Лантух І.С.,
викладач кафедри теорії та історії держави і права Дніпропетровського державного університету внутрішніх справ

ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

Сьогодні кожен розуміє, що з виходом в глобальну мережу можуть виникнути проблеми, пов'язані з порушенням прав людини в процесі використання веб-технологій, в тому числі пов'язані з неналежною поведінкою людей, які діють в межах різних юрисдикцій, правової, політичної та інформаційної культури. Як відзначають дослідники, поява Інтернету не створила набору «нових моделей поведінки» - скоріше, він в значній мірі відтворює колишні моделі. Змінилися лише наслідки такої поведінки і проблеми, пов'язані з його регулюванням.

Станом на сьогодні перед державою і суспільством стоять важливі завдання: визначити і нові права і перспективи розвитку традиційних прав (в тому числі і забезпеченні захисту персональних даних в мережі Інтернет). Запропонувати концептуальні та прийнятні варіанти вирішення цих завдань і проблем, що виникають покликані законодавці, вчені, фахівці в області інформаційно-комунікаційних технологій, і це непросто.

Так, міжнародне визнання важливості проблеми персональних даних було закріплено ще в 1981 році прийняттям країнами Ради Європи Конвенції з захисту даних про особу при автоматизованій обробці інформації. Конвенція виходить з того, що права і інтереси особистості в умовах застосування новітніх інформаційних технологій, комп'ютерних і телекомунікаційних засобів можуть бути порушені в результаті несанкціонованого використання відомостей про особу їй же на шкоду, тим самим, звівши нанівець її природні права, що є основою свободи, справедливості і миру. Зазначені права слід захищати на законодавчому рівні.

В останні десятиліття число користувачів мережі Інтернет збільшилося багаторазово. Велика частина жителів планети так чи інакше використовують «світову павутину», залишаючи в ній свої персональні дані, в тому числі при реєстрації на тих чи інших ресурсу мережі [1, с. 123].

Комплекс заходів по захисту персональних даних включає в себе використання шифрувальних засобів, антивірусного захисту, захисту доступу до інформації індивідуальним паролем, аналіз захищеності, виявлення і запобігання вторгнень, управління доступом, реєстрацію та облік.

Звісно ж необхідно звернути увагу, що при укладенні угоди для користувача більшість компаній, що надають громадянам послуги в мережі Інтер-

нет, не передбачають спеціального отримання згоди суб'єкта на обробку його персональних даних, в той час як отримання такої згоди є необхідним і обов'язковим по ряду підстав.

Ухвалення користувальницької угоди можна розцінювати як укладення договору надання послуг з таких підстав: по-перше, узгоджений предмет договору, як правило, оператор зобов'язується надати користувачеві доступ до своїх сервісів, а користувач зобов'язується дотримуватися режиму користування і приймати рекламні матеріали, що направляються оператором; по-друге, саме врегульовані права і обов'язки сторін в зв'язку з виконанням договору та санкції за порушення встановлених правил; по-третє, передбачені порядок зміни і розірвання договору, а також процедура вирішення виниклих спорів.

Проте в більшості випадків однією з цілей обробки персональних даних користувача є просування товарів і послуг шляхом здійснення прямих контактів з потенційними споживачами за допомогою засобів зв'язку (як правило, таргетована реклама прямо вказана в призначеній для користувача угоді), що покладає на оператора обов'язок отримати попередню згоду суб'єкта персональних даних.

Слід зазначити, що багато рекламних компаній, що пропонують послуги зі створення таргетованої реклами, вказують на відмінність партнерських відносин з провідними поштовими сервісами та сайтами соціальних мереж, які передбачають надання останніми відомостей про користувачів. Передача інформації третім особам також може бути передбачена для користувача угодами конкретних сервісів [1, с. 125].

По-друге, згадка в тексті користувальницьких угод про надання таргетованої реклами часто має на увазі обробку вельми специфічного набору персональних даних, а саме - cookie файлів. Обробка зазначених файлів дозволяє встановити IP-адресу користувача, тип операційної системи, встановленої на комп'ютері, тип браузера, інформацію про відвідування перед цим сайті, іноді - адресу електронної пошти та іншу інформацію [2, с. 188].

Виникає окреме питання про захист персональних даних при користуванні послугами електронної комерції. Здійснюючи онлайн покупки, важливо уважно вивчити сайт на предмет відповідності нормам закону і не варто прив'язувати свою банківську карту до платіжної системи сайту.

Так, в Європейському союзі з метою захисту персональних даних користувачів прийнято Загальний регламент щодо захисту даних (GDPR), прийнятий в травні 2018 року. Одна з ключових особливостей GDPR полягає в тому, що дія цих правил застосовується до компаній, які обробляють персональні дані резидентів і громадян ЄС і явно націлених на таку обробку, незалежно від місцезнаходження такої компанії [3].

Практика залучення європейських компаній до відповідальності за порушення поступово формується: ще в 2018 році в зв'язку з витоком даних і порушенням умови про необхідність зберігання даних користувачів в зашиф-

рованому вигляді на 20 тисяч євро була оштрафована німецька компанія Knuddels GmbH & Co KG (компанія-власник німецького онлайн -чат і сервісу для знайомств Knuddels). За схоже порушення, пов'язане з наданням в недостатній мірі захисту призначених для користувача даних на випадок витоку, на 183 млн фунтів стерлінгів була оштрафована і авіакомпанія British Airways.

Для України в сфері забезпечення прав людини на захист персональних даних в мережі інтернет важливим фактором є підписання Угоди про асоціацію між Україною та Європейським Союзом. Згідно з гл. 14 Угоди про асоціацію сторони зміцнюють своє співробітництво щодо розвитку інформаційного суспільства на користь приватних осіб і бізнесу через забезпечення загальнодоступності ІКТ та через кращу якість послуг за доступними цінами. Це також полегшить доступ до ринків послуг електронних комунікацій, що сприятиме конкуренції та надходженню інвестицій у цю галузь [4].

У висновку хотілося б відзначити, що користувачі мережі Інтернет можуть самі убезпечити свої персональні дані при уважному вивченні сайтів, угоді про обробку персональних даних, уважно стежити за тим, що і кому відправляється в повідомленні, не прив'язувати свої банківські карти до платіжних систем сайтів, як і не довіряти підозрілим сайтам і при виявленні порушень законодавства звертатися до відповідних контролюючих органів.

Оператори сайту також повинні дотримуватися прав власників особистих даних, отримуючи попередню згоду користувача на обробку даних необхідно проінформувати в призначеній для користувача угоді про мету обробки даних, її вигляд, обсяг, строки зберігання, після закінчення яких дані будуть знищені.

Важливо відзначити і той факт, що з поширенням нових технологій необхідно забезпечити більш надійну форму захисту персональних даних як гармонізацією внутрішнього законодавства, так і оперативним законодавчим реагуванням на появу нових загроз.

Використані джерела:

1. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет / М. М. Кравчук // Наукові записки Інституту законодавства Верховної Ради України. – 2013. – № 3. – С. 123-126.

2. Конончук О. Захист персональних даних в умовах соціалізації інтернет-сервісів / О. Конончук // Юридична наука. - 2015. - № 2. - С. 187-193.

3. Загальний регламент захисту даних (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679) щодо захисту персональних даних усіх осіб в межах Європейського Союзу та Європейської економічної зони від 27 квітня 2016 року. - [Електронний ресурс] - Режим доступу: http://yur-gazeta.com/golovna/gdpr-oficiyniy-ukrayinskiy-pereklad.html

4. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом та його державами-членами, з іншої сторони [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/kmu/docs/EA/.