УДК 343.98
DOI https://doi.org/10.32850/LB2414-4207.2020.16.35

ОКРЕМІ АСПЕКТИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ПЕРСОНАЛЬНИХ ДАНИХ У ПРОФІЛАКТИЦІ ПРАВОПОРУШЕНЬ

Савельєва Ірина Валеріївна,
старший викладач кафедри
професійних та спеціальних дисциплін
(Херсонський факультет
Одеського державного університету
внутрішніх справ, м. Херсон, Україна)

Стратонов Василь Миколайович,
доктор юридичних наук, професор,
професор кафедри галузевого права
(Херсонський державний університет,
м. Херсон, Україна)

Статтю присвячено використанню біометричних персональних даних у профілактиці правопорушень.

Автор аналізує чинне міжнародне та національне законодавство щодо визначення складу біометричних персональних даних, їх класифікації.

У статті подано детальний порівняльний аналіз особливостей використання біометричних персональних даних державними органами та приватними особами при провадженні статутної діяльності.

Визначено сфери використання окремих видів біометричних персональних даних для профілактики дисциплінарних, адміністративних та кримінальних правопорушень. Автор наголошує, що сьогодні надзвичайною загрозою є витоки та отримання доступу до біометричних даних сторонніх осіб.

Проведено аналіз міжнародного законодавства та законодавства зарубіжних країн у галузі захисту персональних біометричних даних, зокрема Сполучених Штатів Америки, Російської Федерації, Канади тощо.

Розглянуто судову практику різних країн щодо неналежного збору, обробки, зберігання та використання біометричних персональних даних.

Зроблено висновок, що збір, обробка та використання біометричних персональних даних із метою профілактики правопорушень повинні відповідати певним вимогам. По-перше, власником бази біометричних персональних даних має бути тільки держава в особі спеціального державного органу. Відповідно, держава має забезпечувати зберігання і захист біометричних персональних даних. По-друге, фізично носії (сервери), на яких зберігається база з біометричними персональними даними, повинні розміщуватись на території держави, адже це є питанням національної безпеки. По-третє, держава може надавати можливість використовувати обмежену кількість біометричних персональних даних приватним особам для здійснення їх статутної діяльності тільки за письмової згоди осіб, яких такі дані ідентифікують, та без змоги їх копіювання і накопичення.

Ключові слова: профілактика правопорушень, біометричні персональні дані, голос, відбитки пальців.

CERTAIN ASPECTS OF THE USE OF BIOMETRIC PERSONAL DATA IN OFFENSE PREVENTION

Savelieva Iryna Valeriivna,
Senior Lecturer at the Department of Professional and Special Disciplines (Kherson Faculty of the Odesa State University of Internal Affairs, Kherson, Ukraine)

Stratonov Vasil Mikolayovich,
Doctor of Law, Professor, Professor at the Department of Branch Law (Kherson State University, Kherson, Ukraine)

The article is devoted to the use of biometric personal data in crime prevention.

The author analyzes the current international and national legislation on determining the composition of biometric personal data, their classification.

The article presents a detailed comparative analysis of the features of the use of biometric personal data by government agencies and individuals in carrying out statutory activities.

Areas of use of certain types of biometric personal data for the prevention of disciplinary, administrative, and criminal offenses are identified. The author emphasizes that today the leakage and access to biometric data of third parties is an extreme threat.

The analysis of the international legislation and the legislation of foreign countries in the field of protection of personal biometric data, in particular the United States of America, the Russian Federation, Canada, etc. is carried out.

The case law of different countries on improper collection, processing, storage, and use of biometric personal data is considered.

It is concluded that the collection, processing, and use of biometric personal data for the prevention of offenses must meet the following requirements: first, the owner of the biometric personal database should be only the state represented by a special state body. Accordingly, the state must ensure the storage and protection of biometric personal data. Secondly, physically, the media (servers) on which the database with biometric personal data is stored must be located on the territory of the state, because this is a matter of national security. Third, the state may allow a limited amount of biometric personal data to be used by individuals to carry out their statutory activities only with the written consent of the persons identified by such data and without the possibility of copying and accumulating them.

Key words: crime prevention, biometric personal data, voice, fingerprints.

Постановка проблеми. Дотримання законності та підтримання правопорядку в суспільстві залишається однією з найважливіших функцій демократичної держави. Система державних органів та приватні особи вживають найрізноманітніших заходів із попередження правопорушень у різних сферах соціально-економічного та суспільно-політичного життя. Розвиток технічних засобів та поширення диджиталізації призводить до їх використання в профілактичній діяльності. На перший план висуваються дані про особу, які дозволяють її ідентифікувати, тобто персональні дані. Проте така діяльність містить не лише безперечну користь, але й потенційні загрози правам і свободам людини. Тому необхідно розробити

врівноважений механізм їх використання з максимальною ефективністю та мінімізацією ризиків.

Актуальність теми дослідження зумовлена двома аспектами. По-перше, активною законотворчою діяльністю в цьому напрямі в Україні та світі. Так, протягом кількох останніх років унесено зміни до законів України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» та «Про захист персональних даних». У 2017 р. постановою КМУ від 27.12.2017 р. № 1073 затверджено Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства, а у 2018 р. наказом МВС України від 23.11.2018 р. № 944 затверджено Інструкцію про порядок фіксації біометричних даних (параметрів) іноземців та осіб без громадянства посадовими особами Державної міграційної служби України, її територіальних органів і територіальних підрозділів. У Європі з 25.05.2018 р. почав діяти GDPR (The General Data Protection Regulation, 2016/Загальний регламент захисту даних для європейських держав-членів). У США з 01.01.2020 р. набув чинності CCPA (California Consumer Privacy Act, 2018/Каліфорнійський закон про конфіденційність споживачів).

По-друге, це зумовлено великою кількістю правопорушень у цій галузі. Тільки протягом 2017–2020 рр. зафіксовано понад 20 масштабних витоків персональних даних мільйонів осіб. При цьому власниками баз персональних даних були як державні установи, так і приватні.

Аналіз наукових джерел. Загальнотеоретичні питання використання персональних даних розглядають В. Брижко, Т. Єфременко, В. Іщейнов, А. Кучеренко, М. Лушніков та інші. Проте комплексні дослідження з окресленого питання в українській юридичній науці відсутні, що ускладнює розроблення врівноваженого механізму використання біометричних персональних даних, зважаючи на національне та міжнародне законодавство.

Виклад основного матеріалу дослідження. Персональні дані є різноманітною за змістом та єдиною за походженням інформацією, яка описує особу як єдину біологічну й соціальну динамічну систему. Одним із підвидів персональних даних є біометричні. Їх широко використовують для перевірки особи (ідентифікації) з метою надання права доступу до гаджетів, офісних та виробничих приміщень, транспортних засобів та інформації з обмеженим доступом, для здійснення платежів, для перетину державних кордонів та отримання фінансових послуг. Тому збір, використання та обробка біометричних даних уже давно увійшли до нашого життя.

Міжнародне законодавство зараховує біометричні персональні дані до категорії «вразливих», тобто таких, неналежне користування якими призводить до порушення прав і свобод людини.

Ст. 6 Конвенції № 108 Ради Європи передбачає, що такі відомості не повинні оброблятися автоматично, якщо в національному законодавстві не передбачені достатні гарантії їх захисту. Положення Ради Європи роз'яснює, що згадана ст. 6 Конвенції не містить вичерпного переліку «вразливих» персональних даних у цілому та біометричних персональних даних зокрема [1, с. 28].

Національне українське законодавство визначає біометричні дані як сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та суттєво відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри, а саме: відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук) [2]. Біометричні дані характеризуються біометричними параметрами, які є вимірювальними фізичними характеристиками

або особистісними поведінковими рисами, які використовуються для ідентифікації (впізнання) особи або верифікації наданої ідентифікаційної інформації про особу.

У вузькому розумінні до біометричних даних належить відбиток пальця людини, райдужної оболонки ока або сітківки, особливості кінцівок, обличчя, вуха, відбиток язика, голос, розташування вен, дезоксирибонуклеїнова кислота (далі – ДНК), електрокардіографія, підпис.

У широкому розумінні до складу біометричних даних належить також поведінка людини (особливості, які можна виокремити): фізичні рухи (спосіб ходи), сила/швидкість натискання на екран, клавіатуру; спосіб, яким індивідуум вводить дані (пальцем (яким саме), стилусом), як утримує пристрій (наприклад кут нахилу телефона) тощо [3, с. 92].

Особливий статус біометричних персональних даних зумовлюється також неможливістю їх змінити, на відміну від інших персональних даних [4]. Так, можна змінити ім'я та прізвище, паспортні дані, адресу проживання та телефонний номер. У деяких випадках навіть дата та місце народження та ідентифікаційний номер платника податків підлягає заміні. Однак відбитки пальців, розташування вен, ДНК та голос змінити не можна. Тому саме біометричні персональні дані потребують особливого порядку збору, обробки та зберігання.

Біометричні персональні дані є частиною самої особи, яку можна «зчитати» та зафіксувати, тому немає ризику забути їх або втратити. Оскільки вони унікальні, то їх не можна замінити. Отже, якщо біометричні дані були порушені, то це може призвести до руйнування соціального життя окремої людини.

Рівень безпеки зазначених біометричних даних є пропорційним рівню безпеки їх захисту з боку власника та розпорядника бази даних. На нашу думку, зберігання біометричних персональних даних шляхом їх розподілу в різних місцях, а також багаторівневий спосіб автентифікації особи для надання прав доступу є необхідними умовами убезпечення таких даних.

За останні кілька років зафіксовано масштабні витоки персональних даних по всьому світу: у мережах супермаркетів Morrisons (штраф у розмірі 10,5 тис. фунтів стерлінгів), British Airways (штраф у розмірі 183 млн фунтів), витік даних 500 млн користувачів Marriott у листопаді 2018 р., Нова Пошта (навесні 2018 р. було повідомлено про витік скріншотів бази паспортних даних клієнтів, однак позапланова перевірка не знайшла доказів), Uber у грудні 2017 р. (компанія заплатила викуп у розмірі 100 тис. доларів за нерозголошення даних).

У 2017 р. витік персональних даних стався в найбільшому банку України, а в 2018 р. – у найпопулярнішій у світі соціальній мережі, найпоширенішій службі таксі й найбільшому сервісі доставки в Україні [5].

Дослідник із цифрової безпеки Джон Ветінгтон (John Wethington) знайшов китайську базу даних Smart City, доступну з веббраузера без пароля. Ця база даних містила гігабайти інформації, зокрема дані розпізнавання облич сотень людей. Дані були розміщені на хмарній платформі китайського технологічного гіганта Alibaba [6].

Федеральне бюро розслідувань заарештувало 33-річну програмістку Пейдж Томпсон. Її підозрюють у крадіжці даних 106 мільйонів користувачів американського банку Capital One, зокрема громадян США і Канади [7].

Відомі компанії з різних секторів економіки також стають об'єктами хакерських атак із викраденням персональних даних, наприклад Facebook Inc. (існує вже багато справ, в одній із яких штраф становить 5 млрд доларів). Там містилися дані 133 млн користувачів із США, 18 млн – із Великої Британії і 50 млн – із В'єтнаму [8]. Також мали витоки персональних даних Toyota і Lexus (хакери у березні 2019 р. викрали

інформацію про власників автівок), Suprema Biostar (серпень 2019 р.), Mastercard (серпень 2019 р.), Habr.com (серпень 2019 р.), Yves Rocher (вересень 2019 р.), Даримакс (Російська Федерація, вересень 2019 р.), Novaestrat (витік даних про майже всіх жителів Еквадору, вересень 2019 р.) та багато інших.

Тому особливо актуальним є питання зберігання та обробки біометричних персональних даних.

Звернемо увагу на судову практику в таких справах.

У 2019 р. власник фітнес-клубу в м. Казань (Російська Федерація) оспорював в суді постанову Роскомнагляду про накладення штрафу в розмірі 10 тис. рублів за використання Системи контролю і управління доступом для ідентифікації відвідувачів за фотографією при проході через турнікет без особистої письмової згоди. Суд не задовольнив скаргу, посилаючись на те, що фото є біометричними персональними даними і на їх використання необхідна письмова згода власника [9].

Постанова Верховного суду штату Іллінойс (США) від 25.01.2019 р. у справі корпорації Rosenbach v. Six Flags Entertainment Corporation підтвердила необхідність письмової згоди на збір та обробку біометричних персональних даних. У цій справі батьки неповнолітньої дитини подали позов до суду на парк розваг Six Flags Great America. Вони стверджували, що біометричні дані дитини збирали без згоди та порушували BIPA (здійснення біометричного сканування на турнікеті для запобігання шахрайству та надання можливості доступу у разі втрати квитка). Верховний суд штату Іллінойс вирішив, що Six Flags Entertainment Corporation порушили BIPA. У рішенні суду зроблено висновок про те , що не потрібно доводити завдання шкоди, а достатньо вже того, що збір був неправильним.

Біометричні персональні дані зараз широко використовуються в банківській сфері, у сфері надання фінансових послуг та проведення розрахунків за надані послуги. Так, із 2015 р. до 2020 р. проект «Долоньки» (Російська Федерація) зібрав дані про будову вен долонь десятків тисяч російських дітей для використання в системі оплати за харчування в школі. Незважаючи на 5-річний термін існування проекту, дотепер немає єдиної думки (навіть серед представників державних органів) щодо легальності всіх аспектів такої діяльності.

Є перші спроби використання відбитків пальців для реєстрації робочого часу працівника в приватних компаніях. Таким чином намагаються підтримувати робочу дисципліну, адже відбиток пальця – не картка, його не можна передати іншій особі, щоб вона пройшла реєстрацію.

Банки дедалі більше інвестують у нові технології: машинне навчання; повідомлення про шахрайство в режимі реального часу; розпізнавання голосу, обличчя та відбитків пальців (біометричні дані), а також так звані «поведінкові біометричні дані», які включають профілі взаємодії клієнтів із пристроями та засобами інтернет-банкінгу.

Із 2018 р. Центробанк (Російська Федерація) почав збирати біометричні персональні дані для ідентифікації осіб при наданні фінансових послуг. Ці дані заносяться до Єдиної біометричної системи, а збираються багатьма банківськими установами.

Із 2019 р. ПриватБанк (Україна) запустив технологію оплати за допомогою обличчя – FacePay24 [10].

На протидію кіберзлочинці створили ринок цифрових відбитків пальців, а шахраї навчилися записувати та відтворювати голоси клієнтів, використовуючи нові технології [11, с. 174].

Аналіз чинного законодавства України дозволяє зробити висновок, що наше законодавство значно вужче захищає права українців порівняно з CCPA, BIPA і GDPR, тому, як наслідок, можливі зловживання.

Порушення українського національного законодавства щодо правил поводження з біометричними персональними даними зумовлює адміністративну та кримінальну відповідальність.

Важливим здобутком GDPR є закріплення «права на забуття». Згідно з ним, суб'єкт біометричних персональних даних має право відкликати свою згоду в будь-який час. Наслідком відкликання такої згоди за національним законодавством може бути «архівація» таких даних без можливості подальшого використання або ж видалення з бази даних.

У квітні 2020 р. Європарламент схвалив створення однієї з найбільших у світі біометричної бази даних. Вона матиме назву «Common Identity Repository» (CIR) і буде містити записи про понад 350 млн осіб.

Найбільша біометрична база даних у світі на даний момент створена в Індії (до неї входять дані про понад 90% населення країни, а біометрія використовується всюди) – UIDAI (Unique Identification Authority of India). Кожній особі присвоюється унікальний персональний номер – AADHHAAR.

На нашу думку, збір, обробка та використання біометричних персональних даних із метою профілактики правопорушень повинні відповідати таким вимогам:

1) власником бази біометричних персональних даних має бути тільки держава в особі спеціального державного органу. Відповідно, держава має забезпечувати зберігання і захист біометричних персональних даних;

2) фізично носії (сервери), на яких зберігається база з біометричними персональними даними, повинні розміщуватись на території держави, адже це питання національної безпеки.

3) Держава може надавати можливість використовувати обмежену кількість біометричних персональних даних приватним особам для здійснення їх статутної діяльності тільки за письмової згоди осіб, яких такі дані ідентифікують, та без змоги їх копіювання і накопичення.

Висновки. Хоча біометричні технології спрощують ідентифікацію та мали б захищати людину, їх використання створює нові загрози для безпеки держави та окремої особи, а також є причиною виникнення нових проблем (щодо конфіденційності щодо збору та зберігання біометричних даних).

Було встановлено дві категорії біометричних даних. До першої категорії віднесено інформацію, що стосується тілесних характеристик (фізичні або фізіологічні особливості людини), до другої – інформацію, що стосується поведінки людини (будь-які поведінкові характеристики людини, які є унікальними, завдяки чому є можливість ідентифікації людини).

Використання біометричних персональних даних із метою профілактики дисциплінарних, адміністративних та кримінальних правопорушень можливе лише за умови їх належного захисту з боку держави.

Список використаних джерел:

1. Посібник з європейського права у сфері захисту персональних даних. Київ : К.І.С., 2015. 216 с.

2. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20.11.2012 р. № 5492-VI / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text (дата звернення: 20.10.2020).

3. Різак М.В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2013. № 6-3. Т. 1. С. 91–95.

4. Роз’яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних : Роз’яснення. URL: https://zakon.rada.gov.ua/laws/show/n0003715-14#Text (дата звернення: 20.10.2020).

5. Швиденко В. Болючий захист персональних даних: нові проблеми українського бізнесу через зміну правил ЄС. *Європейська правда*. 31 травня 2018 URL: https://www.eurointegration.com.ua/experts/2018/05/31/7082338/ (дата звернення: 20.10.2020).

6. У Китаї випадково оприлюднили базу даних розпізнавання облич. *Media Sapiens,* 2019 URL: https://ms.detector.media/kiberbezpeka/post/22850/2019-05-10-u-kitai-vipadkovo-oprilyudnili-bazu-danikh-rozpiznavannya-oblich/ (дата звернення: 20.10.2020).

7. У США програмістку підозрюють у крадіжці даних 106 мільйонів осіб. *Media Sapiens,* 2019 URL: https://ms.detector.media/ kiberbezpeka/post/23263/2019-07-30-u-ssha-programistku-pidozryuyut-u-kradizhtsi-danikh-106-milioniv-osib/ (дата звернення: 20.10.2020).

8. База даних з номерами 419 млн користувачів Фейсбука опинилася у відкритому доступі. *Media Sapiens,* 2019 URL: https://ms.detector.media/kiberbezpeka/post/23451/2019-09-05-baza-danikh-z-nomerami-419-mln-koristuvachiv-feisbuku-opinilasya-u-vidkritomu-dostupi/ (дата звернення: 20.10.2020).

9. Беляева Ю. 3 злободневных вопроса об обработке персональных данных: ищем ответы в свежих разъяснениях регулятора и судебных делах. *Гарант.ру,* 2020 URL: http://www.garant.ru/ia/opinion/author/belyaeva/1402489/#ixzz6cFW6QFjV (дата звернення: 20.10.2020).

10. «ПриватБанк» запустив технологію оплати за допомогою обличчя *Media Sapiens,* 2019. URL: https://ms.detector.media/kiberbezpeka/ post/23493/2019-09-12-privatbank-zapustiv-tekhnologiyu-oplati-za-dopomogoyu-oblichchya/ (дата звернення: 20.10.2020).

11. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти : науково-практичний посібник. Київ : К.І.С., 2015. 220 с.