УДК 343.98:070(100)

https://doi.org/10.52058/3041-1254-2025-12(22)-520-530

Танчик Каміла Анатоліївна аспірант кафедри криміналістики та судової медицини Національної академії внутрішніх справ, м. Київ, https://orcid.org/0009-0005-0751-5861

ЗАРУБІЖНИЙ ДОСВІД ВИКОРИСТАННЯ МЕДІА ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Анотація. У статті узагальнений досвід нормативно-правового забезпечення ЄС та практики діяльності окремих країн засвідчив, що медіа розглядаються не лише як канал комунікації з суспільством, а як повноцінний криміналістичний ресурс, інтегрований у методику розслідування кримінальних правопорушень, зокрема на законодавчому рівні унормовано баланс між потребами розслідування і свободою слова.

Авторкою запропоновані шляхи імплементації зарубіжного досвіду використання медіа при розслідуванні кримінальних правопорушень з урахуванням нормативно-правових вимог ЄС та Протоколу Берклі щодо роботи з доказами електронної форми у кримінальному провадженні, серед яких: інституціоналізація їх статусу в межах кримінального процесуального законодавства (Німеччина); утвердження технологічно нейтрального підходу до оцінки та допустимості (Англія, Франція); підвищення вимог до автентичності, цілісності та простежуваності походження медіадоказів (Нідерланди, Швеція); запровадження спеціальних процедур їх збирання, збереження та верифікації; поступова уніфікація національних підходів із міжнародними кримінальними та доказовими стандартами (Німеччина, Франція). При цьому встановлено, що застосування електронних інформаційних систем як засобу обміну доказами зумовлює переведення матеріалів у електронну форму незалежно від первинного носія, що, своєю чергою, потребує підтвердження їх автентичності, цілісності, відтворюваності та збереження мультимедійного контексту.

Ключові слова: медіа, зарубіжний досвід, кримінальне правопорушення, воєнний злочин, кримінальне провадження, розслідування, журналістське розслідування.

Tanchyk Kamila Anatoliivna PhD student, Department of Forensics and Forensic Medicine, National Academy of Internal Affairs, Kyiv, https://orcid.org/0009-0005-0751-5861

FOREIGN EXPERIENCE IN THE USE OF MEDIA IN THE INVESTIGATION OF CRIMINAL OFFENSES

Abstract. The article summarizes the experience of the EU regulatory framework and the practices of individual countries, demonstrating that media are considered not only as a channel of communication with the public but also as a full-fledged forensic resource, integrated into the methodology of investigating criminal offenses. In particular, legislation regulates the balance between investigative needs and freedom of speech.

The author proposes ways to implement foreign experience in the use of media in criminal investigations, taking into account EU regulatory requirements and the Berkeley Protocol on the use of electronic evidence in criminal proceedings. These include: institutionalization of the legal status of media within criminal procedural law (Germany); adoption of a technologically neutral approach to assessing admissibility (England, France); strengthening requirements for the authenticity, integrity, and traceability of media evidence (Netherlands, Sweden); introduction of special procedures for collection, preservation, and verification; and gradual harmonization of national approaches with international criminal and evidentiary standards (Germany, France).

It is also established that the use of electronic information systems as a means of exchanging evidence necessitates the conversion of materials into electronic form regardless of the original medium, which in turn requires confirmation of their authenticity, integrity, reproducibility, and preservation of the multimedia context.

Keywords: media, foreign experience, criminal offense, war crime, criminal proceedings, investigation, investigative journalism.

Постановка проблеми. Зарубіжний досвід використання медіа у розслідуванні кримінальних правопорушень становить значний науково-практичний інтерес, оскільки в правових системах демократичних країн уже сформовано усталені механізми взаємодії органів кримінальної юстиції та медіа, включно з питаннями документування подій, виявлення правопорушень, формування доказової бази та забезпечення прозорості правосуддя. У країнах ЄС, США, Канаді, Великій Британії та інших давно функціонують нормативно врегульовані інструменти співпраці зі ЗМІ й онлайн-платформами, які дозволяють не лише ефективно інформувати населення, але й використовувати оприлюднені медіаматеріали як приводи для відкриття кримінальних проваджень, як джерела доказової інформації, а також як аналітичні ресурси для виявлення нових форм злочинності, включаючи кіберзлочини та тероризм.

Особливої ваги такі напрацювання набули після 2014 р., коли медіа у багатьох конфліктах світу – від Балкан до Сирії та України – відіграють ключову роль у виявленні порушень міжнародного гуманітарного права, сприяючи

діяльності міжнародних трибуналів та Міжнародного кримінального суду. За кордоном накопичено значний досвід алгоритмізації обробки медіадоказів, перевірки їх автентичності, забезпечення правомірності доступу до цифрових матеріалів і запровадження стандартів збереження доказової інформації.

Вивчення такого досвіду є важливим для України, яка в умовах триваючої збройної агресії РФ потребує ефективних механізмів залучення медіа до розслідування воєнних злочинів і забезпечення співпраці з міжнародними юрисдикціями. Саме тому аналіз зарубіжних моделей взаємодії правоохоронних органів із медіасектором, включаючи правовий статус журналістських матеріалів, захист інформаторів, стандарти цифрової верифікації та правила допустимості публікацій як доказів, є необхідним етапом формування сучасних криміналістичних підходів у національній практиці.

Аналіз останніх досліджень і публікацій. Окремі питання криміналістичного забезпечення участі медіа у протидії злочинності висвітлювали свого часу П. Біленчук, А. Данієль, Н. Карпов, В. Пясковський, Ю. Стеценко та ін. Водночас, актуальність проблеми істотно посилилася в умовах воєнного стану, коли медіа стали важливим джерелом інформації для документування та розслідування воєнних злочинів. Відтак, потребує поглибленого дослідження зарубіжний досвід використання медіа при розслідуванні кримінальних правопорушень.

Мета статті – узагальнити зарубіжний досвід використання медіа у розслідуванні кримінальних правопорушень та визначити шляхи імплементації цього досвіду в українське законодавство та практику з урахуванням вимог міжнародних стандартів щодо електронних доказів.

Виклад основного матеріалу. Аналізуючи законодавство країн близького зарубіжжя та досліджуючи питання визначання поняття медіа, окреслено, що деякі країни прямо включають до них Інтернет-ресурси, надаючи їм процесуального статусу, що безпосередньо впливає на можливість використання цифрового контенту у доказуванні. В окремих юрисдикціях Інтернет-ресурси прямо включені до правового режиму медіа, що забезпечує створення передумов для їх процесуального використання у кримінальному провадженні, тоді як інші країни не виділяють їх в окрему категорію, що ускладнює імплементацію отриманих із них даних як доказової інформації.

У Республіці Словенія Закон «Про засоби масової інформації» відносить до таких друковані, аудіовізуальні та електронні форми публікацій, а також телетекст незалежно від технічного способу розповсюдження (ст. 2 п. 1; ст. 3) [1]. Такий підхід забезпечує уніфіковане правове поле для використання матеріалів медіа як потенційних джерел криміналістичної інформації під час здійснення досудового розслідування.

У Республіці Вірменія відповідно до Закону «Про масову інформацію» до медіа належать як традиційні друковані періодичні видання, так і телерадіо-

мовлення та мережеві засоби інформації, які мають конкретну Інтернет-адресу, доступну для невизначеного кола користувачів і містять інформацію незалежно від частоти її оновлення [2]. Такий підхід не лише формалізує цифрові медіа як елемент системи масової комунікації, але й сприяє легітимному використанню медіа-контенту в кримінальному процесі, включаючи оперативне виявлення відомостей про злочини.

У нормативно-правових актах Грузії термін «засоби масової інформації» не вживається, замість нього використовується поняття «мас-медіа», яке включає друковані та електронні форми масової комунікації, а також Інтернет [3], що свідчить про універсалізацію підходу до медіа, хоча й не деталізує механізм залучення інформації до кримінального процесу.

До медіа у Латвійській Республіці належать газети, бюлетені та інші періодичні видання з накладом понад 100 примірників, а також аудіовізуальні програми, радіо та телебачення, кінохроніка й повідомлення інформаційних агентств, призначених для публічного розповсюдження [4]. Така модель унормовує традиційну пресу та мовлення, однак вимагає додаткового осучаснення для ефективного охоплення Інтернет-комунікацій як ключового джерела криміналістично значущої інформації у сучасних умовах.

Таким чином, проведений аналіз окремих країн свідчить, що ступінь нормативно-правового охоплення медіа безпосередньо впливає на можливість їх повноцінного застосування в діяльності правоохоронних органів: чим ширше законодавче визначення медіа, тим більше можливостей для законного отримання, фіксації та використання медіа-даних у кримінальних провадженнях, що має принципове значення для оперативності, об’єктивності та результативності розслідування кримінальних правопорушень.

У криміналістичному аспекті особливе значення має міжнародна практика визначення статусу медіаджерел як відкритих джерел цифрової інформації, придатних для використання у кримінальному провадженні. Так, Протокол Берклі (Berkeley Protocol on Digital Open Source Investigations, 2020), розроблений Управлінням Верховного комісара ООН з прав людини та Berkeley Human Rights Center, пропонує сучасне бачення цифрової інформації у відкритому доступі як інформації, розміщеної в мережі Інтернет на загальнодоступних веб-ресурсах, у базах даних і на платформах соціальних медіа, доступ до якої не потребує спеціального дозволу або порушення технічного захисту. Важливо, що цей документ не лише окреслює перелік можливих відкритих джерел, а й містить вимоги до правомірного пошуку, збору, фіксації, структурування та збереження медіаконтенту, придатного для використання у кримінальному провадженні, судовому розгляді, з дотриманням стандартів автентичності, безперервності, доступності й захисту персональних даних [5].

У межах Протоколу наголошується, що отримання медіаматеріалів з відкритих джерел повинно здійснюватися за допомогою дозволених технологічних

інструментів: відкритого коду та програмного забезпечення, яке є доступним для перевірки й не обмежене патентним чи авторським правом. Саме використання таких інструментів унеможливлює спотворення цифрової інформації та підвищує її доказове значення у кримінальних провадженнях щодо тяжких злочинів, зокрема воєнних злочинів, які дедалі частіше документуються через матеріали журналістів, громадських розслідувачів, очевидців та платформ соціальних медіа.

Сучасна міжнародна практика й наукові підходи однозначно підтверджують: медіа в цифровому середовищі повинні розглядатися як об'єкти криміналістичного дослідження, а їх контент – як потенційно допустимий електронний доказ за умови дотримання процедури його отримання та обробки.

Використання інформації з відкритих джерел у кримінальному провадженні демонструє їх особливу значущість насамперед на етапі досудового розслідування, коли виникає потреба оперативно встановити фактичні дані про подію кримінального правопорушення, місце, час, спосіб його вчинення, а також окреслити коло причетних осіб. Водночас відсутність у КПК України уніфікованих процесуальних процедур перевірки, фіксації та збереження такої інформації зумовлює ризик невідповідності зібраних матеріалів критеріям належності та допустимості доказів. У цьому контексті положення Протоколу Берклі виступають релевантним орієнтиром для слідчих, прокурорів та суддів, оскільки формують методологічну основу документування, верифікації й довгострокового зберігання цифрової інформації з відкритих джерел, що безпосередньо підвищує якість і результативність розслідування [6, с. 325–326].

Аналіз Протоколу Берклі доцільно зосередити на тих його положеннях, які мають безпосереднє практичне значення для суб'єктів кримінального провадження. Розділ II «Принципи» встановлює, що розслідування з використанням цифрових даних у відкритому доступі повинно здійснюватися відповідально, компетентно, об'єктивно, у відповідності до чинного законодавства та із належним урахуванням міркувань безпеки. Особливий акцент робиться на необхідності дотримання етичних стандартів усіма учасниками таких розслідувань. Розділ III «Нормативно-правова база» підкреслює, що визначення застосовного права та його меж є визначальним при вирішенні питання про те, яку інформацію збирати, якими засобами та в якій формі, а також залежить від статусу слідчого, його цілей, контексту розслідування та відповідної юрисдикції. Збереження цифрового матеріалу повинно здійснюватися таким чином, щоб гарантувати його автентичність і забезпечити належне документування ланцюга збереження, що істотно підвищує ймовірність визнання таких даних доказами в суді. Розділ IV «Безпека» виходить із того, що відповідальність за безпеку розслідування й осіб, на яких воно впливає, несуть не лише ІТ-фахівці, а вся команда розслідування. Безпекові міркування охоплюють дві площини: інфраструктурну (апаратне забезпечення, програмне забезпечення, мережеві

ресурси) та поведінкову (поведінка самих слідчих і всіх залучених осіб). Оцінка безпеки повинна проводитися на трьох рівнях: рівень організації, конкретного розслідування (справи) та окремих заходів/завдань. У Розділі V «Підготовка» сформульовано рекомендації щодо підготовки й стратегічного планування як ключових передумов ретельного та безпечного розслідування. Підготовка включає: (a) оцінку загроз і ризиків та план їх мінімізації; (b) оцінку інформаційного ландшафту; (c) розроблення детального плану розслідування [6].

З огляду на суттєву технічну та методологічну складність Протоколу Берклі його ефективне використання вимагає належної спеціальної підготовки, у тому числі для слідчих, прокурорів, суддів та експертів. У цьому зв'язку важливе значення мають науково-практичні джерела, що систематизують та адаптують його положення до українських реалій. Зокрема, для суб'єктів кримінального провадження релевантним є дослідження О. О. Торбаса «OSINT при розслідуванні кримінальних правопорушень» (2024) [7], який у прикладному вимірі демонструє можливості імплементації міжнародних стандартів у національну практику.

Узагальнюючи, Протокол Берклі слід розглядати як комплексний міжнародний стандарт щодо розслідування кримінальних правопорушень з використанням відкритих цифрових джерел, який поєднує методологічні, етичні, технічні та процесуальні вимоги до роботи з такими даними. Для України його імплементація має особливе значення в умовах повномасштабної збройної агресії, коли значна частина інформації про воєнні злочини фіксується саме через медіа. Водночас сучасна практика органів досудового розслідування та судів ще не забезпечує системного застосування положень Протоколу, а чинний КПК України не містить чітко сформульованих норм щодо процедури роботи з інформацією з відкритих джерел, що об'єктивно створює ризики для належності й допустимості доказів, отриманих з таких джерел, та підкреслює необхідність подальшої нормотворчої й методичної роботи, спрямованої на інтеграцію стандартів Протоколу Берклі у кримінальне процесуальне законодавство й практику розслідування кримінальних правопорушень.

Звертаючи увагу на практику окремих країн ЄС, то наприклад у Німеччині відомою є ТВ передача ZDF «Aktenzeichen XY… ungelöst», що з 1967 р. у співпраці з поліцією та прокуратурою відтворює обставини нерозкритих злочинів, показує фотороботи, відео з камер, реконструкції подій та контакти для звернень. За понад 5000 справ, представлених у програмі, приблизно 39% злочинів було розкрито, а щодо деяких категорій, наприклад убивств, рівень розкриття сягає 41% [8]. Такий метод сприяв підвищено рівня розслідування за допомоги появи нових показань, які поліція не могла отримати на початку розслідування; формування громадської довіри до поліції та готовності співпрацювати.

Отже, Німеччина формує збалансовану модель регулювання використання електронних доказів: конституційний пріоритет прав людини над інтересами

обвинувачення; процесуальні гарантії (строгий судовий контроль, обмеження за видами проваджень); розвинена інституційна інфраструктура для цифрової криміналістики; європейська інтеграція стандартів доказування. Зазначена модель демонструє високий рівень технологічної адаптивності, зберігаючи водночас фундаментальні принципи правової держави, що є релевантним орієнтиром для формування національної практики збирання та оцінки медіадоказів у кримінальному провадженні України.

У Франції КПК (Code de procédure pénale) також не містить визначення поняття цифрового доказу [9], однак передбачає спеціальні інструменти для доступу до електронної інформації: приховане комп'ютерне стеження у тяжких справах (ст. 706-102-1 CPP), доступ до збережених даних провайдерів (ст. 706-95-1, 706-95-2 CPP), а також перехоплення онлайн-контенту за аналогією з телефонними прослуховуваннями. В умовах надзвичайного стану законодавство було розширене для підвищення можливостей антитерористичних розслідувань.

Суди Франції послідовно реалізують принцип свободи доказування, визнаючи допустимими електронні листи, GPS-дані, SMS тощо за умови їх законного походження та належної надійності. Ілюстративним є кейс EncroChat: французька жандармерія у 2020 р. отримала мільйони зашифрованих повідомлень учасників ОЗГ у Європі, які стали доказовою базою в сотнях кримінальних проваджень, зокрема у Німеччині та Нідерландах [10], що засвідчило високу ефективність міжнародної співпраці.

Досвід Німеччини та Франції демонструє такі системні підходи, які можуть бути імплементовані Україною: технологічно нейтральна модель доказування (оцінюється зміст, а не носій); поєднання загальних правил кримінального процесу зі спеціальними повноваженнями в цифровому середовищі; інституційне забезпечення (спеціалізовані центри цифрової криміналістики, стандарти ACPO/Forensic Regulator, інтеграція у механізми ЄС); унормування медіадоказів як самостійної категорії; впровадження обов'язкових процедур автентифікації; створення та акредитації мережі ІТ-криміналістичних лабораторій; розширення міжнародної співпраці щодо доступу до даних інтернет-компаній; чітке законодавче визначення доступу до медіаконтенту онлайн.

Вказані рішення сприятимуть підвищенню доказової цінності матеріалів, отриманих із медіа, та забезпечать відповідність національного кримінального провадження сучасним європейським стандартам.

Європейські органи юстиції та правоохоронні органи приділяють значну увагу стандартизації роботи з електронними доказами, включно з медіаконтентом:

• Eurojust і Єврокомісія розробляють рекомендації щодо збирання, збереження й передачі електронних доказів у транскордонних провадженнях – зокрема даних соцмереж, відео з платформ, контенту сайтів [11].

• У низці досліджень, підготовлених для Ради Європи та ЄС, підкреслюється необхідність створення єдиних протоколів фіксації електронних доказів (hash-

ідентифікатори, збереження «цифрових відбитків», використання блок-записів та ін.), щоб уникнути сумнівів у їх автентичності в суді [12]. На практиці це означає, що: відео з YouTube, допис у Facebook, пост у Telegram-каналі чи онлайн-публікація на порталі новин можуть бути долучені як докази, якщо: зафіксовано час, URL, метадані; підтверджено незмінність файлу (хеш-суми, цифровий підпис); дотримано процесуальний порядок одержання (ухвала суду, запит до провайдера, протокол огляду веб-сторінки тощо);

• активна співпраця з платформами (на підставі DSA, e-Evidence Regulation, MLAT-ів) дозволяє отримувати лог-дані, IP, інформацію про акаунт, що трансформує медіаконтент із «фактичного фону» у повноцінний ланцюг цифрових доказів.

Після початку агресії РФ проти України держави ЄС та їхні правоохоронні органи активно використовують відкриті медіа-джерела для документування воєнних злочинів, зокрема:

• ЄС підтримує роботу спільних слідчо-оперативних груп за участі України, Литви, Польщі та Міжнародного кримінального суду, де цифрові докази з медіа (відео обстрілів, супутникові знімки, фото з соцмереж, репортажі телеканалів) інтегруються у доказову базу разом із традиційними джерелами – допитами, експертизами, оглядами місця події [13].

• У низці країн ЄС (наприклад, Німеччина, Нідерланди, Швеція, Норвегія та ін.) прокуратура й поліція мають спеціалізовані підрозділи з OSINT-аналізу, які відбирають, верифікують та зберігають медіаконтент, що може бути важливим для кримінальних проваджень щодо воєнних, транснаціональних злочинів та ін. шляхом: 1) розробки протоколів OSINT-збирання: збереження оригінальних файлів, використання інструментів перевірки геолокації, часу зйомки, метаданих (EXIF), перехресної перевірки із супутниковими знімками та іншими джерелами; 2) включення суб'єктів медіа до «першоджерела повідомлень», які служать підставою для початку кримінального провадження, але потребують проведення подальших слідчих (розшукових) дій.

Для України досвід ЄС тут особливо важливий, позаяк значна частина доказів воєнних злочинів РФ існує саме у формі медіаконтенту (репортажі, стріми, відео з дронів, соцмережі), і без відпрацьованих криміналістичних підходів до їх фіксації й оцінки доказова цінність цих матеріалів може бути втрачена; необхідне поєднання стандартів ЄСПЛ та ЄС щодо електронних доказів, щоб українські матеріали могли бути безперешкодно використані у міжнародних провадженнях інших держав.

Висновок Досвід нормативно-правового забезпечення ЄС та практики діяльності окремих країн засвідчив, що медіа розглядаються не лише як канал комунікації з суспільством, а як повноцінний криміналістичний ресурс, інтегрований у методику розслідування кримінальних правопорушень, зокрема на законодавчому рівні унормовано баланс між потребами розслідування і свобо-

дою слова (ECHR, GDPR, DSA, AVMSD, e-Evidence); інституціоналізовано взаємодію правоохоронних органів з телевізійними програмами розшуку, які демонструють стабільно високі показники сприяння встановленню обставин вчинення тяжких злочинів (39 % розкритих справ у Німеччині, 35% у Нідерландах); сформовано комплекс рекомендацій (Europol, Eurojust) щодо OSINT, онлайн-патрулювання та роботи з електронними доказами (посилення вимог до автентичності, цілісності й простежуваності; запровадження спеціальних процесуальних процедур збирання, збереження та перевірки), що дозволяє широко використовувати медіаконтент як докази, не порушуючи стандартів прав людини. Для України такий досвід корисний і може бути імплементований через закріплення процесуальних стандартів роботи з медіа у КПК України, відомчих інструкціях; створення спеціалізованих підрозділів OSINT-аналізу медіаконтенту, зокрема щодо воєнних злочинів; укладення рамкових угод між правоохоронними органами й ключовими вітчизняними медіагрупами щодо алгоритму публічних звернень, захист журналістських джерел і порядок надання матеріалів органам досудового розслідування та суду; адаптацію європейських підходів до електронних доказів (Eurojust, Europol, e-Evidence) для забезпечення їх допустимості в міжнародних інституціях. Відтак, формування криміналістичних засад використання медіа вимагає одночасного розвитку законодавства, процесуальної практики та професійної культури слідчих і журналістів, що особливо важливо в умовах воєнного стану та розслідування воєнних злочинів, коли медіа стають ключовим каналом документування злочинної діяльності держави-агресора.

Література:

1. Mass Media Act (Zakon o medijih; ZMed) Ljubljana, 25 April 2001. № 010-01/99-8/3. URL: www.srdf.si/File/predpisi/mass_media_act.doc

2. Про масову інформацію: Закон Республіки Арменія від 13.12.2003 р. URL: https://www.arlis.am/hy/acts/62084

3. Про свободу слова та самовираження: Закон Грузії від 24.06.2004 р. URL: https://matsne.gov.ge/ru/document/download/33208/1/ru/pdf

4. Про друк та інші засоби масової інформації : Закон Латвії від 20.12.1990 р. URL:http://lib.rada.gov.ua/LibRada/static/LIBRARY/catalog/law/latv_smi.html

5. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права. Нью-Йорк і Женева. 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

6. Каланча І. Г. Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект : монографія. Київ : Вид-во «SBA Print», 2025. 528 с.

7. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Видавництво «Юридика», 2024. 180 с.

8. Aktenzeichen XY … ungelöst. Вікіпедія. URL: https://de.wikipedia.org/wiki/Aktenzeichen_XY_%E2%80%A6_ungel%C3%B6st?utm_source=chatgpt.com

9. Code de procédure pénale. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/

10. German court finds hacked EncroChat phone evidence inadmissible. URL: https://www.computerweekly.com/news/366617630/German-court-finds-hacked-EncroChat-phone-evidence-inadmissible

11. Service providers under key legal frameworks on e-evidence. European Union Agency for Criminal Justice Cooperation. URL: https://www.eurojust.europa.eu/publication/service-providers-under-key-legal-frameworks-e-evidence

12. Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings. URL: https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2025-06/guidelines-trtmnt-elctrnc.pdf

13. Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services. URL: https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng

References:

1. Mass Media Act (Zakon o medijih; ZMed) (2001, April 25). Ljubljana. Retrieved from http://www.srdf.si/File/predpisi/mass_media_act.doc

2. Pro masovu informatsiiu: Zakon Respubliky Armeniia vid 13.12.2003 r. (Law on Mass Media of the Republic of Armenia, 2003, December 13). Retrieved from https://www.arlis.am/hy/acts/62084

3. Pro svobodu slova ta samovyrazhennia: Zakon Hruzii vid 24.06.2004 r. (Law on Freedom of Speech and Expression, Georgia, 2004, June 24). Retrieved from https://matsne.gov.ge/ru/document/download/33208/1/ru/pdf

4. Pro druk ta inshi zasoby masovoi informatsii: Zakon Latvii vid 20.12.1990 r. (Law on Press and Other Mass Media, Latvia, 1990, December 20). Retrieved from http://lib.rada.gov.ua/LibRada/static/LIBRARY/catalog/law/latv_smi.html

5. Berkeley Protocol on Investigations Using Open-Source Digital Data (2020). Practical Guide for Effective Use of Open-Source Digital Information in Investigating Violations of International Criminal Law, Human Rights, and Humanitarian Law. New York & Geneva. Retrieved from https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

6. Kalancha, I. H. (2025). Dokazy, shcho maiut elektronnu formu, v kryminalnomu protsesi Ukrainy: kontseptual′nyi aspekt (Evidence in Electronic Form in Criminal Proceedings of Ukraine: Conceptual Aspect) [Monograph]. Kyiv: SBA Print.

7. Torbas, O. O. (2024). OSINT pry rozsliduvanni kryminal′nykh pravoporushen′ (OSINT in the Investigation of Criminal Offenses) [Textbook]. Odesa: Yurydyka.

8. Aktenzeichen XY … ungelöst. (n.d.). Wikipedia. Retrieved from https://de.wikipedia.org/wiki/Aktenzeichen_XY_%E2%80%A6_ungel%C3%B6st?utm_source=chatgpt.com

9. Code de procédure pénale. (n.d.). Retrieved from https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/

10. German court finds hacked EncroChat phone evidence inadmissible. (n.d.). Retrieved from https://www.computerweekly.com/news/366617630/German-court-finds-hacked-EncroChat-phone-evidence-inadmissible

11. European Union Agency for Criminal Justice Cooperation. (n.d.). Service providers under key legal frameworks on e-evidence. Retrieved from https://www.eurojust.europa.eu/publication/service-providers-under-key-legal-frameworks-e-evidence

12. Commonwealth Secretariat. (2025). Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings. Retrieved from https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2025-06/guidelines-trtmnt-elctrnc.pdf

13. Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services. (2018). Retrieved from https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng