УДК 351.741'06

О.Є. Користін,
доктор юридичних наук, професор,
заступник директора ДНДІ МВС України, м. Київ,
ORCID ID 0000-0001-9056-5475
Ю.Р. Кардашевський,
аспірант Львівського державного університету
внутрішніх справ, м. Львів,

МОЖЛИВОСТІ ТА ЗАГРОЗИ ЕФЕКТИВНОСТІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ В ЦИФРОВУ ЕПОХУ

У статті зосереджено увагу на епохальних змінах сучасного суспільства та об'єктивній необхідності змін у правоохоронній діяльності. Наголошено на необхідності застосування більш інтелектуальних правоохоронних практик, визначення межі доступу до інформації, необхідності поглиблення дослідницької складової щодо кримінологічного прогнозування та додаткового правового врегулювання правоохоронної діяльності в контексті використання соціальних мереж.

***Ключові слова**: правоохоронна діяльність, інтелектуальні правоохоронні практики, big data, соціальні мережі, кримінологічне прогнозування, прогнозна правоохоронна діяльність, аналітична розвідувальна діяльність.*

В статье сосредоточено внимание на эпохальных изменениях современного общества и объективной необходимости изменения правоохранительной деятельности. Указано на необходимость использования более интеллектуальных правоохранительных практик, определение границ доступа к информации, необходимость углубления исследовательской составляющей криминологического прогнозирования и дополнительного правового урегулирования правоохранительной деятельности в контексте использования социальных сетей.

***Ключевые слова:** правоохранительная деятельность, интеллектуальные правоохранительные практики, big data, социальные сети, криминологическое прогнозирование, прогнозная правоохранительная деятельность, аналитическая разведывательная деятельность.*

Розвиток сучасного суспільства в епоху цифрових технологій безпосередньо залежить від виробництва не матеріальних благ, а знань та інформації. Суспільство наразилося на вибухове зростання інформації про навколишнє середовище, взаємодію людей, предметів та систем. Якщо, наприклад, у 2009 році потоки інформації оцінювалися в обсягах близько 800 петабайт (10^{15}), то вже до 2020 року така оцінка очікувано складатиметься на рівні 40 зеттабайт (10^{21}) [1].

У 2014 році, за підрахунками IBM, глобального й одного з найгучніших брендів у галузі обчислень, 90 % світових даних було створено упродовж останніх двох років, і 80 % з них становили неструктуровані дані [2]. Структуровані дані – це дані, що зберігаються у фіксованих полях у файлах. Неструктуровані дані включають зображення, аудіо-, відеофайли, електронні листи та дані від усіх типів моніторингових пристроїв. У контексті правоохоронної діяльності можливим є вміст свідчень або офіційних записів доказів тощо. Користувачі соцмереж генерують понад екзабайт даних щодня. Швидкість генерації даних зростає експоненціально, але це не просто обсяг доступних даних, це ще повністю не оцінені можливості за умови ефективного використання правильно обраних інструментів. Використовуючи аналітичну розвідку,

можливим є перетворення масиву великих даних на значущу інформацію, що містить певні знання для правоохоронних органів.

Сучасне суспільство перебуває на початку розвитку нової епохи – цифрових, Інтернет і розумних (когнітивних) систем. Навколишнє середовище змінюється, і правоохоронні органи мають можливість використовувати дані більш інтелектуальними способами. Поряд з цим, постає проблема визначення меж доступу до інформації, особливо індивідуальної. Стурбованість суспільства може бути спровокована використанням правоохоронними органами технологій оброблення "великих даних" (*big data*) з причин, які виходять за межі фінансових або інших особистих витрат. Поліцейська легітимація постійно перебуває в русі, зростає та зменшується, виходячи або з успішної діяльності правоохоронних органів, або із засудження помилок та прорахунків. Використання такого масиву даних породжує значні етичні проблеми, і це, своєю чергою, може поставити під загрозу традиційні свободи. Поява *big data*, управління даними, кримінологічного прогнозування – це значний прогрес у протидії злочинності, де активно застосовується аналіз соціальних мереж (SOCMINT – *social media intelligence*). Їх використання є бажаним і не лише через розвідувальні можливості, але також через те, що це може призвести до певного зменшення використання потенційно більш нав'язливих методів кримінальної розвідки.

Розуміння того, що правоохоронні органи можуть використовувати величезні масиви даних та зосереджувати свою увагу на розвідувально-аналітичній роботі з ними, виділяючи тим самим розвідувально-значущу інформацію у формуванні знань про злочини (злочинність), є привабливою можливістю і, перш за все, для керівництва цих правоохоронних органів, але лише настільки, наскільки є можливим покладатися на ці дані. Результати аналітичної розвідувальної роботи оцінюються та багато в чому залежать від походження та надійності інформаційних джерел. Можливість знаходити цінність у даних, що раніше не використовувалися, або об'єднати дані з різних баз даних та джерел, а також представити їх у способах, що дозволяють з'ясувати нову поведінку є достатньою перевагою правоохоронних органів, проте походження великих даних є надзвичайно важливою проблемою.

У зазначеному контексті запровадження IBM у системах моделювання з величезними масивами даних критерію "достовірності" є лакмусовим папірцем для правоохоронних органів. Дослідження IBM засвідчили, що низька якість даних вартувала для економіки США в 2013 році понад 3 трлн доларів США [3]. Точність у зазначеному контексті стосується не лише даних, які є неповними або неточними, а й непевними даними; деякі дані за своєю сутністю є непередбачуваними. Правоохоронні органи з належною обережністю повинні здійснювати екстраполяцію змісту даних та запроваджувати системи оцінювання надійності та достовірності. А обсяг даних є величезним. У 2010 році Бібліотека Конгресу США вирішила архівувати кожен публічний твіт у Twitter; до січня 2013 року архів містив близько 170 млрд твітів [4]. За одну секунду надсилається близько 2,5 млн електронних листів (з яких 67 % – спам); близько 50 тис. пошуків Google; транслюється 9600 твітів; понад 40 тис. повідомлень Facebook [5, с. 109]. Таким чином, правоохоронним органам для сприйняття настільки величезного масиву інформації необхідно формувати власну IT-інфраструктуру, виділяти кошти й формувати відносини з надійними партнерами, зокрема, відносини з IT-компаніями.

Аналіз Twitter-трафіку є цікавим прикладом проблем, з якими зустрічаються аналітики, у розумінні того, які дані належать до великих даних. У серпні 2014 року компанія Twitter у звіті Комісії з цінних паперів та бірж США повідомила, що приблизно 8,5 % або 23 мільйони з 271 мільйона активних користувачів були насправді автоматизованими обліковими записами ("hots"), запрограмованими для трансляції твітів у визначений час або реагування на конкретні події; ще 5 % його

трафіку було спамом [5, с. 110]. Мотті підкреслював, що хоча деякі облікові записи є нешкідливими, вони можуть ввести в оману тих, хто намагатиметься осягнути весь масив даних. Більше того, спам продукує більше шуму в системі та є малозначним для будь-якого користувача [5, с. 110].

Наразі недостатність інформації не може бути принциповою перешкодою для належної юридичної кваліфікації. Річардс Ейєр стверджував, що за певних обставин додаткова інформація дійсно може сприяти більш точному аналізу, але вона не завжди існує; за інших обставин додаткова інформація може бути надзвичайно суперечливою та формувати хибну думку, а не поглиблювати знання. Провівши психологічне дослідження, він дійшов висновку, що знання та припущення аналітиків є найбільш важливими та взаємопов'язаними, а не сума знань, яку вони зібрали [6, с. 58].

Подібним чином Кірк формує запитання щодо можливості оброблення належним чином інформації для прийняття об'єктивних управлінських рішень з найкращим вибором, зважаючи на майже нескінченну кількість даних, яка стає дедалі більш доступною для аналітиків та дослідників [7, с. 84]. Він стверджує, що в сучасну епоху не може бути задоволений апетит на отримання дедалі більшого масиву інформації й що надмірною є витрата енергії організацією на підтвердження того, що вже відомо. Кірк стверджує, зокрема, що: ..."прагнення до інформації – це перевага, яка створює параліч у прийнятті рішення ...пригнічує як творче, так і критичне мислення, оскільки створює надмірну залежність від аналізу фактів та даних, а не продукування нових або рефлексивних ідей" [7, с. 85].

Таким чином, можемо зробити висновок, що співвідношення між обсягами даних та знаннями, які можуть бути виведені з них, не є лінійними.

Наразі існує очевидний симбіоз *big data* та покладанням великої надії держави на зменшення злочинності, а саме прогнозної правоохоронної діяльності, визначеної як "методологія, яка використовується правоохоронними органами для аналізу даних щодо минулих злочинів для прогнозування знань у майбутньому щодо злочинності та її вразливості" [5, с. 112].

Наразі існує надзвичайно багато досліджень щодо прогнозної правоохоронної діяльності, які заслуговують на увагу й можуть застосовуватися вченими та практиками. Поряд з цим, не визначено чітких переваг у зазначеному контексті правоохоронної діяльності. Висновки цих досліджень були неоднозначними, недостатньо було доказів для визначення того, що прогнозні моделі реально описують злочинність майбутнього. Та чи потрібно було формулювати таким чином завдання?

Проте позитивним здобутком стало те, що реальним було сприйняття переваги такої ініціативи; результатом було більш ефективне використання ресурсів; а в деяких випадках це покращило зв'язки з громадськістю [8].

Прикметно, що дослідники дійшли висновку про існування чотирьох категорій методів прогнозної правоохоронної діяльності, а саме:

• методи прогнозування злочинів: ...підходи, що використовуються для прогнозування місць і часу з підвищеним ризиком вчинення злочинів;

• методи прогнозування правопорушників: ...визначення осіб, котрі здатні на вчинення злочинів, ризиків ймовірності цього в майбутньому;

• методи прогнозування ідентичностей правопорушників: ...використовується для створення профілів, що збігаються з конкретним злочинним минулим можливого правопорушника;

• методи прогнозування жертв злочину: ...використовується для визначення груп або, у деяких випадках, осіб, які можуть стати жертвами злочину [9].

З-поміж іншого, важливим висновком щодо ефективності прогнозної правоохоронної діяльності була необхідність забезпечення синергії між аналітичними та дослідницькими зусиллями. Дослідники виявили, що успіх прогнозування, як правило, був зумовлений підтримкою на вищому рівні, достаіостю ресурсів, автоматизованих систем з наданою необхідною інформацією, а також призначеним персоналом, із

урахуванням як свободи рішень щодо аналізу проблем злочинності, так і відповідальністю за це [9]. Поряд з цим, прогнозування є лише половиною роботи; інша половина фактично залежна від безпосередньої операційної роботи. Неприпустимим є збільшення розриву між інтелектуальним та операційним світами, необхідним є заохочення їх синергії. Крім цього, неприпустимим є завищення очікувань від результатів прогнозування. Цими ж дослідженнями було доведено, що для визначення реальної цінності прогнозної правоохоронної діяльності необхідним є забезпечення достатньої незалежності таких дослідження [5, с. 113]. Подальші дослідження повинні включати фундаментальні питання про необхідність та відповідність технологій й методології, що нині використовуються, і про те, якою мірою кримінальне середовище, а не суб'єкти в ньому повинні бути предметом такого детального дослідження.

Продовжуючи розгляд проблематики визначеного предмета дослідження, зазначимо, що швидке розповсюдження соціальних мереж як засобів масової інформації створює низку можливостей і викликів державним інституціям, а також загроз в контексті правоохоронної діяльності.

Незважаючи на те, що багато веб-сайтів дозволяють користуватися певною мірою користувальницькими параметрами, вони не входять до більшості визначень соціальних мереж. Натомість соціальні медіа можна розділити на чотири категорії – соціальні мережі, сайти обміну контентом, інструменти для розміщення контенту та інструменти географічних розташувань, кожен з яких має свої особливі характеристики, і тому кожен з них становить різні загрози та можливості.

Існує низка викликів для розслідування правопорушень, скоюваних через ці засоби масової інформації, і це пов'язано, перш за все, із практикою та законодавством (або за деяких обставин відсутністю законодавчих норм). З точки зору практики, Інтернет не знає фізичних меж, тому існують очевидні виклики у випадках, коли правопорушник перебуває поза межами країни. Злочини, які зазвичай трапляються в соціальних мережах, як правило, переслідуються національними кримінальними законами. Проте в рамках керівних принципів існує очевидна спроба збалансувати це із правом на свободу вираження поглядів (право, захищене загальним правом та статтею 10 ЄСПЛ).

Водночас соціальні медіа використовуються правоохоронними органами як новий спосіб спілкування з громадськістю. Майже кожен суб'єкт має корпоративні облікові записи Facebook і Twitter, а ті самі засоби масової інформації широко використовуються для офіційних цілей різними співробітниками. Вони пропонують потенціал для більш активної взаємодії з різними демографічними групами та традиційно важкими для досягнення групами [5, с. 114]. Вони також можуть допомогти окремим особам краще зрозуміти соціальні проблеми й дозволити їм більш ефективно реагувати на проблеми співтовариства, однак дослідження показали, що соціальні медіа не можуть бути просто пов'язані з існуючими комунікаційними механізмами. У них є "своя логіка, норми та культура", які правоохоронні органи повинні розуміти і поважати, якщо вони хочуть максимально збільшити свій потенціал [10, с. 7]. Так само слід розуміти, що є узгодженість. Наприклад, принцип Парето, здається, застосовується до використання соціальних мереж так само, як і до проблеми злочинності.

Користувачі вільно діляться багатьма деталями свого життя в Інтернеті. Сер Девід Оман був одним із трьох дослідників, який створив термін SOCMINT як лейбл для дивідендів аналітичної розвідки з використання соціальних мереж [11, с. 2]. Вони стверджують, що SOCMINT пропонує можливості покращити громадську безпеку шляхом створення краєзнавчої інформації, нових можливостей для дослідження та розуміння, поінформованості про ситуацію в реальному часі (справжню безпеку в правоохоронній практиці), краще розуміння груп та кращого прогнозування кримінальних подій. Однак дослідники визнають, що суспільна прийнятність використання SOCMINT правоохоронними органами та розуміння громадянами його

пропорційності й необхідності є настільки ж важливими, як і для будь-якої форми збору інформації [11, с. 3].

Безумовно, правозастосування щодо використання соціальних засобів масової інформації як інструменту розслідування в умовах законодавчого вакууму вимагає традиційних концепцій легітимності та відповідності правоохоронної діяльності.

Таким чином, *big data* неминуче впливатиме на правоохоронну діяльність, зокрема на аналітичну розвідувальну практику, так само, як і на будь-який інший аспект соціального світу. Побутує думка, що розвинені країни, за наявності ресурсів, здійснюють масовий відбір даних для забезпечення національної безпеки з усього того, що межує чи співвідноситься із правами громадян. Поряд з тим, немає достатніх підтверджень того, що поліцейські системи зробили те ж саме, хоча чітко йдеться про прагнення використовувати актуальні інструменти та методи обробки даних, задля верифікації інформації в масиві безглуздих даних. Поряд з цим дещо завищеними видаються запити щодо результатів правоохоронної прогнозної діяльності, розвиток якої передовсім потребує набагато більшої кількості досліджень щодо застосовуваних методів. І, наостанок, можна стверджувати, що соціальні медіа дають правоохоронним органам набагато більше можливостей щодо протидії злочинності, ніж загрози, що потребує, у свою чергу, урегулювання правоохоронної діяльності в цьому контексті через конфіденційність особи та достовірність слідства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Корыстин А.Е.* Интеллектуализация правоохранительной деятельности. Public Administration: Theory and Practice. 2017. № 3 (59). С. 127–132.

2. *Dennis M.* (2014) Figuring out the questions to be answered simplifies the search for information within unstructured data. IBM Systems Magazine. 2014. *URL:* www.ibmsystemsmag.com/mainframe/trends/Modernization/unstructured_data

3. IBM (2013) The four Vs of big data. 2013. URL: www.ibmbigdatahub.com/infographic/four-vs-big-data (дата звернення: 12.03.2018).

4. *Joh E.E.* Policing by Numbers: Big Data and the Fourth Amendment.Washington Law Review. 2014. № 89. P. 185–204.

5. *James A.* Understanding Police Intelligence Work. Policy Press: University of Bristol. 2016. P. 172.

6. *Heuer R.* The Psychology of Intelligence Analysis. Washington DC: Central Intelligence Agency. 1999.

7. *Kirk C.J.* The demise of decision-making: how information superiority degrades our ability to make decisions. US Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. 2013.

8. *Hunt P., Saunders J., Hollywood J.S.* Evaluation of the Shreveport Predictive Policing Experiment. Santa Monica. CA: Rand Corporation. 2014.

9. *PerryW.L., McInnis B., Price C.C., Smith S.S., Hollywood J.S.* Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Santa Monica, CA: RAND Corporation. 2013.

10. *Davis E.F., Alves A.A., Sklansky D.A.* Social Media and Police Leadership: Lessons from Boston. New Perspectives in Policing Bulletin. Washington, DC: U.S. Department of Justice, National Institute of Justice. 2014.

11. *Omand D., Bartlett D., Miller C.* Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security. 2012. № 27.

REFERENCES

1. *Korystin, A.E.,* 2017, “Intellectualization of Law Enforcement Activity”, Public Administration: Theory and Practice 3 (59), 127–132.

2. *Dennis M.,* 2014, “Figuring out the Questions to be Answered Simplifies the Search for Information in Unstructured Data”, IBM Systems Magazine. URL: www.ibmsystemsmag.com/mainframe/trends/Modernization/unstructured_data.

3. IBM, 2013, “The Four Vs of Big Data”. URL: www.ibmbigdatahub.com/infographic/four-vs-big-data (application date 12.03.2018).

4. *Joh, E.E.,* 2014, “Policing by Numbers: Big Data and the Fourth Amendment”, Washington Washington Review 89, 185–204.

5. *James, A.,* 2016, “Understanding Police Intelligence Work”, Policy Press: University of Bristol, 172 p.

6. *Heuer, R.,* 1999, "The Psychology of Intelligence Analysis", Washington DC: Central Intelligence Agency.

7. *Kirk, C.J.,* 2013, "The Demise of Decision-Making: How Information Superiority Degrades our Ability to make Decisions", US Naval War College faculty in the partial satisfaction of the requirements of the Joint Military Operations Department.

8. *Hunt, P.J., Saunders, J.S.,* 2014, "Hollywood Evaluation of the Shreveport Predictive Policing Experiment. Santa Monica", CA: Rand Corporation.

9. *Perry, W.L., McInnis, B., Price, C.C., Smith, S.S., Hollywood, J.S.,* 2013, "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations", Santa Monica, CA: RAND Corporation.

10. *Davis, E.F., Alves, A.A., Sklansky, D.A.,* 2014, "Social Media and Police Leadership: Lessons from Boston. New Perspectives in Policing Bulletin", Washington, DC: U.S. Department of Justice, National Institute of Justice.

11. *Omand, D., Bartlett, D., Miller, C.,* 2012, "Introducing Social Media Intelligence (SOCMINT)", Intelligence and National Security 27.

UDC 351.741'06

O.Y. Korystin,
Doctor of Law, Professor, Co-Head of Director of the State Research Institute MIA Ukraine, Kyiv,
ORCID ID 0000-0001-9056-5475
Y.R. Kardashevskyi,
Postgraduate, Lviv State University of Internal Affairs, Lviv

OPPORTUNITIES AND THREATS TO THE EFFECTIVENESS OF LAW ENFORCEMENT ACTIVITIES IN THE DIGITAL ERA

Modern society nowadays is at the very beginning of the development of a new era of digital, Internet and intelligent (cognitive) systems. The environment is changing and law enforcement agencies have the ability to use data in more intelligent ways. In addition, there is the problem of determining the limits of an access to information, especially individual. Society's concern can be provoked by the use by law enforcement agencies of the technologies of processing "big data" because of the reasons beyond the financial or other personal expense. Police legitimacy is constantly on the move, growing and decreasing, either on the basis of successful law enforcement or the condemnation of mistakes and miscalculations. Use of such an array of data generates significant ethical issues, and this, in turn, may endanger traditional freedoms. The emergence of Big data, data management, and criminological prediction is a significant advancement in crime prevention, where SOCMINT (social media intelligence) is actively used. Their use is desirable not only because of intelligence capabilities, but also of of its capacity to lead to a certain reduction in the use of potentially more intrusive methods of criminal intelligence.

The study showed that the relationship between the volume of data and the knowledge that can be derived from them is not linear, but there is an obvious symbiosis between Big data and the high expectation of the state on crime reduction, namely, predictive law enforcement defined as "methodology used by law enforcement agencies to analyze data regarding past crimes for prediction of crime knowledge and vulnerability in the future".

It is stated that there are four scientifically substantiated categories of predictive law enforcement activities and the need to ensure synergy between analytical and research efforts.

It is noted that the rapid spread of social networks as media creates a number of opportunities and challenges for state institutions, as well as threats in the context of law enforcement activities. But social media gives law enforcement agencies much more anti-crime opportunities than threats that, in turn, require regulation of law enforcement activities in this context due to the confidentiality of individuals and the credibility of the investigation.

The necessity of applying more intelligent law enforcement practices, definition of the limits of an access to information, as well the need to deepen the research component of the criminological forecasting and additional legal regulation of law enforcement activities in the context of use of social networks is emphasized.

Keywords: law enforcement activity, intellectual law enforcement practices, big data, social networks, criminological forecasting, prospective law enforcement activity, analytical intelligence activities.

Отримано 30.03.2018