РОЗДІЛ ІІІ. ЦИВІЛЬНЕ ПРАВО ТА ЦИВІЛЬНИЙ ПРОЦЕС; МІЖНАРОДНЕ ПРИВАТНЕ ПРАВО

УДК 342.738:340.134 DOI https://doi.org/10.26661/2616-9444-2019-1-04

Щодо питання правомірності використання біометричних даних особи у цифрову добу

Колодін Д. О., Єременко К. С.

Національний університет «Одеська юридична академія», Фонтанська дорога, 23, м. Одеса, Україна

Ключові слова:
біометричні дані, штучний інтелект, інформаційні технології, правомірність, персональні дані.

Надійшло до редколегії: 02.04.2019
Прийнято до друку: 13.05.2019

У статті досліджуються суспільні відносини щодо питання правомірності та моральності використання державою, соціальними мережами, іншими цифровими технологіями біометричних даних користувача. Авторами висувається теза про те, що у зв'язку зі стрімким розвитком технологій зі збирання та оброблення біометричних даних особи гостро постає питання необхідності законодавчого врегулювання такого роду відносин. Висновком за результатом дослідження стала теза про те, що існуюча вітчизняна нормативно-правова база щодо питання захисту біометричних даних особи є недостатньою, у зв'язку із чим слід, спираючись на закордонний досвід, доповнити її нормами, які б стосувались захисту саме біометричних даних особи.

To the question of the law measures of using the biometric data of the person in the digital epoch

Kolodin D. O., Yeremenko K. S.

National University "Odessa Law Academy", str. Fontanska, 23, Odessa, Ukraine

Key words:
biometric data, artificial intelligence, information technology, lawfulness, personal data.

The article explores social relations on the issue of legality and morality of use by the state, social networks, other digital technologies of biometric data. The problem of using biometric data of the person arose recently – with the development of information technology. The threat to the rights and interests of a wide range of persons arises from the use of personal data of a person for the commission of certain actions which can have legal consequences. For example, in the United States, the term "identity theft" is already used for this kind of offense. But, if we analyze the essence of such a concept, then in fact it is the theft of "identifiable" signs of a person (this includes not only the appearance, fingerprints, the image of the iris of the eye, DNA, as well as emotions, character, peculiarities of the individual's behavior, etc.).
The purpose of the article is to study the problem of using biometric data of a person, namely the possibility of using such information in terms of law and moral principles of society.

The authors put forward the thesis that due to the rapid development of technologies for the collection and processing of biometric data of a person, there is an urgent need for a legislative settlement of this kind of relationship.
Ukraine has now adopted the Law "On Protection of Personal Data", but obviously with the rapid development of technologies, it is necessary to regulate at the legislative level the issues of the person's biometric data and the methods and grounds for their protection.
Analyzing the legislation of Ukraine, it should be noted that Article 2 of the Law of Ukraine "On Protection of Personal Data" of 01.06.2010 stipulates that personal data is the information or set of information about an individual that is identified or can be specifically identified.
The subject of personal data, according to Art. 8 of the specified normative act, has the right: 1) to know about the location of the database of personal data containing his personal data, his purpose and name, the location and / or residence (residence) of the owner or manager of this database, or to give a corresponding order to obtain this information for authorized persons, except in cases established the law; 2) to receive information on the conditions for granting access to personal data, in particular information about third parties to which his personal data is transferred, contained in the appropriate database of personal data; 3) access to their personal data contained in the relevant database of personal data; 4) receive no more than thirty calendar days from the date of receipt of the request, except in cases provided for by law, the answer as to whether his personal data is stored in the appropriate database of personal data, as well as to receive the contents of his personal data which is stored; 5) make a motivated request with a protest against the processing of their personal data by state authorities, local self-government bodies in the exercise of their powers envisaged by law; 6) make a motivated request for the modification or destruction of their personal data by any possessor and manager of this database, if these data are processed illegally or are unreliable; 7) to protect their personal data from unlawful processing and accidental loss, destruction, damage in connection with intentional concealment, failure to provide or untimely provision thereof, as well as protection against providing information that is unreliable or defamatory of honor, dignity and business reputation an individual; 8) apply for the protection of his / her rights regarding personal data to bodies of state power, bodies of local self-government, whose powers consist of the protection of personal data; 9) to apply remedies in case of violation of the legislation on protection of personal data.
The conclusion of the study is the thesis that the existing domestic regulatory framework for the protection of biometric data of a person is insufficient, and therefore, based on international experience, it should be supplemented with norms that would directly regulate the protection of human biometric data.

З розвитком інформаційних технологій викрадення номерів та паролів від банківських карт через перехоплення персональної інформації хакерами – реалії сьогодення. Законодавчі бази багатьох країн світу вже регулюють такого роду правопорушення і встановлюють за них юридичну відповідальність, адже викрадення майна особи однозначно є порушенням її законних прав.

А між тим технології не стоять на місці, і з виходом на нові рівні комфорту та безпеки все одно постають питання доцільності, можливості, правомірності

запровадження тих чи інших інформаційних розроблень у повсякденне життя людини.

Отже, наразі у світі виникла нова загроза: збір біометричних даних людини. Біометричні дані так чи інакше зберігаються у цифровому вигляді і передаються по мережах зв'язку. Якщо вони раптом опиняться в руках хакерів, проблема буде набагато серйознішою, ніж перехоплення номера банківської картки або пароля від інтернет-банку [1]. Карту можна заблокувати і випустити нову, пароль – змінити, а ось біометричні дані людині важко змінити, чи це є зовсім неможливим.

Проблема правомірності використання біометричних даних особи наразі є недостатньо розробленою як на національному рівні, так і у світі. Серед вітчизняних вчених, які вивчали питання використання персональних даних, можна назвати таких, як: Н.С. Кузнєцова, О.В. Кохановська, Є.О. Харитонов, О.І. Харитонова, К.Г. Некіт та ін.

Метою статті є дослідження проблеми використання біометричних даних особи, а саме можливість використання такої інформації з точки зору права та моральних засад суспільства.

Проблема використання біометричних даних особи виникла нещодавно – з розвитком інформаційних технологій. Загроза правам та інтересам широкого кола осіб виникає у зв'язку з використанням особистих даних людини для вчинення тих чи інших дій, які можуть мати юридичні наслідки.

Наприклад, у США для такого роду правопорушення вже застосовується термін «identity theft» (якщо перекладати дослівно – крадіжка особистості). Але, якщо проаналізувати суть такого поняття, то фактично – це викрадення «посвідчувальних» ознак людини (до цього входить не тільки зовнішній вигляд, відбитки пальців, малюнок райдужної оболонки ока, ДНК, а також емоції, характер, особливості поведінки індивіда тощо).

Наразі біометричні дані, які можна отримати найлегше, – це відбитки пальців, які активно використовують власники смартфонів (навіть бюджетних).

Окрім цього, можливо скопіювати зі смартфону голос його володільця, манеру розмови. Почувши фрагмент голосового запису, програми можуть відтворити тембр голосу, переводячи його на будь-яку фразу. Наразі зловмисники активно використовують такі можливості задля, наприклад, вимагання викупу, підставляючи таким чином іншу особу. Більше того, вже виникла можливість відтворення манери набору тексту на комп'ютері (тобто які пальці використовує і з якою силою натискає на які клавіші, з яким інтервалом).

Крім того, використовуються такі біометричні дані, як, наприклад, райдужна оболонка ока. І такий сканер вже застосовується у смартфоні Microsoft Lumia 950.

Слід зазначити, що банкомати CTBC Bank (Тайвань) вже здатні реагувати на риси обличчя та малюнок вен; це використовується замість звичних пластикових карт, сканеру QR-коду або перевірки за номером телефону.

Також цікавим є те, що в Канаді компанія «TD» спільно з «Mastercard» розробила NFC-браслет, який може розпізнати власника рахунку за особливостями його серцебиття та дозволяє здійснювати безконтактні платежі. Браслет працює тільки тоді, коли його носить власник.

Сьогодні відбитки легко «зняти» за допомогою камери високої роздільної здатності на відстані до 6 метрів, що успішно було продемонстровано ще в 2008 році німецькими хакерами: вони роздрукували відбитки пальця міністра внутрішніх справ ФРН, перезняті зі склянки, з якої він пив на прес-конференції. Перенести їх за допомогою лазера на силіконові подушечки і зробити якусь дію «від імені» чиновника (скажімо,

пограбувати ювелірний магазин) – вже простіше простого [2].

Також можливим є злам смартфону та передача біометричних даних хакерам. Так вже були «зламані» смартфони HTC One Max, Samsung Galaxy Note 4, Samsung Galaxy S5 і Galaxy S6, Huawei Mate 8.

А ось випадків масового злому систем на основі сканування райдужної оболонки ока, як у новому Samsung Galaxy Note 7, поки що немає.

Facebook вже давно здійснює аналіз персональних даних для встановлення родинних зв'язків (на основі аналізу лайків, коментарів, хештегів, активності переписки) з метою показу найбільш доцільної реклами користувачам [1]. І як результат, відзначають втрату довіри користувачів до Facebook.

Наведемо яскравий приклад масового контролю владою громадян із використанням новітніх технологій зі збору біометричних даних. Отже, вдається цікавим також зазначити, що на сьогодні в Китаї Синьцзян-Уйгурський автономний район (далі – СУАР) називають найбільшим соціальним експериментом сучасності, місцем, де відпрацьовується, нібито з метою боротьби з тероризмом і екстремізмом, модель встановлення майбутнього тотального електронного та біометричного контролю за населенням [3].

Більше того, ще у 2017 році в рамках «Програми з реєстрації населення» та безкоштовної програми «Медицина для всіх» жителі СУАР були зобов'язані пройти медичний огляд, у ході якого збиралися зразки ДНК, інформація про групу крові, біометричні дані (відбитки пальців, скан райдужної оболонки ока тощо).

Метою таких заходів було створення повної біометричної бази даних кожного мешканця СУАР у віці від 12 до 65 років.

Крім цього, були навіть записані зразки мовлення, тобто була створена голосова база, яка дозволить в подальшому автоматично встановлювати особу за фактом прослуховування будь-якої розмови. Цікаво зауважити, що досвід СУАР поклав початок для створення голосової національної бази в усьому Китаї [3].

У телефони мешканців СУАР також були встановлені додатки, що дозволяють стежити за власником апарату і його активністю в мережі, включаючи всі дані в месенджерах, а також паролі і логіни. Вірніше, всім абонентам були вислані інструкції з установки цього додатка, після чого проводилися вибіркові перевірки на предмет наявності додатків в телефоні. У разі відсутності додатка, за даними місцевих громадських активістів, людину могли затримати на десять діб. Додаток дозволяло відстежувати, які файли переглядає людина на телефоні і пояснювати це тим, що державні органи оцінюють, чи немає в них загрози безпеці держави.

У 2016 році всім, хто користувався зарубіжними месенджерами, в СУАР закривали доступ до Інтернету та мобільного зв'язку.

Громадяни також зобов'язані оснащувати свої автомобілі датчиками, за якими супутники можуть відстежувати пересування машин. Машини без цих систем не можуть бути продані і їх не можна заправити на бензоколонці.

У даному регіоні на сьогодні працює, як мінімум, 40 тисяч камер, оснащених системою розпізнавання облич. У деяких місцях камери розвішані на стовпах через кожні 200 метрів і рутинно ідентифікують людей і номери машин. За деякими даними, камери автоматично повідомляють поліцію, якщо людина, яка викликає інтерес у силових структур, віддаляється від місця проживання або роботи на 300 метрів. Раніше державі треба було показувати свої документи, сьогодні держава без попиту дізнається по обличчю.

Бюджет у СУАР на впровадження IT-інфраструктури, програмне забезпечення та установку камер у регіоні зріс у 5 разів з 2013 року. Сканування і розпізнавання осіб відбувається як на

поліцейських ділянках, так і навіть на бензоколонках або на вході на головну автобусну станцію в Урумчі. За свідченням іноземних журналістів, перед тим як заправити бак машини, мешканцям доводиться підтверджувати свою особистість таким чином [3].

Окрім цього, слід зауважити, що на допиті конгресом США Марка Цукерберга його звинуватили в тому, що Facebook став платформою для наркодилерів. Після цього Facebook розробив штучний інтелект, який виявляє наркодилерів. Зокрема, така програма розпізнає світлини, на яких зображуються наркотики, інформація про купівлю-продаж наркотичних засобів тощо і видаляє їх [1].

Якщо аналізувати законодавство України, то слід зазначити, що стаття 2 Закону України «Про захист персональних даних» від 01.06.2010 р. передбачає, що персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Суб'єкт персональних даних відповідно до ст. 8 зазначеного нормативного акта має право:

1) знати про місцезнаходження бази персональних даних, яка містить його персональні дані, її призначення та найменування, місцезнаходження та / або місце проживання (перебування) володільця чи розпорядника цієї бази або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані, що містяться у відповідній базі персональних даних;

3) на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних;

4) отримувати не пізніш як за тридцять календарних днів із дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи зберігаються його персональні дані у відповідній базі персональних даних, а також отримувати зміст його персональних даних, які зберігаються;

5) пред'являти вмотивовану вимогу із запереченням проти оброблення своїх персональних даних органами державної влади, органами місцевого самоврядування під час здійснення їхніх повноважень, передбачених законом;

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

7) на захист своїх персональних даних від незаконного оброблення 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;

8) звертатися з питань захисту своїх прав щодо персональних даних до органів державної влади, органів місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних [4].

Захист саме персональних даних здійснюється, переважно, за нормами цивільного законодавства, адже найбільш поширеним способом захисту у цьому випадку є відшкодування збитків.

Особа, чиї права було порушено, може застосувати й інші способи захисту прав, передбачені ст. 16 ЦК України, до яких належать:

– визнання права;

– визнання правочину недійсним;

– припинення дії, яка порушує право;

– відновлення становища, яке існувало до порушення;

– примусове виконання обов'язку в натурі;

– зміна правовідношення;

– припинення правовідношення;

– відшкодування збитків та інші способи відшкодування майнової шкоди;

– відшкодування моральної (немайнової) шкоди;

– визнання незаконними рішення, дій чи бездіяльності органу державної влади, органу влади Автономної Республіки Крим або органу місцевого самоврядування, їхніх посадових і службових осіб [5].

При цьому видається за доцільне запровадити спеціальні норми, які б передбачали відповідальність за кожне правопорушення у сфері використання і обігу персональних даних.

За результатами здійсненого дослідження варто зробити висновок, що захист персональних даних набуває важливого значення з огляду на швидкий розвиток новітніх технологій. Наразі в Україні прийнятий Закон України «Про захист персональних даних», але вочевидь зі стрімким розвитком технологій необхідно на законодавчому рівні врегулювати і питання біометричних даних особи та способи і підстави їх захисту. У зв'язку із цим законодавство у сфері охорони і захисту біометричних даних потребує постійного оновлення і вдосконалення, і для цього є можливим використання та застосування закордонного досвіду.

Література

1. Соціальні мережі як чинник інформаційної безпеки : Огляд інтернет-ресурсів. URL : http ://nbuviap.gov.ua/images/sozinfo/2018/20.pdf.
2. В Китае разработали систему цифрового контроля за населением. URL : https ://rusimperia.org/tag/totalnyj-kontrol/.
3. Кража личности : как преступники охотятся за биометрическими данными. URL : https ://rusimperia.org/tag/totalnyj-kontrol/.
4. Про захист персональних даних : Закон України № 2297-VI віл 30.01.2018 р. URL : https ://zakon.rada.gov.ua/laws/show/2297-17.
5. Цивільний кодекс України від 16 січня 2003 року № 435-IV. *Відомості Верховної Ради України (ВВР)*. 2003. № № 40-44. Ст. 356.

References

1. "Social Networking as an Information Security Factor : An Overview of Internet Resources", available at : http ://nbuviap.gov.ua/images/sozinfo/2018/20.pdf.
2. "China has developed a system of digital population contro", available at : https ://rusimperia.org/tag/totalnyj-kontrol/.
3. "Theft of personality : how criminals hunt for biometric data", available at : https ://rusimperia.org/tag/totalnyj-kontrol/.
4. (2010), "On protection of personal : Law of Ukraine", available at : https ://zakon.rada.gov.ua/laws/show/2297-17.
5. (2003), "Civil Code of Ukraine". 16.01.2003. № 435-IV, *Vidomosti Verkhovnoyi Rady Ukrayiny*, no. 40-44, art. 356.