УДК 342.721:004.738.5
DOI https://doi.org/10.32782/2524-0374/2019-6/17

ЗАХИСТ ПРАВ ЛЮДИНИ В СОЦІАЛЬНИХ МЕРЕЖАХ

PROTECTION OF HUMAN RIGHTS IN SOCIAL NETWORKS

Шевчук А.О., студентка ІІІ курсу факультету адвокатури
Національний юридичний університет імені Ярослава Мудрого

Штонда Д.Д., студентка ІІІ курсу факультету адвокатури
Національний юридичний університет імені Ярослава Мудрого

Здійснено аналіз соціальних мереж як однієї зі структур, яка надає користувачам можливість не тільки взаємодії з іншими користувачами, завантаження інформації на особистий профіль, пошуку однодумців, висловлення своєї точки зору тощо, а й платформи загальнодоступності особистих даних, які поширюють користувачі. Чимало людей заради таких переваг віддають пріоритет Facebook, який є найбільшою світовою соціальною мережею. Проаналізовані питання, чи є вони поінформованими щодо всіх тих особистих даних, які зберігаються у базі соціальних мереж, чи відповідають правові норми національного та міжнародного законодавства викликам сьогодення та обсягу порушуваних прав.

Зроблено висновок, що у спеціальному законодавстві необхідно закріпити три основоположні принципи, за ефективної діяльності яких могли б вимагати користувачі: право на прийняття обґрунтованих рішень, право на контроль і право на вихід.

Встановлюючи національні та міжнародні гарантії, законодавці надають користувачам можливість протидії суспільно шкідливим наслідкам соціальних мереж та відновлення основоположних правових принципів як у кіберпросторі, так і в реальному житті особи.

Проте, незважаючи на всі вищезгадані гарантії, користувач має ретельно ознайомлюватися з власними положеннями соціальних мереж, перевіряти дані, які він надає, та розуміти ризики, пов'язані з витоком, передачею та поширенням його особистих даних у кіберпросторі.

Під час написання роботи були проаналізовані праці українських (В.О. Серьогін) та міжнародних науковців (Michael LaForgia, Matthew Rosenberg, Gabriel J.X. Dance, Brian X. Chen), які досліджували питання кібербезпеки у соціальних мережах; проаналізовані втілення правового регулювання у Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, рекомендаційних посібниках Ради Європи та нормативно-правових актах національного законодавства.

Ключові слова: кібербезпека, права людини, соціальні мережі, Facebook, персональні дані.

Social networks have been analyzed as one of the structures that enables users not only to interact with other users, to download information on their personal profile, to find like-minded people, to express their point of view, etc., but also to the platform of public personal data dissemination by users. Many people give priority to Facebook, which is the world's largest social network. The issues analyzed are whether they have been informed of all personal data stored in the social boundaries, whether the legal rules of national and international law meet the challenges of the present and the volume of violated rights.

It is concluded that in the special legislation it is necessary to establish three basic principles that users could demand for effective activity: the right to make informed decisions, the right to control and the right to exit.

By establishing national and international safeguards, lawmakers empower users to counteract the socially damaging effects of social networks and restore fundamental legal principles, both in cyberspace and in a person's real life.

However, notwithstanding all of the aforementioned safeguards, the user must carefully review his or her social networking provisions, verify the information he or she provides, and understand the risks associated with leaking, transmitting and disseminating his/her personal data in cyberspace.

In writing the work, the works of Ukrainian (V.A. Seryogin) and international scholars (Michael LaForgia, Matthew Rosenberg, Gabriel J.X. Dance, Brian X. Chen) were analyzed, examining the issue of cybersecurity on social networks; the implementation of legal regulation in the Convention for the Protection of Persons in connection with the automated processing of personal data, Council of Europe guides and national legislation are analyzed.

Key words: cyber security, human rights, social networks, Facebook, personal data.

Загальне поняття соціальних мереж (англ. *social networking service*) передбачає вебсайт або іншу вебслужбу, яка відображає соціальні взаємини користувачів у кіберпросторі. Нині соціальні мережі є невід'ємним складником життя кожного українця, адже, згідно з даними міжнародного порталу Statista, 42% користувачів смартфонів відвідують соціальні мережі щонайменше один раз на тиждень (і лише на 1% більше використовують гаджети для дослідження інформації у пошуковій системі). Загальнодоступність, ефективність комунікативних засобів та багато інших функцій та можливостей соціальних мереж значно полегшують наше життя, допомагають вирішувати щоденні задачі, знаходити однодумців, поширювати інформацію на свій розсуд. Чимало людей заради таких переваг віддають пріоритет Facebook, який є найбільшою світовою соціальною мережею. За останніми даними, кількість активних акаунтів по всьому світу налічує більше 2000 мільйонів, 10 з яких є українськими.

Але західні дослідники неодноразово зазначали, що соціальні мережі мають доступ не лише до тієї інформації, яку користувачі надають у загальнодоступне користування, що становить потенційну загрозу їхньому приватному життю. Згідно з дослідженням 45 соціальних мереж, проведеним організацією Physorg у 2009 р., було виявлене «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 неспроможні 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 [4].

Більшість користувачів не здогадуються щодо масштабів розширення меж їхньої конфіденційності у системі соціальних мереж. Серед найпоширеніших ризиків у соціальних мережах варто виокремити принаймні три:

1) повна поінформованість про особу;
2) повідомлення інформації третім особам;
3) відсутність у особи реального контролю за домірністю інформації про себе.

Дії, що завдають шкоди приватності користувачів, можуть бути зведені у чотири групи: збір, обробка, поширення і зберігання персональних даних. Така класифікація допомагає не тільки кваліфікувати певні дії, що завдають шкоди користувачам, а й розробляти заходи щодо попередження шкідливих наслідків та усунення завданої шкоди [4].

Основною дією прийняття умов соціальних мереж є згода, яку користувачі дають під час підключення до послуг як повну згоду на вторинне використання персональних даних. Насправді, користувачі мають мінімальну інформацію і жодного контролю над вторинним використанням, у тому числі продажем чи розкриттям їхньої персональної інформації небажаним групам.

Розробники постійно удосконалюють рівень конфіденційності у соціальних мережах, 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 утворює простір для особи, який, як і інший соціальний простір, потребує захисту прав, дотримання основоположних правових принципів та можливості встановлення справедливості за допомогою правових засобів [4].

Одними з найголовніших функцій права за його призначенням є регулятивна та охоронна. І діяльність користувачів у соціальних мережах, що торкається суспільних відносин, потребує регулювання задля додержання основних гарантій прав і свобод людини. Право та соціальні мережі у тандемі мають забезпечувати конфіденційність користувачів, контроль над особистою інформацією, надавати можливості для захисту своїх прав і водночас нести юридичну відповідальність перед іншими користувачами задля дотримання законності та справедливості.

Найфундаментальнішим національним гарантом додержання права є Конституція України, яка чітко встановлює людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку як найвищу соціальну цінність та встановлює відповідальність держави за свою діяльність з головним обов'язком щодо утвердження і забезпечення прав і свобод людини (ст. 3 КУ).

А у статті 31 закріплена гарантія щодо таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції. Проте є можливими винятки, що можуть бути встановлені лише судом, задля запобігання злочинності чи з'ясуванню істини під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Також Конституція вбачає захист втручання в особисту та сімейну сферу життя, а саме збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини, як зазначено у статті 32.

І однією з найголовніших закріплених гарантій є право на судовий захист щодо спростовування недостовірної інформації про себе і членів своєї сім'ї та вимагання вилучення будь-якої інформації, а також відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Важливим правом користувача у соціальних мережах є право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, що закріплене у статті 34, як право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Але здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Отже, аналізуючи норми Конституції, можна встановити загальні межі прав та свобод користувачів, проте законодавець, визначаючи персональні дані як складник загальних прав і свобод людини, врегулював такі відносини шляхом видання Закону України «Про захист персональних даних».

По-перше, було встановлено особливі вимоги до обробки персональних даних:

Заборону обробки персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних. Проте така заборона не застосовується якщо:

– суб'єкт надає однозначну згоду на обробку таких даних;

– така інформація є необхідною для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

– задля захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

– необхідно обгрунтування, задоволення або захист правової вимоги;

– необхідно в цілях охорони здоров'я, встановлення медичного діагнозу;

– стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом у межах його повноважень, визначених законом;

– стосується даних, які були явно оприлюднені суб'єктом персональних даних [3].

По-друге, закон чітко регламентує такі особисті немайнові права на персональні дані, як:

− право знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

− право отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

− право на доступ до своїх персональних даних;

− право на отримання не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповіді про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

− право пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

− право пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

− право на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

− право на звернення зі скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

– право на застосування засобів правового захисту в разі порушення законодавства про захист персональних даних та інші [3].

Також законодавець встановлює обов'язковість надання повідомлення володільцю про передачу персональних даних третій особі протягом десяти робочих днів, якщо цього вимагають умови його згоди.

Але є винятки щодо:

1) передачі персональних даних за запитами під час виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

2) виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;

3) здійснення обробки персональних даних в історичних, статистичних чи наукових цілях [2].

Проаналізувавши цей перелік, можна переконатись у важливості дотримання принципів права у сфері дискреційних повноважень владних органів.

Одним зі способів захисту у сфері персональних даних є звернення до Уповноваженого Верховної Ради України, основними повноваженнями якого є прийняття пропозицій, скарг та інших звернень фізичних і юридичних осіб з питань захисту персональних даних, розробка рішень за результатами їх розгляду, проведення перевірок володільців або розпорядників персональних даних, видання рекомендацій щодо застосування законодавства цієї сфери, подання пропозицій щодо удосконалення регулювання, складання протоколів про притягнення до адміністративної відповідальності та інші [3].

А саме встановлені державою санкції за порушення прав і свобод у сфері приватного життя закріплені у статтях Особливих частин Кримінального кодексу України (наприклад, штрафи щодо порушення недоторканості приватного життя або порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер) та Кодексу України про адміністративні правопорушення (штрафи, передбачені у статті 188-39 щодо порушення законодавства у сфері захисту персональних даних).

ЛІТЕРАТУРА

1. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

2. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28 січня 1981 року № 108. URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 01.03.2019).

3. Про захист персональних даних : Закон України «Про захист персональних даних» від 1 червня 2010 року. URL: https://zakon.rada.gov.ua/laws/show/ru/2297-17 (дата звернення: 01.03.2019)

4. Серьогін В.О. Соціальні мережі як загроза прайвесі. *Форум права*. 2011. Вип. 2. С. 822–827.