ISSN – 0136–8168. Вісник Львівського університету. Серія юридична. 2014. Випуск 60. С. 185–191
Visnyk of the Lviv University. Series Law. 2014. Issue 60. P. 185–191

АДМІНІСТРАТИВНЕ І ФІНАНСОВЕ ПРАВО

УДК 342.721(477)

ПРОТИПРАВНЕ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО МІСТЯТЬСЯ У СОЦІАЛЬНИХ МЕРЕЖАХ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ ТА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

І. Березовська

Львівський національний університет імені Івана Франка
вул. Університетська, 1, 79000 Львів, Україна

Досліджено питання інформаційної та національної безпеки, пов'язані з незаконним збором персональних даних користувачів соціальних мереж та наступним протиправним їх використанням. Обґрунтовано пропозиції щодо протидії такому явищу.

Ключові слова: інформаційна безпека, національна безпека, Інтернет, соціальні мережі, персональні дані.

На процеси глобалізації та інформатизації впливає прогрес науки і техніки, який може мати позитивні та негативні наслідки. З одного боку, людина отримує доступ до нових можливостей. З іншого – стикається з дедалі різноманітнішими ризиками, які є загрозливими для її безпеки, свободи, приватного життя. Останнім часом у глобальних інформаційно-телекомунікаційних мережах щораз більшого поширення набуває новий вид протиправної деструктивної діяльності – збір та аналіз персональних даних користувачів, що згодом передаються для несанкціонованого використання стороннім особам, відбувається розголошення та протиправне використання конфіденційної інформації щодо сфери приватного життя особи, порушуються особисті конституційні права людей.

Актуальність цієї проблеми пов'язана з тим, що у зв'язку з появою нового простору для спілкування й, фактично, можливостей для реалізації найрізноманітніших цілей, зокрема – комерційних, ділових, особистих, виникають нові види та способи незаконного використання інформаційних масивів соціальних мереж в Інтернеті для вчинення різного роду протиправних, а подекуди й злочинних дій.

Чинна на сьогодні в Україні система захисту особи не спроможна забезпечити ефективний захист громадян не лише від реально вчинюваних щодо них протиправних дій з використанням викрадених з соціальних мереж їхніх персональних даних, а й від постійно зростаючих реальних і потенційних загроз.

Фактично, відстеження, збір та аналіз персональних даних користувачів є лише підготовчим етапом для вчинення інших системних та організованих протиправних дій як проти конкретної особи, так і проти певних інституцій, зокрема, і державних інституцій, з якими така особа може мати певні відносини. Варто наголосити, що саме останній аспект створює потенційні передумови для виникнення реальних загроз національній безпеці держави.

Вочевидь, що спілкування пересічного громадянина у мережі навряд чи може зацікавити іноземні спецслужби та організації, проте приватне спілкування «секрето-

носіїв», державних службовців певного рівня та інших категорій осіб, що становлять потенційний оперативний інтерес для таких іноземних служб і організацій, а також їх близьких родичів, навпаки, є досить цінною розвідувальною інформацією, яка надалі використовується з метою здійснення розвідувально-підривної діяльності проти України. Саме така інформація може бути використана на шкоду нашій державі при підготовці вербувальних акцій, акцій протиправного впливу на прийняття певних стратегічних для держави рішень у політичній, економічній чи соціальній сферах тощо.

Безпосередньо науковим дослідженням проблем захисту персональних даних займалися В. М. Брижко, О. О. Баранов, К. І. Беляков, І. Б. Жиляєв, Р. А. Калюжний, Д. В. Ланде, В. М. Фурашев, В. С. Цимбалюк, М. Я. Швець та інші. Проте, на сьогодні наукові дослідження загальних проблем протиправного використання персональних даних, що містяться у соціальних мережах, вітчизняні вчені практично не проводили. Проведенням наукових досліджень окремих аспектів організаційно-правової протидії вчиненню різнорідних деструктивних діянь із використанням для цього специфічних можливостей соціальних мереж займаються такі вчені, як В. М. Бутузов, В. М. Горовий, А. І. Марущак, О. О. Поляруш, В. П. Шеломенцев, О. М. Юрченко та ін.

Отже, метою цієї статті є дослідження загальних проблем інформаційної та національної безпеки, пов'язаних із протиправним використанням персональних даних, що містяться у соціальних мережах (даних користувачів соціальних мереж), а також визначення організаційних і правових напрямів їх вирішення з боку держави.

Доцільно наголосити, що переважна більшість користувачів соціальних мереж навіть не задумуються над ступенем потенційної небезпеки та можливими негативними наслідками у випадку витоку та протиправного використання їхніх персональних даних, що містяться у соціальних мережах, створюючи тим самим передумови для подальших деструктивних дій із такою інформацією. Так, за інформацією Forbes, компанія Appinions провела дослідження, згідно з яким з'ясовано, що користувачі більше бояться втрати даних, що містяться в облікових записах у соціальних мережах, ніж витоку інформації про банківські картки [1].

Власники багатьох соціальних мереж запевняють користувачів, що їх інформація є особистою й закритою від сторонніх осіб. Але, як мінімум, її знають власники соціальних мереж, в яких користувач зареєстрований. Як максимум, – всі. Власники можуть використовувати цю інформацію з метою розвитку свого бізнесу чи надавати особисті дані користувачів на запити, наприклад, поліції або спецслужб. Використовуючи пошук інформації, в аккаунтах користувачів знаходять і пропонують якісь послуги. Як приклад, соціальна мережа Mail.ru, після введення інформації про навчання, автоматично пропонує однокласників і однокурсників.

Впевненість користувачів у тому, що їхня інформація надійно захищена паролем, не відповідає дійсності. Зловмисники активно крадуть паролі та логіни до соціальних мереж, які, за даними експертів «Лабораторії Касперського», на чорному ринку коштують усього близько 5 доларів США [2].

Необхідно констатувати, що кількість злочинів, вчинених із використанням інформації, викраденої з соціальних мереж, постійно зростає. Аналітики вважають, що зростання кількості таких злочинів пов'язано зі збільшенням кількості дітей, підлітків і молоді у соціальних мережах.

Європейською комісією було проведено опитування 25 тисяч дітей в 25 країнах-членах ЄС. Згідно з результатами дослідження 38% дітей віком від 9 до 12 років і 77%

дітей віком від 13 до 16 років мають профайли у соціальних мережах, таких як Facebook, Hyves, Tuenti, Nasza-Klasa, SchuelerVZ та ін. Близько 25% опитаних дітей, які користувалися соціальними мережами, зазначили, що їхні профайли є відкритими для всіх користувачів.

Інститутом соціології НАН України проведено дослідження, яке включало в себе опитування 1200 дітей, батьків і учителів в 11 містах України, які продемонстрували необізнаність про потенційні ризики для дітей в мережі Інтернет. Майже половина опитаних дітей готові були розкрити приватну інформацію про себе, про свою родину, переслати свої фотокартки незнайомим особам.

У практичному аспекті варто наголосити на тому, що раніше мали місце переважно факти лише викрадення персональних даних користувачів. Проте останнім часом дедалі більшого поширення набуває відстеження конкретних користувачів соціальних мереж, їх соціальних та особистих зв'язків і уподобань, пристрастей тощо.

Звертає на себе увагу й той факт, що деякі соціальні мережі майже ідеально створені для прикриття, за необхідності, розвідувально-пошукової діяльності спецслужб та організацій щодо збору різнопланової, придатної для наступного аналітичного дослідження особистісної інформації. Наприклад, за оцінкою співробітників спецслужб, соціальна мережа odnoklassniki.ru є класичним прикладом збору розвідувальної інформації. Така потужна систематизація даних по містах, навчальних закладах, підприємствах, військових частинах із зазначенням дати служби, особистих даних громадян із фотокартками, такими розділами, як «мої друзі», «друзі друзів», «співтовариства», відсутня навіть у спецпідрозділів. Вона є довідником для іноземних спецслужб.

Також можливість відстеження користувачів чітко простежується на прикладі соціальної мережі Facebook. При цьому, як правило, воно проводиться з використанням різних сучасних технологій. Наприклад, із використанням файлу ідентифікатора cookie, за допомогою якого відбувається відстеження користувачів, по-перше, тих у кого вже є аккаунт на Facebook і які працюють у соціальній мережі; по-друге, тоді, коли користувачі, не авторизовані в системі після натискання кнопки «Вихід», насправді залишаються в мережі; по-третє, Facebook може відстежувати ваші дії в мережі Інтернет, навіть якщо ви не є користувачем цієї соціальної мережі.

Варто згадати той факт, що соціальною мережею Facebook у 2007 р. було запущено соціальну маркетингово-рекламну систему Facebook Beacon («Маяк»). Система повідомляла друзям користувача соціальної мережі, які ресурси він відвідав і на яких з них зробив покупки чи щось замовив. Але реакція користувачів була негативною. Позицію незадоволених користувачів підтримали відомі правозахисники та експерти з особистої безпеки і наприкінці того ж року додаток Beacon було відключено в обмін на відкликання колективного позову. Позивачі вважали, що фахівцями Facebook було порушено низку законів щодо охорони особистих даних. У підсумку, незважаючи на ліквідацію функції Beacon, відбувся колективний позов користувачів, і за судовим рішенням Facebook 2009 р. зобов'язали виплатити 9,5 млн доларів США у вигляді компенсації [3].

Доцільно констатувати, що попит на персоніфіковану конфіденційну інформацію про користувачів постійно зростає. Доказом цього є факт, що розробники соціальних мереж створюють усе нові інтерфейси і платформи для збору саме такої інформації. Наприклад, в соціальній мережі Facebook розроблено і впроваджено користувальницький інтерфейс Timeline, який дозволяє користувачам відстежувати

всі події в своєму житті від моменту реєстрації в соціальній мережі. Таку інформацію, вочевидь, будуть використовувати як соціальні мережі, так і їх «замовники» у своїх цілях, зокрема і протиправних.

Більше того, придбавши соціальний геологаційний сервіс Glancee, Facebook може проводити пасивне визначення місцеперебування конкретного користувача мережі. Цей сервіс сповіщає користувача про те, що поруч є його «друзі», їхні зв'язки та особи зі схожими інтересами. На відміну від Forsquare, Glancee показово не вимагає реєстрації. Він працює у «тіні», фактично проводячи моніторинг GPS-даних. Показово, що творці додатку рекламують сервіс, як «спосіб виявити навколо себе приховані зв'язки». Варто звернути увагу на те, що під слушним приводом сьогодні соцмережа Facebook розробляє відповідний додаток і для смартфонів [4].

Відстеження переміщення користувачів соціальних мереж також проводиться через відстеження IP-адрес, з яких користувач заходив, наприклад, в особисту пошту. Зокрема, співробітники Інституту Макса Планка в Німеччині протягом 2009–2011 рр. стежили за кореспонденцією 43 млн користувачів поштового аккаунту Yahoo!

Крім того, відстеження користувачів можливе з використанням кнопки «Like» від Facebook, яка дозволяє користувачам оцінювати інформацію на сайті в режимі онлайн. Німецькі правозахисники у галузі захисту приватності інформації вимагають видалити цю кнопку. Вони заявили, що використання кнопки «Like» суперечить німецькому та європейському законодавству, оскільки як наслідок інформація про користувачів – інтереси, тривалість перебування на тій чи іншій сторінці, переходи з одного сайту на інший надходить до США, де згодом використовується для таргетування реклами, аналізу поведінки користувачів на сайті тощо. Представники соціальної мережі підтвердили, що, натискаючи цю кнопку, така інформація як IP-адреси, могла передаватися. Вони також зазначили, що ці дані, відповідно до європейського законодавства через 90 днів видаляються. Однак Facebook, як і кожна американська компанія, згідно з Патріотичним Актом, зобов'язана зберігати цю інформацію значно довше і за необхідності надавати її спецслужбам США [5].

Окремо зупинимося на діяльності системи візуального розпізнавання, що застосовується у мережі Facebook. Безпосередньо сервіс автоматичного розпізнавання обличчя особи був запущений для того, щоб допомогти користувачам знаходити і позначати друзів на фотографіях. Спеціальна програма аналізує фотографії і пропонує користувачеві різні варіанти імен того чи іншого знайомого. Ця система успішно впроваджується в США, у тому числі відповідна програма написана для мобільних пристроїв Apple і призначена для поліції. Як видається, нові технології можуть допомагати швидше і легше ідентифікувати злочинців, адже зафіксовані на камеру спостереження кадри можна порівняти з базою біометричних даних. Однак тут лунають застереження. Зокрема, Йоганнес Каспар зазначає: «Збирання даних – це також засіб соціальної дискримінації. Це у багатьох випадках може призводити до значних зловживань цим інструментарієм» [6]. Наприклад, аналіз індивідуальних рис обличчя може мати випадкові збіги. Як приклад, якщо профіль футбольного фаната буде схожий на профіль якогось футбольного хулігана, йому навіть не продадуть квиток на матч. У зв'язку з рішучими протестами з боку захисників приватних даних спочатку уряд Німеччини, а потім Євросоюз прийняли рішення про заборону цієї технології, яка, на їхню думку, порушує відразу низку законів про захист даних користувача. І соціальна мережа Facebook відключила сервіс

автоматичного розпізнавання обличчя особи користувачів у Європі. Також було відзначено, що банк із «відбитками облич» мільйонів людей пов'язаний із величезним ризиком зловживань. Як приклад, така система може бути використана в недемократичних країнах з метою стеження за опозицією або використана злочинцями. Так, за інформацією А. Аквісті, спеціаліста з інформаційних технологій, зловмисники, використовуючи цю функцію, зможуть досить швидко з'ясувати п'ять цифр полісу соціального страхування – одного з основних документів США [7].

Для отримання персональних даних громадян постійно розробляються та впроваджуються щоразу нові програми і, варто наголосити, це відбувається не лише розробниками соцмереж. Так, за даними британської газети The Guardian, американський військовий підрядчик Raytheon розробив програмне забезпечення під назвою RIOT (Rapid Information Overlay Technology). Це система, створена для швидкого отримання інформації про підозрюваних громадян із соціальних мереж, у тому числі Facebook, Twitter і Foursquare. Журналісти назвали це доказом того, що влада використовує соціальні мережі для високотехнологічного стеження за громадянами. За допомогою цієї програми можна отримати відомості про активність підозрюваного: про його соціальні контакти, карти переміщень тощо. Інформація отримується також з EXIF-заголовків фотографій, опублікованих в особистих фотоальбомах на різних сайтах. За даними журналістів, ця розробка була передана урядовим агентствам США [8].

Останнім часом дедалі більше окремих активістів, громадських організацій регулярно звинувачують адміністрації соціальних мереж взагалі, й Facebook зокрема, в несанкціонованому і незаконному зборі інформації про користувачів і передачі цих даних третім особам. Варто також зазначити, що в Facebook вимагається реєстрація тільки під своїм реальним іменем, проте, в деяких країнах це визнається порушенням законодавства. Так, згідно з нормами Закону Німеччини «Про телекомунікації», громадяни країни мають право використовувати свої псевдоніми на будь-яких сервісах у мережі Інтернет. Своєю чергою, у «найдемократичнішій країні» – Сполучених Штатах Америки внесено поправки до Закону CFAA (Computer Fraud and Abuse Act «Акт про порушення і зловживання роботою комп'ютера», відповідно до якого американцям забороняється отримувати неавторизований доступ до інформації на захищеному комп'ютері. Тобто, на думку професора Університету імені Джорджа Вашингтона Оріна Керр, який в минулому працював прокурором і є фахівцем з комп'ютерної злочинності, правопорушником може вважатися особа, яка використовує помилкове ім'я (і, звичайно, псевдонім) у соціальній мережі або вказує там неправдиву інформацію про себе [9].

Пошук проводиться по відкритій інформації в аккаунтах, але, напевно, в пошуковику закладено можливості зчитувати закриту інформацію фахівцям соцмережі, а також спецслужб. До того ж, якщо від «інформаційних витоків» потерпають транс-континентальні корпорації, банки, то імовірно, що збором інформації з соцмережі та відстеженням зможуть скористатися маркетингові компанії, а також злочинні угруповання (організації).

Розвиток не анонімних мереж – це прекрасне джерело інформації для спецслужб. Установлення контролю над соціальними мережами, тотальний контроль онлайн-активності громадян – це лише питання часу. Спроби контролювати соціальні мережі та використовувати персональні дані користувачів (з різною метою) будуть з часом лише посилюватися. І, звичайно ж, спецслужби отримають додаткову можливість збирати закриту інформацію про користувачів соцмережі та проводити відстеження.

Отже, необхідно зазначити, що, фактично, нам варто вести мову саме про системне використання іноземними організаціями та спецслужбами соціальних мереж, діяльність яких перебуває і юридично, і фактично поза межами правового регулювання нашої держави. Діюча в Україні правоохоронна система неспроможна забезпечити належний ефективний захист наших громадян і національних інтересів від протиправних діянь, що реально вчиняються проти них із використанням незаконно отриманих із соціальних мереж персональних даних користувачів. Це, своєю чергою, зумовлює об'єктивну необхідність негайного вироблення на державному рівні принципово нових підходів до забезпечення захисту інтересів особи, суспільства та держави у цій сфері. Отож, доцільно наголосити на потребі розробки:

– системи заходів правового регулювання доступу до персональної інформації в соціальних мережах (необхідно чітко врегулювати права та обов'язки власників, адміністрації та технічного персоналу соціальних мереж щодо використання, зберігання та захисту персональної інформації;

– основних засад юридичної відповідальності за незаконне розголошення, розповсюдження та використання персональної інформації, що накопичується в інформаційних масивах соціальних мереж;

– системи обмежень щодо використання соціальних мереж деякими спеціальними категоріями громадян (військовослужбовцями, працівниками право охоронних органів, окремими категоріями державних службовців).

Список використаної літератури

1. Appinions: Пользователи больше боятся потери данных из соцсетей чем из банковских систем [Электронный ресурс]. – Режим доступа : http://www. securitylab.ru/news/ 439417.php
2. *Крымов Г.* Всемирная сеть мошенников. Жертвой киберпреступников может стать каждый [Електронний ресурс] / Георгий Крымов. – Режим доступу : http://cripo.com.ua/?sect_id=6&aid=115837
3. Апелляционный суд встал на сторону Facebook в споре по поводу выплат из-за Beacon [Электронный ресурс]. – Режим доступа : http://www.3dnews.ru/software-news/635594
4. Интернет-паноптикум Facebook [Электронный ресурс]. – Режим доступа : http://www.sostav.ua/news/2012/10/02/127/52214
5. Німецькі поборники приватності угледіли загрозу в соціальній мережі Facebook, а точніше в улюбленій користувачами кнопці like [Електронний ресурс]. – Режим доступу : http://briz.if.ua/9590. htm
6. Обережно! Розпізнавання обличчя [Електронний ресурс]. – Режим доступу : http://www.dw.de/обережно-розпізнавання-обличчя/a-16433613
7. Лицевая идентификация может помогать преступникам [Електронний ресурс]. – Режим доступу : http://www.infox.ru/hi-tech/tech/2011/08/02/Licyevaya_idyentifik_print.phtml
8. Владу США звинуватили у шпигунстві за громадянами за допомогою соціальних мереж [Електронний ресурс] – Режим доступу : http://svit24.net/technology/67-vladu-ssha-zvynuvatyly-u-shpygunstvi-za-gromadjanamy-za-dopomogoju-socialnyh-merezh
9. *Соколова Е.* В США за использование ложного имени в Интернете могут посадить [Электронный ресурс] / Е. Соколова. – Режим доступа : http://radiovesti.ru/article/ show/ article_id/26139

ПРОТИВОПРАВНОЕ ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, СОДЕРЖАЩИХСЯ В СОЦИАЛЬНЫХ СЕТЯХ КАК УГРОЗА ИНФОРМАЦИОННОЙ И НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ УКРАИНЫ

И. Березовская

Львовский национальный университет имени Ивана Франко
ул. Университетская, 1, 79000 Львов, Украина

В статье исследуются вопросы информационной и национальной безопасности, связанные с незаконным сбором персональных данных пользователей социальных сетей и последующим противоправным их использованием. Обоснованы предложения по противодействию такому явлению.

Ключевые слова: информационная безопасность, национальная безопасность, Интернет, социальные сети, персональные данные.

UNLAWFUL USE OF PERSONAL DATA CONTAINED IN SOCIAL MEDIA AS A THREAT TO INFORMATIONAL AND NATIONAL SECURITY OF UKRAINE

I. Berezovska

Ivan Franko National University of Lviv
Universytetska Str.1, UA – 79000, Lviv, Ukraine

The article deals with the investigation of the informational and national security issue related to the illegal collection of personal data of users of the social networks, followed by their wrongful use. The propositions concerning the counteraction of this phenomenon are grounded.

Key words: informational security, national security, the Internet, social networks, personal data.

Стаття: надійшла до редакції 30.12.2013
прийнята до друку 19.06.2014