МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Навчально-науковий інститут права

Кафедра інтелектуальної власності та інформаційного права

«До захисту у ЕК допустити»

Завідувач кафедри
інтелектуальної власності
та інформаційного права
д.ю.н., проф. Кодинець А.О.

_____

МАГІСТЕРСЬКА РОБОТА

на тему:

Правове забезпечення захисту персональних даних за проектуванням і за замовчуванням: національні і міжнародні стандарти

студентки 2 року навчання ОР «Магістр»
№ 2 групи
спеціальності: 081 «Право»
Навчально-наукового інституту права
Денної форми навчання
Парахіної Поліни Вячеславівни

Науковий керівник :
Заярний Олег Анатолійович
д.ю.н., доц.

_____

Рецензент:
Носік Юрій Володимирович
к.ю.н., доц.

_____

Київ – 2022

ЗМІСТ

ЗАТВЕРДЖЕНО:

Науковий керівник:
д.ю.н., доц. Заярний Олег Анатолійович

_____

«10» листопада 2021 року

МАГІСТЕРСЬКЕ ЗАВДАННЯ

Парахіної Поліни Вячеславівни, студентки 2 курсу магістратури, денної форми навчання, за спеціальністю «Право», ОНП «Інтелектуальна власність», спеціалізація «ІТ-право».

1. Тема роботи: «Правове забезпечення захисту персональних даних за проектуванням і за замовчуванням: національні і міжнародні стандарти».

2. Термін здачі роботи керівнику для підготовки відгуку: «10» травня 2022 року.

3. Робота виконується на базі: Інституту права Київського національного університету імені Тараса Шевченка.

4. Теоретичне завдання: аналіз спеціальної юридичної наукової літератури, законодавства України, дослідження законодавства і досвіду іноземних держав; дослідження поняття, правової природи та нормативно-правового регулювання захисту персональних даних за проектуванням і за замовчуванням.

5. Практичне завдання: правовий аналіз практичних аспектів реалізації захисту персональних даних за проектуванням і за замовчуванням, вивчення іноземної практики нагляду та контролю за дотриманням захисту персональних даних за проектуванням і за замовчуванням.

6. Сфера застосування результатів роботи: наукова діяльність, навчальний процес, правотворчість, правозастосовна діяльність.

7. Завдання вручено студентці: «10» листопада 2021 року.

ЗАТВЕРДЖЕНО:

Науковий керівник:
д.ю.н., доц. Заярний Олег Анатолійович

_____

«20» листопада 2021 року

КАЛЕНДАРНИЙ ПЛАН

Парахіної Поліни Вячеславівни, студентки 2 курсу магістратури, денної форми навчання, за спеціальністю «Право», ОНП «Інтелектуальна власність», спеціалізація «ІТ-право».

Тема роботи: «Правове забезпечення захисту персональних даних за проектуванням і за замовчуванням: національні і міжнародні стандарти».

№	Види робіт	План	Фактично
1.	Підбір наукової літератури та нормативних актів за темою роботи.	25.11.2021	01.12.2021
2.	Розробка плану роботи та його погодження.	01.12.2021	10.12.2021
3.	Підготовка першого розділу роботи та подання його на перевірку керівнику.	01.01.2022	01.02.2022
4.	Підготовка другого розділу роботи та подання його на перевірку керівнику.	15.02.2022	15.03.2022
5.	Підготовка третього розділу роботи та подання його на перевірку керівнику.	01.04.2022	01.04.2022

5.	Доопрацювання роботи на підставі зауважень керівника. Написання анотацій.	15.04.2022	22.04.2022
7.	Написання вступу, висновків, додатків, списку використаних джерел.	25.04.2022	01.05.2022
8.	Підготовка остаточного варіанту роботи та її технічне оформлення.	01.05.2022	05.05.2022
9.	Здача роботи керівнику для підготовки відгуку.	09.05.2022	09.05.2022

Студентка: Парахіна Поліна Вячеславівна

АНОТАЦІЯ

Парахіна Поліна Вячеславівна. Правове забезпечення захисту персональних даних за проектуванням і за замовчуванням: національні і міжнародні стандарти. Магістерська робота. Кафедра інтелектуальної власності та інформаційного права Інституту права Київського національного університету імені Тараса Шевченка.

У магістерській роботі здійснюється аналіз поняття і сутності персональних даних, розкривається практичне і юридичне значення принципів обробки і захисту персональних даних. Досліджується питання наукової розробки та нормативного закріплення концептів захисту персональних даних за проектуванням і за замовчуванням. Розкривається питання удосконалення українського національного законодавства та нормативного закріплення захисту персональних даних за проектуванням і за замовчуванням. Окрема увага приділяється сутності і значенню захисту персональних даних за проектуванням і за замовчуванням для реалізації принципів обробки і захисту персональних даних, а також захисту прав і основоположних свобод людини. Аналізується значення захисту персональних даних за проектуванням і за замовчуванням як елементу захисту фундаментального права людини на недоторканність приватного життя. Детально досліджуються практичні аспекти захисту персональних даних за проектуванням і за замовчуванням власниками цифрових сервісів. Розглядається іноземна практика здійснення державного нагляду і контролю за дотримання зобов'язання щодо захисту персональних даних за проектуванням і за замовчуванням.

Ключові слова: персональні дані, захист персональних даних, обробка персональних даних, захист персональних даних за проектуванням і за замовчуванням, фізична особа, право на недоторканність приватного життя, патерн.

ABSTRACT

Polina Parakhina. Legal enforcement of data protection by design and by default: national and international standards. Master's thesis. Department of Intellectual Property and Information Law of Institute of Law of the Taras Shevchenko National University of Kyiv.

The thesis carries out the analysis of the concept and essence of personal data and reveals the practical and legal significance of the principles of processing and protection of personal data. The issue of scientific development and normative consolidation of concepts of data protection by design and by default in normative legal acts is investigated. The issue of improving the Ukrainian national legislation and normative consolidation of data protection by design and default is revealed. Particular attention is paid to the nature and importance of data protection by design and by default for the implementation of the principles of data processing and protection, as well as the protection of human rights and fundamental freedoms. The importance of data protection by design and by default as an element of protection of the fundamental right to privacy is analyzed. The practical aspect of data protection by design and by default by web service owners is studied in detail. The foreign practice of state supervision and control over compliance with the obligation to protect personal data by design and by default is considered.

Keywords: personal data, protection of personal data, processing of personal data, data protection by design and default, private individual, right to privacy, pattern.

ВСТУП

Актуальність теми дослідження. У сучасному цифровому світі життя людини, її індивідуальність, самобутність, трансльовані через її персональні дані, знаходяться у зоні постійної уваги з боку різних компаній, організацій та владних структур. Це викликано тим, що персональні дані стали надважливим ресурсом, який може бути використаний для отримання влади на людиною у найбільш різноманітних проявах: психологічної через вплив на формування поглядів та уподобань, фінансової через нав'язування певних товарів або послуг, політичної через маніпуляції задля зміни результатів демократичних виборів, фізичної через фізичне переслідування осіб тощо.

Неправомірне і надмірне використання персональних даних особи є втручанням у сферу її приватного існування, того, що вона бажає залишити поза межами стороннього доступу і уваги. Коли фізична особа втрачає контроль над своїми даними, вона фактично втрачає себе. Таким чином, захист персональних даних з його принципами і механізмами покликаний допомогти людині зберегти свою індивідуальність, свідомо приймати рішення без стороннього впливу і самостійно визначати, як презентувати себе у суспільстві.

Інформаційні технології та, зокрема, цифрові сервіси усе більше інтегруються у наше життя. Завдяки використанню алгоритмів, що аналізують персональні дані та патерни поведінки, технологічні компанії можуть знати про користувачів більше, аніж вона самі, і передбачати їхню поведінку. Це робить людей вразливими, створює ризики для прав і основоположних свобод, натомість посилюючи власників цифрових сервісів та збільшуючи їхні прибутки.

Як необхідність протидії всеохоплюючому впливу технологій на людину виникли концепти захисту персональних даних за проектуванням і за замовчуванням. Їх основна ідея – зробити захист персональних даних невід'ємною складовою бізнес-процесів, продуктів та послуг шляхом вжиття технічних та організаційних заходів.

Ці концепти почали формуватися наприкінці XX століття, і їхнє наукове дослідження і формування найкращих практик застосування досі формуються.

На нормативному рівні захист персональних даних за проектуванням і за замовчуванням як обов'язкова юридична вимога вперше був закріплений у ст. 25 Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 «Про захист фізичних осіб у зв'язку з обробкою даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» від 27 квітня 2016 року, більше відомому як GDPR. Завдяки тому, що недотримання ст. 25 Регламенту віднесено до категорії найбільш серйозних порушень, уже активно формується практика правозастосування як у рішеннях національних наглядових органів, так і в їхніх методичних рекомендаціях і роз'ясненнях.

Українське законодавство, зокрема, чинний Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI не містить поняття захисту персональних даних за проектуванням і за замовчуванням. Однак, оскільки України перебуває у процесі гармонізації національного законодавства у сфері захисту персональних даних до найвищих стандартів Європейського Союзу та Ради Європи, розуміння і теоретичне осмислення правового забезпечення захисту персональних даних за проектуванням і за замовчуванням є вкрай необхідним та важливим.

Наразі на розгляді у Верховної Ради України перебуває Проект Закону «Про захист персональних даних» № 5628 від 07 червня 2021 року, який вже містить ст. 29, присвячену захисту персональних даних за проектуванням і за замовчуванням. У разі прийняття законопроекту виникне потреба у розробці методичних і практичних рекомендацій щодо правозастосування, оскільки нормативні формулювання є загальними і не дають розуміння того, яким чином їх реалізувати на практиці.

Метою дослідження є з'ясування природи і сутності захисту персональних даних за проектуванням і за замовчуванням, його ролі у захисті права людини на недоторканність приватного життя та реалізації принципів обробки і захисту персональних даних; дослідження іноземного досвіду нормативно-правового

регулювання захисту персональних даних за проектуванням і за замовчуванням та національних перспектив удосконалення законодавства; аналіз практичних аспектів реалізації захисту персональних даних за проектуванням і за замовчуванням власниками цифрових сервісів; аналіз іноземної практики нагляду і контролю за захистом персональних даних за проектуванням і за замовчуванням.

Відповідно до зазначеної вище мети, **основними завданнями** дослідження є:

1) дослідити поняття і сутність персональних даних, їх основні характеристики і еволюцію нормативного закріплення визначення поняття «персональні дані»;

2) проаналізувати принципи обробки і захисту персональних даних, їх нормативне закріплення, практичні аспекти застосування та юридичне значення;

3) розглянути іноземний досвід нормативно-правового регулювання захисту персональних даних за проектуванням і за замовчуванням та національні перспективи щодо удосконалення законодавства у сфері захисту персональних даних;

4) проаналізувати сутність права людини на недоторканність приватного життя і визначити роль захисту персональних даних за проектуванням і за замовчуванням як елементу захисту цього права;

5) дослідити сутність захисту персональних даних за проектуванням і за замовчуванням, принципи реалізації;

6) розглянути практичні аспекти захисту персональних даних за проектуванням і за замовчуванням власниками цифрових сервісів, розкрити основні стратегії, тактики та патерни;

7) здійснити огляд практики правозастосування наглядовими органами у сфері захисту персональних даних держав-членів Європейської економічної зони щодо дотримання обов’язку із захисту персональних даних за проектуванням і за замовчуванням.

Об’єктом дослідження є суспільні відносини, що виникають із захистом персональних даних за проектуванням і за замовчуванням.

Предметом дослідження є явище захисту персональних даних за проектуванням і за замовчуванням.

Методи дослідження. Методологічну основу дослідження склали наступні методи наукового пізнання:

1) загально-наукові (метод аналізу, формально-логічний метод, які застосовувалися при дослідженні положень нормативно-правових актів у сфері захисту персональних даних, методичних рекомендацій та роз’яснень національних наглядових органів тощо);

2) спеціально-наукові (наприклад, метод правового порівняння, який використовувався при дослідженні національного та іноземного нормативно-правового регулювання захисту персональних даних; історико-правовий метод, що застосовувався при вивченні розвитку правового регулювання зазначеної сфери правовідносин).

У результаті використання цих методів встановлено, що захист персональних даних за проектуванням і за замовчуванням є невід’ємною складовою системи захисту персональних у цілому і гарантією права людини на недоторканність приватного життя.

Науково-теоретичну основу дослідження склали праці таких науковців та практиків, як А. Пазюк, М. Бем, І. Городиський, Г. Саттон, О. Родіоненко, Р. Лінс (R. Leenes), А. Кобрін, Д. Корчинський, В. Некрутенко, В. Породько, N. Purtova, R. Jason Cronk, A. Cavoukian, C. Bösch, B. Erb, F. Kargl, H. Kopp, S. Pfaheicher, J.H. Hoepman, N. Doty, M. Gupta, а також роз’яснення та методичні рекомендації наглядових органів із захисту персональних даних іноземних держав.

Нормативну основу дослідження склали Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, Конвенція Ради Європи від 28 січня 1981 року № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», Протокол про внесення змін до Конвенції Ради

Європи від 28 січня 1981 року № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС».

Практичну основу дослідження склали найбільш поширені випадки порушення та справи про притягнення до відповідальності за порушення захисту персональних даних за проектуванням і за замовчуванням.

Новизна одержаних результатів. Наукова новизна дослідження полягає у здійсненні всебічного комплексного аналізу міжнародно-правових стандартів і сучасного національного законодавства у сфері захисту персональних даних на предмет нормативного закріплення захисту персональних даних за проектуванням і за замовчуванням, а також аналізі практичних аспектів правозастосування.

Сферою застосування результатів дослідження можуть бути: наукова діяльність з подальшого дослідження проблемних аспектів захисту персональних даних за проектуванням і за замовчуванням; використання окремих положень магістерської роботи в освітньому процесі, наприклад, під час вивчення дисциплін «Захист персональних даних», «Інформаційне право» тощо; правотворча та правозастосовна діяльність, спрямована на подальше реформування та удосконалення законодавства України у сфері захисту персональних даних, зокрема, нормативне закріплення захисту персональних даних за проектуванням і за замовчуванням та подальші роз’яснення щодо правозастосування.

Структура та обсяг роботи. Структура магістерської роботи обумовлена метою і завданнями дослідження. Вона включає вступ, основну частину, що містить три розділи та вісім підрозділів, висновки та список використаних джерел. Основний текст роботи становить 65 сторінок. Список використаних джерел містить 52 найменування.

РОЗДІЛ 1. Загальні засади організації обробки персональних даних відповідно до норм національного та міжнародного права

1.1. Поняття та властивості персональних даних

За останнє десятиліття вислів «персональні дані – це нова нафта» лунає дуже часто, що пов'язано зі стрімким розвитком цифрових технологій, діяльністю світових технологічних корпорацій, а також новими можливостями для їхнього використання. Усе більше даних про особу стають доступними для інших, що позбавляє людину контролю не тільки над інформацією про себе, а й над своїм життя: завдяки аналізу і використанню даних можна впливати на думки і погляди людини, передбачати її уподобання та поведінку, маніпулювати, навмисно чи ненавмисно вдаватися до дискримінації за певними ознаками, шантажувати, і що найгірше – завдавати як моральної, так і фізичної шкоди (наприклад, через політичні переслідування, знищення представників певної соціальної, національної, релігійної групи тощо).

А. В. Пазюк дуже доречно у своїй дисертаційній роботі зазначив, що персоніфікована (персональна) інформація відображає індивідуальність кожної людини і, з огляду на доступність та поширеність засобів її збирання й використання, несе загрозу можливого неправомірного використання, розголошення відомостей щодо приватного життя, заподіяння шкоди репутації і добробуту людини тощо. У західній правовій доктрині для позначення правового інституту захисту приватного життя людини використовують термін «приватність». Він походить від «приватний» – такий, що протиставляється публічному (суспільному) і характеризує якісний стан об'єкта, випливає з його належності до приватної (не доступної для загалу) сфери життя людини.[1]

Розуміння поняття та властивостей персональних даних є ключовим і складає основу для формування принципів та механізмів їхнього захисту, а також

[1] Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.11 «Міжнародне право» // А. В. Пазюк. – К., 2004. – 15 с. [Електронний ресурс] – Режим доступу до ресурсу: http://cyberpeace.org.ua/files/aref-1.pdf.

визначає матеріальну сферу та межі застосування законодавства у сфері захисту персональних даних.

Поняття персональних даних закріплено як на рівні міжнародних нормативно-правових актів, так і на рівні регіонального та національного законодавства.

Першим юридично обов'язковим нормативно-правовим актом міжнародного рівня у сфері захисту персональних даних була і досі є чинною Конвенція Ради Європи від 28 січня 1981 року № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (надалі – Конвенція № 108), і саме у ній поняття персональних даних отримало своє нормативне визначення.

Відповідно до п. «а» ст. 2 Конвенції № 108 «персональні дані – це будь-яка інформація, яка стосується ідентифікованої особи або особи, яка може бути ідентифікованою (суб'єкт даних)».[2] Слід відмітити, що ця дефініція була навмисно була прописана дуже широко, аби охопити усю інформацію, яка може стосуватися фізичної особи, і таким чином захистити право людини на недоторканість її приватного життя.

Проте, на нашу думку, певним недоліком слід вважати відсутність у визначенні додаткових параметрів, які б допомагали визначити, чи є фізична особа за певних умов такою, що може бути ідентифікованою, і, відповідно, чи належить певна інформація до категорії персональних даних.

Конвенція № 108 стала світовим стандартом у сфері захисту персональних даних, а тому її положення були взяті за основу для розробки регіональних актів, зокрема, Директиви 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року (надалі – Директива), яка у 2018 році була замінена Регламентом Європейського Парламенту і Ради (ЄС) 2016/679 «Про захист фізичних осіб у зв'язку з обробкою даних і про вільний рух таких даних,

[2] Конвенція Ради Європи від 28 січня 1981 року № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/994_326#Text.

та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» від 27 квітня 2016 року (надалі – Регламент), а також актів національного законодавства.

У Директиві поняття персональних даних отримало більш детальне визначення, порівняно з Конвенцією № 108, і це визначення залишилося незмінним і у Регламенті.

Згідно з п. 1 ст. 4 Регламенту «персональні дані – це будь-яка інформація, яка стосується суб'єкта даних, тобто особи, яка ідентифікована або може бути ідентифікована; фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи».[3]

Важливим для розуміння поняття і сутності персональних даних, закріпленого у Директиві, а згодом і в Регламенті, є роз'яснення, надане Робочою групою за статтею 29 (англ. Article 29 Working Party, WP29) у Роз'ясненні 4/2007 щодо концепції персональних даних (надалі – Роз'яснення), яке залишається актуальним і сьогодні.

У Роз'ясненні визначення персональних умовно поділено на чотири складові: 1) будь-яка інформація; 2) яка стосується; 3) ідентифікованої або такої, що може бути ідентифікована; 4) фізичної особи.[4]

По-перше, персональні дані становлять будь-яку інформацію, незалежно від того, чи є вона об'єктивними даними, чи суб'єктивними судженнями; є вона правдивою чи ні; обмежується даними про приватне і сімейне життя чи включає дані про будь-яку діяльність, що здійснюється особою, зокрема, у соціальній та

[3] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

[4] Opinion 4/2007 on the concept of personal data. Article 29 Data Protection Working Party. Adopted June 20, 2007 [Електронний ресурс] – Режим доступу до ресурсу: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

економічній сферах життя; у якій формі та форматі ця інформація представлена (буквенному, числовому, графічному, фотографічному тощо).

Про те, що персональні дані включають будь-яку інформацію, що може набувати різних форм, неодноразово у своїх рішеннях зазначав Європейський суд з прав людини (надалі – ЄСПЛ), який розглядає справи щодо порушення право на недоторканність приватного життя, гарантованого ст. 8 Європейської конвенції про захист прав людини і основоположних свобод від 4 листопада 1950 року. Так, у Рішенні Benedik v. Slovenia (2018) персональними даними була визнана динамічна IP-адреса та інформація користувача інтернету, пов'язана з IP-адресою. У цій ЄСПЛ визнав, що заявник зазнав неправомірного втручання у його приватне життя. За матеріалами справи заявник підозрювався у поширенні матеріалів сексуального насильства над дітьми, а тому поліція звернулася до інтернет-провайдера з вимогою надати ім'я та адресу відповідного користувача Інтернету. Інтернет-провайдер надав таку інформацію поліції, і ЄСПЛ визнав це порушенням права на недоторканність приватного життя, оскільки заявник мав виправдані очікування щодо своєї конфіденційності в Інтернеті.[5]

По-друге, для того, аби вважати певну інформацію персональними даними, необхідно, щоб вона прямо чи опосередковано стосувалася фізичної особи. Інформація може бути про фізичну особу у прямому сенсі (наприклад, ім'я, вік, адреса проживання), а також стосуватися, у першу чергу, певних явищ, об'єктів або процесів, але теоретично дозволяти опосередковано ідентифікувати особу у сукупності з іншими даними (наприклад, номер автомобіля, номер телефону, метадані).

Якщо ж повернутися до питання визнання динамічної IP-адреси персональними даними, необхідно звернути увагу на практику Європейського суду справедливості. Так, ще 2011 року у п. 51 Рішення у справі Scarlet Extended (C-70/10, EU:C:2011:771) IP-адреса була визнана персональними даними, які однозначно ідентифікують особу, оскільки збір та ідентифікація IP-

[5] Рішення ЄСПЛ у справі Benedik v. Slovenia, no. 62357/14, 2018 [Електронний ресурс] – Режим доступу до ресурсу: https://hudoc.echr.coe.int/eng.

адрес Інтернет-користувачів здійснювалася інтернет-провайдером.[6] За інших обставин у Рішенні у справі Patrick Breyer v. Bundesrepublik Deutschland (C-582/14, ECLI:EU:C:2016:779) динамічна IP-адреса, яка змінюється під час кожного з'єднання з інтернетом, була визнана Європейським судом справедливості персональними даними про особу, яка може бути ідентифікована. За матеріалами справа пан Брейєр заперечував проти збереження його динамічної IP-адреси загальнодоступними сайтами німецьких федеральних установ.

На відміну від попередньої справи, збереження IP-адрес здійснювалося постачальниками медіа-послуг, які не могли без отримання додаткової інформації від інтернет-провайдера ідентифікувати інтернет-користувачів. Тим не менш, було встановлено, що постачальник медіа-послуг має засоби, які можуть бути розумно використані для того, аби отримати від Інтернет-провайдера додаткову інформацію, необхідну для ідентифікації особи.[7]

По-третє, персональні дані повинні дозволяти безпосередньо чи опосередковано ідентифікувати особу. Якщо особу можна однозначно і безпомилково виділити з певної групи за одним чи декількома ідентифікаторами, вона є ідентифікованою (наприклад, за повним іменем та ідентифікаційним номером студент може бути однозначно виділений з-поміж інших студентів університету).

За певних умов наявність меншої кількості інформації чи певного обсягу іншої інформації достатньо для того, щоб особу вважати такою, «яка може бути ідентифікованою» (наприклад, знаючи номер квартири та інформацію про заборгованість за комунальні послуги, сусіди мають змогу ідентифікувати особу

[6] Рішення Європейського суду справедливості у справі Scarlet Extended (C-70/10, EU:C:2011:771) [Електронний ресурс] – Режим доступу до ресурсу: https://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2160380.

[7] Рішення Європейського суду справедливості у справі Scarlet Extended (C-70/10, EU:C:2011:771) [Електронний ресурс] – Режим доступу до ресурсу: https://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2160380.

боржника).[8] Тобто, для ідентифікації потрібне поєднання сукупності відомостей, які окремо одна від одної не дозволяють ідентифікувати особу.

У цьому контексті варто звернути увагу на класифікацію ідентифікаторів, запропоновану Рональдом Лінсом:[9]

1. L-ідентифікатори (від англ. Look up) – ідентифікатори, що пов'язані з конкретною людиною та можуть використовуватися за межами ідентифікації. Наприклад, номер телефону, номер паспорту, IP-адреса. Якщо якась особа отримає доступ до L-ідентифікатора, вона зможе поза межами контексту використання ідентифікатора встановити, кому він належить у реальному житті.

2. R-ідентифікатори (від англ. Recognition) – ідентифікатори, що дозволяють розпізнати особу без можливості пов'язати ідентифікатор з іменованою особою за межами контексту. Особа розпізнається за певними патернами та наборами ознак (наприклад, зовнішніх, поведінкових), які відомі чи впізнавані суб'єктом ідентифікації. R-ідентифікатори прив'язані до контексту, у якому вони існують, і не можуть використовуватися за його межами. До R-ідентифікаторів Лінс відносить файли cookie, які не дають можливості ідентифікувати особу у реальному житті. R-ідентифікатори часто можуть використовуватися для аутентифікації. Залежно від контексту R-ідентифікатори можуть перетворюватися на L-ідентифікатори.

3. C-ідентифікатори (від англ. Classification) – ідентифікатори, які ідентифікують особу через приналежність до певної групи чи категорії за поглядами, уподобаннями чи іншими атрибутами, що їх об'єднують. C-ідентифікатори мають значення саме для суб'єктів, що їх формують, наприклад, власників цифрових сервісів, які сегментують користувачів. Особистість у реальному житті у цьому разі фактично не має значення.

---

[8] Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник/М. Бем, І. Городиський, Г. Саттон, О. Родіоненко; Європейський Союз, Рада Європи - К.: К.І.С., 2015. – 220 с. [Електронний ресурс] – Режим доступу до ресурсу: https://rm.coe.int/168059920c.

[9] R. Leenes, Do They Know Me? Deconstructing Identifiability (2008) 4(1&2), University of Ottawa Law & Technology Journal [Електронний ресурс] – Режим доступу до ресурсу: https://pure.uvt.nl/ws/portalfiles/portal/1310856/Leenes_Do_they_know_me_110216_publishers_immediately.pdf.

4. S-ідентифікатори (від англ. Session) – ідентифікатори, що дозволяють відстежувати користувачів під час їхньої взаємодії з веб-сайтом чи застосунком, наприклад, через файли cookie, які містять інформацію про конкретну сесію використання.

Для того, щоб оцінити не гіпотетичну ймовірність, а достатню можливість за певних обставин ідентифікувати особу, мають враховуватися певні об'єктивні фактори. Зокрема, у п. 26 Преамбули до Регламенту серед таких факторів визнаються: витрати і час, необхідні для ідентифікації, технології, доступні на момент обробки персональних даних, і технологічний прогрес.[10] Причому слід враховувати, що ці фактори не є сталими, і якщо зараз немає технологічної можливості ідентифікувати особу, це не означає, що у майбутньому не з'явиться така можливість. Тож оцінка цих факторів має здійснюватися з розумною періодичністю, аби уникнути можливих порушень у сфері захисту персональних даних.

По-четверте, персональні дані мають стосуватися фізичної особи, яка виступає суб'єктом персональних даних. Суб'єктами персональних даних не може бути юридичні особи, тварини або рослини, а також інші неживі об'єкти[11]. За загальним правилом суб'єктами персональних даних є живі фізичні особи, тим не менш інформація про померлу людину також може опосередковано стосуватися інших фізичних осіб, наприклад, про спадкові захворювання, які могли передатися родичам померлої особи. У деяких державах закони про захист персональних даних застосовуються до інформації про осіб, які померли, протягом певного строку після смерті. Наприклад, у Данії протягом 10 років після смерті до інформації про особу застосовується законодавство про захист персональних даних.

З аналізу поняття персональних даних, закріпленого Конвенції № 108 та Регламенті, можемо зробити висновок, що це дуже широка, гнучка і адаптивна

[10] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
[11] GDPR: Посібник з виживання / Артем Кобрін, Дмитро Корчинський, Владіслав Некрутенко; під ред. Д. Іванова. – Одеса: Видавничий дім «Гельветика», 2022. – 228 с.

категорія. Віднесення певної інформації до персональних даних про особу дуже часто залежить від контексту, який береться до уваги.

Як слушно зазначає нідерландська професорка Надія Пуртова, поняття «персональні дані», що визначає матеріальну сферу захисту даних, має бути широким, але воно обов'язково буде розширюватися ще далі і, як наслідок, застосовуватиметься до експоненціально зростаючого діапазону ситуацій. Це пояснюється вбудованими можливостями для еволюційної інтерпретації самої концепції, швидкою генерацією та агрегацією даних, а також прогресом в аналітиці даних. Авторка звертає увагу на те, що наше повсякденне існування опосередковується інформаційними технологіями, а середовище людини швидко наближається до того, що називають «онлайновим життя». Надія використовує термін «датифікація», тобто віднесення до категорії персональних даних все більшого масиву інформації. [12]

1.2. Принципи обробки та захисту персональних даних: сутність, практичне та юридичне значення

Принципи обробки і захисту персональних даних є критеріями, найвищими стандартами та орієнтирами, яким необхідно слідкувати, аби обробка персональних даних не порушувала основні права і свободи людини, зокрема, право людини на недоторканність приватного життя, та не мала для неї негативних моральних, юридичних чи інших наслідків.

Принципи фактично концентрують і узагальнюють усі вимоги до обробки персональних даних, які висуваються законодавством, та виконують функцію своєрідного чек-листа, за яким необхідно перевіряти активність суб'єктів, які беруть участь в обробці персональних даних – контролерів та процесорів.

У контексті захисту персональних даних за проектуванням і за замовчуванням принципи обробки персональних даних виконують ключову роль: захист персональних даних за проектуванням і за замовчуванням спочатку

[12] Nadezhda Purtova (2018) The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, 40-81 [Електронний ресурс] – Режим доступу до ресурсу: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176?scroll=top&needAccess=true.

як теоретичні концепти, а згодом – як юридична вимога виникли саме для дотримання принципів обробки персональних даних та гарантування прав і свобод людини. Спроможність запровадити стандарти захисту персональних даних за проектуванням і за замовчуванням означає, що контролери розуміють принципи захисту персональних даних, а також права і свободи суб'єктів даних.[13] Причому, для кожного окремого принципу існують відповідні заходи із захисту персональних даних за проектуванням і за замовчуванням.

На важливість принципів у системі обробки персональних даних, на нашу думку, вказують декілька факторів:

1) принципи обробки персональних даних отримали своє нормативне визначення в актах міжнародного, регіонального та національного законодавства;

2) принципи сформульовані як чіткі вимоги до діяльності суб'єктів, залучених до обробки персональних даних (контролерів, процесорів), і конкретизуються через встановлення низки юридичних обов'язків;

3) недотримання принципів обробки персональних даних виокремлюється як окремий вид правопорушення. Зокрема, відповідно до Регламенту недотримання основних принципів обробки віднесено до категорії найбільш серйозних порушень. Санкція за такі порушення передбачає накладання штрафу у розмірі до 20 млн євро або 4% від доходу організації, отриманого у всьому світі за попередній фінансовий рік, залежно від того, яка сума більша.[14] Для прикладу, одним з найбільших штрафів, накладених за час дії Регламенту, є штраф, отриманий у 2021 році компанією WhatsApp Ireland Ltd. (входить до холдингу Meta Platforms Inc.) у розмірі 225 млн євро за порушення принципу прозорості, закріпленого у п. «а» ч. 1 ст. 5 Регламенту. До порушення цього принципу призвело невиконання компанією свого обов'язку щодо належного

[13] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[14] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

інформування користувачів щодо своєї практики обробки персональних даних у Повідомленні про обробку персональних даних (англ. Privacy Notice).[15]

Принципи обробки персональних даних були вперше сформульовані Організацією з економічного співробітництва та розвитку (далі – ОЕСР) та закріплені у «Керівних принципах захисту приватності і транскордонних потоків персональних даних» (англ. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), схвалених Рекомендацією Ради ОЕСР від 23 вересня 1980 р., нова редакція яких була затверджена у 2013 році.[16] Наразі документ включає 8 принципів, серед яких: принцип обмеження збору, принцип якості даних, принцип визначення цілі, принцип обмеження використання, принцип гарантії безпеки, принцип відкритості, принцип індивідуальної участі.[17]

Рекомендації ОЕСР не мають нормативного характеру, а тому першим юридично обов'язковим документом, який закріпив принципи обробки, була Конвенція № 108 (ст. 5). Конвенція № 108 заклала підвалини для подальшого формування галузевого законодавства у всьому світі.

Станом на зараз взірцем для розвитку законодавства у сфері захисту персональних даних та документом, який найбільш повно регламентує обробку персональних даних, є Регламент, ст. 5 якого присвячена основним принципам.

У національному законодавстві, зокрема, Законі України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI (надалі – Закон), категорія «принципи обробки персональних даних» не використовується, натомість у ст. 6 Закону закріплені загальні вимоги до обробки персональних даних, а у ст. 24 Закону визначаються вимоги до гарантування безпеки даних. Положення Закону в цілому відтворюють положення Директиви. Єдина

[15] Decision of the Data Protection Commission in the matter of WhatsApp Ireland Limited [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf.

[16] Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник/М. Бем, І. Городиський, Г. Саттон, О. Родіоненко; Європейський Союз, Рада Європи - К.: К.І.С., 2015. – 220 с. [Електронний ресурс] – Режим доступу до ресурсу: https://rm.coe.int/168059920c.

[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Adopted September 23, 1980. Updated July 11, 2013 [Електронний ресурс] – Режим доступу до ресурсу: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

відмінність від Регламенту – це відсутність принцип підзвітності, який став нововведенням Регламенту.

Принципи захисту персональних даних включають:

1. Принцип законності, справедливості та прозорості (англ. Lawfulness, fairness and transparency). Законність обробки вимагає: 1) наявності належної правової підстави для обробки (згода, виконання договірного зобов'язання, дотримання вимог закону тощо); 2) здійснення обробки відповідно до законодавства. Справедливість означає, що суб'єкти даних повинні знати про те, що їхні персональні дані будуть оброблятися і, зокрема, як персональні дані будуть збиратися, зберігатися та використовуватися. На основі цієї інформації суб'єкти повинні прийняти обґрунтоване рішення, чи погоджуються вони на таку обробку, і розуміти, чи є можливість реалізувати свої права на захист персональних даних[18]. Прозорість висуває до контролера вимогу бути відкритим, вчасно, нелажним чином, у повному обсязі, у легкій та доступній формі повідомляти суб'єктів даних про обробку даних, їхні права відносно такої обробки та способи їх реалізації.

2. Принцип обмеження метою (англ. Purpose limitation). Збір і обробка персональних даних повинні здійснюватися для конкретних, чітких та законних цілей. Мета обробки – це той результат, для досягнення якого взагалі виникла необхідність у будь-яких діях з персональними даними. Мета повинна бути визначена ще до того, як дані будуть зібрані, чи у момент збору. Подальша обробка персональних даних для інших цілей, крім історичних, наукових, архівних та статистичних цілей, має бути сумісною з первинною ціллю.

3. Принцип мінімізації даних (англ. Data minimisation). Персональні дані повинні оброблятися виключно у тому обсязі, в якому це необхідно для цілі обробки. Таким чином, збирання надмірних чи нерелевантних даних заборонено. Якщо досягти цілі можливо без обробки даних, необхідно відмовитися від їхнього використання.

[18] GDPR: Посібник з виживання / Артем Кобрін, Дмитро Корчинський, Владіслав Некрутенко; під ред. Д. Іванова. – Одеса: Видавничий дім «Гельветика», 2022. – 228 с.

4. Принцип точності (англ. Accuracy). Персональні дані повинні бути актуальними протягом свого життєвого циклу та за необхідності оновлюватися та доповнюватися.

5. Принцип обмеження зберігання (англ. Storage limitation). Персональні дані не повинні зберігатися у формі, що дозволяє ідентифікацію особи, довше, аніж це необхідно для досягнення цілей обробки. Контролери мають прагнути зберігати дані протягом мінімально можливого строку. Після закінчення цього строку дані можуть бути анонімізовані, тобто позбавлені ідентифікаторів, або видалені, якщо інше не передбачено законодавством.

6. Принцип цілісності і конфіденційності (англ. Integrity and confidentiality). Цей принцип чітко визначений у Регламенті, проте недостатньо сформульований у Законі. Він висуває вимоги до технічних та організаційних заходів, які мають вживатися для гарантування безпеки даних, зокрема, безпеки від несанкціонованої чи незаконної обробки чи доступу (конфіденційність), несанкціонованої зміни, підміни (цілісність).

7. Принцип підзвітності (англ. Accountability). Цей принцип є нововведенням Регламенту і фактично кристалізує необхідність дотримання усіх його вимог. Принцип підзвітності передбачає обов'язок процесора і контролера вести облік діяльності щодо обробки та мати змогу за запитом контролюючого органу продемонструвати дотримання вимог Регламенту.[19] Принцип підзвітності покладає на контролера відповідальність за вибір необхідних організаційних та технічних заходів.

Питання дотримання принципів обробки і захисту персональних даних неодноразово розглядалося ЄСПЛ у контексті порушення права на недоторканність приватного життя. Зокрема, у справі Khadija Ismayilova v. Azerbaijan (2019), зокрема, розглядалося питання дотримання принципу мінімізації даних. Справа стосувалася надмірного порушення права на

[19] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

недоторканність приватного життя і свободи слова азербайджанської журналістки, яка займалася розслідування фактів корупції та порушенні прав людини владою Азербайджану. За матеріалами справи у 2012 році Ісмайлова отримала лист з фотографіями інтимного характеру, знятими у її спальні прихованою камерою, і шантажем, пов'язаним з її професійною діяльністю. Ці фотографії, а також відео інтимного характеру, зняте тією ж прихованою камерою, згодом були опубліковані в Інтернеті. За зверненням Ісмайлової прокуратура почала розслідування за фактом порушення недоторканності приватного життя, і сама згодом допустила такого ж порушення. За результатами розслідування прокуратура опублікувала звіт, у якому розкривалися дані особистого характеру про адресу проживання, членів родини та друзів потерпілої, які вона повідомила з розумінням того, що буде збережена конфіденційність такої інформації. Уже під час розгляду справи у ЄСПЛ влада Азербайджану не змогла пояснити необхідність такого втручання у приватне життя і надмірне розкриття даних особистого характеру у звіті. Мета звіту була проінформувати громадськість про стан розслідування та діяльність правоохоронних органів, і цієї мети можна було досягти без поширення подробиць про особисте життя потерпілої, зокрема, про партнера потерпілої, який також потрапив на відео, які без відома потерпілої зняті у її спальні. ЄСПЛ визнав порушення права на недоторканність приватного життя.[20]

Таким чином, принципи обробки і захисту персональних даних мають важливе практичне значення і визначають критерії того, як мають оброблятися персональні дані, аби не створювалися загрози для прав і свобод людини.

[20] Khadija Ismayilova v. Azerbaijan, nos. 65286/13 and 57270/14, 10 January 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-188993%22]}.

1.3. Іноземний досвід нормативно-правового регулювання захисту персональних даних за проектуванням та за замовчуванням та національні перспективи

Аналіз іноземного досвіду нормативно-правового регулювання захисту персональних даних за проектуванням і за замовчуванням є необхідний, насамперед, для того, аби під час адаптації українського законодавства у сфері захисту персональних даних до найвищих стандартів Європейського Союзу та Ради Європи ці концепти були більш зрозумілими як з теоретичної, так і з практичної точки зору.

Гарантування належного рівня захисту персональних даних – це важлива складова наближення України до членства в Європейському Союзі, а також підвищення привабливості українського ІТ-сектору для європейських партнерів та користувачів.

На виконання ст. 15 Угоди про асоціацію України з Європейським Союзом в Україні вже декілька років триває процес розробки законодавства у сфері захисту персональних даних, яке б відповідало положенням Регламенту та гарантувало в Україні належний рівень захисту права людини на недоторканність приватного життя у розрізі захисту персональних даних.

Необхідно зазначити, що у поточній редакції Закону України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI відсутня юридична вимога щодо захисту персональних даних за проектуванням і за замовчуванням. Це є суттєвим недоліком, адже Україна прагне бути цифровою державою і кластером з розробки інформаційних технологій, продуктів та рішень. А для функціонування багатьох з них необхідна обробка персональних даних. Зокрема, чимало цифрових сервісів державного значення, якими користується більшість українців, мають справу з персональними даними.

Наразі на розгляді у Верховної Ради України перебуває Проект Закону «Про захист персональних даних» № 5628 від 07 червня 2021 року[21], ст. 29 якого

[21] Проект Закону «Про захист персональних даних» № 5628 від 07.06.2021 року [Електронний ресурс] – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160.

присвячена захисту персональних даних за проектуванням і за замовчуванням, що є першою спробою нормативного закріплення цих концептів та свідчить про суспільний та законодавчий інтерес до них. Положення ст. 29 Проекту в цілому відтворює положення ст. 25 Регламенту, проте потребує доопрацювання, зокрема, необхідно деталізувати, що саме слід розуміти під «інтеграцією захисних гарантій в процес обробки персональних даних» (п. 3 ч. 1 ст. 29).

Потреба у науковій розробці концептів захисту персональних даних, які б допомогли інтегрувати ідею захисту персональних даних та приватності у бізнес-практику, продукти та сервіси ще на стадії планування і протягом всього життєвого циклу виникла ще наприкінці XX століття. Це було пов'язано із стрімким технологічним прогресом, цифровізацією суспільства та все більшим використанням персональних даних світовими технологічними гігантами.

У п. 46 Преамбули Директиви, яка була прийнята 1995 року, визначалася необхідність запровадження належних організаційних та технічних заходів як у момент розробки системи обробки, так і під час самої обробки, зокрема, для гарантування безпеки.[22] Окрім цього, питанню безпеки обробки і персональних даних була присвячена ст. 17 Директиви.

Це був лише перший крок до подальшого нормативного закріплення захисту персональних даних за проектуванням і за замовчуванням, адже на момент прийняття Директиви ще була відсутня достатня теоретична база.

Важливою віхою у визнанні захисту персональних даних за проектування як «необхідного компоненту фундаментального захисту персональних даних» була «Резолюція про захист персональних даних за проектування», прийнята у 2010 році на 32-й Міжнародній конференції комісарів із захисту персональних даних.

[22] Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [Електронний ресурс] – Режим доступу до ресурсу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

Конференція запропонувала органам із захисту даних просувати захист персональних даних за проектуванням під час формулювання політики та законодавства в межах їхньої відповідної юрисдикції.[23]

Вперше на законодавчому рівні захист персональних даних за проектуванням і за замовчуванням був визначений як юридична вимога, що висувається до обробки персональних даних, був визначений з прийняттям Регламенту у 2016 році.[24] У ст. 25 Регламенту під назвою «Захист персональних даних за проектуванням і за замовчуванням» (англ. Data protection by design and by default) у нормативну площину запроваджено практику врахування захисту персональних даних з перших стадій розробки продуктів та послуг.[25]

Запровадження концептів у Регламент була викликана необхідністю у новому підході, який би гарантував, що основні права людини беруться до уваги для створення технологій, які стосуються усіх засобів обробки даних.[26]

Оскільки у Регламенті захист персональних даних за проектування і за замовчуванням отримав статус юридично обов'язкових вимог, недотримання цих вимог тягне за собою накладання санкцій відповідно до ст. 83 Регламенту. У свою ж чергу, у разі вчинення суб'єктом інших правопорушень під час визначення ступеня його відповідальності враховується вжиття технічних та організаційних заходів для захисту персональних даних за проектування і за замовчуванням.[27]

---

[23] Resolution on Privacy by Design" adopted by the 32th Conference of Data Protection and Privacy Commissioners in October 2010 [Електронний ресурс] – Режим доступу до ресурсу: http://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.

[24] Information Commissioner's Office (ICO). Data protection by design and default [Електронний ресурс] – Режим доступу до ресурсу: https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-anddefault/.

[25] A Guide to Privacy by Design. Spanish Data Protection Agency (AEPD). Adopted October, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

[26] European Data Protection Supervisor, Opinion 5/2018 Preliminary Opinion on privacy by design. Adopted May 31, 2018 [Електронний ресурс] – Режим доступу до ресурсу: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[27] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Виходячи зі ст. 25 Регламенту та п.78 Преамбули до Регламенту, обов'язок щодо запровадження захисту персональних даних за проектування і за замовчуванням стосується усіх контролерів незалежно від їхнього розміру, категорії даних та природи самої обробки.[28] Тож помилково вважати, що вимоги ст. 25 Регламенту стосуються лише світових корпорацій, які оперують великими масивами персональних даних, таких як Amazon, Meta, Apple, Google.

Хоча захист персональних даних за проектування і за замовчуванням, у першу чергу, є сферою відповідальності контролерів, однак відповідно до ч. 1 ст. 28 Регламенту контролер має використовувати послуги лише тих процесорів, які надають достатні гарантії щодо впровадження належних технічних та організаційних заходів, щоб обробка відповідала вимогам Регламенту та забезпечувала захист прав суб'єктів даних. Таким чином, до процесорів також опосередковано застосовуються вимоги щодо захисту персональних даних за проектування і за замовчуванням, а контролер відповідальних за виконання вимог ст. 25 Регламенту щодо обробки персональних даних, яку здійснюють процесори та субпроцесори.[29] Ця вимога також застосовна до спільних контролерів на підставі відповідальності, яку вони разом беруть на себе під час спільного визначення цілей та засобів обробки.[30]

Окрім Регламенту, вимогу захисту персональних даних за проектування і за замовчуванням передбачено також прийнятим у 2018 році Радою Європи Протоколом про внесення змін до Конвенції Ради Європи від 28 січня 1981 року № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (надалі – Протокол), який вже підписали 27 держав світу, а 12 з них – ратифікували.[31] Зокрема, Протокол доповнює Конвенцію № 108 новою ст. 10, де

[28] A Guide to Privacy by Design. Spanish Data Protection Agency (AEPD). Adopted October, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

[29] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[30] A Guide to Privacy by Design. Spanish Data Protection Agency (AEPD). Adopted October, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

[31] Chart of signatures and ratifications of Treaty. Council of Europe [Електронний ресурс] – Режим доступу до ресурсу: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

у ч. 3 визначено, що кожна держава-член має гарантувати, що контролери, і коли застосовується, процесори вживають технічних і організаційних заходів, які враховують наслідки для права на захист персональних даних на всіх етапах обробки даних.[32]

Протокол набуде чинності, коли її ратифікують 38 держав-підписантів Конвенції № 108, або 11 жовтня 2023 року, якщо станом на цю дату буде не менше 38 сторін Протоколу. У зв'язку з тим, що Конвенція № 108 відкрита до підписання будь-якими державами світу, а не лише членами Ради Європи, та до сьогодні залишається єдиним міжнародним документом, що регламентує обробку і захист персональних даних, усе більше держав будуть запроваджувати високі стандарти захисту персональних даних, зокрема, за проектуванням і за замовчуванням.

Оскільки Україна прагне підвищувати стандарти захисту персональних даних і дотримання прав і свобод людини, питання підписання і ратифікації Протоколу, який модернізує Конвенцію № 108, є вкрай актуальним питанням.

Що стосується перспектив впровадження в українське законодавство концептів захисту персональних даних за проектуванням і за замовчуванням як конкретної юридичної вимоги слід зазначити наступне. По-перше, це є необхідним з огляду на розвиток суспільних відносин і прагнення побудувати в Україні цифрову державу і цифрову економіку із високими стандартами дотримання прав людини, зокрема, у контексті її взаємодії з новітніми інформаційними технологіями (віртуальна та доповнена реальність, машинне навчання, Інтернет речей тощо). По-друге, питання удосконалення законодавства у сфері законодавства є лише питанням часу і пріоритетів у державній політиці України. Строк виконання зобов'язання щодо приведення законодавства у сфері захисту персональних даних до європейських стандартів, передбаченого ст. 15 Угоди про асоціацію України з ЄС, у будь-якому випадку

[32] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [Електронний ресурс] – Режим доступу до ресурсу: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.

уже порушено. Поточна редакція ст. 29 Проекту є цілком прийнятною, однак для її правозастосування необхідна розробка роз'яснень та методичних рекомендацій, адже загальні положення не дають конкретних інструкцій, як діяти контролерам, і потребують уточнень з боку наглядового органу.

Висновки до Розділу 1

У сучасному світі персональні дані стали надцінним ресурсом, який може використовуватися як на благо особи, так і з порушенням її прав і основоположних свобод. Поняття персональних даних в актах міжнародного і національного законодавства охоплює великий обсяг інформації, яка може стосуватися фізичної особи, і трактування цього поняття має тенденцію до розширення, зокрема, у зв'язку із взаємодією людини інформаційними технологіями (віртуальна реальність, використання інтернету речей).

Порушення, пов'язані із використанням персональних даних, можуть мати не лише негативні моральні, юридичні чи фінансові наслідки, але й створювати загрозу для фізичного існування людини чи окремих соціальних, національних, релігійних або інших груп.

У зв'язку з цим набувають критично важливого значення принципи захисту персональних даних та механізми, які допоможуть особі зберігати контроль над використанням даних про неї, з одного боку, а суб'єктам, які для тих чи інших цілей здійснюють обробку даних, дотримуватися вимог законодавства та не порушувати прав і свобод людини.

Як відповідь на нові виклики цифрової економіки виникли концепти захисту персональних даних за проектуванням і за замовчуванням, що покликані вбувати ідею захисту прав людини на всіх етапах створення і реалізації бізнес-процесів, систем, продуктів та послуг. Тобто, ще на етапі планування будь-якої технології і, відповідно, перед початком діяльності з обробки, повинні виникати питання, чи не будуть порушуватися права людини, чи гарантується особі належний захист персональних даних, а не постфактум, коли порушення уже сталося.

Першим нормативно-правовим актом, що визначив захист персональних даних за проектуванням і за замовчуванням як обов'язкову юридичну вимогу, був Регламент Європейського Парламенту і Ради (ЄС) 2016/679 «Про захист фізичних осіб у зв'язку з обробкою даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» від 27 квітня 2016 року. Оскільки Україна прагне побудувати цифрову державу та відповідати високим стандартам Європейського Союзу та Ради у сфері захисту персональних даних, процес удосконалення національного законодавства у цій сфері триває, і вже у Проекті Закону «Про захист персональних даних» № 5628 від 07 червня 2021 року окрема стаття присвячена захисту персональних даних за проектуванням і за замовчуванням. Положення Проекту в цілому відтворюють положення Регламенту, однак потребують доопрацювання, а у подальшому – методичних роз'яснень для правильного правозастосування.

РОЗДІЛ 2. Організація захисту персональних даних за проектуванням і за замовчуванням

2.1. Сутність та особливості захисту персональних даних за проектуванням

Незважаючи на те, що концепти захисту персональних даних за проектуванням і за замовчуванням набули нормативного визначення лише з прийняттям та набранням чинності Регламентом, ці ідеї не є новими. Перші думки щодо захисту персональних даних за проектуванням висловлювалися ще у 1970-х роках, а у 1990-х були частково втілені у Директиві.[33]

Вважається, що авторкою концепту приватності за проектування (англ. Privacy by design) є колишній Комісар з питань інформації та приватності провінції Онтаріо (Канада) Анною Кавукян.[34]

Для коректного розуміння та уникнення неточного розуміння необхідно звернути на термінологічний аспект і співвідношення категорій «приватність за проектування» (англ. Privacy by design) та «захист персональних даних за проектуванням» (англ. Data protection by design).

Приватність за проектуванням – це широка теоретико-практична та етична концепція вжиття технічних заходів для забезпечення приватності, у той же час захист персональних даних за проектуванням – це конкретний юридичний обов'язок контролера відповідно до ч. 1 ст. 25 Регламенту. Фактично, виконання вимог ст. 25 Регламенту щодо захисту персональних даних за проектуванням і за замовчуванням спрямовано на досягнення більш загальної мети приватності за проектуванням (англ. Privacy by design).[35] Таким чином, ці два концепти взаємно доповнюють одне одного і посилюють.

---

[33] GDPR. Privacy by design [Електронний ресурс] – Режим доступу до ресурсу: https://gdpr-info.eu/issues/privacy-by-design/.

[34] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

[35] European Data Protection Supervisor, Opinion 5/2018 Preliminary Opinion on privacy by design. Adopted May 31, 2018 [Електронний ресурс] – Режим доступу до ресурсу: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

У 1990-х роках Анна Кавукян сформувала концепцію приватності за проектуванням (англ. Privacy by design) для вирішення системних проблем, пов'язаних з розвитком інформаційних і комунікаційних технологій та великомасштабних мережевих систем даних.

У 2009 році у своїй статті «Privacy by Design: The 7 Foundational Principles» Анна Кавукян виклала 7 основних принципів приватності за проектуванням, зазначивши, що «приватність за проектуванням просуває думку про те, що майбутнє приватності не може бути забезпечене лише дотримання нормативним вимогам; скоріше, гарантування приватності в ідеалі має стати режимом роботи організації за замовчуванням».[36]

Таким чином, ідея приватності за проектуванням була сформована як своєрідний локомотив, який має спрямовувати проектування процесів, продуктів і сервісів, які з самого початку налаштовані на захист персональних даних. Якщо в людини збирають персональні дані, їх конфіденційність і безпека – це не опція, а налаштування за замовчуванням.[37]

Принципи приватності за проектуванням, запропоновані Анною Кавукян, включають[38]:

1. Проактивність у захисті персональних даних (англ. Proactive not Reactive; Preventative not Remedial). Захист персональних даних має бути одразу продуманий і передбачений у будь-якому продукті, системі чи послузі. Захист персональних даних має визначати дизайн, а не навпаки.[39] Тобто йдеться про те, щоб заздалегідь визначати ризики, вразливості, які можуть вплинути на захист персональних даних, та вживати заходи для зменшення їхнього потенційного впливу. Для цього важливо запровадити методи виявлення процесів і практик,

[36] Privacy by Design: The 7 Foundational Principles, Ann Cavoukian, 2009 [Електронний ресурс] – Режим доступу до ресурсу: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.
[37] GDPR: Посібник з виживання / Артем Кобрін, Дмитро Корчинський, Владіслав Некрутенко; під ред. Д. Іванова. – Одеса: Видавничий дім «Гельветика», 2022. – 228 с.
[38] Privacy by Design: The 7 Foundational Principles, Ann Cavoukian, 2009 [Електронний ресурс] – Режим доступу до ресурсу: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.
[39] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

які не гарантують захисту персональних даних, а також формувати культуру захисту персональних даних серед співробітників.[40]

2. Захист персональних даних як налаштування за замовчуванням (англ. Privacy as the Default Setting). Захист персональних даних і режим приватності має бути налаштований одразу і не вимагати жодних додаткових дій особи. Відповідальність за налаштування режиму приватності та захист персональних даних не має перекладатися на особу. Навіть якщо фізична особа ніяк не змінить стандартні налаштування, високий рівень захисту персональних даних має бути незмінним.[41] Користувач повинен мати право самостійно вирішити, яка інформація про нього буде відкритою у профілі у соціальні мережі, чи буде доступна його публікація лише серед друзів чи публічно тощо. «За замовчуванням» означає збереження статусу-кво недоторканості приватного життя у тій чи іншій ситуації. Визначення того, що має гарантуватися «за замовчуванням», вимагає розуміння контексту ситуації, а також очікування залучених осіб. Наприклад, якщо лікар використовує результати аналізів для визначення діагнозу і лікування, це є очікуваним для пацієнта. Але використання цих же результатів аналізів, наприклад, для публікації у соціальних мережах виходить за межі надання медичних послуг і не гарантує захист персональних даних за замовчуванням.[42]

3. Захист персональних даних вбудований у дизайн (англ. Privacy Embedded into Design). Захист персональних має бути невід'ємною частиною та вимогою до бізнес-практики, функціонування систем, продуктів та сервісів. Невід'ємність у цьому разі означає, що без захисту персональних даних системи, продукти та сервіси не зможуть функціонувати. Наприклад, якщо месенджер використовує

[40] A Guide to Privacy by Design. Spanish Data Protection Agency (AEPD). Adopted October, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

[41] A Guide to Privacy by Design. Spanish Data Protection Agency (AEPD). Adopted October, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

[42] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

наскрізне шифрування, надсилання незашифрованих повідомлень є технічно неможливим.

4. Застосування підходу «позитивної суми» (англ. Full Functionality – Positive Sum, Not Zero Sum). Цей принцип означає, що для захисту приватності не потрібно жертвувати зручністю сервісу.[43] Таким чином захист персональних даних має бути вигідним для усіх сторін: як для розробника і власника сервісу, так і для кінцевого користувача. Цей принцип покликаний вирішити дихотомії приватність-зручність, приватність-функціональність, приватність-вигоди бізнесу, приватність-безпека.[44] У реалізації цього принципу є декілька аспектів:

1) визначення, аналізу та збалансування інтересів контролера і користувача;

2) необхідність чіткого розуміння мети роботи сервісу і використання персональних даних, адже деякі сервіси з самого початку можуть спрямовуватися на порушення права особи на недоторканність приватного життя;

3) використання технологій та рішень, які сприяють захисту персональних даних (англ. Privacy-enhancing technologies).[45]

5. Захист персональних даних на усіх стадіях (англ. End-to-End Security – Full Lifecycle Protection). Захист персональних даних має бути вбудований у дизайн ще до того, як такі дані будуть зібрані, і має гарантуватися на всіх стадіях обробки і життєвого циклу даних, від початку і до кінця. Це включає, зокрема, безпечне зберігання, поширення та видалення даних.

6. Прозорість (англ. Visibility and Transparency – Keep it Open). Особа має бути достатньо проінформована про те, як обробляються її персональні дані, аби прийняти рішення, чи користуватися певним сервісом, як себе поводити, і чи

[43] GDPR: Посібник з виживання/Артем Кобрін, Дмитро Корчинський, Владіслав Некрутенко; під ред. Д. Іванова. – Одеса: Видавничий дім «Гельветика», 2022. – 228 с.

[44] A Guide to Privacy by Design. Spanish Data Protection Agency (AEPD). Adopted October, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

[45] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

самостійно убезпечувати себе (наприклад, надавати неправдиву інформацію тощо).[46] Способами реалізації цього принципу є:

1) розробка Повідомлення про обробку персональних даних (англ. Privacy Notice) простою мовою, у зрозумілій формі;

2) легка доступність інформації про обробку персональних даних та особу контролера, простий спосіб звернення до контролера з питаннями щодо обробки персональних даних, зокрема, для реалізації прав суб'єкта персональних даних;

3) можливість легко відкликати згоду на обробку персональних даних, якщо вона використовується як правова підстава тощо.

7. Орієнтація у захисту персональних даних на кінцевого користувача (анг. Respect for User Privacy – Keep it User-Centric). Захисту прав та інтересів особи-кінцевого користувача має приділятися першочергова увага, оскільки саме користувачі зацікавлені у захисту їхніх персональних даних і зазнають негативних наслідків у разі будь-яких порушень. Суб'єкт даних повинен займати активну позиції в управлінні своїми даними і контролем над тим, що з цими даними роблять інші. У той же, час бездіяльність суб'єктів не повинна впливати на рівень захисту персональних даних.[47] Реалізація цього принципу включає такі кроки:

1) повідомлення суб'єкта про наслідки зміни стандартних налаштувань, які за замовчуванням гарантують максимальний рівень захисту персональних даних;

2) вчасне, повне повідомлення суб'єкту усієї необхідної інформації, яка стосується обробки його персональних даних;

3) забезпечення надання суб'єктом проінформованої, вільно наданої, конкретної згоди на обробку даних, якщо вона застосовується як правова підстава.

---

[46] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

[47] A Guide to Privacy by Design. Spanish Data Protection Agency (AEPD). Adopted October, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

4) надання суб'єкту можливість доступу до його персональних даних та за потреби можливості їхнього видалення чи зміни (наприклад, в інтерфейсі мобільного застосунку);

5) впровадження простих та ефективних механізмів реалізації прав суб'єктів даних.

Запропоновані Анною Кавукян принципи неодноразово критикувалися за їхню загальність, неконкретність для безпосереднього застосування у процесі розробки, за те, що не містять конкретні поради, які б задовольняли потреби конкретних технологій.[48] І хоча вони не отримали свого прямого нормативного закріплення, проте у ст. 25 Регламенту, яка визначає захист персональних даних за проектуванням і за замовчуванням, вони чітко простежуються. Цей факт ще раз підтверджує пов'язаність законодавчих процесів з рівнем наукової розробки окремих питань.

Всесвітньо визнаний спеціаліст із захисту персональних даних Джейсон Кронк проаналізував ст. 25 Регламенту під назвою «Захист персональних даних за проектуванням і за замовчуванням» щодо впровадження у ній принципів, запропонованих Анною Кавукян[49]:

1. Зважаючи на поточний рівень науково-технічного прогресу [Принцип 4. Застосування підходу «позитивної суми»], витрати на впровадження, характер, масштаб, контекст та мету обробки, а також ризики, пов'язані з тією чи іншою ймовірністю та серйозністю порушення прав і свобод фізичних осіб [Принцип 7. Орієнтація у захисту персональних даних на кінцевого користувача], спричинених обробкою, контролер, як у час визначення засобів обробки, так і під час самої обробки [Принцип 1. Проактивність у захисті персональних даних], впроваджує належні технічні та організаційні заходи, наприклад, псевдонімізацію, призначені для ефективної реалізації принципів захисту

[48] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfaheicher, "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Paerns," Proceedings on Privacy Enhancing Technologies 2016, no. 4, Oct. 23, 2016, 237–254 [Електронний ресурс] – Режим доступу до ресурсу: https://www.petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf.

[49] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

персональних даних, таких як мінімізація даних, а також для інтеграції необхідних гарантій [Принцип 3. Захист персональних даних вбудований у дизайн] у обробку з метою дотримання вимог цього Регламенту та захисту прав суб'єктів даних [Принцип 6. Прозорість].

2. Контролер впроваджує належні технічні та організаційні заходи для забезпечення того, щоб за замовчуванням [Принцип 2. З Захист персональних даних як налаштування за замовчуванням] оброблялися лише персональні дані, обробка яких потрібна для конкретної мети обробки. Це зобов'язання поширюється на кількість зібраних персональних даних, ступінь їх обробки, строк їх зберігання та доступність. Зокрема такі заходи повинні гарантувати, що за замовчуванням персональні дані не будуть доступні без втручання особи для невизначеного кола фізичних осіб [Принцип 5. Захист персональних даних на усіх стадіях].

У ч. 1 ст. 25 Регламенту визначений обов’язок вживати під час обробки «належні технічні та організаційні заходи» (англ. appropriate technical and organisational measures), а також «необхідні гарантії» (англ. necessary safeguards). Технічні та організаційні заходи можуть включати широкий спектр можливих дій: від шифрування, псевдонімізації даних, контролю доступу та фізичної безпеки до проведення тренінгів серед співробітників організації.

Належність заходів означає, що вони повинні відповідати поставленим цілям і сприяти ефективній реалізації принципів захисту персональних даних. Принцип належності тісно пов’язаний з принципом ефективності.[50] Ефективність має визначатися контролером за заданими ним параметрами (англ. Key performance indicators). Таким чином, принципи захисту персональних даних виступають у якості цілей, які потрібно досягти завдяки вжиттю відповідних заходів.

[50] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

З аналізу положення ст. 25 Регламенту можна зробити висновок, що немає обов'язкового переліку організаційних і технічних заходів, а також гарантій, які мають вживатися контролером для забезпечення захисту персональних даних за проектуванням. Натомість визначені фактори, які повинні у сукупності враховуватися під час вибору належних заходів:

1) поточний рівень науково-технічного прогресу (англ. State of art) – контролер повинен враховувати актуальний рівень розвитку технологій на ринку чи у певній сфері і відповідальний за вибір заходів з можливих доступних у конкретний момент (наприклад, використання найновіших типів шифрування, практик менеджменту). Оскільки розвиток технологій динамічний, він має аналізуватися на постійній основі;[51]

2) витрати на впровадження – стосуються витрат ресурсів у цілому, зокрема, часу та людських ресурсів. Витрати мають бути пропорційними потенційним ризикам для фізичних осіб, однак контролери повинні гарантувати принципи захисту персональних даних та права суб'єктів незалежно від обсягу витрат;

3) характер, масштаб, контекст та мету обробки: характер обробки стосується її властивостей; масштаб – обсягу та діапазону; контекст – обставин обробки, які впливають на очікування суб'єкта даних; мета – цілей, для досягнення яких обробка необхідна[52];

4) ризики, пов'язані з тією чи іншою ймовірністю та серйозністю порушення прав і свобод фізичних осіб – застосовується ризик-орієнтований підхід, за яким основна цінність – фізична особа через захист її персональних даних.

Відповідно до ч.1 ст. 25 Регламенту, визначення належних заходів чітко прив'язане до часового аспекту – як у час визначення засобів обробки, так і під час самої обробки. Тобто ще на етапі планування обробки, має бути встановлено, як вона буде відбуватися, які механізми і процедури будуть використовуватися.

[51] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[52] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

Після початку обробки зобов’язання контролера продовжується за ст. 25 Регламенту протягом повного циклу активності з обробки і вимагають постійного перегляду заходів, що вживаються, зокрема, контролю за дотриманням вимог ст. 25 Регламенту процесорами.

2.2. Сутність та особливості захисту персональних даних за замовчуванням

Захист персональних даних за замовчуванням (англ. Data protection by default) становить окремий юридичних обов’язок контролерів, передбачений ч. 2 ст. 25 Регламенту. Причому «за замовчуванням» у контексті обробки персональних даних означає, що програмне забезпечення, послуга, пристрій чи процедура обробки даних вручну будуть з самого початку налаштовані та організовані на збір мінімально необхідного для конкретної цілі обсягу даних, зберігання протягом суворо необхідного строку тощо.[53]

Дотримуючись обов’язку щодо захисту персональних даних за замовчуванням, контролер «впроваджує належні технічні та організаційні заходи для забезпечення того, щоб за замовчуванням оброблялися лише персональні дані, обробка яких потрібна для конкретної мети обробки. Це зобов'язання поширюється на кількість зібраних персональних даних, ступінь їх обробки, строк їх зберігання та доступність. Зокрема такі заходи повинні гарантувати, що за замовчуванням персональні дані не будуть доступні без втручання особи для невизначеного кола фізичних осіб».[54]

Зазначене формулювання прямо відсилає до дотримання принципів обробки захисту персональних даних, а саме:

1. Принципу мінімізації даних – контролер не повинен збирати більше даних, а ніж це необхідно для цілі обробки. Мають враховуватися типи, категорії

[53] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[54] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

даних, а також ступінь їхньої деталізації. Якщо досягнути поставлену ціль можливо без використання даних, за якими можна прямо ідентифікувати особу, потрібно уникнути обробки персональних даних. Наприклад, під час створення програми лояльності для клієнтів магазину, мета якої виключно накопичення бонусів, можна уникнути використання прямих ідентифікаторів); або якщо для досягнення цілі немає необхідності отримувати детальні дані, а достатньо збільш загальних (наприклад, якщо для певних цілей потрібно знати, що особа належить до певної вікової категорії, немає потреби в отриманні і точного віку, достатньо знати, що вона належить до категорії 25-30 років).

2. Принцип обмеження метою – контролер зобов'язаний збирати та обробляти лише ті персональні дані, які необхідні для конкретних, чітких та законних цілей; не використовувати дані для інших цілей, несумісних з первинною. За замовчуванням дані не мають використовуватися для цілей інших, аніж для яких вони були зібрані, окрім чітко визначених випадків. Це обмеження пов'язане з тим, що для кожної цілі обробки персональних даних, які контролер визначає ще до початку обробки, має обиратися одна з правових підстав обробки. Якщо вторинна ціль є несумісною з первинною, відповідно, контролер має обґрунтовувати подальшу обробку персональних даних для нових несумісних цілей новою правовою підставою. Наприклад, якщо компанія, що займається виготовленням товарів на замовлення, отримала номер телефону замовника для того, аби направити товар поштою, то використання цього номеру телефону для надсилання рекламних повідомлень не є сумісною ціллю.

Випадками, коли дозволена обробка персональних даних для вторинних цілей, включають:

1) винятки, передбачені п. «b» ч. 1 ст. 5 Регламенту, відповідно до якої «подальша обробка з архівною метою в публічних інтересах, із метою історичних або наукових досліджень або зі статистичною метою відповідно до ч. 1 ст. 89 GDPR не вважається несумісною з початковими цілями».[55] Тобто, ці

[55] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

цілі визначені Регламентом як сумісні автоматично і не потребують від контролера додаткових дій для законності обробки;

2) обробка для вторинної цілі базується на згоді суб'єкта персональних даних чи законодавстві ЄС або держави-члена відповідно до ч. 4 ст. 6 Регламенту;[56]

3) визнання вторинної цілі сумісною з первинною за результатами оцінки сумісності, проведеної контролером. Така оцінка сумісності проводиться з урахуванням декількох факторів, які мають оцінюватися контролером у сукупності. До таких факторів відповідно до ч. 4 ст. 6 Регламенту належать[57]:

– будь-який зв'язок між первинними і запланованими цілями. Це може охоплювати ситуації, коли подальша обробка є більш-менш передбачуваною виходячи з первинної цілі, є логічним продовженням первинної цілі чи певним чином відсилає до неї;[58]

– контекст, у якому було отримано персональні дані, зокрема, розумні очікування суб'єктів даних, засновані на відносинах із контролером. Щодо цього необхідно враховувати, чи могла фізична особа з урахуванням характеру відносин з контролером, балансу сил між ними розумно очікувати таку подальшу обробку;

– характер персональних даних та той факт, чи належать вони до категорії чутливих даних (наприклад, біометричних, генетичних, даних про здоров'я чи сексуальне життя). Від того, чи мається на увазі обробка чутливих даних, напряму залежить потенційних вплив такої обробки на права і свободи людини;

– можливі наслідки ймовірної подальшої обробки для суб'єктів даних. Контролер повинен враховувати як позитивні, так і негативні наслідки. Це,

---

[56] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

[57] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

[58] Opinion 03/2013 on purpose limitation. Article 29 Working Party. Adopted April 2, 2013 [Електронний ресурс] – Режим доступу до ресурсу: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

зокрема, може включати потенційні майбутні рішення чи поведінка третіх сторін відносно фізичної особи, а також ситуації, коли обробка може призвести до дискримінації;[59]

– наявність відповідних гарантій первинної та ймовірної обробки. Ці гарантії включають належні організаційні та технічні заходи, що вживаються контролером для уникнення небажаних наслідків обробки (псевдонімізація, агрегація даних). У разі зміни цілі суб'єкт даних має бути повідомленим про це.

3. Принцип обмеження зберігання – контролер не повинен зберігати дані довше, аніж це необхідно для цілей їх обробки, крім випадків, коли існують інші підстави для обробки даних (наприклад, виконання вимог законодавства). Строк зберігання має обмежуватися необхідним мінімумом, а контролер повинен за замовчуванням забезпечити періодичне видалення чи анонімізацію персональних даних.[60]

Окрім втілення принципів захисту персональних даних, ч. 2 ст. 25 Регламенту важлива також тим, що встановлюється зобов'язання контролера заходи, пов'язані з контролем доступу. Таким чином, має бути гарантовано, що доступ до персональних даних мають лише особи, яким це необхідно, зокрема, для забезпечення діяльності контролера (наприклад, співробітникам служби підтримки, які контактують з клієнтами сервісу).

Окрім цього, встановлюється вимога вживати заходи, які б за замовчуванням не допускали оприлюднення персональних даних і їхнє подальше поширення. Таким чином, опублікування даних чи оприлюднення іншим чином невизначеному колу осіб має здійснювати за активної участі фізичної особи, наприклад, через надання дозволу на опублікування даних у соціальній мережі чи через відповідні налаштування. Це допомагає особі зберігати контроль над

[59] Opinion 03/2013 on purpose limitation. Article 29 Working Party. Adopted April 2, 2013 [Електронний ресурс] – Режим доступу до ресурсу: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[60] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

своїми даними, уникнути небажаного розкриття та поширення фактів про своє приватне чи сімейне життя, а також будь-яких наслідків, пов'язаних з прийняттям третіми особами рішень на основі таких даних. Прикладом порушення цієї вимоги є публікування фото у соціальній мережі зі збереженням GPS метатегу з інформацією про місце, де фото було зроблене.

2.3. Захист персональних даних за проектуванням і за замовчуванням як складова забезпечення права людини на недоторканність приватного життя

Право людини на недоторканність приватного життя – це не лише невід'ємне право людини, але й критично важливий атрибут суспільства, у якому панує свобода та демократія. Це право дозволяє людині, серед іншого, обирати, яким чином позиціонувати себе у суспільстві, як самовиражатися, які стосунки будувати з іншими; зберігати контроль над своїм тілом, будувати і захищати свою репутацію, протидіяти будь-якому незаконному втручанню чи впливу, а також контролювати, яка інформація про неї відома іншим особам та як вона використовується.

Фактично, право на недоторканність приватного життя дозволяє людині залишатися самою собою, зберігати свою ідентичність та неповторність, самостійно визначати свою поведінку.

Право людини на недоторканність приватного життя закріплено як фундаментальне право людини у ст. 12 Загальної декларації прав людини 1948 року, ст. 8 Європейської конвенції про захист прав людини і основоположних свобод 1950 року, ч.1 ст. 17 Міжнародного пакту про громадянські і політичні права 1966 року, ст. 32 Конституції України, а також у багатьох галузевих актах національного законодавства.

Необхідно відзначити, що наразі немає термінологічної єдності, і у національному законодавстві та судовій практиці паралельно застосовується

категорії «приватне життя», «особисте життя», «сімейне життя».[61] Для уникнення дискусії та відповідно до західних тенденцій будемо послуговуватися поняттям «приватне життя», що включає найрізноманітніші прояви життєдіяльності людини.

Одним із аспектів недоторканності приватного життя є здатність людини, по перше, залишитися на самоті (англ. Right to be left alone), тобто бути вільною від стороннього спостереження; по-друге, зберігати контроль над своїми персональними даними, тобто самостійно визначати коли, як і якою мірою інформація про особу стає доступною для інших, знати, ким, на яких підставах та яким чином вона використовується. Це дає особистості простір для автономного існування.

У персональних даних фактично втілюється життя людини: її відносини, страхи, сподівання, слабкості, уподобання, що вона купує, їсть, дивиться, читає, як і з ким проводить свій час, який вигляд має, як звучить її голос і що відбувається з її здоров'ям. Людина є дуже вразливою, коли йдеться про використання її персональних даних, оскільки можливостей для зловживань дуже багато як з боку представників бізнесу, так і з боку владних структур.

Персональні дані можуть виступати ресурсом, товаром та джерелом влади над рішеннями і діями окремої людини та суспільства в цілому. Використання різноманітних інструментів відстежування, аналітики та профілювання, автоматичного прийняття рішень, маніпулятивних технологій за зразком темних патернів (англ. Dark patterns) в інтерфейсі – це те, що, з одного боку, приносить очевидні вигоди для бізнесу, політики та інших сфер, дозволяючи, прицільно таргетувати свої товари, послуги чи ідеї, впливати на вибір, однак разом з тим збільшує стурбованість щодо їхнього впливу на основні права та свободи людини.

[61] Породько В. Право на недоторканність особистого життя людини: проблема термінології. Підприємництво, господарство і право. 2018. № 11. С. 146–149 [Електронний ресурс] – Режим доступу до ресурсу: http://pgp-journal.kiev.ua/archive/2018/11/29.pdf.

У зв’язку з цим вже більше уваги приділяється захисту персональних даних, а представники бізнесу усвідомлюють, що серед конкурентних переваг, які сприяють формування довіри та лояльності клієнтів чи користувачів, є саме гарантування законної та безпечної обробки даних, яка не порушує права людини на недоторканність приватного життя через використання її персональних даних. Здатність захищати як свої дані, так і дані клієнтів чи користувачів уже визнається бізнес-імперативом, що дає конкурентну перевагу.[62]

Окрім цього, сучасне законодавство із захисту персональних даних стає більш деталізованим та встановлює суворі обов’язки для суб’єктів, які працюють з персональними даними, а також суттєві санкції за порушення. Для прикладу, Регламент встановлює максимальну санкцію у вигляді штрафу у розмірі до 20 млн євро, а у разі, якщо порушник – суб’єкт господарювання, – до 4% від загального річного світового обороту за попередній фінансовий рік, залежно від того, яка сума є більшою.[63] І така санкція, зокрема, застосовується за порушення принципів обробки даних та прав суб’єктів даних.

Так, усе більше суб’єктів, які пропонують товари чи послуги фізичним особам, зокрема, з використанням інформаційних технологій, зацікавленні у тому, аби захист персональних даних був частиною їхніх бізнес-процесів, таким чином задовольняти потребу відповідати вимогам законодавства та пропонувати своїм клієнтам сервіси, яким вони можуть довіряти.

З огляду на це, концепції захисту персональних за проектуванням і за замовчуванням, які через належні технічні та організаційні заходи допомагають на практиці реалізовувати принципи захисту персональних, є необхідною складовою забезпечення права на недоторканність приватного життя.

---

[62] Privacy by Design Setting a new standard for privacy certification. Deloitte [Електронний ресурс] – Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF.

[63] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Висновки до Розділу 2

Ідея захисту персональних даних за проектуванням і за замовчуванням не є новою і сформувалася під впливом стрімкого розвитку інформаційних технологій і збільшення їхнього впливу на приватну сферу життя людини. Уже наприкінці XX століття Анною Кавукян були сформовані сім основоположних принципів приватності за проектуванням, які у подальшому стали базисом для формулювання нормативних положень, що стосуються захисту персональних даних за проектуванням і за замовчуванням ст. 25 Регламенту.

Захист персональних даних за проектуванням і за замовчуванням передбачає впровадження ідеї захисту прав людини як невід'ємної складової будь-яких процесів, систем та продуктів. Це сприяє, по-перше, дотриманню принципів обробки персональних даних, зокрема, прозорості, справедливості, мінімізації даних, а, по-друге, зберігає за суб'єктом даних контроль на його персональними даними і разом з тим над своїми рішеннями, діями та навіть життям.

Механізми захисту персональних даних за проектуванням і за замовчуванням є необхідними елементами захисту права на недоторканність приватного життя, адже спрямовані на мінімізацію обсягу даних про особу, які стануть відомі стороннім суб'єктам, та, відповідно, обмеження їхнього впливу на ті сфери чи аспекти життя, які людина прагне залишити приватними.

РОЗДІЛ 3. Окремі особливості захисту персональних даних за проектуванням і за замовчуванням

3.1. Захист персональних даних за проектуванням і замовчуванням власниками цифрових сервісів: стратегії, тактики та патерни

Для розгляду питання захисту персональних даних за проектуванням і за замовчуванням власниками цифрових сервісів, необхідно надати визначення поняттю «цифровий сервіс».

Цифровим сервісом (англ. Web service) є ідентифікована веб-адресою програмна система зі стандартизованими інтерфейсами. Фактично, цифровими сервісами називають послуги, що надаються в Інтернеті.[64]

Відповідно до ДСТУ ISO/IEC 20000- 3:2017 «Інформаційні технології. Керування послугами. Частина 3. Настанова щодо визначення сфери та застосовності ISO/IEC 20000-1» (ISO/IEC 20000-3:2012, IDT), цифровий сервіс – це задоволення потреб споживачів у послугах через інформаційно-комунікаційні технології в розподіленому, обчислювальному середовищі глобальної мережі Інтернет, яким властивий переважно цифровий спосіб подання.[65]

До цифрових сервісів можна віднести веб-сайти та застосунки у сфері електронної комерції, інтернет-банкінгу, поштові сервіси, стрімінгові платформи, соціальні мережі, новинні ресурси та інші сервіси, які користувачі використовують для задоволення своїх різних потреб.

Захист персональних даних за проектуванням і за замовчуванням вимагає від власників цифрових сервісів ще на етапі планування та розробки своїх продуктів враховувати, яким чином будуть збиратися та оброблятися персональні дані користувачів; яким чином користувачі будуть повідомлятися про обробку даних, чи не будуть користувачі вводитися в оману; чи буде

[64] Що таке веб-сервіс та їх види? [Електронний ресурс] – Режим доступу до ресурсу: https://2ip.ua/ua/blog/web-services.

[65] ДСТУ ISO/IEC 20000-3:2017 Інформаційні технології. Керування послугами. Частина 3. Настанова щодо визначення сфери та застосовності ISO/IEC 20000-1 (ISO/IEC 20000-3:2012, IDT). [Електронний ресурс] – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=74969.

технічно реалізована можливість користувачів приймати свідомі рішення стосовно своїх персональних даних, зокрема, надавати вільну та проінформовану згоду на обробку даних та без зайвих зусиль відкликати її у будь-який момент; де, як і протягом якого строку будуть зберігатися персональні дані, які заходи безпеки будуть вживатися, чи буде налаштоване автоматичне видалення даних тощо.

Запровадження, розгортання, постійне функціонування та керування функціями із захисту персональних даних та відповідними контролями, що включає технічні можливості і процеси управління, називається інженерією приватності (англ. Privacy engineering)[66]. Елементами інженерії приватності є патерни та стратегії.[67] Патерни – це рішення, які повторно використовуються для частих задач. Мета патернів в інженерії приватності – втілювати і конкретизувати принципи приватності за проектуванням, розроблені Анною Кавукян. Стратегії ж мають більш загальних характер і описують фундаментальний підхід до досягнення певної мети. Стратегії можуть конкретизуватися через патерни.[68]

Стратегії інженерії приватності сформульовані нідерландським науковцем у сфері захисту персональних даних та інформаційної безпеки Йаапом-Генком Гопманом. На думку Гопмана, стратегії поділяються на стратегії, орієнтовані на обробку персональних даних, та стратегії, що спрямовані на організаційні аспекти та процедури[69]:

---

[66] Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices ,1st Edition, William Stallings, 2020.

[67] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfaheicher, "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Paerns," Proceedings on Privacy Enhancing Technologies 2016, no. 4, Oct. 23, 2016, 237–254 [Електронний ресурс] – Режим доступу до ресурсу: https://www.petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf.

[68] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfaheicher, "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Paerns," Proceedings on Privacy Enhancing Technologies 2016, no. 4, Oct. 23, 2016, 237–254 [Електронний ресурс] – Режим доступу до ресурсу: https://www.petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf.

[69] Jaap-Henk Hoepman, "Privacy Design Strategies (Lile Blue Blook)", Radboud UniversityInstitute for Computing and Information Sciences, Radboud University, 2022 [Електронний ресурс] – Режим доступу до ресурсу: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf.

1. Стратегії, орієнтовані на обробку персональних даних

1) Мінімізувати – зменшувати обробку персональних даних настільки, наскільки це можливо. Першим кроком є визначення, які персональні дані є насправді необхідними для досягнення цілей обробки, і збирати лише ці дані. Тактики мінімізації включають:

–відбір тільки необхідних даних (наприклад, на етапі реєстрації профілю на веб-сайті уникати зайвих питань чи граф для заповнення, аби не стимулювати особу надавати зайві дані);

–відсіювання даних, які не є необхідними (наприклад, не збирати дані про дату народження, якщо потрібно знати вік особи для надання певного сервісу);

–видалення частини даних, яка вже непотрібна для подальшої обробки;

–знищення даних, якщо дані зібрані випадково, у їх збереженні більше немає потреби чи особа вимагає видалення.

2) Розділяти – розділяти обробку персональних даних настільки, наскільки це можливо. Йдеться про організаційне та фізичне розділення обробки даних для зменшення ризиків. Тактики розділення включають:

– ізоляцію, тобто логічне розділення у різних базах даних для різних процесів та залучених до обробки даних осіб;

– розподілення, тобто фізичне розміщення даних на різних серверах, пристроях (наприклад, збереження даних локально на пристрої користувача замість централізованого збереження на серверах певного продукту).

3) Абстрагувати – зменшувати деталізацію персональних даних настільки, наскільки це можливо. Три основні характеристики набору даних – це точність, достовірність та придатність. Абстрагування – це зменшення точності даних зі збереженням їх достовірності та придатності для певної мети.[70] Тактики абстрагування включають:

– узагальнення, тобто переведення специфічних характеристик у більш загальні;

[70] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

– групування, що передбачає поєднання інформації про всю групу замість обробки даних про кожного члена такої групи (наприклад, оцінювати вподобання чи інтереси певної групи користувачів (діти, пенсіонери) і знаходити кореляції);

– використання наближених значень та додавання випадкових даних (наприклад, визначати місцезнаходження людини лише приблизно, у заданому діапазоні, замість збереження точних координат).

4) Приховувати – захищати персональні дані і робити їх такими, що не дозволяють прив'язку (тобто робити так, аби за даними не можна було визначити, кого вони стосуються) чи розрізнення (стосується даних про поведінку, таких як місцезнаходження або інформації, з ким спілкується особа; про існування даних взагалі невідомо). Тактики приховання включають:

– обмеження доступу до персональних даних, ускладнення можливості випадкового поширення чи зливу даних (наприклад, використовувати авторизацію та аутентифікацію для доступу до певних даних чи функцій систем);

– затуманення, тобто перетворення даних на незрозумілий масив даних для тих, хто не може їх розшифрувати (наприклад, зберігати паролі для входу в облікових запис у вигляді хеш-файлів);[71]

– руйнування кореляції між подіями, людьми і даними, видалення даних, що прямо ідентифікують особу (наприклад, видаляти зв'язок між товаром, замовленим в онлайн-магазині, та особою замовника, коли замовлення вже доставлене);

– змішування даних для приховання зв'язків між даними (наприклад, зберігати дані у великому масиві даних).

2. Стратегії, спрямовані на організаційні аспекти

1) Інформувати – інформувати суб'єктів даних про обробку персональних даних вчасно та в належний спосіб. Тактики інформування включають:

[71] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

– надання повної інформації про те, які персональні дані обробляються, яким чином і чому, строки зберігання даних, особу, що здійснює обробку, третіх сторін, яким можуть передаватися дані тощо (наприклад, розробка інформаційної панелі, де користувач може ознайомитися з тим, які його персональні обробляються, які дозволи на обробку були надані);

– пояснення різним групам користувачів, навіщо здійснюється обробка даних (наприклад, використовувати символи, малюнки для пояснення інформації про обробку даних дітям);

– вчасне повідомлення про те, що здійснюється обробка даних, передачу даних, зміни в процедурі обробки даних (наприклад, загорання червоним кольором індикатора, який сигналізує про те, що камера ввімкнена і здійснюється відеозапис)[72] .

2) Надавати контроль – надавати суб'єктам даних належний контроль над обробкою персональних даних. Тактики контролю включають:

– отримання добровільної, конкретної, інформованої, однозначної згоди на обробку даних з можливістю відкликати її у будь-який момент (наприклад, створення окремого непроставленого чек-боксу для отримання згоди на використання файлів cookie з достатньою інформацією для прийняття рішення користувачем та залишення на інтерфейсі іконки, розгорнувши яку користувач може змінити цей вибір);

– надання користувачам реального вибору за умови, що у разі ненадання згоди стандартний функціонал не обмежується (наприклад, якщо користувач не надав згоду на отримання пуш-повідомлень у мобільному застосунку чи трекінг, це не має впливати на стандартно гарантований функціонал);

– надання користувачу можливості оновлювати та доповнювати персональні дані (наприклад, через налаштування облікового запису);

– надання користувачу можливості видаляти чи просити видалення своїх даних, якщо відсутні обмеження щодо реалізації цього права.

[72] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

3) Виконувати – обробляти персональні дані у спосіб, що гарантує захист персональних даних. Ця стратегія стосується організаційних (або інколи адміністративних) заходів, які мають вживатися для зменшення ризиків для персональних даних.[73] Тактики виконання включають:

– створення внутрішніх політик, які стосуються обробки персональних даних та забезпечення їхнього виконання (наприклад, політики доступу до даних, політики зберігання і видалення даних, політики шифрування даних);

– підтримання актуальності політики організації щодо захисту персональних даних, перегляд і зміни у зв'язку зі зміною обставин.

4) Демонструвати – показувати, що персональні дані обробляються належним чином. Тактики демонстрування включають:

– документування діяльності з обробки персональних даних (наприклад, оформлення політик, ведення реєстрів обробок даних, логування дій з даними);

– регулярне проведення аудитів активності, пов'язаної з обробкою персональних даних (наприклад, проведення оцінку впливу на захист даних для виявлення потенційних ризиків, пов'язаних із запуском нового сервісу, запровадження нового функціоналу);

– звітування за результатами аудитів.

Як уже зазначалося вище, стратегії приватності конкретизуються через патерни приватності – тобто технічні рішення, інструменти, що можуть застосовуватися під час проектування цифрових сервісів для вирішення загальних проблем, та сприяють захисту персональних даних користувача.[74] Через патерни приватності втілюються стратегії захисту персональних даних за проектуванням і за замовчуванням. Серед патернів приватності виділяють наступні[75]:

[73] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

[74] Privacy design patterns and anti-patterns patterns misapplied *and* unintended consequences. N. Doty, M. Gupta. 34, 2013 [Електронний ресурс] – Режим доступу до ресурсу: https://cups.cs.cmu.edu/soups/2013/trustbusters2013/Privacy_Design_Patterns-Antipatterns_Doty.pdf.

[75] Privacy Patterns [Електронний ресурс] – Режим доступу до ресурсу: https://privacypatterns.org/.

1. Розробка багаторівневої Політики приватності. Реалізується шляхом виділення у Політиці приватності на перший план найважливіший аспектів, які користувач, скоріше за все, точно прочитає, з наданням можливості детальніше ознайомитися з кожним аспектом. Такий підхід підвищить шанс, що користувач буде належним чином проінформований про обробку його даних. Для зручності окремі частини Політики приватності можуть відображатися на різних етапах взаємодії з сервісом, використовуватися стандартизовані іконки для оформлення документу.

2. Мінімізація асиметрії в інформації. Асиметрія виникає між інформацією, якою оперує користувач про власника цифрового сервісу, та інформацією, яку відповідний власник має про ризики, з якими він стикається під час обробки даних. Така асиметрія може бути як навмисною, коли користувач спеціально вводиться в оману, та ненавмисною.[76] Мінімальна асиметрія може досягатися, з одного боку, зі зменшенням обсягу даних, що обробляються, відмовою від збору чутливих даних, наданням користувачам можливості добровільно приймати рішення щодо збільшення обсягу даних, що збираються; а з іншого боку, з наданням користувачу повної інформації про власника цифрового сервісу, написання зрозумілого, чіткого, лаконічного Повідомлення про обробку персональних даних (Політику приватності) без складної юридичної термінології, з розставленими акцентами та виділенням основної інформації.

3. Отримання конкретної згоди. Реалізується через створення простого і зрозумілого механізму надання згоди, зокрема, через непроставлений чек-бокс (англ. Opt-in checkbox) У такому чек-боксі користувачу має бути чітко зазначено, на що він погоджується з поясненням наслідків надання згоди. Мета обробки має бути деталізованою. Наприклад, формулювання «для цілей маркетингу та аналітики» не є конкретним і не дає користувачу розуміння, для чого його дані будуть використані.

[76] Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.

4. Захист від відстежування або трекінгу. Реалізується через обмеження використання технологій відстежування, наприклад, файлів cookies, пікселів, тегів, SDK, API тощо. Ці технології дозволяють фіксувати та аналізувати поведінку користувачів, їхні уподобання, використовувати зібрану інформацію для профілювання і поширення таргетованої реклами. Захист від технологій відстежування може включати, зокрема, невикористання в цілому файлів cookies, які не є необхідними для функціонування веб-сайту, періодичне видалення файлів cookies).

5. Створення інформаційної панелі з налаштуваннями приватності. Користувачі часто забувають, які дані про них збираються та на що вони надали свою згоду. Для уникнення цього створюється сторінка з налаштуваннями приватності, де користувач також може керувати своїми згодами на обробку (наприклад, на отримання маркетингових повідомлень) чи дозволів на доступ (наприклад, дозволу на доступ до камери пристрою, даних про місцезнаходження).

6. Уникнення деталізації місця розташування. Для надання певних сервісів збір інформації про місцезнаходження особи є необхідним (наприклад, для сервісів таксі, доставки, прогнозу погоди, знайомств). Тим не менш, поширення інформації про точне місцезнаходження може мати негативні наслідки у вигляді переслідування, фізичного вторгнення тощо. Рівень деталізації даних про місцезнаходження має визначатися для кожного конкретного випадку. Наприклад, для надання інформації про погоду не потрібно знати вулицю і будинок, де перебуває особа, достатньо встановити місто, де вона знаходиться. Таким чином, сервіс має бути одразу налаштований на збір поштового індексу замість точних координат.

7. Гарантування безпечності паролів. Для використання багатьох цифрових сервісів необхідно створити обліковий запис та авторизуватися за допомогою логіну та паролю (наприклад, соціальні мережі, поштові сервіси, онлайн-банкінг). Оскільки користувачі, як правило, використовують багато сервісів і створюють велику кількість облікових записів, вони часто нехтують

створенням складних паролів з різними комбінаціями символів, унікальних для кожного сервісу, а також періодичною зміною паролів. Зі свого ж боку, сервіси можуть не зволікати на недоліки паролів, пропускати короткі, слабкі та повторювані паролі. Вирішити це можна через пояснення користувачам важливості надійних паролів, їх складових, надання посилань на ресурси, які допомагають створити безпечний пароль і зберігати його, періодичне надсилання нагадувань про необхідність змінити пароль.

8. Шифрування ключами, якими володіє користувач. Шифрування, яке не дозволяє власнику сервісу отримати доступ до інформації, що зберігається чи передається користувачем.

9. Приховання реальних дій користувачів. Коли користувач взаємодіє з цифровими ресурсами, наприклад, здійснює пошук у пошуковій системі, грає в ігри, його поведінка розкриває багато інформації: уподобання, сферу діяльності, фінансове становище, стан здоров'я, деталі особистого життя тощо. Отримання цієї інформації третіми особами, зокрема, зловмисниками може мати негативні наслідки, наприклад, втрату репутації, погіршення відносин з близькими, роботодавцем тощо. Для приховання реальних дій до них одночасно додаються фейкові дії, які неможливо відрізнити від справжніх. Наприклад, щоб приховати, що особа вбивала у пошуковому запиті інформацію про розлучення, смертельні хвороби генеруються випадкові несправжні запити.

10. Повідомлення від псевдоніму. Для забезпечення конфіденційного обміну повідомлень у поштових сервісах, дошках оголошень, групах новин може використовуватися заміна сервером адреси відправника на псевдонім. Повідомлення з відповіддю буде надсилатися на псевдонімну адресу, яка потім буде замінюватися на оригінал. Таким чином, з використанням цього патерну можна запобігти непередбачувані наслідки комунікації, наприклад, політичних переслідувань.

Окрім патернів, які забезпечують захист персональних також існує категорія «темні патерни», які здебільшого використовуються під час

проектування користувацького інтерфейсу веб-сайтів та застосунків, який і забезпечує взаємодію людини з технологією.

Мета темних патернів – впливати на поведінку користувачів, обмежити їх можливість ефективно захищати персональні дані та робити свідомий вибір.[77]

Темні патерни здійснюють психологічний влив через використання певних кольорів, особливого розміщення інформації, створення оманливого вибору з приховванням невигідних для власника сервісу опцій («Пропустити», «Відмовитися», «Не питати», «Пізніше», «Відмінити») та виділення потрібних («Погодитися», «Прийняти»), приховання небажаного у великому масиві інформації тощо. Усе для того, аби схилити особу до вибору чи рішення, яке, насправді, не відповідає її інтересам. Так, фактично, людина втрачає контроль над своїми даними.

Необхідно звернути увагу на те, що Регламент як взірцевий нормативний документ із захисту персональних даних не містить визначення поняття «темні патерни». Проте визначення цієї категорії закріплено у прийнятому Законі Каліфорнії «Про права на недоторканність приватного життя» (CPRA), який набуде чинності 1 січня 2023 року: «користувацький інтерфейс, розроблений або яким маніпулюють з істотним ефектом підриву чи зменшення автономії користувача, прийняття рішень або вибору».[78] Аналогічне визначення також закріплено у Законі Колорадо «Про захист персональних даних» (CPA), який набуде чинності у липні 2023 року.[79]

Той факт, що під час розробки актів, які забезпечують захист персональних даних приділяється окрема увага питанню використання темних патернів, свідчить про поширеність і збільшення негативного впливу цього явища на користувацький досвід і розширення можливостей впливу на людину.

[77] Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. European Data Protection Board. Public consultation [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.

[78] California Privacy Rights Act of 2020 (CPRA) [Електронний ресурс] – Режим доступу до ресурсу: https://transcend.io/laws/cpra/.

[79] Colorado Privacy Act [Електронний ресурс] – Режим доступу до ресурсу: https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

Незважаючи на те, що Регламент не містить визначення темних патернів, їх використання з метою спонукання користувачів до рішень чи дій, які обмежують контроль над персональними даними, становить порушення принципів обробки персональних даних, прав суб'єктів даних та зобов'язання із захисту персональних даних за проектуванням і за замовчуванням. Ключовим для визначення того, чи є певна складова інтерфейсу темним патерном, є відповідність принципу справедливості, закріпленому у п. «а» ч. 1 ст. 5 Регламенту. Принцип справедливості вимагає, щоб персональні дані не оброблялися у спосіб, що є невиправдано шкідливим, незаконно дискримінаційним, неочікуваним або таким, що вводить в оману.[80]

Загалом, є різні класифікації темних патернів, які можуть використовувати власники цифрових сервісів. Так, у проекті Керівних принципів Європейської ради із захисту даних (від англ. European Data Protection Board) «Про темні патерни в інтерфейсах платформ соціальних мереж: як розпізнати та уникати їх» виділяються наступні темні патерни[81]:

1. Перевантаження (англ. Overloading) – це практика, коли користувач навмисно отримує велику кількість запитів, інформації, функцій для того, аби змусити його погодитися на певну практику обробки даних. Формами такого перевантаження можуть бути:

1) повторювані неодноразові запити на доступ до персональних даних, надання згоду на обробку для інших цілей з аргументацією, для чого це потрібно. Користувач, скоріше за все, втомиться від постійних запитів і надасть згоду/дозвіл, аби щоразу перед використанням цифрового сервісу не з'являлися ці запити. Наприклад, після кожної авторизації користувачу надходить запит на використання його номеру телефону з обґрунтуванням, що це необхідно для гарантування безпеки облікового запису, хоча під час реєстрації облікового

[80] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[81] Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. European Data Protection Board. Public consultation [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.

запису користувач відмовився надавати свій номер телефону. Така практика порушує принцип обмеження цілі, конкретності та добровільності згоди;

2) лабіринт приватності, коли інформація про обробку персональних даних або щодо реалізації прав суб'єктів схована на різних сторінках і складно доступна для користувача. Користувачу потрібно продивитися багато сторінок, і не знайшовши потрібну інформацію, користувач, скоріше за все, відмовиться від подальших пошуків та реалізації прав або погодиться на обробку, яка не відповідає його інтересам. Така практика порушує принцип прозорості, справедливості, інформованої згоди;

3) надмірна кількість варіантів, з яких потрібно зробити вибір, наприклад, у налаштуваннях приватності. Користувачі можуть взагалі пропустити такі налаштування, аби швидше створити обліковий запис і почати користуватися сервісом. Така практика порушує принцип прозорості та справедливості.

2. Пропуск (англ. Skipping) – це практика проектування інтерфейсу чи створення користувацького досвіду таким чином, аби користувачі забули чи не думали про всі чи деякі аспекти захисту персональних даних. Формами такого пропуску можуть бути:

1) оманливе самозаспокоєння – за замовчуванням увімкнені функції та параметри, які найбільше впливають на обробку даних. Користувач покладається на власника цифрового сервісу і не змінює стандартні налаштування, навіть якщо надається така можливість. Так можуть використовуватися проставлені чек-бокси чи мовчазна згода. Така практика свідчить про невиконання обов'язку щодо захисту персональних даних за проектуванням і за замовчуванням, добровільності згоди;

2) відволікання від дій чи інформації, що стосуються захисту персональних даних. Така практика порушує принцип прозорості, перешкоджає реалізації прав суб'єктів даних.

3. Хвилювання (англ. Stirring) – це практика впливу на вибір користувачів із зверненням до їхніх емоцій з використанням візуальних елементів. Формами такого хвилювання можуть бути:

1) емоційне хвилювання – це практика надання користувачам інформації з використанням формулювань чи візуальних зображень таким чином, аби створити у них максимально позитивне враження, відчуття безпеки, чи навпаки – страху, вини. Через такий вплив на емоційний стан користувачі можуть вчиняти дії чи приймати рішення, які суперечать їхнім інтересам. Можливе використання спонукань, заохочень, імперативних формулювань, контрасту кольорів. Наприклад, використання формулювань «ти втратиш зв'язок з друзями», «ти не зможеш відновити свій обліковий запис». Така практика порушує принцип прозорості, справедливості, перешкоджає реалізації прав суб'єктами даних, наданню проінформованої згоди;

2) приховання на виду – це використання візуальних елементів таким чином, аби спонукати користувача обрати той варіант, що є більш інвазивним по відношенню до нього самого, або приховати посилання на Політику приватності чи налаштування. Така практика порушує принцип справедливості, добровільності згоди.

4. Перешкоджання (англ. Hindering) – це практика, коли користувачам навмисно створюються перешкоди в отриманні інформації щодо захисту їхніх персональних даних. Формами такого перешкоджання можуть бути:

1) створення глухого кута – коли користувач проходить за посиланням, де має бути розміщена інформація про обробку його персональних даних, а посилання недоступне чи інформація відсутня. Така практика порушує право користувача мати легкий доступ до інформації, реалізовувати свої права, а також захист персональних даних за проектуванням і за замовчуванням;

2) створення для користувача більшої кількості кроків, для обрання параметрів налаштувань, які забезпечують захист персональних даних, аніж для обрання більш інвазивних варіантів. Так, користувачів фактично відмовляють зробити налаштування, які відповідають їх інтересам. Така практика обмежує право користувачів на легкий доступ до інформації, реалізовувати права як суб'єкта даних, можливість відкликати згоду, порушує захист персональних даних за проектуванням і за замовчуванням;

3) надання оманливої інформації – це створення невідповідності між інформацією та фактичними доступними діями, яка спонукає користувачів робити те, що вони не мали наміру робити. Така практика порушує принцип прозорості, справедливості, обмежує можливість надання поінформованої згоди;

5. Нестабільність (англ. Fickle) – це практика створення нестабільного та непослідовного інтерфейсу, у якому користувачу важко зрозуміти, де знаходяться налаштування приватності. Формами такої нестабільності можуть бути:

1) відсутність ієрархії – виклад інформації, яка стосується обробки і захисту персональних даних, не має ієрархії, а тому вона з'являється декілька разів, представлена різними способами. Як наслідок, користувачі не матимуть повного уявлення про те, як обробляються їхні персональні дані та як вони їх можуть контролювати. Така практика обмежує можливість користувачів отримувати легкий доступ до інформації та реалізовувати свої права;

2) розміщення інформації про захист персональних даних чи можливості зробити певні налаштування на сторінках, що не пов'язані з цією темою. Наприклад, розміщення інформації про обробку персональних даних на сторінці «Безпека», що не є очевидним для користувача. Така практика обмежує можливість користувачів отримувати легкий доступ до інформації та реалізовувати свої права.

6. Залишення в темряві (англ. Left in dark) – це практика проектування інтерфейсу таким чином, щоб приховати елементи, пов'язані із захистом персональних даних. Формами залишення у темряві можуть бути:

1) відсутність мови, зрозумілої користувача – інформація, що стосується захисту персональних даних, не представлена офіційною мовою держави, де проживають користувачі, що може обмежувати їх у доступі до інформації. Така практика порушує принцип справедливості, обмежує доступ до зрозумілої інформації;

2) надання користувачам суперечливої інформації – внаслідок надання суперечливої інформації користувачів не розуміють, що вони повинні робити і які наслідки їхніх дій, а тому, скоріше за все, залишать налаштування за замовчуванням. Така практика порушує принцип справедливості;

3) використання неоднозначної інформації, формулювань, загальних термінів. Така практика порушує принцип справедливості, прозорості, обмежує доступ до зрозумілої, повної інформації.

Також існує ще інша класифікація найбільш поширених темних патернів[82]:

1. Цукеринг приватності (англ. Privacy Zuckering) – названий на честь медіамагната та генерального директора компанії Meta – Марка Цукерберга. Суть цього темного патерну полягає у тому, щоб максимально ускладнити для користувача та зробити незручною зміну стандартних налаштувань приватності. Цифровий сервіс декларує захист персональних даних, однак створює усі можливі перешкоди для користувача. Як наслідок, користувач зупиняється на півшляху і припиняє пошук потрібної інформації чи налаштувань.

2. Погані налаштування за замовчуванням (англ. Bad defaults) – стандартні параметри цифрового сервісу налаштовані таким чином, аби полегшити чи сприяти, аби користувач надавав найбільшу кількість інформації. Так, користувачі залишають налаштування за замовчуванням і, як наслідок, роблять доступним більший обсяг даних, наприклад, у профілі у соціальній мережі.

3. Вимушена реєстрація (англ. Forced registration) – патерн, суть якого полягає у тому, аби робити обов'язковою реєстрацію користувача на цифровому сервісі у випадках, коли це не є необхідним для досягнення цілі його використання. Наприклад, для користування новинним ресурсом створення акаунту не є необхідним, крім випадків платної підписки з розширеним

[82] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfaheicher, "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Paerns," Proceedings on Privacy Enhancing Technologies 2016, no. 4, Oct. 23, 2016, 237–254 [Електронний ресурс] – Режим доступу до ресурсу: https://www.petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf.

доступом. Примусова реєстрація використовується для того, аби отримати більшу кількість даних та відстежувати поведінку користувачів.

4. Приховані юридичні умови (англ. Hidden Legalese Stipulations) –патерн, суть якого полягає у написанні довгих і складних для розуміння пересічного користувача правил користування цифровим сервісом (англ. Terms of use, Terms and Conditions), у яких приховуються положення, що стосуються персональних даних користувачів.

5. Безсмертні акаунти (англ. Immortal Accounts) – це патерн, суть якого полягає у відсутності механізму для видалення акаунтів або ускладнення цього процесу. Цей патерн є найбільш «ефективним» у поєднанні з вимушеною реєстрацією.

6. Поглинання адресної книги (англ. Address book leeching) – патерн, суть якого полягає у тому, щоб спонукати користувачів надавати доступ до контактів, аби мати можливість користуватися певним функціоналом. Надалі цифровий сервіс може використовувати контакти для цілей, які раніше не були повідомлені.

7. Тіньові профілі користувачів (англ. Shadows User Profilers) – патерн, суть якого полягає у тому, що цифровий сервіс створює профілі та здійснює спостереження за особами, які не є користувачами цього цифрового сервісу і не знають, що їхні персональні дані обробляються. Цей патерн працює у поєднанні з патерном поглинання адресної книги.

8. Видавлювання інформації (англ. Information Milking) – патерн, суть якого полягає у зборі даних у кількості, більшій, аніж потрібно для надання послуг чи використання функціоналу цифрового сервісу.[83]

9. Дружній спам (англ. Friendly Spam) – патерн, суть якого полягає у тому, що цифровий сервіс запитує у користувачів доступ до електронної пошти чи профілю у соціальних мережах ніби для того, аби досягти певної цілі (наприклад, відшукати друзів, колег), але натомість починає розсилку спаму

[83] Information milking, Privacy dark patterns [Електронний ресурс] – Режим доступу до ресурсу: https://dark.privacypatterns.eu/#/patterns/information-milking.

(наприклад, запрошення приєднатися до сервісу) всім контактам користувача. Причому такий спам надсилається нібито від імені такого користувача.

Проаналізовані вище темні патерни є несправедливою та неетичною практикою досягнення власниками цифрових сервісів своїх бізнес-цілей та отримання вигоди за рахунок впливу на вразливості психіки людини. Окрім шкоди, що завдається людині через неправомірне використання її персональних даних та нехтування її інтересами, використання темних патернів також негативно впливає на репутацію цифрових сервісів та підриває довіру користувачів до бренду.

Темні патерни не виникають випадково, а є чітко продуманою тактикою, яка має відслідковуватися, а власники цифрових сервісів – отримувати санкції, зокрема, за порушення вимог законодавства щодо захисту персональних даних за проектуванням і за замовчуванням.

3.2. Іноземний досвід здійснення державного нагляду та контролю за дотриманням захисту персональних даних за проектуванням і за замовчуванням

Оскільки захист персональних даних за проектуванням і за замовчуванням був вперше визначений як нормативна вимога до контролерів саме у Регламенті, слід розглянути практику правозастосуванням ст. 25 Регламенту у державах-членах Європейської економічної зони (ЄЕЗ).

Здійснення державного нагляду у контролю за дотриманням законодавства у сфері захисту персональних даних у цілому, а також захисту персональних даних за проектуванням і за замовчуванням зокрема у державах-членах ЄЕЗ належить, до компетенції незалежних наглядових органів та національних судів. Для нагляду за дотриманням законодавства у сфері захисту персональних даних інституціями Європейського Союзу у процесі здійснення ними своїх публічних функцій створена окрема посада Європейського інспектора із захисту даних. Оскільки обробка персональних даних інституціями ЄС має своє специфічне регулювання та здійснення контролю, воно не є предметом цього дослідження.

Відповідно до ст. 51 Регламенту кожна держава-член ЄЕЗ має забезпечити існування одного чи декількох незалежних наглядових органів, які повинні бути самостійними у вирішенні питань, адже їхні наглядові повноваження поширюються на представників як приватного, так і публічного сектору.[84]

За ст. ст. 57-56 Регламенту незалежні наглядові органи, серед іншого, контролюють дотримання Регламенту та розглядають скарги щодо його порушення, уповноважені проводити розслідування, обмежувати чи забороняти обробку даних, накладати адміністративні штрафи за порушення вимог Регламенту та мають право звернутися до суду за фактом порушення Регламенту.[85] Керівники усіх наглядових органів формують Європейську раду із захисту даних, яка забезпечує єдність у правозастосуванні у сфері захисту персональних даних та в окремих випадках здійснює моніторинг за дотриманням законодавства у випадках, коли у справі залучені наглядові органи декількох держав. Юридично обов'язкові рішення наглядових органів чи ігнорування скарги можуть бути оскаржені до суду, що передбачено ст. 78 Регламенту.[86]

Окрім звернення до наглядових органів, суб'єкт, який вважає, що порушено його права, гарантовані Регламентом, може звернутися за захистом до суду.

Незважаючи на те, що цифрові сервіси стали невід'ємною частиною життя людини, а порушення захисту персональних даних за проектуванням і за замовчуванням можливі у дуже різноманітних формах, частка порушень захисту персональних даних за проектуванням і за замовчуванням у практиці наглядових є не такою значною, як за порушення конкретних принципів чи прав суб'єктів даних.

---

[84] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

[85] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

[86] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Проте, якщо в цілому проаналізувати весь масив штрафів за порушення вимог Регламенту, кількість накладених адміністративних штрафів за порушення ст. 25 Регламенту наразі складає близько 50. Тим не менш, їх аналіз є дуже важливим для розуміння, які помилки допускають цифрові сервіси у своєму відношенні до персональних даних їхніх користувачів.

Набрання чинності Регламентом було особливим моментом не лише через те, що він ознаменував уніфікацію європейського законодавства у сфері захисту персональних даних та запровадження його екстратериторіальної дії, але й тим, що саме 25 травня 2018 року правозахисні асоціації None Of Your Business (NOYB) і La Quadrature du Net (LQDN) подали скаргу на американського технічного гіганта та найбільшу у світі пошукову систему – Google (компанія Google LLC) до французького наглядового органу – CNIL.[87] А підстава звернення – порушення вимог Регламенту. Правозахисні асоціації представляли інтереси 10 000 користувачів, чиї права були порушені. Після проведеного інспектування було виявлено, що обробка персональних даних, здійснювана Google не відповідала принципу прозорості. Інформація, яка стосується захисту персональних даних (цілі обробки, категорії персональних даних), не була легко доступною для користувачів: вона містилася у різних документах, а тому користувачам доводилося переходити із сторінку на сторінку, аби зрозуміти, як обробляються їхні дані. Іноді це вимагало від користувачів здійснити 5-6 кроків. Окрім цього, інформація подавалася дуже загально, що не давало можливість сформувати повну картину про обробку даних. Таким чином, користувачі були позбавлені належного контролю над своїми даними.

Окрім цього, CNIL виявив, що для застосування персоналізованої реклами, яка вимагає отримання однозначної, конкретної і активної згоди, Google презюмував згоду користувачів і під час створення облікового запису чек-бокс зі

[87] The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, EDPD [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

згодою на персоналізовану рекламу був уже проставлений.[88] Причому, від користувача вимагалися додаткові дії, аби змінити налаштовані за замовчуванням параметри.

За перераховані порушення у 2019 році на Google було накладено штраф у розмірі 50 млн євро, який до 2021 року залишався рекордним. Важливо відмітити, що у рішенні CNIL відсутнє посилання на порушення ст. 25 Регламенту, однак вважаємо, що практика Google свідчить про ігнорування ідеї захисту персональних даних на етапі проектування сервісу і навмисне використання темних патернів. А отже, Google не виконав свого зобов'язання щодо захисту персональних даних за проектуванням і за замовчуванням.

У контексті нагляду за захистом персональних даних за проектуванням і за замовчуванням цікавою є практика Італійського органу із захисту персональних даних (Garante) щодо функціонування цифрових платформ служб доставки їжі.

У липні 2021 року одразу на два популярні італійські сервіси були накладені великі штрафи: Foodinho s.r.l., що контролюється материнською компанією Glovoapp 23 s.l – 2,6 млн євро[89], Deliveroo (компанія Deliveroo Italy srl) – 2,5 млн євро[90]. Справи досить схожі, оскільки стосувалися неправомірної обробки персональних даних, зокрема, використання дискримінаційних алгоритмів оцінки роботи водіїв, розподілу замовлень та бронювання змін без належного повідомлення про це водіїв та можливості втрутитися у процес прийняття автоматизованих рішень.

У ситуації з Foodinho s.r.l. Garante встановив, що компанія без повідомлення водіїв створила внутрішню рейтингову систему на основі історії доставок, відгуків клієнтів та ресторанів у якості бізнес-партнерів. Foodinho s.r.l. не

[88] The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, EDPD [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

[89] Italy: Garante fines Foodinho €2.6M for unlawful employee management algorithms [Електронний ресурс] – Режим доступу до ресурсу: https://www.dataguidance.com/news/italy-garante-fines-foodinho-%E2%82%AC26m-unlawful-employee.

[90] Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 luglio 2021 [9685994] [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.

провела належної перевірки точності і правильності роботи алгоритмів, аби попередити факти дискримінації, а також не надала водіям можливість вимагати людського втручання у прийняття рішень, заперечувати проти автоматизованого прийняття рішень та профілювання. Причому, на основі результатів роботи алгоритмів приймалися рішення щодо припинення співробітництва з водієм, що слід вважати серйозним юридичним наслідком.

Окрім сплати штрафу, компанія була зобов'язана перевірити правильність роботи алгоритмів та актуальність даних, якими вона оперує, для виключення можливих відхилень в оцінці продуктивності водіїв та відповідної дискримінації.[91]

У справі з Deliveroo Garante наклав штраф у розмірі 2,5 млн євро за незаконну обробку персональних даних 8 000 водіїв служби. Garante виявив у діяльності Deliveroo багато порушень, зокрема: 1) порушення принципу прозорості у повідомленні про методи обробки персональних даних водіїв; 2) непрозорість використання автоматизованого прийняття рішень та профілювання (алгоритму розподілу замовлень та бронювання робочих змін з наданням пріоритетів за певними ознаками); 3) порушення принципу обмеженого зберігання даних, адже був визначений загальний строк зберігання – 6 років; 4) порушення принципу мінімізації даних і захисту персональних даних за проектуванням і за замовчуванням. Garante виявив, що системи Deliveroo налаштовані таким чином, аби збирати усі дані, які стосуються управління замовленнями, із різних систем і надання доступу до них операторам: 1) історії замовлень, карти виконання замовлень, час доставки, платежі, відхилення у доставці, деталі всіх окремих етапів замовлень тощо із застосунку; 2) дані про місцезнаходження, які оновлюються кожні 12 секунд, що виходить за межі необхідного для доставки замовлення (причому дані про переміщення

[91] Ordinanza ingiunzione nei confronti di Foodinho s.r.l. - 10 giugno 2021 [9675440] [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440.

зберігалися протягом 6 місяців); 3) дані комунікації з клієнтами із чатів, переписки електронною поштою.

Таким чином, без належного роз'яснення своєї практики обробки персональних даних, зі збиранням надмірної кількості даних та використання їх з метою автоматизованого прийняття рішень і профілювання, що може призводити до дискримінації та інших негативних наслідків, служби доставки Foodinho s.r.l. та Deliveroo показали, що захист персональних даних не запроектований ні на технічному, ні на організаційному рівні.

Ще одна цікава справа щодо порушення обов'язку із захисту персональних даних за проектуванням, передбаченого ч. 1 ст. 25 Регламенту, була розглянута Берлінським комісаром із захисту даних і свободи інформації (надалі – Комісар), який наклав штраф у розмірі 14,5 млн євро на німецьку компанію з нерухомості – Deutsche Wohnen SE.[92] Комісар двічі проводив виїзні перевірки компанії, за результатами яких було виявлено, що Deutsche Wohnen SE зберігає дані орендаторів протягом необмеженого строку, не перевіряючи, чи є зберігання законним та необхідним. Дані включали особисту, фінансову та податкову інформацію, банківські виписки, інформацію про соціальне та медичне страхування орендарів. Причому, у деяких випадках дані роками зберігалися, що взагалі не відповідало первинним цілям їхньої обробки.

Ще під час першої перевірки у 2017 році було встановлено, що Deutsche Wohnen SE використовує систему архівування, яка не дозволяє видаляти дані, що більше непотрібні для досягнення цілі обробки. До другої перевірки компанія удосконалила свою систему архівування, проте Комісар відзначив, що вжиті заходи не є достатніми, і до моменту другої перевірки мали місце порушення принципів обмеження зберігання і мінімізації даних.

[92] Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft [Електронний ресурс] – Режим доступу до ресурсу: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf.

Комісар дійшов висновку, що Deutsche Wohnen SE навмисно створила таку архівну структуру і неналежним чином здійснював обробку даних протягом довгого строку.

Первинний розмір штрафу складав 28 млн євро, просто з урахуванням того, що Deutsche Wohnen SE співпрацювала з наглядовим органом, остаточний штраф призначили у розмірі 14,5 млн євро. У 2021 році Берлінський регіональний суд скасував мільйонний штраф, однак не з причини відсутності порушень Регламенту, а у зв'язку з процесуальними недоліком: Берлінський комісар не зазначив у рішенні, які конкретні дії керівництва юридичної особи призвели до порушення. А оскаржити рішення суду Берлінський комісар може лише через прокуратуру, що ускладнило доведення справи до логічного завершення.[93]

Як відомо, великий масив персональних даних використовується компаніями для рекламних цілей та маркетингу. І далеко не завжди захист персональних даних є невід'ємною частиною такої діяльності, що є ключовою вимогою захисту персональних даних за проектуванням і за замовчуванням.

Чимало рішень наглядових органів за порушення ст. 25 Регламенту стосуються неправомірної обробки персональних даних телекомунікаційними компаніями. Однією з найбільш масштабних була справа проти Vodafone (компанія Vodafone Italia S.p.A), що розглядалася Італійським органом із захисту персональних даних (Garante).

За незаконну обробку персональних даних мільйонів клієнтів і потенційних клієнтів у цілях телемаркетингу на Vodafone Italia S.p.A було накладено штраф у розмірі 12,25 млн євро.[94] Розслідування почалося після отримання Garante сотень скарг на небажані дзвінки від Vodafone. Було встановлено, що Vodafone без належної правової підстави (згоди фізичних осіб) зберігав та використовував для телемаркетингу дані близько 4,5 млн осіб. Велику частку даних Vodafone

[93] Landgericht Berlin stellt Bußgeldverfahren gegen Deutsche Wohnen ein [Електронний ресурс] – Режим доступу до ресурсу: https://www.deutsche-wohnen.com/ueber-uns/presse-news/pressemitteilungen/landgericht-berlin-stellt-bussgeldverfahren-gegen-deutsche-wohnen-ein/.

[94] Telemarketing aggressivo. Dal Garante privacy sanzione a Vodafone per 12 milioni 250 mila euro [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485754.

придбав у сторонніх постачальників, на що не було вільної, інформованої та конкретної згоди суб'єктів даних.

Окрім цього, Garante з'ясувала, що Vodafone не вжила адекватних заходів безпеки для системи управління клієнтами, оскільки оператори Vodafone вимагали від фізичних осіб відправляти документи, що посвідчують особу, через WhatsApp з потенційною метою розсилки спаму, фішингу чи інших незаконних дій.[95]

Garante, крім іншого, визнала порушення ст. 25 Регламенту, оскільки Vodafone не запровадила системи контролю «ланцюга» збору персональних даних до з моменту першого контакту потенційного клієнта. Незаконні та небажані дзвінки здійснювалися з метою активації послуг або підписання договорів. [96]

Порушення захисту персональних даних за проектуванням і за замовчуванням може здійснюватися на будь-яких рівнях та у різних масштабах. Суб'єкти публічного права часто допускають такі порушення, проте досить навряд чи притягуються до відповідальності за це. У цьому контексті цікавим є рішення Ісландського органу із захисту даних (Persónuvernd) щодо накладення штрафу на Міністерство промисловості та інновацій, яке виступало контролером, у розмірі 51 000 євро, та компанію YAY ehf., яка була процесором, у розмірі 27 200 євро.

Штраф був пов'язаний із реалізацією урядової кампанії щодо заохочення дорослих ісландців до подорожей всередині держави шляхом надання цифрових подарункових сертифікатів. Міністерство уклало договір з YAY ehf., яка випустила застосунок для цифрових подарункових сертифікатів.[97]

---

[95] Telemarketing aggressivo. Dal Garante privacy sanzione a Vodafone per 12 milioni 250 mila euro [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485754.

[96] Ordinanza ingiunzione nei confronti di Vodafone - 12 novembre 2020 [9485681] [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485681.

[97] Icelandic DPA issues fine to the Ministry of Industries and Innovation and YAY ehf. for data processing through a digital gift card app [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/news/national-news/2021/icelandic-dpa-issues-fine-ministry-industries-and-innovation-and-yay-ehf_en.

Persónuvernd ініціював розслідування після того, як почали надходити скарги, що застосунок вимагає велику кількість даних та запитує доступ до даних із пристроїв користувачів. Зокрема, окрім того, що для реєстрації використовувався номер телефону та електронна адреса, застосунок також вимагав дані про стать та вік під час входу. Для того, щоб передати сертифікат іншій людині та надіслати їх електронне привітання, потрібно було надати доступ до камери, мікрофона, контактів. У деяких випадках такі доступи застосунок отримував без відома, а також інформацію про власника пристрою, місцезнаходження, дані з календаря.[98]

Було встановлено, що мало місце порушення принципу прозорості, адже для отримання сертифікату користувачі повинні були погодитися із Загальними умовами використання застосунку (англ. General Terms of use), натомість було відсутнє Повідомлення про обробку персональних даних чи Політика приватності. Persónuvernd також визнав порушення принципу законності, адже не було отримано чітку згоду на обробку даних.[99]

Крім того, ні Міністерство, ні YAY ehf. Не вжили належних технічних та організаційних заходів щодо безпеки даних. Зокрема, за замовчуванням застосунок отримував широкий доступ до даних з пристроїв користувачів (наприклад, доступ до календаря), який об'єктивно не був потрібен для цілі видачі цифрового сертифікату.

Persónuvernd визначив, що через помилку конфігурації застосунок збирав даних більше, аніж це необхідно, що є прямим порушення принципу мінімізації даних та захисту персональних даних за проектуванням і за замовчуванням. Перед запуском застосунку не проводилося жодних аудитів чи тестувань для оцінки ефективності налаштувань за замовчуванням, а також того, яка

[98] Ákvörðun um sekt vegna ferðagjafar stjórnvalda Mál nr. 2020092288 [Електронний ресурс] – Режим доступу до ресурсу: https://www.personuvernd.is/urlausnir/akvordun-um-sekt-vegna-ferdagjafar-stjornvalda.
[99] Ákvörðun um sekt vegna ferðagjafar stjórnvalda Mál nr. 2020092288 [Електронний ресурс] – Режим доступу до ресурсу: https://www.personuvernd.is/urlausnir/akvordun-um-sekt-vegna-ferdagjafar-stjornvalda.

інформація запитувалася автоматично. Міністерство та YAY ehf. визнали порушення, проте до закінчення кампанії вони не були усунуті. [100]

Проаналізовані рішення розкривають різні аспекти порушень захисту персональних даних за проектуванням і за замовчуванням. Тим не менш, вони доводять, що правомірна обробка персональних даних і захист прав та інтересів фізичних осіб неможливі без впровадження ідеї і розуміння захисту персональних в усі процеси та технологічні рішення.

Зазначені справи стосувалися масштабних порушень, коли впливу зазнають мільйони осіб, однак вимога захисту персональних даних за проектуванням і за замовчуванням застосується для контролерів та процесорів незалежно від організаційно-правової форми, розміру та інших параметрів.

Висновки до Розділу 3

Практична реалізація концептів захисту персональних даних за проектуванням і за замовчуванням є багатогранною і охоплює впровадження організаційних та технічних заходів фактично у всі процеси, продукти та сервіси, функціонування яких пов’язане з обробкою персональних даних.

Особливого значення захист персональних даних за проектуванням і за замовчуванням набуває у зв’язку інтеграції великої кількості цифрових сервісів у життя сучасної людини, якими вона користується щодня (онлайн-магазини, служби доставки, поштові сервіси, соціальні мережі тощо). Така взаємодія з технологіями опосередковується збором і обробкою персональних даних, а отже робить особу вразливою перед неправомірним стороннім втручанням у сферу її приватного життя та небажаним, а інколи майже непомітним впливом на прийняті нею рішення, поведінку.

Для визначення технічного запровадження, розгортання, постійного функціонування та керування функціями із захисту персональних даних виникло поняття «інженерія приватності». Елементами інженерії приватності є стратегії

[100] Ákvörðun um sekt vegna ferðagjafar stjórnvalda Mál nr. 2020092288 [Електронний ресурс] – Режим доступу до ресурсу: https://www.personuvernd.is/urlausnir/akvordun-um-sekt-vegna-ferdagjafar-stjornvalda.

та патерни, які сприяють тому, аби обробка персональних даних, з одного боку, не порушувала прав та відповідала інтересам людини, а, з іншого боку, допомагають цифровим сервісам та іншим суб'єктам досягати своїх цілей.

Стратегії відображають фундаментальний підхід до вирішення певних задач, досягнення цілей, у той же час патерни є конкретними рішення найбільш поширених задач. Власники цифрових сервісів можуть використовувати патерни приватності, щоб забезпечити захист персональних даних за проектуванням і за замовчуванням, а можуть вдаватися до навмисного використання темних патернів, аби маніпулювати користувачами, обмежувати їхній контроль над обробкою персональних даних та прийнятими рішеннями. Темні патерни є неетичною практикою, боротьба з якою уже починає здійснюватися на рівні законодавства.

Державний нагляд і контроль за захистом персональних даних за проектуванням і за замовчуванням у державах ЄЕЗ здійснюється незалежними наглядовими органами та судами. Наразі з моменту набрання чинності Регламенту було розглянуто близько 50 справ, пов'язаних з порушенням ст. 25 Регламенту, що свідчить про те, що практика ще формується і потребує подальшого аналізу. Хоча слід зазначити, що справ, у яких простежується порушення захисту персональних даних за проектуванням і за замовчуванням значно більше.

ВИСНОВКИ

За результатами проведеного магістерського дослідження можна зробити наступні висновки:

1. Поняття персональних даних, закріплене на рівні міжнародного, регіонального та українського національного законодавства, навмисно сформульовано достатньо широко для того, аби охопити більше інформації, яка стосується фізичної особи, і забезпечити захист її права на недоторканність приватного життя. Причому, у зв'язку з виникненням нових форм взаємодії людини з технологіями, усе більше інформації відносять до персональних даних людини.

2. Визначення терміну «персональні дані» у Законі України «Про захист персональних даних» потребує уточнення у розрізі параметрів, які впливають на можливість ідентифікації особи та, відповідно, віднесення певної інформації до персональних даних.

3. Принципи обробки і захисту персональних даних є імперативами та критеріями для визначення правомірності обробки і належного захисту персональних даних. Вони втілюються у конкретні обов'язки суб'єктів, які залучені до обробки персональних даних, і їх недотримання має бути віднесено до категорії найбільш серйозних порушень у сфері захисту персональних даних, як це реалізовано у Регламенті (ЄС) 2016/679.

4. Пропонуємо у Законі України «Про захист персональних даних» окрему статтю «Принципи обробки персональних даних» та до принципів, які можна виокремити у ст. 6 чинної редакції, додати також принцип підзвітності як вимогу до контролера бути здатним продемонструвати дотримання законодавства у сфері захисту персональних даних.

5. Першим нормативно-правовим актом, який визначив захист персональних даних за проектуванням і за замовчуванням як обов'язкову юридичну вимогу був Регламент (ЄС) 2016/679, хоча наукова розробка цих концептів розпочалася ще наприкінці XX століття. Наразі українське

законодавство не містить поняття захисту персональних даних за проектуванням і за замовчуванням, проте у контексті удосконалення українського законодавства у сфері захисту персональних даних відповідно до найвищих стандартів Європейського Союзу та Ради Європи ця категорія має бути нормативно визначена з подальшими методичними рекомендаціями та роз'ясненнями щодо правильного правозастосування.

6. Право на недоторканність приватного життя – це фундаментальне право людини, що дозволяє їх протидіяти будь-якому незаконному та небажаному сторонньому втручанню і впливу. Механізми захисту персональних даних за проектуванням і за замовчуванням є необхідними елементами захисту права на недоторканність приватного життя, адже спрямовані на мінімізацію обсягу даних про особу, які стануть відомі стороннім суб'єктам, та, відповідно, обмеження їхнього впливу на ті сфери чи аспекти життя, які людина прагне залишити приватними.

7. Захист персональних даних за проектуванням і за замовчуванням є не лише юридичною вимогою, але й вагомою конкурентною перевагою для власників цифрових сервісів. Для забезпечення захисту персональних даних за проектуванням і за замовчуванням в організаційні та технічні процеси власники цифрових сервісів мають використовувати стратегії та патерни приватності та, разом з тим, уникати темних патернів як неетичної і незаконної практики по відношенню до користувачів.

8. Темні патерни, які часто використовуються в інтерфейсах цифрових сервісів, становлять порушення захисту персональних даних за проектуванням і за замовчуванням, а тому мають бути нормативно визначені у законодавсті.

9. Пропонуємо у новій редакції Закону України «Про захист персональних даних» передбачити визначення темних патернів, заборону на використання темних патернів, зокрема, як способу отримання згоди користувача. Визначення терміну «темний патерн» може бути здійснено наступним чином:

«темний патерн – це елемент користувацького інтерфейсу, розроблений з метою маніпулювання поведінкою користувача, позбавлення автономії у прийнятті

рішень, можливості контролювати обробку персональних даних та реалізовувати свої права як суб'єкта даних».

10. Практика державного нагляду та контролю за дотриманням захисту персональних даних за проектуванням і за замовчуванням у країнах ЄЕЗ ще формується і потребує подальшого аналізу. Кількість рішень національних наглядових органів, пов'язаних з порушенням цієї вимоги, є незначною, порівняно з кількість справ за порушенням інших положень Регламенту.

11. У разі запровадження в українське законодавство вимоги щодо захисту персональних даних за проектуванням і за замовчуванням виникне велика необхідність у розробці методичних рекомендацій та роз'яснень щодо правозастосування, оскільки як у Регламенті (ЄС) 2016/679, у Проекті Закону «Про захист персональних даних» № 5628 від 07.06.2021 року положення щодо захисту персональних даних за проектуванням і за замовчуванням є дуже загальними. Виконати їх без розуміння інженерії приватності, знання відповідних стратегій, тактик та патернів неможливо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.11 «Міжнародне право» // А. В. Пазюк. – К., 2004. – 15 с. [Електронний ресурс] – Режим доступу до ресурсу: http://cyberpeace.org.ua/files/aref-1.pdf.
2. Конвенція Ради Європи від 28 січня 1981 року № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/994_326#Text.
3. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
4. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [Електронний ресурс] – Режим доступу до ресурсу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
5. Про захист персональних даних: Закон України від 01.06.2010 р. № у редакції від 13.02.2022 р. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
6. Opinion 4/2007 on the concept of personal data. Article 29 Data Protection Working Party. Adopted June 20, 2007 [Електронний ресурс] – Режим доступу до ресурсу: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
7. Рішення ЄСПЛ у справі Benedik v. Slovenia, no. 62357/14, 2018 [Електронний ресурс] – Режим доступу до ресурсу: https://hudoc.echr.coe.int/eng.
8. Рішення Європейського суду справедливості у справі Scarlet Extended (C-70/10, EU:C:2011:771) [Електронний ресурс] – Режим доступу до ресурсу: https://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2160380.
9. Рішення Європейського суду справедливості у справі Patrick Breyer v. Bundesrepublik Deutschland (C-582/14, ECLI:EU:C:2016:779) [Електронний ресурс] – Режим доступу до ресурсу:

https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2157169.

10. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник/М. Бем, І. Городиський, Г. Саттон, О. Родіоненко ; Європейський Союз, Рада Європи - К.: К.І.С., 2015. – 220 с. [Електронний ресурс] – Режим доступу до ресурсу: https://rm.coe.int/168059920c.
11. R. Leenes, Do They Know Me? Deconstructing Identifiability (2008) 4(1&2), University of Ottawa Law & Technology Journal [Електронний ресурс] – Режим доступу до ресурсу: https://pure.uvt.nl/ws/portalfiles/portal/1310856/Leenes_Do_they_know_me_110216_publishers_immediately.pdf.
12. GDPR: Посібник з виживання / Артем Кобрін, Дмитро Корчинський, Владіслав Некрутенко; під ред. Д. Іванова. – Одеса: Видавничий дім «Гельветика», 2022. – 228 с.
13. Nadezhda Purtova (2018) The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, 40-81 [Електронний ресурс] – Режим доступу до ресурсу: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176?scroll=top&needAccess=true.
14. Privacy by Design. Setting a new standard for privacy certification. Deloitte [Електронний ресурс] – Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF.
15. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. Adopted October 20, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.
16. Decision of the Data Protection Commission in the matter of WhatsApp Ireland Limited [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf.
17. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Adopted September 23, 1980. Updated July 11, 2013 [Електронний ресурс] – Режим доступу до ресурсу: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

18. Khadija Ismayilova v. Azerbaijan, nos. 65286/13 and 57270/14, 10 January 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-188993%22]}.
19. Resolution on Privacy by Design" adopted by the 32th Conference of Data Protection and Privacy Commissioners in October 2010 [Електронний ресурс] – Режим доступу до ресурсу: http://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.
20. Проект Закону «Про захист персональних даних» № 5628 від 07.06.2021 року [Електронний ресурс] – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160.
21. Information Commissioner's Office (ICO). Data protection by design and default [Електронний ресурс] – Режим доступу до ресурсу: https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-anddefault/.
22. A Guide to Privacy by Design. Spanish Data Protection Agency (AEPD). Adopted October, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.
23. European Data Protection Supervisor, Opinion 5/2018 Preliminary Opinion on privacy by design. Adopted May 31, 2018 [Електронний ресурс] – Режим доступу до ресурсу: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.
24. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [Електронний ресурс] – Режим доступу до ресурсу: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.
25. Chart of signatures and ratifications of Treaty. Council of Europe [Електронний ресурс] – Режим доступу до ресурсу: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.
26. Information milking, Privacy dark patterns [Електронний ресурс] – Режим доступу до ресурсу: https://dark.privacypatterns.eu/#/patterns/information-milking.
27. GDPR. Privacy by design [Електронний ресурс] – Режим доступу до ресурсу: https://gdpr-info.eu/issues/privacy-by-design/.

28. Strategic Privacy by Design (Second Edition), R. Jason Cronk, International Association of Privacy Professionals, 2022, - 162.
29. Privacy by Design: The 7 Foundational Principles, Ann Cavoukian, 2009 [Електронний ресурс] – Режим доступу до ресурсу: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.
30. Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfaheicher, "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Paerns," Proceedings on Privacy Enhancing Technologies 2016, no. 4, Oct. 23, 2016, 237–254 [Електронний ресурс] – Режим доступу до ресурсу: https://www.petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf.
31. Opinion 03/2013 on purpose limitation. Article 29 Working Party. Adopted April 2, 2013 [Електронний ресурс] – Режим доступу до ресурсу: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
32. Породько В. Право на недоторканність особистого життя людини: проблема термінології. Підприємництво, господарство і право. 2018. № 11. С. 146–149 [Електронний ресурс] – Режим доступу до ресурсу: http://pgp-journal.kiev.ua/archive/2018/11/29.pdf.
33. Що таке веб-сервіс та їх види? [Електронний ресурс] – Режим доступу до ресурсу: https://2ip.ua/ua/blog/web-services.
34. ДСТУ ISO/IEC 20000-3:2017 Інформаційні технології. Керування послугами. Частина 3. Настанова щодо визначення сфери та застосовності ISO/IEC 20000-1 (ISO/IEC 20000-3:2012, IDT). [Електронний ресурс] – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=74969.
35. Privacy Patterns [Електронний ресурс] – Режим доступу до ресурсу: https://privacypatterns.org/.
36. Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices ,1st Edition, William Stallings, 2020.
37. Jaap-Henk Hoepman, "Privacy Design Strategies (Lile Blue Blook)", Radboud UniversityInstitute for Computing and Information Sciences, Radboud University, 2022 [Електронний ресурс] – Режим доступу до ресурсу: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf.
38. Privacy design patterns and anti-patterns patterns misapplied and unintended consequences. N. Doty, M. Gupta. 34, 2013 [Електронний ресурс] – Режим доступу до ресурсу:

https://cups.cs.cmu.edu/soups/2013/trustbusters2013/Privacy_Design_Patterns-Antipatterns_Doty.pdf.
39. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. European Data Protection Board. Public consultation [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.
40. California Privacy Rights Act of 2020 (CPRA) [Електронний ресурс] – Режим доступу до ресурсу: https://transcend.io/laws/cpra/.
41. Colorado Privacy Act [Електронний ресурс] – Режим доступу до ресурсу: https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.
42. Information milking, Privacy dark patterns [Електронний ресурс] – Режим доступу до ресурсу: https://dark.privacypatterns.eu/#/patterns/information-milking.
43. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, EDPD [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.
44. Italy: Garante fines Foodinho €2.6M for unlawful employee management algorithms [Електронний ресурс] – Режим доступу до ресурсу: https://www.dataguidance.com/news/italy-garante-fines-foodinho-%E2%82%AC26m-unlawful-employee.
45. Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 luglio 2021 [9685994] [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.
46. Ordinanza ingiunzione nei confronti di Foodinho s.r.l. - 10 giugno 2021 [9675440] [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440.
47. Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft [Електронний ресурс] – Режим доступу до ресурсу: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf.
48. Landgericht Berlin stellt Bußgeldverfahren gegen Deutsche Wohnen ein [Електронний ресурс] – Режим доступу до ресурсу: https://www.deutsche-wohnen.com/ueber-uns/presse-news/pressemitteilungen/landgericht-berlin-stellt-bussgeldverfahren-gegen-deutsche-wohnen-ein/.

49. Telemarketing aggressivo. Dal Garante privacy sanzione a Vodafone per 12 milioni 250 mila euro [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485754.
50. Ordinanza ingiunzione nei confronti di Vodafone - 12 novembre 2020 [9485681] [Електронний ресурс] – Режим доступу до ресурсу: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485681.
51. Icelandic DPA issues fine to the Ministry of Industries and Innovation and YAY ehf. for data processing through a digital gift card app [Електронний ресурс] – Режим доступу до ресурсу: https://edpb.europa.eu/news/national-news/2021/icelandic-dpa-issues-fine-ministry-industries-and-innovation-and-yay-ehf_en.
52. Ákvörðun um sekt vegna ferðagjafar stjórnvalda Mál nr. 2020092288 [Електронний ресурс] – Режим доступу до ресурсу: https://www.personuvernd.is/urlausnir/akvordun-um-sekt-vegna-ferdagjafar-stjornvalda.