ISSN 1995-6134

УДК 342.72
В.О. СЕРЬОГІН, канд. юрид. наук, доц., Харківський національний університет внутрішніх справ

СОЦІАЛЬНІ МЕРЕЖІ ЯК ЗАГРОЗА ПРАЙВЕСІ

Ключові слова: *соціальні мережі, права людини, прайвесі, недоторканність приватного життя*

За останні п’ять років величезної популярності набули сайти соціальних мереж (англ. – social network sites, скорочено – SNS). Це сайти, що дозволяють користувачам завантажувати інформацію на загальнодоступний профайл, створювати он-лайн список друзів і переглядати профайли інших користувачів. Чимало людей віддають свої персональні дані до таких мереж заради спілкування в Інтернеті. Мільйони людей викладають деталі свого особистого життя на загальний огляд на Facebook, безумовному лідерові серед соціальних мереж і другому за відвідуваністю інтернет-ресурсі світу, що поступається лише пошуковій системі Google. У серпні 2010 р. кількість учасників цієї мережі досягла астрономічної цифри у 500 млн., – це близько 20 % користувачів Інтернету в цілому! Причому половина цих людей відвідують свою сторінку щоденно, у середньому проводячи в он-лайні близько години. Крім Facebook, до найбільших соціальних мереж на сьогодні належать MySpace, Twitter і ВКонтакте (110 млн., 105 млн. і 86 млн. користувачів відповідно) [1, с.35].

Західні дослідники неодноразово зазначали, що соціальні мережі отримали змогу відстежувати взаємодію користувачів на своїх сайтах і зберігати відповідну інформацію для подальшого використання [3–6], чим становлять потенційну загрозу прайвесі. Навпаки, у пострадянській державознавчій літературі, присвяченій різним аспектам теорії й практики захисту права на недоторканність приватного життя (зокрема, у працях Н.Г. Бєляєвої, Г.О. Мітцукової, І.Л. Петрухіна, В.С. Сивухіна, Е.О. Цадикової та ін.), проблема соціальних мереж досі перебуває поза межами уваги, хоча кількість користувачів Інтернету з колишніх радянських республік зростає з геометричною прогресією. Означені фактори визначають актуальність даної статті, її теоретичну та практичну значущість.

Метою даної статті є з’ясування характеру тих ризиків і загроз, що несуть із собою соціальні мережі, а також визначення політико-правових і технологічних можливостей запобігання їм. Досягнення означеної мети є можливим при використані порівняльно-правового, історико-правового, формально-юридичного (догматичного) та системно-структурного методів дослідження. Новизна даної статті полягає у тому, що в ній уперше у вітчизняній юридичній науці соціальні мережі розглядаються через призму правозахисної діяльності, зокрема в аспекті забезпечення права на недоторканність приватного життя (прайвесі).

Приступаючи до висвітлення теми, зауважимо, що дослідження 45 соціальних мереж, проведене організацією Physorg у 2009 р., виявило «серйозне занепокоєння» з приводу як самих учасників спілкування, так і охорони персональних даних. Близько 90 % сайтів, наприклад, для надання дозволу приєднатися до них необґрунтовано вимагають вказувати прізвище, ім’я або дату народження. 80 % сайтів не спроможні використовувати стандартні протоколи шифрування для захисту конфіденційних даних користувачів від атак хакерів. 71 % сайтів у своїй політиці конфіденційності залишають за собою право на передачу даних про користувачів третім особам [2]. Такий стан речей об’єктивно вимагає розробки певних стандартів поведінки у соціальних мережах, у тому числі й на законодавчому рівні.

Користувачі соціальних мереж розкривають доречну для ідентифікації інформацію іншим. Ця інформація є або довідковою, що безпосередньо стосується людини, або атрибутивною, що описує певні ознаки об’єкта даних. І хоча більшість існуючих інструкцій і правил обмежують доступ довідковою інформацією, атрибутивна інформація виявляється також не захищеною. При цьому, накопи-

ISSN 1995-6134

чення великої кількості атрибутивної інформації щодо профайлів соціальних мереж породжує нові ризики для прайвесі.

Через соціальні мережі інформація поширюється значно швидше, ніж через мережу реального життя. Інформація може бути розкрита цілій групі людей зовсім неочікувано, оскільки цифрова інформація легко копіюється, може зберігатися необмежено довго і є доступною для пошуку. Особливо шкідливими для користувачів є ті випадки, коли інформація «подорожує» через різні сфери і надходить до людей, яким вона зовсім не призначалася.

Більшість користувачів не знають, що можуть змінити параметри конфіденційності і, якщо не зроблять цього, то їхні персональні дані будуть відкритими для громадськості. У підсумку, вже сьогодні спостерігаються негативні наслідки зайвої відвертості у соціальних мережах.

Наприклад, нещодавно у США спалахнув «віртуальний» скандал. Ешлі Пейн, вчительку школи Apalachee High School, що в містечку Віндер, штат Джорджія, звільнили з роботи за те, що вона розмістила на своїй сторінці на Facebook фотографії, на яких вона пила алкоголь. Скандальна фотосесія виявилася нічим іншим, як звітом про подорож Пейн до Європи. Переглянувши фотографії своєї співробітниці на Facebook, адміністрація школи зробила висновок, що Пейн подає негідний приклад дітям і вирішила її звільнити.

Цей випадок далеко не єдиний: наприклад, необдумані пости на особистій сторінці Facebook іншого викладача, Глорії Гадсден з університету Іст-Страудебурга у Пенсільванії, також ледве не коштували їй робочого місця. А вона тільки-но й робила, що ділилася з віртуальними друзями своїм настроєм: «ніхто не знає, де узяти пристойного Міллера? Так, сьогодні той іще день». Коли ж день Гадсден вдавався, запис на її сторінці виглядав приблизно так: «Сьогодні був хороший день. Не хотіла вбити жодного студента» [1, с.34-35].

Цей феномен відвертості, у свою чергу, не міг не зацікавити роботодавців. Згідно з даними дослідження американського рекрутингового порталу Careerbuilder.com, 53 % опитаних роботодавців у Великобританії підтвердили, що використовують соціальну мережу для перегляду інформації про кандидатів на роботу. Аналогічне дослідження у США показало подібні результати: 45 % респондентів також зізналися, що відбирають кандидатів на роботу за допомогою соціальних мереж.

«У наш час грань між особистим і професійним дедалі більше стирається», – стверджує британський фахівець із рекрутингу Луї Купер. Він передбачає, що скоро традиційне резюме перетвориться на певний гібрид профайлів людини у соціальних мережах Facebook та Linkedin плюс посилання, відео й записи на Twitter, що мають відношення до кандидата [1, с.35].

Аналогічний погляд висловлює й відомий американський конституціоналіст Д. Солов. На його думку, той факт, що молоді люди діляться найінтимнішими подробицями особистого життя на сторінках соціальних мереж знаменує собою перегляд кордонів між приватним і публічним. Але порівняно з твердженням Л. Купера, висновки Д. Солова значно більш песимістичні: він вважає соціальні мережі смертельно небезпечними для прайвесі [7, с.100–106].

Слід визнати, що для таких висновків є доволі вагомі підстави. Для цього достатньо навести випадок із Меган Мейєр, що приголомшив Сполучені Штати і мав серйозні наслідки для прайвесі на сайтах соціальних мереж [8]. Меган Мейєр, 13-річна дівчина з м. Сент-Луїс, штат Міссурі, вкоротила собі віку одразу після того, як її 16-річний «друг» по спілкуванню в мережі MySpace, написав їй: «Без тебе світ став би кращим». Проте, як з'ясувалося, «16-річний хлопець» був насправді групою осіб, що жили по сусідству і створили фіктивний профайл. Участь у цій містифікації брала й Лорі Дрю, мати одноклассника Меган, котра була притягнута до кримінальної відповідальності за обвинуваченням у порушенні Закону «Про комп'ютерне шахрайс-

ISSN 1995-6134

тво і зловживання» (Computer Fraud and Abuse Act – CFAA) за трьома статтями: створення фіктивних профайлів, відправка образливих повідомлень і вимагання персональних даних від неповнолітніх.

Люди часто забувають, що живуть у світі, де необхідно контролювати інформацію про себе. Адже особа в соціальній мережі ніколи не знає, скільки людей її моніторить і хто читає її пости, а також коментарі на інших сторінках. У цьому контексті проблеми з працевлаштуванням – усього лише один зі зворотних боків спілкування в соціальній мережі. У травні 2010 р. американський пошуковий сервіс Retrevo провів опитування серед 1 тис. осіб, що перебували в режимі он-лайн, чи жалкували вони коли-небудь про зміст своїх постів в Інтернеті. 32 % респондентів відповіли ствердно, причому 3 % з них визнали, що необдумані пости зруйнували їхній шлюб або особисті відносини.

Дії, що завдають шкоди прайвесі користувачів соціальних мереж, можуть бути зведені у чотири групи: збір, обробка, поширення і зберігання персональних даних. Така класифікація допомагає кваліфікувати певні дії, що задають шкоди користувачам, а розробляти заходи щодо попередження таких дій та усунення завданої шкоди.

Серед багатьох ризиків для прайвесі у соціальних мережах варто виокремити, принаймні, три: 1) повна поінформованість про особу; 2) повідомлення інформації злочинцям; 3) відсутність у особи реального контролю за домірністю інформації про себе.

Соціальні мережі відстежують діяльність користувачів своїх сайтів та сайтів своїх партнерів по маркетингу. Вони здатні зібрати безпрецедентну кількість вторинної інформації на своїх користувачів, іноді навіть без їхньої згоди. Коли ж цю інформацію збирають державні органи і використовують її для контролю за громадянами, виникає так звана «архітектура вразливості».

Через великі обсяги інформації про особу, що поширюється через соціальні мережі, вона може врешті-решт легко стати відомою злочинцям, хуліганам, вимагателям. Використання атрибутивної інформації дає змогу їм у мережі видавати себе за жертву і скориставшись цим, отримати дані, аби зв'язатися з нею. Про файли користувачів у поєднанні з простотою зв'язку з користувачами роблять соціальні мережі корисною платформою для зловмисників. Інформація на веб-сайті легко може бути використана для спричинення шкоди репутації певній особі, а значна кількість атрибутивних даних може бути використана для так званого «викрадення особистості». І хоча немає жодних доказів того, що ці речі впливають на всіх користувачів соціальних мереж, експерти сходяться на думці, що вони впливають на значну кількість користувачів і можуть завдати їм значної шкоди.

Соціальні мережі тлумачать згоду, яку користувачі дають при підключенні до їхніх послуг, як повну згоду на вторинне використання персональних даних. Насправді користувачі мають мінімальну інформацію і жодного контролю над вторинним використанням, у т.ч. продажем чи розкриттям їхньої персональної інформації небажаним групам.

Розробники постійно удосконалюють соціальні мережі, роблячи їх дедалі більш функціональними. Не покидаючи Facebook можна пограти в ігри, взяти участь у різноманітних групах за інтересами, читати новини, переглядати відео, робити друзям і знайомим віртуальні подарунки. По суті, мережа перетворюється на другий дім для людини.

Законодавство, що діє сьогодні у переважній більшості країн світу, виявляється непридатним для вирішення усіх цих проблем, пов'язаних із забезпеченням прайвесі у соціальних мережах. Зокрема, американське деліктне право може захистити особу тільки від оприлюднення приватних фактів та забезпечити відшкодування завданих збитків. Однак коли користувач сам відправляє певні дані на профіль соціальної мережі, дуже важко довести їх приватність і встановити розмір грошової компенсації. Соціальні мережі порушують чимало принципів чесної інформаційної практики, встановлених Організацією еконо-

ISSN 1995-6134

мічного й соціального розвитку (ОЕСР) і визнаних переважною більшістю країн [9]. Зокрема, використання інформації в цих мережах не обмежується зазначеною метою, а обробка інформації є прихованою від суб'єкта даних. Через брак законодавства органи, що здійснюють контроль за додержанням інформаційного законодавства, зокрема за порушення принципів Чесної інформаційної практики, накладати санкції на соціальні мережі не мають права.

До того ж просування законопроектів із питань захисту прайвесі у соціальних мережах викликає потужний спротив із боку самих мереж. Так, у період із квітня по червень 2010 р. Facebook витратив 6600 дол. на лобістську діяльність, аби депутати законодавчих зборів штату Каліфорнія голосували проти прийняття Закону «Про прайвесі у соціальних мережах» [10].

Можна, звісно, піти на радикальні кроки і зробити певні соціальні мережі просто недоступними для користувачів своєї країни, як це нещодавно зробив уряд Узбекистану стосовно Facebook [11], однак такий підхід є недемократичним і мало відповідає сучасним світовим тенденціям. Більш доцільно йти шляхом удосконалення правового регулювання відносин у соціальних мережах, поєднуючи його з іншими видами регуляції.

Так, на загальнодержавному рівні захистити користувачів соціальних мереж намагається уряд Німеччини. У серпні 2010 р. він схвалив законопроект про захист персональних даних найманих працівників. Зокрема, роботодавцям мають намір заборонити перегляд особистих профайлів здобувачів вакансій у соціальних мережах. Заборона не буде поширюватися тільки на пошукову систему Google або професійний сайт Linkedin. Однак експерти вже заздалегідь дійшли висновку, що в разі прийняття такого закону відстежувати його виконання буде вкрай важко.

Водночас кількість користувачів соціальних мереж стрімко збільшується, а отже, питання безпеки й захисту інформації залишаються відкритими. У середньому темпи зростання Facebook за останні півроку складають близько 20 млн. учасників на місяць, а це свідчить про бажання людей дедалі глибше занурюватися у віртуальну реальність. Мережа позбавляє від самотності й створює ілюзію того, що ти є частиною співтовариства, хоча насправді так званими «друзями» стають абсолютно чужі люди, а іноді, як засвідчує практика, – й люди із зовсім недоброзичливими намірами.

У новітній літературі висловлено чимало пропозицій із питань правового захисту прайвесі у соціальних мережах. У Канаді, окремих штатах США та країнах Євросоюзу такого роду законодавство вже діє. Фахівці спільні у тому, що соціальні мережі повинні надавати своїм користувачам конкретні можливості для захисту свого права на приватність і водночас нести юридичну відповідальність перед користувачами за дотримання своєї політики конфіденційності. Соціальні мережі мають забезпечувати, аби користувачі не втрачали свою конфіденційність і контроль над особистою інформацією, що зберігається у постачальника послуг. Користувачі – не товар, і їхні права повинні поважатися. Інновації у сфері соціальних мереж є важливими, але повинні узгоджуватися з правом на прайвесі, а не підривати його, гарантувати недоторканність приватного життя користувачів і їхній контроль за персональними даними.

На підставі тих процесів, що відбуваються сьогодні у соціальних мережах, можемо зробити наступний висновок: у загальному законодавстві про прайвесі або у спеціальних законах про прайвесі у соціальних мережах необхідно закріпити три фундаментальні принципи, дотримання яких могли б вимагати користувачі:

1. Право на прийняття обґрунтованих рішень. Користувачі повинні мати право на зрозумілий користувацький інтерфейс, що дозволить їм зробити свідомий вибір із приводу того, хто може бачити їхні дані та як вони використовуються. Користувачі повинні мати змогу легко побачити, хто має право доступу до тієї чи іншої інформації про них, у

ISSN 1995-6134

т.ч. інші особи, посадові й службові особи органів публічної влади, веб-сайти, рекламодавці та ін. За можливості, соціальна мережа повинна надавати користувачам повідомлення, коли урядова чи приватна установа використовує юридичні чи адміністративні процедури для отримання інформації про них, аби користувачі мали реальну змогу для відповіді.

2. Право на контроль. Соціальні мережі повинні гарантувати, що користувачі зберігають контроль над використанням і розкриттям своїх даних. Соціальна мережа має отримувати тільки обмежене право на використання даних для цілей, для яких вони були первісно надані постачальнику послуг. Коли служба хоче здійснити вторинне використання даних, він має отримати явну відмову від первинного дозволу користувача. Право на контроль включає в себе право користувачів вирішувати, які з їхніх «друзів» можуть дозволяти службі розкривати свої персональні дані стороннім веб-сайтам і додаткам. Соціальні мережі повинні питати дозволу на зміну будь-яких можливостей щодо використання персональних даних. Якщо соціальна мережа додає якісь нові функції, яких користувачі справді бажають, то вона не повинна вдаватися до незрозумілих і таких, що можуть ввести в оману, інтерфейсів, аби змусити людей використовувати його.

3. Право на вихід. Користувачі надають свої дані, і користувачі повинні мати право їх забрати. Одним з основних способів, за допомогою яких користувачі можуть ефективно захистити своє приватне життя, є можливість залишити соціальну мережу, яка недостатньо його захищає. Таким чином, користувач повинен мати право на видалення окремих даних або усього свого облікового запису із соціальної мережі. Мається на увазі дійсно видалення. Для служби недостатньо відключити доступ до даних, продовжуючи зберігати чи використовувати його. Має бути забезпечена можливість повного й остаточного виключення зі серверів служби.

Крім того, якщо користувачі вирішили залишити соціальну мережу, то вони повинні мати змогу легко, ефективно й вільно отримати свої персональні дані від цієї служби і перемістити їх в іншу у зручному форматі. Ця концепція, відома як «портативність даних» або «Data Liberation», має основоположне значення для розвитку конкуренції й забезпечення того, щоб користувачі дійсно зберігали контроль над своєю інформацією, навіть якщо вони розірвали усі зв'язки з конкретною послугою.

Розробка пропозицій щодо спеціального законодавства, яке б стояло на захисті прайвесі в Інтернеті, у тому числі й у соціальних мережах, є перспективним напрямком подальших досліджень у даній сфері.

ЛІТЕРАТУРА

1. Мечетная Н. Общая раздевалка / Н. Мечетная // Корреспондент. – 10.09.2010. – С. 35.

2. Ganslandt M. Social network privacy standards / M. Ganslandt // Talkstandards. – 2010. – august 13 [Електронний ресурс]. – Режим доступу: http://www.talkstandards.com/social-network-privacy-standards.

3. Coppola N. Building trust in virtual teams / N. Coppola, S. Hiltz, N. Rotter // IEEE Transactions on professional communication. – 2004. – Vol. 2 (47). – P. 95–104.

4. Acquisti A. Imagined communities: awareness, information sharing and privacy on the Facebook / A. Acquisti, R. Gross // Proceedings of the 6-th workshop on privacy enhancing technologies. – Cambridge, UK, 2006. – P. 6–12.

5. Dwyer C. Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. Americas Conference on information systems / C. Dwyer, S. Hiltz, K. Passerini // Proceedings of the 13-th Americas conference on information systems, Keystone, Colorado, August 9–12, 2007. – P. 2–9.

6. Lampe C. A face(book) in the crowd: social searching versus social browsing / C. Lampe, N. Ellison, C. Steinfield // Proceedings of the 20-th anniversary conference on computer supported cooperative work. – Banff, Alberta, Canada, 2007. – P. 167–170.

ISSN 1995-6134

7. Solove D. J. Do social networks bring the end of privacy? / D. J. Solove // Scientific American. – 2008. – Vol. 299. – P. 100–106.

8. Who's the bully? // Los Angeles Times. – 2008. – MAY 19.

9. Organisation for Economic Co-operation and Development (OECD). Guidelines on the protection of privacy and transborder flows of personal data [Електронний ресурс]. – Режим доступу: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

10. Van Grove J. Facebook lobbied to kill Social Networking Privacy Act / J. Van Grove // Mashable. – 2010. – October, 27 [Електронний ресурс]. – Режим доступу: http://mashable.com/2010/10/27/facebook-lobbying.

11. Facebook теперь закрыт для жителей Узбекистана [Електронний ресурс]. – Режим доступу: http://www.seoded.com/2010/11/facebook.html.

Серьогін В. О. Соціальні мережі як загроза прайвесі / В. О. Серьогін // Форум права. – 2011. – № 2. – С. 822–827 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2011-2/11cvojzp.pdf

Здійснено спробу системної, розгорнутої характеристики потенційних загроз прайвесі, що містять у собі соціальні мережі. Узагальнено зарубіжний досвід у даній сфері. Зроблено висновок, що у спеціальному законодавстві необхідно закріпити три фундаментальні принципи, дотримання яких могли б вимагати користувачі: право на прийняття обґрунтованих рішень, право на контроль і право на вихід.

***

Серегин В.А. Социальные сети как угроза прайвеси

Предпринята попытка системной, развернутой характеристики потенциальных угроз прайвеси, которые содержат в себе социальные сети. Обобщен зарубежный опыт в данной сфере. Сделан вывод, что в специальном законодательстве необходимо закрепить три фундаментальных принципа, соблюдение которых могли бы требовать пользователи: право на принятие обоснованных решений, право на контроль и право на выход.

***

Seryogin V.A. Social Networks as a Threat to Privacy

Attempted system deployed by the characteristics of potential threats to privacy, which contain a social network. Summarizing the foreign experience in this field is made. Concluded that a special legislation is necessary to consolidate three fundamental principles, compliance with which could require that users: the right to make informed decisions, the right to control and the right to exit.