UDC 343.1

Корчагіна Анастасія Миколаївна
аспірант кафедри галузевого права
Херсонський державний університет, Україна

ВИКОРИСТАННЯ ДАНИХ ОТРИМАНИХ ІЗ СОЦІАЛЬНИХ МЕРЕЖ З МЕТОЮ ПОПЕРЕДЖЕННЯ, РОЗСЛІДУВАННЯ І РОЗКРИТТЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Процес глобалізації та інформатизації сучасного світу призвели до того, що отримуючи доступ до нових можливостей, особа стикається з усе більш різноманітними ситуаціями, які є загрозливими її безпеці, свободам, приватному життю. Саме тому актуальним є дослідження соціальних мереж як способу вчинення, попередження та розслідування кримінальних правопорушень.

Головною проблемою, яка виникає при дослідженні значенні інформації, яка міститься в соціальних мережах, полягає в тому, що переважна більшість користувачів в більшості випадків ігнорують потенційну небезпеку та негативні наслідки витоку чи протиправного використання їх персональних даних, які містяться у соціальних мережах. До того ж дані, отримані із облікових записів користувачів соціальних мереж, можуть бути використані не лише для вчинення противоправних дій проти самої особи, але й проти їх близьких осіб чи певних державних інституцій, з якими така особа може мати певні відносини.

Проведене дослідження серед користувачів соціальних мереж дало змогу зробити такі висновки. Більшість користувачів віком 20-35 років мають профілі у Facebook (86, 2%), Instagram (72,4 %), а також ВКонтакте (51,7 %).

При цьому майже 60 % при реєструванні ознайомлювалися із повним текстом згоди на оброблення персональних даних та політикою конфіденційності лише частково. Тобто більше половини користувачів не знають про обсяг персональних даних та пособи їх використання в подальшому. П’ята частина користувачів при наданні прав доступу додаткам (зокрема, доступ

до медіафайлів, динаміків, даних календаря, геолокацій тощо) не перевіряють, які саме дані, обсяг та можливості використання їх компаніями чи передання даної інформації певним органам. Майже 60 % користувачів не беруть до уваги, що деякі ресурси (зокрема, Facebook, Twitter, MySpace тощо) не видаляють повністю їх сторінку та зберігають всю історію користування (медіафайли, листування, коментарі, вподобання, історію запитів тощо), що може бути в подальшому використано як для противоправних дій як щодо самої особи, так і її оточення.

Практика звернення до правоохоронних органів дає можливість зробити висновок, що якщо раніше мали місце переважно факти викрадення та використання персональних даних користувачів, то останнім часом усе більшого поширення набуває відслідковування конкретних користувачів, соціальних та особистих зв'язків, їх політичних, культурних, ідеологічних уподобань чи антипатій.

Так, розширення, які використовують більшість соціальних мереж, можуть бути використані для соціальної дискримінації. Зокрема, інформація з використання кнопки «Like», дає доступ до інтересів, тривалості перебування на тій чи іншій сторінці, переходів з одного сайту на інший. Потім ця інформація використовується для цільової реклами та аналізу поведінки відвідувачів.

Уся отримана інформація зберігається не менше 730 днів згідно з Патріотичним Актом і за необхідності може бути передана спецслужбам США.

Виникає ситуація, коли отримання незаконного доступу до сторінки (а отже і до її активності) може призвести до дискримінації особи в соціальному середовищі та кримінально-карним діянням, наприклад, вимагання (ст. 189 КК України), шахрайство (ст. 190 КК України) тощо. Зокрема коментування від імені особи, схвалення кнопкою ««Like» чи іншими емоційними знаками, репости та поширення дописів на особистих сторінках чи групах можуть скласти певний соціальний портрет особи.

Актуальним в останні роки є поширення інформації, яка містить ознаки публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій (ст. 109 КК України).

Розповсюдження таких матеріалів в соціальних мережах від імені особи може призвести до притягнення її до кримінальної відповідальності та її негативних наслідків.

Проте моніторинг інформації в соціальних мережах може мати і запобіжний характер. Так, варто звернути увагу на можливість використання соціальних мереж для вчинення таких кримінальних злочинів як: доведення до самогубства (ст. 120 КК України), посягання на здоров'я людей під приводом проповідування релігійних віровчень чи виконання релігійних обрядів (ст. 181 КК України), втягнення особи в заняття проституцією або примушування її до зайняття проституцією (ст. 303 КК України), сексуальної експлуатації, втягнення у зайняття жебрацтвом, втягнення у злочинну діяльність, використання у збройних конфліктах тощо.

Своєчасне виявлення випадків використання можливостей соціальних мереж для здійснення зазначених злочинів дає змогу попередити подальші незаконні дії, притягнути до відповідальності винуватих та провести заходи реабілітації постраждалих осіб.

Окрему увагу слід звернути увагу на ст. 182 КК України, яка передбачає кримінальну відповідальність за порушення недоторканності приватного життя, тобто незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації. Такі дані можуть бути одержані, наприклад, із особистих повідомлень, доступ до яких можна одержати отримавши логін та пароль відповідної мережі.

Опитування серед користувачів соціальних мереж показало, що своєчасна зміна паролів відбувається лише коли особа забуває попередній (83 %), а 41% не використовують антивірусні та «антихакерські» програми. Користування

інтернет-магазинами (90% опитуваних), які мають опцію оплати на сайті, використання інтернет-банкінгу, тобто доступ до банківських операцій та рахунків особи, призводять до того, що виникає можливість «витоку» інформації та її використання у злочинних цілях. При цьому третина опитуваних осіб стикалась з шахрайством в інтернеті і 93 % навіть не зверталися до правоохоронних органів для захисту порушених прав, а ті, що зверталися, не отримали належної допомоги.

Отже, інформація, яка міститься в соціальних мережах може мати кримінально-процесуальне значення для виявлення, розкриття і розслідування, попередження кримінальних правопорушень та злочинів. Розвиток програмного забезпечення сприяє підвищенню надійності більшості облікових записів, проте відбувається і зворотна діяльність.

На жаль, українська правоохоронна система неспроможна забезпечити належний рівень захисту від протиправних діянь, пов’язаних із використанням незаконно отриманих даних користувачів соціальних мереж, що зумовлює нагальну необхідність розроблення принципово нових підходів до забезпечення захисту інтересів особи, суспільства та держави у цій сфері.

Список джерел:

1. Німецькі поборники приватності угледіли загрозу в соціальній мережі Facebook, а точніше в улюбленій користувачами кнопці like. URL: http://briz.if.ua/9590.htm (дата звернення – 20.04.2020).
2. Кримінальний кодекс України від 05.04.2001 № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення – 20.04.2020).