СВИРИДЮК Н. П.,
доктор юридичних наук, професор,
старший науковий співробітник науково-дослідної лабораторії
з актуальних питань кримінального аналізу,
(Одеський державний університет внутрішніх справ)
orcid.org/ 0000-0001-9772-1119

УДК 004.056.5:343.326:343.97:343.14:341.231.14
DOI https://doi.org/10.32842/2078-3736/2025.5.2.47

КІБЕРЗЛОЧИННІСТЬ ТА КІБЕРТЕРОРИЗМ: БАЛАНС ДОСТУПУ ДО ЦИФРОВИХ ДОКАЗІВ І ЗАХИСТУ ПРАВ ЛЮДИНИ

У статті досліджуються проблеми, пов'язані з кіберзлочинністю та кібертероризмом, які стали одними з найсерйозніших загроз для безпеки та прав людини в еру цифрових технологій. Особлива увага приділяється питанням правової регламентації доступу до цифрових доказів і проведення онлайн-розслідувань, які часто вступають у конфлікт з правами на приватність. Кіберзлочинність і кібертероризм ставлять перед правоохоронними органами нові виклики, адже виявлення та розслідування таких злочинів вимагає технологічної підготовленості та відповідних юридичних механізмів.

У статті розглядається важливість дотримання балансу між забезпеченням національної безпеки та захистом основних прав людини, зокрема права на приватність, при використанні технологій для боротьби з кіберзлочинністю. Одним із основних інструментів для розслідувань є розвідувальні дані з відкритих джерел (OSINT), що використовуються для виявлення кіберзлочинців та збору доказів. Проте, їх використання потребує чіткої правової регламентації, щоб уникнути порушення прав людини, зокрема у випадках незаконного збору особистих даних.

Стаття також аналізує міжнародні правові норми, такі як Європейська конвенція з прав людини, та їх вплив на діяльність правоохоронних органів у сфері кібербезпеки. При цьому, увага звертається на різні підходи в законодавствах окремих країн (Велика Британія, Нідерланди, Франція, США) щодо проблеми доступу до цифрових доказів, а також проблем міжнародної співпраці у боротьбі з кіберзлочинністю.

Окремо розглядаються етичні аспекти онлайн-розслідувань, пов'язаних із захистом персональних даних, та важливість дотримання процедурної прозорості. У статті також надаються рекомендації щодо удосконалення міжнародних правових стандартів і національних законодавств для забезпечення ефективної боротьби з кіберзлочинністю при збереженні прав людини.

Ключові слова: *кіберзлочинність, кібертероризм, права людини, цифрові докази, онлайн-розслідування, OSINT.*

Svyrydiuk N. P. Cybercrime and cyberterrorism: balancing access to digital evidence and protecting human rights

This article examines issues related to cybercrime and cyberterrorism, which have become some of the most serious threats to security and human rights in the age of digital technologies. Particular attention is given to legal regulations regarding

access to digital evidence and conducting online investigations, which often conflict with privacy rights. Cybercrime and cyberterrorism present new challenges for law enforcement, as detecting and investigating these crimes requires technological preparedness and appropriate legal mechanisms.

The article discusses the importance of balancing national security with the protection of fundamental human rights, particularly the right to privacy, when using technologies to combat cybercrime. One of the main tools for investigations is open-source intelligence (OSINT) data, which is used to identify cybercriminals and gather evidence. However, its use requires clear legal regulation to avoid violating human rights, especially in cases of illegal collection of personal data.

The article also analyzes international legal norms, such as the European Convention on Human Rights, and their impact on the activities of law enforcement agencies in the field of cybersecurity. At the same time, the article focuses on different approaches in the legislation of individual countries (the UK, the Netherlands, France, the USA) to the issue of access to digital evidence, as well as the challenges of international cooperation in combating cybercrime.

Ethical aspects of online investigations related to the protection of personal data and the importance of procedural transparency are also discussed. The article provides recommendations for improving international legal standards and national legislation to ensure effective combat against cybercrime while preserving human rights.

Key words: *cybercrime, cyberterrorism, human rights, digital evidence, online investigations, OSINT.*

Постановка проблеми. У сучасному світі, де цифрові технології стали невід'ємною частиною повсякденного життя, кіберзлочинність і кібертероризм постають як серйозні глобальні загрози. Ці явища мають не лише технічний, але й глибокий соціальний, економічний та політичний характер, оскільки вони порушують базові принципи безпеки, приватності та прав людини. У зв'язку з цим виникає необхідність у створенні ефективних механізмів правового регулювання та слідчих повноважень для боротьби з кіберзлочинами, водночас зберігаючи баланс між безпекою та захистом основних прав громадян.

Кіберзлочинність охоплює широкий спектр незаконних дій, які здійснюються за допомогою сучасних технологій, таких як хакерські атаки, фішинг, крадіжки персональних даних тощо. Кібертероризм, у свою чергу, передбачає використання інформаційних технологій з метою здійснення терористичних актів або дестабілізації державних структур. Обидва ці явища становлять загрозу не лише для окремих осіб, а й для національної безпеки, критичної інфраструктури та глобального миру.

Виявлення і розслідування таких злочинів вимагають високого рівня технологічної підготовленості правоохоронних органів та наявності спеціальних законодавчих інструментів. У той же час, доступ до цифрових доказів часто суперечить правам людини, зокрема праву на приватність, що викликає серйозні етичні та юридичні дилеми. Важливим є пошук оптимального балансу між необхідністю забезпечення національної безпеки та захистом основних прав громадян.

На тлі таких викликів ключовим аспектом стає роль міжнародних правових норм і стандартів у боротьбі з кіберзлочинністю та кібертероризмом. Важливе місце серед таких норм займають положення Європейської конвенції з прав людини та інші міжнародні документи, що регламентують діяльність правоохоронних органів у сфері кібербезпеки. Поряд з ними, національні законодавства, а також рішення судів різних країн мають важливе значення для формування єдиного підходу до регулювання доступу до цифрових доказів та здійснення розслідувань у мережі.

Вивчення питань щодо юридичних та етичних викликів, що виникають при боротьбі з кіберзлочинністю та кібертероризмом, зокрема у контексті використання розвідувальних даних з відкритих джерел (OSINT) є важливим для розвитку ефективних та правомірних

механізмів боротьби з кіберзлочинами в умовах сучасних цифрових реалій. Разом з тим, корисним та важливим у даному аспекті є аналіз правових інструментів та судової практики, що дозволяють здійснювати онлайн-розслідування, не порушуючи основних прав людини.

Виклад основного матеріалу дослідження. Випадки кіберзлочинності та кібертероризму стрімко зростають і становлять серйозну загрозу як для окремих осіб, так і для суспільства. Вони порушують права людини та завдають великої шкоди від громадян до критично важливих об'єктів інфраструктури. Оскільки ці злочини здійснюються у кіберпросторі, їх виявлення і розслідування вимагає доступу правоохоронних органів до цього середовища, що може зачепити більшу кількість осіб, ніж традиційні кримінальні справи. У зв'язку з цим виникає дилема: захищати громадян за рахунок їхніх прав чи обмежити ці права в інтересах безпеки. Одним з найяскравіших прикладів є справа 2016 року між ФБР і Apple, де компанія виступила проти запиту на доступ до iPhone, що могло б порушити принципи приватності [1]. Такі суперечності піднімають важливі питання щодо балансу між правами людини та необхідністю боротьби з кіберзлочинністю.

Система кримінального правосуддя в більшості країн розглядає кіберзлочинність через адаптацію існуючих кримінальних законів, проте, через труднощі з отриманням цифрових доказів, деякі держави приймають спеціальні закони для забезпечення доступу до цифрової інформації. Це створює серйозну проблему для захисту приватності громадян, адже багато законодавчих актів надають правоохоронним органам розширені повноваження, що часто порушують основні права людини, такі як право на недоторканність приватного життя.

Такі ініціативи як звіт Комітету з питань розвідки та безпеки Великої Британії щодо перехоплення комунікаційних даних [2] або запропоновані законопроекти в Нідерландах та Франції, що дозволяють широке спостереження за цифровими комунікаціями, викликають серйозну критику від правозахисних організацій, які стурбовані можливістю порушення прав на приватність [3; 4]. Незважаючи на це, такі ініціативи необхідні для боротьби з кіберзлочинністю, що не знає кордонів і часто виходить за рамки національних юрисдикцій.

З точки зору етики і права, кожен випадок доступу до персональних даних повинен бути ретельно оцінений, з урахуванням законодавчих обмежень та норм, що регулюють обробку персональних даних. Під час онлайн-розслідувань за допомогою відкритих джерел слід уникати будь-якого порушення приватності громадян. Розслідування за допомогою OSINT використовують публічні веб-джерела для збору інформації, яка може бути критично важливою для виявлення і переслідування кіберзлочинів. Однак такі практики не повинні порушувати права громадян на конфіденційність [5].

Розвиток інструментів для збору цифрових доказів та нові технології, які використовуються під час розслідувань, мають бути підкріплені чіткими юридичними та етичними стандартами. Важливою задачею є забезпечення балансу між ефективністю розслідувань і захистом прав людини. Для цього необхідно вдосконалювати міжнародну співпрацю і гармонізувати законодавство, що дозволить створити єдині стандарти для боротьби з кіберзлочинністю на глобальному рівні.

Пропоновані зміни в законодавстві, зокрема, щодо розширення повноважень правоохоронців, потребують глибшого аналізу та обговорення на міжнародному рівні. У зв'язку з цим важливою є роль міжнародних організацій, зокрема Ради Європи, яка надає рекомендації щодо застосування європейських стандартів прав людини в контексті боротьби з кіберзлочинністю.

У підсумку, з огляду на глобальний характер кіберзлочинності, країни повинні розробляти правові механізми, що дозволяють забезпечити безпеку в інтернеті без порушення основних прав людини. Правоохоронні органи повинні працювати в рамках чітких процедурних норм, що гарантують дотримання законодавства про захист персональних даних та право на приватність, щоб уникнути зловживань у сфері цифрового спостереження.

Законодавство ЄС щодо захисту даних встановлює важливі принципи, що регулюють обробку персональних даних у різних сферах, зокрема, в контексті кримінальних

розслідувань. Основним нормативним актом є Директива про захист даних [6], яка визначає, що обробка персональних даних повинна мати правову основу і бути необхідною в демократичному суспільстві. Якщо законною метою є розслідування злочинів, суд все одно розглядає принципи необхідності та пропорційності при обробці даних [7; 8]. Крім того, ці принципи повинні дотримуватися, навіть коли обробка персональних даних здійснюється для поліцейських цілей, таких як розслідування кіберзлочинів.

Захист прав на недоторканність приватного життя і захист персональних даних закріплено в Хартії основних прав Європейського Союзу [9]. Обробка персональних даних без відповідної правової підстави є порушенням статті 8 Європейської конвенції з прав людини (ЄКПЛ), що захищає право на приватне життя. Європейський суд з прав людини послідовно підтверджує, що будь-яке втручання у приватне життя повинно бути обґрунтованим і здійснюватися на підставі закону [10; 11]. У разі використання даних з відкритих джерел (OSINT), особливо якщо це включає зберігання інформації про осіб, які не є підозрюваними, виникає додаткове занепокоєння щодо порушення їхніх прав на приватність.

З метою забезпечення захисту даних на європейському рівні, основним міжнародним правовим актом є Конвенція 10845 Ради Європи [12], яка регулює захист даних, зокрема в діяльності поліції. Принципи цієї конвенції аналогічні тим, що закріплені в Директиві про захист даних. У 2016 році були ухвалені два важливі законодавчі акти, які надають правила щодо обробки персональних даних правоохоронними органами: Загальний регламент про захист даних (GDPR) [13] та Директива щодо поліцейської діяльності [14]. GDPR накладає зобов'язання на органи, що обробляють персональні дані, зокрема, щодо їх зберігання та використання у розслідуваннях. Директива регулює збереження та обробку персональних даних під час поліцейських розслідувань. Ці правила продовжують діяти навіть після виходу Великої Британії з ЄС, оскільки Британія повинна дотримуватись стандартів для обміну даними з європейськими правоохоронними органами.

Концепція Privacy by Design (конфіденційність за задумом), яка згадується в GDPR, передбачає вбудовування механізмів захисту конфіденційності в процеси збору даних з самого початку їх обробки [15]. Основні принципи цієї концепції включають проактивність, конфіденційність за замовчуванням, забезпечення прозорості та поважання прав користувачів. Збір даних для розслідувань, зокрема з відкритих джерел, має відповідати цим принципам, зокрема шляхом мінімізації збору даних, їх приховування та забезпечення конфіденційності на всіх етапах процесу. Відповідно до цих принципів, особисті дані мають бути доступними лише тим, хто має на це законне право, і зберігатися тільки стільки, скільки це необхідно для досягнення цілей розслідування.

Збір і обробка даних з відкритих джерел мають важливе значення для виявлення та розслідування кіберзлочинів. Однак такий процес має дотримуватися принципів необхідності та пропорційності, що є основою для забезпечення прав людини. Порушення цих принципів може призвести до порушень прав на приватність та недоторканність персональних даних. Наприклад, національні та міжнародні закони, що захищають права на конфіденційність, накладають обмеження на зберігання та обробку таких даних. Це є особливо важливим після скандалу з викриттям даних, пов’язаних зі Стівеном Сноуденом, який підняв питання про масове спостереження за громадянами [16].

Зберігання даних з відкритих джерел регулюється низкою законодавчих актів. Європейська директива з питань зберігання даних була визнана недійсною у 2014 році через порушення прав на приватність і захист даних [17]. Замість цього, країни-члени ЄС повинні приймати національні закони для врегулювання зберігання даних, і в таких випадках, як у Великій Британії, існують відповідні законодавчі акти, такі як Закон про збереження даних і слідчі повноваження [18], хоча ці закони також можуть бути визнані неконституційними, якщо вони порушують принципи конфіденційності та пропорційності.

У зв’язку з міжнародною природою кіберзлочинності, правоохоронні органи часто стикаються з труднощами при отриманні доказів, збережених на серверах в інших країнах. У таких випадках застосовуються національні закони країни, де знаходяться ці сервери.

Якщо дані зберігаються в країнах, таких як США, можуть виникнути додаткові труднощі, зокрема, при спробі отримати доступ до персональних даних, збережених компаніями, що мають обмежену співпрацю з правоохоронними органами. Наприклад, у справі між ФБР та Apple щодо доступу до iPhone, компанія відмовилася надавати доступ до пристрою, що призвело до значних затримок у розслідуванні кіберзлочинів [19].

Збір і обробка даних із відкритих джерел для розслідувань кіберзлочинів вимагають дотримання принципів конфіденційності та прав людини. Водночас, зберігання та використання таких даних повинні відповідати законодавчим вимогам щодо захисту персональних даних і забезпечення пропорційності. Це є важливим аспектом для підтримки правосуддя та ефективної боротьби з кіберзлочинністю, враховуючи міжнародні стандарти та правові обмеження.

Правила доказування в кримінальних справах існують для забезпечення справедливого судового процесу. Вони регулюють, як докази повинні бути зібрані, досліджені та представлені в суді, щоб вони могли бути прийняті та використані для підтримки обвинувачення. Перший етап доказування включає ідентифікацію та вилучення матеріалів, які можуть бути використані як докази. У контексті кіберзлочинів більшість країн ухвалили закони, що дозволяють поліції отримувати цифрові докази, важливі для кримінального розслідування, зберігати їх до їх оприлюднення. Зберігання та дослідження доказів повинно здійснюватися під суворим контролем для демонстрації безперервності та цілісності процесу.

Щодо вилучення цифрових доказів заслуговують на увагу настанови про отримання, дослідження та представлення цифрових доказів, які у Великій Британії розробила Асоціація старших офіцерів поліції. Ці настанови сприяють стандартизації процесу вилучення та збереження доказів. Особливу увагу приділяють цілісності даних, оскільки цифрові докази можуть бути легко змінені або підроблені. Всі дії щодо оригінальних даних мають здійснюватися лише уповноваженими особами.

Крім того, цифрові докази повинні бути вивчені експертами, оскільки оригінальний формат може бути непридатним для представлення в суді. Для цього можуть застосовуватися додаткові процедури. Слідчі також повинні бути вибірковими у вилученні даних, оцінюючи, чи мають вони відношення до конкретного розслідування. Наприклад, вилучення сімейного комп'ютера без підстав може порушити право на приватність відповідно до законодавства.

У разі використання відкритих джерел, важливо залишати "слід" під час доступу до вебсайтів, щоб попередити їх власників про інтерес правоохоронців. Також необхідно вести чіткий облік всіх дій під час вилучення даних. Докази з відкритих джерел повинні бути зібрані та представлені згідно з вимогами, які забезпечують їх законність і достовірність.

Розкриття матеріалів, зібраних або створених під час розслідування, у Великій Британії регулюється та керується Законом про доступ до інформації та Кодексом [20], виданим відповідно до цього закону, а також вказівками Генерального прокурора та судовим протоколом. Порушення правил розкриття може призвести до зриву судового процесу або закриття справи. Всі матеріали, які можуть допомогти захисту або підірвати обвинувачення, мають бути розкриті. Це особливо важливо для справ, де розслідування включає період спостереження до вчинення злочину.

У випадках, коли використовуються тактики, що потребують захисту (наприклад, відповідно до Закону про розслідування і прослуховування), інформація може бути розкрита лише як конфіденційна. Також важливо зазначити, що частина зібраних матеріалів може містити персональну чи конфіденційну інформацію осіб, не пов'язаних із розслідуванням, наприклад, дані з акаунтів у соціальних мережах. У таких випадках необхідно використовувати відредаговані версії матеріалів або обмежити доступ до невідредагованих даних.

Розслідування кіберзлочинів часто охоплює кілька юрисдикцій, що може викликати складнощі через різні національні закони. Наприклад, складно визначити, хто має проводити розслідування та де має бути проведене кримінальне переслідування. Зазвичай, це залежить від місця скоєння злочину та від того, де було завдано найбільших збитків. Також можуть виникати проблеми зі збором даних, оскільки закони різних країн визначають доступ до

інформації по-різному. У таких випадках можуть бути затримки в процесі, що впливає на оперативність розслідувань.

Використання розвідданих з відкритих джерел кіберзлочинності означає проведення розслідувань в умовах відсутності кордонів. Це може викликати проблеми на кількох фронтах через різні національні закони залучених країн. Часто виникають труднощі з визначенням того, хто має проводити розслідування і де має здійснюватися кримінальне переслідування. Як уже згадувалося, між деякими країнами також існують труднощі щодо збору даних.

У 2016 році Європарламент ухвалив Регламент ЄС, який дозволяє Європолу ефективніше боротися з транскордонною злочинністю, включаючи кіберзлочинність. За цим законодавством, Європол може безпосередньо звертатися до компаній, таких як Facebook, щоб вимагати видалення матеріалів, що підтримують тероризм.

Також важливим інструментом є мережа Спільних слідчих груп (ССГ), створена у 2005 році в рамках реалізації Гаазької програми [21] для підтримки співпраці та взаємодії слідчих груп між державами-членами ЄС. Ці групи включають представників правоохоронних органів, суддів і прокурорів, що дозволяє здійснювати прямий обмін інформацією та доказами без використання офіційних каналів взаємної правової допомоги.

Висновок. Проблематика кіберзлочинності та кібертероризму є однією з найбільш актуальних у сучасному правовому та соціально-економічному контексті. Технологічний прогрес сприяє швидкому розвитку нових форм злочинів, що здійснюються у кіберпросторі, створюючи серйозні виклики для державних інститутів і правоохоронних органів, а також для громадян, чиї права можуть бути порушені в процесі розслідувань. У зв'язку з цим, одним із найбільш важливих аспектів є створення ефективної правової бази, яка дозволяє боротися з кіберзлочинністю, не порушуючи основних прав людини, зокрема, права на приватність.

Здійснення онлайн-розслідувань та використання цифрових доказів, зокрема даних з відкритих джерел, надає правоохоронним органам нові можливості для ефективної боротьби з кіберзлочинами та кібертероризмом. Проте, це вимагає значної уваги до етичних та юридичних аспектів, оскільки збори та використання персональних даних без належної правової регламентації можуть призвести до серйозних порушень прав людини. Правоохоронці повинні діяти в межах національного та міжнародного законодавства, що гарантує недоторканність приватного життя громадян.

Одним із важливих питань є необхідність досягнення балансу між забезпеченням національної безпеки та захистом прав громадян. Кожен випадок доступу до цифрових даних або проведення онлайн-розслідувань потребує ретельної оцінки ризиків порушення прав людини та визначення доцільності втручання. Для ефективного розв'язання цієї проблеми на міжнародному рівні необхідно забезпечити гармонізацію національних законодавств, що дозволить зменшити правові бар'єри і сприятиме більш ефективній міжнародній співпраці в боротьбі з кіберзлочинністю.

Список використаних джерел:

1. Hern, A. (2016, March 29). Apple declares victory in battle with FBI, but the war continues. The Guardian. Retrieved from https://www.theguardian.com/technology/2016/mar/29/apple-victory-battle-fbi-but-war-continues-san-bernardino-iphone?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+main+NEW+H&utm_term=164296&subid=13209147&CMP=EMCNEWEML6619I2

2. Intelligence and Security Committee of Parliament. (2015, March 12). Privacy and security: A modern and transparent legal framework. HMSO. Retrieved from https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cqVUAbEn1Wlwy7jBr_BmXr5OO72-sBuBienMmDWi5kUa5hxQOafIjfEREk8eMJIL5ssJov7xru8L-Omuu2mtMnCZi_gEKs2t55QqorpbNX9k5oI_q3p8-xG3cpB7yHC-RWXX8wGGhWnhDKVkorvJjgeSLgDwpzH3p2ktFSi79_8RuQEJfmdLmi-LPk2iWZF6zMhiZmA2EFvfTft-b2rHRKOyzxeqwhfr5ekhEaE2zSSk5W4dAlACpqjJM5qUJ9kMBvFkn-2d&attredirects=0

3. Siedsma, T., & Austin, E. (2016, May 4). Dutch dragnet surveillance bill leaked. European Digital Rights (EDRi). Retrieved from https://edri.org/

4. Siedsma, T., & Austin, E. (2015, July 24). France: New surveillance law a major blow to human rights. Amnesty International. Retrieved from https://www.amnesty.org/en/latest/news/2015/07/france-new-surveillance-law-a-major-blow-to-human-rights/

5. Hill, M. QC, & Davis, W. (2013, Winter). Social media and criminal justice (Issue 4, pp. 5–?). Criminal Bar Quarterly. Retrieved from https://www.criminalbar.com/files/download.php?m=documents&f=141106211508-CBQWinter2013.pdf

6. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31, as amended.

7. S and Marper v. United Kingdom, Appl. No. 30562/04 (ECtHR 4 December 2008)

8. Z v. Finland, Appl. No. 2209/93 (ECtHR 25 February 1997).

9. Charter of Fundamental Rights of the European Union, [2010] OJ C 83/02.

10. ECtHR. Leander v. Sweden, No. 9248/81, 26 March 1987.

11. ECtHR. M.M. v. the United Kingdom, No. 24029/07. 13 November 2012.

12. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 108 1981.

13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

14. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

15. Cavoukian, A. (2011). 7 foundational principles of privacy by design. https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

16. Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105.

17. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Siochana, Ireland, The Attorney General, intervener: Irish Human Rights Commission and Karntner Landesregierung, Michael Seitlinger, Christof Tschohl and others [2014].

18. Mason Hayes and Curran. (2015, July). Stopping the 'DRIP' of data—UK Court finds revised data retention legislation unlawful. Institute of Paralegals. Retrieved from http://www.lexology.com/library/detail.aspx?g=c2b1a42b-5fa9-435f-a201-c0458e35fbe6

19. Summary of case and issues available. Apple iPhone Standoff Ends, for Now (2016). The New York Times. Retrieved from http://www.nytimes.com/indexes/2016/03/29/technology/bits/index.html?nlid=70241408

20. The Criminal Procedure and Investigations Act 1996 (Code of Practice) Order 2015.

21. The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53, 3.3.2005, p. 1, and the Council and Commission action plan implementing the Hague.

Дата першого надходження рукопису до видання: 27.09.2025
Дата прийнятого до друку рукопису після рецензування: 29.10.2025
Дата публікації: 28.11.2025