УДК 351.741:004(100) DOI: https://doi.org/10.32631/pb.2021.1.11

ЮРІЙ ВАЛЕРІЙОВИЧ ГНУСОВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ;
https://orcid.org/0000-0002-9017-9635,
e-mail: duke6969@i.ua;

ВОЛОДИМИР МИХАЙЛОВИЧ СТРУКОВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ;
https://orcid.org/0000-0003-4722-3159,
e-mail: struk_vm@ukr.net;

ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ МОЖАЄВ,
доктор технічних наук, професор,
Харківський національний університет внутрішніх справ;
https://orcid.org/0000-0002-1412-2696,
e-mail: mozhaev1957@gmail.com

ПРОБЛЕМА УЗГОДЖЕННЯ ПРАВОВИХ НОРМ ІЗ ПОТРЕБАМИ ПОЛІЦЕЙСЬКИХ РОЗСЛІДУВАНЬ З ВИКОРИСТАННЯМ ВИСОКОТЕХНОЛОГІЧНИХ ІНСТРУМЕНТІВ ПОШУКУ ДАНИХ

Проаналізовано проблеми узгодження правових норм із потребами поліцейських розслідувань з використанням високотехнологічних інструментів пошуку даних. Визначено, що шляхи вирішення сформульованої проблеми лежать як у правовій площині, так і в технічній, причому її правовий аспект має дві складові – міжнародну і національну. Проаналізовано досвід світової практики у сфері досліджуваної проблеми. Визначено, що врегулювання будь-якого одного аспекту не означає вирішення проблеми в цілому. Наголошено, що повне вирішення проблеми має комплексний характер і повинно містити низку як нормативно-правових актів на рівні міжнародного і національного права, так і певні заходи технічного характеру, які забезпечують законність процедур збору персоналізованих даних в інтернеті, що застосовуються поліцейськими структурами у найсучасніших інструментальних високотехнологічних аналітичних системах.

Ключові слова: *глобалізація, високі технології, проактивна поліцейська діяльність, інформаційно-аналітичні системи, «слабкі сигнали».*

Оригінальна стаття

Постановка проблеми

Світ стрімко входить в епоху глобалізації на тлі блискавичних змін у сфері високих технологій, що у найближчі 5–7 років докорінно змінять світ. Ці зміни супроводжуються зростаючими масштабами загроз із боку злочинних угруповань, ставлять світову спільноту перед необхідністю розроблення нових підходів до гармонізації століттями напрацьованих демократичних цінностей і потребують адекватної реакції правоохоронних органів на нові виклики з боку вуличної та організованої злочинності й тероризму. Справа в тому, що в контексті стрімкого розвитку найсучасніших технологічних інструментів, які вже стали доступними не лише організованим злочинним угрупованням, а й невеликим вуличним бандам і навіть окремим злочинцям, правоохоронні структури в усьому світі постають перед безумовною необхідністю переходу від реактивної парадигми діяльності до проактивної – від реакції на вже вчинені злочини до попередження і профілактики злочинності. І цей процес останніми роками відбувається у розвинених країнах дуже активно і в різноманітних формах. Яким є ключовий механізм практичної реалізації предикативної парадигми? Теоретично єдиний ефективний і дієвий підхід – це всеохоплююче спостереження за всіма без винятку громадянами. Такий тотальний контроль містить у собі два компоненти – відеоспостереження у режимі 24/7 і контроль фінансових транзакцій громадян і юридичних осіб. Ключовими інструментами реалізації такої діяльності є інформаційно-аналітичні системи нового покоління, які у

своєму складі, як правило, мають модулі сканування кіберпростору у режимі 24/7, побудовані на основі штучного інтелекту. Такі системи в автоматичному режимі сканують кіберпростір з метою збору інформації та її подальшої обробки для виявлення на ранніх етапах підготовки злочинів і терактів. Оскільки правопорушники всіляко маскують свої злочинні наміри, аналітичні модулі таких систем застосовують аналіз так званих «слабких сигналів», тобто інформації, яка прямо не вказує на можливу злочинну активність, але її опрацювання із застосуванням певних математичних моделей і методів надає можливість з певною вірогідністю зробити висновок про можливий злочин, місце і час його вчинення та його суб'єктів. Така інформація обов'язково містить у собі не лише дані про правопорушення і правопорушників, а і персоналізовані дані про законослухняних громадян та організації, які опосередковано сприяють виявленню і попередженню злочинної активності.

Описаний механізм вступає у колізію із національним законодавством демократичних країн, зокрема Євросоюзу та США, а також деякими міжнародними нормативними актами, серед іншого Європейською конвенцією з прав людини. З іншого боку, злочинців не стримують жодні нормативні, бюрократичні, моральні, територіальні та інші обмеження. Ця категорія осіб є абсолютно прагматичною та здатною на швидке ухвалення рішень. Усе це забезпечує правопорушникам перевагу у протистоянні з правоохоронними органами, обмеженими міжнародними і національними нормативно-правовими актами та численними бюрократичними перешкодами.

Отже, суспільство постає перед дуже актуальною проблемою пошуку консенсусу між збереженням традиційних демократичних цінностей, таких як недоторканність приватного життя і приватної власності, з одного боку, й імперативом безпеки життя та здоров'я громадян – з іншого. Це, у свою чергу, порушує питання про законність процедур отримання необхідної інформації про підготовку до вчинення злочинів або терактів із будь-яких джерел, серед іншого відкритих – соціальних мереж, месенджерів, телеграм-каналів тощо [1].

Стан дослідження проблеми

У зарубіжних країнах досліджуване у статті питання вивчали розробники відомої платформи «ePOOLICE», у складі якої функціонує модуль пошуку інформації у відкритих джерелах OsintSM. Велика увага цим питанням була приділена у навчальному посібнику з ILP OSCE [2, с. 24–30]. Крім того, питання внормування пошуку інформації правоохоронними органами неодноразово порушувалося в роботах М. Баззеля, Р. Кларка, К. Козери, В. Мітчела, Дж Ретклiфа, С. Стренга, Н. Хасана, Р. Хейера, Р. Хіджазі та ін. Достатньо глибокий аналіз досліджуваної проблеми виконали О. Ларіна та В. Овчинський. Серед вітчизняних фахівців це питання опрацьовували С. Албул, О. Богінський, О. Бочковий, М. Грібов, Є. Жицький, В. Захаров, К. Ісмайлов, О. Користін, О. Манжай, В. Некрасов, Д. Никифорчук, Ю. Орлов, В. Струков, Д. Узлов, А. Ханькевич, В. Школьніков, працівники профільних департаментів Національної поліції України та багато інших.

Незважаючи на згадані дослідження, слід констатувати, що питання нормативного внормування автоматизованого пошуку, обробки та аналізу інформації правоохоронними органами фахівці вивчили недостатньо. Серед іншого це пояснюється тим, що модулі автоматичного сканування кіберпростору в інтересах правоохоронних органів з'явилися не дуже давно і працюють у небагатьох країнах. Так, система «ePOOLICE», яку оплачує Євросоюз, була запущена в 2013 р., а перша версія відомої платформи Palantir, яка вийшла із надр ЦРУ, з'явилася у 2012 р. У практиці діяльності правоохоронних органів України системи такого типу наразі відсутні. Але їх поява у недалекому майбутньому не має альтернативи, оскільки системи такого типу в сучасних умовах є основним інструментальним засобом ефективної реалізації проактивної діяльності поліції у протистоянні сучасним викликам з боку всіх типів злочинності.

Мета і завдання дослідження

Метою цієї статті є аналіз проблеми узгодження міжнародних і національних нормативних актів з потребами поліцейських розслідувань із використанням сучасних високотехнологічних інструментів пошуку і збору даних. *Завданням* статті є структуризація цієї проблеми й окреслення шляхів її подолання.

Наукова новизна дослідження

Ця робота є однією з перших вітчизняних публікацій щодо міждисциплінарної проблеми взаємовідносин правових норм із законним використанням високотехнологічних інструментів в інтересах поліцейських розслідувань з метою збору й обробки персональних даних. Сформульовано проблему координації

міжнародних і національних нормативних документів у галузі недоторканності приватного життя, приватної власності та персональних даних із сучасними потребами поліцейських розслідувань з використанням високотехнологічних інструментів, які в режимі 24/7 сканують кіберпростір. Виокремлено правовий і технічний аспекти проблеми. Окреслено шляхи подолання сформульованої проблеми.

Виклад основного матеріалу

Одним із факторів, який посилює розглядувану колізію, є те, що останнім часом у зв'язку з усеохоплюючим поширенням смартфонів та інших подібних до них пристроїв лавиноподібно зростає кількість шахрайств, пов'язаних із незаконним заволодінням персональними даними. Цьому сприяють такі обставини: 1) слабкий рівень захищеності користувацьких гаджетів (смартфони, планшети, ноутбуки, нетбуки тощо); 2) низький рівень обізнаності більшості користувачів у сфері інформаційної безпеки; 3) постійно зростаюча кількість кібершахраїв; 4) можливість здійснювати протиправні вчинки дистанційно, що створює ілюзію безкарності; 5) збільшення кількості незаконних брокерів даних, які торгують персональними даними, отриманими незаконним шляхом; 6) нерозвинена вітчизняна нормативна база у сфері протидії кіберзлочинності тощо.

Ці обставини стимулюють розвиток двох діаметрально протилежних процесів: 1) посилення убезпечення персональних даних з використанням правових механізмів; 2) потреба у законному доступі до персональних даних законослухняних громадян та організацій в їхніх же інтересах.

Дуже цікавим є досвід підходу до радикального вирішення досліджуваної проблеми у Китаї, який, як мінімум, заслуговує уважного вивчення і розумного використання у національній правозастосовній сфері. З одного боку, в цій країні останніми роками ухвалено безпрецедентну кількість нормативно-правових актів у сфері захисту персональних даних – понад 200 [2], з іншого, – Китай є світовим лідером у провадженні державної політики тотального контролю за своїми громадянами.

У 2014 р. Уряд КНР опублікував Програму створення системи соціального кредиту (2014–2020)[1]. Згідно з цим документом кожен житель материкового Китаю відстежується та оцінюється цією системою в режимі реального часу. Рейтинг довіри фізичних осіб прив'язано до внутрішнього паспорту. Рейтинги публікуються в централізованій базі даних, яка перебуває у відкритому доступі в мережі Інтернет. Чим нижчим є рейтинг, тим більше уваги приділяють державні органи відповідним особам.

Суть системи полягає у створенні всеосяжного державного моніторингу ділового життя, громадянської активності та життєдіяльності населення, принаймні великих міст, що забезпечує прямі та зворотні зв'язки між завданнями державного будівництва й поведінки окремих громадян, груп населення і господарюючих суб'єктів. По суті, створюється система суцільного скринінгу, яка дозволить у режимі реального часу оцінювати внесок окремого громадянина, поселення або компанії у вирішення державних завдань.

Система передбачає використання потужної розподіленої системи штучного інтелекту, яка обробляє п'ять різнорідних масивів інформації та містить:

1) зведену воєдино і прив'язану до конкретного ідентифікатора громадянина або компанії інформацію, що отримується різними державними органами на всіх рівнях;

2) офіційну інформацію про ділову активність будь-якої китайської компанії або китайського громадянина, включно з їх взаємовідносинами з фінансовими, податковими органами, банківською системою, проведенням ділових транзакцій тощо;

3) дані про інтернет-активність громадян, одержувані від пошукових систем та інших інтернет-ресурсів, що діють на території Китаю;

4) персоналізовану інформацію з листування громадян і компаній по електронній пошті, в соціальних мережах, месенджерах тощо;

5) дані відеоспостереження за поведінкою громадян і їх діловою активністю; відповідно до ухваленої в 2018 р. постанови, в містах Китаю з населенням понад 1 млн мешканців має бути до 2020 р. встановлено більше 30 млн відеокамер, що постійно відстежують дії в приміщеннях і на вулицях міст.

Система вже працює принаймні в тридцяти містах Китаю. Передовим у цій справі є місто Жунчен у провінції Шаньдун. Усім мешканцям міста (670 тис.) дається стартовий рейтинг 1000 балів. Далі залежно від їх поведінки рейтинг або зростає, або знижується. У Жунчені єдиний інформаційний центр аналізує 160 тис. різних параметрів з 142 установ.

[1] Система соціального кредиту // Вікіпедія : віл. енцикл. URL: https://uk.wikipedia.org/wiki/Система_соціального_кредиту (дата звернення: 13.01.2021).

Рейтинг, що становить більше 1050 балів, відповідає зразковому громадянину і маркується трьома літерами А. З тисячею балів можна розраховувати на АА. З 900 балами – на В. Якщо рейтинг впав нижче 849, то особа заноситься до списку підозрілих осіб, яку можуть звільнити зі служби в державних і муніципальних структурах. Із рейтингом 599 балів і нижче записують в чорний список з приписку D. Такі особи стають ізгоями суспільства, їх не беруть майже на жодну роботу, не дають кредити, не продають квитки на швидкісні потяги та літаки, не дають в оренду автомобіль і велосипед без застави.

Для юридичних осіб правила гри сформульовано більш чітко. Компанії перевіряються на відповідність їх діяльності екологічним та юридичним нормам, інспектуються умови і безпека праці й фінансова звітність. Якщо жодних претензій немає – компанії присвоюється високий рейтинг, і вона користується пільговим режимом оподаткування та хорошими умовами кредитування, стосовно неї спрощуються адміністративні процедури за принципом «прийняття неповного комплекту». Це означає, що якщо в разі звернення в якусь інстанцію компанія надала неповний комплект документів, її звернення все одно береться в роботу, а відсутні документи просто можна донести потім або навіть надіслати сканкопії.

Для юридичних осіб з низьким рейтингом надаються дорогі кредити, підвищені ставки податків, забороняються емісія цінних паперів та інвестування в компанії, акції яких виставляються на торги на біржі, а також передбачається необхідність отримувати державний дозвіл на інвестування навіть у ті галузі, доступ до яких у принципі ніяк не обмежується.

Для наступної стадії реалізації проєкту соціального кредиту в Китаї створено технологію розпізнавання обличь, яку застосовують для стеження за учнями старшої школи (в Ханчжоу вона пройшла апробацію). Кожні 30 секунд технологія розпізнавання обличь фіксує обличчя учнів, які перебувають в класних кімнатах старшої школи № 11 в Ханчжоу. Завдання технології – визначити настрій кожного учня. Вона класифікує стан як щасливий, сердитий, наляканий, зніяковілий або засмучений. Крім того, система фіксує дії учнів і розуміє, коли вони пишуть, читають, відповідають викладачеві або сплять під час занять [2].

Така система стеження використовується насамперед для підвищення ефективності навчального процесу, проте вона також допомагає запобігти можливим інцидентам у навчальних закладах. При цьому учням не потрібно носити з собою будь-які посвідчення або картки. Система розпізнавання обличь працює в шкільній їдальні і бібліотеці.

У 2017–2018 рр. основні параметри нової технологічної китайської системи безпеки були опубліковані ЗМІ в різних країнах світу. Китайський проєкт став предметом аналізу й обговорень. Спільна для більшості західних країн позиція полягає в тому, що практична реалізація такого проєкту зробить Китай погіршеним варіантом суспільства, описаного Дж. Оруелом у романі «1984». Але слід зауважити, що системи спостереження за громадянами, що формуються в країнах Заходу, створюють не менше проблем (як про це неодноразово писали розробники системи «ePOOLICE») [2].

І це, на жаль, зумовлено об'єктивними обставинами. Китайські аналітики ще в 1999 р. в фундаментальній праці «Необмежена війна» відзначили, що одним із законів, які діють протягом століть у всьому світі, є нарощування деструктивних можливостей дедалі менших груп. XXI століття наочно підтверджує цю гіпотезу. Сьогодні групи кірберзлочинців або терористів можуть призвести до катастроф, зіставних із застосуванням ядерної зброї. При цьому контроль над кіберзброєю практично неможливий. Відповідно до цього Китай не лише відреагував на цю проблему, але й одним із перших у світі почав шукати шляхи вирішення превентивного попередження можливостей малих груп та одинаків заподіяти непоправну шкоду суспільству.

На відміну від Китаю, в країнах західної Європи і США, де сторіччями формувалися і закріплювалися на законодавчому рівні традиції недоторканності приватного життя і приватної власності, такий підхід викликає у спільноти несприйняття і протидію. Із цим зіткнулися, зокрема, розробники відомої платформи «ePOOLICE» [2; 3]. Але і в демократичному суспільстві обставини спонукають уряди рухатися в напрямку сприяння проактивним діям правоохоронних органів.

Незважаючи на суперечності, які дедалі більше загострюються, в базових документах, що розглядаються міжнародним правом як основоположні документи у сфері національної безпеки, чиї вимоги і принципи мають пріоритет порівняно зі змістом будь-яких інших документів, а саме в доповіді ООН «Про безпеку людини» (2003 р.) і в Європейській Доктрині з безпеки (2004 р.), безпека визначається як «безумовне забезпечення прав,

свобод і недоторканності приватного життя законослухняних громадян за дотримання вимог національної та міжнародної безпеки».

Як зазначають О. Ларіна і В. Овчинський [1], така юридична конструкція в казуїстичному, буквально юридичному сенсі слова ставить індивідуальне право вище не лише групових і державних, а і громадських прав. Однак у Стратегії безпеки ЄС, ухваленій у тому ж 2004 р., підкреслюється «необхідність діяти активно у вирішенні ключових загроз національній безпеці та прав громадян», що в сучасних умовах з урахуванням вищезазначених обставин можна трактувати лише як безумовну необхідність реалізації проактивної парадигми діяльності правоохоронними структурами. Аналіз цих документів свідчить про те, що навіть в Європі, яка має найбільш давні правові традиції, сьогодні двозначно трактуються взаємовідносини між національною і приватної безпекою. У численних документах ООН, ЄС, НАТО й інших міжнародних організацій є ідентичні заголовні пункти, які передбачають «активну позицію держави і міжнародного співтовариства щодо ризиків і загроз, включно з новими непізнаними ризиками і загрозами, пов'язаними з тероризмом, ОЗ, кіберкримінальними угрупованнями, міжнародною мережею тіньового банкінгу, корупції і відмивання грошей» [2].

Проактивна діяльність правоохоронних структур на сучасному рівні передбачає можливість застосовувати передові методи аналізу «великих даних», штучного інтелекту, а також системи збору інформації про поодинокі події, осіб, суб'єктів та об'єктів, не лише залучених у злочинну діяльність або пов'язаних з нею, а й тих, чиї інформаційні файли можуть підвищити якість прогнозів.

Через це дедалі більше політиків, представників правоохоронних органів, розвідувального співтовариства та відповідальних мислителів доходять висновку, що *тотальне цифрове спостереження стає невід'ємним компонентом політики безпеки у високоризикованому цифровому суспільстві*.

У цих умовах перед демократичними державами постає завдання встановити відповідно до обстановки, що змінилася, новий баланс між двома акторами безпеки – державами і громадянами. Цей новий баланс повинен дозволити не на словах, а на ділі реалізовувати проактивну, а не реактивну стратегію боротьби зі злочинністю, поступово переходити від підвищення рівня розкриття злочинів до превентивного їх припинення вже на стадії їх планування [2].

Відомо, що права і прозорість діяльності громадянина для суспільств і держав не суперечать один одному. Виходячи з історичних традицій, інформаційна прозорість життя громадянина не суперечить демократії тоді й лише тоді, коли держава сама по собі контролюється і є підзвітною громадянам, а не тоталітарним правителям. Кордон між демократією і авторитаризмом проходить не за ступенем відкритості приватного життя громадян в умовах високотехнологічного, а відповідно, і нестійкого ризикового суспільства, а по межі підзвітності держави суспільству, можливості суспільства змінити в легітимному порядку будь-яку посадову особу в разі, якщо вона порушила найважливіший принцип демократії – рівність прав і відповідальності.

«Експерти Європолу вважають, що держава може запропонувати за згодою всіх основних політичних сил громадянам новий контракт безпеки, який змінить контракт, що проіснував майже століття. Попередній контракт ґрунтувався на тому, що головні загрози суспільству несуть зовнішні вороги, а тому держава може забезпечити безпеку громадян в умовах недоторканності їх приватного життя. У новому соціальному контракті держава повинна чесно повідомити громадянам, що у високоризикованому турбулентному світі немає більше внутрішніх і зовнішніх ворогів, є законослухняні громадяни, ті, що налаштовані на творення і живуть не лише за законами, а й за цінностями, з одного боку, і злочинці , терористи, зловмисні мафіозні держави – з іншого. У цих умовах держава може забезпечити безпеку лише тих громадян та організацій, які добровільно підуть на пом'якшення стандартів недоторканності приватного життя і комерційної таємниці в межах, необхідних для дотримання вимог національної, континентальної або іншої колективної безпеки. При цьому в контракті мають бути чітко прописані заходи, за допомогою яких громадяни, суспільство і бізнес можуть контролювати не абстрактну державу, а конкретні інститути і персонально чиновників – від голів урядів до голів департаментів – стосовно невикористання ними даних в будь-яких цілях, ніж відбиття загроз безпеки» [2].

Будь-які обмеження цифрових прав громадян на приватність повинні бути чітко сформульовані з таким ступенем точності, щоб громадяни точно розуміли, в яких випадках, із чиєї санкції і як збиратимуться їх особисті дані, як використовуватимуться, як і коли знищуватимуться. Усе це слід прописати не у відомчих документах, а в законодавствах

окремих країн. Крім того, додаткові можливості збору персональної інформації слід збалансувати з реальними потребами розслідувальних і прогнозно-моніторингових інформаційних платформ [2; 3].

Ці обмеження повинні мати часовий характер і мають бути пов'язані не з конкретними побажаннями парламентарів та урядовців, а спиратися на підтверджені компетентними фахівцями вимоги до інформації, що збирається, з боку проєктантів прогнозно-моніторингових і розслідувальних платформ. Треба чітко усвідомити, що в цьому випадку не програмно-апаратні рішення слідують за законом, а навпаки, закон відгукується на нові потреби правоохоронців, при цьому чітко встановлюючи терміни дозволу. Якщо з'ясується, що система виявилася неефективною, дозвіл має бути відкликано. З іншого боку, якщо з'явилося нове покоління систем, дозвіл слід модифікувати [2].

Щоб звести до мінімуму порушення прав на недоторканність приватного життя та оцінити обґрунтованість обмежень, необхідно на основі узгоджених оцінок встановити отриманий ефект у боротьбі з ОЗ за рахунок експлуатації платформи, база даних якої поповнюється даними, що знову збираються. Можливо, в першу чергу слід покінчити з приватністю у власності та джерелах її придбання. З одного боку, щодо цього є відповідні конвенції ООН, є численні рішення на рівні урядів, парламентів і ЄС про припинення відмивання грошей і проникнення злочинних доходів у легальні сфери. Останніми роками уряди низки країн, перш за все США, Великобританії, Швейцарії та багатьох країн ЄС, ухвалили законодавство про обов'язкове розкриття кінцевих бенефіціарів, зареєстрованих юридичних осіб. Крім того, вживаються активні заходи щодо поступового переходу на електронні гроші.

Нарешті, широка громадськість спонукає уряди і парламенти вжити активних заходів проти тих мільярдерів і мультимільйонерів, які не платять податки або за допомогою податкових юристів в законні способи мінімізують власне оподаткування.

Одним із найсуворіших і найдієвіших міжнародних нормативних актів у сфері захисту персональних даних, ухвалених останнім часом, є Загальний регламент захисту даних (General data protection regulation – GDPR), який з 25 травня 2018 р. регулює збір, уніфікацію і використання персональних даних у країнах ЄС. Дія цього Регламенту поширюється і на компанії за межами ЄС, тому підприємства, які здійснюють діяльність на території Євросоюзу або в процесі своєї діяльності збирають дані громадян ЄС, повинні відповідати вимогам GDPR. Дотримання зазначених правил має велике значення для компаній, що працюють із даними клієнтів з усього світу. За порушення Регламенту компанії доведеться заплатити до 20 млн євро або 4 % річного доходу[1].

З огляду на досвід України слід відзначити, зокрема, Наказ Державної служби фінансового моніторингу України від 24 грудня 2019 р. № 159 «Типологічне дослідження "Відмивання доходів від привласнення коштів і майна державних підприємств та інших суб'єктів, які фінансуються за рахунок державного та місцевих бюджетів"». У цьому документі задекларовано запровадження інноваційних інструментів для посилення автоматичного моніторингу закупівель, що ґрунтується на алгоритмах штучного інтелекту та системі автоматизованих ризик-індикаторів. Система індикаторів (risk.dozorro.org) дозволяє швидко провести оцінювання ризику неефективного проведення процедури закупівлі чи обмеження конкуренції. Ризик-індикатори охоплюють усі процедури закупівель зі статусом «Завершено», оголошені з 1 січня 2016 р., з очікуваною вартістю від 1 млн гривень.

З огляду на досліджувану проблему важливим є сам факт появи таких аналітичних інструментів автоматичного сканування, а також системи ризик-індикаторів. Цей досвід можна поширити на застосування у правоохоронній сфері.

Існують також певні технічні механізми і засоби компромісного вирішення зазначеної проблеми. Можливим варіантом компромісного вирішення суперечності між конфіденційністю персональних даних і потребами поліцейських розслідувань може слугувати застосування гомоморфного шифрування під час використання правоохоронними органами хмарних платформ з метою збереження та обробки даних, а також у процесі збору і подальшої обробки персоналізованої інформації під час сканування кіберпростору в автоматичному режимі. Збереження конфіденційності інформації в цьому разі можна досягти цілком легальним шляхом, якщо обробка даних здійснюватиметься на віддалених серверах у

[1] Общий регламент по защите данных // Википедия : свобод. энцикл. URL: https://ru.wikipedia.org/wiki/Общий_регламент_по_защите-данных (дата звернення: 13.01.2021).

зашифрованому вигляді без можливості їх розшифрування на стороні серверів. Тобто під час передання інформації на сервер вона має бути зашифрована на стороні клієнта, оброблена в зашифрованому вигляді на сервері, і результати обробки розшифровуватимуться на стороні клієнта [4]. При цьому слід розуміти, що персоналізована інформація у переважній більшості випадків зберігається у текстовому форматі, який без ускладнень піддається процедурі гомоморфного шифрування. Певні труднощі існують для шифрування числової інформації, але і для таких випадків вже розроблено відповідні механізми [4]. До того ж зазначимо, що такі механізми необхідно застосовувати у тих випадках, коли над числовими даними на сервері виконуються арифметичні або математичні перетворення. Якщо такі перетворення не виконуються, то числові дані піддаються процедурі гомоморфного шифрування так само легко, як і текстові дані.

Для вирішення досліджуваної проблеми в систему «ePOOLICE» включили програмний модуль, що виконує функцію, аналогічну гомоморфному шифруванню, і дозволяє примирити вимоги захисту персональних даних і потреби поліцейських розслідувань. Під час надходження персональних даних у систему модуль стирає такі ідентифікатори, як ім'я, прізвище і замінює їх на довільно обрані номери. У підсумку всі дані зберігаються не на громадян країн ЄС, що мають прізвища, ім'я, а на номери, які володіють певним набором ознак. У такий спосіб вдалося повністю забезпечити вимоги європейського законодавства й одночасно включити до складу баз даних значні масиви персональної інформації. Експерти Європейського суду з прав людини ретельно вивчили проєктну документацію платформи. У підсумку вони винесли вердикт, що система «ePOOLICE» повністю відповідає суворим стандартам європейського законодавства [2].

Іншим технічним механізмом забезпечення конфіденційності зібраних автоматичним шляхом персональних даних є обмеження (заборона) на технічному рівні доступу до зібраних таким чином даних – користувач отримує доступ лише до результату обробки даних, тобто до результуючої аналітичної довідки, яка не містить персональних даних, на збір та обробку яких відсутній дозвіл. Але в такому разі програмний код аналітичної системи повинен гарантовано забезпечити унеможливлення неавторизованого доступу до використовуваних персональних даних.

Висновки

У цілому зазначимо, що шляхи вирішення сформульованої проблеми лежать як у правовій площині, так і в технічній, причому її правовий аспект має дві складові – міжнародну і національну. Відповідно, врегулювання будь-якого одного з них не визначає повного вирішення проблеми в цілому. Технічні варіанти рішення повністю не вирішують проблеми. Питання про її принципове вирішення лежить у правовій площині, а оскільки організована злочинність в умовах глобальної цифровізації світового суспільства дедалі більше набуває транснаціонального характеру, то насамперед це є сферою міжнародного права. Отже, повне вирішення проблеми має комплексний характер і повинно містити низку як нормативно-правових актів на рівні міжнародного і національного права, так і певні заходи технічного характеру, які забезпечують законність процедур збору персоналізованих даних в Інтернеті, що застосовуються поліцейськими структурами у найсучасніших інструментальних високотехнологічних аналітичних системах.

Список бібліографічних посилань

1. Ларина Е. С., Овчинский В. С. Искусственный интеллект. Большие данные. Преступность. М. : Книжный мир, 2018. 166 с.

2. OSCE Guidebook. Intelligence-Led Policing. OSCE. Vienna, June 2017, 105 p.

3. Інформаційні технології у правоохоронній діяльності. Частина 1: Високотехнологічні тренди у правоохоронній сфері зарубіжних країн : навч. посіб. / В. М. Струков, Д. Ю. Узлов, Ю. В. Гнусов та ін. ; за заг. ред. В. М. Струкова. Харків : Діса плюс, 2020. 276 с.

4. Струков В. М., Гуділін В. В. Гомоморфне шифрування як засіб убезпечення баз даних НПУ на хмарних платформах // Протидія кіберзлочинності та торгівлі людьми : матеріали міжнар. наук.-практ. конф. (м. Харків, 27 трав. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2020. С. 193–196.

Надійшла до редколегії 18.01.2021

ГНУСОВ Ю. В., СТРУКОВ В. М., МОЖАЕВ А. А. ПРОБЛЕМА СОГЛАСОВАНИЯ ПРАВОВЫХ НОРМ С ПОТРЕБНОСТЯМИ ПОЛИЦЕЙСКИХ РАССЛЕДОВАНИЙ С ИСПОЛЬЗОВАНИЕМ ВЫСОКОТЕХНОЛОГИЧНЫХ ИНСТРУМЕНТОВ ПОИСКА ДАННЫХ

Проанализирована проблема согласования правовых норм с потребностями полицейских расследований с использованием высокотехнологичных инструментов поиска данных. Определено, что пути решения сформулированной проблемы лежат как в правовой плоскости, так и в технической, причем ее правовой аспект имеет две составляющие – международную и национальную. Проанализирован опыт мировой практики в области исследуемой проблемы. Определено, что урегулирование какого-либо одного из аспектов не определяет полного решения проблемы в целом. Отмечено, что полное решение проблемы имеет комплексный характер и должно содержать ряд как нормативно-правовых актов на уровне международного и национального права, так и определенные меры технического характера, обеспечивающие законность процедур сбора персонализированных данных в интернете, которые применяются полицейскими структурами в современных инструментальных высокотехнологичных аналитических системах.

Ключевые слова: *глобализация, высокие технологии, проактивная полицейская деятельность, информационно-аналитические системы, «слабые сигналы».*

HNUSOV YU. V., STRUKOV V. M., MOZHAYEV O. O. PROBLEM OF HARMONIZATION OF LEGAL NORMS WITH THE NEEDS OF POLICE INVESTIGATIONS BY USING HIGH-TECH INSTRUMENTS FOR SEARCHING INFORMATION

The problem of harmonization of legal norms with the needs of police investigations with the use of high-tech data search tools has been analyzed. It has been determined that the transition of police structures from a reactive to a proactive paradigm is unalterable in the modern high-tech turbulent world. The problem's structuring has been accomplished. It has been determined that the ways of its solution lie both in the legal plane and in the technical one, where the legal aspect of the problem has two components – international and national. The experience of world practice in the field of the researched problem has been analyzed. The authors have accomplished the analysis of international legal norms in the field of personal data protection, as well as the analysis of the most typical national regulations – starting from the approach of solving the problem in democracies, which for centuries strictly adhere to the doctrine of privacy and private property, to the most radical approach in China. The ways of its solution have been outlined. Technical mechanisms of the solution have been suggested. It has been determined that the settlement of any of the aspects does not mean the solution of the problem in the whole. The matter of its fundamental solution lies in the legal plane, and since organized crime in the context of global digitalization of the world community is becoming increasingly transnational in nature, it is primarily a field of international law. It has been determined that the complete solution of the problem has a complex character and should contain a number of normative and legal acts at the level of international and national law, as well as certain technical measures that ensure the legality of personal data collection procedures used by police in the most modern high-tech, tool-making, analytical systems.

Key words: *globalization, high technologies, proactive policing, information and analytical systems, "poor signals".*