Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Кафедра приватного права

Магістерська робота

освітній ступінь – магістр

на тему: **«ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ ОСНОВОПОЛОЖНИХ ПРИНЦИПІВ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ДАНИХ (GDPR)»**

Виконала: студентка 2-го року навчання,
Спеціальності
081 Право
Клюс Марія Олександрівна
Керівник: Смирнова Т. С._____
кандидат юридичних наук, доцент
Рецензент: Цельєв О.В._____
кандидат юридичних наук, доцент
Магістерська робота захищена
з оцінкою _____
Секретар ЕК _____
«___» _____ 20__ р.

Київ – 2020

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Директива 95/46	Директива №95/46/ЕС Європейського парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995
Європейська конвенція	Конвенція про захист прав людини і основних свобод від 04.11.1950
ЄСПЛ	Європейський суд з прав людини
Конвенція 108	Конвенція № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.1981
Рекомендації	Рекомендації офісу ICO «Guide to the GDPR»
Суд ЄС	Суд справедливості Європейського Союзу
GDPR, Регламент	Регламент Європейського Парламенту і Ради (ЄС) № 2016/679 «Про захист фізичних осіб у зв’язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» від 27.04.2016 (Загальний регламент про захист даних)
ICO	Уповноважений з інформації Великобританії
CCPA	The California Consumer Privacy Act
Article 29 WP	Робоча група захисту персональних даних зі статті 29 Директиви 95/46
Угода про асоціацію	Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони
CNIL	Національна комісії з захисту даних Франції
NJCM	Голландська секція Міжнародної комісії юристів

ВСТУП

Актуальність дослідження практичних аспектів реалізації основних принципів GDPR полягає в їх визначальній ролі у створенні та розумінні стандартів захисту персональних даних у всьому світі. Для України GDPR відіграє особливу роль, перш за все, через тісну співпрацю українських компаній із європейськими, а отже – необхідність відповідати вимогам GDPR для можливості обробляти дані жителів європейських держав. А, по-друге, через проєвропейський напрямок розвитку нашої держави, оскільки відповідно до Угоди про асоціацію, ми офіційно взяли на себе зобов'язання забезпечити належний рівень захисту персональних даних, відповідно до європейських та міжнародних стандартів.

Забезпечення належного захисту можливе лише за умови глибинного вивчення та розуміння. Ці процеси не повинні зводитись до копіювання тексту Регламенту в Закон. Треба зрозуміти причину виникнення і функцію норм, так само як і сутність всієї системи захисту, що існує в ЄС, і намагатись її пристосовувати до специфіки відповідних правовідносин, що вже існують в Україні. В цьому аспекті основоположні принципи є найбільш вдалим об'єктом для вивчення, адже вони є уособленням ідей та духу нормативно-правового акту. І в межах такого вивчення критично важливим є дослідження практики держав-членів Союзу щодо імплементації і втілення цих норм, а також дослідження підходів до їх розуміння уповноваженими органами. Це дозволяє розкрити реальний зміст кожного із принципів.

Зважаючи на вищезазначене, основоположні принципи у будь-якій сфері традиційно є об'єктом особливої уваги науковців. Принципи захисту персональних даних не є винятком. Їх часто розглядають у поєднанні із захистом права на приватність, тому багато наукових робіт, що досліджують принципи права на приватність в Європейському Союзі, висвітлюють і захист персональних даних, як

один із її аспектів.

Серед українських науковців окремі питання щодо захисту персональних даних та їх основних принципів висвітлювали такі дослідники як І. Арістова, Ю. Базанов, О. Баранов, В. Бойко, В. Брижко, Б. Кристальний, Л. Сергієнко, В. Цимбалюк, М. Швець та деякі інші. Але актуальним дослідженням в Україні принципів інституту захисту персональних даних, тобто з урахуванням недавніх змін у нормативно-правовому регулюванні Європейського Союзу, присвячено небагато праць, майже всі із них були опубліковані за часів чинності попередньої Директиви 95/46. Тоді як норми GDPR досить ґрунтовно змінили розуміння наявних принципів захисту персональних даних і закріпили деякі нові. Щодо досліджень європейських та американських науковців на тему основоположних принципів захисту персональних даних, то серед них можна виділити роботи таких авторів та авторок як N.A.G. Arachchilage, J. Ausloos, A. Ferreira, G. Lenzin, C.Patsakis, E.Politou, S.-D. Șchiopu, A. Senarath, D. Spagnuelo. В основу цієї роботи покладені переважно висновки цих дослідників, оскільки проаналізовані роботи українських науковців хоч і стосуються окремих аспектів системи захисту персональних даних, однак є дещо фрагментарними і не достатньо актуальними.

Мета даної роботи полягає в комплексному дослідженні питань практичної реалізації основоположних принципів GDPR, у розробленні на цій основі окремих висновків, необхідних для імплементації європейських норм і стандартів в зазначеній сфері.

Відповідно до мети дослідження були сформульовані такі *основні завдання:*

– висвітлити процес розвитку і становлення основоположних принципів захисту персональних даних в ЄС;

– розглянути прямий та непрямий вплив нормативно-правових актів ЄС на держави, що не є членами Союзу;

– здійснити характеристику основоположних принципів захисту персональних даних GDPR, розкрити їх сутність;

– розглянути як втілюються закріплені принципи у практиці компаній та рішеннях щодо них;

– дослідити особливості трактування окремих основоположних принципів національними уповноваженими органами захисту даних;

– продемонструвати зв'язок між реалізацією основоположних принципів GDPR та окремими правами суб’єкта даних;

– дослідити рішення судових органів щодо прав суб’єкта даних, які пов’язані із здійсненням основоположних принципів;

– надати загальні рекомендації щодо імплементації основоположних принципів GDPR в українське законодавство;

Об'єктом дослідження є суспільні відносини щодо захисту персональних даних, зокрема в Європейському Союзі.

Предметом дослідження є практичні аспекти реалізації основоположних принципів GDPR щодо захисту персональних даних.

Щодо *методологічної основи дослідження*, то у даній роботі використовувались звичні для правової науки аналіз, системний аналіз, порівняння, узагальнення, синтез, індукція і дедукція.

РОЗДІЛ 1
ОСНОВОПОЛОЖНІ ПРИНЦИПИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ І ЇХ РЕАЛІЗАЦІЯ В УКРАЇНІ

1.1. Загальний регламент про захист даних (GDPR) і його вплив на правове регулювання захисту персональних даних

Нормативно-правові акти, які приймаються як на державному, так і на міжнародному рівні, як правило, є віддзеркаленням проблеми, що потребує певного правового врегулювання [1, с. 98]. Не є винятком і Загальний регламент про захист даних [2]. Цей акт став наслідком наявності проблем у суспільстві, пов'язаних із приватністю, і результатом довготривалої роботи європейської спільноти щодо їх вирішення.

Активна робота над прийняттям Регламенту розпочалась у 2012 році і закінчилась 12 березня 2014 року, коли Європейський парламент прийняв акт, відомий як GDPR. Він вступив у силу 24 травня 2016 року, а його застосування розпочалось із 25 травня 2018 року, після дворічного відтермінування для приведення локальних актів і практики підприємств у відповідність до нових норм [3]. Форма акту – регламент, що не потребує окремої імплементації у національне законодавство, на противагу до попередньої директиви, підкреслює обов'язковість дотримання державами ЄС стандартів, закріплених у GDPR. Така єдність регулювання у всіх країнах Європейського Союзу навіть сама по собі є певним захистом для суб'єктів даних, оскільки зникає правова невизначеність і можливість частково уникати відповідальності за порушення захисту персональних даних через посилання на національне законодавство.

Актуалізація необхідності прийняття GDPR відбувалась прямопропорційно до розвитку новітніх технологій. Адже з розвитком технологій все більше людей

почали користуватись соціальними мережами чи отримувати послуги через Інтернет, надаючи при цьому свої дані в користування іншим особам і не маючи можливості контролювати подальші дії із цими даними.

Незважаючи на глобальний характер цієї проблеми, Європейський Союз виявився чи не єдиною інституцією, яка ще до виникнення проблеми серйозно зайнялася створенням ефективної та впорядкованої системи, що забезпечувала б захист персональних даних осіб. Вже коли GDPR був прийнятий і набирав чинності, в Сполучених Штатах було продемонстровано чітку необхідність запровадження схожих норм для держав, що не є членами ЄС. Ідеться про кейс компанії Cambridge Analytica, яка у 2018 році була звинувачена у незаконному отриманні персональних даних громадян США із їх Facebook сторінок, з метою використання під час президентської кампанії, і громадян Великобританії під час голосування за Brexit [4]. Ця ситуація показала наскільки потужним є вплив осіб, що мають доступ до великих масивів персональної інформації, і що ігнорувати необхідність запровадження ефективних норм щодо захисту персональних даних вже неможливо. Питання захисту персональних даних стало питанням забезпечення демократії в державі.

Прийняття GDPR неабияк позначилось на захисті персональних даних навіть у державах поза межами ЄС, що можна розглядати у двох напрямках. Перш за все, це прямий вплив, що зумовлений екстратериторіяльною дією норм акту. Так, частина 1 статті 3 GDPR вказує, що цей акт застосовується, незалежно від того, відбувається обробка в ЄС чи ні. Частина 2 цієї статті деталізує це положення, визначаючи за яких умов Регламент застосовний до контролерів та процесорів, які не розташовані в країнах Європейського Союзу. Завдяки таким нормам вимоги акту стали обов’язковими для всіх, хто обробляє персональні дані громадян ЄС, а також тих, хто тарґетує свої послуги на Європейський Союз. Саме тому питання відповідності вимогам GDPR стали актуальними для компаній США чи Китаю, що активно співпрацюють з ЄС.

Іншим важливим напрямком впливу є те, що GDPR, по суті, став модельним актом, на основі якого інші суб'єкти розробили свої нормативно-правові акти. Так, можна прослідкувати схожість із Data Protection Bill, що наразі перебуває на стадії законопроекту в Індії [5]; бразильським General Data Protection Law [6]; Law 81, що був прийнятий у Панамі [6]; Data Protection Act 2018, що після виходу Великобританії із ЄС тепер є основним актом, який забезпечує захист персональних даних там [6]; а також із CCPA, який навіть називають «каліфорнійським GDPR» [6]. І хоча кожен із цих актів має свою специфіку, що зумовлена особливостями суспільних відносин у державі чи штаті, в них є спільні риси із нормами GDPR в частині підвищення рівня стандартів обробки і встановлення дієвої відповідальності за порушення таких стандартів.

До прикладу, як визначено в статті 1798.140, за CCPA дещо ширше розуміють, що таке персональна інформація, включаючи в цю категорію не лише дані, що дозволяють ідентифікувати особу, а будь-яку інформацію, яка ідентифікує, стосується, описує, чи розумно може бути пов'язана з певним споживачем чи домогосподарством [7]. Крім цього, норми CCPA стосуються комерційних організацій, що займаються бізнесом у штаті Каліфорнія, збирають персональну інформацію і або мають річний валовий дохід більший за 25 мільйонів доларів, або працюють з даними 50 000 чи більше споживачів, домогосподарств чи пристроїв, або 50% і більше річного доходу отримують від продажу даних користувачів. GDPR ж стосується всіх організацій, які обробляють персональні дані. Але, незважаючи на ці відмінності, вони мають спільні основи та мету – правомірність, справедливість і прозорість обробки, безпека процесів обробки і забезпечення прав суб'єкта щодо даних, які його стосуються.

Так, стаття 5 GDPR закріплює основоположні принципи обробки персональних даних: це принципи правомірності, справедливості та прозорості, обмеженості ціллю, мінімізації даних, точності, обмеження зберігання, цілісності та конфіденційності, а також принцип підзвітності. Саме в межах цих принципів

закріплено вимоги щодо поінформованості, яка включає в себе і надання поінформованої згоди на обробку кожної категорії персональних даних, обмеження обсягів і тривалості обробки даних, наявність в контролера чи процесора ефективної системи захисту даних, які обробляються тощо. Всі ці норми розкривають основоположні принципи Регламенту і саме вони стали основою для розробки законодавчих актів не-членів ЄС [6]. Більшість із них не є новими, адже GDPR базується на нормах, що були закріпленими у попередній Директиві 95/46, так само як і у Конвенції 108 та інших нормативно-правових актах ЄС. Однак GDPR деталізував і систематизував кожен із них, створивши ефективну систему, яка вже стала базисом для розуміння захисту приватності і персональних даних на світовому рівні.

Отже, у 2018 році для захисту персональних даних на території Європейського Союзу почав застосовуватись Регламент, відомий як GDPR. Він став результатом багаторічної роботи щодо вирішення проблеми захисту даних осіб і їх приватності. Екстратериторіальна дія та ефективність системи зробили його характер модельним і зумовили його вплив на нормативно-правові акти інших держав. Це створює необхідність глибокого дослідження основоположних принципів Регламенту, тобто тих його норм, що передають його дух та ідеї. Адже вони визначають тенденції розуміння захисту персональних даних далеко поза межами Європейського Союзу на найближчий період.

1.2. Основні принципи, закріплені в GDPR

1.2.1. Принцип правомірності, справедливості та прозорості

Закріплені у пункті (а) частини 1 статті 5 Регламенту критерії правомірності, справедливості та прозорості є тріадою, що об’єднує у собі вимоги до суб’єкта та процесу обробки. Всі ці три складові мають певне самостійне значення, тому кожен

із них також можна називати принципом, але їх повне розуміння неможливе без взаємного поєднання. Тобто можна виокремлювати особливості кожного із них, однак загалом їх варто трактувати, враховуючи їх єдність. Адже досить часто тріаду навіть позначають єдиним терміном «принцип» (в однині), що підкреслює їх нерозривний зв'язок [8].

Перший із тріади – критерій правомірності – перш за все, встановлює вимогу наявності правомірної підстави обробки. Так, стаття 6 GDPR пояснює, що обробка є правомірною лише в тому випадку, і тою мірою, в якій застосовується хоча б одна із підстав. Однак, часто зазначають і про широке розуміння правомірності, що, окрім підстави, включає в себе і вимогу відсутності загалом будь-яких неправомірних дій із персональними даними. Такий підхід можна прослідкувати, до прикладу, у Рекомендаціях ICO [8]. Іноді зазначається, що принцип правомірності буде дотриманий, якщо буде наявна одна із перелічених підстав для обробки і вона також буде «відповідати [всім основоположним] принципам, викладеним у статті 5» [9]. Існує і третя група науковців, які наполягають на тому, що буквальне тлумачення формулювань GDPR (особливо у порівнянні із Директивою 95/46) вказує, що дотримання принципу правомірності «конкретно і винятково стосується наявності правомірної підстави для обробки відповідно до статті 6» [10].

Пункт 40 Преамбули GDPR з цього приводу зазначає, що для того, щоб обробка було правомірною, персональні дані повинні оброблятись на основі певної підстави правомірності. Однак далі у цьому ж пункті роз'яснюється, що складовими принципу є також (i) необхідність дотримання юридичних зобов'язань, яким підлягає контролер, або (ii) необхідність виконання договору, учасником якого є суб'єкт даних, або (iii) необхідність вжиття заходів на вимогу суб'єкта даних до укладення договору. Мається на увазі, що оцінюванню також підлягає поведінка і виконання обов'язків контролером у відносинах, в межах і на підставі яких відбувається обробка персональних даних. Тобто по суті, текст GDPR не вказує на оцінювання правомірності всієї поведінки щодо персональних даних, однак

зазначає, що сама наявність підстави не означає автоматичне виконання вимог принципу правомірності. Окрім цього, варто звернути увагу на об'єднаність зі справедливістю обробки, оскільки, як вже зазначалось, в тексті Регламенту вони закріплені як єдиний принцип. Тому в цьому аспекті є виправданим підхід ICO, що зазначає про необхідність відсутності будь-яких неправових дій із персональними даними, в загальному значенні цього терміну [8]. Особливо якщо взяти до уваги те, що як і у випадку встановлення порушення інших принципів GDPR, тут наявна певна дискреція уповноваженого органу, що зумовлена оціночним характером закріплених категорій та понять.

Однак, такої неоднозначності варто уникати, коли мова йде про межі основоположних принципів. Перш за все тому, що відповідно до частини 5 статті 83 Регламенту, штраф за їх порушення є вдвічі вищим, ніж штраф за порушення багатьох інших положень GDPR. По друге, трактування неправомірної обробки має безпосередній вплив на реалізацію інших положень Регламенту [10]. До прикладу, відповідно до статті 17, суб'єкт має право на видалення у випадку, якщо його дані обробляються неправомірно. Зважаючи на це, необхідні чіткіші роз'яснення з приводу того, яка обробка вважатиметься неправомірною, крім випадків відсутності правової підстави.

Стаття 6 GDPR встановлює шість категорій підстав для правомірної обробки персональних даних: (i) наявність згоди суб'єкта даних; (ii) необхідність виконання договору, укладеного з суб'єктом даних (або коли необхідне здійснення певних кроків перед укладенням такого договору); (iii) необхідність дотримання зобов'язань, що встановлені нормативно-правовими актами ЄС чи законодавством держави-члена ЄС; (iv) необхідність захистити життєвоважливі інтереси особи; (v) необхідність виконання завдання в інтересах суспільства або здійснення офіційних повноважень, покладених на контролера; а також (vi) необхідність для цілей законних інтересів контролера або третьої сторони, якщо вони переважають над інтересами суб'єкта даних.

Для всіх підстав (окрім наявності згоди суб'єкта даних) необхідно задовольняти критерій «необхідності» обробки. У Рекомендаціях ICO Великобританії (які є одним із прикладів тлумачення і роз'яснення норм GDPR уповноваженими національними інституціями) з цього приводу вказується: «Це не означає абсолютну необхідність обробки. Однак, це має бути щось більше, ніж просто користь чи стандартна практика. Це має бути цілеспрямованим і пропорційним способом для досягнення конкретної мети» [11].

Деякі підстави для обробки персональних даних яскраво відображають новий підхід, що був закріплений GDPR. До прикладу, правомірна обробка на основі згоди суб'єкта даних існувала і раніше, але йдеться про зміну розуміння самого поняття згоди, яка відповідно до пункту 11 статті 4 Регламенту, має бути вільно дана, конкретна, поінформована та однозначна, а також виражатись заявою або чіткою підтверджувальною дією (принцип opt-in). Тобто вимоги до отримання такої згоди деталізовано із забезпеченням дотримання прозорості і поінформованості. Стаття 7 Регламенту, яка встановлює умови для отримання згоди, також і закріплює право відкликати згоду у будь-який час, що має бути так само легко, як і надати її. Окрема згода, відповідно до положень GDPR, надається для кожної окремої конкретної цілі, а при зміні цілей у більшості випадків потрібно отримувати нову згоду [11]. Всі ці вимоги демонструють намір зосередити контроль і надати реальний вибір суб'єкту даних. Тобто відносини між контролером та суб'єктом даних повинні бути побудовані на довірі і залученості останнього у всі процеси.

Щодо інших підстав правомірності, то решта із них зазнали не таких значних змін, порівняно із їх розумінням в Директиві 95/46. Серед них можна виділити унеможливлення посилатись на національне законодавство країн, що не є членами ЄС, як на підставу обробки. Це стосується таких пунктів як дотримання зобов'язань, що встановлені нормативно-правовими актами, а також виконання завдання в інтересах суспільства або для здійснення офіційних повноважень, покладених на контролера. Однак, що зазнало найбільш відчутних змін, то це практичні аспекти

реалізації цих принципів, адже тепер на контролерах лежить обов’язок підзвітності, тобто кожна із підстав повинна бути детально обґрунтована і відображена у відповідній документації [11]. Також змінює практику і вплив принципу прозорості, адже контролери повинні оновити свої повідомлення про конфіденційність, включивши туди свою основу правомірності, і повідомити деталі про це особам [11].

Прозорість, як пояснюється у пункті 58 Преамбули GDPR, вимагає, щоб будь-яка інформація, що надається суб'єкту даних, була лаконічною, легкодоступною та зрозумілою, написана чіткою та зрозумілою мовою, а також, де це можливо, була доповнена відповідною візуалізацією. Відповідно до пункту 39 Преамбули, прозорість також означає і чітке доведення до відома самого факту обробки, так і само як і всіх її обставин.

Як зазначається дослідниками, «прозорість включає у себе як «попередню прозорість» (ex ante transparency), так і «пост-прозорість» (ex post transparency)» [12]. Попередня прозорість «інформує про передбачуваний збір, обробку та розкриття даних і, таким чином, дає змогу передбачити наслідки перед тим, як дані будуть фактично зібрані, наприклад, за допомогою заяв про політику конфіденційності». У свою чергу, пост-прозорість «дає змогу зрозуміти, які дані були зібрані, оброблені чи розкриті (…) та чи відповідає обробка даних заявленій політиці, так само як й інформування про наслідки, якщо дані вже були зібрані» [12].

Прозорість дещо відрізняється від інших складових тріади, адже містить не лише соціальну, а й технічну складову. Як зазначалось в роз’ясненнях Article 29 WP, прозорість «повинна бути реалізована як технічна характеристика, коли це доречно» [13, с. 6]. Тобто відбувається поєднання вимог зрозумілості (соціальний аспект) і доступності (технічний аспект). Оцінка на відповідність цим вимогам, звісно, здійснюється на індивідуальній основі. Однак щодо технічної складової, то існують організації та дослідники, що постійно випускають власні рекомендації на тему впровадження Інструментів підвищення прозорості – «Transparency Enhancing

Tools» [14]. А щодо соціальної складової, то навіть розроблені та функціонують проекти, типу CLAUDETTE, в яких штучний інтелект оцінює та перевіряє Політики та документи організацій на предмет їх зрозумілості [15]. Існують вже і рішення уповноважених органів, деякі з яких будуть розглянуті надалі, які роз'яснюють їх розуміння положень GDPR щодо прозорості, як це має реалізовуватись на практиці і які дії вважатимуться порушенням цього принципу.

Справедливість, третя складова тріади, є найбільш загальним елементом і означає відповідність правомірності та прозорості, у поєднанні із задоволенням розумних очікувань суб'єкта даних щодо того, як оброблятимуться дані [8]. Однак, таке формулювання не дає змоги чітко зрозуміти, яка обробка вважатиметься несправедливою. Також відсутні положення щодо справедливості у преамбулі GDPR. ICO, намагаючись відповісти на це запитання, використовує потрійний критерій, вказуючи на заборону обробляти дані «надто згубно», «несподівано» або «вводячи в оману» [8]. Article 29 WP як приклад несправедливої обробки наводить дискримінаційне профілювання осіб фінансовими інституціями [16, с. 10]. Загалом, у наявних поки рішеннях питання справедливої обробки ще не порушувалось. Це наводить на висновок, що порушення цього критерію не буде встановлюватись часто та існує для випадків, коли обробка буде здійснене на основі неправового закону (як можливість для маневру уповноваженого органу) або буде застосовуватись лише у поєднанні з іншими складовими принципу, тобто із правомірністю та прозорістю.

Отже, загалом, принцип правомірності, справедливості і прозорості обробки має досить базисний і загальний характер, що дає змогу органам, уповноваженим на здійснення контролю, оцінювати всі обставини здійснюваної обробки в кожному конкретному випадку. Складова правомірності встановлює вимогу наявності правомірної підстави для обробки та правомірної поведінки контролера та процесора щодо своїх обов'язків у відносинах, в межах яких відбувається обробка даних. Прозорість об'єднує вимоги зрозумілості, чіткості, легкодоступності в

аспектах змісту комунікації з суб'єктом даних та її технічної організації. Справедливість вимагає задоволення розумних очікувань суб'єкта даних щодо того, як його дані оброблятимуться. Ці три критерії є тріадою, яку об'єднують як єдиний принцип, в якому кожен з елементів має самостійне значення, однак повинен тлумачитись з огляду на інші складові.

Рішення щодо Google. Для більш глибокого розуміння основоположних принципів, їх слід розглядати також і у межах рішень національних органів, уповноважених на захист персональних даних в межах GDPR. Саме так можна прослідкувати, які дії вважатимуться порушенням оціночних категорій та норм Регламенту. Рішення французького органу захисту даних CNIL, винесене 21 січня 2019 року, є одним із найвідоміших серед них (зокрема, через розмір пені, що був на той час найвищим із доти призначених) [17]. Цим рішенням CNIL наклав штраф на компанію Google у розмірі 50 мільйонів євро за недотримання положень Регламенту, що полягало у порушенні принципу прозорості (через недоступність та невідповідність інформації) та принципу правомірності обробки (через відсутність належної згоди щодо персоналізованої реклами). Такий значний розмір штрафу зумовлений публічністю та тим, що були порушені саме основоположні принципи GDPR [17].

Перш за все, щодо порушення прозорості обробки даних. Комітет провів дослідження і виявив, що інформація, яка вимагається GDPR і стосується захисту персональних даних, не була легкодоступною для суб'єктів даних.

У свою чергу, Google звернув увагу на те, що ще під час створення облікового запису, користувачам доступна вся інформація у документі «Політика конфіденційності та умови надання послуг» [18, п. 90]. І та ж сама інформація доступна і в інших документах, тобто згодом можна перейти ще раз як до згаданої «Політики конфіденційності та умов надання послуг», так і до інших окремих документів, що мають назву «Політика конфіденційності» та «Умови надання послуг» [18, п. 91]. Більше того, як звертає увагу відповідач: «Електронний лист

надсилається користувачеві під час створення його облікового запису, в якому, зокрема, зазначено: «Ви можете будь-коли змінити налаштування конфіденційності та безпеки свого облікового запису Google (…)». В листі також надаються посилання, що перенаправляють до різних інструментів налаштувань [18, п.91]. Також для них доступні такі інструменти як «Перевірка конфіденційності», що дозволяє користувачам обирати власні параметри конфіденційності, та «Інформаційна панель», яка дозволяє здійснити загальний огляд використання служб Google [18, п. 92-93].

Але як підкреслив уповноважений орган, основна інформація, серед якої роз'яснення про цілі обробки, період протягом якого заплановано зберігати дані, категорії даних, які використовуються для персоналізації реклами – всі вони були надмірно і розрізнено розкидані по декількох документах. Потрібно було переходити за посиланнями та натискати на різні кнопки, щоб отримати більш детальну інформацію. Це призвело до фрагментації даних і значно збільшило кількість дій, необхідних для доступу до різних документів. CNIL провів експертизу і виявив, що всі дані, що мають основоположний характер для прозорості та інформування, були доступними лише через кілька кроків: «П'ять дій необхідні користувачеві для доступу до інформації, що стосується персоналізованої реклами, і шість для геолокації». [18, п. 101].

Після цього користувачі повинні були уважно прочитати значну кількість інформації, щоб визначити відповідний абзац. А опісля – ще перевірити та порівняти зібрану інформацію, щоб зрозуміти, які дані збираються відповідно до налаштувань [18, п. 97].

Як результат, у рішенні визнано, що компанія Google все ж таки порушила складову прозорості, яка вказує, що інформація повинна бути доступною.

Під питанням були й інші складові цього принципу. Як зазначив CNIL, інформація, яка надавалась Google, не відповідала критеріям чіткості та повноти [18, п. 127]. Компанія здійснювала масштабні операції з обробки і нав'язувала

значну кількість послуг, тоді як роз'яснення, які категорії даних і для яких цілей збираються, були недостатньо конкретними [17]. Роз'яснення, що надавались користувачам, не давали змоги повною мірою «зрозуміти, що правовою основою операцій з обробки персоналізації реклами є згода, а не законний інтерес компанії» [17]. І, крім цього, CNIL зауважив, що не надавалась належна інформація про період зберігання деяких категорій даних [18, п. 119-120].

Іншим аспектом порушення є питання персоналізованої реклами та оголошень. Компанія стверджувала, що отримує згоду користувача на обробку даних для персоналізації реклами. Однак CNIL вважає таку згоду недійсною через недостатню поінформованість суб'єктів даних в момент її надання, а також через неконкретність та неоднозначність такої згоди [18, п. 148, 166].

Так, аналогічно з іншими категоріями, інформація про збір даних для персоналізації рекламних оголошень також була розміщена у декількох окремих документах. На думку уповноваженого органу, це намагання штучно применшити масштаби і обсяг операцій, які проводяться. Користувач, який намагатиметься віднайти інформацію про веб-сайти та додатки, які є учасниками процесу, не матиме змоги цього зробити повною мірою. Адже Google використовує різні сервіси – Google фото, карти, пошук, Play Store тощо. Але інформація всіх цих сервісів ніяким чином не була взаємопов'язана, що не давало можливості користувачам усвідомлювати масштаби інформації, що зосереджується в одного контролера [18, п. 145-147].

CNIL вирішив, що згода, яка використовувалася для персоналізації реклами, не відповідала також і критеріям конкретності та однозначності. Для того, щоб змінювати налаштування оголошень, потрібно було перейти до додаткових параметрів в налаштуваннях облікового запису. Більше того, окрім недостатньої доступності сторінки налаштувань, усі категорії на ній були попередньо відміченими як такі, на які надано згоду, тобто персоналізація оголошень має попередньо поставлену галочку. Це не відповідає критеріям належної згоди,

оскільки відповідно до GDPR згода має надаватись активною дією суб'єкта даних [18, п. 160].

Порушення правомірності полягало і у тому, що згода на всі операції обробки, які здійснювалися контролером, надавалась під час створення облікового запису користувача. Так, під час реєстрації Google пропонував відмітити галочками погодження з умовами надання компанією послуг та надати згоду на обробку даних у спосіб, описаний в Політиці [18, п. 157]. Але, відповідно до GDPR і принципу цільової обробки, у поєднанні із правомірністю, суб'єкт має надавати окрему згоду для кожної цілі обробки. Тому така згода не може вважатись дійсною, що робить обробку даних неправомірною.

Усі ці порушення не були одноразовими, а тривали значний період часу, і на час винесення рішення CNIL досі існували. Так, компанія запроваджувала певні заходи, щоб відповідати вимогам GDPR – інструменти, документи та налаштування, але це не вплинуло на описувані невідповідності вимогам Регламенту [17], через значущість порушень. Як відзначає CNIL: «Порушення, що спостерігаються, позбавляють користувачів істотних гарантій щодо операцій з обробки, які можуть розкрити важливі частини їхнього приватного життя, оскільки вони базуються на величезному обсязі даних, широкому спектрі послуг та майже необмеженій кількості можливих комбінацій» [17].

Отже, уповноважений орган захисту даних у Франції виніс рішення щодо компанії Google, в якому констатоване порушення основоположних принципів GDPR, а саме прозорості та правомірності. Принцип прозорості був порушений через те, що інформація, яка надавалась користувачам не була доступною, чіткою та повною. Таких висновків дійшов орган через те, що доступ до інформації вимагав 5-6 кроків користувача, була відсутня інформація про строки зберігання деяких даних, кожен із сервісів Google надавав інформацію відокремлено тощо. А правомірність була порушена через те, що згода, яку запитувала компанія для персоналізованої реклами, була недійсною, адже не запитувалась відповідно до

кожної конкретної дії і не була побудована за принципом opt-in, який означає, що згода не може бути попередньо наданою і потребує активної дії суб'єкта даних.

1.2.2. Принцип обмеженості ціллю

Обмеженість ціллю складається з двох основних складових. Перш за все це встановлене пунктом (b) частини 1 статті 5 GDPR положення про те, що персональні дані потрібно збирати для конкретних, недвозначних і правомірних цілей (purpose specification). Цілі, для яких здійснюється обробка персональних даних, повинні бути визначені до того, як почнеться обробка, і бути задокументовані та представлені для ознайомлення суб'єкту даних [19]. Суб'єкт надає згоду на обробку даних винятково в певних конкретних цілях, і їх розкриття є необхідним для дотримання принципу прозорості, а закріплення – для принципу підзвітності [19]. При цьому процедурне дотримання цього положення не робить обробку автоматично відповідною GDPR, тобто характер зазначених цілей та їх конкретність, недвозначність та правомірність оцінюватиметься окремо.

Конкретність, як роз'яснюється в актах рекомендаційного характеру, означає, що до або не пізніше моменту збору даних цілі повинні бути точно та повністю визначені, щоб дозволити оцінити відповідність законодавству та застосувати гарантії захисту даних, якщо це потрібно [20, с. 15]. Недвозначність означає, що цілі повинні чітко розкриватися, пояснюватися або виражатися в такій формі, щоб переконатися, що суб'єкти мають однакове і однозначне розуміння цілей обробки незалежно від будь-якого культурного чи мовного різноманіття [20, с. 17]. Правомірність в контексті даного принципу вживається в широкому значенні і «виходить за рамки простого посилання на [одну з правових підстав для обробки]» [20, с. 19-20]. Тобто правомірність самої цілі обробки оцінюватиметься окремо від наявності правової підстави, але з кумулятивним ефектом [20, с. 11].

Друга складова принципу обмеженості ціллю закріплена в цій же ж статті 5

GDPR – це заборона в подальшому обробляти дані у спосіб, що є несумісним з вказаними цілями (compatible use). У Регламенті також зазначається про винятки з цього положення і вказується, що подальшу обробку можна здійснювати лише для суспільних інтересів, для статистичних цілей або для наукового чи історичного дослідження.

Як роз'яснюється на офіційному сайті Європейською комісією, якщо цілі змінюються, то контролер може використовувати персональні дані, перевіривши сумісність нової цілі початковій, лише «якщо дані були зібрані на підставі законних інтересів, договору або життєвих інтересів» [21]. Якщо ж підставою обробки даних є згода суб'єкта даних, а ціль обробки хоча б частково змінюється або доповнюється – потрібно отримати нову згоду [19].

Питання оцінки сумісності із раніше зазначеними цілями розкривається в рекомендаціях та практичних посібниках уповноважених органів. До прикладу, Article 29 WP, так само як і Європейська комісія, зазначають, що коли постає питання чи є нова ціль сумісною, до уваги можуть братись різні критерії як-от: зв'язок між початковою ціллю та новою; контекст, в якому збиралися дані; тип даних та їх чутливість; можливі наслідки обробки; наявність відповідних гарантій, для уникнення несправедливої обробки (шифрування, псевдонімізація)» тощо [20, с. 3; 19]. Article 29 WP у своїх висновках детально пояснюють кожен із цих елементів а також наводять 22 приклади для кращого розуміння того, які цілі є сумісними в контексті даного принципу, водночас вказуючи на умовність таких прикладів і окреслюючи наскільки багато факторів підлягають оцінюванню у кожній ситуації [20, с. 56-70]. У висновках також наголошується, що ці положення «повинні заохочувати контролерів краще дотримуватися всіх горизонтальних положень Директиви: [тобто,] чим більше уваги вони приділено захисту персональних даних в цілому, тим більше шансів, що будь-яке подальше використання, яке вони передбачають, може бути визнане сумісним» [20, с. 56].

Зважаючи на характер та специфіку реалізації, принцип обмеженості ціллю

часто розглядається як бар'єр для інновацій, що пов’язані із даними, особливо у його поєднанні із принципом мінімізації даних [22]. В основному це стосується Великих даних (Big Data) та методів їх аналізу. Цей термін позначає «величезні і об'ємні набори даних, які можуть бути структурованими або неструктурованими», щодо яких регулярні методи обробки даних не працюють через їх значний такий їх обсяг та варіативність [23].

Аналіз Великих даних відіграє важливу роль у багатьох сферах: від освіти (для створення індивідуальних програм навчання; для оцінювання; прогнозування кар'єри тощо) до банківської сфери (зменшення ризиків під час кредитування, відстеження відмивання коштів тощо); так само як і для потенційних стартапів (дослідження ринку і затребуваність можливої послуги); чи у медичній сфері (для вивчення досвіду інших лікарів, екологічних чинників) тощо [23]. Часто компанії використовують такий аналіз і для збільшення ефективності їх маркетингу. Тобто загалом, обробка Великих даних може здійснюватись як для виявлення загальних тенденцій, так і для прийняття рішень, що стосуються конкретної особи.

На практиці часто буває так, що мета аналізу виявляється уже в процесі або як результат аналізу великих масивів даних. На це звертають увагу практики, зазначаючи, що спочатку може бути не до кінця зрозуміло, як дані будуть використовуватися, чи буде виявлено якісь закономірності чи особливості поведінки суб’єкта у них тощо [23; 24]. В свою чергу, «твердження, що дані збираються для (будь-якої можливої) аналітики Великих даних не є достатньо визначеною метою» в розумінні вимог GDPR [23].

Частково обробка персональних даних в межах Великих даних може здійснюватись як один із винятків GDPR і вважатись, до прикладу, обробкою для статистичних цілей. Однак, це все одно вагомо зменшує обсяг можливого застосування аналізу Великих даних, оскільки в пункті 162 Преамбули GDPR вказано, що обробка для статистичних цілей вимагає обробки не персональних, а сукупних даних, і що цей результат не може використовуватись для підтримки

заходів чи рішень стосовно будь-якої конкретної фізичної особи. Як результат – такі вимоги виключають можливість на основі проаналізованих даних, до прикладу, створювати тарґетовану рекламу, що базується на поведінці людини тощо.

З іншого боку деякі дослідники вважають, що положення GDPR навпаки є корисними для інновацій, що пов'язані із даними. Перш за все, їх користь проявляється у принципі прозорості. Завдяки реалізації положень цього принципу, підвищується рівень довіри суб'єктів даних до контролерів та їх процесорів, що є однією із найважливіших умов для інноваційних досліджень [25]. Окрім цього, завдяки GDPR, дані, які збираються, стали більш якісними і точними. Тому і дослідження, що будуть базуватись на їх основі є більш вірогідними та надійними [26, с. 3].

Отже, принцип обмеженості ціллю обробки персональних даних встановлює дві вимоги: перш за все, визначення цілей до початку обробки і інформування суб'єкта даних щодо них під час запитування згоди та, по друге, заборона обробляти дані, якщо ціль обробки змінилась, а нової згоди не було отримано. Окрім цього, встановлені цілі мають відповідати критеріям конкретності, недвозначності і правомірності. Встановлення цілі є необхідною передумовою для дотримання інших основоположних принципів персональних даних, до прикладу, таких як підзвітності, прозорості чи мінімізації даних.

1.2.3. Принцип мінімізації даних

Закріплений у пункті (c) частини 1 статті 5 GDPR, принцип мінімізації даних охоплює собою декілька вимог. В основному, це вимоги щодо обсягу і змісту даних, які обробляються. Такі дані повинні бути належними (адекватними), відповідними і обмеженими до необхідного обсягу, з огляду на цілі обробки.

Як і в більшості принципів, встановлення відповідності критеріям належності, відповідності і обмеженості до необхідного обсягу відбувається у

кожній конкретній ситуації, з урахуванням як об’єктивних критеріїв, так і суб’єктивного сприйняття контролером певних даних як належних, відповідних і необхідних [27].

Щоб виконати принцип мінімізації даних і обмежити обсяг даних до необхідного, потрібно точно встановити цілі обробки. Тобто принцип обмеженості ціллю є необхідною умовою для реалізації принципу мінімізації даних [27]. Після конкретизації цілей, дані перевіряють і припиняють обробку тих, які не стосуються цілі чи не допомагають її досягти [27]. Неналежні дані не просто не використовують, а, як правило, видаляють, щоб забезпечити виконання принципу обмеження зберігання, що розкриватиметься надалі.

У деяких випадках такі дані, які не підпадають під критерії належності, відповідності і обмеженості до необхідного обсягу, не видаляються, але до них застосовують техніки анонімізації, в результаті яких дані перестають бути персональними в розумінні GDPR. Як роз’яснюється у пункті 26 Регламенту, анонімізація це продовження зберігання даних так, що за допомогою них суб'єкт даних не є або більше не може бути ідентифікований. Як правило, це здійснюється для того, щоб в подальшому використовувати дані з дослідницькими чи статистичними цілями. Однак, в таких випадках важливо забезпечувати повну анонімізацію, оскільки, якщо контролер чи процесор здійснює певні заходи, але в результаті за допомогою певних дій чи використання додаткової інформації встановити суб’єкта даних все ще можливо, то це буде псевдонімізацією, яка підпадає під регулювання GDPR і на яку поширюються норми щодо персональних даних [24].

Прикладом недостатності заходів для анонімізації даних є справа Taxa 4×35 – датської служби для виклику таксі [28]. Для податкових та інших цілей система Taxa збирає важливі дані про користувачів, як-от: ім’я, номер телефону, час та GPS координати початку та завершення поїздки, деталі щодо оплати тощо. У 2018 році датське агентство захисту даних виявило, що компанія без необхідності протягом

п'яти років продовжувала зберігання таких даних щодо декількох мільйонів поїздок. Як підкреслив уповноважений орган, «таке зберігання записів суперечило статті 5 GDPR», а саме принципам мінімізації даних та обмеження зберігання [28].

Керівництво компанії ж вважало, що «вони звільнені від виконання [цих положень], оскільки вони анонімізували дані, видаляючи імена користувачів зі своєї бази даних через два роки» [28]. Але такі заходи були визнані уповноваженим органом неналежною анонімізацією, вказуючи, що «навіть без імені користувача компанія все ще мала достатньо особистої інформації для ідентифікації особи», і Таха зобов'язали виплатити штраф у розмірі майже 160 000 євро [28]. Тобто заходи анонімізації мають виключати будь-яку подальшу можливість встановлення особи суб'єкта даних.

Як було вказано, відповідно до GDPR, дані, що продовжують оброблятись, повинні відповідати трьом критеріям. І якщо належність і відповідність даних викликають менше складнощів, то з практичного досвіду можна зазначити, що встановлення необхідних даних може бути проблемним. Адже контролеру часто складно оцінити, чи весь обсяг наявної інформації потрібно обробляти, щоб досягти цілей обробки, і чи можна цей обсяг зменшити без шкоди для досягнення цілей. Крім цього, важливо пам'ятати, що потрібно зменшувати обсяг не лише різних за змістом даних, а й обсяг зберігання одних і тих самих персональних даних. Це стосується ситуації, коли великі компанії створюють дзеркальні сервери, на які повністю дублюється інформація з головних серверів, щоб у випадках недоступності чи знищення інформації з основного сервера, її можна було повністю відновити, використовуючи дзеркальний сервер. Такі заходи є допустимими, коли створюється один чи два (якщо даних багато) таких дзеркальних сервери. Однак практика показує, що їх створюють у значно більшій кількості, іноді до 10 штук. Все це підвищує ризики витоку даних і може оцінюватись як порушення мінімізації даних.

Для досягнення реалізації принципу мінімізації даних на практиці, необхідне

запровадження підходу «privacy by design» ще на стадії розробки користувацького інтерфейсу, бази даних та архітектури відповідної програми, в межах якої відбуватиметься збір даних. Для цього існують різноманітні стандарти, рекомендації та принципи для розробників, такі як Fair Information Practices (FIPs) [29], Privacy by Design (PbD) [30] або Data minimization (DM) [31].

Однак, реалізація цих принципів розробниками ще потребує вдосконалення. Як показують дослідження, лише частка розробників намагається впровадити інструменти мінімізації даних у свої програми. Більшість із них зазначає про відсутність чітких роз'яснень чи критеріїв оцінки інструментів DM. В основному, ними запроваджуються лише окремі інструменти і лише на стадії зберігання даних [31, с. 2-3]. Важливою проблемою для розробників є також нездатність заздалегідь визначити потенціал даних, які вони могли б зібрати [31, с.3]. Окрім цього, якщо виникає вибір між впровадженням інструментів privacy by design чи відповідність потребам бізнесу, для якого створюється конкретна програма, то статистика свідчить про надання переваги останньому [31, с. 4; 30, с.3]. Тому для належної реалізації принципу мінімізації даних необхідними заходами є підвищення професійної культури та обізнаності розробників програмного забезпечення у питаннях захисту персональних даних [32, с. 5].

Також ICO звертає увагу, що на практиці може бути важко забезпечити баланс між мінімізацією даних і точністю, а також правом суб'єкта на виправлення [33]. Адже обмеження обсягу даних може впливати на їх цілісність, а висновки, що будуть зроблені на основі таких даних можуть бути недостовірними, тобто принцип точності не буде реалізований. Також цілком ймовірною є ситуація коли суб'єкт даних, користуючись своїм правом на виправлення, вимагатиме внесення даних, що не є належними чи відповідними для досягнення встановлених цілей обробки. В таких ситуаціях суб'єкту, що здійснює обробку, потрібно оцінювати дані з урахуванням цілей такої обробки і намагатись дотримуватись балансу між дотриманням цих принципів [33].

Можна підсумувати, що принцип мінімізації даних об’єднав у собі вимоги до обсягу тих даних, що обробляються, а також до їх змісту. Для визначення того в якому обсязі і які дані потрібно зберігати, контролер повинен визначати цілі обробки і періодично здійснювати перегляд того, чи є подальша обробка потрібною для досягнення таких цілей. Дані, які не відповідають критеріям даних положень, повинні бути видалені або повністю анонімізовані (якщо контролеру чи процесору необхідно їх використовувати для статистичних чи дослідницьких цілей).

1.2.4. Принцип точності

Принцип точності закріплений в пункті (d) частини 1 статті 5 GDPR, де зазначається, що персональні дані повинні бути точними, і у разі необхідності – оновлені. GDPR підкреслює, що повинно бути здійснено всі розумні дії, щоб пересвідчитись, що персональні дані, які є неточними, зважаючи на цілі обробки, були видалені або виправлені без затримки.

Є дві групи даних, обробка яких становить порушення принципу точності – неправильні (incorrect) або ті, які вводять в оману (misleading). Якщо неправильні дані є об’єктивно суперечливими щодо конкретних фактів, то дані, які вводять в оману, можуть бути і правильними, однак через їх обсяг вони створюють певне враження і наводять на висновки, які є оманливими. Для того, щоб ідентифікувати дані, що вводять в оману, потрібно визначити цілі їх обробки, так як необхідно оцінювати функцію сукупності даних, зважаючи на цілі обробки [33].

Існує ще одна група даних, які називаються неактуальними даними. Вони не є неточними за замовчуванням, однак можуть бути такими. Неактуальні дані можна обробляти для історичної довідки чи для відображення послідовності дій і подій тощо, однак з відповідними примітками про це [33]. До прикладу, якщо особа змінила своє ім’я, зазначення її попереднього імені може бути неточною інформацією, однак якщо це здійснюється саме для того, щоб зазначити, що особа

раніше мала таке ім’я, то такі дані не можна вважати неточними. Іноді необхідним може бути обробка і зберігання власне неточної інформації, однак із чітким визнання її такою. Це може стосуватись поставлених діагнозів під час лікування чи здійснених помилкових транзакцій тощо [33].

На практиці трапляється, що точність деяких даних неможливо оцінити. Це стосується оцінок та суджень. Так, дослідники звертають увагу, що «лише факти («суб'єкт даних є чоловіком») можуть бути об'єктивно переглянуті та виправлені, тоді як ціннісні судження («суб'єкт виглядає чоловіком») не дають такої змоги». Тому рекомендується обмежувати обробку оціночних суджень, щоб уникнути можливих порушень прав суб’єкта даних [34].

Процедура дотримання принципу точності складається із превентивних заходів та пост-перегляду, тобто після того, як дані вже почали обробляти [35]. В межах обох стадій GDPR вимагає від організацій вжиття всіх розумних кроків та заходів, щоб забезпечити точність оброблюваних даних. Особливо актуальним це є у випадках, коли до обробки даних залучається штучний інтелект [36]. У таких випадках рекомендують як належні превентивні заходи: (i) «забезпечити втручання людини і не покладатися лише на машину»; (ii) «використовувати технології аналізу точності даних» (контроль продуктивності AI та використання Machine Learning); (iii) «провести оцінку впливу на захист даних (DPIA) та надійну оцінку штучного інтелекту»; (iv) «провести суворі випробування, наприклад, тести на проникнення та оцінки кібербезпеки»; (v) «забезпечити відстеження, перевірюваність та прозоре спілкування щодо можливостей системи» штучного інтелекту. [36].

Щодо пост-перегляду, то наскрізний аналіз норм GDPR дає можливість зробити висновок, що суб’єкт, який обробляє дані, повинен переглядати їх як самостійно з певною періодичністю, так і за зверненням суб’єкта. За результатами перегляду, у випадку виявлення неточних даних, їх потрібно змінити, доповнити або видалити. Для того, щоб забезпечити практичну можливість дотримання цього принципу, потрібно пересвідчитись, що існує визначена процедура, за якою суб’єкт

даних може звернутись і отримати інформацію про те, які дані про нього обробляються, а також подати відповідний запит на виправлення чи видалення даних. Тобто важливими є процедури реалізації окремих прав суб'єкта: права на виправлення, права на стирання даних, права на доступ (ст. 15-17 GDPR) та інших [33].

Сама процедура виправлення/стирання даних має здійснюватися із дотриманням принципу прозорості: передбачені механізми звернення та інформування мають бути у доступній для розуміння формі, з використанням чітких і простих формулювань. Доступ до відповідних механізмів має бути легким для суб'єкта, не ускладненим додатковими умовами, складною покроковою структурою тощо [33].

У випадках, якщо контролер чи процесор самостійно визначив неточність певних даних, під час періодичного перегляду, і вирішив їх змінити, доповнити чи видалити, він повинен сповістити про це суб'єкта даних, відповідно до статті 19 GDPR [2]. Це є складовою принципу прозорості.

Як вже згадувалось, точність даних є одним із тих принципів, що має потенціал неабиякого впливу на розвиток інновацій, пов'язаних із даними [26]. Саме вдосконалення точності у поєднанні із ефективною комунікацією із суб'єктом даних в межах принципу прозорості має стати парадигмою поведінки із даними для компаній, у володінні у яких зосереджені великі масиви персональних даних. При забезпеченні безпеки таких даних можна буде досягти довіри зі сторони суб'єктів даних, що є базисом для розвитку і прогресу, коли мова йде про роботу із персональними даними [25].

Отже, принцип точності, що є одним із основоположних принципів захисту персональних даних, пов'язаний із обмеженням обробки персональних даних, що є неправильними або які вводять в оману. Крім цього, в межах цього принципу встановлюються особливі умови для обробки неактуальних даних. Реалізація цього принципу пов'язана зі створенням умов для суб'єктів даних на реалізацію своїх

прав, зокрема на виправлення чи на стирання даних, а також покладає на суб’єкта, що обробляє дані обов’язок самостійно періодично переглядати їх, щоб пересвідчитись, що вони є точними, незалежно від звернень суб’єктів даних.

1.2.5. Принцип обмеження зберігання

Принцип обмеження зберігання закріплений у пункті (e) частини 1 статті 5 GDPR. Відповідно до цього положення, персональні дані повинні зберігатись у формі, яка дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для досягнення цілей обробки. Винятки, що передбачені із загального правила, передбачають, що персональні дані можуть зберігатися на більш тривалі терміни для цілей архівування в суспільних інтересах, наукових, історичних або статистичних цілях. Порядок зберігання в межах цих винятків деталізується статтею 89 (1) GDPR. Важливою умовою зберігання даних довше, ніж це необхідно, є виконання відповідних технічних і організаційних заходів, передбачених GDPR, щоб захистити права і свободи суб'єкта даних.

У вимогах до обробки даних довше, ніж це необхідно, вказано, що архівування в суспільних інтересах, а також наукові, історичні або статистичні цілі можуть досягатись, якщо дані будуть змінені так, що за допомогою них вже не можна буде ідентифікувати суб’єкта даних. Але, як зазначалось в межах принципу мінімізації даних, анонімізація повинна бути повною, і, окрім цього, обґрунтованою, а дані, які зберігаються в таких цілях, не можуть бути використані потім у будь-яких інших [24].

Для того, щоб мати можливість довести, що принцип обмеження зберігання не порушено, потрібно передбачати стандартні терміни зберігання даних у відповідній документації (наприклад, у Політиці конфіденційності). Але при цьому наявні дані все одно потрібно періодично переглядати, в межах реалізації мінімізації даних, і видаляти чи анонімізувати ті дані, які вже не є потрібними [37].

Аналогічно до принципу точності, принцип обмеження зберігання і процес його реалізації є відмінним від обов'язку видаляти дані за зверненням суб'єкта. Тобто контролер чи процесор повинен самостійно видаляти дані, якщо є така необхідність, навіть за відсутності звернення суб'єкта.

На практиці суб'єктам, що обробляють дані, часто важко визначити, який саме період зберігання даних є необхідним для них. Як показує практичний досвід, при розрахунку цього строку необхідно брати до уваги декілька чинників. Перш за все, варто зважати на правомірну основу обробки даних. Якщо така обробка, до прикладу, відбувається на основі договору, то строк зберігання даних не буде меншим за строк дії договору. Найчастіше він буде навіть більшим за період чинності договору, оскільки повинен включати також ймовірність пред'явлення претензії чи звернення до суду щодо виконання цього договору.

Також, очевидно, варто зважати на цілі обробки. З моменту, коли основна ціль досягнута, довести необхідність обробки будь-яких даних ускладнюється. Адже дані не можуть зберігатися на невизначений термін «про всяк випадок», через теоретичну користь в майбутньому. При продовженні строку потрібно мати змогу чітко продемонструвати ймовірність необхідності персональних даних у майбутньому.

При оцінюванні виправданості зберігання до уваги беруться всі обставини. Так, ICO наводить як один із прикладів, що виправданим буде зберігання чутливих медичних даних працівника, якщо він може отримати ушкодження на робочому місці. Тоді як коли ризик отримати ушкодження є невисоким, подальше зберігання даних про групу крові буде порушенням принципів обмеження зберігання так само як і мінімізації даних [27].

У межах визначення періоду зберігання даних потрібно враховувати також й вимоги нормативно-правових актів, що стосуються діяльності суб'єкта, що обробляє інформацію. Це можуть бути вимоги, що стосуються оподаткування, вимог у сфері обліку і аудиту, строків позовної давності тощо. Але й у межах цих

строків все одно потрібно періодично перевіряти, чи є зберігання даних справедливим і правомірним. І чим довшим є встановлений стандартний період зберігання, тим частіше потрібно здійснювати періодичний перегляд, оскільки при тривалій обробці, необхідність може із кожним роком зменшуватися.

В цьому аспекті виникає питання необхідності внесення змін до національного законодавства в Україні в межах імплементації GDPR, оскільки законодавчі вимоги стосовно строків збереження деяких даних не відповідають критеріям розумності і можуть суперечити принципу обмеження зберігання. До прикладу, відповідно до Наказу Міністерства юстиції № 578/5, в органах державної влади та місцевого самоврядування вся документація, що стосується кадрових питань повинна зберігатись протягом 75 років [38]. І якщо зберігання окремих загальних даних ще може бути обґрунтовано можливою необхідністю цих документів при оформленні пенсії, то необхідність зберігання всіх інших документів (щодо зміни біографічних даних, заохочення, нагородження, преміювання, всіх видів відпусток та відряджень тощо) повинна бути переглянута, оскільки ймовірність того, що ці документи знадобляться через 75 років є надто малою, а отже – не переважає ризики, що виникають у зв’язку зі збереженням такого широкого обсягу персональних даних особи.

Отже, принцип обмеження зберігання є певним продовженням принципу мінімізації даних і встановлює вимоги до контролера і процесора щодо періоду, протягом якого можуть зберігатись дані. Для дотримання цього принципу важливо оцінити всі аспекти щодо необхідності зберігання даних. В межах цього, ймовірно, необхідним буде врахування правової основи і цілей обробки, дослідити вимоги національного законодавства щодо строків, які можуть стосуватись персональних даних та інтереси контролера чи процесора щодо можливої необхідності продовжувати зберігання даних. Якщо ж продовження зберігання не є обґрунтованим, то такі дані потрібно видалити або повністю анонімізувати для реалізації принципу обмеження зберігання.

Справа Deutsche Wohnen SE. Обмеження зберігання є одним із тих принципів, для розуміння якого також необхідно детально розглядати практику його реалізації. Одним із актуальних рішень в цьому аспекті є рішення німецьких уповноважених органів у справі Deutsche Wohnen SE. 30 жовтня 2019 року уповноважений орган з питань захисту персональних даних та свободи інформації в Німеччині призначив штраф у розмірі близько 14,5 мільйонів євро компанії Deutsche Wohnen SE за порушення окремих основоположних принципів GDPR, а саме: принципів обмеження зберігання та правомірності обробки [39].

Deutsche Wohnen SE є великою компанією з нерухомості, і під час перевірок у червні 2017 та березні 2019 року було встановлено, що у неї є архівна система для зберігання персональних даних орендарів. Вона була організована таким чином, що не передбачалось технічної можливості вилучати персональні дані, навіть після спливу значного періоду часу [40]. Це становить порушення принципу обмеження зберігання, оскільки в його межах контролеру необхідно організовувати процеси компанії таким чином, щоб дані не зберігались довше, ніж це необхідно. Також було констатовано порушення статті 25 GDPR, що містить вимогу privacy by design, оскільки вона вимагає, щоб приватність була вбудованою у всі процеси, що відбуваються у компанії, а створення архівів, з яких неможливе видалення даних очевидно цьому суперечить [40].

Крім відсутності технічної можливості для видалення, як вказується уповноваженим органом «персональні дані орендарів зберігалися без будь-яких перевірок чи зберігання взагалі дозволене чи потрібне». Експертизи, проведені ним в Берліні у червні 2017 та березні 2019 року, встановили, що дані орендарів, що зберігаються в архіві, не є важливими для ведення ділових операцій [41]. Тобто там зберігались дані, обробка яких вже не була необхідною для досягнення визначених цілей. Це є порушенням принципів обмеження зберігання і мінімізації даних, а також правомірності обробки, оскільки зберігання даних означає їх обробку, а підстав для її здійснення у компанії не було [39].

Персональні дані, що зберігались в архівах, вміщували, в тому числі, «інформацію про особисті та фінансові обставини орендарів, зокрема заяви про їх заробітну плату, (…) виписки з трудових та навчальних договорів, податкові дані, дані про соціальне та медичне страхування та виписки з банку» [41].

Під час перших випадків виявлення архіву, уповноважений орган рекомендував терміново змінити систему зберігання даних. Тим не менш, у березні 2019 року, через півтора роки після першої інспекції та через дев'ять місяців після початку застосування GDPR, компанія все ще не змогла ні продемонструвати видалення застарілих даних із бази, ні надати причини для необхідності подальшого зберігання [40].

Компанія фактично зробила попередні кроки для усунення недоліків. Однак цих заходів було недостатньо для приведення у відповідність зберігання персональних даних із вимогами Регламенту [39; 41].

Щодо призначеного штрафу, то GDPR вимагає від уповноважених органів гарантувати, що штрафи в кожному окремому випадку є ефективними, пропорційними та превентивними [41]. Тому відправною точкою обчислення штрафних санкцій є річний оборот коштів відповідних компаній. Оскільки річний оборот Deutsche Wohnen SE перевищив 1,4 мільярда євро відповідно до його річного звіту за 2018 рік, законодавчо встановлений ліміт штрафу становив близько 28 мільйонів євро [41].

Під час визначення розміру штрафу, були визнані обтяжуючими фактами, що Deutsche Wohnen SE навмисно створив відповідну архівну структуру, і що ці дані оброблялись неправомірно протягом тривалого періоду. З іншого боку, було враховано як пом'якшуючий фактор те, що компанія вже почала реалізовувати деякі заходи для виправлення протиправної ситуації та офіційно співпрацювала з уповноваженим органом [41].

Справа Deutsche Wohnen SE є знаковою для Німеччини і імплементації основоположних принципів Регламенту у державі, оскільки, як зазначає

уповноважений орган щодо захисту персональних даних: «На жаль, ми часто стикаємось з кладовищами даних, такими як ми знаходили в Deutsche Wohnen SE, в наглядовій практиці» [41].

Рішення у цій справі також демонструє, що мільйонні штрафи можуть стягуватися навіть у випадках, коли не відбулося витоку даних, неправильного використання, чи не було завдано матеріальної шкоди. Тобто контролери повинні превентивно переглядати, як відбувається процес обробки і чи всі принципи дотримуються при цьому.

Уповноважений орган звертає увагу, що порушення у даному випадку складається з двох складових і недостатньо лише створити можливість стирати дані, обробка яких вже не є необхідною; саме стирання також повинно бути здійсненим [41].

Отже, справа Deutsche Wohnen SE демонструє взаємопов'язаність принципів мінімізації даних, обмеження зберігання та правомірності обробки, а також концепції privacy by design. Зберігання персональних даних в архівах, довше ніж це необхідно, без можливості видалення, буде становити порушення усіх цих положень, навіть якщо не відбулось витоку даних чи завдання матеріальної шкоди суб'єкту.

1.2.6. Принципи цілісності та конфіденційності

У GDPR закріплено ще два важливі для ЄС принципи захисту персональних даних, а саме принципи цілісності та конфіденційності. Обидва принципи декларуються у пункті (f) частини 1 статті 5 GDPR. Цілісність стосується як і певного стану якості даних, так і процесу його забезпечення. З цього приводу зазначають: «Цілісність даних як стан визначає набір даних, який є і дійсним, і точним. З іншого боку, цілісність даних як процес, описує заходи, що застосовуються для забезпечення достовірності та точності набору даних» [42].

Конфіденційність даних – це «захист даних від ненавмисного, незаконного або несанкціонованого доступу, розкриття чи крадіжки» [43]. Іншими словами, це така організація всіх процесів обробки персональних даних, при якій доступ до даних може отримати лише той, хто уповноважений на це.

Ці два принципи часто об’єднують в єдиний принцип безпеки, оскільки саме в такій формі відповідні положення були закріплені в Директиві 95/46, хоч і не в межах основоположних принципів [44]. Відповідно до цієї норми, персональні дані повинні оброблятись таким чином, щоб забезпечити належну безпеку персональних даних, в тому числі захист від несанкціонованої чи неправомірної обробки, а також від випадкової втрати, знищення або пошкодження. GDPR в статті 32 розкриває безпеку як перелік необхідних для здійснення заходів, серед яких (i) псевдонімізація та шифрування даних; (ii) здатність забезпечити постійну конфіденційність, цілісність, доступність і стійкість систем обробки; (iii) можливість своєчасно відновити доступність та доступ до персональних даних у випадку фізичного або технічного інциденту; (iv) регулярне тестування, оцінки ефективності технічних та організаційних заходів для забезпечення безпеки. При цьому, впровадження таких заходів не повинно створювати перешкоди для реалізації інших принципів, тобто безпека має технічно уможливлювати інші складові.

Рівень заходів, які є необхідними, визначається у кожному конкретному випадку суб’єктом, що здійснює обробку. При цьому потрібно враховувати особливості наявної техніки, так само як і «стан і рівень витрат на реалізацію [заходів], а також сутність, обсяг, контекст і мету обробки» [45]. Для того, щоб визначитись із необхідними заходами, потрібно визначити, які в суб’єкта загалом є дані, де вони зберігаються, визначити чи є вони чутливими і чи потребують особливих технічних умов для обробки, окреслити коло осіб, що мають до них доступ тощо [45].

Окрім вимог у технічній сфері, реалізація принципів цілісності та конфіденційності передбачає проведення організаційних заходів. Потрібно

провести навчання працівників, що будуть мати доступ до обробки, визначити особу відповідальну за безпеку персональних даних, забезпечити належну внутрішню комунікацію між такою відповідальною особою та технічними працівниками, забезпечити фізичну безпеку підприємства (охорона, сигналізація) тощо [45].

Окремим аспектом є визначення і перевірка процесорів – суб'єктів, яким передаються персональні дані на обробку. У випадках, якщо контролер, що отримує дані від суб'єкта, передає їх на обробку процесору, то він повинен здійснити моніторинг рівня відповідності процесора вимогам GDPR. Тобто контролер має забезпечити, щоб при передаванні даних і при обробці їх процесорами, рівень безпеки був таким же, як і міг би бути, якщо б обробка здійснювалась ним самостійно [46]. Це важливо в контексті досвіду України, оскільки саме це положення вже змушує деякі українські компанії приводити практику обробки персональних даних у відповідність до GDPR. Для уможливлення ефективної співпраці українських компаній із європейськими, це має стати загальнодержавною практикою.

У статті 32 GDPR, де розкривається аспект безпеки обробки, цілісність і конфіденційність доповнюється доступністю, а також принципом стійкості. Доступність, як і цілісність та конфіденційність, стосується як систем, за допомогою яких здійснюється обробка, так і самих даних. Якщо конфіденційність означає неможливість отримання даних для неуповноважених осіб, то доступність – навпаки «означає, що інформація доступна авторизованим користувачам», навіть у випадках, коли на бази даних здійснюється атака [47].

Стійкість має відношення лише до систем і об'єднує вимоги, що спрямовані на забезпечення їх нормальної роботи при технічних чи фізичних інцидентах. Тобто стійкість уможливлює продовження функціонування під час збоїв та стосується здатності організації відновити системи до ефективного стану [45].

За втручання чи технічних збоїв у системі, коли відбувається витік персональних даних, в організації повинен бути чіткий план подальших дій,

прописаний в її внутрішній документації. Під витоком даних, в термінології GDPR розуміється «порушення безпеки, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розголошення або доступу до персональних даних» [47]. Тобто витоки даних є наслідком як випадкових, так і навмисних причин. І вони можуть мати низку несприятливих наслідків для людей, від емоційних страждань до фізичної шкоди [47].

Коли відбувається якийсь інцидент із безпекою, слід невідкладно встановити, чи відбувся витік персональних даних, і, якщо це так – вжити заходів щодо його усунення та повідомити уповноважений орган про це. Якщо витік підлягає повідомленню, контролер повинен повідомляти про нього «не пізніше ніж через 72 години після того, як він про це дізнається» [47]. На випадок, якщо витік стається у процесора, в контракті між ним та контролером повинні бути прописані положення про негайне звітування останньому [48]. Повідомляти потрібно уповноважений орган, та у випадках ризику для прав і свобод – також суб'єкта даних [47]. Як показує практика, неповідомлення є одним із факторів призначення найвищого із можливих штрафів у випадку виявлення уповноваженим органом, що такий витік відбувся. Усі випадки витоку також потрібно відображати у внутрішній документації для подальшої можливої реалізації принципу підзвітності [48].

Отже, принципи цілісності і конфіденційності закріплені поряд із іншими основоположними принципами захисту персональних даних і висувають вимоги забезпечення організаційної, фізичної та кібербезпеки при обробці персональних даних. В інших положеннях GDPR вони пов'язуються із принципами доступності та стійкості. Всі заходи спрямовані на те, щоб унеможливити ризик витоку даних. Якщо ж він все-таки відбувається – контролер повинен діяти невідкладно і здійснювати заходи для зменшення шкоди для прав та свобод суб'єкта даних.

Справа Gesthotel Activos Balagares. Під час характеристики принципів цілісності та конфіденційності, основна увага звертається на технічні характеристики, необхідні для того, щоб забезпечити кібербезпеку. Однак, не менш

важливими є організаційні аспекти цих принципів. Вони спрямовані на забезпечення обізнаності всіх працівників компанії щодо основоположних принципів та процесів, яких необхідно дотримуватись. ICO у своїх роз'ясненнях неодноразово звертає на це увагу.

У даній справі скаржник надіслав приватний лист керівництву готелю «Лос-Балагарес» та делегатам профспілки, щоб проінформувати їх про цькування, якого він зазнав на роботі. Окрім деталей конфліктної ситуації, цей лист також містив чутливі дані, пов'язані з особливостями його медичного стану [49, с. 1].

Заявник стверджує, що «після отримання листа, керівництво готелю та делегати профспілки (…) скликали у березні 2018 року зустріч з рештою колег, щоб прочитати зміст надісланого [скаржником] листа» [49, с. 1]. Прочитання було зафіксоване у протоколі відповідного зібрання.

У свою чергу, відповідач стверджує, що під час зібрання і прочитання листа не було розкрито медичні дані особи, а «єдиною прямою транскрипцією змісту листа була та, яка з'являється у протоколі зборів і є тією, що стосується ситуації цькування, про яку стверджує працівник-скаржник» [49, с. 1]. Це здійснювалось для того, щоб проінформувати працівників щодо деталей ситуації, яка для них не є новою, а тягнеться у компанії вже протягом декількох років і в загальному відома усім, оскільки скаржник уже відкрито заявляв про попередні випадки цькування [49, с. 1].

Тобто, як вважають представники готелю, оскільки частину про медичні захворювання безпосередньо на засіданні не обговорювали, то обставини, які було розголошено на зібранні, не були приватними або медичними даними. Також вони вказують на необхідність такого розголошення: «Єдиною метою такого заходу було знайти вирішення конфлікту, який було порушено [в цьому листі, і в межах цього необхідно було] звернутися до запиту, який сам заявник передав керівництву та офіційному представництву працівників» [49, с. 2].

Представники профспілки також добавили, що для них ігнорувати скаргу,

вміщену в листі, було б відмовою від здійснення своїх основних функцій та засвідчення неспроможності захистити інших працівників у схожій ситуації [49, с. 2]. Представники профспілки, аналогічно до керівництва готелю, підкреслюють, що весь лист на зустрічі був викладений підсумовано, і здійснювалось посилання лише на ту частину листа, в якому заявник стверджує, що «він став об'єктом жорстокого поводження з боку багатьох колег, які ізолюють його,(…) не розмовляють з ним, та ігнорують посилання на страждання від тривоги і стресу через його тимчасову недієздатність» [49, с. 2]. При цьому факт його недієздатності для них усіх був очевидним, через довгу відсутність заявника на роботі.

Щодо викладених аргументів і ситуації загалом, уповноважений орган з питань захисту даних Іспанії зазначає, що «хоча протокол дій компанії щодо випадків цькування на робочому місці відповідачем не був наданий, вважається доведеним, що лист працівника був прочитаний на засіданні, який скликала профспілка, тому про його зміст було повідомлено всіх працівників [готелю]» [49, с. 4]. І сам факт публічного прочитання приватного листа особи, навіть для певної потрібної мети (у нашого випадку – для доведення до відома і обговорення ситуації цькування), є порушенням статті 5 GDPR, а саме принципів цілісності та конфіденційності персональних даних. Оскільки не лише медичні дані захищаються в межах Регламенту, але й будь-які персональні дані суб'єкта.

Так, дії керівництва готелю та представників профспілки були ненавмисними, але в межах Регламенту відповідальність настає, як за умисні порушення, так і за вчинені з необережності. Зважаючи на це, а також на те, що дані, які були розголошені, включали основні ідентифікатори особи (а це, відповідно до статті 82 Регламенту – ім'я, прізвище чи адреса суб'єкта), уповноважений орган констатував порушення основоположних принципів GDPR і призначив штраф у розмірі 15 000 євро [49, с. 5].

Отже, принципи цілісності та конфіденційності позначають не лише технічну вимогу забезпечення безпеки, а й необхідність проведення організаційних заходів,

щоб усі працівники та керівництво компанії були ознайомлені із правилами поводження із персональними даними. В даному випадку керівництво готелю та представники профспілок публічно прочитали приватний лист, що містив персональні дані особи. Навіть той факт, що та його складова, що стосувалась особливостей медичного стану, тобто містила чутливі дані, була пропущена під час прочитання листа, не означає, що не відбулось неправомірного розкриття даних. Адже під час прочитання було вказано дані, що дають змогу точно ідентифікувати особу, як і дані, які стосувались її цькування на робочому місці. Як результат – уповноважений орган визнав ненавмисне, але значне порушення основоположних принципів цілісності та конфіденційності.

1.2.7. Принцип підзвітності

В статті 5 GDPR, поряд із частиною 1, де закріплені всі розкриті вище принципи, є також частина 2, яка закріплює принцип підзвітності. Його суть полягає у двох ключових елементах: відповідальності контролера за виконання всіх основоположних принципів GDPR і обов'язок мати змогу продемонструвати відповідність їм. Для реалізації підзвітності контролеру необхідно мати належну документацію або інші докази, за допомогою яких він зможе показати, як ним здійснюється реалізація всіх принципів захисту даних і які ним створено умови для реалізації суб'єктами даних своїх прав.

Контролер сам вирішує, що повинно бути зроблено, щоб принцип підзвітності вважався виконаним [50]. Для цього він має оцінити характер, обсяг, контекст і цілі обробки, врахувати ризики різної ймовірності щодо прав і свобод фізичних осіб тощо. Як роз'яснює з цього приводу ICO, «бути відповідальним за дотримання GDPR означає, що вам потрібно проявляти активність та організованість щодо свого підходу до захисту даних, тоді як демонструвати свою відповідність означає, що ви повинні бути в змозі довести кроки, які ви здійснюєте для відповідності» [50].

В межах цього принципу, перш за все, рекомендують прийняти та впровадити політику захисту даних, яка роз’яснює, як і яка інформація збирається і всі обставини її подальшої обробки [51]. Вона складається із частини, що надається для ознайомлення суб’єкту даних, до надання ним згоди, і частини, що призначена для внутрішнього використання. Остання – це офіційні внутрішні правила, що будуть обов’язковими для виконання працівниками, де буде вказано як потрібно здійснювати обробку, як відповідати на відповідні запити; інструкція, що робити працівникам, якщо ними виявлено несанкціонований доступ чи витік даних тощо [50].

Для більшості організацій цей документ є найбільшою складовою їх забезпечення та демонстрації дотримання. Обсяг та деталізація політики залежить від кількості даних, які обробляються, їх чутливості тощо. Але як належно звертає увагу ICO, важливо, що політика захисту даних повинна бути не лише прийнятою, а й ефективно впровадженою. Тому необхідним є здійснення певних заходів, що «можуть включати підвищення рівня обізнаності, навчання, моніторинг та аудит» [50].

Окрім цього, важливим є укладення письмових договорів з процесорами та ведення документації щодо діяльності з обробки. GDPR в статті 28 деталізує вимоги до договорів, зазначаючи, що в них обов’язково повинні бути положення про предмет, тривалість характер і призначення обробки даних; деталізовано тип персональних даних та категорії суб'єкта даних; а також закріплено зобов'язання та права контролера. Окрім цього, такі договори повинні встановлювати, що обробка відбувається лише за документально підтвердженими інструкціями контролера; мають деталізовувати та закріплювати відповідні заходи безпеки; використання субпроцесорів; права суб'єктів даних; надання допомоги контролеру; положення про закінчення контракту; встановлювати порядок ревізій та перевірок тощо.

Укладення письмових договорів є критично важливим для контролера, оскільки саме він несе основну відповідальність за загальну відповідність GDPR та

демонстрацію цієї відповідності. Процесор ж несе відповідальність тільки у випадках, коли він прямо діє за межами або всупереч вказівкам і домовленостям із контролером [50].

Для того, щоб реалізувати принцип підзвітності необхідне здійснення відповідних заходів безпеки, зокрема, призначення посадової особи із захисту даних. Така особа повинна бути відповідальною за облік та повідомлення суб'єкта чи уповноважений орган про порушення обробки [50]. Посадова особа із захисту даних також повинна організовувати і проводити оцінки впливу на захист даних з високим ризиком. Результати такої оцінки рекомендують також втілювати у матеріальній формі [50]. Якщо організація обробляє великий масив персональних даних, то функції посадової особи може виконувати окремий відділ.

Принцип підзвітності передбачає регулярний перегляд і актуалізацію відповідних документів, залежно від змін, що відбуваються як всередині підприємства, так і поза його межами (зміни, що стосуються рівня техніки, запровадження нових правил і принципів захисту даних тощо) [50].

Реалізація принципу підзвітності пов'язана також із впровадженням концепцій «privacy by design» та «privacy by default», які вимагають, щоб приватність була буквально вбудованою у всі процеси, що відбуваються на підприємстві, а також і у продукти, які виробляються підприємством [52, с. 5-6]. Дотримання цих концепцій забезпечує належний рівень взаємодії із суб'єктами при обробці їх даних. Privacy by design вже частково розкрито в межах реалізації принципу мінімізації даних. Однак, в аспекті реалізації підзвітності, це проявляється як необхідність організовувати діяльність всієї організації чи функціонал розроблюваного програмного додатку так, щоб підзвітність ставала майже автоматизованою. Це означає автоматичний запис кожного із рішень щодо персональних даних, разом із відомостями хто і коли його прийняв, невідкладне створення звітності протягом певного періоду тощо [52, с. 22-23]. Такі активні та превентивні дії будуть свідченням намірів контролера відповідати положенням

GDPR, що має значення у випадках, коли трапляється витік даних чи порушуються права суб'єкта даних. Адже саме в таких випадках контролеру потрібно довести, що ним здійснювались заходи, спрямовані на відвернення такої ситуації.

Отже, принцип підзвітності закріплює відповідальність контролера за виконання всіх основоположних принципів GDPR і можливість продемонструвати відповідність їм. Принцип підзвітності дає змогу контролеру самому визначати, які заходи і в якому обсязі мають бути ним здійснені, щоб дотримання GDPR можна було довести. Для цього йому потрібно оцінити обсяг даних, які він обробляє, їх чутливість, рівень можливого ризику у випадку порушення обробки для прав та свобод суб'єкта даних тощо. Як правило, в межах підзвітності організації основними заходами є розроблення політики даних, проведення навчання та моніторингу її виконання, укладення письмових договорів з процесорами, впровадження privacy by design та by default, а також призначення посадової особи із захисту даних.

1.3. Реалізація Загального регламенту про захист даних в Україні

Застосування норм GDPR в Україні можна розглядати в декількох напрямках: (i) його застосування компаніями в Україні, які є контролерами чи процесорами в розумінні Регламенту; (ii) добровільне запровадження політики GDPR-комплаєнсу компаніями в межах України, у яких немає зобов'язання його здійснення; (iii) законодавчі заходи державних органів, для приведення законодавства у відповідність до acquis ЄС.

Перші дві напрямки є взаємопов'язаними, однак кожен із них має свою специфіку. Так, перш за все, вимоги GDPR в Україні почали виконуватись тими компаніями, на яких такий обов'язок прямо покладається Регламентом. Тобто на момент початку застосування GDPR вони були контролерами або процесорами і підпадали під один із пунктів юрисдикції Регламенту. Прикладом такої компанії є

«Міжнародні авіалінії України», які є контролером в розумінні GDPR, що обробляє дані і тарґетує свої послуги, в тому числі, і на громадян країн ЄС, адже сайт компанії доступний англійською мовою, а оплата квитків можлива в євро і з території інших держав [53]. До цієї ж категорії належать компанії, що на момент початку застосування GDPR мали укладені договори із європейськими компаніями, в межах яких вони обробляли персональні дані як «процесори» в форматі сторонніх виконавців (outsourcing) тощо.

Другою категорією є компанії, які на момент набуття чинності, хоч і обробляли персональні дані, але не підпадали під юрисдикцію GDPR, і при цьому вирішили добровільно впровадити заходи, щоб відповідати вимогам Регламенту. Такі заходи здійснювались із різних причин: можлива подальша перспектива співпрацювати з компаніями в ЄС і стати контролером, або, частіше, процесором; бажання підвищити рівень соціальної орієнтованості та іміджу компанії; ціль досягнути високого рівня захисту персональних даних в загальноукраїнському масштабі, щоб уможливити активну співпрацю України із країнами ЄС та спростити процеси перевірки всіх українських компаній тощо. До цієї ж категорії можна віднести і міжнародні компанії, які не зобов'язані дотримуватись вимог GDPR щодо суб'єктів даних в Україні, однак добровільно поширюють на них такі ж стандарти, як і на користувачів ЄС. Такої політики, до прикладу, дотримується компанія Microsoft, що «у 2018 році […] була першою, що на добровільній основі розширила основні права на конфіденційність даних, включені до Генерального регламенту із захисту персональних даних (GDPR) Європейського Союзу, для клієнтів у всьому світі, а не тільки для користувачів у країнах ЄС» [54].

Однак, найбільш проблемним та неоднозначним наразі є третій аспект, якого стосується дія GDPR в Україні – це закріплення законодавцем положень для приведення у відповідність до європейської системи захисту. Загалом, історію законодавчого захисту персональних даних в Україні (окремо від захисту приватності) зазвичай висвітлюють з 2010 року, коли було ратифіковано Конвенцію

108. Разом із цим, 1 червня 2010 року було прийнято Закон України «Про захист персональних даних», написаний за зразком Директиви 95/46 [55]. Однак, наслідки прийняття цього закону не були успішними: були відсутні належні роз'яснення щодо механізмів його реалізації, і як результат – спеціально створений орган не зміг впоратись із непомірною кількістю «баз даних» поданих на реєстрацію, бо володільці баз даних зрозуміли це положення як обов'язок надіслати всі персональні дані, які ними оброблялись [56]. Згодом, норми Закону цілковито перестали ефективно реалізовуватись і у 2013 році механізм реєстрації всіх баз даних було відмінено, а наступного року і ліквідовано Державну службу України з питань захисту персональних даних [57].

Одночасно із ліквідацією спеціалізованого органу, повноваження щодо захисту персональних даних були покладені на Уповноваженого Верховної Ради України з прав людини [57]. Загалом, це відповідає європейським тенденціям, адже для забезпечення безсторонності та незалежності, захистом персональних даних не повинен займатись орган, що належить до системи виконавчої влади. Однак, сфера повноважень Уповноваженого Верховної Ради України з прав людини є надзвичайно широкою, а на практиці основними пріоритетами залишаються захист конституційних прав у місцях позбавлення волі (для відстеження і припинення катування та жорсткого поводження), захист прав дітей та захист прав осіб у сфері судочинства [58]. Через це, питанням захисту персональних даних не приділяється достатньої уваги, а їх «моніторинг» є формальним та поверхневим.

У червні 2014 року Україна підписала Угоду про асоціацію, в статті 15 якої вказано, що ми домовились співпрацювати з Європейським Союзом «з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи» [59]. На час підписання Угоди про асоціацію, тут ще не мався на увазі GDPR, однак наразі це зобов'язання включає у себе відповідність і його положенням. Так, 25 жовтня 2017 року Кабінет Міністрів України прийняв План

заходів з виконання Угоди про асоціацію, пункт 11 якого закріплює зобов'язання «удосконалення законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679» (тобто – з GDPR) [60]. Як результат – ми взяли на себе обов'язок імплементації положень GDPR в національне законодавство.

Під час прийняття Плану заходів з виконання Угоди про асоціацію, строк для прийняття відповідного законопроекту був встановлений на 25 травня 2018 року, однак він не був дотриманий [58]. У січні 2017 року розпочався проект Twinning «Посилення потенціалу інституції Українського омбудсмана», в межах якого розроблявся і проект внесення змін до Закону України «Про захист персональних даних», однак, розроблені зміни так і не були прийняті [61]. З урахуванням останніх змін у вищезгаданому Плані заходів, строк приведення національного законодавства у відповідність до GDPR було продовжено до 25 травня 2020 року [60]. Але станом на початок травня 2020 року будь-який законопроект, що пропонував би відповідні зміни, відсутній. Хоча офіс Ради Європи в Україні анонсував новий етап проекту Twinning, що наразі повинен займатись розробкою нового законопроекту для приведення законодавства у відповідність до європейських стандартів [62].

Новий законопроект є критично важливим для України, оскільки поточний текст Закону «Про захист персональних даних», що несистемно доповнювався частинами, взятими із нормативно-правових актів ЄС, належного захисту персональних даних не забезпечує.

По-перше, тому що вищезазначений Закон є надмірно фрагментарним і загальним, тобто він не містить детальних положень щодо реалізації закріплених прав та обов'язків. До прикладу, законодавством не передбачено можливість і порядок блокування на веб-сайтах чи видалення інформації, що порушує право на захист персональних даних. Також не передбачено конкретних механізмів реалізації прав суб'єкта даних, через що стаття 8 має декларативний характер [63, с.158, 162].

Недоліком є також відсутність положень, що стосувались би відносин між володільцем та розпорядником даних і закріплювали обов'язки цих суб'єктів та вимоги до договору між ними, аналогічно до положень GDPR [63, с. 164].

По-друге, в Законі «Про захист персональних даних» відсутня єдність термінології та узгодженість норм. Як приклад, не розмежовуються такі категорії як «персональні дані» та «конфіденційна інформація», хоча обидва терміни використовуються в тексті. Також відсутні визначення понять доступу до даних та передачі, розкриття, поширення, оприлюднення персональних даних з визначенням суб'єктів, яких стосуються ці терміни [63, с. 163]. Неузгоджені повною мірою між собою і з європейськими нормативно-правовими актами положення статті 7 та 11 Закону «Про захист персональних даних», які передбачають підстави для обробки чутливих даних і загальні підстави для обробки, відповідно [63, с. 159-160].

Окремим питанням є законодавчі положення щодо відповідальності за порушення законодавства про захист персональних даних. Так, законодавством передбачені положення щодо адміністративної та кримінальної відповідальності за порушення норм про захист персональних даних. Мається на увазі стаття 188-39 Кодексу України про адміністративні правопорушення «Порушення законодавства у сфері захисту персональних даних» і стаття 182 Кримінального кодексу «Порушення недоторканості приватного життя» [64; 65].

Оскільки норма Кримінального кодексу стосується лише незаконної обробки конфіденційної інформації, то найчастіше застосовуватись за неправомірну обробку персональних даних загалом мала б адміністративна відповідальність. Однак, стаття 188-39 Кодексу України про адміністративні правопорушення залишається неефективною.

Частини 1-3 аналізованої статті передбачають порушення порядку повідомлення Уповноваженого Верховної Ради України з прав людини і невиконання його приписів, тому відповідальність за цими нормами напряму залежить від ефективності діяльності Уповноваженого, яка, як вже зазначалось, не

є такою. Щодо частин 4 і 5, то вони передбачають відповідальність за недодержання встановленого порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних. Однак, категорія «порядок захисту» персональних даних не визначена законодавством однозначно, як і не конкретизовано і її співвідношення із «порядком обробки» персональних даних. Виникає питання, порушення яких саме положень Закону «Про захист персональних даних» становитиме склад цього правопорушення [63, с. 142].

Ще одним суттєвим недоліком є використання терміну «незаконний доступ до даних», оскільки в Законі «Про захист персональних даних» розмежовуються поняття «доступу до даних» і «поширення/передачі персональних даних». І категорія «доступ» охоплює лише випадки надання відповіді на запит, тоді як поширення даних без попереднього запиту вже не охоплюється поняттям доступу, а отже – і не становитиме порушення статті 188-39 Кодексу України про адміністративні правопорушення [63, с.142].

Також набагато доцільніше виділяти порушення прав суб'єкта даних в склад окремого правопорушення, а не встановлювати його як наслідок недодержання встановленого порядку захисту, оскільки це суттєво обмежує можливість настання відповідальності за недотримання прав суб'єкта даних, що посилює їх декларативність [63, с. 143]. Тобто, для настання відповідальності за порушення частини 4 і 5 статті 188-39 Кодексу України про адміністративні правопорушення, представники Національної поліції повинні мати достатню компетенцію, щоб належно скласти протокол, а потім надати суду докази, що підтверджували б порушення порядку захисту персональних даних і причиново-наслідковий зв'язок із незаконним доступом до персональних даних або із порушенням прав суб'єкта даних. І додатково до цього – поліція також має і ідентифікувати конкретну особу, внаслідок дій якої відбулось описане порушення, оскільки можливість накласти штраф на юридичну особу нормами Кодексу України про адміністративні правопорушення не передбачена. Такий ускладнений механізм робить норми

частин 4 та 5 статті 188-39 навіть менш ефективними ніж відповідальність за порушення приписів Уповноваженого. У поєднанні із низькими розмірами передбачених статтею штрафів (від 1700 до 34000 гривень) це призводить до практичної відсутності юридичної відповідальності за порушення законодавства про захист персональних даних в Україні.

Описані та інші наявні недоліки законодавства про захист персональних даних часто мають спільну рису – це необхідність деталізації і конкретизації законодавчих вимог. З іншого боку – норми самого GDPR є досить загальними та за винятком окремих сфер, таких як захист персональних даних неповнолітніх чи чутливих даних, вони сформульовані як стандарти, а не як правила (тобто описують, що потрібно досягнути, а не як це зробити). Однак, ефективність стандартів можлива лише в країнах з високим рівнем правової культури населення, і для яких такі формулювання норм є звичними. Навіть в країнах ЄС видаються роз'яснення положень Регламенту, хоч і рекомендаційного характеру (до прикладу, такі як Рекомендації ICO).

В Україні ж, де панує правовий нігілізм, потрібен підхід, за яким в законодавстві основну частину складатимуть, все-таки, правила, а не стандарти, і де роз'яснення будуть частиною зобов'язального нормативно-правового акту. Саме тому для створення ефективної системи захисту, недостатньо навіть перенести текст норм GDPR в Закон «Про захист персональних даних», необхідно також закріпити на рівні законодавства і відповідні роз'яснення, рекомендовані заходи та конкретні механізми реалізації положень закону. Так, до прикладу, Закон «Про захист персональних даних» наразі досить деталізовано визначає поняття «згоди суб'єкта персональних даних», зазначаючи, що це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. Здавалося б, таке положення встановлює достатню кількість вимог щодо отримання

такої згоди: добровільність, активний характер дії (волевиявлення), поінформованість, обмеженість метою обробки, дотримання форми. Однак, на практиці в Україні отримання згоди в переважній більшості випадків все одно не відповідає вимогам GDPR. Тому дослідники часто пропонують доповнити визначення згоди, до прикладу, вказавши, що ««поінформованість» передбачає виконання володільцем персональних даних положень статті 12 Закону [оскільки] це явно не визначено у Законі» [63, с. 160]. Тобто, щоб забезпечити належне виконання відповідних норм в Україні, є потреба в деталізації та конкретизації кожного із закріплених положень.

Як буде продемонстровано надалі в цій роботі, в Україні необхідним кроком є також внесення відповідних змін у законодавство щодо свободи слова для забезпечення її додаткового захисту і балансу із захистом персональних даних; щодо розслідувань корупційних правопорушень, щоб захист персональних даних не ставав інструментом перешкоджання таким розслідуванням; а також розглянути можливість зниження вимог, диференціації чи пільгових умов щодо захисту персональних даних для зменшення тиску на малий та середній бізнес. Тільки за умови врахування цих та інших національних особливостей, Закон «Про захист персональних даних» буде дієвим та відповідатиме запитам суспільства.

Отже, серед причин неефективності системи захисту персональних даних в Україні можна виділити чотири причини, що взаємодоповнюють одна одну: (i) неможливість Уповноваженого з прав людини приділяти належну увагу питанням захисту персональних даних через надмірний обсяг зон відповідальності; (ii) неналежна якість тексту Закону і його адаптації до українських реалій; (iii) відсутність ефективної юридичної відповідальності за порушення наявного законодавства про захист персональних даних; (iv) недостатній рівень правової культури населення в сфері захисту персональних даних і необізнаність із цією проблематикою. І ці проблеми необхідно вирішити в процесі імплементації норм GDPR в Україні.

***

Висновки до розділу 1

GDPR став відображенням нагальної проблеми захисту персональних даних в епоху розвитку технологій. За допомогою нього в межах Європейського Союзу вдалось створити ефективну систему захисту суб'єктів даних. Його пряма дія на території всіх держав ЄС уніфікувала стандарти щодо обробки даних, а екстериторіальність розширила межі застосування GDPR на більшість розвинених держав світу, що тарґетують свої послуги на Європейський Союз. Завдяки своїх актуальності, положення GDPR також вплинули на законодавство інших держав, яке почало змінюватись, щоб відповідати тенденціям ЄС.

Стаття 5 GDPR закріплює 8 основоположних принципів: правомірності, справедливості та прозорості обробки, обмеженості ціллю, мінімізації даних, точності, обмеження зберігання, цілісності та конфіденційності та підзвітності. Вони об'єднують ряд вимог до контролера та процесора, що обробляють дані.

Правомірність, справедливість та прозорість обробки закріплені як один принцип. Правомірність буде дотриманою, якщо для обробки буде наявна одна із підстав, що встановлені Регламентом і, окрім цього, не буде здійснюватися інших неправомірних дій у відносинах щодо обробки даних. Справедливість означає, що дані оброблятимуть так, як цього розумно очікує суб'єкт даних. Прозорість є новелою GDPR і закріплює ряд вимог щодо чіткого та зрозумілого інформування суб'єкта даних про обробку і всі її обставини та щодо доступності суб'єкта даних до обробки. Самостійне визначення необхідних дій в межах кожного із принципів є одним із обов'язків контролера. Тому для їх розкриття потрібен аналіз практики уповноважених органів щодо констатованих порушень. Одним з найвідоміших є рішення щодо компанії Google, де визначено умови дотримання прозорості та дійсності згоди (для дотримання правомірності) на обробку персональних даних.

Принцип обмеженості ціллю означає, що до збору даних контролер має чітко і однозначно визначити для яких цілей здійснюватиметься обробка. Цілі потрібно довести до відома суб'єкта даних до надання ним згоди і якщо вони змінюються – треба запитувати нову згоду.

Принцип мінімізації даних вимагає обробляти лише ті дані, які необхідні для досягнення цілей обробки. Порушенням є обробка даних, які не стосуються цілей, так само як і релевантних даних, але в більшому обсязі, ніж це необхідно.

Точність означає, що контролер має пересвідчитись, що оброблювані дані є точними, і, у разі необхідності, оновити їх. Неточними є дані, які суперечать фактам, або ті, які через неповноту вводять в оману. Збереження неточних даних для певних цілей має бути чітко визначеним як таке.

Принцип обмеження зберігання вимагає, щоб дані, які вже не є необхідними для досягнення цілей обробки, повинні були видалені або повністю анонімізовані, тобто не давати змогу ідентифікувати суб'єкта даних. Щодо цієї справи показовою є справа Deutsche Wohnen SE, яка проводила поширену практику «кладовища даних».

В межах цілісності та конфіденційності закріплюється ряд вимог до безпеки даних і до баз, в яких відбувається обробка. Основна мета – це захист даних від несанкціонованого доступу чи витоку даних. Важливою для розуміння цього принципу є справа Gesthotel Activos Balagares, оскільки вона демонструє, настільки важливою, окрім забезпечення технічної безпеки, є організаційна складова конфіденційності.

Принцип підзвітності закріплений в другій частині статті 5 Регламенту і є, гарантом реалізації всіх інших принципів. В межах підзвітності на контролера покладається обов'язки виконання всіх принципів і спроможності продемонструвати дотримання. Рішення, які саме заходи для цього запроваджувати – залишається на розсуд контролера, однак вони мають бути необхідними і достатніми, зважаючи на всі обставини обробки.

Імплементація стандартів, включно із тими, що містяться в основоположних принципах GDPR, є обов’язком, який взяла на себе Україна в межах асоціації із ЄС. Однак, строки для його виконання вже минули, а наявна система захисту персональних даних залишається недієвою. Перед законодавцем стоять завдання створення якісного тексту закону, вдосконалення механізмів відповідальності за його порушення, вирішення проблеми перенавантаження Уповноваженого з прав людини, на якого покладено обов’язки з нагляду у цій сфері, і загальне підвищення правової культури і обізнаності населення щодо захисту персональних даних.

РОЗДІЛ 2
ПРОБЛЕМИ ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ ПРИНЦИПІВ GDPR В МЕЖАХ ОКРЕМИХ ПРАВ СУБ'ЄКТА ДАНИХ

2.1 Основоположні принципи і право на забуття

2.1.1 Проблеми реалізації права на забуття

Під час свого прийняття GDPR став об'єктом активних дискусій та обговорень. Чимало його новел зазнавали критики науковців та практиків як в Європейському Союзі, як і за його межами. Одним із таких положень, що критикували чи не найчастіше є так зване «право на забуття». Це право суб'єкта ретроактивно вилучати свої дані, які обробляються [66]. Стаття 17 GDPR визначає умови реалізації цього права. Так, вказується, що суб'єкт даних має право на стирання контролером персональних даних щодо нього у випадку існування конкретних підстав.

Першою із таких підстав для видалення даних є зникнення необхідності обробляти дані для цілей обробки. Ця підстава прямо перекликається із основоположними принципами обмеженості ціллю, мінімізації даних та обмеження зберігання. Тобто в межах цієї підстави Регламент ще раз підкреслює необхідність видаляти дані, коли вони перестають бути необхідними для досягнення заявлених цілей обробки.

Наступною підставою для «забуття» суб'єкта даних є відкликання ним своєї згоди на обробку. Як розглядалось в межах принципу правомірності, надання суб'єктом згоди є підставою для обробки його персональних даних, однак Регламент також закріплює можливість безумовно відкликати таку згоду. Сам процес відкликання згоди має не порушувати принципу прозорості, тобто бути

доступним, чітким, зрозумілим. ICO неодноразово наголошує на важливості цього права, підкреслюючи, що його реалізація не має бути ускладненою [11]. Продовжувати обробку у випадку відкликання згоди можна лише якщо у суб'єкта з'явилась інша підстава для правомірної обробки або його нова ціль сумісна із попередньою [21].

Також контролер та процесор зобов'язані видалити всі дані про особу у випадках, коли вона заперечує проти обробки. Таке заперечення має відбуватись відповідно до положень статті 21 GDPR. У цій статті вказано, що суб'єкт даних може в будь-який час заперечувати проти обробки, що ґрунтується на таких двох підставах правомірності як необхідність виконання завдання в інтересах суспільства або здійснення офіційних повноважень контролера і необхідність для цілей законних інтересів контролера або третьої сторони. Якщо суб'єкт заперечує проти обробки в цих випадках і якщо немає вагоміших підстав для подальшої обробки, то має бути реалізоване і право на забуття. Частина 2 статті 21 також закріплює право на заперечення обробки у випадках, коли дані обробляються для чітких маркетингових цілей. В такій ситуації право на забуття спрацьовує автоматично і не оцінюється наявність вагомих підстав для подальшої обробки.

Іще однією підставою для реалізації права на стирання даних є неправомірність обробки даних. Текст GDPR прямо не відсилає до статті 5, однак в даному випадку мається на увазі порушення правомірності як основоположного принципу. У зв'язку із цим виникає питання обсягу і меж принципу правомірності – розуміти його у вузькому значенні, тобто в межах наявності відповідних підстав правомірності; чи все таки вдаватись до розширюваного тлумачення і включати туди ще і будь-які неправомірні дії щодо персональних даних. Це питання залишається відкритим, що, безумовно, може зашкодити юридичній визначеності положень щодо права на забуття.

GDPR закріплює ще два випадки, коли суб'єкт даних має право на забуття – коли таке видалення потрібне для того, щоб відповідати нормативно-правовим

актам ЄС або держав-членів, під дію яких підпадає контролер; або коли суб'єктом є дитина, а самі дані були зібрані для пропозиції послуг інформаційного суспільства.

Відповідно до статті 17 Регламенту, особа може вимагати видалення своїх персональних даних від кожного контролера, який їх обробляє (і їх процесорів), а не лише від того, хто в першу чергу їх обробив. Тобто зобов'язання про стирання виникає у всіх, хто обробляє дані, як тільки особа відкликає згоду надану первинному контролеру. Відповідно у первинного контролера виникає обов'язок знати всіх інших, хто також обробляє надані дані і, більше того, забезпечити технічні заходи, які дозволяли б відслідковувати особисту інформацію та доводити її реальне видалення у випадку отримання запиту на стирання. І якщо частину відслідковування можливо виконати, запровадивши концепт privacy by design, належним чином зберігаючи та реєструючи будь-яку передачу даних та зберігаючи зв'язки скопійованої інформації тощо, то доведення повного видалення даних залишається проблематичним [67]. До прикладу, ретельна перевірка часто використовуваних великими корпораціями EDL (enterprise data lake), що використовують сервери Hadoop для зберігання даних, показала, що вся система Hadoop створена таким чином, що файли з неї видалити неможливо, вони лише позначаються як неактивні [67]. І чимало інших платформ також мають схожий функціонал, тому для них повне видалення даних може бути проблематичним.

Окрім технічних складнощів під час реалізації, право на забуття часто критикують через його можливі ризики для свободи слова чи діяльності журналістів. Часто право на забуття навіть називають «найбільшою загрозою для свободи слова та вираження поглядів в Інтернеті» [68]. Таку оцінку надають через широкі межі застосування права на забуття, яке стосується будь-яких персональних даних особи і всіх обробників таких даних. Як підкреслюють дослідники, претензії щодо захисту даних можуть бути зручним інструментом для управління репутацією: адже на відміну від претензій про наклеп, у них немає обмеження в

часі, немає необхідності демонструвати серйозну шкоду чи можливості захисту матеріалу як власної думки автора [69].

Стаття 85 GDPR підкреслює важливість забезпечення пропорційності між правами, які стосуються захисту персональних даних з правом на свободу вираження поглядів та інформації, включаючи обробку для журналістських цілей та цілей академічного, художнього чи літературного вираження. Однак, як вказано у цій же ж статті 85, завдання такого збалансування покладається, в першу чергу, на державу. Саме в межах національного законодавства повинен бути прийнятий нормативно-правовий акт, що передбачає так звані «журналістські винятки» [70]. Це створює можливість для двох ризиків: перш за все, ризик нерівномірного захисту прав журналістів та свободи слова у різних державах в межах ЄС, а по друге, ймовірність того, що національне законодавства взагалі не буде прийняте чи ніяк не захищатиме свободу слова.

Так, дослідження, що були проведені на кінець 2018 року, після початку застосування GDPR показали, що формулювання і прийняття журналістських винятків, зі справжнім потенціалом захисту свободи слова, значно відставало від Регламенту [70]. Як вказують дослідники, фактично через два з половиною роки після того як GDPR був прийнятий «лише шістнадцять із двадцяти восьми держав-членів прийняли законодавство щодо звільнення журналістів [від дії деяких положень Регламенту], і якість цих положень сильно відрізняється, що спричиняє непослідовність правового ландшафту захисту свободи вираження поглядів» в межах ЄС [70].

Аналізуючи вже прийняте законодавство, що містить журналістські винятки, можна зробити висновок, що можливість захисту свободи вираження поглядів перебуває у значність залежності від того, чи застосовуватимуть їх національні органи відповідно до чинних стандартів міжнародного права. До прикладу вказують, що Закон про захист даних Словацької Республіки може бути проблематичним, оскільки він побудований за принципом «виняток із винятку»,

тобто вказує, що «персональні дані можуть оброблятись для журналістських цілей без згоди суб'єкта даних, за винятком випадків, коли це може порушити захист його особистості чи приватності» [70]. Таке формулювання може унеможливити, до прикладу, можливість використовувати персональні дані під час корупційного розслідування. В свою чергу, закон про захист даних в Іспанії взагалі не деталізує умови узгодження журналістської діяльності і свободи вираження поглядів, а лише в загальному висловлює та констатує у преамбулі та в одному із положень, що кожен має право на свободу вираження поглядів в Інтернеті [70].

Очевидно, що такий підхід не можна назвати збалансованим, оскільки залишається багато можливостей для утисків журналістів під егідою захисту персональних даних. Одним із прикладів використання GDPR проти свободи слова є випадок організації RISE Project. Це некомерційна журналістська організація в Румунії, що займається розслідуваннями корупційних правопорушень. Після публікації ними чергового розслідування корупційного скандалу за участю відомого місцевого політика, національний уповноважений орган захисту даних намагався змусити власників розкрити джерела своїх даних. І хоча Європейська Комісія зробила відповідні попередження, можливості такої практики залишаються [70].

GDPR передбачає великі штрафні санкції, а його застосування є значно швидшим, ніж звернення до ЄСПЛ за захистом свободи слова, що наразі залишається головним способом захисту цього права. Саме тому держави ЄС повинні звернути особливу увагу на подальше збалансування цих прав, щоб і правом на забуття не можна було зловживати.

Дослідники, що вказують на непропорційність абсолютного підходу до права на забуття, пропонують використовувати альтернативний підхід [67]. Замість того, щоб гарантувати абсолютне забуття і видалення даних, це право може базуватись на ускладненні рівня кодування чи пошуку інформації. Така позиція іноді критикується як цензура пошуку інформації, яка є «найменш серйозним, але і

найефективнішим засобом для забезпечення існування […] цензури» [67]. Але в цілому вона перекликається із рішенням Суду ЄС щодо права на забуття, а також із ідеєю пункту 65 Преамбули GDPR, де вказано, що суб'єкт даних повинен мати право на забуття, однак подальше зберігання даних має бути правомірним там, де це необхідно для здійснення права на свободу вираження поглядів та інформації.

Отже, право на забуття закріплюється в статті 17 GDPR і є проявом декількох основоположних принципів, зокрема правомірності, обмеженості ціллю, мінімізації даних і обмеження зберігання. Право суб'єкта даних на стирання даних або є умовою виконання якихось із цих принципів, або навпаки є наслідком невиконання.

Однак, практична реалізація цього права залишається проблематичною. Більшість вже наявних баз даних потрібно докорінно змінювати, щоб зробити можливим видалення; вже зібрані персональні дані могли до часу прийняття Регламенту не відстежуватись, що ускладнює їх видалення в усіх вторинних контролерів і їх процесорів, неможливість перевірення остаточності та повноти видалення даних тощо.

Крім цього, непропорційним є і співвідношення права на забуття із журналістською діяльністю та свободою слова. Багато держав не встановили у національному законодавстві «журналістські винятки», а деякі з тих, хто закріпили – зробили це занадто нечітко, тому GDPR і право на забуття може використовуватись як інструмент боротьби із журналістськими розслідуваннями в деяких державах. Через загрози та неоднозначності пропонується звужувати широке застосування права на забуття, щоб пропорційність і баланс між цим правом та вільним висловленням поглядів був дотриманий. Для цього можливо використовувати ускладнення пошуку інформації при збереженні правомірності її зберігання.

2.1.2 Рішення Європейського Суду справедливості щодо права на забуття

Рішення Google Spain SL v. Agencia Española de Protección de Dato (Spain). Одне із найперших рішень Суду ЄС, що має базовий характер для розуміння права на забуття, закріпленого в GDPR, було прийнято ще за дії попередньої Директиви. Стаття 12 Директиви, що розкривала право доступу, закріплювала положення про право на виправлення, стирання або блокування персональних даних, обробка яких не відповідає положенням Директиви, зокрема через неповний або неточний характер даних [71, п. 60]. Тобто це було базою для створення права на забуття в такій формі, як вона відома зараз у GDPR, як окреме право.

5 березня 2010 року громадянин Іспанії Маріо Костеха Гонсалес звернувся до уповноваженого органу щодо захисту даних в Іспанії – AEDP, зі скаргою на місцеве новинне видання La Vanguardia Ediciones SL та Google. Скарга була подана через те, що при введенні імені заявника пошукова система надавала посилання на дві сторінки La Vanguardia, датовані 1998 роком, де зазначалось про участь заявника у аукціоні нерухомості, пов'язаного з процедурами примусового стягнення боргів із соціального страхування. Заявник просив газету видалити або змінити відповідні статті, а Google не надавати відповідні посилання під час пошуку, оскільки ці провадження були давно врегульовані, а тому – не є релевантними [71, п. 14-15].

Рішенням від 30 липня 2010 року AEDP відхилила позов в частині претензій до газети, оскільки публікація нею відповідної інформації була правомірною і необхідною, так як це відбувалось за наказом відповідного міністерства для забезпечення достатньої кількості учасників торгів. Однак щодо пошукової системи, то уповноважений орган підтримав скаргу, зазначивши, що оператори пошукових систем є суб’єктами, що підпадають під дію відповідного законодавства про захист персональних даних, адже вони «виконують посередницьку функцію в сучасному інформаційному суспільстві» [71, п. 17]. Саме тому уповноважені органи можуть приймати відповідні рішення щодо таких суб’єктів як Google про ненадання посилань під час пошуку, при цьому не зобов’язуючи видаляти саму інформацію [71, п. 17].

Google звернувся до Національного вищого суду (Audiencia Nacional) з метою оскаржити дане рішення. Національний вищий суд в свою чергу вирішив, що це питання потребує тлумачення положень Директиви, з урахуванням розвитку технологій, що відбулись за час її чинності, тому звернувся до Суду ЄС [71, п. 20].

Упускаючи процесуальні моменти, зокрема щодо територіальної підсудності, і звертаючись до змісту звернення до Суду ЄС, перед ним були поставлені такі запитання: (i) чи діяльність Google з пошуку інформації, опублікованої чи включеної в мережу третьою стороною, її автоматичної індексації, та тимчасового зберігання і надання в доступ користувачам є обробкою даних в розумінні Директиви 95/46; (ii) якщо так, то чи є Google контролером персональних даних з веб-сторінок, які він індексує (iii) чи може AEDP, з метою захисту прав, накладати вимогу про відкликання з індексів певної частини інформації, не звертаючись при цьому до власника веб-сторінки, навіть якщо інформація опублікована правомірно; і насамкінець (iv) чи слід вважати, що права на видалення та блокування даних, передбачені Директивою 95/46, поширюються на можливість суб'єкта даних звертатися до пошукових систем, висловлюючи своє бажання, щоб його персональні дані не надавались під час пошуку користувачам, якщо він вважає, що це може завдати йому шкоди, навіть якщо відповідна інформація була опублікована правомірно [71, п. 20].

З приводу поставлених запитань Суд ЄС вказав, що незважаючи на те, що Google не змінює персональні дані, його діяльність щодо них все одно варто вважати обробкою, більше того – він сам визначає цілі і засоби такої обробки, а отже є і контролером, в розумінні законодавства про захист персональних даних. Обмеження дії Директиви на таку діяльність означало б компрометування ефективності і повноти системи захисту відповідних прав та свобод фізичних осіб [71, п. 32-38].

Що ж до обов’язку оператора вилучати певні посилання під час пошукового запиту, то Суд підкреслює, що саме пошукові системи дають можливість

безперешкодного доступу до багатьох аспектів приватного життя людини, пов’язуючи інформацію, яку без них проблематично було б пов’язати. Зважаючи на це, а також на доступність Інтернету, діяльність операторів пошукових систем, що є втручанням у права суб'єкта даних, не може бути виправдана лише економічними інтересами. У деяких конкретних випадках вона може бути збалансована лише публічним інтересом, однак оцінку пропорційності в таких випадках треба проводити в кожному конкретному випадку [71, п. 99].

Зважаючи на все вищезазначене Суд встановив, що для того щоб не допускати порушення права на захист персональних даних та права на приватність, оператор пошукової системи зобов'язаний вилучити зі списку результатів, що відображаються під часу пошуку, посилання на веб-сторінки, опубліковані третіми особами, які містять персональні дані, навіть якщо публікація є правомірною і якщо вона не видаляється із самого веб-сайту [71].

Рішення Google LLC v. Commission nationale de l'informatique et des libertés (France). 24 вересня 2019 року Велика палата Суду ЄС винесла ще одне рішення за позовом Google, на цей раз – до Національної комісії з захисту даних, що є уповноваженим органом з питань захисту персональних даних у Франції. Як і у попередній справі, позов стосувався тлумачення положень Директиви 95/46, що була ще чинною на час прийняття відповідачем оскаржуваного заявником рішення, однак Суд ЄС здійснює тлумачення також і стосовно GDPR, який вже підлягав застосуванню на час винесення рішення [72, п. 40].

У даній справі від 21 травня 2015 року CNIL виніс рішення, в якому зобов’язав Google під час пошуку даних, що є об’єктом права на забуття і мають бути видалені, не надавати відповідних посилань на всіх доменних іменах своєї пошукової системи, тобто по всьому світу [72, п. 30]. Google відмовився виконувати це рішення, застосувавши обмеження лише на доменних іменах країн ЄС. Окрім того, компанія обмежила можливість знайти такі результати просто скориставшись пошуковим сервісом з доменним іменем іншої країни, поза межами ЄС. Тобто було

здійснене так зване «геоблокування» і користувачі з відповідними з IP-адресами бачили під час пошуку лише обмежені результати, незалежно від того, версію пошукової системи якої країни вони використовували [72, п. 31-32].

За невиконання рішення 10 березня 2016 року Національна комісія з захисту даних наклала штраф в розмірі 100 000 євро, тому Google вирішив звернутись до Державної ради Франції (Conseil d'État) для скасування такого рішення [72, п. 33].

Державна рада зазначила, що пошукова система Google «розбита на різні доменні імена за географічними розширеннями з метою адаптації результатів, зокрема, до мовних особливостей різних держав, в яких ця компанія здійснює свою діяльність. Якщо пошук ведеться з «google.com», Google автоматично перенаправляє цей пошук до доменного імені відповідної держави, в якій цей пошук вважається здійсненим, через ідентифікацію IP-адреси користувача». Однак, все ж таки, незалежно від того, де знаходиться особа, вона має можливість здійснити пошук за допомогою інших доменних імен пошукової системи, наприклад змінивши свою IP-адресу [72, п. 36].

На основі цього Державна рада зробила висновок, що «через те, що всі доменні імена Google можуть бути доступні з французької території, а також через наявність шлюзів між цими різними доменними іменами [та через деякі інші технічні ознаки], обробку в різних системах з різними доменними іменами слід розцінювати як єдиний акт обробки персональних даних для цілей застосування їх відповідного національного закону». Тому дані повинні бути видалені з усіх пошукових систем [72, п. 37].

Google заперечив таке рішення Державної ради, стверджуючи, що воно ґрунтується на помилковому тлумаченні положень національного законодавства. Компанія стверджує, що право на вилучення посилань, в тій формі як воно було визнане Судом ЄС у рішенні щодо Google Іспанія, не обов'язково вимагає видалення спірних посилань без географічних обмежень з усіх доменних імен його пошукової системи. Крім того таке тлумачення є нехтуванням принципами

ввічливості та невтручання, визнаними міжнародним публічним правом, і непропорційно шкодить свободам вираження поглядів, інформації, спілкування та преси [72, п. 38].

Державна рада вирішила, що такі аргументи піднімають складні питання щодо тлумачення Директиви 95/46, тому вирішила припинити розгляд справи та направити ці проблеми на розгляд Суду ЄС [72, п. 39].

Тобто перед Судом ЄС було поставлено такі три основні питання: (i) чи означає «право на вилучення посилань» (в тій формі, як воно було визнане у його рішеннях Судом ЄС) те, що оператор пошукової системи при наданні відповідного запиту зобов'язаний вилучити відповідні посилання, незалежно від місця, звідки ініційований пошук, тобто навіть якщо він здійснюється з місця, що виходить за межі територіальної сфери Директиви; (ii) (2) якщо ні, то оператор пошукової системи, при наданні запиту на вилучення посилань, повинен видаляти спірні посилання лише з пошукових систем з доменними іменами відповідної держави чи зі всіх доменних імен держав-членів ЄС; (iii) чи слід оператору пошукової системи також застосовувати методику «геоблокування» для тих пошукових запитів з IP-адрес, що вважаються розташованими в державі, де прийнято рішення про видалення посилань, чи в одній із держав-членів, на які поширюється Директива, незалежно від доменного імені, що використовується [72, п. 39].

Відповідаючи на задані питання Суд ЄС проаналізував їх як стосовно Директиви, що була чинною на час винесення рішення проти Google, так і стосовно GDPR. У рішенні підкреслено, що ціль Директиви та Регламенту – це гарантувати високий рівень захисту персональних даних у всьому Європейському Союзі. І, звісно, видалення посилань у всіх версіях пошукової системи в повній мірі відповідатиме цій цілі. Однак, право на захист персональних даних не є абсолютним правом і повинно розглядатися у зв'язку з його функцією в суспільстві та бути збалансованим з іншими основними правами, відповідно до принципу пропорційності [72, п. 55, 60].

Більше того, рівень захисту персональних даних відрізняється в різних державах світу і Суд ЄС вважає, що з положень Директиви чи GDPR не вбачається, що у нормотворця був намір тут розширити сферу дії прав, що захищаються цими актами, поза межі дії ЄС [72, п. 62]. Тут варто розмежувати екстратериторіальну дію Регламенту, про яку згадувалось на початку цієї роботи з даним висновком суду. В розширенні дії GDPR за межі Європейського Союзу прослідковується чітка мета – захист осіб, що проживають чи перебувають в ЄС від неправомірної обробки їх даних суб'єктами, що знаходяться поза межами ЄС. При цьому, це не означає наміру поширювати такий же ж рівень захисту права на захист персональних даних на такі держави, а лише є проявом високого ступеня захисту власних громадян та осіб, що перебувають на їх території. Не розширюються за межі Союзу і можливості уповноважених органів, які можуть спільно прийняти рішення у кількох державах в межах співпраці [72 п. 63].

Зважаючи на такі аргументи, таких операторів як Google не можна зобов'язати видалити посилання у пошукових системах поза межами ЄС. Більше того, навіть у межах ЄС необхідним є певне узгодження такого рішення між уповноваженими органами держав. Адже це питання стосується співвідношення права на захист персональних даних та інших прав, таких як право на свободу слова та інформації. А як вже зазначалось під час аналізу практичних проблем реалізації права на забуття – вирішення цього питання GDPR частково покладає на держави-члени. Саме тому, Суд підкреслює, що до того як винести рішення, яке зобов'язуватиме видалення посилань на території ЄС уповноважений орган повинен провести консультації та роз'яснення із уповноваженими органами інших держав, окрім випадків, де потрібен негайний захист прав і свобод особи. Якщо все таки рішення про видалення посилань було прийнято, оператор повинен вжити належних заходів, що унеможливлять або належно ускладнюватимуть доступ до таких даних з території ЄС [72, п. 67-70].

Отже, Суд ЄС виніс рішення, які сформували основу права на забуття. Саме завдяки рішенню Google v. Spain право на забуття було закріплене як відокремлене в GDPR і саме в такій формі. Такі рішення є вирішенням окремих проблем розуміння та реалізації права на забуття, однак вони стосуються лише окремих його аспектів. Тоді як проблематика права на забуття є дещо глибшою і не може бути обмежена лише зобов'язаннями операторів пошукових систем. Адже їх дія поширюється на всіх суб'єктів, що обробляють дані, тому встановлення балансу і пропорційності залишаються актуальними завданнями у цій сфері.

2.2. Основоположні принципи і доступ до персональних даних

2.2.1. Право на доступ до даних: межі та можливі загрози

Право на доступ є одним із базових для суб'єкта даних, оскільки уможливлює реалізацію інших прав, таких як право на виправлення (що є одним із проявів здійснення принципу точності) чи видалення даних. Доступ осіб до даних також дає їм змогу перевірити обробку після того, як вона вже розпочалась [73].

Також саме право на доступ до персональних даних відіграє ключову роль у виконанні принципу прозорості, оскільки вона означає, що контролери зобов'язані, серед іншого, максимально інформувати особу про деталі обробки і про дані, які обробляються. Основоположний характер цього права підкреслюється його закріпленням в статті 8 Хартії основних прав ЄС, у межах роз'яснення права на захист персональних даних [74].

Зміст права на доступ розкривається в статті 15 GDPR, де вказано, що суб'єкт даних має право отримати від контролера підтвердження того, чи обробляються його персональні дані і, якщо так, то отримати доступ до таких даних та необхідної інформації щодо них. Так, у статті 15 вказано, що у випадку отримання запиту в межах права на доступ, контролер має повідомити також які цілі обробки; до яких

категорій належать дані, що обробляються; яким третім особам були або будуть розкриті дані; протягом якого періоду зберігатимуться дані (або які критерії для визначення такого періоду); а також інформацію щодо автоматизованого прийняття рішень, включаючи профілювання (зокрема, про логіку, значення та передбачені наслідки такої обробки для суб'єкта даних). На контролера також покладається обов’язок проінформувати суб’єкта щодо його базових прав, які стосуються даних, таких як право на виправлення, стирання, оскарження до уповноваженого органу тощо. Якщо особисті дані збирались не від суб'єкта, треба надати всю наявну інформацію щодо їх джерела.

На практиці доступ до даних надається або в електронній формі або в паперовій, іноді – за допомогою телефонного зв’язку, хоча це не рекомендується задля уникнення складнощів підзвітності. Письмові запити подаються, відповідно, через веб-форми, листи на електронну скриньку або у формі звичайних листів [75]. Частина 3 статті 15 GDPR вказує, що якщо запит робиться в електронній формі, то відповідь надається таким же шляхом, крім випадків, коли суб’єкт прямо зазначив в своєму запиті інше. Щодо запитів, які здійснюються не за допомогою електронних засобів, то форма відповіді на них залежить від специфіки потреб суб’єкта. Часто така відповідь здійснюється шляхом надання копій відповідних документів, які вимагає суб’єкт даних. GDPR прямо зазначає, що у таких випадках, через адміністративні витрати, контролер має право стягувати плату в розумному розмірі.

Для уможливлення здійснення права на запит він контролера вимагаються активні дії на кожній зі стадій. Перш за все, він повинен організувати можливість подавати запити без складнощів. Це може означати створення веб-форми або зазначення контактних даних чи електронної адреси в легкодоступному місці [75].

Після отримання запиту необхідно ідентифікувати особу, що звертається. Саме ця стадія є однією із найпроблемніших для контролерів [76]. Підтвердження особи, що запитує, є важливою стадією, адже важливо унеможливити несанкціонований витік даних третім сторонам. До прикладу, після набуття

чинності GDPR дослідниками було проведено спроби отримати доступ до персональних даних осіб, зловживаючи правом на доступ [76]. Вони звернулись до 55 різних організацій із відповідними запитами, використовуючи для ідентифікації лише загальнодоступну інформацію взяту із публічних джерел, типу соціальних мереж. У 15 випадках із 55 їхні запити було задоволено і їм надали доступ до персональних даних інших осіб [76].

З іншого боку – занадто складна і багатоступенева ідентифікація теоретично може бути визнана створенням перешкод для реалізації свого права на доступ. Ще одним аспектом є те, що сама ідентифікація суб'єкта може бути причиною фінансових витрат для компанії, а GDPR зазначає про можливість стягування плати лише за копії певних документів, якщо особа вимагає такі. Тобто фінансові витрати від створення та підтримання ефективної системи ідентифікації осіб покладається на організацію. Тому реалізація права на доступ може бути викликом для деяких із них.

Баланс під час встановлення рівня складності перевірки намагаються роз'яснювати на місцевому рівні. Через те, що проблема ідентифікації осіб стала досить поширеною проблемою в багатьох країнах, уповноважені органи з питань захисту даних почали надавати свої рекомендації. В них роз'яснюється якими стандартами повинен керуватись контролер під час встановлення особи. Так, до прикладу, такі настанови було прийнято в Німеччині Органом нагляду Баварії для державного сектору [77]. В основному вони роз'яснюють положення частини 6 статті 12 GDPR, де вказано, що коли у контролера є розумні сумніви щодо ідентифікації фізичної особи, яка робить запит, то він може вимагати надання додаткової інформації, необхідної для підтвердження особи суб'єкта даних.

Настанови уповноваженого органу уточнюють, що перш за все слід з'ясувати, чи виникають сумніви щодо особи, яка подала запит. У роз'ясненнях вказується: «Як правило, немає сумнівів, якщо заявник особисто відомий відповідальній особі, наприклад, оскільки відповідальний службовець знає заявника та контактні дані

(електронна адреса, поштова адреса) з адміністративного процесу». Однак в таких випадках все одно потрібно звертати увагу, чи не змінились при цьому звичні засоби зв'язку (номер, електронна пошта) або прояви поведінки (наприклад, манера висловлювання) тощо [77].

З іншого боку, якщо заявника особисто не знають, то це не означає, що автоматично мають виникати сумніви щодо його особи. Контролер може вимагати підтвердження особи заявника, якщо сумніви під час ідентифікації є «виправданими». Тобто просто висловлення обґрунтованого сумніву не є достатнім. Мають бути вжиті всі розумні засоби для ідентифікації особи, а також має бути дотримано підзвітності, де треба продемонструвати підстави для сумнівів [77].

Важливо під час ідентифікації не забувати про дотримання іншого основоположного принципу – а саме мінімізації даних. Тому під час підтвердження особи, від неї потрібно вимагати саме тих документів чи даних, які абсолютно необхідні для ідентифікації [77].

Якщо сумніви не було усунуто, то контролер може відмовитись виконувати запит [77]. Відмова також має місце у випадках, коли особа не має права доступу до конкретних даних через те, що вони належать до винятків, передбачених законодавством. Положення, що були закріплені в GDPR описують ситуації, коли реалізація деяких прав особи може бути обмеженою, через національну безпеку та оборону, громадську безпеку, запобігання, розслідування, виявлення чи переслідування кримінальних правопорушень, запобігання загрозам суспільній безпеці тощо. Стаття 23 GDPR пояснює, що такі обмеження повинні не порушувати суть основних прав і свобод і мають бути необхідним і пропорційним заходом демократичного суспільства, що спрямовані на захист. Однак, деталізація винятків віднесена до сфери державного рівня, тобто держави-члени повинні передбачати у своєму національному законодавстві такі винятки більш конкретно. У Великобританії, яка донедавна була однією із держав-членів ЄС, застосовуються

безпосередньо до права на доступ винятки щодо виявлення і запобігання злочинів, сфери оподаткування, професійних зобов’язань юристів щодо конфіденційності, самообвинувачення, імміграційного контролю, таємниці усиновлення, ембріології, потенційної серйозної шкоди для здоров’я, чутливих медичних чи соціальних даних тощо [78]. Тобто, коли наявний один із винятків, контролер може відмовити у доступі. Однак ця підстава є частою причиною звернення до уповноважених та судових органів, оскільки не завжди є очевидним, чи в цьому випадку контролер може відмовити, чи повинен від надати доступ.

Іноді контролерам також складно визначити, чи дані, до яких запитується доступ, є персональними, а тому підпадають під сферу дії GDPR. До прикладу, в Бельгії була ситуація, коли особа подала запит до роботодавця після того як його кандидатуру, уже затверджену на посаду, було відкликано. Запит на доступ було подано з метою дізнатись причини такого рішення, однак роботодавець відмовив. Особа звернулась до уповноваженого органу з питань захисту персональних даних, який виніс рішення про те, що роботодавець зобов’язаний надати доступ, проте не було роз’яснено в якому обсязі і до якої документації [79].

Article 29 WP зазначає, що суб'єктивні судження та оцінки є персональними даними, навіть якщо вони є неправильними, тобто за такою логікою доступ мав би бути наданий і до даних особи і до документів, де вказані причини відкликання його кандидатури [79]. Суд ЄС має дещо вужчий погляд, зазначаючи у двох своїх рішеннях: «Дані юридичного аналізу, що містяться в цьому документі, є «особистими даними» [...] тоді як, навпаки, цей аналіз сам по собі не може бути класифікований як такий». При чому в іншій справі, що стосувалась права на забуття, цей же ж Суд ЄС вважає, що видалення має застосовуватись до екзаменаційних відповідей, а також до коментарів екзаменатора щодо них [79]. Тому у випадку бельгійського роботодавця залишається незрозумілим, чи повинен він, разом із доступом до даних особи, які компанія обробляє, надавати ще й доступ до їх коментарів чи причин, чому кандидатуру особи було відкликано.

У GDPR також передбачено можливість відмовити на запит до доступу, якщо він є несправедливим або надто обтяжливим. Обтяжливість, як правило, визначається обсягом документації або способом, в якому потрібно надати доступ суб'єкту даних. Якщо контролер обробляє великий об'єм інформації, з залученням багатьох процесорів, то він має право, у відповідь на запит, уточнити його щодо конкретної обробки або виду інформації. На практиці складнощі виникають із визначенням того, чи потрібно надавати безпосередньо копії усіх даних, чи можна надати їх резюме [80]. Відповідь на це питання часто відрізняється навіть в межах держави. До прикладу, Наглядовий орган регіону Гессен в Німеччині зазначив, що «термін «копія», який використано у статті 15 GDPR не варто розуміти буквально», тобто надати можна і резюме [80]. При цьому є рішення Трудового апеляційного суду Штутгарта, в якому навпаки – роботодавця було зобов'язано надати безпосередньо копії даних щодо діяльності та поведінки працівника, що зберігаються компанією [80].

Отже, право на доступ є одним із базових прав суб'єкта даних, що закріплюється в GDPR, так як воно є передумовою для здійснення ним інших прав, а також необхідним для реалізації основоположних принципів, особливо правомірності, справедливості та прозорості. Відповідно до положень Регламенту, це право означає можливість отримати від контролера підтвердження того, що персональні дані обробляються, та отримати до них доступ і їх характеристику.

Під час реалізації права на доступ, контролер повинен здійснювати активні заходи на кожній зі стадій процесу – він повинен зробити доступним канал подання запитів, докласти зусиль для ідентифікації суб'єкта, здійснювати вчасний розгляд запитів та їх виконання тощо. Однією із найбільш проблематичних стадій є ідентифікація суб'єкта, оскільки переважна більшість запитів подаються за допомогою онлайн інструментів або телефонним зв'язком. Контролер, при цьому, повинен запитувати у суб'єкта лише ті документи або вимагати таких дій, які є необхідними для його ідентифікації, а все інше може трактуватись як порушення

принципу мінімізації даних чи як створення перешкод для здійснення права на доступ.

Положення права на доступ частково також захищають і права контролера, дозволяючи не виконувати запит, коли він є несправедливим або надто обтяжливим, однак це не врівноважує цих суб'єктів між собою, що в принципі відповідає всьому характеру GDPR.

2.2.2. Судові рішення щодо права на доступ

Справа RE v. European Commission. Заявник у цій справі був працівником Директорату з питань міжнародного співробітництва та розвитку Європейської комісії. Щодо нього проводилось адміністративне розслідування, яке стосувалося його роботи в секретній службі, зокрема того, що під час конфлікту між двома третіми державами, він доніс до однієї з них конфіденційну інформацію [81, п. 1-2].

5 грудня 2013 року заявник звернувся з проханням, щоб управління безпеки «надало йому всю персональну та/або професійну інформацію і дані щодо нього, що зберігаються Дирекцією» [81, п. 3]. Йому було відмовлено із зауваженнями, що деякі документи були вже надані раніше, а на решту поширюється дія винятків та обмежень. Заявник звернувся зі скаргою до уповноваженого органу з захисту даних (EDPS), який прийняв рішення на користь заявника. Тому йому було видано ще деяку частину документів. Заявник попросив надати доступ до іншої частини, однак його запит не був задоволений [81, п. 5-9].

Повторне звернення до уповноваженого органу з аргументацією, що Управління безпеки досі не виконало рішення EDPS, на цей раз не було задоволене, оскільки вони також погодились, що запит вже виконано у достатньому обсязі. Тобто було ухвалене рішення, що Управління безпеки повністю виконало рекомендації уповноваженого органу [81, п. 10-11].

Через декілька місяців після цього Управління знову зв’язалось із заявником і його повідомили, що розслідування щодо нього було закінчене два тижні тому. Заявник уточнив список документів, до яких він все таки хотів отримати доступ і обґрунтував причини своїх вимог, однак йому відмовили посилаючись на рішення EDPS, що було ухвалене кілька місяців до того. Через неоднозначність обставин, необхідним стало звернення до Суду ЄС [81, п. 12-15].

Суд, перш за все, звернув увагу на те, що право особи на доступ не є обмежене у часі, тобто звертатись вона може будь-коли і не один раз. Більше того, переглядати такі звернення, якщо вони відбуваються періодично, є певним завданням контролера оскільки обставини обробки змінюються і кожне своє рішення потрібно базувати на ситуації, яка є в даний момент, а не на рішенні, що було прийняте задовго до того. Контролер має пересвідчитись, що не відбулось ніяких нових або істотних умов, що могли б змінити його рішення [81, п. 50, 56].

В цьому рішенні Суд також розрізняє доступ до документів і доступ до персональних даних. Ці права відрізняються між собою і кожне з них захищається іншим нормативно-правовим актом. Право на доступ до документації спрямоване на забезпечення прозорості під час прийняття рішень органами державної влади [81, п. 32]. Право на захист персональних даних має на меті забезпечити захист свобод та основних прав людей, зокрема їхнього приватного життя. Суд підкреслює, що хоча заявник не може за допомогою запиту на доступ до персональних даних отримати доступ до документів, що містять ці дані, це не впливає на зацікавленість заявника отримати доступ до даних як таких. Тобто Управління могло надати доступ до даних без доступу до документів, наприклад описавши інформацію в них [81, п. 36-42].

При відмові особі у реалізації права на доступ ключовим аспектом є мотивування. Воно має бути у рішенні, що надсилається суб’єкту і повинно чітко та однозначно розкривати міркування, якими керується установа, яка прийняла рішення. Це необхідно для того, щоб дозволити зацікавленим особам з'ясувати

причини відмови та у разі необхідності надати можливість суду здійснювати свою перевірку. Вимоги до такого мотивування залежать від обставин кожної справи, зокрема від змісту розглядуваного заходу, характеру наведених причин тощо [81, п. 80-82].

Особливо мотивація важлива, коли мова йде про винятки. Тоді як у відмові Управління, що була надіслана суб'єкту після закриття адміністративного провадження щодо заявника, такої мотивації не було. Записка лише посилалась на рішення кількамісячної давності і ніякого обґрунтування не містила. Беручи до уваги також те, що деякі із документів все таки були надані заявнику для ознайомлення і не підпали під винятки, а також відсутність належної мотивації і періодичності перегляду під час прийняття рішення про відмову, Суд ЄС вважає її неправомірною і такою, що підлягає скасуванню [81, п. 82-84].

Справа College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer. У попередньо проаналізованій справі Суд ЄС висловив тезу, що право особи на доступ не є обмеженим у часі, і особа може надати цей запит у будь-який час. Однак, реалізація цього твердження насправді є обмеженою, оскільки відповідно до принципу обмеження зберігання та мінімізації даних, якщо обробка перестає бути необхідною, то дані слід видаляти. Тому можуть перестати зберігати в тому числі і інформацію, яка запитується в межах права на доступ, як це було у даній справі.

Це рішення стосується тлумачення положень Директиви 95/46, однак аналогічні були закріплені в GDPR, тому підхід, очевидно, має залишатись таким же. Суд ЄС розглядає питання співвідношення права на доступ, зокрема, до інформації щодо передачі даних третім особам і принципу обмеження зберігання [82].

Заявник в межах здійснення права на доступ подав запит, «щоб бути поінформованим про всі випадки, коли дані, що стосуються його, […] були розкриті третім сторонам» за попередні два роки. Заявник хотів також отримати інформацію,

які саме дані передавались та хто одержувачі. Однак, місцева адміністрація міста Роттердам виконала його запит лише частково, надавши інформацію за попередній рік [82, п. 3-4]. Причина полягала у тому, що у місцевому законодавстві було передбачене положення, за яким адміністрація повинна зберігати дані про будь-яке повідомлення даних протягом одного року, якщо воно не відображається в іншій формі в базі даних. Тому інформація щодо передання персональних даних заявника за період більше ніж один рік вже була відсутня [82, п. 25].

Заявник намагався оскаржити такі дії адміністрації, оскільки він вважав їх неправомірною відмовою в наданні йому інформації. Його скаргу було відхилено, тому пан Рійкебер подав позов до Суду Роттердама. Суд підтримав позов, зазначивши, що він вважає, що національне законодавство у цьому випадку суперечить положенням Директиви 95/46 [82, п. 26-27]. Він також постановив, що у цьому випадку не застосовуються винятки, зазначені у статті 13, які передбачають можливість державам-членам обмеження положення Директиви 95/46, якщо це необхідно для захисту суспільних інтересів, захисту суб'єкта даних або прав та свобод інших осіб тощо [82, п. 30-32].

Однак при цьому Суд Роттердама звернувся до Суду ЄС, щоб розтлумачити, чи «можуть положення, які містяться в Директиві зокрема, її статті 12 (a), що закріплює право фізичної особи на доступ до інформації про одержувачів його персональних даних, та на зміст повідомлених даних, бути обмежені періодом у рік, що передує запиту» [82, п.31]. Тобто Суд Роттердама виділяє два положення Директиви у поставленому питанні і це звернення є вирішенням проблеми співвідношення статті про обмеження зберігання персональних даних та статті про право доступу до цих даних [82, п. 32-35].

Суд ЄС зазначає, що для того, щоб оцінити сферу права доступу, яку Директива повинна зробити можливою, слід, по-перше, «визначити, які дані охоплюються правом доступу, а потім, звернутися до мети статті 12 (a) з урахуванням цілей Директиви» [82, п. 40]. У даній справі є дві категорії даних.

Перш за все це основні персональні дані, що зберігаються місцевою владою про особу, такі як його ім'я та адреса. Вони складають персональні дані у значенні Директиви і відповідно до роз’яснень уряду Нідерландів, «можуть зберігатися протягом тривалого часу» [82, п. 42].

Друга категорія – це «інформація про одержувачів або категорії одержувачів, яким розкриваються основні персональні дані, та про зміст» останніх. Тобто це інформація, що стосується обробки основних даних. Відповідно до національного законодавства, ця інформація зберігається лише один рік. Строки права доступу до інформації, про які йдеться в цій справі, стосуються, таким чином, другої категорії даних [82, п. 43-44].

Суд вказує: «Для того, щоб визначити, чи санкціонує стаття 12 (а) Директиви такий строк, доцільно інтерпретувати цю статтю з урахуванням цілей Директиви [якими є] захист основних прав та свобод фізичних осіб, зокрема їх права на приватне життя щодо обробки персональних даних, а отже, уможливлення вільного потоку персональних даних між державами-членами» [82, п. 45-46]. Принципи такого захисту втілюються у обов’язках, покладених на контролерів та процесорів і у правах, якими наділяються суб’єкти даних. А право на приватність, закріплене у цілях означає, що суб'єкт даних може бути впевнений, що його персональні дані обробляються правильно та правомірно, тобто, зокрема, що вони розкриваються уповноваженим одержувачам. Тому в Директиві і передбачене відповідне право на доступ, щоб особа могла у цьому пересвідчитись і за необхідності використати інші свої права такі як право на виправлення чи стирання [82, п. 48-51].

Право на доступ до даних в першу чергу пов’язане із вже здійсненою обробкою, тому постає питання про обсяг такого права у минулому. Визнаючи деяку свободу держав під час імплементації положень Директиви, Суд ЄС вказує, що якщо тривалість часу для зберігання основних даних дуже довга, суб'єкт даних довго зацікавлений у реалізації своїх засобів правового захисту. Звісно, це не означає покладення на обробника непропорційного тягаря зберігання всієї

супутньої інформації протягом усього періоду зберігання основних даних, однак принцип пропорційності повинен бути дотриманим [82, п. 58-66].

Тобто повинен бути забезпечений справедливий баланс між, з одного боку, зацікавленістю суб'єкта даних у захисті його приватності, зокрема, шляхом забезпечення його прав на виправлення, стирання та видалення даних у випадку, якщо обробка персональних даних не відповідає Директиві, а з іншого – тягар зобов'язання зберігати цю інформацію, що покладається на суб’єкта, який обробляє дані [82, п. 66].

У даній справі Суд вирішив, що основні дані зберігаються набагато більш тривалий період, ніж супутні, які необхідні для реалізації прав, що не є справедливим балансом спірних інтересів та зобов'язань, якщо тільки не можна довести, що довше зберігання цієї інформації буде представляти надмірне навантаження. Однак національні суди повинні зробити перевірки, необхідні з огляду на міркування, викладені в рішенні Суду [82, п.66-69].

Отже, Суд ЄС у своїх рішеннях розглядає різні аспекти права на доступ, зокрема його часові обмеження, періодичність, обов’язки контролера надання відповідей і їх мотивування тощо. Суд також розмежовує право на доступ до інформації і на доступ до документів і збалансовує права суб’єкта даних та тягар покладений на контролера.

2.3. Обмеження автоматизованої обробки і профілювання

2.3.1. Суперечності між основоположними принципами і автоматизованою обробкою та профілюванням

Стаття 22 GDPR закріплює право особи не бути суб’єктом щодо рішення, яке ґрунтується винятково на автоматизованій обробці, в тому числі і профілюванні, якщо це спричиняє юридичні наслідки чи іншим способом значуще впливає на неї.

До цього положення прямо передбачений ряд винятків в цій же ж статті, які схожі із підставами правомірності обробки. Так, обмеження щодо автоматизованої обробки не застосовуються, якщо (i) це є необхідним для укладення або виконання договору між суб'єктом та контролером; (ii) контролер уповноважений на це нормативно-правовими актами ЄС чи його країн-членів, що встановлюють заходи щодо захисту прав і свобод та законних інтересів суб'єкта даних; або (iii) вона ґрунтується на однозначній згоді суб'єкта даних.

Автоматизоване прийняття рішення означає «прийняття рішення автоматизованими засобами, тобто без будь-якого залучення людини» [83]. Наразі, коли мова йде про повністю автоматизовану обробку, то мається на увазі залучення штучного інтелекту, особливістю якого є те, що йому необхідно обробляти великі масиви даних для самонавчання і вдосконалення подальшої обробки. Всі процеси при цьому базуються на закладені у машину алгоритми [84, с. 8]. Тобто, якщо традиційна обробка означала визначеність результату і побудови запиту так, щоб досягнути цього результату, то обробка штучним інтелектом означає застосування великої кількості алгоритмів на Великі дані із неможливістю передбачити, які будуть знайдені кореляції [84, с. 10]. Такі методи називають «глибинним навчанням» і вони передбачають «подання […] інформації через нелінійні нейронні мережі, які класифікують дані на основі результатів кожного наступного шару». Складність таких процесів означає неможливість пояснити деякі рішення штучного інтелекту і їх причини [84, с. 10-11].

Профілювання або профайлінг, за визначенням статті 4 GDPR, це автоматизована обробка персональних даних, коли дані використовують для оцінки певних особистих аспектів, пов'язаних з фізичною особою. До прикладу, вони можуть використовуватись для аналізу або прогнозування інформації, що стосується діяльності цієї фізичної особи на роботі, економічної ситуації, здоров'я, особистих вподобань, інтересів, поведінки, місця розташування тощо.

Компанії використовують цей інструмент для того, щоб дізнатись про те, чому люди надають перевагу, щоб передбачити їх поведінку чи для того, щоб приймати рішення про них [83]. Найчастіше це використовують у маркетингу, однак загалом сфера застосування профайлінгу, у поєднанні з машинним навчанням є надзвичайно широкою. До прикладу, такі інструменти використовуються у медицині, адже застосовуючи штучний інтелект, можна здійснювати прогнозування здоров'я пацієнтів або вираховувати ймовірність успішного лікування певного пацієнта, базуючись на певних характеристиках. Також активним є використання автоматизованої обробки у сфері навчання – для виявлення можливих покращень у системі освіти, викладанні матеріалу, взаємодії зі студентами; в сфері транспорту – для планування навантаження на публічний транспорт, створення більш комфортних умов для користування автобусами чи електричками тощо [84, с. 15-17].

Навіть аналітика в маркетингових цілях є вигідною не лише фінансово і для власників бізнесу, оскільки саме вона змушує вивчати потреби клієнта, розуміти чому надає перевагу особа і чого вона хоче. Тобто маркетинг стає більш цілеспрямованим та ефективним, а бізнес – більш орієнтованим на споживача і зручнішим для нього [84, с. 17].

Менш очевидні форми профілювання передбачають отримання висновків із очевидно неспоріднених аспектів поведінки людей. Наприклад, аналіз публікацій у соціальних мережах можуть використати для аналізу особи і її безпечності як водія, щоб призначити рівень ризику та встановити відповідний страховий внесок [84, с. 27, 31].

Використання штучного інтелекту означає не лише прибуток підприємств, а й відчутний розвиток економіки держав. До прикладу, у Великобританії експерти оцінюють загальну вигоду для економіки країни від аналітики Великих даних у розмірі 241 мільярдів фунтів стерлінгів з 2015 по 2020 рік, або в середньому 40 мільярдів фунтів стерлінгів на рік [85].

Тобто використання штучного інтелекту може в сотні разів пришвидшувати процеси обробки і обробляти значно більші масиви даних, що робить їх ефективними для бізнесу і ефективного використання коштів. І обробка все більших масивів даних зумовлює розвиток штучного інтелекту, що, в свою чергу, дозволяє створювати все більш досконалі машини, точність яких є вищою за людську. Але при цьому GDPR обмежує автоматизовану обробку та профілювання, якщо це є основою для прийняття якогось рішення, що матиме юридичні чи інші серйозні наслідки. Під юридичними наслідками мається на увазі вплив на законні права особи, її правовий статус чи її права в межах договірних відносин. Серед прикладів наводять такі як вирішення питання соціальних виплат (субсидії, допомоги на дитину), відмова у в'їзді на національному кордоні тощо [86]. До серйозних наслідків можуть належати відмови від онлайн-заявки на кредит, автоматизовані рішення щодо кредитних лімітів, певні види цільової реклами та профілювання в Інтернеті, яке призводить до пропозиції різним особам різних цін через їхню платоспроможність [86].

Як часто вказується, обмеження GDPR цих інструментів може створювати перешкоди чи сповільнювати розвиток технологій у сфері машинного навчання. Але з іншого боку – це здійснюється з метою захисту суб'єктів даних, оскільки така обробка не може відповідати всім необхідним вимогам і вона буде порушувати їх права. Як відзначає Управління захисту даних в Норвегії, розробники штучного інтелекту стикаються з чотирьома проблемами, які пов'язані з основоположними принципами. Це можливі проблеми із справедливістю, обмеженістю ціллю, мінімізацією даних, прозорістю, та, окрім принципів, правом на інформацію.

Так, однією із проблем автоматизованої обробки і особливо профайлінгу є можливий дискримінаційний характер. Обробляючи великі масиви даних, штучний інтелект навчається, в тому числі, і за допомогою упереджених даних, яких є чимало. Також можливими є певні відхилення в алгоритмічних моделях. З цих причин штучний інтелект може здійснювати расову, гендерну, медичну, релігійну

чи ідеологічну дискримінацію. Для дотримання принципу справедливості такі відхилення мають бути повністю усунуті [87]. Окрім цього, незрозумілість та надмірна складність принципів роботи штучного інтелекту ставить під загрозу виконання умови про те, що обробка має здійснюватися, відповідно до розумних очікувань суб'єкта, що є основною вимогою для реалізації принципу справедливості [84, с. 22]. Для того, щоб суб'єкт даних надав свою згоду на обробку, і більше – згоду на обробку штучним інтелектом, повинна бути довіра між ним та контролером, що базується на доступності, зрозумілості, прозорості. Поки що це залишається викликом для розробників.

Щодо принципу обмеженості ціллю, то, як вже зазначалось, його важливою складовою є інформування суб'єкта про цілі, для яких здійснюється обробка. І вихід за межі заявлених цілей без нової згоди, якщо такі цілі не є сумісними із попередніми, є порушенням цього принципу. Тоді як іноді штучний інтелект може іноді використовувати інформацію, яка є побічним результатом оригінального збору даних, що є процесом його навчання і розгортання. Виникає запитання, чи може це вважатись одним із винятків GDPR для цього принципу, а саме пов'язаність із науковими дослідженнями. Тобто чи може розвиток штучного інтелекту вважатися науковим дослідженням. Чіткого визначення, що таке наукові дослідження немає, тому наразі відповідь на це питання залишається відкритою [87]. Так чи інакше, очевидно, що під таку категорію штучний інтелект може підпадати лише на початку свого глибинного навчання і на якийсь момент він вже явно не буде мати ознак наукового дослідження. Тому потрібно мати змогу чітко визначити момент, коли його навчання переходить в стадію повноцінного функціонування.

Принцип мінімізації даних також є неабияким викликом для розробників штучного інтелекту, оскільки він передбачає, що зібрана інформація повинна бути адекватною, обмеженою та відповідною. Однак визначити, які дані і яка кількість необхідна для проекту на практиці є дуже складно, оскільки не завжди можливо

передбачити, як і що машина дізнається з даних. Тобто під час навчання штучного інтелекту, розробники повинні постійно переоцінювати їх відповідність та кількість, що необхідна для виконання принципу мінімізації даних [87].

Окрім цього, суперечності є і між принципом прозорості і правом на інформацію та штучним інтелектом. Однією із цілей GDPR є надання суб'єкту повноважень щодо розпорядження даними. Але для цього контролери даних повинні бути максимально відкритими та прозорими у своїх діях. Вони повинні детально та доступно описувати та роз'яснювати, що вони роблять з особистими даними власникам цих даних. Тоді як із системами штучного інтелекту це зробити важко, тому що не завжди до кінця зрозуміло, як модель приймає певні рішення, що унеможливлює пояснення складних процесів користувачеві [84, с. 27].

ICO надаючи схожі висновки, також зазначає, що для того, щоб обробка із залученням штучного інтелекту відповідала GDPR, необхідно переглянути процес надання згоди. Адже наразі від є бінарним, тобто допускає варіанти «так/ні» у відповідь на запитування згоди. Тоді ж як більш виправданим буде підхід градуйованої згоди, зважаючи на постійну змінність цілей обробки під час застосування штучного інтелекту [84, с. 30].

Профілювання і автоматизоване прийняття рішення часто є пов'язаними і можуть продовжувати одне одного. Наприклад контролер вирішує передати штучному інтелекту вивчення певних аспектів приватного життя, тобто здійснюється профілювання, і після цього на базі цих даних машина приймає відповідне рішення щодо суб'єкта [83]. Також можливо, що спершу здійснюється обробка усіх даних, а на основі цього віднаходиться кореляція, що уможливлює профілювання тощо.

Можливі й інші варіанті використання цих інструментів, коли до такого процесу залучається людина і приймає рішення на основі профілювання, здійсненого штучним інтелектом. Саме для того щоб відповідати GDPR, компанії почали залучати в процеси аналізу та прийняття рішень людину. Робота за такою

системою отримала назву «human-in-the-loop» або «людина-в-циклі» [88]. У таких випадках штучний інтелект створюється і програмується так, що він потребує людини під час навчання та під час прийняття рішення. Однак, для того, щоб дійсно виконувати вимоги втручання людини повинно бути значимим. Саме людина повинна проаналізувати всі наявні дані та мати повноваження та компетенцію змінювати рішення [86]. Тоді як штучний інтелект більшою мірою зосереджують на структуруванні та представленні інформації у зручному форматі для особи, яка прийматиме рішення, або на обробці на окремих стадіях [88].

Отже, GDPR встановлює обмеження щодо автоматизованої обробки та профілювання суб'єктів даних, коли це впливає на їхні юридичні зобов'язання чи може спричинити інші серйозні для них наслідки. Такі обмеження часто характеризують як сповільнення технологічного прогресу у сфері застосування штучного інтелекту. Останній, однак, може бути вигідним для бізнесу, споживачів та держави. Також він є корисним і для людей як суб'єктів даних, оскільки може відстежувати кореляції у сфері здоров'я, освіти чи публічного транспорту. Тим не менше, наразі сфера використання штучного інтелекту ще не розвинена достатньо, щоб не суперечити основоположним принципам Регламенту, серед яких справедливість, прозорість обробки, обмеженістю ціллю, мінімізація даних тощо. Неможливість пояснити як машина обробляє дані, у поєднанні зі змінністю цілей під час обробки та необхідністю залучати якомога більше даних для глибинного навчання створює перешкоди на шляху розробників, які хочуть бути у комплаєнсі з GDPR. Окрім цього, у зв'язку із такими особливостями, необхідним є і перегляд концепції згоди, яка повинна стати градуйованою і надаватись, відповідно до нових змінених цілей.

2.3.2. Судові рішення щодо автоматизованої обробки та профілювання

Одним із нещодавніх рішень, що пов’язані із положеннями статті 22 GDPR, є рішення Окружного суду Гааги щодо ризикованого профілювання, яке було прийняте 5 лютого 2020 року. Воно стосувалось програми SyRi (Systeem Risicoindicatie) – правового інструменту, який застосовується урядом Нідерландів для виявлення різних форм шахрайства, включаючи правопорушення, пов’язані із соціальними виплатами, надбавками та податковим шахрайством [89, п. 3.1-3.6].

SyRi є технічною інфраструктурою з певними процедурами, за допомогою яких можна пов’язати та анонімно проаналізувати дані в безпечному середовищі. Її функціонування відповідає концепціям глибинного навчання та самонавчання [89]. На основі аналізу SyRi створюються звіти про ризики. Як зазначає суд, складання звіту про ризик означає, що дії юридичної чи фізичної особи є достатніми для початку розслідування щодо можливого шахрайства, незаконного використання коштів та порушення законодавства. Тому в даному випадку наслідки профілювання є значущими для відповідних осіб, оскільки воно суттєво та тривало впливає на обставини, поведінку та вибір суб'єктів даних [89, п. 4.30, 6.46].

Через використання SyRi, уряд поєднується із іншими органами і всі файли цих органів стають пов'язаними, що дозволяє виявляти пов'язані зловживання та збільшувати шанси відслідкувати дії правопорушників [89, п. 4.28].

Окрім уряду, до такої пов’язаної системи належить муніципальна влада, податкова та митна адміністрація, служба імміграції та натуралізації, інспекція з питань соціальних питань та зайнятості тощо. Перелік цих органів може змінюватись, оскільки інші органи можуть подавати заявки, щоб також доєднатись до альянсу. Всі ці органи зобов'язані надавати необхідну інформацію одне одному, і, як підкреслює Суд, в цьому випадку «вони є спільними контролерами за змістом статті 26 GDPR». Перелік категорій даних, які вони збирають, є широким та різноманітним [89, п. 4.6, 4.17].

Нормативно-правовий акт, що визначає основи використання SyRi, обмежує можливість використовувати дані, які наявні в системі. Так, їх можна використати

лише для подання відповідного звіту про ризик щодо фізичної або юридичної особи. В окремих випадках такий звіт подається не лише уряду або іншим органам, які подали запит на використання SyRi, а й до прокуратури та поліції – «на прохання таких органів та в межах необхідності для виконання їх статутних обов'язків» [89, п. 4.11-4.13].

Національне законодавство також обмежує і строк зберігання складених звітів. Так, звіти зберігаються міністром, який їх створює не довше, ніж це необхідно, але не більше двох років. Уряд чи інший орган, який отримали звіт, можуть використовувати його протягом двох років і повинен надати міністру зворотній зв'язок щодо результатів протягом 20 місяців з моменту початку SyRi. У будь-якому випадку дані, що обробляються в SyRi, мають бути вилучені з не пізніше ніж через два роки після їх подання [89, п. 4.15].

Дані, які завантажуються в систему, перед цим псевдонімізуються. Коли після аналізу на основі моделей, певні фізичні чи юридичні особи позначаються як такі, що мають підвищений ризик, то їх дані дешифруються. Усі позначені і дешифровані дані передаються відповідному міністру для подальшого аналізу. А будь-які файли, які не були позначені і які залишаються в SyRi після передачі, знищуються через чотири тижні [89, п. 4.29].

На наступному етапі передані дані розглядаються відділом аналізу Інспекції з соціальних питань та зайнятості. Вони «оцінюються на предмет їхньої необхідності для більш детального дослідження. Це призводить до остаточного вибору ризикових суб’єктів. Міністр подає звіти про ризики на основі інформації щодо таких осіб, остаточно обраних ризиковими» [89, п. 4.30].

Незважаючи на значну кількість заходів, запроваджених для того, щоб відповідати європейським нормативно-правовим актам, NJCM вбачає суперечливість між національним законодавством і GDPR та Європейською конвенцією, тому з цього приводу звернулась до Гаагського окружного суду. NJCM зазначає, що така практика є втручанням у приватне життя людини, а законодавство

не містить достатніх гарантій, щоб забезпечити права відповідних суб'єктів [89, п. 6.1].

Суд, у свою чергу, підкреслює, що «соціальне забезпечення є одним із стовпів суспільства Нідерландів», тому боротьба з шахрайством є ключовою умовою підтримки громадянської системи. І, звісно, треба використовувати нові технологічні можливості для такої боротьби. Тому цілі та мета відповідного законодавства, що регулює дані правовідносини є важливими [89, п. 6.3-6.4].

Однак, Суд також звертає увагу, що «розвиток нових технологій також означає, що і право на захист персональних даних стає все більш вагомим» [89, п. 6.5]. Наявність належного законодавчого захисту приватності при обміні особистими даними із урядом чи іншими державними органами сприяє такій же ж довірі громадян до уряду, як і запобігання шахрайству та боротьба з ним. Саме тому важливим є досягнення правильного балансу між вигодами при застосуванні технологій для протидії шахрайству, з одного боку, та можливим втручанням у право на повагу до приватного життя через таке використання – з іншого [89, п. 6.6].

В результаті ґрунтовного дослідження, Суд приходить до висновку, що законодавство, що регулює використання SyRi не відповідає вимогам європейських нормативно-правових актів. Перш за все, мова йде про встановлену у пункті 2 статті 8 Європейської Конвенції вимогу про те, що втручання у реалізацію права на повагу до приватного життя повинно відповідати законодавству, бути необхідним та пропорційним. Не заглиблюючись у критерій відповідності закону, Суд вказує, що для того, щоб критерій пропорційності був дотриманим, повинні бути гарантії, достатні для запобігання зловживань, чого актуальне національне законодавство не містить. Як наслідок, у своєму актуальному вигляді воно не відповідає вимогам статті 8 Європейської Конвенції. А отже – не забезпечується і необхідного справедливого балансу [89, п. 6.95].

Також Суд аналізує відповідність основоположним принципам, які лежать в основі захисту даних, що закріплені в Хартії та GDPR. Зокрема принципи

прозорості, справедливості, обмеженості ціллю та мінімізації даних. Так, законодавець не зміг повною мірою пояснити, якою є модель прийняття рішень і які показники можуть використовуватися в проекті, тому принцип прозорості не може вважатись дотриманим [89, п. 6.7]. Через недостатнє роз'яснення принципів та деталей роботи механізмів SyRi, не можна також оцінити, чи було недопущене дискримінаційне профілювання, а отже – чи не є порушеним принцип справедливості. На момент збирання даних, законодавець не знає, з якою ціллю вони використовуватимуться, однак все одно збирає велику кількість даних у багатьох категоріях, без належної перевірки необхідності, що призводить до порушення принципів цільової обробки та мінімізації даних. Отже, після аналізу національного законодавства, Окружний суд вважає, що воно не відповідає також вимогам Хартії ЄС та основоположним принципам GDPR [89, п. 6.86].

І, насамкінець, порушеними є положення статті 22 GDPR, яка обмежує профілювання осіб. Безперечно, те, що здійснює програма, відповідає визначенню профілювання, адже звіт про ризик має значний вплив на приватне життя особи, тобто підпадає під категорію серйозних наслідків. Той факт, що звіт про ризик не завжди призводить до подальшого розслідування або до адміністративної чи кримінально-правової відповідальності не змінює суттєвого впливу на приватне життя суб'єкта. Але під жоден із винятків, зазначених у статті 22 GDPR, діяльність SyRi не підпадає, тому вона не відповідає вимогам Регламенту [89, п. 6.55-6.60].

Отже, окружний суд Гааги виніс рішення, яке відображає кумулятивний підхід європейських судових органів у справах із застосуванням профілювання та автоматизованої обробки. Оскільки така діяльність є втручанням у право на повагу до приватного життя та право на захист персональних даних, то оцінці підлягають критерії, що застосовуються до них обох. Щодо права на приватне життя, то Суд розглядає класичний трискладовий тест, який застосовує ЄСПЛ при встановленні втручання у приватність – встановлення законом, необхідність у демократичному суспільстві і пропорційність. Розглядаючи ж цю ситуацію щодо права на захист

персональних даних, суд вказує на порушення основоположних принципів GDPR та положень, які встановлюють умови автоматизованої обробки та профілювання. Як результат – використання системи SyRi було визнано неправомірним.

***

Висновок до розділу 2

Основоположні принципи є окремою складовою GDPR, однак вони тісно пов’язані і з іншими положеннями Регламенту. Оскільки ціллю Регламенту є захист прав суб’єкта даних, то часто такий зв'язок є із нормами про права. Але реалізація прав може ускладнюватися вимогами принципів, суперечити їм, або у поєднанні із ними – мати негативний ефект на інші сфери діяльності суб’єкта даних. Найскладнішими для здійснення є право на забуття, право на доступ до даних та право не підлягати автоматизованій обробці та профілюванню.

Право на забуття є об’єктом дискусій з часу його створення і його закріплення в межах Регламенту лише посилило дискусії. За ним, суб’єкт даних має право на стирання контролером персональних даних, коли зникає необхідність їх обробляти; коли відкликано згоду або надано заперечення проти обробки; коли обробка є неправомірною; коли забуття потрібне, щоб відповідати нормативно-правовим актам ЄС; або коли суб’єктом є дитина, а дані були зібрані для пропозиції послуг інформаційного суспільства.

Здійснення права на забуття необхідною передумовою для реалізації більшості із принципів – обмеженості ціллю, мінімізації даних, обмеження зберігання, правомірності, справедливості обробки. Але тягар, покладений на контролера і технічна складність реалізації зменшує ефективність цього засобу правового захисту. Адже контролер має забезпечити доступний процес звернення суб’єкта, можливість видаляти усі дані з серверів та підтверджувати повне

видалення, а також повинен пересвідчитись, що такі ж дії здійснюють інші контролери, яким передавались персональні дані.

Суперечливим є баланс права на забуття із правом на свободу вираження поглядів та інформації, включаючи обробку для журналістських цілей. GDPR декларує необхідність забезпечення пропорційності між цими правами, однак їїсзабезпечення покладає на національний рівень. Аналіз національного законодавства показує, що ризики для свободи інформації досі є вагомими.

Право на доступ до даних є необхідним для виконання прозорості, а також уможливлює реалізацію принципів точності та справедливості обробки. Це одне із базових прав, завдяки якому особа може дізнатись, що його дані обробляються, та дізнатись все про їх обробку. Але його виконання є проблемним для контролерів, особливо – на стадії ідентифікації суб'єкта даних, адже у більшості випадків вона здійснюється онлайн чи за допомогою телефонного зв'язку. Ідентифікація ускладнюється через принцип мінімізації даних, тобто контролер може вимагати лише мінімально необхідні документи. Занадто складна ідентифікація може бути порушенням прозорості або створенням перешкод для реалізації права на доступ даних.

Також контролер може вважати, що його обробка даних підпадає під дію винятків, а тому він не зобов'язаний надавати доступ до даних, однак потім судові органи визнають протилежне. Контролери, які обробляють великі обсяги даних захищені лише твердженням загального характеру про те, що вони мають право відмовити у здійсненні запиту, якщо це становить непосильний тягар або є несправедливим, однак такі положення потребують деталізації, щоб вважатись ефективним збалансуванням прав обох сторін.

І, насамкінець, право не бути суб'єктом автоматизованої обробки, в тому числі – профілювання. Це положення критикується за його стримування технологічного розвитку, адже автоматизована обробка та профілювання використовуються розробниками штучного інтелекту і подальше його застосування

допомагає оптимізувати бізнесові процеси, налагоджує маркетинг, створює унікальні можливості у сферах охорони здоров'я, навчання, розслідування та припинення правопорушень, громадського транспорту тощо. Однак, така обробка суперечить положенням статті 22, яка закріплює відповідне право, так само як і основоположним принципам, справедливості, прозорості, обмеженості ціллю, мінімізації даних тощо. Як результат – наразі це суттєво можливість використання штучного інтелекту.

Ґрунтовний аналіз прав показує, що практика застосування GDPR ще не є налагодженою і потребує подальших роз'яснень уповноважених органів, так само як і роботи над подальшими змінами до тексту самого Регламенту.

ВИСНОВКИ

GDPR був прийнятий в Європейському Союзі у 2014 році, вступив у силу у 2016 році, а почав застосовуватись – із 25 травня 2018 року. Така довготривалість зумовлена основоположним характером акту для права на захист персональних щодо усіх суб'єктів і категорій персональних даних. Форма Регламенту означає його обов'язковість для всіх держав-членів ЄС без необхідності окремої імплементації в національне законодавство. Вона зумовила єдність правового регулювання в державах ЄС.

GDPR був прийнятий для захисту осіб в Європейському Союзі, але його вплив поширився далеко за його межі завдяки екстратериторіальній дії. Він є обов'язковим для всіх, хто обробляє персональні дані і, при цьому, надає свої послуги чи продає товари у державах ЄС і для їх громадян. Лише надання можливості оплати товару у євро чи реклами в країні ЄС компаніями, що обробляють персональні дані, достатньо, щоб підпадати під дію GDPR.

Можливість співпрацювати з європейськими компаніями є заохоченням до приведення своєї практики у відповідність норм Регламенту. GDPR встановлює відповідальність контролерів за обробку даних процесорами, тому компанії в межах ЄС обирають своїми контрагентами тих, чия діяльність не порушує норм GDPR. Це стосується IT компаній, які часто є процесорами персональних даних.

GDPR вплинув і на нормативно-правове регулювання інших держав. Його прийняття створило тенденцію підвищення рівня стандартів і посилення захисту суб'єктів даних у значній кількості держав. Тому його часто називають «модельним актом» у сфері захисту персональних даних.

Найважливішою частиною Регламенту є його основоположні принципи, в них закладені ідеї всієї системи захисту. Основоположними є такі принципи як правомірність, справедливість та прозорість обробки, обмеженість ціллю,

мінімізація даних, точність, обмеження зберігання, цілісність та конфіденційність та підзвітність.

Кожен із принципів об’єднує ряд вимог до суб’єктів, що обробляють дані. Правомірність означає вимогу наявності однієї із підстав для обробки; справедливість – обробляти дані так, як цього розумно очікує суб’єкт; прозорість позначає ряд вимог щодо лаконічної, зрозумілої комунікації та доступності інформації щодо обробки.

Обмеженість ціллю – вимагає наявність конкретних, необхідних та задокументованих цілей обробки, на кожну із яких надається окрема згода. Мінімізація даних – обмеження даних до того обсягу і кількості, який необхідний для досягнення встановлених цілей. Точність – закріплює вимоги щодо якості даних. Обмеження зберігання – вимогу не зберігати персональні дані, коли вже немає необхідності.

Цілісність та конфіденційність – позначає організаційні та технічні вимоги щодо безпеки даних. І, насамкінець, підзвітність – це встановлення зобов’язання контролера проявляти активність і мати змогу показати відповідність усім цим принципам.

Кожен із цих принципів має загальний характер і повинен оцінюватись в конкретних випадках, з урахуванням всіх обставин. Це має і негативну сторону – часто контролери та процесори не можуть зрозуміти, чи порушуватимуть їхні дії вимоги Регламенту. Тому важливим є аналіз діяльності компаній та рішень щодо них органів, уповноважених на захист персональних даних, які пояснюють їх бачення принципів і формують практику розуміння в межах ЄС.

Основоположні принципи не існують відокремлено від інших норм Регламенту, вони пов’язані зі всіма його нормами, особливо з правами суб’єкта даних. Реалізація прав є необхідною для виконання вимог Регламенту, але вона ускладнюється необхідністю дотримання усіх принципів, або у поєднанні із ними

порушує інші права суб’єкта даних. Дискусійними є права на забуття, на доступ до даних та право не підлягати автоматизованій обробці та профілюванню.

Всебічне дослідження основоположних принципів і прав, включно практикою їх застосування як на державному рівні, у практиці національних судів, так і на рівні ЄС і у рішеннях Суду ЄС, є необхідним для імплементації аналогічних норм в систему українського законодавства. Тому що як видно із поточної ситуації – перенесення фрагментів GDPR до національного закону не може створити ефективну систему захисту, її потрібно пристосовувати до реалій держави.

У випадку України варто звернути увагу додатковий захист свободи слова, забезпечення можливості розслідування корупційних правопорушень, а також зниження вимог для малого та середнього бізнесу. Текст закону повинен враховувати ці особливості і бути більш узгодженим та якіснішим, ніж наявний наразі. Важливим є і створення ефективної системи відповідальності за порушення і підвищення спроможності Уповноваженого з прав людини щодо нагляду у цій сфері.

Для дієвості прийнятих норм варто також підвищувати рівень правосвідомості та обізнаності громадян і державних службовців щодо необхідності захисту персональних даних. Саме тому необхідними є розуміння основ, духу та ідей, закладених в GDPR як в одному із найбільш прогресивних наразі актів у цій сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Загальна теорія права: Підручник / Козюбра М.І., Погребняк С.П., Цельєв О.В., Матвєєва Ю.І. Київ: Ваіте, 2015. 392 с.

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 04.05. 2016. L 119. Vol. 59. URL: http://data.europa.eu/eli/reg/2016/679/oj (дата звернення: 02.04.2020).

3. The History of the General Data Protection Regulation. European Data Protection Supervisor: веб-сайт. URL: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (дата звернення: 18.02.2020).

4. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian: веб-сайт. URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (дата звернення: 18.02.2020).

5. Burman A., Rai S. What Is in India's Sweeping Personal Data Protection Bill? Carnegie India: веб-сайт. URL: https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985 (дата звернення: 18.02.2020).

6. The impact of the GDPR outside the EU / Anastasia Petrova and others. Ius Laboris: веб-сайт. URL: https://theword.iuslaboris.com/hrlaw/whats-new/the-impact-of-the-gdpr-outside-the-eu (дата звернення: 18.02.2020).

7. California Consumer Privacy Act of 2018. Added by Stats. 2018. Ch. 55, Sec. 3. California Legislative Information: веб-сайт. URL: http://leginfo.legislature.ca.gov/faces/home.xhtml (дата звернення: 20.02.2020).

8. Principle (a): Lawfulness, fairness and transparency. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ (дата звернення: 23.02.2020).

9. Șchiopu S.-D. Some Considerations On The Lawfulness Of Personal Data Processing By Public Administration Authorities Under Regulation (EU) 2016/679. Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law. 2018. Vol. 11 (60) № 2. P. 203–208. URL: https://www.ceeol.com/search/article-detail?id=745500 (дата звернення: 23.02.2020).

10. Ausloos J. Giving meaning to Lawfulness under the GDPR. KU Leuven Centre for IT & IP Law: веб-сайт. URL: https://www.law.kuleuven.be/citip/blog/2761-2/ (дата звернення: 23.02.2020).

11. Lawful basis for processing. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (дата звернення: 23.02.2020).

12. Murmann P., Fischer-Hübner S. Tools for Achieving Usable Ex Post Transparency: A Survey. IEEE Access. 2017. Vol. 5. P. 22965-22991. URL: https://ieeexplore.ieee.org/document/8078167 (дата звернення: 25.02.2020).

13. Guidelines on Transparency under Regulation 2016/679. Article 29 Data Protection Working Party. 2017. 17/EN. WP260 rev.01. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (дата звернення: 25.02.2020).

14. Spagnuelo D., Ferreira A., Lenzin G. Accomplishing Transparency within the General Data Protection Regulation. 5th International Conference on Information Systems Security and Privacy. 2019. DOI: 10.5220/0007366501140125. Також доступний у PDF: URL: https://cs.vu.nl/en/Images/ICISSP_2019_47_CR_tcm210-907859.pdf (дата звернення: 25.02.2020).

15. CLAUDETTE project: веб-сайт. URL: http://claudette.eui.eu/ (дата звернення: 25.02.2020).

16. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Article 29 Data Protection Working Party. 2017. 17/EN. WP251rev.01. URL: https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826 (дата звернення: 25.02.2020).

17. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. Commission nationale de l'informatique et des libertés: веб-сайт. 2019. URL: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (дата звернення 14.03.2020).

18. Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC. Commission nationale de l'informatique et des libertés: веб-сайт. URL: https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf (дата звернення 14.03.2020).

19. Principle (b): Purpose limitation. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (дата звернення: 28.02.2020).

20. Opinion 03/2013 on purpose limitation. Article 29 Data Protection Working Party. 2013. 00569/13/EN. WP 203. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (дата звернення: 28.02.2020).

21. Can we use data for another purpose? European Commission: веб-сайт. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en (дата звернення: 28.02.2020).

22. Moerel L., Prins C. On the Death of Purpose Limitation. International Association of Privacy Professionals: веб-сайт. 2015. URL: https://iapp.org/news/a/on-the-death-of-purpose-limitation/ (дата звернення: 28.02.2020).

23. Verma A. Why is Big Data Analytics So Important? Whizlabs: веб-сайт. 2018. URL: https://www.whizlabs.com/blog/big-data-analytics-importance/ (дата звернення: 28.02.2020).

24. Arnbak A. Pseudonymisation: big data opportunities in the GDPR. De Brauw Blackstone Westbroek: веб-сайт. URL: https://www.debrauw.com/legalarticles/pseudonymisation-big-data-opportunities-in-the-gdpr/?output=pdf (дата звернення: 28.02.2020).

25. Наведено за: Osborne C. GDPR's silver lining: Data-driven AI and innovation in the enterprise. ZDNet: веб-сайт. 2018. URL: https://www.zdnet.com/article/gdprs-silver-lining-a-catalyst-for-machine-learning-artificial-intelligence-in-the-enterprise/ (дата звернення: 28.02.2020).

26. Ausloos J. GDPR Transparency as a research method. University of Amsterdam - Institute for Information Law (IViR). 2019. URL: https://ssrn.com/abstract=3465680 (дата звернення: 28.02.2020).

27. Principle (c): Data minimisation. Information Commissioner’s Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ (дата звернення: 01.03.2020).

28. Data anonymization and GDPR compliance: the case of Taxa 4×35. GDPR.eu: веб-сайт. URL: https://gdpr.eu/data-anonymization-taxa-4x35/ (дата звернення: 01.03.2020).

29. Fair Information Practice Principles. International Association of Privacy Professionals: веб-сайт. URL: https://iapp.org/resources/article/fair-information-practices/ (дата звернення: 01.03.2020).

30. Cavoukian A. Privacy by Design: The 7 Foundational Principles. International Association of Privacy Professionals: веб-сайт. URL: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ (дата звернення: 01.03.2020).

31. Senarath A., Arachchilage N.A.G. Understanding Software Developers' Approach towards Implementing Data Minimization. 2018. URL: https://www.researchgate.net/publication/326851229_Understanding_Software_Developers'_Approach_towards_Implementing_Data_Minimization (дата звернення: 01.03.2020).

32. Senarath A., Arachchilage N.A.G. Why developers cannot embed privacy into software systems? EASE'18. 2018. Christchurch, New Zealand. URL: https://arxiv.org/ftp/arxiv/papers/1805/1805.09485.pdf (дата звернення: 01.03.2020).

33. Principle (d): Accuracy. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/ (дата звернення: 01.03.2020).

34. Marschall K. General Data Protection Regulation: data accuracy in practice. Datenschutz Praxis: веб-сайт. URL: https://www.datenschutz-praxis.de/fachartikel/general-data-protection-regulation-data-accuracy-in-practice/ (дата звернення: 04.03.2020).

35. Accuracy. International Association of Privacy Professionals: веб-сайт. URL: https://iapp.org/resources/article/accuracy/ (дата звернення: 04.03.2020).

36. Tang A. AI or GDPR? Isaca Now Blog: веб-сайт. 2019. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/ai-or-gdpr (дата звернення: 04.03.2020).

37. Principle (e): Storage limitation. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ (дата звернення: 04.03.2020).

38. Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів: Наказ Міністерства юстиції України від 12.04.2012 № 578/5. URL: https://zakon.rada.gov.ua/laws/show/z0571-12 (дата звернення: 04.03.2020).

39. Ritzer C., Filkina N. First multi-million GDPR fine in Germany: €14.5 million for not having a proper data retention schedule in place. Data Protection Report – Norton Rose Fulbright: веб-сайт. 2019. URL: https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/ (дата звернення 20.03.2020).

40. Tidbury N. GDPR, data cemeteries, and million-dollar fines: Deutsche Wohnen SE Case Study. CryptoNumerics: веб-сайт. URL: https://cryptonumerics.com/blog/gdpr-data-cemeteries-and-million-dollar-fines-deutsche-wohnen-se-case-study/ (дата звернення 20.03.2020).

41. Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft. Berliner Beauftragte für Datenschutz und Informationsfreiheit: веб-сайт. 2019. URL: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf (дата звернення 20.03.2020).

42. Brook C. What is Data Integrity? Definition, Best Practices & More. Digital Guardian's Blog: веб-сайт. URL: https://digitalguardian.com/blog/what-data-integrity-data-protection-101 (дата звернення: 05.03.2020).

43. Managing data confidentiality. Secure UD – University of Delaware: веб-сайт. URL: https://www1.udel.edu/security/ (дата звернення: 05.03.2020).

44. Директива № 95/46/ЕС Європейського парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242 (дата звернення: 05.03.2020).

45. Security. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ (дата звернення 05.03.2020).

46. Controllers and processors. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/ (дата звернення 05.03.2020).

47. Scarfone K., Jansen W., Tracy M. Confidentiality, Integrity, and Availability. NIST Special Publication 800-123, Guide to General Server Security. MDN Web Docs: веб-сайт. 2018. URL: https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Confidentiality,_Integrity,_and_Availability (дата звернення 05.03.2020).

48. Personal data breaches. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ (дата звернення 05.03.2020).

49. Resolución De Procedimiento Sancionador. Procedimiento Nº: PS/00358/2019. Agencia Española de Protección de Datos. 2019. URL: https://www.aepd.es/es/documento/ps-00358-2019.pdf (дата звернення 16.03.2020).

50. Accountability and governance. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/ (дата звернення 05.03.2020).

51. Torre L. F. What does "accountability" mean under EU Data Protection law? Medium: веб-сайт. 2019. URL: https://medium.com/golden-data/what-does-accountability-mean-under-eu-data-protection-law-af630e40648b (дата звернення 07.03.2020).

52. A Guide to Privacy by Design. Agencia Española de Protección de Datos. 2019. URL: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf (дата звернення 07.03.2020).

53. Privacy Policy. Ukraine International Airlines: веб-сайт. 2019. URL: https://www.flyuia.com/ua/en/information/rules-and-regulations/privacy-policy (дата звернення 22.04.2020).

54. Звіт корпорації Майкрософт про конфіденційність. Microsoft: веб-сайт. 2019. URL: https://privacy.microsoft.com/uk-UA/privacy-report (дата звернення 22.04.2020).

55. Закон України від 01.06.2010 № 2297-VI «Про захист персональних даних». Законодавство України: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення 22.04.2020).

56. Черніков А. Чому закон про захист персональних даних неможливо виконати. Економічна правда: веб-сайт. 2012. URL: https://www.epravda.com.ua/publications/2012/01/27/314140/ (дата звернення 22.04.2020).

57. Закон України від 03.07.2013 № 383-VII «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних». Законодавство України: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/383-18 (дата звернення 22.04.2020).

58. GDPR та Україна: quo vadis? Василь Кісіль і Партнери: веб-сайт. URL: http://www.kisilandpartners.com/ua/publications/articles/gdpr_ta_ukraina_quo_vadis/(дата звернення 22.04.2020).

59. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014. Законодавство України: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення 22.04.2020).

60. Постанова Кабінету Міністрів від 25 жовтня 2017 р. № 1106 «План заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони». Законодавство України: веб-сайт. URL:

https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF (дата звернення 22.04.2020).

61. Анонс круглого столу: «Рекомендації щодо наближення закону України «Про захист персональних даних» до нового загального регламенту ЄС про захист персональних даних». Уповноважений Верховної Ради України з прав людини: веб-сайт. URL: http://www.ombudsman.gov.ua/ua/all-news/pr/231018-cq-anons-kruglogo-stolu-rekomendatsiii-schodo-nablizhennya-zakonu-ukraiin/ (дата звернення 22.04.2020).

62. European Union and Council of Europe working together to strengthen the Ombudsperson's capacity to protect human rights. Council of Europe Office in Ukraine: веб-сайт. URL: https://www.coe.int/en/web/kyiv/ombudsperson#{%2257424131%22:[1]} (дата звернення 22.04.2020).

63. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. Київ. 2015. 220 с. URL: https://rm.coe.int/168059920c (дата звернення 22.04.2020).

64. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. Законодавство України: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення 22.04.2020).

65. Кримінальний кодекс України від 05.0.2001 № 2341-III. Законодавство України: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення 22.04.2020).

66. Terwangne C. Internet Privacy and the Right to Be Forgotten/Right to Oblivion. Monograph «VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet». Universitat Oberta de Catalunya. 2012. URL: http://www.crid.be/pdf/public/7064.pdf (дата звернення 22.03.2020).

67. Politou E., Alepis E., Patsakis C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of Cybersecurity. 2018. Vol. 4, Issue 1. DOI: https://doi.org/10.1093/cybsec/tyy001 (дата звернення 22.03.2020).

68. Krulwich R. Is The 'Right To Be Forgotten' The 'Biggest Threat To Free Speech On The Internet'? NPR: веб-сайт. 2012. URL: https://www.npr.org/sections/krulwich/2012/02/23/147289169/is-the-right-to-be-forgotten-the-biggest-threat-to-free-speech-on-the-internet (дата звернення 22.03.2020).

69. Mendonca-Richards A. Using data protection law to defend your reputation: what about the new Data Protection Bill? Farrer & Co: веб-сайт. 2017. URL: https://www.farrer.co.uk/news-and-insights/using-data-protection-law-to-defend-your-reputation-what-about-the-new-data-protection-bill/ (дата звернення 22.03.2020).

70. Reventlow N. J. Can the GDPR and Freedom of Expression Coexist? AJIL Unbound. 2020. Vol. 114. P. 31-34. URL: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/can-the-gdpr-and-freedom-of-expression-coexist/C8C5B4F0BFF87B9CAD78ED4BDDF27BBC/core-reader (дата звернення 22.03.2020).

71. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Judgment of the Court (Grand Chamber). 13 May 2014. Case C-131/12. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (дата звернення 22.03.2020).

72. Google LLC v. Commission nationale de l'informatique et des libertés (CNIL). Judgment of the Court (Grand Chamber). 24 September 2019. Case C-507/17. URL: http://curia.europa.eu/juris/document/document.jsf?text=erasure&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2938101#ctx1 (дата звернення 22.03.2020).

73. Mahieu R. L. P., Asghari H., Eeten M. Collectively exercising the right of access: individual effort, societal effect. Internet Policy Review – Journal on internet regulation. 2018. Vol., Issue 3. DOI: 10.14763/2018.3.927 (дата звернення 24.03.2020).

74. Charter of Fundamental Rights of the European Union. Official Journal of the European Union. 26.10.2012. C 326. Vol. 55. URL: http://data.europa.eu/eli/treaty/char_2012/oj (дата звернення 24.03.2020).

75. Right of access. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ (дата звернення 24.03.2020).

76. Personal Information Leakage by Abusing the GDPR "Right of Access"/ Martino M.D. and others. Proceedings of the Fifteenth Symposium on Usable Privacy and Security. Santa Clara, CA. 2019. URL: https://www.usenix.org/system/files/soups2019-di_martino.pdf (дата звернення 24.03.2020).

77. Aktuelle Kurz-Information 22: Identifizierung bei der Geltendmachung von Betroffenenrechten. Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD). 2018. URL: https://www.datenschutz-bayern.de/datenschutzreform2018/aki22.html (дата звернення 24.03.2020).

78. Exemptions. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/ (дата звернення 24.03.2020).

79. 'I want my data!'- Recent Developments in the Right to Access One's Personal Data. Stibbe: веб-сайт. URL: https://www.stibbe.com/en/news/2019/august/i-want-my-data-recent-developments-in-the-right-to-access-ones-personal-data (дата звернення 24.03.2020).

80. Elteste U., Quathem K. German court decides on the scope of GDPR right of access. Covington & Burling LLP: веб-сайт. 2019. URL: https://www.insideprivacy.com/international/european-union/german-court-decides-on-the-scope-of-gdpr-right-of-access/ (дата звернення 24.03.2020).

81. RE v. European Commission. Judgment of The General Court (Ninth Chamber, Extended Composition). 14 February 2019. Case T-903/16. URL:

http://curia.europa.eu/juris/document/document.jsf;jsessionid=40A93D9079FBCAED4308D5B6D2E31F8B?text=&docid=210763&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=12795709#Footnote1 (дата звернення 26.03.2020).

82. College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer. Judgment of The Court (Third Chamber). 7 May 2009. Case C-553/07. URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=481465 (дата звернення 26.03.2020).

83. Rights related to automated decision making including profiling. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ (дата звернення 28.03.2020).

84. Big data, artificial intelligence, machine learning and data protection. Data Protection Act and General Data Protection Regulation. Information Commissioner's Office: веб-сайт. URL: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (дата звернення 28.03.2020).

85. The Value of Big Data and the Internet of Things to the UK Economy. Report for SAS. Centre for Economics and Business Research. 2016. URL: https://www.sas.com/content/dam/SAS/en_gb/doc/analystreport/cebr-value-of-big-data.pdf (дата звернення 28.03.2020).

86. Sloan M. Profiling and Automated Decision Making under the GDPR. Brodies LLP: веб-сайт. 2017. URL: https://brodies.com/blog/ip-technology/profiling-and-automated-decision-making-under-the-gdpr/ (дата звернення 28.03.2020).

87. Oleksiuk A. How to Train an AI with GDPR Limitations. Intellias: веб-сайт. 2019. URL: https://www.intellias.com/how-to-train-an-ai-with-gdpr-limitations/ (дата звернення 28.03.2020).

88. Клюс М. Privacy by design: як використовують GDPR в AI технологіях. Legal IT group: веб-сайт. 2019. URL: https://legalitgroup.com/privacy-by-design/ (дата звернення 28.03.2020).

89. Nederlands Juristen Comité Voor de Mensenrechten and others v. the State of the Netherlands. The Hague District Court. 05.02.2020. Case C/09/550982. URL: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 (дата звернення 30.03.2020).