Захист персональних даних

План лекції

Вступ
1. Зарубіжний досвід захисту персональних даних
2. Вимоги законодавства України щодо захисту персональних даних
3. Окремі аспекти роботи з персональними даними в МВС України та Національній поліції
Висновки

Рекомендована література

Основна

1. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: наук.-практ. посіб. К. : К.І.С., 2021. 160 с. URL: https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69.
2. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : BAITE, 2021. 106 с.
3. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: BAITE, 2021. 262 с.
4. Щодо захисту персональних даних в умовах воєнного стану. URL: https://ombudsman.gov.ua/storage/app/media/Воєнний%20стан/Захист%20персональних%20даних/Захист%20персональних%20даних%20в%20умовах%20воєнного%20стану.pdf.

Допоміжна

5. Про захист персональних даних: Закон України від 01.06.2010. Офіційний вісник України. 2010. № 49 (09.07.2010). ст. 1604.
6. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: постанова Кабінету Міністрів України від 29.03.06 № 373. Офіційний вісник України. 2006. № 13 (12.04.2006). ст. 878.
7. Про доступ до публічної інформації: Закон України від 13.01.2011. *Офіційний вісник України.* 2011. № 10 (18.02.2011). ст. 446.
8. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. Баланс. 2014. № 19. С. 5. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n11.
9. Про інформацію: Закон України від 02.10.1992. *Відомості Верховної Ради України.* 1992. № 48 (01.12.1992). ст. 650.
10. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний вісник Європейського Союзу.* 04.05.2016. L 119. С. 1. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Інформаційні ресурси в Інтернеті

11. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

Текст лекції

Вступ

Персональні дані є однією з ключових складових приватного життя людини. Відповідно до ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення *конфіденційної інформації про особу* без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

1. Зарубіжний досвід захисту персональних даних

Захист персональних даних, які містять інформацію про особу, є одним із найважливіших аспектів побудови громадянського суспільства. Як і в Україні (2010 р.), спеціальні закони про захист персональної інформації були прийняті в більшості європейських країн: Австрії (1978 р.), ФРН (1977 р.), Великобританії (1984 р.), Франції (1987 р.), Норвегії (1988 р.), Португалії (1991 р.), Бельгії (1992 р.), Іспанії (1993 р.) та ін.

Радою Європи ухвалено Конвенцію про захист особи у зв'язку з автоматизованою обробкою персональних даних (1981 р.), 15 директив і рекомендацій у галузі захисту даних, у тому числі про захист: персональних даних у приватному (1973 р.) та державному (1974 р.) секторах; даних, що використовуються у медичних цілях (1981 р.), наукових дослідженнях та статистиці (1983 р.), прямому маркетингу (1985 р.), соціальному забезпеченні (1986 р.), правоохоронній сфері (1987 р.); даних у галузях зайнятості (1981 р.), платежів (1990 р.) тощо. Нормативні акти та рекомендації у вказаній сфері прийняті також Європейським Союзом (95/46/CE), Організацією економічного співробітництва та розвитку.

У 2016 році в Європейському Союзі було прийнято Загальний регламент про захист даних у ЄС (General Data Protection Regulation /GDPR/). У 2018 році цей регламент набув чинності. Як і в Конвенції про захист особи у зв'язку з автоматизованою обробкою персональних даних (ст. 2), згідно з п. 1 ст. 4 GDPR персональними даними визнається інформація про фізичну особу, яка ідентифікована або може бути ідентифікована. Фізичну особу можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор, або за одним чи кількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.

У п. 30 GDPR наголошується, що фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів, зокрема IP-адрес, ідентифікаторів «cookie» (реп'яшків) або інших ідентифікаторів, таких як мітки радіочастотної ідентифікації. Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з серверів, можна використати для створення профілів фізичних осіб та їхньої ідентифікації.

Одним з головних завдань, що його мало вирішити впровадження GDPR, було підвищення спроможності громадян контролювати опрацювання своїх персональних даних. Для того, щоб опрацювання було законним, персональні дані необхідно опрацьовувати на підставі згоди відповідного суб'єкта даних або на іншій законній підставі.

Суб'єкт даних повинен дати згоду на опрацювання своїх персональних даних, а також мати право доступу до персональних даних, які збирають щодо нього, і реалізовувати таке право вільно та через розумні проміжки часу для того, щоб бути обізнаним про законність опрацювання та перевірити її (п. 63 GDPR). Зважаючи на це великі компанії, які працюють з персональними даними в Інтернеті, мають форму зворотного зв'язку для запиту відповідних персональних даних:

- Google (https://takeout.google.com);
- Apple (https://support.apple.com/en-us/HT208502);
- Viber (https://help.viber.com/hc/en-us/articles/9062953104029-Request-Review-and-Delete-Your-Data-on-Viber#request-your-data-file);
- Facebook (https://www.facebook.com/help/212802592074644);
- Instagram (https://help.instagram.com/181231772500920);
- TikTok (https://support.tiktok.com/en/account-and-privacy/personalized-ads-and-data/requesting-your-data);
- Telegram (https://t.me/EURegulation);
- Microsoft (https://support.microsoft.com/en-us/windows/accessing-your-data-17e3d0dc-1351-3b03-9127-cc126a4e9568);
- WhatsApp (https://faq.whatsapp.com/526463418847093/?cms_platform=iphone);
- ClubHouse (https://support.clubhouse.com/hc/en-us/articles/4407302577939-How-do-I-request-a-copy-of-my-personal-data-);
- Signal (https://support.signal.org/hc/en-us/articles/360007059412-Signal-and-the-General-Data-Protection-Regulation-GDPR-).

Важливими нормами GDPR є встановлене право особи на виправлення (ст. 16) та стирання (ст. 17) своїх персональних даних. Інструменти для реалізації цих норм також передбачені у великих компаніях, які здійснюють свою діяльність у кіберсфері. Наприклад, Google реалізував та запропонував користувачам кілька способів та інструментів видалення даних (https://blog.google/products/search/new-privacy-tools/).

Принципами опрацювання персональних даних згідно зі ст. 5 GDPR є:

- законність, правомірність і прозорість;
- цільове обмеження;
- мінімізація даних;
- точність;
- обмеження зберігання;
- цілісність і конфіденційність;
- підзвітність.

2. Вимоги законодавства України щодо захисту персональних даних

Національне законодавство у сфері захисту персональних даних значною мірою наслідує європейську практику з цього питання. Наразі в Україні є чинним Закон України від 01.06.2010 «Про захист персональних даних». Відповідно до ч. 2 ст. 5 цього Закону ***персональні дані*** можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. При цьому персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 11 Закону України від 02.10.1992 «Про інформацію»). Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.

Первинними джерелами відомостей про фізичну особу є: *видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.* Інформацію про особу можна поділити на:

- **загальну,** яка є відкритою і може використовуватися іншими особами. Це, наприклад, ім'я фізичної особи, право на використання якого відповідно до ч. 3 ст. 296 Цивільного кодексу України допускається без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (звітах, стенограмах, протоколах, аудіо-, відеозаписах, архівних матеріалах тощо).

  Також згідно з ч. 2 ст. 5 Закону України «Про захист персональних даних» не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень. У даному випадку варто підкреслити, що саме інформація стосовно виконання посадовцем публічних обов'язків є відкритою. Це наприклад, можуть бути такі дані, як копії наказів про заохочення, надання відпустки, відомості про відповідні витрати бюджетних коштів тощо.

Публічною за законом є і інформація з декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування. Така інформація розміщується на сайті Національного агентства з питань запобігання корупції.

При цьому згідно з ч. 1 ст. 47 Закону України від 14.10.2014 «Про запобігання корупції» у відкритому доступі **не відображається** така інформація з декларації (має обмежений доступ):

1) відомості щодо реєстраційного номера облікової картки платника податків або серії та номера паспорта громадянина України;
2) унікальний номер запису в Єдиному державному демографічному реєстрі;
3) місця проживання, дати народження фізичних осіб, щодо яких зазначається інформація в декларації;
4) місцезнаходження об'єктів, які наводяться в декларації (крім області, району, населеного пункту, де знаходиться об'єкт);
5) номер рахунку в банківській чи іншій фінансовій установі.

- **вразливі персональні дані (конфіденційна інформація про особу),** що є інформацією з обмеженим доступом. Саме про такі дані йдеться у ст. 32 Конституції України та у ст. 302 Цивільного кодексу України: «Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До таких даних належать, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до кримінального покарання. Також згідно з Рішенням Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка) від 30.10.1997 до *конфіденційної інформації про особу,* зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані.

У 2012 році Конституційний Суд України додатково розтлумачив, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка обіймає посаду, пов'язану зі здійсненням функцій держави або органів місцевого

самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини[1].

Відповідно до ч. 2 ст. 21 Закону України «Про інформацію» ***конфіденційною*** є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону.

Оскільки персональні дані є інформацією, вимога щодо захисту якої встановлена Законом «Про захист персональних даних», відповідно до п. 4 Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373, вона підлягає захисту в системі.

Враховуючи викладене, відповідно до Закону України «Про захист персональних даних», Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та інших нормативних актів у сфері захисту інформації **загальна інформація про особу,** що зберігається в інформаційних системах держави, повинна бути захищена як відкрита інформація, а **вразливі персональні дані** – як службова інформація відповідно до вимог чинного законодавства у державних органах, або як окремий вид інформації – згідно з вимогами Закону України «Про захист персональних даних».

Дія цього Закону *поширюється* на діяльність з обробки персональних даних, яка здійснюється повністю або частково *із застосуванням автоматизованих засобів,* а також на обробку персональних даних, що містяться в *картотеці* (будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами) чи призначені до внесення до картотеки, із застосуванням *неавтоматизованих засобів.*

Відповідно до ст. 2 Закону України «Про захист персональних даних» ***база персональних даних*** – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

Суб'єктами відносин, пов'язаних із персональними даними, є:

- суб'єкт персональних даних;
- володілець бази персональних даних;
- розпорядник бази персональних даних;
- третя особа;
- Уповноважений Верховної Ради України з прав людини.

[1] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. Офіційний вісник України. 2012. № 9 (10.02.2012). ст. 332.

Володільцем чи розпорядником бази персональних даних можуть бути *підприємства, установи й організації* **всіх форм власності,** *органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці,* які обробляють персональні дані відповідно до законодавства.

Розпорядником бази персональних даних, володільцем якої є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише *підприємство державної або комунальної форми власності.* Прикладами бази персональних даних можуть бути бази даних комп'ютерних соціальних мереж, реєстраційних даних інтернет-магазинів, медичні картки пацієнтів в реєстратурі закладу охорони здоров'я, шкільний журнал тощо.

Персональні дані, крім знеособлених персональних даних, за порядком доступу **є інформацією з обмеженим доступом** (рис. 1).

Рис. 1. Класифікація інформації за порядком доступу

Склад і зміст персональних даних мають бути **відповідними, адекватними та ненадмірними** стосовно визначеної мети їх обробки.

Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, **без її згоди,** крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Для обробки персональних даних суб'єктом персональних даних має бути надана згода на обробку його даних. Згідно із законом така згода повинна бути задокументованою, зокрема у письмовій формі або в окремих випадках – в електронному вигляді. Згідно з нормами Цивільного та Сімейного кодексів України згоду на обробку персональних даних **дітей** дають **законні представники.**

Повну цивільну дієздатність має фізична особа, яка досягла вісімнадцяти років (повноліття) (ч. 1 ст. 34 ЦК). Фізична особа, яка не досягла чотирнадцяти років (малолітня особа), має часткову цивільну дієздатність і має право: 1) самостійно вчиняти дрібні побутові правочини; 2) здійснювати особисті немайнові права на результати інтелектуальної, творчої діяльності, що охороняються законом (ч. 1 ст. 31 ЦК).
Частиною 1 ст. 242 ЦК визначено, що батьки (усиновлювачі) є законними представниками своїх малолітніх та неповнолітніх дітей.

Розголошення чи публікація будь-якої інформації про дитину, що може заподіяти їй шкоди, без згоди законного представника дитини забороняється (ст. 10 Закону України «Про охорону дитинства»).

У 2018 році в м. Одеса розглядалась справа, у якій мати оскаржила публікацію фотографій своєї маленької доньки. Вони були опубліковані у Facebook без згоди мами. Відповідачі, зі свого боку, вважали, що публікація даних на приватних сторінках соцмереж з обмеженим доступом «рідним та друзям» не є поширенням на широкий загал. До того ж, це було зроблено з відома та за згоди батька дитини, який має рівні права на її виховання. Проте суд став на бік матері, аргументуючи це тим, що розміщення та поширення зображення у соцмережах може бути здійснено за згодою обох батьків (https://www.radiosvoboda.org/a/zahyst-personalnyh-danyh-dytyny/31603271.html, https://reyestr.court.gov.ua/Review/75031032, https://reyestr.court.gov.ua/Review/82910394).

Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

Суб'єкта персональних даних наділено низкою прав, зокрема на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних. Причому відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості. Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю бази персональних даних на обробку цих даних, або відповідно до вимог закону. Для отримання доступу складається запит.

Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, в тому числі незаконного знищення чи доступу до персональних даних.

В органах державної влади та органах місцевого самоврядування, організаціях, установах і на підприємствах усіх форм власності створюється *структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних* під час їх обробки відповідно до закону.

Цей самий підрозділ нерідко відповідає за надання за запитами осіб публічної інформації, пов'язаної з персональними даними. Під час прийняття рішення про надання такої інформації керуються так званим «трискладовим тестом», суть якого полягає у визначенні можливості надання інформації шляхом відповіді на три ключових запитання (ч. 2 ст. 6 Закону України від 13.01.2011 «Про доступ до публічної інформації»):

1. Чи слугує засекречення цієї інформації інтересам:
   - національної безпеки;
   - територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням;
   - охорони здоров'я населення;
   - захисту репутації або прав інших людей;
   - запобігання розголошенню інформації, одержаної конфіденційно;
   - підтримання авторитету і неупередженості правосуддя?
2. Чи може завдавати розголошення цієї інформації істотної шкоди таким інтересам?
3. Чи шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні?

За порушення роботи з персональними даними передбачена дисциплінарна, цивільно-правова, адміністративна та кримінальна відповідальність. У випадку адміністративного правопорушення треба звертатися до Уповноваженого

Верховної Ради України з прав людини. Власне види правопорушень та відповідальність за їх учинення викладені у ст. 188-39 Кодексу України про адміністративні правопорушення. У відповідній статті виділено три основні види правопорушень:

1. неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей;
2. невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних;
3. недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних.

Передбачена також більш сувора відповідальність за повторне вчинення таких правопорушень.

За незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації передбачено кримінальну відповідальність згідно зі ст. 182 Кримінального кодексу України.

3. Окремі аспекти роботи з персональними даними в МВС України та Національній поліції

У системі МВС України захист персональних даних урегульовано наказом МВС від 25.09.2020 № 685 «Про організацію роботи, пов'язаної із захистом персональних даних при їх обробці». Наказом передбачено організацію моніторингу та контроль за розглядом звернень з питань обробки та захисту персональних даних, що надходять до структурних підрозділів апарату МВС, територіальних органів надання сервісних послуг МВС, закладів, установ та підприємств, що належать до сфери управління МВС, Національної гвардії України, центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України. Відповідний моніторинг здійснюється за результатами звітування (2 рази на рік) окремими підрозділами перед МВС про стан розгляду звернень з питань обробки та захисту персональних даних. Крім того, Управління моніторингу дотримання прав людини МВС України також узагальнює стан організації щодо обробки та захисту персональних даних, для чого підрозділи МВС надсилають відповідні організаційно-розпорядчі документи.

Певні особливості щодо роботи з персональними даними існують і в Національній поліції. В цілому, вони є типовими для всієї правоохоронної системи. Так, наприклад, збирання інформації про осіб, доступної через відкриті джерела, може кваліфікуватися як посягання на недоторканність приватного життя. Зокрема, Європейський суд з прав людини своїм рішенням у справі «Швеція проти Сегерстед Віберг» кваліфікував дії правоохоронних органів зі збирання інформації, яка є відкрито доступною для користувачів мережі Інтернет, як порушення права на недоторканність приватного життя, гарантованого ст. 8 Конвенції Ради Європи про захист прав людини і основоположних свобод від 04.11.1950. Систематичне збирання інформації розцінюється як втручання у приватне життя у зв'язку з тим, що особа, яка розміщує інформацію, розраховує на зберігання відомостей та відсутність моніторингу за її профілем. Збирання відомостей є допустимим тільки відповідно до закону та в цілях боротьби зі злочинністю (ст. 8 (2) Конвенції).

У 2023 році за процесуального керівництва Тернопільської обласної прокуратури до суду направлено обвинувальний акт щодо працівника правоохоронного органу з Тернопільщини, який незаконно збирав персональні дані громадян. Встановлено, що фігурант систематизував та зберігав імена жителів Тернопільщини, дати їх народження, місця реєстрації та проживання, наявність у власності рухомого та нерухомого майна, вогнепальної зброї та спецзасобів. Ці дані він пересилав іншому працівнику правоохоронного органу незахищеними каналами зв'язку, під час чого могло статись несанкціоноване поширення цієї інформації.

Правоохоронця обвинувачують в незаконному збиранні, зберіганні, поширенні конфіденційної інформації (частини 1, 2 ст. 182 КК України). Досудове розслідування здійснювалось слідчими ТУ ДБР, розташованого у місті Львові. Санкція інкримінованої статті КК України передбачає покарання у вигляді позбавлення волі на строк до п'яти років (https://www.facebook.com/permalink.php?story_fbid=pfbid0FAso5vWz3P4tsYFXtcDk4u6n7XfbALWkYjmUaVRY9MspTeC3jf6WkkvQosMNyygSl&id=100064561967246).

Враховуючи викладене, правоохоронні органи мають право збирати будь-яку інформацію, якщо це передбачено законом, а також накопичувати безособову відкриту інформацію. Відомості щодо окремих осіб вони мають право збирати лише в межах визначених адміністративних процедур, у межах заведеної оперативно-розшукової справи або відкритого кримінального провадження. У ч. 2 ст. 264 Кримінального процесуального кодексу України наголошується, що здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або

утримувачем чи не пов'язаний з подоланням системи логічного захисту, не потребує дозволу слідчого судді.

Регуляторні процедури щодо персональних даних з кожним роком стають все жорсткішими, особливо в частині захисту конфіденційної інформації про особу. У багатьох країнах передбачена серйозна відповідальність для юридичних осіб за втрату персональних даних або порушення під час роботи з ними (https://www.enforcementtracker.com). Більш того, вже стає звичною практикою накладання великих штрафів регуляторами по всьому світу за незаконне збирання та використання інформації про осіб, навіть із відкритих джерел.

У травні 2023 року британський орган з нагляду за даними (Information Commissioner's Office) оштрафував компанію Clearview AI на £7,552,800 за використання зображень осіб з Об'єднаного Королівства без їх згоди. Регулятор також зобов'язав Clearview перестати надавати та використовувати дані підданих Об'єднаного Королівства, а також наказав видалити такі дані з бази даних компанії. (https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/). Власне база зображень збирається компанією з відкритих джерел, у тому числі з соціальних мереж, з метою надання послуг з розпізнавання облич. Компанія Clearview часто надає послуги з розпізнавання облич правоохоронним органам та спеціальним службам по всьому світу. Ця технологія є дуже корисною для вирішення завдань у сфері безпеки.

Враховуючи викладене, під час роботи з персональними даними слід не лише дуже уважно вивчати національне законодавство, а й досліджувати відповідну зарубіжну практику правозастосування, адже персональні дані часто поширюються в електронному вигляді, а відтак – можуть бути доступними і за кордоном.

Висновки

Для забезпечення безпеки персональних даних слід здійснити низку кроків організаційного та технічного характеру. Серед них можна виділити такі:

1. Неухильно дотримуватись вимог чинного законодавства в частині збирання, обробки, зберігання та захисту персональних даних.
2. Призначити відповідальну особу за організацію захисту персональних даних та затвердити внутрішні інструкції щодо захисту персональних даних.

3. Постійно вивчати та застосовувати кращі вітчизняні та зарубіжні практики щодо захисту персональних даних.
4. Мінімізувати кількість накопичених персональних даних та своєчасно видаляти вже непотрібні дані.
5. Не зберігати всі персональні дані в одному місці. Найкраще розділити їх таким чином, щоб без наявності однієї з частин неможливо було ідентифікувати конкретну особу.
6. Забезпечити заходи фізичного та технічного захисту місць і технічних засобів, які використовуються для збирання, обробки, збереження та забезпечення доступу до персональних даних.
7. Заборонити доступ до баз персональних даних з неавторизованих пристроїв та локацій.
8. Здійснювати регулярний контроль за станом збирання, обробки, зберігання та захисту персональних даних.
9. Відбирати зобов'язання у відповідних осіб про нерозголошення персональних даних, які стали їм відомі під час виконання функціональних обов'язків.
10. У випадку інцидентів безпеки, пов'язаних з персональними даними, своєчасно інформувати особу, відповідальну за безпеку в організації.
11. Організувати регулярне підвищення кваліфікації персоналу в частині захисту персональних даних.