РОЗДІЛ 9
КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.1(73):004.45.5-027.552
DOI https://doi.org/10.32782/2524-0374/2021-4/124

ВИКОРИСТАННЯ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У КРИМІНАЛЬНОМУ ПРОЦЕСІ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ

USE AND PROTECTION OF PERSONAL DATA IN THE CRIMINAL PROCESS OF THE UNITED STATES OF AMERICA

Бабаєва О.В., к.ю.н., доцент,
асистентка кафедри кримінального процесу та оперативно-розшукової діяльності
Національний юридичний університет імені Ярослава Мудрого

Ахмедова А.О., студентка III курсу міжнародно-правового факультету
Національний юридичний університет імені Ярослава Мудрого

Гахраманова І.Б., студентка III курсу міжнародно-правового факультету
Національний юридичний університет імені Ярослава Мудрого

Стаття присвячена дослідженню особливостей правового регулювання порядку отримання, використання та захисту персональних даних у кримінальному процесі Сполучених Штатів Америки (далі – США). У статті розкрито сутність Четвертої поправки до Конституції США (далі – Четверта поправка) в контексті отримання та використання персональних даних крізь призму деяких нормативно-правових актів та рішень Верховного Суду США (далі – ВС США). Також проаналізовано сутність тристоронньої доктрини, що розглядається як виняток із Четвертої поправки з огляду на обмеження її дії на виключне коло осіб у контексті рішення ВС США у справі «США проти Вердуго-Уркві дес». Окрім того, проаналізовано Федеральний закон США «Про недоторканність приватного життя» 1974 року, який є одним з основних нормативно-правових актів, який спрямований на регулювання питання захисту персональних даних. Проаналізовано методи збирання інформації, що містить персональні дані, зокрема: 1) використання брокерів комерційних даних; 2) застосування адміністративних та судових повісток; 3) електронне спостереження та доступ до електронних повідомлень. Висвітлено характерні риси та особливості нормативного регулювання, переваги та недоліки кожного із зазначених методів.

Окрему увагу зосереджено на забезпеченні захисту конфіденційності персональних даних у практичному правовому полі. Так, зокрема, проаналізовано рішення ВС США «Акціонерне товариство «Сузлон Енерджі» проти Microsoft» та «Тієріна проти Уолтерса». У першій справі визначено історичну цінність Федерального закону США «Про конфіденційність електронних повідомлень», який, до речі, регулює третій метод збору персональних даних, та зазначено, на яких суб'єктів поширюється його дія. Встановлено, що особливістю другої справи є те, що у ній констатовано випадки розголошення персональної інформації для так званого "Routine use", яку Федеральний закон США «Про недоторканність приватного життя» розглядає як розкриття інформації з метою, для якої вона була зібрана. А також розглянуто види та особливості перебігу строку позовної давності у справах про захист персональних даних.

Ключові слова: персональні дані, тристороння доктрина, "Routine use", судовий ордер, Четверта поправка Конституції США, методи збору інформації, адміністративні повістки.

The article is devoted to the research of features of legal regulation of reception, use and protection of personal data in the criminal procedure of the United States of America (hereinafter – the USA). The article uncovers the sense of the Fourth Amendment to the Constitution of the USA (hereinafter – the Fourth Amendment) in context of reception and use of personal data with a help of some legal acts and Supreme Court of the USA decisions. Also there is an analysis of the sense of "tripartite doctrine", which is considered as exception to the Fourth Amendment in view of the limitation of its effect on an exceptional category of people in context of Supreme Court decision in case "The USA v. Verdugo-Urquidez". Moreover, there is an analysis of Privacy act of 1974, which is one of the mail legal acts and regulates the question of personal data protection. The article also analyzes the methods of collecting of information that contains personal data, for example: 1) use of commercial data brokers; 2) application of administrative and judicial subpoenas; 3) electronic surveillance and access to electronic messages. The features and peculiarities of legal regulation, advantages and disadvantages of each of the mentioned methods are highlighted.

Special attention is paid to providing protection of personal data privacy in practice. Thus, Supreme Court decisions in cases "Suzlon Energy Ltd v. Microsoft Corp." and "Tijerina v. Walters" are analyzed. The historical value of Electronic Communications Privacy Act, which by the way regulates the third method of personal data collecting, is defined and the list of subjects covered by its action is noted. The article constitutes, that the feature of the second case is that it contains the occasions of disclosure of information under Routine Use, which is defined by Electronic Communications Privacy Act as disclosure of information including the purpose of such disclosure. The types and and features of statute of limitations in cases of personal data protection are also noted.

Key words: personal data, tripartite doctrine, Routine use, judicial warrant, Fourth Amendment to the Constitution of the USA, collecting information methods, administrative subpoenas.

Постановка проблеми. Натепер в Україні, як і по всьому світу, набуває поширення процес діджиталізації, що має свої переваги та недоліки. До першого можна віднести передусім полегшення життя суспільства, оскільки нині кожна людина може отримати освітні, державні та інші послуги, не виходячи з дому. Негативним же аспектом цифровізації багатьох сфер життя є недостатня урегульованість питання захисту персональних даних. Так, у своїй доповіді Уповноважена Верховної Ради України з прав людини звернула увагу на проблематику захисту персональних даних та, зокрема, відзначила велику кількість звернень, що стосуються незаконного втручання у права осіб щодо захисту їхньої персональної інформації. Такими втручаннями здебільшого є порушення недоторканності особистого і сімей-

ного життя під час здійснення діяльності зі стягнення грошового зобов'язання, витребування згоди на обробку даних у випадках, коли така згода не повинна бути надана, а також незаконне поширення персональних даних, наприклад, у соціальних мережах та різноманітних месенджерах [1, с. 21]. Саме тому важливим аспектом у контексті визначених питань є аналіз та використання зарубіжного досвіду розвинутих держав, зокрема США.

Аналізуючи законодавство США, слід зазначити, що воно не має чіткої системи нормативно-правових актів, які регулюють питання захисту персональних даних. Натомість у цій державі наявна розгалужена система актів, які регулюють питання конфіденційності як на федеральному, так і на рівні штатів. Проте, незважаючи на відсутність чіткої ієрархії, у США наявне демократичне ставлення до захисту персональних даних, що виявляється у захисті прав не тільки громадян, а й іноземців та осіб без громадянства. Крім того, законодавство США спрямоване на захист прав осіб не тільки "de jure", але й "de facto", що можна спостерігати відповідно до судової практики. Отже, врахування досвіду розвинутих зарубіжних держав у сфері використання та захисту персональних даних є необхідною запорукою охорони фундаментальних прав та свобод особи у контексті реформування національної правової системи.

Аналіз останніх досліджень та публікацій. Питання використання та захисту персональних даних ставали предметом наукового дослідження в національній доктрині таких учених, як: В.І. Теремецький, Д.В. Цвірюк, А.В. Туні, В.Г. Пилипчук, В.М. Брижко, М.А. Важорова, К.С. Мельник, О.Д. Сидєльніков, О.І. Яременко. Серед зарубіжних науковців розгляд визначеної проблематики здійснювали К.Д. Хуфнегл, Ч. Дойль, Ш. Бойн, Р. Хейсті, М. Суб'яллі, С. Чабінські, П. Пітман, Р. Джейн та інші.

Метою статті є аналіз теоретичних і практичних аспектів отримання, використання та захисту персональних даних у кримінальному процесі США, а також виявлення недоліків та переваг його нормативного регулювання.

Виклад основного матеріалу. У законодавстві США є низка законів, дія яких спрямована на регулювання питань, що стосуються отримання та захисту персональних даних, проте предметом нашого дослідження будуть лише деякі з них, а саме: Конституція США, Закон «Про недоторканність приватного життя» 1974 року [2], Закон «Про конфіденційність електронних повідомлень» 1986 року [2], Закон «Про прослуховування телефонних розмов» [2], Закон «Про збережені повідомлення» [2] та Закон «Про реєстратор набраних номерів» [2].

Так, Четверта поправка гарантує право особи на охорону особистості, житла, майна, паперів від необґрунтованих обшуків і арештів. Необґрунтованим у такому разі вважається обшук або арешт без належного оформленого на те ордера, тобто судового наказу, який повинен містити законні підстави такого обшуку або арешту та докладний опис місця, що підлягає обшуку, та предметів, які підлягають арешту [3, с. 11]. Але важливим моментом є те, що навіть за відсутності одного з цих пунктів ордер вважається таким, що має законну силу. Слід зазначити, що захистом Четвертої поправки користуються тільки резиденти цієї країни. Такого висновку дійшов ВС США у справі «США проти Вердуго-Урквідес», де агенти з Управління по боротьбі з наркотиками провели обшук у житлі резидента Мексики та вилучили документи, що підтверджували його причетність до розповсюдження наркотиків. Відповідач стверджував, що ці докази слід визнати недопустимими, оскільки вони отримані без ордера, натомість ВС зазначив, що, оскільки підсудний є громадянином Мексики, на нього це положення Конституції не поширюється [4]. Винятком з цього правила також є персональні дані, які надані третім особам, наприклад банкам чи телефонним компаніям. У такому разі ці дані, наприклад банківські записи, діють під впливом тристоронньої доктрини ("third-party doctrine"), зміст якої полягає у тому, що доступ до таких даних правоохоронні органи можуть отримати без законного ордера, тобто такі дані не користуються механізмом «захисту недоторканності приватного життя» [5, с. 10].

Закон «Про недоторканність приватного життя» 1974 р. є одним з основних нормативно-правових актів, який спрямований на захист персональних даних. Нормативні положення цього закону спрямовані на регулювання порядку збору, обробки, використання персональних даних всіма видами агентств, включаючи правоохоронні органи. Деякі вчені зазначають, що цей акт є аналогом європейських актів про захист персональних даних. Прикладом може слугувати Директива Європейського Союзу (далі – ЄС) 2016/680 Європейського Парламенту та Ради ЄС про захист фізичних осіб у разі обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або переслідування кримінальних правопорушень або виконання кримінальних покарань, а також щодо вільного руху таких даних [6]. Певна «нормативна схожість» цих законодавчих актів полягає, зокрема, у дотриманні різноманітних принципів у разі здійснення обробки персональних даних, таких як: а) принцип «прозорості» ("transparency") передбачає інформування громадськості про існування системи особистих даних шляхом опублікування такої інформації у Федеральному реєстрі; б) принцип цільового використання персональних даних, тобто агентство повинне збирати та зберігати тільки ту інформацію, яка є необхідною для досягнення поставленої ними мети; 3) принцип точності, повноти, актуальності інформації, яку збирає, зберігає агентство [5, с. 11].

Ще однією спільною рисою у правовому регулюванні захисту персональних даних ЄС та США є наявність окремого співробітника або навіть спеціального підрозділу, який слідкує за дотриманням правил обробки інформації. Так, відповідно до Директиви ЄС такою особою є Інспектор з питань захисту даних [6], у США цим займається не окремий співробітник, а спеціальний підрозділ: Управління з питань невтручання у приватне життя Міністерства національної безпеки та Управління з питань невтручання у приватне життя та цивільних свобод Міністерства юстиції США [5, с. 12]. Але принциповою різницею є те, що у ЄС функцію щодо дотримання захисту персональних даних здійснює незалежний орган, а в США – підрозділи державних органів, що може слугувати підставою для сумнівів щодо прозорості та чесності діяльності таких органів.

Щодо Закону «Про недоторканність приватного життя», то слід зазначити, що він гарантує особам право на доступ до зібраної щодо них інформації, виправлення її у разі неправдивості деяких її частин. Суб'єкт таких даних також може подати три види позовів до суду: два з яких стосуються порушення його права на доступ та виправлення його персональних даних та один – на отримання компенсації за незаконне розкриття персональних даних. Але важливим аспектом є те, що особа не може подати перші два позови щодо порушення наданих їй Законом прав правоохоронними органами, оскільки останні звільнили свої бази даних від виконання вимог зазначеного закону. Тобто у такому разі особа може подати тільки позов для отримання компенсації за незаконне злиття інформації щодо неї [5, с. 11]. Таким чином, Перша поправка Конституції США, яка гарантує право особи на подання скарги у разі порушення її прав, не поширює свою дію на діяльність правоохоронних органів щодо обробки персональних даних.

Під час розслідування кримінальних правопорушень правоохоронним органам США дозволено застосовувати такі методи збирання персональних даних: 1) використання брокерів комерційних даних (брокери даних – це

компанії, які самостійно або з чиєюсь допомогою збирають дані про особу з різноманітних Інтернет-ресурсів та продають її третім особам для різних цілей. До таких персональних даних можуть належати: ім'я, вік, стать, освіта, ідентифікаційний код, паспортні дані, рід занять, дохід, дані про нерухомість та інше); 2) застосування судових та адміністративних повісток (адміністративна повістка – це документ, який вручається федеральними агентствами без здійснення попереднього судового контролю щодо необхідності надання такої повістки фізичним особам, який зобов'язує останніх з'явитися до них та дати показання або надати документи, які є необхідними для розслідуваного ними кримінального правопорушення; 3) електронне спостереження та доступ до електронних повідомлень, що дозволяється лише за наявності постанови суду. Зазначені методи збирання персональних даних є досить суперечливими, оскільки не гарантують належного захисту персональних даних особи [5, с. 15].

Розглядаючи перший метод збирання інформації, що містить персональні дані, слід зазначити, що правоохоронні органи наділені правом отримувати інформацію від комерційних та некомерційних організацій, таких як брокери даних, про яких ми зазначили вище, або безпосередньо звертатися до онлайн-ресурсів, тобто соціальних мереж [5, с. 15]. У такому разі брокери даних виступають певними посередниками між фізичною особою та правоохоронними органами. Такий спосіб отримання інформації є набагато легшим, оскільки правоохоронним органам не треба самостійно шукати всю необхідну інформацію. Спектр інформації про фізичну особу, яку знаходять брокери даних, справді вражає, і це не стосується лише місця проживання особи або її віку. Знаючи лише ім'я особи або її адресу, брокери даних можуть отримати інформацію про все нерухоме майно, що має особа, транспортні засоби, зброю, всі позови, які вона колись подавала до суду, активи, свідоцтво про реєстрацію шлюбу, борги, дані карток тощо. Законодавство США не регулює діяльність брокерів даних, тому така їх практика не має правових обмежень. Співробітництво між брокерами даних та правоохоронними органами полягає в тому, що перші продають зібрану ними інформацію другим, на основі чого останні складають досьє на кожну потрібну їм особу. Як зазначають деякі вчені, це є проявом свавілля з боку правоохоронних органів та порушенням Закону «Про недоторканність приватного життя», оскільки отримання інформації таким чином створює ризик для порушення права особи на захист її персональних даних, тому що така інформація може бути використана в політичних або особистих цілях [7, с. 597]. Це питання було також предметом обговорення Комісії з питань щодо недоторканності приватного життя особи, яка зазначає, що таким чином порушується баланс між владою та народом, що призводить до підвищення впливу першого шляхом застосування досить легкого способу отримання інформації щодо окремих осіб та людей загалом [7, с. 597].

Наступним методом отримання інформації правоохоронними органами є застосування адміністративних та судових повісток. Адміністративна повістка, як уже було зазначено, – це документ, який надається адміністративними органами фізичним особам для того, щоб останні прибули до суду і надали показання, документи або допомогу першим у здійсненні покладених на них функцій. Адміністративні повістки є дещо неординарним інструментом для отримання інформації в ході кримінального розслідування, але не є і маловідомим. Уперше ідея про застосування адміністративних повісток у кримінальних справах виникла на 108-му засіданні Конгресу США, де Президент запропонував розширити межі застосування такого виду повісток. Зазвичай такі повістки застосовуються у кримінальних справах щодо шахрайства, жорсткого поводження з дітьми, кримінальних правопорушень проти статевої недоторканності особи та інше. Такі повістки повинні відповідати декільком вимогам: 1) відповідати умовам дозвільного статуту такого органу; 2) запитувані документи мають відношення до розслідування; 3) запитувана інформація не повинна перебувати у володінні правоохоронних органів; 4) приведення у виконання повістки не передбачатиме собою зловживання судовим процесом [8]. У разі недотримання особою обов'язку щодо з'явлення до суду за адміністративною повісткою Генеральний прокурор США відповідно до §1386 Кодексу США має право звернутися до суду, до територіальної юрисдикції якого належить розгляд такого кримінального правопорушення. Наслідком такого звернення, відповідно до зазначеного розділу, є те, що суд видає розпорядження, яким зобов'язує особу з'явитися до Генерального прокурора для дачі показань або для надання необхідних документів [2]. На осіб, які дають показання, поширюється П'ята поправка Конституції США, яка гарантує право особи не свідчити проти себе [3]. Є думка, що отримання інформації шляхом видачі адміністративної повістки є порушенням Четвертої поправки, оскільки документи надаються адміністративним органам без оформленого на те ордера.

Основним законом, що регулює третій метод збирання інформації, є Закон «Про конфіденційність електронних повідомлень» 1986 р., який діє на федеральному рівні. Цей нормативно-правовий акт складається ще з трьох документів, а саме: 1) Закону «Про прослуховування телефонних розмов»; 2) Закону «Про збережені повідомлення»; 3) Закону «Про реєстратор набраних номерів». Відповідно до цього акта всі повідомлення, які можуть отримати органи розслідувань, поділяється на три типи: а) інформація отримана через дротові зв'язки й телефонні повідомлення, які являють собою голосові повідомлення, що проходять через телефон або кабельний дріт; б) усні повідомлення, тобто такі, які висловлені особисто за умови, що особа вважала, що таке повідомлення має конфіденційний характер; в) електронні повідомлення, які розглядаються як сигнали, звуки, зображення, листи, що передаються через кабель, електромагнітну, фотооптичну, фотоелектронну систему [5, с. 17]. До речі, перший тип повідомлення користується найбільшою захищеністю порівняно з іншими. Положення Закону «Про прослуховування телефонних розмов» застосовуються в тих випадках, коли органи розслідування бажають отримати текст повідомлення з необхідної їм телефонної розмови шляхом прослуховування. Для реалізації цієї дії прокурор по кримінальних справах повинен звернутися до суду та отримати відповідну постанову. Але обов'язковою умовою є доведення необхідності проведення такої дії. Тобто прокурор повинен довести суду наявність підстав щодо готування або вчинення кримінального правопорушення, а також те, що шляхом перехоплення такого телефонного дзвінка та прослуховування розмови органи розслідування зможуть отримати необхідну їм інформацію [5, с. 17]. Таким чином, вимоги до доведеності підстав проведення такої негласної дії мінімізують ризики прослуховування інформації, що не має жодного відношення до розслідуваного кримінального правопорушення.

Положення Закону «Про збережені повідомлення» застосовуються до записів та повідомлень, які зберігаються двома видами провайдерів послуг: провайдерами, що надають послуги електронного зв'язку, та провайдерами, що надають віддалені обчислювані послуги. Таким чином, перший тип провайдерів дає можливість відправляти та отримувати електронні повідомлення, наприклад шляхом створення облікового запису в електронній пошті; другий тип надає послуги щодо зберігання та обробки персональної інформації особи у так званому "cloud". Також законодавством США передбачений спеціальний порядок отримання тексту повідомлень з електронної пошти: для отримання змісту повідомлень, які зберігаються менше

180 днів, правоохоронним органам досить надати звичайний ордер на обшук. У разі, якщо таким повідомленням понад 180 днів, правоохоронні органи мають два варіанти: або можуть надати судову чи адміністративну повістку з повідомленням особи та з отриманням постанови суду про те, що така інформація є справді необхідною, або знову ж таки отримати таку інформацію за допомогою ордера на обшук. Слід зазначити, що законодавство США дозволяє отримання такої інформації та розголошення її лише тією мірою, якою це є необхідним для розслідуваного ними кримінального правопорушення [5, с. 18]. Крім того, Кодекс США, а саме § 2517, дозволяє правоохоронним органам, у тому числі слідчому, розкривати таку інформацію іншим співробітникам. У разі порушення вимог Закону «Про збережені повідомлення» посадові особи підлягають або цивільній, або кримінальній відповідальності залежно від характеру правопорушення [2].

Аналізуючи Закон «Про реєстратор набраних номерів», слід зазначити, що він стосується здебільшого метаданих, пов'язаних з телефонними дзвінками, Інтернет-повідомленнями та сайтами, які відвідувала фізична особа (таким шляхом можна отримати IP-адрес та визначити місцезнаходження особи). Для отримання такого роду інформації також необхідним є отримання судового ордера за умови наявності підстав, що така інформація має відношення до розслідуваного кримінального правопорушення. Але цікавим фактом є те, що цим законом передбачено право замовчування правоохоронних органів про факт «спостереження» за такою особою, тобто у двох попередніх законах правоохоронні органи протягом 90 днів після закінчення розслідування повинні повідомити фізичну особу про те, що вона була об'єктом спостереження [5, с. 18–19]. До того ж в ордері щодо отримання метаданих не зазначаються ніякі обмеження щодо обробки та поширення такої інформації, що, на нашу думку, є недоліком цього нормативно-правового акта та потребує виправлення, оскільки «злиття» такої інформації або її використання у непередбачених кримінальним розслідуванням межах може призвести до порушення права особи, гарантованого Четвертою поправкою.

Розглянувши питання захисту персональних даних на законодавчому рівні, неможливо не приділити увагу щодо визначеної проблематики практиці ВС США як невід'ємної складової частини джерел права цієї держави. Це є необхідним для розуміння підходу до вирішення правового спору щодо захисту персональних даних, але вже у практичному аспекті.

Так, відповідно до обставин справи акціонерного товариства «Сузлон Енерджі» проти корпорації Microsoft АТ «Сузлон Енерджі» вимагало від останнього обліковий запис електронної пошти Раджагопалана Срідхара, громадянина Індії, проте Microsoft відмовилася від надання таких відомостей. Окружний суд погодився із таким рішенням, оскільки це відповідає положенням Закону «Про конфіденційність електронних повідомлень».

Щодо обставини цієї справи: АТ «Сузлон Енерджі» звернулося до Microsoft для отримання облікового запису електронної пошти Срідхара на підставі пункту 28 Кодексу США § 1782 [2]. Відповідно до положення цього пункту окружний суд відповідної території, в якому проживає особа, може надати останній показання або інформацію щодо іншої особи для використання нею цих даних у судовому процесі в іноземному чи міжнародному трибуналі. Слід наголосити, що така інформація може надаватися лише за умови наявності судового прохання або згоди будь-якої зацікавленої особи. Microsoft зазначила, що якщо вона б надала такі дані щодо Срідхара акціонерному товариству, то це вважалося б порушенням Закону «Про конфіденційність електронних повідомлень». Саме тому «Сузлон Енерджі» звернулося до ВС США, щоб домогтися скасування рішення окружного суду та отримати інформацію з облікового запису електронної пошти Срідхара.

Першим питанням, яке викликало сумніви, було: «Чи поширюються положення Закону «Про конфіденційність електронних повідомлень» на іноземців. Отже, виникла суперечка з приводу того, чи поширюються положення пункту 28 Кодексу США та Закону «Про конфіденційність електронних повідомлень» на іноземців, зважаючи на те, що там міститься конструкція «будь-яка зацікавлена особа». Натомість ВС США підтвердив, що позиція окружного суду з приводу того, що «будь-яка особа» охоплює також й іноземних громадян, є правильною [2]. Таким чином, відповідно до висновку ВС дія Закону «Про конфіденційність електронних повідомлень» поширюється на громадян США, іноземців, осіб без громадянства та юридичних осіб, які: 1) використовують електронні комунікаційні сервіси; 2) належним чином уповноважені на використання таких сервісів. Така думка також знаходить свій прояв у справі «O'Rourke проти Міністерства юстиції США» [11].

Також слід зазначити, що АТ «Сузлон Енерджі» вказувало на те, що Закон «Про конфіденційність електронних повідомлень» покликаний для того, щоб захищати положення Четвертої поправки, яка поширює свою дію виключно на громадян США, обґрунтовуючи це таким твердженням: «З появою комп'ютеризованих систем зберігання інформації в американців з'явилася можливість блокувати особисту та ділову інформацію... Закон повинен розвиватися разом із технологіями для того, щоб Четверта поправка не втрачала своєї сили... Конгрес повинен діяти так, щоб захищати інтереси громадян США... Комітет вважає, що Закон повинен забезпечувати баланс між конфіденційністю американців та законними потребами правоохоронних органів». Проте ВС США дійшов висновку, що, незважаючи на те, що Закон «Про конфіденційність електронних повідомлень» повинен захищати громадян США на підставі Четвертої поправки, це зовсім не означає, що він не повинен захищати інтереси іноземців та осіб без громадянства. Навпаки, Закон «Про конфіденційність електронних повідомлень» має бути спрямований на захист усіх внутрішніх обмінів повідомленнями не тільки громадян США, але й іноземців, осіб без громадянства та юридичних осіб. Іншою проблемою було те, що «Сузлон Енерджі» стверджувало, що воно заздалегідь отримало дозвіл Срідхара на отримання відомостей з його облікового запису, на що ВС відповів, що має сумніви через нелогічність такого твердження. Таким чином, розглянувши всі обставини справи, Суд дійшов висновку, що «Сузлон Енерджі» не отримувало згоду на отримання даних з облікового запису електронної пошти Срідхара.

Отже, зважаючи на те, що положення Закону США «Про конфіденційність електронних повідомлень» поширюються на іноземців, ВС США підтвердив відмову окружного суду щодо надання даних з облікового запису електронної пошти Срідхара. [9]

Втім проблема поширення дії Закону «Про конфіденційність електронних повідомлень» не є єдиною у законодавстві США щодо захисту персональних даних. Прикладом також може слугувати справа «Тієріна проти Уолтерса», відповідно до обставин якої Марія Тієріна та Лоренцо Тієріна подали заявку на отримання позики на допомогу ветеранам. У заяві Лоренцо Тієріна зазначив, що він працює у Ісаака Барфілда та надіслав форму, заповнену Барфілдом про працевлаштування. Проте під час випадкової перевірки Адміністрацією у справах ветеранів було виявлено, що пан Тієріна сам заповнив форму-підтвердження працевлаштування. Дізнавшись про це, Адміністрація у справах ветеранів звернулася до Офісу Генерального інспектора для проведення розслідування. Своєю чергою останній звернувся до Генерального прокурора США, який відмовився виступати обвинувачем у цій справі через недостатність доказів. Коли Адміністрації у справах ветеранів стало відомо, що пан Тієріна мав складати адвокатський іспит у Техасі, заступник

Генерального інспектора Адміністрації у справах ветеранів надіслав до екзаменаційної комісії адвокатів у Техасі лист, у якому була зазначена інформація щодо фальсифікації паном Тієріним документів для отримання позики на допомогу ветеранам. Також у листі зазначалося, що Адміністрація готова надати будь-яку детальну інформацію щодо пана Тієріна, що і було зроблено надалі. В результаті чого Марія Тієріна та Лоренцо Тієріна подали позов про порушення захисту персональних даних на підставі Конституції США, Закону «Про недоторканність приватного життя» та Закону «Про свободу інформації».

Для вирішення справи Суд звернувся до положень Закону США «Про недоторканність приватного життя». Підрозділ b цього Закону зазначає, що підприємствам, установам і організаціям заборонено розголошувати інформацію про особу будь-якій іншій особі або органу. Проте є винятки, відповідно до яких інформація може бути розголошена у порядку "Routine use", яку Закон визначає як розголошення з метою, з якою вона була зібрана. При цьому для того щоб розкрити інформацію, орган, який безпосередньо розголошує цю інформацію, зобов'язаний внести до Федерального реєстру примітку «згідно з положеннями "Routine use" (для наданої системи записів), включаючи категорію користувачів і мету такого використання. Наприклад, Адміністрація у справах ветеранів стверджувала, що відповідно до "Routine use five" до Закону «Про недоторканність приватного життя» органами публічної влади може бути розголошена інформація у випадках, коли є підстави вважати, що має місце підозра про скоєння злочину. Проте ВС заперечив проти "Routine use five" до Закону «Про недоторканість приватного життя», адже в цьому разі інформація може бути передана тільки органам, що провадять розслідування. На що Адміністрація зазначила, що відповідно до "Routine use three" органи публічної влади можуть надавати інформацію про особу у відповідь на офіційні запити органів, що мають надати такій особі ліцензію, як у нашому випадку, на зайняття адвокатською діяльністю. Та головним контраргументом ВС США було те, що екзаменаційна комісія не вимагала інформації щодо пана Тієріна, оскільки саме заступник Генерального інспектора був першим, хто запропонував її надати.

Ще однією підставою для відмови окружного суду в задоволенні позову Лоренцо Тієріна стала позовна давність, яку встановлює Закон «Про недоторканність приватного життя» щодо позовів, які подаються для захисту персональних даних. Окружний суд не задовольнив позов подружжя Тірієна через порушення ними строку подання позовної заяви. У законодавстві передбачено два види перебігу позовної давності – жорсткий та менш жорсткий. Окружний суд застосував у цьому разі перший вид перебігу позовної давності, сутність якого полягає у тому, що перебіг позовної давності у справах про захист персональних даних становить два роки з дня порушення права на такий захист (слід мати на увазі, що цим днем вважається день, коли позивач не міг ще дізнатися про таке порушення). У менш жорсткому перебігу відлік часу починається з дня, коли позивач дізнався про таке порушення, строк у цьому випадку також становить два роки. Проте ВС не погодився з позицією застосування жорстокого перебігу, зазначаючи, що у цьому разі слід усе ж таки застосувати менш жорсткий перебіг позовної давності, тому що це буде більш справедливо стосовно позивача [10].

Висновок. Таким чином, на підставі проведеного аналізу можна зазначити, що правове регулювання захисту персональних даних у кримінальному процесі США не можна вважати простим та однозначним. Це, зокрема, полягає в існуванні досить розгалуженої системи законодавчих актів, які певним чином суперечать один одному, та відсутності єдиного федерального закону, який значним чином полегшив би регулювання питання захисту конфіденційності та кібербезпеки. Ще одним недоліком є застарілість цих законів, які, на жаль, не відповідають у деяких своїх положеннях сучасним реаліям. Проте в контексті визначеної проблематики «на допомогу з'являються» рішення ВС США, в яких інтерпретуються положення цих численних законів та певним чином доповнюються з урахуванням усіх проблем, що існують на практиці. Досить сумнівними, на нашу думку, є деякі методи збору інформації правоохоронними органами, особливо це стосується отримання персональних даних особи від комерційних брокерів, що, як уже зазначалося, породжує ризик порушення права особи на захист її персональної інформації. Крім того, незрозумілим залишається сутність триторонньої доктрини, оскільки її положення прямо суперечать Четвертій поправці Конституції США. Так, вважаємо, що будь-яка інформація, що стосується особи, повинна бути отримана лише на підставі судового ордера (рішення), що підтверджуватиме законність такої дії з боку правоохоронних органів.

Проте поряд із недоліками є й переваги підходу до регулювання захисту персональних даних у США. Передусім, це стосується поширення положень Закону «Про конфіденційність електронних повідомлень» не лише на громадян США, але й на іноземців та осіб без громадянства, що своєю чергою гарантує захист від свавілля з боку держави всіх осіб, а не лише резидентів. Разом з тим досить суперечливим є те, що Четверта поправка Конституції США не поширює свою дію на іноземців, що породжує певні колізії, оскільки зазвичай усі законодавчі акти повинні відповідати Конституції та ґрунтуватися на її приписах. Ще однією вагомою перевагою законодавства США у сфері захисту персональних даних є те, що дані осіб захищаються у будь-якому разі, навіть якщо через захист таких прав може бути нанесена шкода морально-етичним принципам органів публічної влади.

ЛІТЕРАТУРА

1. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні. Уповноважена Верховної Ради України з прав людини. Київ, 2020. URL: file:///C:/Users/User/Downloads/zvit_2020_rik_%20(1).pdf (дата звернення: 23.04.2021).

2. Code of Laws of the United States of America. 1926. 53 titles. URL: https://www.law.cornell.edu/uscode/text (дата звернення: 23.04.2021).

3. The Constitution of the United States of America of 17th September 1787. URL: https://constitutioncenter.org/media/files/constitution.pdf (дата звернення: 23.04.2021).

4. United States v. Verdugo-Urquidez. 494 U.S. 259, 110 S. Ct. 1056. 1990. URL: https://core.ac.uk/download/pdf/144226381.pdf (дата звернення: 23.04.2021).

5. The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens. *DIRECTORATE GENERAL FOR INTERNAL POLICIES. POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS.* 2015. P. 36. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf (дата звернення: 23.04.2021).

6. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Entered in force in 5th of May, 2016. P. 89. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504 (дата звернення: 23.04.2021).

7. Chris J. Hoofnagle. Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. *J. INT'L L.* 595. 2003. Volume 29. URL: https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1774&context=ncilj (дата звернення: 23.04.2021).

8. Charles Doyle. Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis. *Congressional Research Service. The Library of Congress.* 17th of March. URL: https://fas.org/sgp/crs/intel/RL33321.pdf (дата звернення: 23.04.2021).

9. Suzlon Energy Ltd. v. Microsoft Corp., 10-35793. 9th Cir. 2011. URL: https://cases.justia.com/federal/appellate-courts/ca9/10-35793/10-35793-2011-10-03.pdf?ts=1411064222 (дата звернення: 23.04.2021).

10. Tijerina v. Walters 821 F.2d 789. D.C. Cir. 1987. URL: https://casetext.com/case/tijerina-v-walters (дата звернення: 23.04.2021).

11. Shawn Boyne. Data Protection in the United States. *The American Journal of Comparative Law.* No. 66. July 2018. URL: https://www.researchgate.net/publication/326257651_Data_Protection_in_the_United_States (дата звернення: 23.04.2021).