулося «ядра приватного життя», а за наявності чіткої законодавчої бази і пропорційності не суперечить Основному Закону; додатково підтверджено, що національна перевірка Федерального суду Німеччини (*Bundesgerichtshof, BGH*) співзвучна вимозі «внутрішньої еквівалентності» права ЄС [36; 37]. BVerfG, розглядаючи конституційну скаргу щодо ***EncroChat****,* уточнив, що втручання у приватність не виходило за межі «ядра приватного життя», а отже, за наявності достатньо чіткої законодавчої підстави і дотримання принципу пропорційності використання доказів не суперечить Основному Закону; додатково наголошено, що BGH фактично реалізував вимогу «внутрішньої еквівалентності» (*internal equivalence*) права ЄС [36; 37].

На наднаціональному рівні Суд ЄС у *справі C-670/22, M.N.* сформулював загальний орієнтир: передача «вже наявних» у держави-виконавця доказів у порядку EIO є допустимою лише тоді, коли аналогічний захід міг би бути застосований у подібній внутрішній ситуації за правом цієї держави; таким чином, пропорційність і «внутрішня еквівалентність» утворюють подвійний фільтр законності [26]. Власне ця позиція Суду ЄС концептуально пов'язує «презумпцію законності» взаємного визнання з обов'язковою локальною валідацією засобів збору/використання даних у державі-виконавці.

Практичний наслідок *C-670/22, M.N.* – вимога, щоб «внутрішня еквівалентність» перевірялася не лише на етапі передачі, а й при подальшому використанні у суді; це підсилює роль слідчого судді/прокурора у державі-виконавці при оцінці релевантності, необхідності і пропорційності отриманого масиву даних [26].

Узагальнюючи напрацьовану практику у справах ***EncroChat,*** можна констатувати таке:

(1) Франція забезпечила первинну процесуальну «точку законності» (судовий дозвіл і контроль), що легітимувало транскордонний рух даних [33];

(2) Нідерланди, спираючись на взаємне визнання, виходили з презумпції законності іноземного збору доказів за відсутності явних вад [34; 38];

(3) Німеччина виробила модель індивідуальної оцінки допустимості із вмонтованими обмеженнями використання результатів (§§ 100b/100e(6)/261 StPO) [30] і з подальшою конституційною верифікацією (BVerfG) [35; 36; 37];

(4) Суд ЄС додав наднаціональний «клапан безпеки» – тест «внутрішньої еквівалентності» у поєднанні з пропорційністю [26]. Такий синтез підтримує баланс між ефективністю кримінального переслідування і гарантіями основоположних прав.

У практиці Європейського суду з прав людини (ЄСПЛ) особливе значення для аналізу операцій типу ***EncroChat*** мають два рішення Великої палати – *Roman Zakharov v. Russia* (2015) [27] та *Big Brother Watch and Others v. the United Kingdom* (2018/2021) [28]. Обидві справи стосуються масштабного перехоплення комунікацій і встановлюють стандарти, які є ключовими для оцінки законності, пропорційності та процесуальних гарантій під час здійснення таких заходів, зокрема в транскордонному вимірі.

У справі *Roman Zakharov v. Russia* (заява № 47143/06, рішення від 4 грудня 2015 року) [27] ЄСПЛ досліджував російську систему оперативно-розшукових заходів (СОРМ), яка дозволяла Федеральній службі безпеки (ФСБ) здійснювати прямий технічний доступ до мобільних мереж без необхідності щоразу отримувати індивідуальний судовий дозвіл. Суд встановив, що таке регулювання не відповідало вимогам «якості закону» і передбачуваності, оскільки не містило достатньо чітких норм про умови та обсяг допустимого перехоплення, коло правопорушень, строки, порядок зберігання і знищення даних. Було констатовано відсутність ефективного незалежного попереднього контролю (*ex ante*) та дієвих засобів правового захисту, зокрема можливості повідомлення особи про факт втручання після завершення оперативних дій. ЄСПЛ наголосив на необхідності суворого обмеження дискреційних повноважень органів влади і встановлення дієвих процесуальних запобіжників від зловживань.

У справі *Big Brother Watch and Others v. the United Kingdom* (заяви № 58170/13, 62322/14, 24960/15, рішення від 25 травня 2021 року) [28] ЄСПЛ розглянув британські режими масового перехоплення інтернет-комунікацій, отримання даних від іноземних спецслужб та доступу до даних від провайдерів зв'язку, розкриті у 2013 році внаслідок публікацій Едварда Сноудена. Суд визнав, що масове перехоплення саме по собі не є несумісним зі ст. 8 Конвенції, але воно повинно супроводжуватися «сильними запобіжниками» (*robust safeguards*), серед яких: чіткі правила авторизації перехоплення; незалежний попередній контроль, бажано судовий; конкретні критерії відбору та пошуку даних; гарантії щодо зберігання, використання, передачі та знищення інформації. Було підкреслено, що навіть при отриманні даних з-за кордону вони повинні підпадати під ті ж процесуальні гарантії, що й внутрішні. Особливу увагу приділено захисту журналістів та їхніх джерел, для яких необхідні додаткові гарантії з огляду на ст. 10 Конвенції.

З урахуванням цих двох рішень можна сформулювати єдиний комплекс стандартів, релевантних для аналізу ***EncroChat:***

Правова визначеність і якість закону – операція з інфільтрації зашифрованого сервісу повинна мати чітке, доступне і передбачуване нормативне підґрунтя, що окреслює підстави, цілі, коло правопорушень і процесуальні межі збору даних.

Незалежний попередній контроль – санкціонування має здійснюватися незалежним органом (переважно судом) із реальною перевіркою необхідності та пропорційності, а не формально.

Мінімізація і селекція – необхідні конкретні критерії відбору даних, щоб уникнути невибіркового збору інформації про осіб, непричетних до злочинів.

Регламентація строків, зберігання і знищення – строки втручання та зберігання мають бути чітко обмежені; порядок доступу до даних і їх знищення – чітко визначений.

Міжнародний обмін – передача зібраних даних між державами повинна підпорядковуватися тим самим гарантіям, що й внутрішнє використання, із застосуванням принципу «внутрішньої еквівалентності» (*internal equivalence test*).

Постфактум-контроль і засоби правового захисту – передбачення механізму повідомлення особи після завершення операції та можливості оскарження втручання.

Додатковий захист привілейованих категорій – особливі процесуальні гарантії для журналістів, адвокатів

та інших суб'єктів, діяльність яких пов'язана з охороною конфіденційної інформації.

Узагальнені стандарти, вироблені у зазначених справах, мають принципове значення для оцінки правомірності операції ***EncroChat***. Вони вимагають, щоб: законодавче підґрунтя інфільтрації було чітким, доступним і передбачуваним; санкціонування відбувалося за результатами незалежної та реальної перевірки необхідності і пропорційності; масиви отриманих даних оброблялися із застосуванням чітких критеріїв відбору і мінімізації; строки зберігання та порядок знищення інформації були належно врегульовані; міжнародна передача даних здійснювалася з дотриманням принципу «внутрішньої еквівалентності»; існували ефективні засоби постфактум-контролю і правового захисту, а також особливі гарантії для привілейованих категорій комунікацій. Інтеграція цих стандартів у національні процедури використання даних, отриманих унаслідок транскордонних операцій, є необхідною умовою їх відповідності статтям 8 і 10 Конвенції та запобігання визнанню таких доказів недопустимими.

Інтеграція зазначених стандартів у національні процедури використання даних, отриманих унаслідок операцій на кшталт *EncroChat*, є необхідною умовою забезпечення відповідності статтям 8 і 10 Конвенції про захист прав людини і основоположних свобод, підвищення довіри до цифрових доказів у кримінальному процесі та мінімізації ризику їх визнання недопустимими як на національному, так і на міжнародному рівнях. Досвід *EncroChat* наочно підтверджує, що масштабні інфільтраційні операції можуть здійснюватися правомірно лише за наявності чітко врегульованої процесуальної бази та ефективного судового контролю.

Для національного законодавства це означає необхідність детальної нормативної регламентації спеціальних технічних заходів із проникнення до захищених інформаційних систем, зокрема визначення підстав і меж їх застосування, обов'язковості санкції слідчого судді, а також закріплення процесуальних гарантій пропорційності та мінімізації втручання у приватне життя.

Практика Німеччини щодо «*внутрішньої еквівалентності*», відображена у рішенні Суду Європейського Союзу, може бути використана як орієнтир для формування критерію допустимості доказів, що надходять від іноземних органів у порядку міжнародної правової допомоги, – такі докази мають відповідати умовам і стандартам, передбаченим для аналогічних випадків у внутрішньому провадженні [6; 7]. Доцільним є також нормативне закріплення обмежень на використання результатів негласного доступу за зразком § 100e(6) Кримінально-процесуального кодексу Німеччини (StPO), яке передбачає можливість використання таких даних виключно у зв'язку з тим злочином і метою, для яких захід було санкціоновано, та лише у випадку прямої вказівки закону і за наявності нової судової санкції. У сфері міжнародної співпраці варто впроваджувати європейську концепцію презумпції законності дій іноземних органів, за якою докази, отримані в межах офіційної та судово санкціонованої операції, визнаються допустимими, якщо відсутні очевидні підстави вважати, що вони здобуті з грубим порушенням прав людини або фундаментальних засад кримінального процесу.

Запропоновані зміни до Кримінального процесуального кодексу України (далі – КПК) повинні забезпечити практичне втілення зазначених підходів. Зокрема, пропонується доповнити статтю 84 КПК принципом «внутрішньої еквівалентності» для транскордонних доказів, передбачивши у частині п'ятій таку норму: «Докази, отримані від компетентних органів іноземних держав у порядку міжнародного співробітництва, визнаються допустимими за умови, що спосіб їх отримання відповідав би вимогам цього Кодексу у порівнюваному внутрішньому провадженні та не суперечить засадам верховенства права та основоположним правам людини».

Впровадження принципу внутрішньої еквівалентності на рівні статті 84 КПК забезпечить, щоб будь-які цифрові докази, отримані від іноземних органів, оцінювалися за тими самими критеріями допустимості та процесуальної належності, що й докази, здобуті у внутрішньому провадженні, тим самим гармонізуючи національну практику з вимогами міжнародних стандартів та рішень провідних європейських судових інституцій.

Зміни до статті 99 КПК України повинні передбачати включення електронних комунікаційних даних, здобутих унаслідок спеціальних технічних операцій іноземних органів, до переліку допустимих документальних джерел доказів. У цьому зв'язку пропонується доповнити статтю 99 (Документи) пунктом 5 частини другої такого змісту: «електронні комунікаційні дані, отримані внаслідок спеціальних технічних операцій, проведених іноземними компетентними органами за судовим дозволом та передані в Україну у порядку міжнародного співробітництва».

Важливим нововведенням має стати регламентація онлайн-обшуку як окремої НСРД у статті 258 КПК. Пропонується доповнити цю статтю частиною десятою в такій редакції: «Негласне проникнення до інформаційних систем або пристроїв електронних комунікацій (онлайн-обшук) здійснюється виключно за ухвалою слідчого судді у провадженні щодо тяжких або особливо тяжких злочинів. Такі заходи повинні відповідати принципам необхідності, пропорційності та мінімізації втручання у приватне життя. Результати таких заходів можуть бути використані лише для розслідування злочину, зазначеного в ухвалі, та в межах встановленої мети».

Запровадження інституту онлайн-обшуку обумовлено поширенням зашифрованих комунікаційних сервісів, що суттєво ускладнюють доступ до релевантних доказів. Така регламентація не лише узгоджується зі стандартами Європейського Союзу (ЄС), а й відповідає вимогам, виробленим у практиці Європейського суду з прав людини (ЄСПЛ), зокрема у справах *Roman Zakharov v. Russia* [27] та *Big Brother Watch and Others v. the United Kingdom* [28], де було підкреслено необхідність чіткого правового регулювання, незалежного контролю та пропорційності при втручанні у сферу приватного життя.

Окремої уваги заслуговує запровадження нової статті 99-1 КПК «Обмеження використання результатів негласного доступу». Її пропонується викласти у такій редакції: «Результати негласного проникнення до інформаційних систем та електронних комунікацій, включно з отриманими від іноземних компетентних органів, можуть використовуватися як докази лише у зв'язку зі злочином, для розслідування якого вони були санкціоновані, та лише у межах цілей, визначених ухвалою суду або міжнародним запитом. Використання таких результатів у інших провадженнях допускається лише у випадках, коли це прямо передбачено законом та підтверджено ухвалою суду».

Крім того, доцільно передбачити зміни до статті 557 КПК України, яка регулює виконання запитів про міжнародну правову допомогу. Пропонується доповнити її частиною четвертою такого змісту: «При виконанні запиту про передачу вже наявних у компетентного органу України доказів перевіряється, чи міг би відповідний захід бути санкціонованим у порівнюваному внутрішньому провадженні. Передача таких доказів здійснюється за умови дотримання принципів необхідності та пропорційності».

Узгоджене впровадження цих змін дозволить створити системну, узгоджену з міжнародними стандартами модель доступу, використання та оцінки цифрових доказів, що надходять від іноземних партнерів, та посилить процесуальні гарантії захисту прав людини у кримінальному процесі.

Запровадження нової редакції статті 558 КПК України, що регулюватиме порядок виконання Європейського наказу про розслідування (*European Investigation Order – EIO*), повинно передбачати чітку та деталізовану процедуру перевірки принципу «внутрішньої еквівалентності». Така перевірка має полягати у з'ясуванні, чи був би запитуваний захід допустимим і можливим за українським законодавством у порівнюваному внутрішньому кримінальному провадженні. Передбачення можливості відмови у виконанні ЕІО у випадках, коли захід не допускається національним правом за аналогічних обставин, забезпечить узгодженість процесуальних стандартів та захист фундаментальних прав учасників провадження.

Крім того, нова редакція статті повинна прямо закріпити обов'язкове дотримання процесуальних гарантій приватності та права на захист під час виконання таких запитів, у тому числі шляхом незалежного судового контролю, фіксації всіх процесуальних дій та забезпечення права сторони захисту на доступ до матеріалів, пов'язаних з виконанням ЕІО.

Вдосконалення правил виконання міжнародних запитів, закріплених у статтях 557 та 558 КПК, дозволить на законодавчому рівні інституціоналізувати механізм перевірки внутрішньої еквівалентності, а також гарантувати, що передача вже наявних доказів іноземним компетентним органам здійснюватиметься виключно за умови дотримання принципів необхідності та пропорційності.

Таке реформування сприятиме гармонізації національних процесуальних норм із європейськими стандартами, зміцненню процесуальних гарантій, підвищенню рівня довіри судів до цифрових доказів, отриманих як в Україні, так і за її межами, та забезпечить більш ефективну участь нашої держави у спільних міжнародних розслідуваннях без виходу за межі вимог пропорційності та захисту приватності.

Висновки: Проведене дослідження дозволяє сформулювати узагальнені теоретичні та практичні висновки, які мають значення для розвитку національної моделі регламентації та використання цифрових доказів у кримінальному провадженні України з урахуванням досвіду операції з інфільтрації платформи зашифрованих комунікацій ***EncroChat*** та відповідної європейської судової практики. Операція ***EncroChat***, проведена французькими та нідерландськими правоохоронними органами за координації Європолу, стала прецедентом масштабного та технічно складного транскордонного збору цифрових доказів, що підтвердило можливість здійснення подібних інфільтраційних операцій у правовому полі за умови чіткого процесуального регулювання, незалежного судового контролю та дотримання принципів необхідності й пропорційності.

Європейський наказ про розслідування (ЕІО) у контексті Директиви 2014/41/ЄС виступає ключовим механізмом транскордонної передачі цифрових доказів, а рішення Суду ЄС у справі *C-670/22, M.N.* закріпило тест «внутрішньої еквівалентності» як правовий фільтр, що вимагає перевірки можливості застосування аналогічного заходу у внутрішньому провадженні держави-виконавця. Цей стандарт варто імплементувати в українське законодавство для забезпечення належної оцінки доказів, отриманих від іноземних органів. Практика ЄСПЛ у справах *Roman Zakharov v. Russia* (2015) та *Big Brother Watch and Others v. the United Kingdom* (2018/2021) визначає комплекс гарантій, необхідних при масовому чи цілеспрямованому перехопленні комунікацій, зокрема правову визначеність, незалежний попередній контроль, чіткі критерії відбору даних, обмеження строків зберігання та використання, постфактум-контроль і спеціальний захист для привілейованих категорій комунікацій. Ці стандарти мають безпосереднє значення для української моделі регулювання спеціальних технічних заходів.

Аналіз зарубіжних моделей, зокрема німецької (§§ 100b, 100e(6), 261 StPO), свідчить про доцільність внесення змін до КПК України, зокрема закріплення принципу «внутрішньої еквівалентності» у ст. 84, розширення ст. 99 на електронні комунікаційні дані, отримані від іноземних органів, виокремлення онлайн-обшуку як окремої негласної слідчої (розшукової) дії у ст. 258 з чіткими процесуальними гарантіями, запровадження ст. 99-1 про обмеження використання результатів негласного доступу, а також доповнення ст. 557 і 558 нормами про перевірку «внутрішньої еквівалентності» та забезпечення пропорційності при передачі й використанні вже наявних доказів. Для ефективного впровадження таких норм необхідно створити в органах досудового розслідування спеціалізовані підрозділи з обробки великих масивів зашифрованих даних, запровадити уніфіковані стандарти збереження (*chain of custody*), хешування та ведення журналу доступу (реєстрації) до цифрових доказів, а також політику мінімізації та псевдонімізації персональних даних відповідно до Директиви (ЄС) 2016/680.

Імплементація зазначених пропозицій забезпечить узгодженість українських процесуальних норм із європейськими стандартами, зменшення ризику визнання цифрових доказів недопустимими, підвищення ефективності міжнародного співробітництва у боротьбі з кіберзлочинністю та організованою злочинністю, а також зміцнення гарантій захисту прав людини в умовах зростання технічних можливостей правоохоронних органів.

Таким чином, досвід ***EncroChat*** та практика провідних європейських судових інституцій повинні стати основою для побудови в Україні збалансованої системи регламентації цифрових доказів, яка поєднуватиме ефективність кримінального переслідування з надійними процесуальними запобіжниками та повагою до фундаментальних прав**.**

ЛІТЕРАТУРА

1. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. Рада Європи. Ратифікована Законом України від 17 липня 1997 р. № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004

2. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. *Official Journal of the European Union*. 2014. L 130. P. 1–36. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0041

3. Oerlemans, J.J., van Toor, T. Legal Aspects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime, Criminal Law and Criminal Justice* (Brill), 2023. URL: https://brill.com/view/journals/eccl/eccl-overview.xml

4. Oerlemans, J.J., van Toor, T. Data-Driven Investigations in a Cross-Border Setting: The Dutch Experience with EncroChat (accepted manuscript). URL: https://jjoerlemans.com/docs/Brill_Encrochat_2023.pdf

5. Stoykova, R. EncroChat: The hacker with a warrant and fair trials? *Forensic Science International: Digital Investigation*, 2023, Vol. 46, Article 301602. URL: https://doi.org/10.1016/j.fsidi.2023.301602

6. Mason, S., Seng, D. (eds.). *Electronic Evidence and Electronic Signatures* (5th ed.). London: Institute of Advanced Legal Studies / University of London, 2021. Open access. URL: https://archive.org/details/elect

7. Сергєєва Д. Б. Правові та криміналістичні засади зняття інформації з каналів зв'язку. Монографія. Х.:Арсіс ЛТД, 2009. 203 с.

8. Метелев О. П. Проблемні аспекти фіксації відомостей отриманих з транспортних телекомунікаційних мереж. *Вісник кримінального судочинства*. 2022. № 3-4. С. 28–37. URL: https://doi.org/10.17721/2413-5372.2021.3-4/28-37

9. Скрипник А.В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні: дисертація на здобуття ступеня доктора філософії за спеціальністю 081 Право. Харків: Нац. юрид. у-т ім. Ярослава Мудрого, 2021. 369 с.

10. Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2. С. 112–124. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/05/47-2.pdf

11. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*, 2013, Вип. 5, с. 256–260. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58

12. Погорецький М. А. Прослуховування телефонних розмов: європейські стандарти. *Вісник прокуратури*. 2003. № 9. С. 45–51.

13. Погорецький М. А., Шумило М. Є. Проблеми використання матеріалів оперативно-розшукової діяльності в доказуванні у кримінальних справах: теоретичний та практичний аспекти. *Вісник Луганського ін-ту внутр. справ*. Луганськ: РВВ ЛІВС, 2001. Вип. 3. С. 199–209.

14. Погорецький М. А. Докази у кримінальному процесі. *Вісник прокуратури*. 2003. № 2. С. 59–65.

15. Погорецький М.А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: монографія. Харків: Арсіс ЛТД, 2007. 576 с.

16. Погорецький М., Шеломенцев В. Міжнародне співробітництво у сфері протидії комп'ютерній злочинності. *Юрид. радник*. 2008. № 6 (26). С. 6–9.

17. Погорецький М. А., Шеломенцев В. П. Комп'ютерна система як знаряддя вчинення злочину. *Вісник Харківського нац. ун-ту ім. В. М. Каразіна. Серія «Право»*. 2009. № 872. Вип. 6. С. 117–121.

18. Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчення злочину. *Інформаційна безпека людини, суспільства, держави*: наук.-практ. журнал. Київ : НАСБУ, 2009. № 2 (2). С. 77–81.

19. Погорецький М., Шеломенцев В. Правове забезпечення боротьби з кіберзлочинами в Україні: проблемні питання. *Вісник прокуратури*. 2011. № 8 (122). С. 30–38.

20. Погорецький М. А., Шеломенцев В. П. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.

21. Погорецький М.А. Негласні слідчі (розшукові) дії: проблеми провадження та використання результатів у доказуванні. *Юридичний часопис Національної академії внутрішніх справ*. Київ, 2013, № 1. С. 270-Погорецький М. А. Проведення негласних слідчих (розшукових) дій та використання їх результатів у доказуванні. *Актуальні питання досудового розслідування слідчими органів внутрішніх справ: проблеми теорії та практики*: матеріали всеукраїнської науково-практичної (м. Дніпропетровськ, 18–19 квітня 2013 року). Київ : Хлі-Тек Прес, 2013. С. 186–193.

22. Погорецький М.А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). *Вісник кримінального судочинства.* 2023. № 3-4. С. 84–102. URL: https://vkslaw.knu.ua/ua/3-4-2023-aktualni-problemi-kriminalnogo-sudochinstva-ua-ua/problemi-kriminalnogo-proczesu-kriminalistiki-ta-operativno-rozshukovo%D1%97-diyalnosti

23. Погорецький М. А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. *Аналітично-порівняльне правознавство*. 2025. № 4. ч. 3. С. 269–279. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42-2.pdf

24. Europol. *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe* (EncroChat). Joint press release Europol/Eurojust, 02.07.2020. URL: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

25. Court of Justice of the European Union. *Case C-670/22 (M.N.) – Judgment of 30 April 2024 on the European Investigation Order in the context of EncroChat*. *Reports of Cases (electronic)*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0670

26. European Court of Human Rights (Grand Chamber). Roman Zakharov v. Russia, no. 47143/06, Judgment of 4 December 2015. URL: https://hudoc.echr.coe.int/eng?i=001-159324

27. European Court of Human Rights (Grand Chamber). Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14, 24960/15, Judgment of 25 May 2021. URL: https://hudoc.echr.coe.int/eng?i=001-203614

28. Bundesgerichtshof. Urteil vom 2. März 2022 – 5 StR 457/21. URL: https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/2022/03/050stR045721.html

29. Strafprozessordnung (StPO) in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 5 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411). URL: https://www.gesetze-im-internet.de/stpo/

30. Council of the European Union. Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union. *Official Journal of the European Communities*. C. 197. 12.07.2000. P. 1–23. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0712%2801%29

31. Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence. *Official Journal of the European Union*. L 196. 02.08.2003. P. 45–55. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577

32. Tribunal correctionnel de Lille. Décision autorisant l'infiltration technique du service EncroChat (2020) – цит. за: CURIA, *Case C-670/22, MN* (EncroChat). URL: https://curia.europa.eu/juris/liste.jsf?num=C-670%2F22

33. Hoge Raad der Nederlanden. *Supreme Court issues preliminary ruling in EncroChat and SkyECC cases*, 13.06.2023. URL: https://www.hogeraad.nl/actueel/nieuwsoverzicht/2023/juni/supreme-court-issues-preliminary-ruling-encrochat-and-skyecc-cases/

34. Bundesverfassungsgericht. *Constitutional complaint challenging conviction based on EncroChat data inadmissible* (Press Release No. 104/2024), 11.12.2024 (orders of 01.11.2024). URL: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2024/bvg24-104.html

35. Bundesgerichtshof. *Urteil vom 02.03.2022 – 5 StR 457/21* (voller Text / case materials). *Review and selection of materials: eucrim*. URL: https://eucrim.eu/news/germany-federal-court-of-justice-confirms-use-of-evidence-in-encrochat-cases/

36. Bundesverfassungsgericht. *EncroChat cases – further materials and orders (First Senate)*. Press release no. 69/2025 of 7 August 2025. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2025/bvg25-069.html

37. Bundesgerichtshof. *EncroChat-Data may be used for the Investigation of serious criminal Offences* (Press Release No. 038/2022), 25.03.2022; Decision of 02.03.2022 – 5 StR 457/21. URL: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/EN/2022/2022038.html

Дата першого надходження рукопису до видання: 15.08.2025
Дата прийнятого до друку рукопису після рецензування: 18.09.2025
Дата публікації: 26.09.2025