УДК 342.7

КАРЄВ І.Ю., аспірант ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0003-2503-4007.

СУЧАСНЕ ПРАВОВЕ СТАНОВИЩЕ ПРИСТРОЇВ З ТЕХНОЛОГІЄЮ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ В УКРАЇНСЬКОМУ ЗАКОНОДАВСТВІ

DOI…

Анотація. *У статті досліджується правове становище пристроїв розпізнавання обличчя в сучасному українському законодавстві. Дане питання є комплексним, тому що дані пристрої використовують біометричні персональні дані особи. Беручи до уваги, що біометричні персональні дані мають певні властивості, а саме – відсутність можливості їхньої зміни на сучасному технологічному рівні розвитку людства, існує необхідність захищати зібрані дані більш ретельно, ніж інші персональні дані. Бізнес розуміє переваги такого роду ідентифікації та верифікації особи, тому розвиток систем розпізнавання обличчя розвивається у всьому світі, але для його регуляції необхідна спеціалізована законодавча база.*

Ключові слова: *приватність, захист персональних даних, GDPR, біометричні персональні дані, FRT, FRS, розпізнавання обличчя, ISO, кібербезпека.*

Summary. *The article examines the legal status of face recognition devices in modern Ukrainian legislation. This issue is complex because these devices use biometric personal data of a person. Given that biometric personal data have certain properties – namely, the inability to change them at this technological level of human development, there is a need to protect the collected data more carefully than other personal data. Businesses quickly realized the benefits of this type of identification and verification. That is why the development of face recognition systems is growing all over the world, but a specialized legal framework is needed to regulate it.*

Keywords: *privacy, personal data protection, GDPR, biometrics, FRT, FRS, face recognition, cybersecurity.*

Постановка проблеми: Завдяки розвитку інформаціфних технологій (далі – ІТ), систем на основі штучного інтелекту (далі – ШІ) та нейромереж було створено технологію для розпізнавання обличчя людини. Дане технологічне рішення дозволяє ідентифікувати та верифікувати особу за притаманними лише їй параметрами. Завдяки точності та легкості застосування і використання таких систем, швидкість розповсюдження та імплементації даного виду ідентифікації дедалі більше завойовує ринок у багатьох сферах, починаючи від банківської та закінчуючи сферою розваг. Використання біометричних персональних даних особи виявилося новою задачею у сфері безпеки персональних даних, при роботі з пристроями з технологією розпізнавання обличчя. Ця технологія збирає та використовує саме біометричні персональні дані. Тому можливості для профілювання та відслідковування користувача виходять на новий рівень, вже не кажучи про можливість використання біометричних даних для створення нових видів кіберзлочинів. Сучасне українське законодавство, зокрема Закон України “Про захист персональних даних” [1], не регулює зазначені дії.

Відсутність класифікації, регуляторних політик та правил застосування технологічних рішень в українському законодавстві не дає змоги для створення модернізованого законодавства у сфері застосування систем розпізнавання обличчя. Аналіз європейського законодавства дає можливість для створення підґрунтя, що сприятиме модернізації українського законодавства до рівня ЄС, що необхідно для подальшої інтеграції України до вступу в ЄС в умовах цифрових трансформаційних процесів.

Метою статті є визначення сучасного стану у сфері використання камер з функцією розпізнавання обличчя, проблем та перспектив у розвитку українського законодавства.

Результати аналізу наукових публікацій. Захист конфіденційності користувачів при використанні будь-якого програмно-апаратного комплексу – це питання з'явилося досить нещодавно. Завдяки світовій тенденції щодо приватності особи це питання стає дедалі більш актуальним і необхідним у сучасному суспільному житті.

Правові питання використання систем розпізнавання обличчя – це комплексне питання, яке знаходиться відразу у площині кібербезпеки, захисту персональних даних, роботи з біометричними даними, а також у площині досить нових сфер, таких як діяльність систем з ШІ і використання нейромереж. Якщо питання приватності, захисту персональних даних та конфіденційності вже неодноразово підіймалось вітчизняними вченими, серед яких В. Брижко, А. Баранов, В. Пилипчук [2], О. Костенко [3] та інші, то у плані регуляції діяльності систем з ШІ та нейромереж питання майже не вивчене в Україні.

Виклад основного матеріалу. Сучасний розвиток ІТ та глобальної комунікаційної мережі Інтернет створили умови для імплементації технологій у життя сучасної людини. З самого початку ідентифікація користувачів відбувалася за допомогою логіну та паролю, які були необхідні для виконання певних дій та правочинів. На певному етапі даного технологічного рішення вистачало і у залежності від вимог забезпечення кібербезпеки були імплементовані різні механізми підтвердження користувача. З часом та розвитком технік "зламу" даний принцип перейшов у стадію перетворення, коли вже загальноприйняті методи захисту зазнали необхідності модифікації, які постійно поліпшуються. Паралельно йшли розробки альтернативних методів підтвердження особи користувача, таких як використання відбитку пальця, ДНК-датчики та подібні технології. Кожен з цих методів базується на використанні технічних засобів поєднаних з програмним забезпеченням. Деякі з даних способів мають відмінну ефективність, але мають високу вартість чи складність у застосуванні. Одним із завдань розвитку ідентифікації користувача є легкість використання, застосування мінімуму сторонніх пристроїв та змога працювати без підключення до мережі Інтернет. Завдяки розвитку технологій у сфері оптичних приладів та винахід такого явища як нейромережа, розпочався новий етап у розвитку ідентифікації користувача, а саме – розробка та імплементація системи розпізнавання обличчя (*Facial Recognition System* – FRS).

Технологія розпізнавання обличчя – це система, що використовує для ідентифікації та верифікації фізичної особи біометричні дані на основі візуального аналізу. Для аналізу використовуються різноманітні алгоритми, які здатні виявити особливості рис обличчя та створити математичну модель, на основі якої відбувається подальша верифікація та ідентифікація особи.

Не зважаючи на тип програмно-апаратного забезпечення та властивостей нейромережі, роботу системи розпізнавання обличчя можна описати у наступних етапах:

Отримання зображення обличчя. Даний процес можна отримати завдяки технічним засобам відеоспостереження, відеокамери, з потокового відео та з відеофайлу. Суть етапу – отримати зображення суб'єкту у найкращій якості, яке буде придатне для використання у подальших етапах.

Виявлення обличчя. На готовому зображенні нейромережі виявляють місцезнаходження обличчя. Можна застосувати різні методики та алгоритми визначення обличчя. Не зважаючи на обраний метод чи їх сукупність, на зображенні виявляють ту частину, на якій знаходиться обличчя. Після того як, відповідна частина зображення

знайдена, її відокремлюють та покращують якість. У залежності від того, який тип програмного забезпечення буде використовуватися, визначається необхідна якість зображення. Слід відмітити, що чим краща якість взятого зображення, тим важче буде підробити зображення за допомогою інших нейромереж або спеціальних програмно-апаратних засобів.

Створення математичної моделі. Завдяки особливостям обличчя, можна створити математичну модель, яка буде застосовуватися на подальших етапах. Для створення даної моделі аналізується форма обличчя, губ, очей, носа, вух, довжина та товщина шиї, їхнє розташування, наявність або відсутність шрамів та татуювань.

Створення шаблону. Отриману математичну модель обробляють спеціальною методикою для створення шаблону, завдяки якому можна швидко і точно проводити порівняння. Даний шаблон може бути використаний для подальшої ідентифікації як певного користувача, так і для верифікації у системі. До речі, поява шрамів та татуювань не завжди впливає на необхідність заміни або модифікації вже готового шаблону користувача.

Порівняння. На даному етапі вже готовий шаблон порівнюється з тими, що знаходяться у базі. За умови, що існують збіги, то система визначає, чи шаблон збігається з визначеним обличчям, чи ні.

Прийняття рішення. Залежно від мети пошуку, відбувається процес верифікації користувача або його ідентифікація.

Технологія розпізнавання обличчя використовується у багатьох сферах суспільного життя таких як ідентифікація та верифікація користувачів певних програмних засобів, камерах спостереження та сфері розваг. Але розвиток технологій, особливо пов’язаних з ІТ сферою, випереджає розвиток законодавства.

Робота камер з FRS в українському законодавстві не регламентована спеціальним законом. Специфіка роботи даної технології вимагає постійної взаємодії з біометричними персональними даними особи.

У Законі України “Про захист персональних даних” існує визначення, що таке персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1], але відсутнє визначення “біометричні дані”.

У Законі України “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”, ідентифікація особи визначається як – сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри – оцифрований підпис особи, оцифрований образ обличчя особи, оцифровані відбитки пальців рук) та біометричні параметри – вимірювані фізичні характеристики або особистісні поведінкові риси, що використовуються для ідентифікації (впізнання) особи або верифікації наданої ідентифікаційної інформації про особу [4].

У Положенні “Про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства” вказано, що біометричні дані це оцифровані відбитки пальців рук, оцифроване зображення обличчя [5].

Хоча у Положенні “Про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства” вказано, що біометричні дані повинні оброблятися та зберігатися згідно Закону України “Про захист персональних даних”, останній містить лише у ст. 13 норму щодо того, що дані повинні зберігатися таким чином, щоб забезпечити їх цілісність та відповідний режим доступу до

них. У статті 24 Закону України “Про захист персональних даних” відсутнє розмежування персональних даних та чутливих даних. Таким чином не враховано специфіку біометричних даних.

Розглядаючи специфіку біометричних даних треба відмітити те, що більшу частину з них неможливо змінити. Можна змінити певні особливості особи, такі як хода у залежності від вікових особливостей, травми та інші фактори, але інші ідентифікатори особи як ДНК, міміка, рухи, розташування очей не змінюються. За умови, що особа виконає пластичну операцію зі зміни обличчя, існує великий шанс її ідентифікувати за параметрам, які були до операції, адже змінити розташування очей, вух та носа – не є можливим. Якщо біометричні дані зазнали витоку, тоді даний факт може призвести до незаконного втручання у життя особи, руйнування її соціальних зв’язків та незаконних дій, виконаних від імені даної особи. Завдяки використанню оцифрованої дактилоскопічної інформації можливо підробити відбиток пальця за допомогою спеціалізованих засобів. З обличчям також можна створити цифрову копію на основі математичної моделі. Один з таких варіантів – це використання спеціалізованих нейромереж, які зможуть максимально точно відтворити обличчя особи з усіма супутніми параметрами.

Виток біометричних даних, а саме оцифрованого обличчя та інших оцифрованих даних, включаючи міміку та рухи, може привести до “викрадання особистості” – одного з видів кіберзлочинів. Він характеризується тим, що зловмисники беруть під свій контроль всі акаунти людини у соціальних мережах, банківські рахунки. Іноді ця ситуація закінчується отриманням викупу, але з урахуванням можливостей біометричної ідентифікації та можливістю видавати себе за жертву, зловмисники можуть повністю порушити життя жертви через завдання матеріальної або моральної шкоди. Головне у тому, що довести невинність завжди буде досить проблематично.

В українському законодавстві існує відповідальність за порушення законодавства щодо захисту персональних даних, а саме незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації та про її обробку або про зміну відомостей, які підлягають повідомленню згідно із законом, неповних чи недостовірних відомостей [6; 7]. Проте, ці законодавчі акти розглядають персональні дані у загальному вигляді, здебільшого у вигляді документів особи. Відсутнє розділення на різні типи персональних даних, а саме – біометричні та чутливі. В залежності від того, які дані було втрачено, можуть настати різні наслідки за ступенем тяжкості та впливу на потерпілу особу. Також відсутня процедура захисту особи, персональні дані якої зазнали витоку. Якщо мова йде про паспортні дані, то паспорт можна змінити, але якщо мова йде про біометричні дані, то така можливість поки що відсутня. Також існує питання про те – хто повинен займатися питанням забезпечення безпеки особи, чиї персональні дані зазнали витоку та мають ризик використання злочинцями у їхній протиправній діяльності.

Стосовно захисту інформації та персональних даних в Україні діє стандартизація – Комплексна система захисту інформації (КСЗІ) [8]. Цей стандарт є вразливим для кібератак та витоків персональних даних. Питання постає у використані сертифікованого програмного забезпечення, яке досить вразливе та не відповідає світовим стандартам. Також існує проблематика обмежених ресурсів для розгортання та підтримки КСЗІ. Відсутність постійних заходів з підготовки та підвищення рівня кваліфікації персоналу несе ризики людського фактору. Адже ефективність захисту системи від кіберзагроз потребує постійного вдосконалення навичок та вдосконалення програмно – апаратного комплексу.

У Регламенті (ЄС) 2016/679 від 27.04.16 р. (далі – GDPR), найжорсткішому і найефективнішому законі, визначення біометричних даних має тільки одне формулювання, яке визначене у статті 4. А стаття 9 регламентує опрацювання таких даних [9; 10]. Стаття 25 GDPR дає чіткі рекомендації стосовно програмно-апаратного забезпечення захисту від стороннього втручання та витоку даних, посилаючись на стандарт ISO 27001. Кожен контролер та володілець персональних даних мусять пройти затверджений механізм сертифікації по даному стандарту, як підтвердження того, що існує відповідність вимогам. Сама сертифікація включає як програмно-апаратні вимоги до програмного забезпечення, так і певну роботу з працівниками для того, щоб унеможливити витік та втрату персональних даних. З родини стандартів ISO слід відмітити, що не тільки 27001 бере участь у формуванні принципів захисту персональних даних. Тому для сертифікації зазвичай використовують навчання і по іншим стандартам ISO, а саме :

ISO 27002:2013 (Security Techniques – Code of practice for information security controls) – Кодекс практичних заходів для контрою за захистом інформації.

ISO 27003:2017 (Security Techniques – Information security management systems) – Техніка безпеки для систем захисту персональних даних.

ISO 31000 – (Best Practice Guidelines) – Практикум з застосування гайдів з захисту персональних даних як у технічному, так і адміністративному сегментах.

Реальність практики свідчить про різницю між рекомендаціями та практичним застосуванням певних заходів та демонструє на прикладах можливості вирішення певних, специфічних питань.

Всі стандарти ISO постійно оновлюються. Такі оновлення ґрунтуються на практичному досвіді та теоретичній основі стосовно розвитку можливостей витоку та хакерських атаках, з можливістю застосування нових методів, вразливостей нульового дня та новітнього програмно-апаратного комплексу. Один з варіантів таких практичних заходів – інфільтрація комп'ютерної мережі хакерським програмним забезпеченням, яке встановлюється з флеш-накопичувача, принесеного до офісу, або завдяки скриптам, які прописані у фото-, відео- або текстових файлах. Тобто атаки на систему, які відбуваються з її середини, минаючи захисний функціонал, розроблений для відбиття атаки ззовні.

Завдяки комплексним заходам відбувається постійне оновлення захисних систем володільця та розпорядника персональних даних. Такий підхід до захисту персональних даних дає більш серйозний ступінь захисту, а ніж принципи морально застарілого КСЗІ.

Беручи до уваги ступінь захисту баз даних з персональними даними, Регламент дає чітку імперативну норму, прописану у статті 17 GDPR щодо права особи на видалення персональних даних, включаючи біометричні, базуючись на праві на забуття. Тобто видалення даних за запитом особи. У той самий час українське законодавство не передбачає вказаного інструменту захисту персональних даних. Регламентований строк у 75 років, у затвердженому наказі Мінюста України "Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів" [11] вважається мінімальним та таким, який не можна скорочувати.

Слід особливо відзначити, що в Україні контроль за дотриманням законодавства у сфері захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини. А в той самий час у ЄС кожна країна має свого регулятора, який займається виключно даним питанням, що дає можливість більш детально займатися контролем, перевірками та визначенням порушень у даній сфері.

Завдяки тому, що біометричні дані відносяться до сфери чутливих даних, а технологія розпізнавання FRS розвивається дуже швидко, для уникнення ризиків порушення GDPR було розроблено спеціальні правила. EDPB випустило гайд для використання камер з технологією розпізнавання обличчя [10]. Для того, щоб не залежати від типу системи розпізнавання, даний гайд бере за основу загальне поняття технології розпізнавання обличчя – FRT. Даний гайд оснований на Фундаментальних правах людини та на вказівках Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62 – це правила обробки біометричних даних в контексті правоохоронної діяльності з метою забезпечення конфіденційності та безпеки з урахуванням використання ШІ та систем машинного навчання. Також враховано рекомендації щодо обробки, зберігання та застосування біометричних даних згідно статті 29 Директиви (ЄС) 2016/680 [14].

Гайд визначає дві основні функції використання FRT – ідентифікація та верифікація особи. А також дає визначення, що верифікація – це процес, спрямований на перевірку того, що особа є тією, за кого вона себе видає. У такому випадку системою порівнюється вже готовий, попередньо створений біометричний шаблон або зразок (наприклад, збережений на смарт-картці або біометричному паспорті) з обличчям визначеної особи.

Як на нашу думку, гайд дає досить цікаве визначення ідентифікації – процес пошуку певної визначеної особи серед групи людей в певній визначеній області, на зображені або базі даних. У такому випадку пристроєм FRT фіксується, обробляється, генерується шаблон і перевіряється чи він співпадає до кожної особи. Ця функціональність базується на порівнянні одного шаблону з базою шаблонів або зразків (базовим значенням). Це також називається ідентифікацією один до багатьох. Наприклад, це може пов'язувати запис про особу (прізвище, ім'я) з обличчям, якщо порівняння відбувається з базою фотографій, пов'язаних з прізвищами та іменами. Чітке визначення основних термінів дає можливість чіткого законодавчого регулювання і зниження ризиків маніпуляції термінів при розробці доктрин та стандартів використання пристроїв, не кажучи вже про зниження ризиків маніпулювання законодавством при судових процесах. В той самий час даний гайд розглядає взаємовідносини між контролером та процесором персональних даних у форматі взаємодії з біометричними даними. Хоча Регламент і регулює подібні взаємодії, але слід зазначити, що біометричні дані хоч і відносяться до чутливих даних, але до них необхідний своєрідний підхід з підвищенням рівня безпеки даних, навіть серйозніший ніж при взаємодії з іншими категоріями персональних даних, як під час роботи так і під час передачі даних.

Гайд характеризується чіткими визначеннями та посиланнями на чинні законодавчі акти, які в свою чергу можуть посилатися на стандарти безпеки ISO та інші законодавчі акти, які регламентують використання стандартизації. Так як технологія FRT використовує ШІ та нейромережі, гайд також посилається на використання даних програмно-апаратних засобів, тим самим поєднує законодавство про захист персональних даних з законодавством про інструменти ШІ та нейромережі.

Українське законодавство щодо питань взаємодії з біометричними даними та ШІ інструментами кардинально відрізняється від законодавства ЄС. На сьогоднішній день в законодавстві України відсутній закон, який регулює використання нейромереж, що використовують для роботи біометричні дані та ШІ.

До речі, у 2021 році Єврокомісія розробила закон про використання ШІ та нейромереж, а саме Artificial Intelligence Act, який регламентує правила щодо ШІ та вносить певні зміни у законодавчі акти ЄС, щоб забезпечити правове поле для використання систем на основі ШІ [15]. Основна мета цього закону – створити умови

безпечного застосування ШІ в країнах ЄС та створити правила використання систем на основі ШІ у різних сферах соціальної взаємодії. Але закон бере за основу забезпечення конфіденційності особи, захист прав людини та регламентує, як і де можна використовувати програмно-апаратні комплекси так, щоб цим не порушувати інше законодавство у сфері захисту персональних даних. Як побічний вплив – він регулює подальший технологічний розвиток даних систем та можливості їх застосування у нових сферах життєдіяльності людини. Хоча безпека даних у роботі з ШІ цього законопроекту базується на вже існуючих стандартах захисту персональних даних ISO, цілком імовірно, що у найближчому майбутньому буде створено нові стандарти для більш гармонійної і простої взаємодії з продуктами на основі нейромереж та ШІ.

В Україні вже певний час використовуються системи з FRT, проте немає жодного законодавчого акту, який би регламентував їх роботу. Наприклад, телефони з розблокуванням обличчям, оплата за ідентифікацією особи по обличчю, а також система "ДІЯ" при реєстрації вимагає оцифрувати обличчя користувача. Проте існує законопроект "Про єдину систему відеомоніторингу стану публічної безпеки", який створений щоб легалізувати та регламентувати єдину систему відеомоніторингу стану публічної безпеки [16]. У статті 14 цього законопроекту стосовно безпеки персональних даних дається відсилка на GDPR, але у правах особи відсутнє право людини на забуття. Також не визначено особливостей зберігання біометричних даних, місце, де вони будуть зберігатися, якими саме стандартами безпеки буде оснащений захист і найголовніше – не вказано, яка саме адміністративна відповідальність буде для процесора та володільця персональними даними у випадку витоку інформації. Цей законопроект цінний тим, що він вже створюється і намагається відповідати нормам Регламенту, що вже має на меті конкретні ефективні дії у сфері захисту біометричних даних громадян та інших осіб без громадянства. Хоча цей документ має велику кількість недоліків, але це початок врегулювання використання пристроїв з технологією FRT в Україні. Таким чином можливо створити законодавство про ідентифікаційні системи. Воно призначене спеціально для регулювання всіх систем управління ідентифікацією даних, незалежно від їх типу, структури, технології або мети. Законодавство про ідентифікаційні системи такого рівня також є державним законодавством, і воно призначене для вирішення проблем, які створює чинне національне законодавство для всіх систем управління ідентифікації даних, може заповнювати деякі прогалини, які не охоплені законодавством національного рівня [3].

Висновки.

Завдяки бурхливому розвитку нейромереж та систем на основі ШІ було створено новий засіб ідентифікації та верифікації особи. Питання у тому, що цей технічний засіб для роботи використовує біометричні дані, які, у свою чергу, є персональними даними особи. На момент виходу на ринок даних пристроїв, світове законодавство було не готове до такого виклику, але вже за кілька років було створено і розроблено спеціалізовані законодавчі акти для регулювання використання, виробництва та розробки даних виробів. Основний виклик у сфері регуляторних політик цих засобів та технологій постає у тому, що це питання комплексне, яке полягає у кількох сферах, а саме захисту персональних даних, регулювання використання систем на основі ШІ та нейромереж.

Українське законодавство наразі не має законодавчих актів стосовно регуляторної політики використання нейромереж та ШІ.

Також існує питання стандартизації та регуляторних політик у сфері захисту персональних даних. На відміну від України країни ЄС створили певні регуляторні політики у кожному з даних питань, таким чином, щоб дотримуватись балансу між

жорсткою політикою, яка блокує розвиток науково-технологічного прогресу методом заборони на використання, чим призведе до значних економічних втрат. Системи на основі FRT виробляються та розробляються переважно приватними компаніями, тому регуляторна політика має бути спрямована на подальший розвиток та імплементацію цих систем.

Для того, щоб привести правове становище стосовно камер з розпізнаванням обличчя та систем на основі FRS в Україні до рівня ЄС, існує два шляхи – повністю створити своє власне законодавство, яке буде регулювати дану сферу, або імплементувати вже існуючі, робочі варіанти з ЄС.

З урахуванням того, що Україна ратифікувала у 2014 році угоду про асоціацію з ЄС, то виникла необхідність щодо модернізації сучасного вітчизняного законодавства у сфері захисту персональних даних, яке не обмежується лише GDPR.

Постає питання щодо стандартів захисту персональних даних. Сучасна КЗСІ не отримувала оновлень з 2012 року, проте стандарти ISO мають постійне оновлення і вже прийняті ЄС за основу. Багато українських приватних компаній, які працюють з країнами ЄС, вже отримали сертифікацію та використовують стандарти ISO у своїй повсякденній роботі. Проте слід зазначити, що стандарти ISO прописані в законодавстві ЄС, зокрема у тому самому GDPR.

В сучасному українському законодавстві захист біометричних даних особи майже не врегульовано, тобто відсутні певні стандарти, які прописані у законодавчих актах, що дають можливість для маніпулювання при втраті, знищенні або зміні останніх.

У законодавстві ЄС та України на даний момент відсутня методика захисту особи від використання її персональних біометричних даних зловмисниками, адже з постійним рівнем розвитку технологій не виключений варіант того, що зловмисники зможуть використати скомпрометовані біометричні дані для того, щоб створювати “клони” жертв для своїх певних цілей.

Використана література

1. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI. – Стаття 2. URL: https://zakon.rada.gov.ua/laws/show/2297-17/conv#n11 (дата звернення: 20.02.2024).

2. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право.* № 1(32)/2020. С. 33-46; Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник ; за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ “Видавничий дім “АртЕк”, 2017. 226 с.; Пилипчук В.Г., Брижко В.М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху: монографія ; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса: Фенікс, 2020. 260 с.

3. Костенко О.В., Маньгора В.В. Напрями розвитку правового регулювання управління ідентифікаційними даними. *Інформація і право.* № 3(42)/2022. С. 65-79. URL: https://ippi.org.ua/kostenko-ov-mangora-vv-napryami-rozvitku-pravovogo-regulyuvannya-upravlinnya-identifikatsiinimi-dani (дата звернення: 20.02.2024).

4. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.12 р. № 5492-VI. – Стаття 3. URL: https://zakon.rada.gov.ua/laws/show/5492-17/conv#n51 (дата звернення: 20.02.2024).

5. Про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства: Постанова Кабінету Міністрів України від 27.12.17 р. № 1073-2017-п. URL: https://zakon.rada.gov.ua/laws/show/1073-2017-%D0%BF#Text (дата звернення 20.02.2024).

6. Кримінальний кодекс України: Закон України від 05.04.01 р. № 2341-ІІІ. – Стаття 182. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n1190 (дата звернення: 20.02.2024).

7. Кодекс України про адміністративні правопорушення: Закон України від 07.12.84 р. № 8073-Х. – Стаття 188-39. URL: https://zakon.rada.gov.ua/laws/show/80731-10#n2619 (дата звернення: 20.02.2024).

8. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. URL: https://tzi.com.ua/down loads/ 3.7-003-2005.pdf (дата звернення: 20.02.2024).

9. General Data Protection Regulator (GDPR) від 25 травня 2016 року. – Art 4. URL: https://gdpr -text.com/uk/read/article-4 (дата звернення: 20.02.2024).

10. General Data Protection Regulator (GDPR) від 25 травня 2016 року. – Art 9. URL: https://gdpr -text.com/uk/read/article-9 (дата звернення: 20.02.2024).

11. Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів: наказ Міністерства Юстиції України від 12.04.12 р. № 578/5. URL: https://zakon.rada.gov.ua/laws/show/z0571-12#Text (дата звернення: 20.02.2024).

12. EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj; https://edpb.europa.eu/sys tem/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (дата звернення: 20.02.2024).

13. Contribution of the EDPB to the European Commission’s evaluation of the Data Protection Law Enforcement Directive (LED) under. Article 62. EDPB. URL: https://edpb_contribution_led_rev iew_en.pdf (europa.eu) (дата звернення 20.02.2024).

14. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA EUROLex. URL: Directive 2016/680-EN-Law Enforce ment Directive; LED-EUR-Lex (europa.eu) (дата звернення: 20.02.2024).

15. Regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts 2021/0106(COD). URL: EUR-Lex-52021PC0206-EN-EUR-Lex (europa.eu) (дата звернення: 20.02.2024).

16. Про єдину систему відеомоніторингу стану публічної безпеки: проект закону України від 20.02.24 р. № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~