УДК 343.98
DOI https://doi.org/10.32782/2524-0374/2024-2/119

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕДІА ДЛЯ ВИРІШЕННЯ ІДЕНТИФІКАЦІЙНИХ ЗАВДАНЬ ПІД ЧАС ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ДЕРЖАВНОЮ ЗРАДОЮ

THE USE OF SOCIAL MEDIA TO SOLVE IDENTIFICATION TASKS DURING THE DETECTION AND INVESTIGATION OF CRIMES RELATED TO TREASON

Цехан Д.М., д.ю.н., професор,
професор кафедри криміналістики, детективної та оперативно-розшукової діяльності
Національний університет «Одеська юридична академія»

Мурашко А.С., аспірантка кафедри криміналістики,
детективної та оперативно-розшукової діяльності
Національний університет «Одеська юридична академія»

Представлена стаття має постановочний характер та присвячена дослідженню проблематики використання соціальних медіа для вирішення ідентифікаційних завдань під час виявлення та розслідування злочинів, пов'язаних із державною зрадою. У статті на підставі аналізу статистичних даних звернуто увагу на тенденційні зміни у структурі та динаміці злочинності, що зумовлено триваючим на території України збройним конфліктом. Звернуто увагу, що у структурі механізму такої злочинної діяльності значна роль належить різним типам соціальних медіа, що зумовлено широкою доступністю інформаційних технологій для усіх верств населення. На підставі наявних статистичних даних детально проаналізовано структуру та поширеність різних типів соціальних медіа серед населення України.

Наголошено, що оптимізація розслідування таких кримінальних правопорушень на сучасному етапі, значним чином зумовлена якістю ідентифікаційних досліджень, які проводяться із використанням кіберпростору. Виокремлено основні позиції вчених щодо форм та напрямів використання соціальних медіа під час розслідування злочинів. На підставі наявних наукових позицій виокремлено три основні напрями використання соціальних медіа під час розслідування. Виокремлено основні напрями та завдання моніторингу соціальних мереж правоохоронними органами. Наголошено, що, фактично, такий моніторинг є однією із форм оперативного обслуговування кіберпростору та виокремлено основні завдання такої діяльності. Авторами звернуто окрему увагу на важливості використання таких ідентифікаційних методів на початковому етапі кримінального провадження залежно від типових слідчих ситуацій. Виокремлено різне функціональне призначення таких ідентифікаційних завдань для відповідних ситуацій.

Ключові слова: кримінальне провадження, досудове розслідування, слідча ситуація, доказування, ідентифікація, профайлінг, інформаційний профайлінг, особа злочинця, злочин, державна зрада, кіберпростір, соціальні мережі.

The presented article has a procedural nature and is devoted to the study of the problems of using social media to solve identification tasks during the detection and investigation of crimes related to treason. Based on the analysis of statistical data, the article draws attention to the trend changes in the structure and dynamics of crime caused by the ongoing armed conflict on the territory of Ukraine. Attention is drawn to the fact that in the structure of the mechanism of such criminal activity, a significant role belongs to various types of social media, which is due to the wide availability of information technologies for all segments of the population. Based on the available statistical data, the structure and prevalence of various types of social media among the population of Ukraine were analysed in detail.

It is emphasized that the optimization of the investigation of such criminal offenses at the current stage is largely determined by the quality of identification research conducted using cyberspace. The main positions of scientists regarding the forms and directions of using social media during the investigation of crimes are highlighted. On the basis of the available scientific positions, three main directions of using social media during the investigation are distinguished. The main directions and tasks of monitoring social networks by law enforcement agencies are highlighted. It is emphasized that, in fact, such monitoring is one of the forms of operational cyberspace maintenance, and the main tasks of such activity are highlighted. Particular attention is paid to the importance of using such identification methods at the initial stage of criminal proceedings depending on typical investigative situations. The different functional purpose of such identification tasks for the relevant situations is highlighted.

Key words: criminal proceedings, pre-trial investigation, investigative situation, evidence, identification, profiling, information profiling, identity of the criminal, crime, treason, cyberspace, social networks.

Військова агресія проти України та повномасштабне вторгнення російської федерації поряд з іншими негативними змінами у соціально-економічному житті нашої держави, призвела й до суттєвих змін у структурі та динаміці злочинності, у частині тенденційного зростання кількості та ускладнення внутрішньої структури злочинів, які раніше мали фрагментарний характер і не набували значного поширення, що призвело й до відсутності в окремих випадках усталених та апробованих методик їх виявлення, розслідування та збирання окремих фактичних даних із метою подальшого використання у доказуванні. Одним із таких правопорушень є державна зрада. Як свідчить статистика, надана Офісом Генерального прокурора [7], протягом 2021 року було обліковано 208 кримінальних правопорушень, передбачених ст. 111 Кримінального кодексу України (далі – КК України) (державна зрада), протягом 2022 року – 1957, а за 2023 рік – 1169, водночас вручено повідомлення про підозру у 2021 році – 64, у 2022 році – 609, а у 2023 році – 469 особам. Відповідно до ст. 111 КК України державна зрада може бути вчинена у трьох формах: перехід на бік ворога в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України [2].

Аналіз практики роботи правоохоронних органів за такими кримінальними провадженнями свідчить, що досить часто у структурі механізму їх вчинення велику роль відіграють сучасні засоби комунікації, зокрема різні типи соціальних мереж та інших форм соціальних медіа, що пов'язано із інтенсивними процесами цифровізації українського суспільства та широкою доступністю цифрових технологій для населення.

Так, зважаючи на триваючі процеси діджиталізації та збільшення попиту на користування соціальними мережами, месенджерами та іншими засобами з обміну інформацією в цифровій формі, зокрема, як свідчать матеріали опитувань (станом на 2022 рік), «повномасштабне вторгнення рф в Україну призвело до різкого зростання використання соціальних мереж як джерела новин. Серед 76,6% громадян України, які використовують соціальні

мережі як джерело інформації, 66% обирають Telegram, 61% – YouTube, 58% – Facebook» [10]. Водночас у джерелі відзначається, що станом на 2022 рік «рейтинг популярності соцмереж серед українців на виглядає так: YouTube – 28 млн; Instagram – понад 16,1 млн; Facebook – 15,45 млн; TikTok – понад 10,55 млн» [10].

Інші опитування надають наступну статистику (станом на 2023 рік): «найпопулярнішим джерелом інформації для українців залишаються соціальні мережі – їх для отримання новин обирають 77,9% опитаних (минулого року цей показник був співмірним – 76,6%, а до повномасштабного вторгнення – на рівні 63%). Найбільше соцмережами для отримання новин очікувано користується молодь (95,8%), однак за останній рік дещо зросло використання соцмереж серед сорокарічних (до 87%) та людей старших 70 років (до 36%)» [5]. Тобто, як вбачається, з початком повномасштабного російського вторгнення попит на користування соціальними мережами різко підвищився, водночас збільшилася і кількість правопорушень, пов'язаних із розголошенням інформації, яка є власністю держави та охороняється законом (віднесена до державної таємниці або службової інформації, яка в подальшому використовується проти інтересів держави).

Наведена статистична інформація не викликає жодних сумнівів, що російсько-українська війна призвела до неухильного збільшення кількості протиправних діянь, пов'язаних із державною зрадою, що у свою чергу вимагає винайдення нових способів та методів розслідування вказаної категорії злочинів, які несуть небезпеку насамперед українській державності та українському суспільству зокрема. Отже, можна стверджувати, що в розрізі заявленої проблематики доволі актуальним постає питання щодо ідентифікації особи, яка вчиняє злочини, пов'язані із державною зрадою в обстановці кіберпростору, оскільки останній як складова інфраструктури злочинної діяльності, *по-перше,* слугує «платформою» для вчинення окресленого виду протиправних діянь; *по-друге,* забезпечує умови для миттєвого передавання та розповсюдження інформації. Спираючись на концептуальний підхід запропонований О. А. Самойленко, яка слушно відзначила, що кіберпростір у даному випадку виконує подвійну функцію: є як середовищем, так і способом вчинення злочину [8]. У межах цієї статті, яка значним чином має постановочний характер у контексті дослідження цієї проблематики, необхідно звернути увагу на окремі аспекти використання соціальних мереж як джерел ідентифікації осіб, які вчиняють державну зраду, або інші суміжні кримінальні правопорушення. Серед дослідників, які займалися розробленням методики розслідування державної зради варто відмітити таких як О. Гарасимів, К. Мартинеко, О. Сухачов та інших вчених. Окремі аспекти використання соціальних мереж під час розслідування злочинів розглядали у своїх наукових роботах Р. Благута, О. Дуфенюк, О. Лисенко, Т. Павлиш, О. Терещенко, В. Шевчук та інші науковці.

Перш за все, необхідно звернути увагу на загальні напрацьовані у криміналістиці підходи щодо використання соціальних мереж у розслідуванні кримінальних правопорушень. Як відзначає О. Дуфенюк, успішне використання соціальних мереж у правоохоронній діяльності передбачає насамперед розуміння механізму функціонування таких платформ для комунікації, кожна з яких має свій набір опцій та задач, які вона покликана вирішувати [1, с. 57]. Водночас інші науковці слушно зауважують, що аналіз профілей соціальних інтернет-мереж не тільки дозволяє виявити коло друзів, інтереси і вподобання, місцезнаходження досліджуваної особи, перелік запланованих для відвідування заходів, а й скласти соціально-психологічну характеристику особи користувача [6, с. 53].

Соціальні інтернет-мережі є цінним джерелом криміналістичної інформації, яка може орієнтувати слідчого для прийняття тактичних рішень при розслідуванні кіберзлочинів. Криміналістична інформація у соціальній інтернет-мережі являє собою сукупність даних, повідомлень та відомостей, про джерела й механізм виникнення ідеальних та матеріальних слідів, що мають відношення до злочинної події, отримані в мережі Інтернет із застосуванням спеціальних засобів, з метою встановлення обставин злочинної події у кримінальному провадженні [9, с. 143].

Інформаційно-аналітична робота зі збору інформації про користувачів соціальних мереж дає змогу отримати важливі дані для викриття осіб, які займаються неправомірною діяльністю. Так, аналізуючи найбільш популярні соціальні мережі серед користувачів, можна отримати такі дані: 1) Facebook − ім'я, унікальний код (ID), геолокацію, коло друзів, підписників, пристрій, який використовувала особа, час активності; 2) Twitter − ім'я, назву облікового запису, унікальний код (ID), підписників, місцезнаходження користувача, а також пристрій, з якого були зроблені записи; 3) Instagram − ім'я користувача, назву облікового запису, кількість та імена підписників, верифікаційний статус; 4) YouTube − ім'я користувача, назву каналу, кількість підписників, дату та час викладених матеріалів [3].

Фактично, аналіз наявних підходів дозволяє виокремити три основні напрями використання соціальних мереж під час розслідування кримінальних правопорушень, які, на нашу думку, можуть повністю бути екстрапольовані й на розслідування державної зради: *по-перше,* отримання відповідної системи установчих даних на особу, яка притягується до кримінальної відповідальності на початковому етапі розслідування кримінального провадження чи попереднього документування злочинної діяльності; *по-друге,* виявлення та вилучення різних типів слідів з метою подальшого формування доказів у межах кримінальних проваджень; *по-третє,* використання таких даних для встановлення місцезнаходження осіб, які причетні до вчинення кримінального правопорушення.

Щодо першого напряму, а саме формування відповідної системи установчих даних щодо особи, яка може бути причетною до вчинення державної зради, то однією з ефективних методологій є використання інформаційного профайлінгу, під яким, на нашу думку, необхідно розуміти сукупність методик оцінювання інформації, що знаходиться у соціальних мережах, інших засобах, які використовуються для обміну чи розміщення інформації, задля діагностики та формування «портрета» особи, яка розміщує такого роду інформацію [4, с. 473].

Моніторинг правоохоронними органами соціальних мереж задля виявлення злочинів, пов'язаних із державною зрадою, передбачає: *по-перше*, перегляд вподобань, поширень та коментарів в групах/спільнотах тощо, які носять дискредитаційний характер щодо України, ворожі пропагандистські заклики тощо; *по-друге*, аналіз інформації, наданої в інформаційних мережах (у тому числі, каналах в Telegram), задля виявлення проявів сепаратизму, поширення інформації, яка не може перебувати у вільному обігу, розповсюдження якої несе загрозу державі, тощо; *по-третє*, впровадження працівників правоохоронних органів або інших осіб, які співпрацюють з правоохоронними органами, до груп та спільнот, які носять дискредитаційний характер щодо України, задля встановлення учасників та визначення характеру розповсюджуваної ними інформації, що несе загрозу українській державності.

Варто зазначити, що дуже часто особи мають профілі в декількох соціальних мережах, при цьому використовують таке саме або схоже ім'я, тому маючи певні вихідні дані (наприклад, логін, ім'я користувача тощо) можна спробувати знайти інші профілі особи; маючи фото, що використовується в акаунті, за допомогою пошуку є можливість знайти схожі фото, що знаходяться в мережі, які приведуть до сторінок в інших соціальних мережах, або

до осіб, які виставляли спільні фото з розшукуваною особою та перебувають в безпосередньому зв'язку з нею. Так, наприклад, дослідницька пошукова мережа «Bellingcat» наголошує на тому, що для аналізу контенту достатньо критичного підходу та ретельного вивчення контексту зображення або посту в поєднанні з такими простими інструментами, як пошук у Google або на інших платформах зворотного пошуку зображень [6, с. 53].

Водночас варто зазначити, що злочин, передбачений статтею 111 КК України, може бути вчинений лише громадянином України, проте, зважаючи на те, що на сьогодні певна частина території України перебуває у тимчасовій окупації країною-агресором, можлива ситуація, коли особа, яка вчиняє протиправне діяння, перебуває на непідконтрольній Україні території, що також можна встановити аналізуючи дані із відповідних соціальних медіа для здійснення заочного кримінального переслідування таких осіб.

Фактично, можна констатувати, що використання методики розвідувальної аналітики, а інформаційного профайлінгу як її складової є однією із моделей оперативного обслуговування кіберпростору з метою: *по-перше,* своєчасного виявлення як окремих осіб так і спільнот, які потенційно можуть вчиняти будь-які правопорушення проти держави з метою оперативного контролю за ними; *по-друге,* вчинення заходів ранньої профілактики щодо таких осіб; *по-третє,* своєчасне припинення їх злочинної діяльності. У контексті цього необхідно наголосити, що оперативний контроль за такими спільнотами та соціальними медіа має важливе значення для виявлення усіх учасників злочинної діяльності як на етапі її попереднього документування, так і безпосередньо у процесі розслідування конкретних кримінальних правопорушень, а також встановлення інфраструктурних елементів такої діяльності, зокрема джерел фінансової підтримки таких груп.

Крім того, зауважимо, що не менш важливим є використання інформаційного профайлінгу після початку кримінального провадження за фактами вчинення державної зради, зважаючи на специфіку відповідних слідчих ситуацій. Так, доволі часто такі кримінальні провадження розпочинаються за фактами розміщення особами у соціальних медіа даних щодо окремих подій та фактів, які не підлягають оприлюдненню згідно положень чинного законодавства в умовах воєнного стану, наприклад, інформації щодо ураження ворогом тих чи інших об'єктів військової чи цивільної інфраструктури, пересування військової техніки та місця дислокації особового складу та техніки, які задіянні чи можуть бути задіянні у бойових діях. Загалом аналіз матеріалів кримінальних проваджень свідчить, щодо можливості виокремлення двох слідчих ситуацій, коли основою початку кримінального провадження є інформація, розміщена у соціальних медіа, або передана із використанням комунікативних інструментів соціальних медіа відповідним особам з метою її подальшого використання проти України: *по-перше,* оперативне документування діяльності конкретної особи, яка містить ознаки складу злочину та подальша реалізація такої інформації у формі початку кримінального провадження; *по-друге,* початок кримінального провадження за фактами одиничних публікацій, зокрема щодо ураження ворогом окремих об'єктів. Необхідно відзначити, що у ідентифікаційні завдання, які вирішуються за допомогою соціальних медіа для таких слідчих ситуацій різнитимуться, зокрема: у *першому випадку* – спрямованість не лише на отримання установчих даних щодо особи, яка поширює відповідну інформацію, а й за можливості даних щодо інших осіб, які можуть бути причетними до злочинної діяльності, наприклад, за допомогою побудови матриці звязків; у *другому випадку* – основним завданням є ідентифікація конкретної особи, встановлення її місцезнаходження та проведення щодо неї необхідної системи процесуальних заходів.

Беручи до уваги все вищезазначене, можна зробити висновок, що використання соціальних мереж під час розслідування кримінальних правопорушень, пов'язаних із державною зрадою, що вчиняються з використанням кіберпростору у соціальних мережах, задля ідентифікації особи злочинця передбачає: *по-перше*, створення сторінок/акаунтів або залучення осіб, які співпрацюють з правоохоронними органами, задля виявлення, збору та фіксації інформації, яка носить дискредитаційний характер та/або несе загрозу державі; *по-друге,* моніторинг найбільш популярних спільнот, які займаються розповсюдженням новин; *по-третє,* вирішення ідентифікаційних завдань у межах початкового етапу розслідування кримінального провадження.

ЛІТЕРАТУРА

1. Дуфенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Напрями реформування кримінальної юстиції в Україні* : матеріали науково-практичного семінару (м. Львів, 22 травня 2020 р.). Львів : Львівський державний університет внутрішніх справ, 2020. С. 56–61. URL : https://www.lvduvs.edu.ua/documents_pdf/ biblioteka/nauk_konf/22_05_2020.pdf
2. Кримінальний кодекс України : Закон України від 05 квітня 2001 р. № 2341-III. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text
3. Лисенко О. В. Використання інформаційних технологій для розшуку осіб, які переховуються від органів досудового розслідування та суду. *Науковий вісник Національного університету ДПС України.* 2014. № 2 (65). С. 194–201.
4. Мурашко А. С. Перспективні напрями використання профайлінгу в Україні. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття : синергія наукових, освітніх та технологічних рішень* : матеріали Міжнародної конференції (м. Одеса, 19 травня 2023 р.). м. Одеса, 2023. С. 472–474. URL : https://dspace.onua.edu.ua/items/f488416f-4fc3-4fcb-8929-a5a04c4f62da
5. Нокаут телебаченню: як соціальні мережі утримують першість в постачанні новин українцям. *Українська правда* : вебсайт. URL : https://www.pravda.com.ua/columns/2023/08/16/7415807/
6. Павлиш Т. Г., Терещенко О. О. Аналіз інформації із соціальних мереж під час розслідування та в ході протидії злочинам. *Українська поліцеїстика: теорія, законодавство, практика.* 2022. № 1 (3). С. 49–56. URL : https://policeyistika.dnuvs.ukr.education/wp-content/uploads/2022/04/pavlish.pdf
7. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора* : сайт. URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
8. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія. Одеса : ТЕС, 2020. 372 с.
9. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми. *Криміналістичні загрози в секторі безпеки: практики ефективного реагування* : матеріали III Харківського міжнародного юридичного форуму (м. Харків, 26 вересня 2019 р.). Харків, 2019. С. 142-146. URL : https://dspace.nlu.edu.ua/bitstream/123456789/17042/1/Shevchuk_142-146.pdf
10. Якими соцмережами користуються українці під час війни: статистика. *SPEKA* : вебсайт. URL : https://speka.media/yakimi-socmerezami-koristuyutsya-ukrayinci-pid-cas-viini-doslidzennya-p22nyp