

Пімонов Г.П.

Національний університет «Одеська юридична академія»

Здобувач кафедри кримінального права

ПЕРСОНАЛЬНІ ДАНІ ЯК ПРЕДМЕТ КРАДІЖКИ: ЄВРОПЕЙСЬКИЙ ВИМІР

Відомо, що визначення ознак характеристик діянь, що криміналізуються є важливим етапом кримінальної політики, оскільки саме правильне з'ясування характеру діяння завдяки положенням норм вищезазначених нормативно-правових актів та практичному досвіду правозастосовувача, а також точне встановлення спричинених наслідків та інших обов'язкових для певних теоретичних конструкцій складів ознак злочинів (спосіб, місце) дозволить відмежувати вказані діяння від суміжних злочинів, передбачених статтями інших розділів Кримінального кодексу, належним чином виконати покладені на компетентних осіб функції по здійсненню правосуддя та досягти таким чином поставлених цілей.

Саме цьому нашим завданням буде розгляд первинних особистостей такого специфічного діяння як крадіжка персональних даних. З одного боку, персональні дані як невід'ємну якість особистості неможливо викрасти. З другого, - розповсюдження інформаційних технологій зробило за можливе існування віртуальної приватності особистості, посягання на яку здебільшого отримує відповідні кримінально-правові ознаки.

Це комплексне посягання на інформаційну та особисту безпеку людини та громадянина.

Стаття 8 Конвенції «Про захист прав людини і основоположних свобод» особливо підкреслює: «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції» [1]. З цього приводу кримінально-правовий захист посягань на приватність особи сягає особливого значення. Проте Конвенція - це живий механізм, отже характеристики приватності будуть змінюватись залежно

від того, якій рівень аналізу (глобальний чи фрагментарний) буде застосовано.

З точки зору О.П.Горпинюк, ознаки, притаманні приватності (в інформаційному аспекті кримінально-правових відносин України): це певна частина життєдіяльності особи, яка стосується інформації; до цієї інформації особою встановлені межі та умови доступу для інших суб'єктів, в тому числі для держави, її органів та посадових осіб, органів місцевого самоврядування, будь-яких фізичних та юридичних осіб; ці межі та умови доступу стосуються нагромадження, зберігання, впливу і розповсюдження інформації про життя особи [2, с.9].

Інший дослідник цього питання А.В.Пазюк [3, с.5], розглядаючи право на приватність персоніфікованої інформації у глобальному міжнародно-правовому вимірі, з'ясував, що право на приватність персоніфікованої інформації становить складову права на повагу до приватного життя, а не права на доступ до інформації.

Специфіка захисту приватності персоніфікованої інформації обумовлюється необхідністю забезпечення конкуруючих інтересів людини у захисті від несанкціонованого розголошення чи іншого використання персоніфікованої інформації без її відома, а також інтересів держави та інших осіб у використанні персоніфікованої інформації. Це право не є абсолютним і підлягає пропорційному обмеженню на визначених законом підставах, в інтересах забезпечення свободи слова, боротьби із злочинністю тощо. До того ж, за даними дослідника, відсутність загальновизнаних універсальних стандартів міжнародно-правового захисту персоніфікованої інформації обумовлюється розбіжностями у концептуальних підходах до захисту права на приватність персоніфікованої інформації на національному рівні, зокрема, в законодавстві Європейського Союзу та Сполучених Штатів Америки.

Східної позиції підтримуються й інттні дослідники проблеми [4]

При виникненні питання тлумачення приватності Європейський суд з прав людини розглядає факт втручання в приватне життя людини в кожному окремому випадку на предмет відповідності вимогам, зазначеним у ч.2 ст.8 конвенції: органи державної влади не можуть втручатися у здійснення цього права (тобто

передбаченого ч.1 цієї статті), за винятком випадків, коли таке втручання передбачено законом і необхідно в демократичному суспільстві в інтересах національної безпеки та громадського порядку, економічного добробуту країни, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі або захисту прав і свобод інших осіб [5]. У цілому ж як вважає Європейський суд з прав людини (рішення у справі «Костелло Робертс проти Сполученого Королівства», 1993 р), «поняття приватного життя є широким і не може бути визначено вичерпно» [6, 7].

Таке тлумачення положень ст.8 Європейської конвенції базується на двох методологічно значущих положеннях.

Перше. Посягання на втручання в приватне життя розглядаються на предмет порушень лише у випадку подібних зловживань з боку держави та органів державної влади та самоуправління за умов перевищення влади чи службових повноважень, встановлених діючим законодавством з метою забезпечення безпеки суспільства. Відомо прагнення держав щодо розширення тотального електронного контролю над громадянами різних країн. Наприклад, у 2014 році в США було запропоновано прийняти Cyber Information Sharing Act of 2014 (Закон про укріплення кібербезпеки в США за допомогою розширення обміну інформацією про загрози кібербезпеці, а також для інших цілей), завданням якого було б створення мережі державних та приватних пунктів моніторингу загроз кібербезпеці, що певним чином порушує права громадян на приватність [8].

Друге. Враховуючи живий, динамічний характер тлумачення норм Конвенції, ЄСПЛ приходить до висновку про необмеженість характеристик поняття приватного життя жорсткими елементами правових норм, оскільки саме його склад, елементна база, залежать не тільки від характеристик культури суспільства, але й від стану законодавства, особливостей профілактики злочинності та зловживань правом у державі.

Крадіжка персональних даних у найбільш загальному вигляді розглядається як неправомірне використання особистої персональної інформації. Але термін «крадіжка персональних даних», як бачимо, використовується не в усіх юрисдикціях.

Якщо це є типовим для Сполучених штатів, то Великобританія використовує словосполучення «шахрайство з персональною інформацією», деякі інші країни використовують терміни «злочини, пов'язані із посяганням на персональні дані», «взлом рахунку», тощо. Загалом така дефініція охоплює два ключових елементи - об'єкт (дані або документи, що належать потерпілій особі) і дві дії, які необхідні для криміналізації діяння (отримання даних та використання останніх з корисливою метою чи з іншою злочинною метою).

Вважається, що злочинність, пов'язана із крадіжками персональних даних, об'єднує усі види злочинної діяльності у яких персональні дані жертви виступають у якості предмета злочинного посягання чи способу досягнення злочинної мети. Ця позиція частіше усього відстоюється у роботах експертів Комітету ООН по наркотикам та попередженню злочинності, задля яким найбільш адекватний термін для праці виглядає як кримінальне зловживання та фальсифікація персональних даних. Вона також може виражатися у шахрайстві з персональними даними; спробах представлення себе за іншу особу; скоєння відповідних дій за жертву, незалежно жива вона чи мертва; присвоєння імені жертви, формування та використання фіктивної особистості чи загально відомого псевдоніма, що належить іншій особі, тощо)[9].

Отже, найбільш небезпечною тенденцією виглядає прагнення держави через введення, контроль та об'єднання різних реєстрів з персональною інформацією до повної інформаційної контрольованості суспільства. Для нейтралізації цього потрібно.

По-перше, через здійснення правової просвіти та надання правової допомоги громадянам запобігти, попередити та захистити їх право на використання та захист персональної інформації.

По-друге, через здійснення моніторингу використання та захисту персональних даних виявити основні проблеми та порушників права на приватність, а також сприяти вдосконаленню відповідної нормативної бази та практики її застосування.

Література

1. Конвенція «Про захист прав людини і основоположних свобод» Ц^:
http://zakon1.rada.gov.ua/laws/show/995_004
2. Горпинюк О.П. Кримінально-правова охорона інформаційного аспекту приватності в Україні - автореф. дис...канд.юр.наук . Львів, 2011 .
3. Пазюк А.В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації Автореф. дис. . канд.юр наук - 12.00.11 Київ. 2004. 20 с.
4. А.А.Баранов, В.М.Брыжко, Ю.К.Базанов Права человека и защита персональных данных. К., Государственный комитет связи и информатизации Украины, 2000 г. 280 с.
5. Богунов В. Спецслужбы и Google не будут посягать на частную жизнь - люди откажутся от нее сами *Закон і бізнес* № 25 (1115) 22.06—28.06.2013 URL:
http://zib.com.ua/ru/27158-specsluzhbi_i_google_ne_budut_posyagat_na_chastnuyu_zhizn____1.html
6. CASE OF COSTELLO-ROBERTS v. THE UNITED KINGDOM
(Application no. 13134/87) URL:
[http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?N=001-57804#{"itemid":\["001-57804"\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?N=001-57804#{);
7. ECHR Press Unit Factsheet - Data protection - September 2014 -
[електронний ресурс] URL:
http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
8. Cyber Information Sharing Act of 2014 URL:
https://www.feinstein.senate.gov/public/index.cfm/files/serve/?File_id=08de1c1b-446b-478c-84a8-0c3f35963216
9. Handbook on identity related crime: UNDOC - UN, New York, 2012 - 336 p URL:
http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf