

DOI <https://doi.org/10.51647/kelm.2022.7.55>

NASZE DOŚWIADCZENIA WE WDROŻENIU INFORMACJI I ANALITYK ZAPEWNIAJĄCYCH DZIAŁALNOŚĆ ORGANÓW POLICJI

Jana Kowalczuk

laureat Naukowego Instytutu Prawa Publicznego (Kijów, Ukraina)

ORCID ID: 0000-0002-3757-6241

yanakovalchuk@ukr.net

Adnotacja. W artykule zbadano doświadczenia USA w zakresie wykorzystania najnowszych technologii we wdrażaniu wsparcia informacyjno-analitycznego działań organów Policji. Autor stwierdza, że wykorzystanie analityki danych i algorytmów w działaniach policji niesie ze sobą wiele potencjalnych korzyści, ale niesie ze sobą także znaczne ryzyko, w tym stronniczość. Należą do nich nieuczciwa dyskryminacja ze względu na chronione cechy, rzeczywiste lub pozorne zniekształcenia procesu decyzyjnego lub wyniki i procesy, które są systematycznie mniej sprawiedliwe dla jednostek w określonej grupie. W konkluzji stwierdzono, że organizacje policyjne mogą wykorzystywać duże zbiory danych i sztuczną inteligencję do zwalczania przestępczości i poprawy bezpieczeństwa. Można je jednak również wykorzystać jako narzędzia wzmacniające pozycję obywateli i ograniczające skutki dyskryminacyjne dla jednostek, grup i społeczeństwa jako całości. W USA do efektywniejszych działań informacyjnych i analitycznych policji wykorzystywane są różne platformy chmur narodowych, np. PredPol i HunchLab, które wykazały całkiem dobre wyniki.

Słowa kluczowe: policja, big data, sztuczna inteligencja, wsparcie informacyjno-analityczne, USA, doświadczenia zagraniczne.

US EXPERIENCE IN IMPLEMENTING INFORMATION AND ANALYTICS ENSURING THE ACTIVITIES OF POLICE BODIES

Yana Kovalchuk

laureate of the Scientific Research Institute of Public Law (Kyiv, Ukraine)

ORCID ID: 0000-0002-3757-6241

yanakovalchuk@ukr.net

Abstract. The article examines the experience of the USA in the use of the latest technologies in the implementation of information and analytical support for the activities of police bodies. The author states that the use of data analytics and algorithms for policing has numerous potential benefits, but also carries significant risks, including bias. These include unfair discrimination on the basis of protected characteristics, real or apparent distortions of the decision-making process, or outcomes and processes that are systematically less fair to individuals in a particular group. It concludes that police organizations can use big data and artificial intelligence to fight crime and improve security. But they can also be used as tools to empower citizens and reduce discriminatory effects on individuals, groups and society as a whole. In the USA, various national cloud platforms are used for more effective information and analytical activities of the police, for example, PredPol and HunchLab, which showed quite good results.

Key words: police, big data, artificial intelligence, information and analytical support, USA, foreign experience.

ДОСВІД США ЩОДО ЗДІЙСНЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ПОЛІЦІЇ

Яна Ковальчук

здобувач

Науково-дослідного інституту публічного права (Київ, Україна)

ORCID ID: 0000-0002-3757-6241

yanakovalchuk@ukr.net

У статті досліджено досвід США щодо використання новітніх технологій при здійсненні інформаційно-аналітичного забезпечення діяльності органів поліції. Автором констатовано, що використання аналітики даних і алгоритмів для поліцейської діяльності має численні потенційні переваги, але також несе в собі значні ризики, включно з упередженістю. Йдеться зокрема про несправедливу дискримінацію на підставі захищених характеристик, реальне чи очевидне спотворення процесу прийняття рішень або результати та процеси, які систематично є менш справедливими щодо окремих осіб у певній групі. Зроблено висновок, що поліцейські організації можуть використовувати великі дані та штучний інтелект для боротьби зі злочинністю та підвищення безпеки. Але вони також можуть бути використані як інструменти для розширення можливостей громадян і зменшення дискримінаційного впливу на окремих осіб, групи та суспільство в цілому. В США використовують різні національні хмарні платформи для більш ефективної інформаційно-аналітичної діяльності поліції, наприклад, PredPol і HunchLab, які показали доволі непогані результати.

Ключові слова: поліція, великі дані, штучний інтелект, інформаційно-аналітичне забезпечення, США, зарубіжний досвід.

Вступ. Використання аналітики даних і алгоритмів для поліцейської діяльності має численні потенційні переваги, але також несе в собі значні ризики, включно з упередженістю. Йдеться зокрема про несправедливу дискримінацію на підставі захищених характеристик, реальне чи очевидне спотворення процесу прийняття рішень або результати та процеси, які систематично є менш справедливими щодо окремих осіб у певній групі.

Пристрої та технології, які колись, можливо, використовувалися як засоби для спрощення повсякденного життя, перетворилися на потужні інструменти, які дозволяють правоохоронним органам, в тому числі і поліції, точно визначати їхні ресурси, запобігати злочинам і створювати систему профілактичних заходів. Експоненціальна ескалація мобільних обчислень і аналітики забезпечила працівників поліції «розумними» даними, чим значно підвищила їхні шанси опинитися в потрібному місці в потрібний час.

Хоча ці інструменти мають величезну користь як для підвищення ефективності роботи працівників поліції, так і спільнотам, яким вони служать, є наслідки, які поширюються далеко в публічний простір, а також міркування, які необхідно враховувати, щоб запобігти неправильному використанню «розумних» даних та порушенню громадянських прав. Ці ризики можуть виникати на різних етапах інформаційно-аналітичної діяльності, а тому правова основа для мінімізації їх проявів має бути належно сформованою.

Тому в останні десятиліття в рамках різноманітних ініціатив, які діють на національних рівнях, були розроблені відповідні додатки у сфері контролю за великими даними. Зокрема контроль великих даних використовується наднаціональними організаціями, такими як Європол і Євроюст. Наприклад, Європол створив інформаційну систему, яка містить дані поліцейських організацій Європейського Союзу у (European Union Agency for Criminal Justice Cooperation, 2022). Контроль за великими даними також розвивається завдяки співпраці між національними урядами на міжнародному рівні. Сучасним прикладом є система Prüm, пан'європейська мережа, створена для автоматизованого обміну відбитками пальців, профілями ДНК та інформацією про автомобілі (Neiva, Granja, Machado, 2022). Іншим прикладом є Егмонтська група (Connecting Financial Intelligence Units Worldwide, 2022) підрозділів фінансової розвідки (FIUs), міжнародна ініціатива, яка сприяє співпраці та обміну розвідувальною інформацією між різними національними підрозділами. У брифінгу «Egmont Group» вказується, що вона бере участь у «включенні різних цифрових інструментів для підтримки своїх операційних зусиль». Ці інструменти варіюються від автоматизації до використання великих наборів даних, великих даних і розширеної аналітики, такої як штучний інтелект (AI) і машинне навчання» (Digital Transformation of Aml/Cft for Operational Agencies, 2022).

Причому великі дані та штучний інтелект також є важливими напрямками Стратегії безпеки Європейського Союзу (2020–2025). Європейський Союз стверджує, що: «штучний інтелект, космічні можливості, великі дані та високопродуктивні обчислення інтегровані в політику безпеки таким чином, що є ефективним як у боротьбі зі злочинністю, так і в забезпеченні основних прав» (Communication from the commission on the eu security union strategy, 2020). При цьому вказується на ризики, пов'язані з тероризмом, організованою злочинністю, торгівлею наркотиками, торгівлею людьми та кіберзлочинністю, серед іншого.

Між тим, охорона великих даних не є винятковою прерогативою поліції чи інших спеціалізованих органів, що працюють у сфері громадської безпеки. Швидке зростання та зростання популярності контролю за великими даними частково пояснюється тим, що приватні компанії розвивають все більше цифрових видів діяльності, щоб зробити суспільство безпечнішим. Багато приватних компаній, від «Amazon» і «Google» до «Tesla», застосовують контроль за великими даними, щоб підвищити громадську безпеку, і вони пов'язані меншою кількістю правил, ніж ті, що встановлені для державних органів. Часто їхні продукти призначені для класичних цілей стеження, таких як відповідність вимогам і запобігання злочинам. Однак приватні актори також можуть використовувати контроль за великими даними для інших цілей, починаючи від перевірки особи до отримання прибутку та отримання стратегічних переваг (Marx, 2016). Комерційні постачальники додають програми для обробки великих даних до пристроїв автоматизації «розумного дому» (Sadowski, Strengers, Kennedy, 2021) і приватних автомобілів (Cooke, 2021), щоб сигналізувати про підозрілі випадки в цих об'єктах і навколо них. Яскравим прикладом цього є захисний режим «Sentry» в електромобілях виробництва «Tesla». Цей режим відстежує та записує як поведінку водія за кермом, так і оточення автомобіля на предмет підозрілих рухів, наприклад, щоб зафіксувати потенційних викрадачів (Eski, Schuilenburg, 2022).

Отже, з метою виокремлення шляхів розвитку законодавства та ефективних практик у сфері інформаційно-аналітичного забезпечення діяльності органів поліції України, актуальним є компаративістичний аналіз такого досвіду провідних країн світу, основоположною з яких є США.

Виклад основного матеріалу. Оскільки Сполучені Штати стикаються зі зростанням рівня насильницької злочинності, уряд країни та відповідні правоохоронні органи постійно у пошуках різних інструментів для кращого прогнозування вчинення майбутніх злочинів та їх недопущення. Так, наприклад, група вчених Чиказького університету оприлюднила алгоритм, похвалившись у прес-релізі своєю здатністю передбачати злочини з «90% точністю» (Wood, 2022). Інструмент було протестовано та підтверджено з використанням історичних даних міста Чикаго щодо двох найпоширеніших груп злочинів: насильницькі злочини (вбивства,

напади та побиття) та майнові злочини (крадіжки зі зломом, крадіжки та викрадення автомобілів) (Wood, 2022). Однак, у 2020 році програму було скасовано через критику правозахисних організацій щодо того, що якщо уряд збирається передати процес прийняття рішень комп'ютеру, то як громадськість має перевірити відповідні рішення, їх ефективність та справедливість (Dunke, Main, 17). Але це не єдиний інструмент, який використовує уряд США для інформаційно-аналітичного забезпечення діяльності поліції. Вказаний приклад лише демонструє активність громадськості щодо питань вирішення такого забезпечення.

За останні 15 років найбільші поліцейські департаменти США, такі як Нью-Йорк, Лос-Анджелес і Чикаго, почали використовувати штучний інтелект, щоб не просто аналізувати злочини, а й прогнозувати їх. Для цього вони зверталися до компаній з аналізу даних, таких як PredPol (Pearsall, 2009) і Palantir (Palantir, 2024), які створюють програмне забезпечення (Verma, 2022).

Інструменти PredPol (перекладається як прогнозована або інтелектуальна поліція) побудовані шляхом передачі даних – таких як звіти про злочини, записи про арешти та зображення номерних знаків – до алгоритму, який навчений шукати закономірності, щоб передбачити, де і коли певний тип злочину станеться в майбутньому (Eidam, 2016). Зазначені інструменти роблять більше, ніж просто вказують поліцейським у правильному напрямку; це також усуває можливість упереджень на основі раси та доходу, які часто викликають занепокоєння в поліції та громадськості. Платформа прогнозування не бачить раси, фінансового стану чи будь-яких інших показників, які часто призводять до сприйняття поліцейського профілювання. Усе, що бачить PredPol, – це звіти про скоєні злочини, які потім переводять у те, де вони ймовірно відбудуться далі (Eidam, 2016).

Інші інструменти, такі як Alteryx (MacIsaac, 2020), надають можливість автоматизованої та прогнозованої аналітики, скорочуючи час, необхідний для створення звітів, а також зменшуючи вірогідність вчинення помилок вручну. Завдяки скороченню часу, необхідного дослідникам і аналітикам для збору даних, їх підготовки та опрацювання, дослідники можуть витратити більше часу на аналіз ресурсів, які використовуються недостатньо або надмірно, і вживати заходів, які скорочують час реагування, підвищують безпеку офіцерів і покращують громадську безпеку у (Atkinson, Vuas, 2022).

Останніми роками поштовх до включення альтернативних методів ідентифікації в щоденну роботу поліції у порівнянні з відбитками пальців і класичною фотографією набув не аби якої популярності. Програма ідентифікації наступного покоління Федерального Бюро Розслідувань надала нові інструменти ідентифікації осіб, як для федеральних, так і для державних та місцевих правоохоронних органів. Це в свою чергу, провокує критиків, які вірять, що ця система – це не більше ніж спосіб каталогізації людей – винних, невинних і тих, хто десь посередині. Але на думку експертів програма здається наступним логічним кроком у національному процесі, де відбитки пальців і фотографії не завжди розповідають всю історію кримінального минулого людини (Eidam, 2016). Однак, попри критику з боку правозахисних організацій США, правоохоронні органи загалом, у тому числі і органи поліції впроваджують ці системи у свою діяльність.

Наприклад, у Сан-Дієго міське управління поліції (SDPD) використовує обладнання для розпізнавання обличчя, щоб ідентифікувати людей, з якими контактують його офіцери. Зокрема, якщо особа не показує посвідчення під час зупинки, розпізнавання обличчя може закрити інформаційну прогалину для офіцера (Automated Regional Justice Information System, 2022).

Поширеною є ситуація, коли поліцейські звертаються до особи через підозру у вчиненні правопорушення, яке може варіюватися від незначного, наприклад, викидання сміття чи вигул собаки у забороненому місці, до більш серйозного, як-от побиття чи крадіжка. Якщо особа не має документів або відмовляється називати своє ім'я, поліцейські можуть скористатися спеціальним пристроєм для підтвердження її особи та оформлення протоколу безпосередньо на місці, уникаючи необхідності транспортування до відділку для зняття відбитків пальців. Водночас ці технології мають значно ширше застосування: їх також використовують для взаємодії з бездомними чи встановлення особи людей, які можуть перебувати у розшуку або бути зниклими безвісти (Eidam, 2016).

Ще один інструмент, який використовується для більш ефективного інформаційно-аналітичного забезпечення діяльності поліцейських щодо забезпечення громадської безпеки та порядку – це поліцейське відео. Це почалося як використання матеріалів з приватних камер відео спостереження і переросло в камери, встановлені, здавалося б, на кожному перехресті вулиць. Також за останні кілька років правоохоронні органи по всій території США оснащують офіцерів натільними камерами для документування взаємодії з громадянами.

Поширеність поліцейського відео та його переваги для суспільства є причиною того, що дослідники з Університету Пердью працюють над CAM2 (Lu, 21), хмарною платформою, яка об'єднує загальнодоступні камери через єдиний легкодоступний портал. Масштабована відеоплатформа дозволяє користувачам входити в систему та переглядати безліч загальнодоступних камер, зібраних з усього світу, які можна переглядати в режимі реального часу або згодом. Щодо регулювання такої діяльності, то існує серія нормативно-правових актів, в тому числі Закон США про конфіденційність 1974 року з поправками (Privacy Act 1974),

які регулюють питання використання системи розпізнавання облич. Наприклад, питання щодо порушення конфіденційності вирішено наступним чином: якщо вся інформація, яку люди розміщують у соціальних мережах, стає загальнодоступною, якщо в них не ввімкнено налаштування конфіденційності, – порушення конфіденційності немає (The Office of the Deputy Assistant Secretary for Privacy, 2020). Отже, питання конфіденційності та громадянської свободи критично пов'язані з прогностичною поліцейською діяльністю, і їх необхідно вирішувати шляхом створення чітких правових рамок для використання таких технологій.

Висновки. Поява великих даних і алгоритмів суттєво змінила поліцейську діяльність і, відповідно, поліцейські операції. Зрештою, великі дані та алгоритми є онтогенетичними та трансформаційними за своєю природою, у тому сенсі, що вони вносять зміни в робочі процеси, а це означає, що технологічні можливості, які пропонують великі дані, також впливатимуть на організацію поліції та її працівників. Їх не можна вважати суто технологічним явищем, оскільки їх застосування також має соціальні та культурні наслідки для поліцейських організацій. Як і будь-який інший інструмент, великі дані та алгоритми можуть мати як позитивний, так і негативний ефект залежно від того, як вони використовуються. Поліцейські організації можуть використовувати їх для боротьби зі злочинністю та підвищення безпеки. Але вони також можуть бути використані як інструменти для розширення можливостей громадян і зменшення дискримінаційного впливу на окремих осіб, групи та суспільство в цілому.

В США використовують різні національні хмарні платформи для більш ефективної інформаційно-аналітичної діяльності поліції, наприклад, PredPol і HunchLab, які показали доволі непогані результати.

Однак, розгортання програм великих даних призводить до значних змін у навичках і посадах у поліцейській організації. Зокрема є посади та групи програмістів, спеціалістів із обробки даних, розробників хмарних технологій, спеціалістів з тестування та розробників серверних програм. Це логічно, адже робота з великими даними та алгоритмами вимагає інших навичок і знань, ніж ті, які були потрібні для систем аналізу ризику та статистичних систем, які використовувалися поліцією до стрімкого розвитку інформаційно-аналітичних технологій. Тому Україна має врахувати цей досвід і вже починати проводити навчання фахівців щодо роботи з великими даними та проведенням аналітичних досліджень.

Для ефективного використання сучасних інформаційно-аналітичних технологій у діяльності поліції необхідно, в першу чергу, фінансове забезпечення, що для України сьогодні є найбільш болючим питанням.

Література:

1. Automated Regional Justice Information System. San Diego Association of Governments, 2022. <https://www.sandag.org/data-and-research/criminal-justice-and-public-safety/automated-regional-justice-information-system>
2. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy. COM/2020/605 final. European Union, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605>
3. Connecting Financial Intelligence Units Worldwide. The Egmont Group, 2022. <https://egmontgroup.org/>
4. Cooke, P. (2021). Three Disruptive Models of New Spatial Planning: “Attention”, “Surveillance” or “Sustainable” Capitalisms? *Journal of Open Innovation: Technology, Market, and Complexity*. 7(46): 46–20.
5. Digital Transformation of Aml/Cft for Operational Agencies. The Egmont Group, 2022. <https://egmontgroup.org/wp-content/uploads/2022/01/Digital-Transformation-executive-summary.pdf>
6. Dumke, Mick and Frank Main. A look inside the watch list Chicago police fought to keep secret. Chicago Sun-Times Media, Inc., 2017. <https://chicago.suntimes.com/2017/5/18/18386116/a-look-inside-the-watch-list-chicago-police-fought-to-keep-secret>
7. Eidam, Eyragon. The Role of Data Analytics in Predictive Policing. e.Republic LLC., 2016. <https://www.govtech.com/data/role-of-data-analytics-in-predictive-policing.html>
8. Eski, Y. and Schuilenburg, M. (2022). On Tesla: Balancing Sustainable Car Connectivity, Silent Lethality and Luxury Surveillance. *Criminological Encounters*. 5(1): 234–251.
9. Get AI Into Operations. Palantir, 2022. <https://www.palantir.com/>
10. Laura Neiva, Rafaela Granjaa, Helena Machado. Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union. *International Journal of Research and Policy*, 2022. Volume 32, Issue 10. <https://doi.org/10.1080/10439463.2022.2029433>
11. Lu, Yung-Hsiang. Continuous Analysis of Many CAMeras. Purdue University, 2021. <https://engineering.purdue.edu/VIP/teams/cam2>
12. MacIsaac, Andy. Empowering Investigation Analysis With Predictive Geospatial and Text Mining Analytics. Alteryx, 2020. <https://www.alteryx.com/blog/empowering-investigation-analysis-with-predictive-geospatial-and-text-mining-analytics>
13. Marx, G. (2016). *Windows into the Soul, Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.
14. Pearsall, Beth. Predictive Policing: The Future of Law Enforcement? NIJ Web site, 2009. <https://www.ojp.gov/pdffiles1/nij/230414.pdf>
15. Privacy Act 1974. U.S. Department of the Treasury. [https://home.treasury.gov/footer/privacy-act#:~:text=The%20Privacy%20Act%20grants%20individuals,of%20Information%20Act%20\(FOIA\).](https://home.treasury.gov/footer/privacy-act#:~:text=The%20Privacy%20Act%20grants%20individuals,of%20Information%20Act%20(FOIA).)

16. Sadowski, J., Strengers, Y., and Kennedy, J. (2021). More Work for Big Mother: Revaluing Care and Control in Smart Homes. *Economy and Space* Volume 56, Issue 1: 1–16. doi:10.1177/0308518X211022366.
17. The Office of the Deputy Assistant Secretary for Privacy, Transparency, & Records. U. S. Department of the Treasury, 2020. <https://home.treasury.gov/system/files/236/Privacy-Act-Handbook-Final.pdf>
18. Verma, Pranshu. The never-ending quest to predict crime using AI. *The Washington Post*, 2022. <https://www.washingtonpost.com/technology/2022/07/15/predictive-policing-algorithms-fail/>
19. What we do. European Union Agency for Criminal Justice Cooperation, 2022. <https://www.eurojust.europa.eu/about-us/what-we-do>
20. Wood, Matt. Algorithm predicts crime a week in advance, but reveals bias in police response. *The University of Chicago*, 2022. <https://biologicalsciences.uchicago.edu/news/algorithm-predicts-crime-police-bias>