УДК 343.9:004.056:342.7
DOI 10.31732/2708-339X-2026-19-A15

ВИКОРИСТАННЯ ВІДКРИТОЇ ІНФОРМАЦІЇ ПРИВАТНИМИ ДЕТЕКТИВАМИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА: ПРАВОВІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ ЗАХИСТУ ПРАВ ЛЮДИНИ

Чернетченко О.М.,
к.ю.н., доцент, доцент кафедри державно-правових дисциплін
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: OlenaCH@krok.edu.ua
ORCID: https://orcid.org/0000-0002-4653-4871

Щербакова О.О.,
здобувач ступеня вищої освіти «магістр»
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: ShcherbakovaOO@krok.edu.ua
ORCID: https://orcid.org/0009-0003-8417-4277

USE OF OPEN INFORMATION BY PRIVATE DETECTIVES IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF SOCIETY: LEGAL CHALLENGES AND PROSPECTS FOR THE PROTECTION OF HUMAN RIGHTS

Chernetchenko O.M.,
Candidate of Law
Associate Professor of the Department of State and Legal Disciplines,
«KROK» University,
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: OlenaCH@krok.edu.ua,
ORCID: https://orcid.org/0000-0002-4653-4871

Shcherbakova O.O.,
graduate of the Master's degree of
«KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: ShcherbakovaOO@krok.edu.ua
ORCID: https://orcid.org/0009-0003-8417-4277

***Анотація**. У статті здійснено комплексний аналіз особливостей використання відкритої інформації (Open Source Intelligence, OSINT) у діяльності приватних детективів в умовах інтенсивної цифрової трансформації суспільства. Дослідження спрямоване на з'ясування правових викликів, пов'язаних із доступом, збиранням, обробкою та використанням відкритих джерел інформації, а також на оцінку їх впливу на забезпечення та захист фундаментальних прав і свобод людини.*

Охарактеризовано сучасний інформаційний ландшафт, який формується публічними державними реєстрами, порталами відкритих даних, соціальними мережами, картографічними сервісами та іншими загальнодоступними цифровими ресурсами, порталами. Встановлено, що широке використання OSINT суттєво розширює інструментарій приватної детективної діяльності, підвищує ефективність встановлення фактів, перевірки відомостей, аналізу соціальних, майнових і ділових зв'язків, а також сприяє оперативності прийняття рішень у межах приватних розслідувань. Водночас наголошено, що зростання обсягів доступної інформації супроводжується підвищеними ризиками порушення права на

приватне життя особи, незаконної обробки її персональних даних, розголошення чутливої інформації та виникнення потенційних загроз безпеці окремих осіб, особливо в умовах воєнного стану та цифрових конфліктів.

На основі змістовного аналізу чинного законодавства України (Конституції України, постанов та ухвал, кодексів та законів України), міжнародно-правових стандартів та практики Європейського суду з прав людини визначено ключові проблеми правового регулювання OSINT-практик, зокрема відсутність спеціального чинного закону про приватну детективну діяльність, невизначеність меж допустимих методів збору відкритої інформації, а також недостатність механізмів контролю, відповідальності та відновлення порушених прав. Обґрунтовано напрями вдосконалення правового регулювання використання відкритої інформації приватними детективами, що передбачають диференціацію категорій публічних даних, упровадження вимог до мінімізації, псевдоанонімізації та зберігання інформації, розвиток системи ліцензування, професійних стандартів і етичних принципів приватної детективної діяльності з пріоритетом балансу між ефективністю розслідувань і захистом прав людини.

***Ключові слова**: приватний детектив; відкрита інформація; захист прав людини; цифрова трансформація суспільства.*

***Формул**: 0, рис.: 0, табл.: 0, бібл.: 8.*

***Abstract**. The article provides a comprehensive analysis of the use of open source intelligence (OSINT) in the activities of private investigators in the context of intensive digital transformation of society. The study aims to identify legal challenges related to access, collection, processing, and use of open sources of information, as well as to assess their impact on ensuring and protecting fundamental human rights and freedoms.*

It characterizes the modern information landscape, which is shaped by public state registries, open data portals, social networks, mapping services, and other publicly available digital resources and portals. It has been established that the widespread use of OSINT significantly expands the tools of private detective work, increases the effectiveness of establishing facts, verifying information, analyzing social, property, and business connections, and also contributes to the speed of decision-making in private investigations. At the same time, it is emphasized that the growth in the volume of available information is accompanied by increased risks of violation of the right to privacy, illegal processing of personal data, disclosure of sensitive information, and potential threats to the security of individuals, especially in conditions of martial law and digital conflicts.

Based on a substantive analysis of the current legislation of Ukraine (the Constitution of Ukraine, resolutions and decrees, codes and laws of Ukraine), international legal standards, and the practice of the European Court of Human Rights, key problems in the legal regulation of OSINT practices have been identified, in particular the absence of a specific law on private detective activities, the uncertainty of the limits of permissible methods of collecting open information, and the insufficiency of mechanisms for control, accountability, and restoration of violated rights. The directions for improving the legal regulation of the use of open information by private detectives are substantiated, providing for the differentiation of categories of public data, the introduction of requirements for minimization, pseudo-anonymization, and storage of information, and the development of a licensing system, professional standards, and ethical principles for private detective activities, with a priority on balancing the effectiveness of investigations and the protection of human rights.

***Keywords**: private detective; open information; human rights protection; digital transformation of society.*

***Formulas**: 0, fig.: 0, tabl.: 0, bibl.: 8.*

Постановка проблеми. Цифрова трансформація суспільства суттєво змінила характер обігу інформації, відкривши нові можливості для її збору, аналізу та використання. У сучасних умовах доступ до відкритих джерел даних Open Source Intelligence (OSINT) став невід'ємним елементом як діяльності державних органів, так і приватного сектору. Особливого значення він набуває для приватних детективів, які використовують відкриту інформацію для вирішення завдань із пошуку осіб, встановлення фактів чи перевірки відомостей.

Разом із тим, широке застосування цифрових технологій створює низку правових та етичних конфліктів. З одного боку, суспільство вимагає максимальної прозорості, а держава забезпечує відкритий доступ до багатьох реєстрів і баз даних. З іншого боку, зростає ризик порушення права людини на приватність (ст. 8 ЄКПЛ), захист персональних даних, честь та гідність. Баланс між потребами розслідування та гарантіями прав і свобод особи стає ключовим завданням правового регулювання у сфері приватної детективної діяльності.

В умовах відсутності в Україні чіткого закону про приватну детективну

діяльність особливої ваги набуває аналіз правових аспектів використання відкритої інформації. Необхідним є дослідження міжнародного досвіду, стандартів Європейського суду з прав людини, а також перспектив формування національної нормативної бази, що забезпечувала б як ефективність роботи детективів, так і належний захист прав людини.

Аналіз останніх досліджень і публікацій. У низці досліджень розглядаються сучасні виклики, пов'язані із захистом персональних даних в умовах цифровізації. Зокрема, О.М. Биков і В.В. Савченко у роботі «Захист персональних даних у сучасному законодавстві» аналізує вплив інформаційних технологій і кіберзагроз на право на приватність, а також підкреслює, що існуюче законодавство потребує адаптації до нових технологічних викликів [1]. Аналогічно й В.Г. Пилипчук та В.М. Брижко у роботі «Реформування і розвиток системи захисту персональних даних в Україні» розглядає історико-правові аспекти й перспективи розвитку системи захисту персональних даних в Україні в контексті євроінтеграції [2].

Обидва джерела створюють теоретичну базу для розуміння того, як обробка відкритих даних і їх використання (у тому числі приватними детективами) можуть вступати в протиріччя з правом на приватне життя.

Що стосується теми використання відкритих джерел (OSINT) та їх інтеграції у практику безпеки та розслідувань, публікація Д. Дрижакова і Р. Волинець «Використання відкритих джерел інформації повна назва(OSINT) у сфері безпеки держави: технології та перспективи» [3] фокусується на технологічних і організаційних аспектах, демонструючи, що OSINT-інструменти стають важливими елементами в системах безпеки держави. Також стаття А.Й. Француза (зі співавтором Ю.К. Тупіченко) «Організаційно правові засади діяльності приватних детективів в Польщі та Україні» [4] висвітлює, що діяльність приватних детективів в Україні має слабко розвинене правове регулювання, що створює прогалини в контролі та захисті прав громадян.

Не вирішені раніше частини загальної проблеми. Попри наявність наукових досліджень у сфері захисту персональних даних, цифровізації та застосування відкритих джерел інформації, питання використання OSINT у діяльності приватних детективів залишається недостатньо врегульованим і фрагментарно висвітленим. У більшості праць акцент зроблено на діяльності державних органів або загальних інформаційно-правових аспектах, тоді як специфіка правового статусу приватних детективів, межі допустимості використання відкритої інформації, критерії законності автоматизованого збору та повторного використання публічних даних, а також відповідальність за порушення права на приватне життя практично не досліджені. Відсутній комплексний аналіз механізмів контролю за OSINT-практиками приватних детективів, включно з питаннями ліцензування, професійних стандартів і ефективного відновлення порушених прав, що зумовлює наукову актуальність та необхідність подальшого дослідження зазначеної проблематики.

Формулювання мети. Обґрунтування ключових особливостей використання відкритої інформації приватними детективами в умовах цифрової трансформації, аналіз правових викликів, які виникають у цій сфері, та визначення перспектив удосконалення механізмів захисту прав людини.

Виклад основного матеріалу. Open Source Intelligence, далі (OSINT), означає розвідка на основі відкритих джерел. Це метод збору та аналізу інформації з загальнодоступних джерел, таких як вебсайти, соціальні мережі, новинні статті та інші [5]. Даний метод збору інформації є головним інструментом роботи для приватних детективів. З року в рік розвиток інформаційних технологій є невід'ємним атрибутом прогресивних країн. Відкриті реєстри, соціальні мережі, новині статті та вебсайти є суцільним інформаційним озерами роботи для детективів, юристів та правоохоронних органів, але на які зміни

можна очікувати надалі, чи можливий в майбутньому доступ до усієї інформації на особу в публічному просторі, якщо це є порушенням прав людини на приватність.

Для розуміння: Україна надала публічний доступ, що є повним або обмеженим, що не являється таким, який надає повну інформацію, до більше 70-ти відкритих реєстрів та баз даних країни. За допомогою лише цих джерел можливо сформувати справу стосовно певного об`єкту пошуку. Проте, офіційного переліку усіх реєстрів в державі немає і тому за сукупністю від усіх сайтів налічується приблизно 350 реєстрів. Їх кількість може змінюватись через реформи та законодавчі зміни.

Відповідно до ст. 1 Закону України «Про доступ до публічної інформації» публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації [6]. Використання публічної інформації приватними детективами в умовах цифрової трансформації суспільства створює новий якісний рівень практичної діяльності й водночас ставить низку правових та етичних викликів, що вимагають системного підходу до захисту прав людини. Сучасна цифрова екосистема забезпечує широкий доступ до публічних державних реєстрів, відкритих даних, публікацій у соціальних мережах, картографічних сервісів і бізнес-реєстрів, що істотно розширює інструментарій для збору інформації. Так, національний портал відкритих даних України data.gov.ua налічує десятки тисяч наборів даних, які охоплюють сфери економіки, інфраструктури, охорони здоров'я та інших суспільних ресурсів; за оцінками зовнішніх оглядів, на платформі доступні понад 80 000 наборів станом на 2025 рік, що ілюструє масштаби доступної публічної інформації [7].

Ця доступність створює для приватних детективів можливість більш ефективного й оперативного виконання замовлень: перевірка бізнес-контрагентів через відкриті реєстри, верифікація даних про майно та нерухомість, з'ясування зв'язків і поведінкових патернів за публічними повідомленнями. Водночас з'являються ризики щодо порушення приватності та інших фундаментальних прав. Наприклад, коли збір і публікація персональних даних можуть призвести до ідентифікації вразливих осіб, розголошення медичної чи фінансової інформації, або становити загрозу безпеці через геолокацію та відстеження. Питання визначення меж законного збору публічної інформації стає ключовим, бо публічність джерела не завжди автоматично означає необмежене право на обробку й поширення зібраних даних.

Внутрішнє законодавство і практична юриспруденція в Україні намагаються реагувати на ці виклики, але процес регулювання має фрагментарний характер. Питання правового статусу приватної детективної діяльності тривалий час перебували в площині законодавчих ініціатив і проектів; у публічних обговореннях згадувалися проекти і пропозиції щодо формалізації діяльності детективів, що датуються кінець 2010-х і початком 2020-х років. Водночас чинна практика та наукові розробки відзначають, що суб'єкти приватної детективної діяльності обмежені у виконанні дій, віднесених до виключної компетенції державних оперативно-розшукових органів, зокрема у питаннях оперативно-розшукових заходів, що прямо регламентовано відповідними нормативними актами. Це створює правову межу між інформаційною діяльністю на основі відкритих джерел і діями, які вимагають спеціальних повноважень або дозволів [1].

Практична імплементація цих обмежень викликає складнощі: детективи часто працюють без встановлених законом прямих повноважень, де застосування сучасних OSINT-інструментів (open source intelligence) перетинається з питаннями

незаконного збору даних або зловживань. Моделі ризиків включають використання автоматизованого збору даних (web scraping) з обхідними методами, витягання персональних даних із приватних акаунтів через інструменти дедуплікації й агрегації, а також розголошення чутливої інформації, що може спричинити шкоду особі (doxxing). Аналіз міжнародних і вітчизняних публікацій демонструє, що в умовах війни та збройних конфліктів ризики мультиплікуються: публічні дані можуть бути використані для ідентифікації журналістів, цивільних активістів чи поранених, що ставить питання сумісності практик OSINT із стандартами захисту прав людини.

Ключовими правовими проблемами є: невизначеність статусу й меж дозволених методів збору інформації приватними детективами; відсутність єдиних правил обробки персональних даних, адаптованих до особливостей OSINT; ризик перетікання публічних даних у сферу незаконного розповсюдження чутливої інформації; недосконалі механізми контролю та відповідальності за порушення прав суб'єктів даних.

У відповідь на це необхідно розвивати комплексне регулювання, яке б поєднувало галузеві стандарти, ліцензійні вимоги, вимоги до професійної підготовки й етичні кодекси. Функція ліцензування має бути спрямована не тільки на формальний облік учасників ринку, але й на встановлення конкретних технічних і процедурних обмежень щодо методів збору й зберігання даних [4].

Захист прав людини в цій сфері потребує декількох практичних підходів. Спочатку необхідно впровадити чіткі норми щодо допустимості збору різних категорій даних: загальнодоступні відомості про юридичні особи, публічні реєстри і статистичні дані мають оброблятися за спрощеною процедурою, тоді як персональні дані, пов'язані з охороною здоров'я, національною безпекою або приватним життям, повинні мати підвищений захист і оброблятися лише за умов згоди або на підставі явної законної підстави. Також, потрібно визначити вимоги до зберігання й анонімізації даних: застосування псевдонімізації, мінімізація обсягу зібраної інформації, строкове обмеження зберігання – все це повинно бути закріплено нормативно та контролюватися аудитом. Доцільно ввести обов'язкові професійні стандарти і навчання для детективів, орієнтовані на права людини, кібергігієну і етичні принципи OSINT-розслідувань. Використання OSINT-інформації має відповідати національному та міжнародному законодавству [3].

Технічно-організаційні заходи захисту мають поєднуватися з процесуальними гарантіями. Для цього державні реєстри й портали відкритих даних повинні розробити алгоритми оцінки ризиків і механізми обмеження доступу до чутливих наборів даних (наприклад, через класифікацію наборів як «публічних», «умовно-публічних» і «обмежених»). Паралельно регулятор повинен передбачити інструменти контролю за діяльністю приватних детективів: реєстри суб'єктів, механізми скарг від громадян, адміністративні та кримінальні санкції за зловживання. Громадянське суспільство і професійні об'єднання (наприклад, профільні асоціації детективів) можуть відігравати важливу роль в розробці етичних кодексів і внутрішніх стандартів; існування публічних об'єднань галузі створює платформу для самоорганізації і взаємного контролю.

Окрему увагу слід приділити судовим і позасудовим механізмам відновлення порушених прав. Доступ до оперативних механізмів захисту (швидке видалення незаконних публікацій, блокування публікацій в мережах, відшкодування шкоди) має бути технічно і процедурно забезпечений; при цьому судові процедури повинні бути адаптовані до швидкоплинності цифрового контенту, щоб надавати ефективні і своєчасні засоби правового захисту. На міжнародному рівні важливим є урахування практики Європейського суду з прав людини та

рекомендацій міжнародних організацій щодо балансу між свободою інформації і правом на приватне життя, особливо в контексті OSINT [8].

Перпективи правового регулювання вказують на необхідність комбінованого підходу: поєднання спеціального законотворчого врегулювання приватної детективної діяльності, оновлення законодавства про персональні дані з урахуванням OSINT-технологій, а також розвитку інституційного нагляду й саморегулювання галузі. Такий підхід має передбачати чіткі процедури ліцензування, технічні стандарти безпеки, обов'язкову підготовку фахівців і дієві механізми захисту постраждалих осіб. Невід'ємною частиною повинні стати публічні політики щодо відкритих даних, які враховують потребу в прозорості й одночасну вимогу щодо захисту вразливих категорій населення [4].

Висновки. Цифрова трансформація значно підвищила імпульс для використання відкритої інформації у роботі приватних детективів, водночас створивши широкий спектр ризиків для прав людини. Розв'язання цих викликів можливе через комплексне регулювання, що поєднуватиме законодавчі зміни, технічні стандарти, професійне навчання й ефективні механізми захисту постраждалих осіб. Баланс між доступом до публічної інформації та гарантіями приватності має стати основною орієнтирною лінією державно-громадського діалогу, спрямованого на забезпечення безпеки, законності та поваги до прав людини в цифрову епоху.

Література:

1.Биков О.М., Савченко В.В. Захист персональних даних у сучасному законодавстві. *Legal Bulletin.* 2024. С. 67–72. URL: https://doi.org/10.31732/2708-339x-2024-14-a9 (дата звернення: 08.12.2025).

2.Пилипчук В.Г., Брижко В.М. Реформування і розвиток системи захисту персональних даних в Україні. *Інформація і право.* 2017. № 3. С. 5–21.

3.Дрижакова Д., Волинець Р. Використання відкритих джерел інформації (OSINT) у сфері безпеки держави: технології та перспективи. *Матеріали IV Міжнародної наукової конференції «Цифрове наукове суспільство*: соціально-економічні, правові та міжнародні аспекти» (Дніпро, 28.02.2025) : зб. наук. праць. Дніпро : [б. в.]. 2025. С. 138–141.

4.Француз А.Й., Тупіченко Ю.К. Організаційно-правові засади діяльності приватних детективів в Польщі та Україні. Legal Bulletin. 2022. № 6. С. 54–59.

5.Що таке OSINT (Open Source Intelligence, розвідка на основі відкритих джерел). *The Transmitted.* 31.10.2023. URL: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/ (дата звернення: 21.11.2025).

6.Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. *База даних «Законодавство України».* Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2939-17 (дата звернення: 21.11.2025).

7.Кожушко О.О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. *Науковий вісник Інституту міжнародних відносин НАУ.* 2011. Т. 2. № 4. С. 74.

8.Тополевський Р.Б. Інформаційні права людини та їх місце в системі прав людини. *Київський часопис права.* 2022. № 3. С. 39–43.

References:

1.Bykov O.M., Savchenko V.V. *Zakhyst personalnykh danykh u suchasnomu zakonodavstvi [*Protection of Personal Data in Modern Legislation]. *Legal Bulletin,* 2024. P. 67–72. Available at: https://doi.org/10.31732/2708-339x-2024-14-a9 (accessed 08 December 2025) [in Ukrainian].

2.Pylypchuk V.H., Bryzhko V.M. *Reformuvannia i rozvytok systemy zakhystu personalnykh danykh v Ukraini* [Reforming and Developing the Personal Data Protection System in Ukraine]. Informatsiia i pravo, 2017, № 3. P. 5–21 [in Ukrainian].

3.Dryzhakova D., Volynets R. *Vykorystannia vidkrytykh dzherel informatsii (OSINT) u sferi bezpeky derzhavy: tekhnolohii ta perspektyvy* [Use of Open Source Intelligence (OSINT) in State Security: Technologies and Prospects]. Materials of IV Int. Scientific Conference "Digital Scientific Society: Socio-Economic, Legal and International Aspects" (Dnipro, 28 Feb 2025). Dnipro, 2025. P. 138–141 [in Ukrainian].

4.Frantsuz A.Y., Tupichenko Y.K. *Orhanizatsiino-pravovi zasady diialnosti pryvatnykh detektyviv v Polshchi ta Ukraini [*Organizational and Legal Principles of Private Detectives in Poland and Ukraine]. Legal

Bulletin, 2022, № 6. P. 54–59 [in Ukrainian].

5.*Shcho take OSINT (Open Source Intelligence, rozvidka na osnovi vidkrytykh dzherel)* [What is OSINT – Open Source Intelligence]. *The Transmetted,* 31 Oct 2023. Available at: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/ (accessed 21 November 2025) [in Ukrainian].

6.*Pro dostup do publichnoi informatsii: Zakon Ukrainy vid 13.01.2011* № 2939-VI [Law of Ukraine on Access to Public Information]. Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/go/2939-17 (accessed 21 November 2025) [in Ukrainian].

7.Kozhushko O.O. *Rozvidka vidkrytykh dzherel informatsii (OSINT) u rozviduvalnii praktytsi SSHA* [Open Source Intelligence in US Intelligence Practice]. *Naukovyi visnyk Instytutu mizhnarodnykh vidnosyn NAU*. 2011, Vol. 2, № 4. P. 74 [in Ukrainian].

8.Topolevskyi R.B. I*nformatsiini prava liudyny ta yikh mistse v systemi prav liudyny* [Information Rights of the Human and Their Place in Human Rights System]. Kyivskyi chasopys prava, 2022, № 3. P. 39–43 [in Ukrainian].

Стаття надійшла до друку 05 січня 2026 року