УДК 342.9

Колодін Д.О.,
к.ю.н., доцент, доцент кафедри кримінального права,
декан факультету цивільної та господарської юстиції
Національний університет «Одеська юридична академія»

Єременко К.С., магістр права

ПРАВОВИЙ АСПЕКТ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ДАНИХ ОСОБИ

THE LEGAL ASPECT OF THE REGULATION OF THE USE OF BIOMETRIC DATA OF A PERSON

В статті досліджуються суспільні відносини щодо питання використання біометричних даних особи. Авторами розглянутий зарубіжний досвід щодо законодавчого регулювання даного питання та зроблений акцент на необхідності спонукання ІТ-компаній та розробників програмного забезпечення по збиранню та обробці персональних даних до саморегулювання та підвищення надійності збереження такого роду персональної інформації. Висновком за результатом дослідження авторами зроблений висновок про те, що у вирішення питання відшкодування шкоди за неправомірне використання біометричних даних особи слід відкидати аргументи компаній щодо, наприклад, необхідності доведення настання шкоди або інших негативних наслідків і захищати інтереси споживачів
Ключові слова: біометричні дані, штучний інтелект, інформаційні технології, правомірність використання, персональні дані.

В статье исследуются общественные отношения по вопросу использования биометрических данных человека. Авторами рассмотрен зарубежный опыт законодательного регулирования данного вопроса и сделан акцент на необходимости побуждения ИТ-компаний и разработчиков программного обеспечения по сбору и обработке персональных данных к саморегулированию и повышения надежности сохранения такого рода персональной информации. Заключением по результатам исследования авторами сделан вывод о том, что в решении вопроса возмещения вреда за неправомерное использование биометрических данных человека следует отбрасывать аргументы компаний по, например, необходимости доказывания наступления вреда или других негативных последствий и защищать интересы потребителей
Ключевые слова: биометрические данные, искусственный интеллект, информационные технологии, правомерность использования, персональные данные.

Almost every discussion of the social consequences of the collection and use of biometric data begins with the confidentiality of such information. Biometric information is part of individual identity, and the loss of control over this information may endanger human freedom.

The article explores public relations on the use of human biometric data. The development of advanced technologies and the widespread use of biometric data leads to the need for detailed legal regulation of the relevant public relations in order to ensure the protection and protection of the rights and legitimate interests of individuals and legal entities.

The authors reviewed the foreign experience of legislative regulation of this issue and focused on the need to encourage IT companies and software developers to collect and process personal data to self-regulation and improve the reliability of preserving this kind of personal information. A company that guarantees high biometric data protection will have a market advantage. Another way of protecting a person's biometric data may be to conclude an agreement under which the company guarantees the preservation of such confidential information and is liable in the event of access to it by third parties.

Law creation concerns the creation of legal measures to combat malicious use of biometric data of a person (fraud by using biometric features belonging to another person, changing biometric references or using counterfeit biometric samples to personalize a person).

The conclusion of the study, the authors concluded that in addressing the issue of compensation for unlawful use of human biometric data should discard the company's arguments on, for example, the need to prove the occurrence of harm or other negative consequences and protect the interests of consumers.
Key words: biometric data, artificial intelligence, information technology, legitimacy of the use, personal data.

Постановка проблеми. Розвиток новітніх технологій і широке використання біометричних даних призводять до необхідності детальної правової регламентації відповідних суспільних відносин з метою забезпечення охорони і захисту прав і законних інтересів фізичних і юридичних осіб.

Серед важливих проблем, які потребують якнайшвидшого вирішення, є такі, як забезпечення надійного захисту біометричних даних від неправомірного використання, порядок відновлення втрачених або вкрадених біометричних даних, максимальне збереження приватності осіб, чиї біометричні дані містяться в офіційних базах даних.

Незважаючи на всю важливість питання захисту біометричної інформацію про особу, законодавство більшості країн світу наразі не містить правових норм, які б забезпечували належний рівень захисту біометричних даних. Відповідно, наукове осмислення досліджуваної проблематики та розробка пропозицій до чинного законодавства у сфері захисту біометричних даних набувають особливого значення.

Стан дослідження теми. Проблема правового регулювання відносин, що виникають з приводу використання біометричних даних, є недостатньо розробленою в правовій доктрині. Окремими аспектами використання персональних даних в Україні займались наступні науковці: Н.С. Кузнєцова, О.В. Кохановська, Є.О. Харитонов, О.І. Харитонова, К.Г. Некіт та інші.

Мета статті. Метою статті є дослідження особливостей правової охорони і захисту біометричних даних особи.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів.

Створення ефективних правових засобів для боротьби зі зловмисним використанням біометричних даних особи (шахрайство шляхом використання біометричних ознак, які належать іншій особі; зміна біометричних посилань або використання підроблених біометричних зразків для персоналізації особи тощо) належить до компетенції правотворчих органів.

Втім, важливо не тільки створювати належну нормативно-правову базу, яка буде стримувати правопорушників, але й спонукати розробників програмного забезпечення створювати потужніші ступені захисту інформації (тобто програма, що використовує біометричні дані особи, повинна бути максимально захищена від шахрайства або помилок).

Таким чином, важливо, щоб політика держави у сфері новітніх технологій була спрямована на захист біометричних даних особи, а також на охорону цих даних (превентивні заходи). Зокрема, варто створити умови, за яких власники комп'ютерних систем створюватимуть середовище, яке мінімізує можливості для зловживання біометричними зразками особи.

Таким чином, надійність використання і убезпечення біометричних даних від протиправного використання мають бути абсолютними.

Що стосується правосуддя, то судді також повинні бути абсолютно впевнені в достовірності біометричних даних. Таким чином буде гарантовано неможливість

притягнення до юридичної відповідальності невинної особи.

Достовірність біометричних даних має важливе значення і для інших правоохоронних органів. Зокрема, спеціальні служби, що можуть вести розслідування терористичної діяльності і обґрунтовувати обвинувачення біометричними даними (наприклад, аналізом голосу), повинні бути впевнені, що затриманий є терористом, а не випадковою особою. При цьому, біометричні дані можуть бути достатньою підставою для початку розслідування, але недостатніми, щоб притягнути особу до відповідальності.

Практично кожне обговорення соціальних наслідків збору і використання біометричних даних починається з питання конфіденційності такої інформації. Біометрична інформація є частиною індивідуальної ідентичності, а втрата контролю над цією інформацією може загрожувати свободі людини.

Наразі, на жаль, не існує єдиного набору правил, який би гарантував, що система збору біометричних даних повністю захищає конфіденційність. Натомість, є можливим, на даному етапі, сформулювати політику державних та наддержавних утворень щодо реагування на конкретні ситуації і оцінити їх життєздатність з плином часу. За умови належного правового регулювання відповідних відносин сучасні біометричні технології не загрожують конфіденційності персональних даних особи.

Неспроможність уряду захищати особисту інформацію може призвести до зловживання інформацією, може нашкодити свободі слова тощо, і неможливість мати основу для отримання інформації може призвести до необґрунтованого пошуку та вилучення такої інформації, а також до дискримінації.

Звертаючись до іноземної судової практики, слід зазначити справу Верховного суду США «Whalen проти Roe», в якій суддя зазначив про загрозу конфіденційності, яку можуть містити бази біометричних даних: «І що тоді вже казати про інформацію, що зберігається в приватних руках? Багато громадян так само стурбовані, коли надають інформацію роботодавцю або укладають приватні угоди онлайн.

Сьогодні банки активно запроваджують банкомати, оснащені сканерами відбитків пальців замість звичних нам паролів. Банки вважають, що це підвищує конфіденційність, оскільки пароль може бути легко вкрадений.

Але якщо база даних відбитків пальців банку не забезпечена належним захистом, цілеспрямоване або випадкове розкриття цих даних може призвести до крадіжки біометричних даних клієнтів» [1].

Окрім цього, в США поширюється практика щодо доступу до інформації про здоров'я працівника задля створення безпечного робочого місця. У разі викрадення таких даних ця інформація може бути неправомірно використана страховими компаніями тощо [2].

Порушення конфіденційності приватною організацією, включаючи конфіденційність біометричної інформації, є неприпустимим і має бути може бути захищене законодавством. Крім того, дієвим механізмом захисту біометричних даних може стати саморегуляція. Компанія, яка гарантує високий захист біометричних даних, буде мати ринкову перевагу.

Іншим способом захисту біометричних даних особи може бути укладання договору, за яким компанія гарантує збереження такої конфіденційної інформації і несе відповідальність в разі доступу до неї третіх осіб.

Також зазначимо, що у січні цього року Верховний суд штату Іллінойс (США) прийняв важливе рішення, яким приватним компаніям забороняють збирати біометричні дані людей, включаючи технологію сканування та розпізнавання обличь, відбитків пальців тощо без надання письмового пояснення того, що вони планують робити з даними та отриманням згоди такої особи на конкретні дії [3].

Вже більше 10 років в штаті Іллінойс існує закон, який має назву Закон «Про конфіденційність біометричної інформації» (англ. – Biometric Information Privacy Act; далі скор.– BIPA). Цей закон створив надійний інструмент захисту біометричних даних особи, зібраних в штаті Іллінойс від їх прихованого збору, використання та перепродажу [4].

BIPA дозволяє будь-якій постраждалій від порушення особі застосовувати його положення щодо відшкодування шкоди в грошовій або в будь-якій іншій формі. Відповідачі у такого роду справах, наприклад, підприємства, які прагнуть збирати біометричні дані – у тому числі технологічні гіганти Facebook, Google і Amazon – стверджували, що особу в такій справі може бути визнано потерпілою лише якщо вона зможе довести, що зазнала збитків.

Проте Верховний суд Іллінойсу постановив, що особа не повинна доводити наявність збитків для того, щоб отримати можливість захищати свої права в судовому порядку.

Отже, наразі в Сполучених Штатах не існує єдиного федерального закону, що регулює збір та використання біометричних даних. Проте окремі штати здійснюють законотворчу діяльність в цьому напрямку. Зокрема, Вашингтон, після Іллінойсу та Техасу, у 2017 році прийняв закон про біометричну конфіденційність. У кінці 2018 року Каліфорнія також прийняла законодавчий акт про захист біометричних даних [5].

А у серпні 2017 року Верховний суд Індії визнав конфіденційність «фундаментальним правом», що свідчить про те, що захист біометричних даних зараз знаходиться на вершині порядку денного у найбільших демократіях світу [4].

Законодавство ЄС про захист даних визначає біометричні дані як спеціальні категорії персональних даних і забороняє їх обробку, тим самим захищаючи людей від надання такої інформації без їхньої згоди.

Таким чином, зазначимо, що біометричні дані – це «персональні дані, які є результатом специфічної технічної обробки, що стосується фізичних, фізіологічних або поведінкових характеристик фізичної особи, що дозволяє підтвердити унікальну ідентифікацію цієї фізичної особи, наприклад, зображення обличчя або дактилоскопічні дані».

Їх обробка в країнах ЄС з метою однозначної ідентифікації фізичної особи заборонена.

Однак законодавство містить деякі винятки:

- Якщо згода явно вказана;
- Якщо біометрична інформація необхідна для виконання зобов'язань суб'єкта даних у сфері працевлаштування, соціального захисту;
- Якщо це необхідно для захисту життєвих інтересів особи, і він / вона не здатний давати згоду;
- Якщо це необхідно з міркувань суспільного інтересу в галузі охорони здоров'я.

Крім того, Регламент дозволяє державам-членам вводити інші обмеження щодо обробки біометричної інформації.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Отже, за результатами здійсненого дослідження варто зробити висновок, що масштабні порушення конфіденційності сьогодні стали звичайним явищем. Інколи потерпіла особа практично позбавлена можливості захистити свої права у випадку неправомірного використання конфіденційних біометричних даних про неї.

В епоху, коли недобросовісні юридичні і фізичні особи мають більші можливості накопичувати та монетизувати персональні дані людей, надзвичайно важливо, щоб законодавчі органи створили дієві закони, які захищали б право людей на конфіденційність біометричних даних. При створенні таких нормативно-правових актів законодавцям слід виходити з того, що неправомірне використання біометричних даних людини є правопорушенням з усіченим складом, тобто потерпіла особа не повинна доводити наявність негативних наслідків для себе. Також слід дотримуватися балансу між інтересами компаній, які використовують біометричні дані, і споживачами, чиї права можуть бути порушені.

ЛІТЕРАТУРА

1. WHALEN v. ROE (1977) No. 75-839 // United States Supreme Court. 2019. URL: https://caselaw.findlaw.com/us-supreme-court/429/589.html.
2. Biometric Recognition: Challenges and Opportunities. // Washington (DC): National Academies Press (US). 2010. URL: https://www.ncbi.nlm.nih.gov/books/NBK219893/.
3. Nathan Freed Wessler «Ruling Is a Warning to Companies Collecting Biometric Scans Without Permission» // ACLU. 2019. URL: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/ruling-warning-companies-collecting-biometric.
4. Biometric Information Privacy Act // Wikipedia. 2008. URL: https://en.wikipedia.org/wiki/Biometric_Information_Privacy_Act.
5. Biometric data and data protection regulations (GDPR and CCPA). 2019. URL: https://www.gemalto.com/govt/biometrics/biometric-data.