Міністерство освіти і науки
Національний університет «Києво-Могилянська Академія»
Факультет правничих наук
Кафедра міжнародного та європейського права

Магістерська робота

освітній ступінь — магістр

на тему: «**НАБЛИЖЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ ПРО ЦИФРОВИЙ МАРКЕТИНГ НА ШЛЯХУ ДО ЧЛЕНСТВА В ЄС»**

«Harmonisation of the Ukrainian legislation on digital marketing on the way to membership in the EU»

Виконала: студентка 2-го року навчання
Спеціальності 081 Право
Парфенюк Юлія Станіславівна

Керівник Петров Р.А., професор, доктор юридичних наук, доктор філософії

Рецензент Петров Р. А.

Магістерська робота захищена
з оцінкою «_____»
Секретар ЕК _____
«____» _____20 __ р.

КИЇВ – 2023

Декларація академічної доброчесності

Я, Парфенюк Юлія, студентка 2 року навчання магістерської програми за спеціальністю 081 «Право» факультету правничих наук НаУКМА:

- підтверджую, що написана мною магістерська робота на тему «НАБЛИЖЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ ПРО ЦИФРОВИЙ МАРКЕТИНГ НА ШЛЯХУ ДО ЧЛЕНСТВА В ЄС» відповідає вимогам академічної доброчесності та не містить порушень, передбачених пунктами 3.1.1-3.1.6 Положення про академічну доброчесність здобувачів НаУКМА від 07.03.2018 року, зі змістом якого я ознайомлена;
- підтверджую, що надана мною електронна версія роботи є остаточною і готовою до перевірки;
- згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності, у будь-який спосіб, у тому числі порівняння змісту роботи та формування звіту подібності за допомогою електронної системи Unicheck;
- даю згоду на архівування моєї роботи в репозитаріях та базах даних університету для порівняння цієї та майбутніх робіт.

10 травня 2023 року  Парфенюк Ю.С.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

GDPR	General data protection regulation
EDPB	European Data Protection Board
UCPD	Unfair Commercial Practices Directive
CJEU	Court of Justice of the European Union
TFEU	Treaty on the Functioning of the European Union
DMA	Digital Markets Act
DSA	Digital Services Act
ICC Code	ICC Advertising and Marketing Communications Code
EASA	The European Advertising Standards Alliance
EDAA	European Interactive Digital Advertising Alliance

ВСТУП

Цифровий маркетинг, або ж іншими словами, способи комунікації з цільовою аудиторію з використанням цифрових технологій, розвивається із неабиякою швидкістю. Поведінкова реклама та таргетування на веб-сайтах та у соціальних мережах — одні з найбільш ефективних способи здійснення цифрового маркетингу.

Як зазначає CEO TrustArc Inc., технологічної компанії з дотримання конфіденційності, Кріс Бабел [Chris Babel]: «*Сайт — це вже не одна компанія. Сайт — це десятки чи сотні компаній, які знають, де ви знаходитесь та що ви переглядаєте*» [1].

Згідно з дослідженням Всеукраїнської рекламної асоціації, ринок інтернет реклами у проміжку між 2020 – 2021 рр. зріс на 48% та за підсумками 2021 року становить майже 30 млн. гривень, а в 2022 році прогнозувалось фактичне зростання щонайменше на 34% та збільшення оцінки майже до 40 млн. гривень [2]. Більше того, згідно з дослідженням "Digital 2021: Ukraine" від компанії We Are Social і платформи Hootsuite, на початку 2021 цифрова реклама складала більше половини (близько 60%) усієї реклами в Україні [3].

Стрімке зростання високоприбуткової індустрії цифрового маркетингу є проявом розвитку та нових можливостей для її гравців, однак, водночас, зростає і кількість юридичних викликів. Серед таких викликів є гармонізація існуючого законодавства України із законодавством, що існує в Європейському Союзі та її державах-членах, а також наслідування найкращих світових практик у регулюванні цифрового маркетингу.

Для цілей дослідження правового регулювання цифрового маркетингу, у даній роботі пропонується правовий аналіз найбільш поширених практик здійснення цифрової реклами, використання cookies та таргетингу. Аналіз вимог щодо використання, збору та обробки персональних даних становитиме основу для окреслення меж допустимості відслідковування та аналізу поведінки користувачів для маркетингових цілей у соціальних мережах, на веб-сторінках та у додатках.

Актуальність дослідження. Україна на шляху до повноцінного членства повинна здійснити низку реформ та адаптувати українське законодавство відповідно

до вимог ЄС. Серед таких вимог містяться, зокрема, забезпечення відповідного рівня захисту персональних даних та створення безпечного цифрового середовища. Оскільки в мережі Інтернет особа існує як сукупність персональних даних, захист таких даних стає невід'ємною частиною захисту фундаментальних прав особи.

Практичне значення даної роботи полягає у здійсненні аналізу законодавства ЄС на предмет регулювання цифрового маркетингу та цифрової реклами, як його основної складової, а також відповідного аналізу українського законодавства на предмет відповідності вимогам ЄС. Результати аналізу слугуватимуть правовим орієнтиром для бізнесу, чия маркетингова стратегія побудована на сучасних тенденціях.

Теоретичне значення даної роботи полягає у дослідженні та висвітленні актуальних проблем регулювання цифрового маркетингу у законодавстві України крізь призму законодавства ЄС. Дане дослідження слугуватиме новим підходом у інтерпретації та аналізі правового регулювання цифрового маркетингу в Україні.

Мета даної роботи полягає у виокремленні основних кроків у наближенні законодавства України про цифровий маркетинг на шляху до членства в ЄС.

Серед основних завдань даної роботи варто виокремити:

- характеристика законодавства ЄС у сфері цифрового маркетингу;
- характеристика національного законодавства у сфері цифрового маркетингу;
- виділення основних тенденцій гармонізації законодавства України про цифровий маркетинг на шляху до членства в ЄС.

Предметом дослідження у даній роботі є європейське та національне рекламне законодавство, нормативно-правові акти, що стосуються правил збору, обробки та використання персональних даних, здійснення електронної комерції, захисту прав споживачів, а також механізми контролю та відповідальності за порушення законодавства.

Об'єкт дослідження. Об'єкт дослідження є суспільні відносини, щодо забезпечення правомірності здійснення цифрового маркетингу на території ЄС та в Україні.

Методи. Дослідження здійснено за допомогою загальнонаукових та спеціально наукових методів.

За допомогою методу діалектики вдалось дослідити європейське та національне законодавство, а також інші нормативно правові акти які здійснюють регулювання сфери цифрового маркетингу в ЄС та Україні.

Аналіз та систематизацію дослідженого законодавства було здійснено за допомогою аналітичного методу.

Формально-юридичний метод застосовано для тлумачення норм та судової практики, а метод порівняння — для встановлення спільних та відмінних підходів у регулюванні сфери цифрового маркетингу в ЄС та Україні.

Теоретичну основу дослідження склали праці таких українських та іноземних науковців: Харитонової О.,Берназ-Лукавецька О., Самагальської Ю., Бем М., Городиський І., Саттон Г., Родіоненко О.

Наукове та практичне значення дослідження. Напрацювання, що містяться у цій роботі можуть бути використанні для (1) дослідження регулювання цифрового маркетингу в майбутньому (2) проведення аналізу розвитку законодавства України в сфері цифрового маркетингу.

Структура роботи. Магістерська робота складається із вступу, трьох розділів, восьми підрозділів, двох частин підрозділів, проміжних висновків, загальних висновків та списку використаних джерел. Загальний обсяг дослідження - 70 сторінок, у тому числі список використаних джерел (97 найменувань) складає 12 сторінок.

РОЗДІЛ 1. ПРАВОВЕ РЕГУЛЮВАННЯ ЦИФРОВОГО МАРКЕТИНГУ В ЄС

1.1. Загальна характеристика законодавства ЄС у сфері цифрового маркетингу

Перш ніж переходити до регулювання, варто більш детально окреслити основні правові виклики, що існують в ЄС у зв'язку зі здійсненням цифрової реклами та дослідження поведінки користувачів за допомогою інструментів цифрового маркетингу.

Як стверджують автори доповіді від Європейської Комісії «Дослідження впливу нещодавніх досягнень в цифровій рекламі на приватність, паблішерів та рекламодавців»[1] індустрія цифрової реклами спирається на неконтрольований масив персональних даних, відстеження та створення масштабних профілів користувачів, вплив на їх поведінку, в той час як користувачі не мають достатнього контролю над своїми персональними даними, що явно не відповідає принципу пропорційності та призводить до порушення фундаментальних прав людини [4. с. 9-10]. Автори доповіді надалі в дослідженні влучно цитують почесну професорку права та цифрових технологій Амстердамського університету Наталі Хельбергер [*Natali Helberger*]: «*Тоді як споживачі історично сприймали рекламу як засіб отримання безкоштовного або пільгового доступу до контенту у ЗМІ, втрата контролю над персональними даними та конфіденційністю не була частиною угоди*» [5].

На додаток до юридичних викликів, сучасні способи за засоби ведення цифрового маркетингу піднімають багато етичних питань, серед яких найбільш актуальним є застосування поведінкової реклами (англ. *behavioral advertising*). Поведінкова реклама працює на великій кількості персональних даних, в тому числі чутливих, та спрямована на свідомість споживача. Відмінність поведінкової реклами в цифровому просторі та офлайн полягає в тому, що в першому випадку користувач фактично не може контролювати кількість такої реклами, цілковито відмовитись від

[1] Переклад здійснено мною, Парфенюк Юлією.

неї чи «попередити» її появу. Показовими є результати досліджень відповідно до яких, до 40% онлайн-реклами, яка відображалась перед вразливими користувачами в Іспанії була таргетною [6]. Особливу увагу приділяють таргетній рекламі направленій на осіб із важкими захворюваннями такими як рак, ВІЛ, інфекційні хвороби, генетичні порушення [7. с. 42].

Ще одну етичну проблему поведінкової реклами пов'язують із всебічним відстеженням поведінки користувача. Зокрема, завдяки збиранню даних із різних девайсів користувача та обміну такими даними між різними застосунками та платформами, створюється його цілісний профіль, що дозволяє підібрати надзвичайно релевантну рекламу, та, водночас, відстежувати такого користувача щосекунди.

Окрім того, сучасні технологічні інструменти дозволяють на основі такого профілю передбачити поведінку користувача в режимі реального часу та фактично продати користувача на рекламній біржі (англ. *real time bidding* або «RTB»). Ірланська Рада Громадських Свобод називає RTB найбільшим світовим порушенням захисту даних, та на підтвердження наводить статистику за 2022 рік: лише в Європі персональні дані кожної особи передаються на рекламні біржі 376 разів на день, а щорічна кількість розкриття таких даних в Європі становить 71 трильйон разів [8]. Таким чином, відбувається тотальне розмиття права на приватність, дискримінація та так звана втрата особистості [7. с. 11].

Ще одна надзвичайно актуальна юридично-етична проблема виникає через використання так званих практик темних патерів (анг. *dark patterns*). Темні патери – це налаштування інтерфейсів, додавання фічів та застосування таких технік створення дизайнів інтерфейсів, які маніпулятивно спонукають споживача вчинити певні дії.

Норвезька рада споживачів у своїй доповіді щодо впливу темних патерів на права користувачів влучно підсумовує дослідження всесвітньовідомого професора Вудроу Харцога й зазначає: «*Замість того, щоб приймати рішення раціонально, індивіди мають тенденцію піддаватися впливу різноманітних когнітивних упереджень, часто не усвідомлюючи цього»* [9].

З юридичної точки зору у цифровому просторі найбільшої уваги потребують темні патери, які застосовуються для «виманювання» у користувачів згоди на збір персональних даних та маніпуляції за допомогою дефолтних налаштувань.

***

На сьогодні в ЄС відсутній уніфікований нормативно – правовий акт, який би комплексно регулював здійснення цифрового маркетингу та враховував особливу правову природу таких відносин. Водночас, можна стверджувати, про те, що законодавство ЄС, яке застосовується до регулювання цифрового маркетингу є одним із найбільш врегульованих у світі.

Основу правової регламентації цифрового маркетингу в ЄС становлять GDPR та ePrivacy Directive. За своєю юридичною природою GDPR є регламентом, він поширює свою дію на всіх членів ЄС та є обов'язковим до виконання, в той час як ePrivacy Directive встановлює основні цілі, які кожній державі-члену необхідно досягнути, однак надає їм дискрецію у визначенні шляхів їх досягнення [10]. Враховуючи основну проблематику цифрової реклами — надмірне та неконтрольоване використання та поширення персональних даних, саме GDPR та ePrivacy Directive покликані вирішити ці проблеми. GDPR закріплює що таке персональні дані, правила, принципи та правові підстави їх збирання, обробки та використання в цілях цифрового маркетингу, а також встановлює механізм відповідальності за порушення. Стаття 2 GDPR окреслює сферу його застосування, а саме: «*GDPR поширюється на опрацювання персональних даних повністю чи частково із застосуванням автоматизованих засобів та до опрацювання персональних даних із застосуванням неавтоматизованих засобів, які формують частину картотеки або призначені для внесення до картотеки*»[2] [11].

В свою чергу, сфера застосування ePrivacy Directive звужена до регулювання електронної комунікації, вона доповнює GDPR та застосовується як *lex specialis* до GDPR [12. с.12]. ePrivacy Directive називають ще "Cookies law", оскільки директива встановлює вимоги до згоди на обробку даних через так звані банери cookies. Більш

[2] Офіційний переклад на сайті Верховної Ради України: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

детальний огляд та практику кожного з документів GDPR та ePrivacy Directive буде розглянуто в Розділі 1.2.

Надмірне використання персональних даних користувачів та застосування нечесних комерційних практик для впливу на прийняття ними рішень порушує також законодавство ЄС про захист прав споживачів. UCPD містить ряд положень, які забороняють маніпулятивну комерційну практику (стаття 6 UCPD) та введення в оману споживача (стаття 7 UCPD) задля отримання згоди на обробку персональних даних, а також використання так званих «агресивних практик» [4. с. 243], тобто методів здійснення реклами, які суперечать етичним та моральним принципам, а також порушують права споживачів [13]. В цифровому середовищі маркетингу UCPD застосовується як додаткове регулювання персоналізації реклами та попередження використання персональних даних у недобросовісний спосіб [4. с. 244]. Як зазначається у Керівництві по застосуванню та інтерпретації UCPD:

> "*Порушення продавцем GDPR або ePrivacy Directive саме по собі не завжди призводить до порушення UCPD. Однак порушення конфіденційності та захисту даних як такі, слід враховувати під час оцінки загальної несправедливості комерційної практики відповідно до UCPD, особливо в ситуації, коли продавець обробляє дані споживача з порушенням вимог щодо конфіденційності та захисту даних, наприклад, для цілей прямого маркетингу чи будь-якої іншої комерційні цілі, як-от створення особистого профілю, утворення ціни під кожного окремого споживача або додатків, які обробляють великий масив даних*" [14. с. 19].

Тут варто зазначити, що вище перелічені приклади можливих порушень UCPD самі по собі є вартісними інструментами, які доступні лише великим платформам. Саме тому левову частку ринку цифрового маркетингу займають тех-гіганти. Домінуюча позиція дає їм змогу не лише контролювати персональні дані більшості наявних в ЄС користувачів цифровими послугами, а й встановлювати власне регулювання. Тому на додаток до порушень законодавства ЄС про захист

персональних даних та прав споживачів виникають питання й щодо порушення антиконкурентного регулювання ЄС.

Зокрема статті 102 та 103 TFEU слугують правовою основою боротьби із антиконкурентною практикою в сфері цифрової реклами [4. с. 233].

Таким чином, можна зробити проміжний висновок, що законодавство ЄС комплексно регулює здійснення цифрового маркетингу та направлене на всебічний захист фундаментальних прав споживачів.

Як приклад комплексного підходу, варто звернути увагу на Рішення Апеляційного суду Берліна (Kammergericht Berlin) у справі проти Facebook. Зокрема, суд встановив, що функція Facebook «Знайти друзів» є оманливою для споживача, порушує GDPR та антимонопольне законодавство. Алгоритм «Знайти друзів» передбачає можливість вже зареєстрованому користувачу Facebook надати доступ до своїх контактів, далі Facebook аналізує контакти (друзів) користувача, визначає тих, хто ще не зареєстрований та пропонує користувачу надіслати запрошення на реєстрацію у Facebook. На думку суду, такий алгоритм порушує як права вже наявного користувача Facebook, оскільки сам користувач не надає явної згоди на обробку його персональних даних (адресної книги), а також тих осіб, кому приходять запрошення приєднатись до Facebook. В останньому випадку, суд стверджує, що такі запрошення варто розглядати як комерційні, а не приватні повідомлення, які надсилаються особі без її згоди [15]. Новелою у рішенні суду є те, що фактично порушується саме законодавство про захист персональних даних, але правова регламентація зводиться до того, що таке порушення призвело до антиконкурентних дій [16].

Ця справа стала резонансною і поділила експертів та юристів на тих, хто підтримує позицію суду щодо комплексного застосування законодавства про захист персональних даних разом із антиконкурентним законодавством (таку ж позицію поділяє CJEU [16]) , та тих, хто наполягає на їх чіткому розмежуванні [17].

Допоки теоретичні дискусії тривали, Європейська Комісія нещодавно прийняла DMA та DSA, акти ЄС, які до існуючого антимонопольного регулювання додають цілковито нові правила щодо захисту прав споживачів та використання персональних

даних. Сама Європейська Комісія називає їх політичними угодами, що встановлюють принципово інші правила гри для технічних гігантів та основною метою яких є створення безпечного цифрового середовища [19].

Як зазначають експерти Digital Security Lab: *«У результаті Інтернет-буму початку нового тисячоліття виникла група компаній, що контролюють важливі екосистеми у світовій цифровій економіці […] [такі компанії] часто оперують системами алгоритмів, якими можуть маніпулювати для власних цілей або самі платформи, або окремі користувачі»* [19].

Надалі екосистема цифрової реклами належатиме саме тим платформам та паблішерам, які збирають дані із найбільш розгалужених та популярних мереж та сайтів. До таких компаній належать Meta (соціальні мережі та засоби комунікації), Amazon (e-commerce), Alphabet (Google та YouTube), Yahoo! (інтернет пошук та реклама), Apple (інноваційні технології) [4. с. 19].

DMA та DSA містять низку важливих норм, які стосуються згоди на обробку персональних даних, аналізу й використання персональних даних для цілей таргетингу, надання згоди на подальшу передачу даних третім особам, а також ряд due diligence обов'язків, обов'язків щодо проведення заходів із оцінки ризиків пов'язаних із застосуванням алгоритмів, створення конкурентного середовища в сфері цифрової реклами [7, с. 12].

Отже, законодавство ЄС стрімко адаптується до неузгодженостей та правових викликів. Прикладом цього можуть слугувати DMA та DSA, які приймались для забезпечення балансу в індустрії цифрової економіки, де ключову роль відіграють великі компанії.

Окрім основного регулювання, беручи до уваги динамічний характер індустрії цифрової реклами, а також значний вплив великих корпорацій-монополістів на неї, на рівні ЄС розвинені органи саморегулювання, які розробляють кодекси та рекомендації, в тому числі щодо цифрової реклами.

Органи саморегулювання реагують на скарги споживачів, конкурентів чи просто зацікавлених сторін, а також можуть за власною ініціативою провести перевірку в рамках виконання своїх функцій з моніторингу. Скарги розглядають журі,

або комітет із розгляду скарг на вимогу Секретаріату органу саморегулювання. Оскільки органи саморегулювання не мають повноважень накладати штрафи, найбільш ефективним засобом реагування є вимога привести у відповідність із законодавством рекламу чи маркетингову стратегію, або ж відмовитись від неї. Додатковий вплив на порушника має й факт того, що такі порушення публікуються й, відповідно, створюється додатковий ефект громадського осуду [20. с. 14-16]

Серед таких органів саморегулювання варто виділити EASA, яка об'єднує 42 організації із яких 28 органів рекламної саморегуляції, представлених у різних європейських країнах [21]. На рівні із EASA діє EDAA, основною метою діяльності якої є реалізація Європейської програми саморегуляції цифрової реклами (поведінкової реклами) («Програма»). Програма розроблена на пан'Європейському рівні у співпраці із органами ЄС та представниками індустрії та є обов'язковою для всіх підписантів.

Окрім того, компанії-підписанти зобов'язані в рамках виконання Програми пройти самосертифікацію у одного із авторизованих органів сертифікації протягом 6 місяців з дати приєднання до Програми. За результатами самосертифікації компанія отримує Trust Seal (печатку довіри). Trust Seal є показником високого рівня професійності та клієнт орієнтованості компаній, що використовують цифрову рекламу. Список таких компаній відкритий, до них належать й вже згадані Google, Amazon, Facebook, Microsoft. Станом на 2022 рік у Програмі брали участь 121 компанія [22]. Програма містить 7 ключових принципів здійснення цифрової реклами:

- Повідомлення
- Вибір користувача
- Безпека даних
- Сегментування чутливих даних
- Навчання
- Дотримання та виконання
- Перегляд [23].

В рамках реалізації принципу повідомлення користувачів щодо факту збору їх персональних даних для цілей поведінкової реклами, компанія зобов'язується проставляти на кожному рекламному банері чи повідомлені на веб-сторінці іконку із надписом «AdChoices». Натикаючи на таку іконку користувач отримує детальний опис того, як його дані збираються та використовуються, а також опцію відписатись від рекламних повідомлень (*opt-out*).

Окрім того, важливим проєктом EDAA є YourOnlineChoices («YOC»). YOC — інструмент, що дає змогу користувачам дізнатись про те, як працює поведінкова реклама, збираються їх персональні дані та як функціонують cookies. За допомогою цього інструменту користувач може в один клік отримати інформацію про те, які компанії використовують його персональні дані та навіть здійснити їх налаштування. Водночас, як зазначається на сторінці проєкту, його метою є імплементація найкращих бізнес-практик, а не створення юридичних передумов для дотримання нормативно-правових актів ЄС [24].

Отже, підсумовуючи, органи саморегулювання об'єднують учасників індустрії цифрового маркетингу та за підтримки ЄС створюють додаткове регулювання. Акти органів саморегулювання є обов'язковими для членів-підписантів, а Trust Seal слугує своєрідним показником якості сервісів компанії. Норми, що містяться в таких актах повторюють загальні вимоги, що містяться в регулюванні ЄС, а також деталізують їх. Як і на рівні ЄС, так і на рівні органів саморегулювання основну увагу приділено регулюванню використання персональних даних у маркетингових та рекламних цілях й захисту прав споживачів.

Більш детальний аналіз заслуговує ICC Code, який можна вважати основою наступних документів органів саморегуляції, а також формальним вираженням найкращих бізнес-практик у сфері цифрового маркетингу. З часу його першого прийняття у 1937 році, ICC Code був змінений та доповнений десяток разів, відповідаючи викликам нових часів. На даний час, ICC Code містить цілий розділ присвячений регулюванню цифровому маркетингу (Розділ C), водночас інші розділи також застосовуються до реклами в цифровому середовищі [25].

Уваги заслуговують положення, які відсутні у вищезгаданих директивах та регулюваннях. Зокрема, статтею 5 ICC Code заборонено так звані тактики високого тиску (англ. *high pressure tactics*), тобто використання засобів впливу на споживача, які він може сприйняти як переслідування, а споживачі не повинні бути примушені підписуватись на пропозиції, попередньо не ознайомившись з умовами договору. Стаття 6 забороняє рекламні повідомлення у блогах, новинних групах, веб-сторінках та інших «публічних місцях» без надання явної чи неявної згоди такої сторінки чи веб-сайту.

Актуальною є норма статті 10, що встановлює дозволені межі демонстрації реклами та маркетингових повідомлень під час використання інтерактивних медіа: «[демонстрація] не повинна заважати звичайному використанню інтерактивних медіа чи [звичайному за такого використання] досвіду користувача» [25]. В контексті використання персональних даних ICC Code встановлює наступні обмеження та заборони. У статті 22 ICC Code надано визначення поведінкової реклами, відповідно до якого практика використання поведінкової реклами включає збір даних про користувача для подальшого створення його профілю, сегментування такого профілю та представлення реклами відповідно до інтересів користувача. Це стосується рекламних операцій на комп'ютері, у налаштуваннях мобільних пристроїв, відео чи ТБ, соціальних мереж або IoT, та включає відстеження та таргетування на різних пристроях [25].

Використання поведінкової реклами дозволяється тільки у випадку чіткого та ясного інформування користувача щодо типу даних які збираються та способу їх використання, а також повідомлення про те, як користувач може відмовитись від обробки даних для цілей такої реклами. Водночас, забороняється використовувати чутливі дані для налаштування поведінкової реклами, а у випадках передбачених застосовним законодавством, використання чутливих даних для цілей поведінкової реклами дозволяється лише у випадку надання явної згоди користувача [25].

У окрему статтю виділено норму щодо використання геолокації користувача. Зокрема, передбачено обов'язок надавати детальну інформацію щодо способів та шляхів збирання геолокаційних даних, а також заборону «обходити» згоду

користувача на збір геолокаційних даних шляхом використання інших способів, ніж ті, про які проінформований користувач.

ICC Code містить також важливе регулювання щодо перехресного відстеження пристроїв (*Cross-device tracking*), не включене в жодний нормативний документ ЄС. Якщо користувач відмовляється від отримання рекламних повідомлень, відписується і забороняє використовувати його персональні дані на одному пристрої, то така його відмова поширюється й на інші пристрої.

Отже, органи саморегулювання в ЄС здійснюють вагомий внесок у встановлення допустимих меж здійснення цифрового маркетингу та сприяють захисту фундаментальних прав користувачів. ICC Code — взірець найактуальнішого регулювання на якому ґрунтуються більшість наступних кодексів у країнах-членах ЄС.

Підсумовуючи вищевикладене щодо загальної характеристики законодавства ЄС в сфері цифрового маркетингу, на мою думку, ЄС є прикладом збалансованого регулювання, яке пропорційно втручається у індустрію в тій мірі, аби захистити фундаментальні права користувачів. Багатоаспектність самої індустрії цифрового маркетингу призводить до потреби здійснювати крос-регулювання, тобто встановлювати взаємопов’язані норми з декількох законодавчих сфер, основу якого становить законодавство в сфері захисту персональних даних. Органи саморегулювання виступають своєрідним діалогом між законодавчими органами ЄС, представниками індустрії та користувачами, а їх діяльність направлена на поступовий розвиток і впровадження нових технологій в індустрії цифрового маркетингу із сприянням дотриманню прав користувачів та допомозі з реалізацією цих прав.

1.2. GDPR та E-Privacy Directive як основні інструменти регулювання цифрового маркетингу в ЄС

Право на приватність закріплено в ECHR [26] та є фундаментальним, невід'ємним правом, що належить фізичним особам [27]. Право на приватність застосовується й в тих випадках, коли інформація [персональні дані] вже знаходяться у публічному доступі, що, однак, не позбавляє індивіда гарантій, передбачених конвенцією [28]. Аби забезпечити право на приватність на організації покладається кореспондуючий обов'язок здійснювати обробку персональних даних відповідно до норм законодавства ЄС у сфері захисту персональних даних.

Оскільки законодавство ЄС у сфері захисту персональних даних є комплексним та достатньо дослідженим українськими та європейськими науковцями й практиками, у цьому розділі я обмежу коло дослідження до аналізу норм GDPR та E-Privacy Directive, які застосовуються для адресування правових викликів, що постають у зв'язку з обробкою незліченної кількості персональних даних у маркетинговій індустрії та про які згадувалось вище.

1.2.1. Регулювання GDPR щодо захисту персональних даних під час здійснення цифрового маркетингу

GDPR становить фундамент законодавства ЄС у сфері захисту персональних даних, а тому принципи, що містяться в ньому можна вважати основоположними принципами обробки персональних даних.

Принципи GDPR є дечим загальним, що, з однієї сторони, ще не встановлює імперативних правил, однак, з іншої сторони, створює чітке розуміння щодо всього наступного регулювання [29]. Аналіз рішень CJEU та висновків EDPB свідчить про те, що більшість порушень GDPR зводяться до порушень статей, які лише доповнюють та розкривають зміст визначених у статті 5 GDPR принципів.

До таких принципів відносяться:

- законність, правомірність і прозорість (lawfulness, fairness and transparency)

- цільове обмеження (purpose limitation)
- мінімізація даних (data minimisation)
- точність (accuracy)
- обмеження зберігання (storage limitation)
- цілісність і конфіденційність (integrity and confidentiality)
- підзвітність (accountability)

Перший та, на мою думку, найважливіший принцип закріплений у пункті (a) статті 5 GDPR, він є трискладовим та визначений як «законність, правомірність і прозорість». У преамбулі до цього пункту вказується що: «*Фізичні особи повинні бути обізнані про те, що їх персональні дані збирають, використовують, обговорюють або іншим чином опрацьовують […]. Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення щодо опрацювання таких персональних даних були доступними і зрозумілими, з використанням чітких і простих формулювань*» .

На переконання EDPB принцип правомірності є найважливішим принципом, оскільки він забороняє обробку персональних даних у невиправдано згубний, дискримінаційний та оманливий спосіб [30. с. 17]. У контексті здійснення цифрового маркетингу принцип правомірності забороняє застосування практик темних патерів, незалежно від того чи узгоджуються вони з іншими принципами GDPR [30. с. 17].

У маркетинговій сфері часто трапляються випадки, коли політика конфіденційності та повідомлення про використання персональних даних не містять достатньої інформації про контролера персональних даних або згадують лише контролера, хоча насправді передача даних здійснюється до невідомих третіх сторін. Ці інші треті сторони можуть передавати дані своїм власним партнерам-третім сторонам [7. с. 60]. Тому в епоху складних цифрових технологій особливо важливим є принцип прозорості, оскільки суб'єкти, чиї персональні дані збираються та оброблюються, не можуть зрозуміти, для яких цілей, за яких умов та ким обробляються їх дані [7. с. 59].

Однак, EDPB звертає увагу на те, що надання інформації користувачам лише за допомогою терміну "реклама" не є достатнім, щоб повідомити їм про моніторинг їхньої активності з метою таргетної реклами [31. с. 26]. Принцип прозорості вимагає

від контролера надавати інформацію "лаконічно, прозоро, зрозуміло та в легкодоступній формі, використовуючи зрозумілу та просту мову" [32. с. 6-7].

Як приклад такого формулювання EDPB наводить такий опис: "*Ми зберігатимемо Вашу історію покупок і використовуватимемо деталі щодо товарів, які ви раніше придбали, щоб надати вам пропозиції щодо інших товарів, які ми вважаємо вам також можуть бути цікаві*"[33. с. 9].

Відповідно, принцип прозорості вимагає від контролера надання інформації про цілі, способи та мету використання персональних даних у зручний для сприйняття та зрозумілий пересічному користувачу спосіб.

Принцип законності тісно пов'язаний із підставою обробки персональних даних. У статті 8 (2) EHRC встановлено, що персональні дані повинні оброблятись «на основі згоди такої особи, або на іншій законній підставі» [26]. Відповідне положення міститься і в статті 6 GDPR, відповідно до якої будь-яка обробка персональних даних повинна мати «законну підставу» [11]. На додаток, в GDPR наведено вичерпний перелік підстав обробки персональних даних:

- згода
- необхідність виконання договору,
- необхідність виконання юридичних обов'язків
- необхідність захисту життєво важливих інтересів
- необхідність виконання завдань в публічних інтересах чи в якості публічної особи,
- законний інтерес контролера чи третьої особи [11].

Встановлення однієї із цих підстав повинно відбутись до початку обробки персональних даних [34. с. 17]

Наступні принципи пропоную розглядати в сукупності. Зокрема, принцип цільового обмеження нерозривно пов’язаний із мінімізацією даних. Обидва принципи покликані запобігти зловживанню щодо цілей та обсягу персональних даних з боку контролерів.

В сфері цифрового маркетингу зловживання зазначеними принципами має назву «Function Creep». Наприклад, користувач купує онлайн товар, надає згоду на отримання повідомлень щодо знижок, а магазин (контролер) використовує персональні дані користувача, аби відстежувати його покупки, активність та навіть кількість витрачених коштів в інших застосунках [35].

Принципи цільового обмеження та мінімізації даних були розглянуті та протлумачені Європейським Судом Справедливості у нещодавній справі *C-77/21 Digi Távközlési és Szolgáltató Kft. (“Digi”) v. Nemzeti Adatvédelmi és Információszabadság Hatóság* («NAIH») [36]. Digi – один із основних інтернет-провайдерів в Угорщині. Через збій у роботі бази даних користувачів, Digi створив ще одну базу даних під назвою «тест» та скопіював туди 1/3 від минулої бази клієнтів. «Тестова» база даних містила оновлену інформацію щодо клієнтів, дані осіб, які надали згоду надсилати їм повідомлення із ціллю прямого маркетингу та деякі інші дані. Тут варто наголосити, що «тестова» база була створена саме з метою тестування та налагоджування роботи попередньої системи. Цю «тестову» базу даних було взламано хакером, який отримав доступ до сотні тисяч профілів користувачів. Digi уклав угоду з хакером відповідно до якої хакер зобов'язався не розголошувати дані, тому фактичного витоку далі не відбулось. Однак, справа була передана до місцевого суду, який оштрафував Digi за порушення положень GDPR, а саме принципів обмеження зберігання, цільового обмеження та мінімізації даних. Далі, для інтерпретації GDPR, положень спір було передано для розгляду до Європейського Суду Справедливості. Суд здійснив аналіз зазначених принципів та дійшов висновку, що (1) зберігання персональних даних у «тестовій» базі сумісне із принципом цільового обмеження, якщо така обробка сумісна із конкретними цілями, на досягнення яких надавалась згода користувачів та (2) принцип цільового обмеження не надає права контролеру зберігати дані, що містяться у «тестовій» базі довше, аніж це необхідно для цілей тестування та усунення помилок [36. п. 61-63].

Такий підхід, на мою думку, був радше case–oriented і не повинен тлумачитись як такий, що дозволяє контролеру обробляти персональні дані у спосіб та для цілей інших, аніж погоджені суб'єктом. Із аналізу суду також випливає, що він «неявно»

посилається на необхідність, яка виникла через незалежні від контролера обставини. Водночас, я схиляюсь вважати, що щонайменше принцип цільового обмеження сформульований таким чином, що не дозволяє без додаткового повідомлення суб'єкта здійснювати обробку необумовлену згодою.

Ще один принцип GDPR, на який варто звернути окрему увагу в контексті правомірності здійснення цифрового маркетингу – конфіденційність. Зміст цього терміну не потребує додаткового пояснення, тому пропоную одразу розглянути найрезонансніші порушення.

У 2020 році відбувся витік «мільярдів» персональних даних із платформи з обробки даних Oracle BlueKai, яка власне збирала персональні дані за допомогою онлайн-трекінгу (online tracking infrastructure) [4. с. 71]. Серед таких персональних даних були дані щодо підписок на газети, покупок та навіть дані веб-браузера, що використовувались для підбору реклами [37].

Порушення принципу конфіденційності може призвести й до загрози національній безпеці.

На понад 69% телефонів європейців із операційною системою Android та 30% телефонів на iOS встановлені так звані ідентифікатори реклами (mobile advertising identifiers або MAIDs) (належать Google та Apple) [38], що використовуються для збору даних, профілювання та сегментування користувачів для цілей реклами у дуже точний спосіб [4. с. 40-41]. Експерти помітили, що ці дані передавались до російської платформи Yandex. Особливе занепокоєння виникає у зв’язку з тим, що користувачами є й державні службовці та вищі посадові особи європейських держав. Відповідно, існує висока ймовірність, що їх дані передаються для обробки до країни-агресора [4. с. 61].

Підсумовуючи, дотримання принципу конфіденційності контролерами персональних даних під час здійснення маркетингових заходів в цифровому середовищі є важливим для збереження персональних даних суб’єктів від несанкціонованого доступу третіх осіб, а в глобальних масштабах, за деяких умов, і для захисту національної безпеки.

Наостанок, принцип підзвітності можна вважати додатковим гарантом дотримання вищезазначених принципів, а також інших положень GDPR в цілому. Для цілей цієї роботи, принцип підзвітності варто розглядати крізь призму наступних обов'язків: (1) обов'язок контролера та розпорядника даних вести записи щодо процесу обробки персональних даних (такі записи повинні містити найменування усіх сторін, залучених до такої обробки, визначену мету обробки, опис категорій даних, які обробляються і т.д.) (2) зберігати умови надання згоди на обробку персональних даних, тобто копію самої згоди чи іншої підстави, відповідно до якої відбувається обробка; (3) відшкодовувати збитки суб'єкту персональних даних у випадку порушення його права та нести адміністративну відповідальність перед контролюючими органами у випадку порушення положень GDPR [11].

Ще одна вимога, на яку потрібно звернути увагу, це обов'язок контролера передбачений в статті 35 GDPR проводити оцінювання впливу на захист персональних даних, якщо обробка персональних даних призводить до «виникнення високого ризику для прав і свобод фізичних осіб» [11].

Такий ризик може бути, якщо товари, які призначені для вразливих груп населення рекламуються за допомогою таргетингу. Окрім того, додаткові ризики можуть виникнути залежно від цілей рекламної кампанії та її нав'язливості, або якщо таргетування передбачає обробку даних отриманих через спостереження чи виведення даних, або якщо вони є похідними [31. с. 30].

Оцінка впливу передбачає здійснення додаткових заходів задля забезпечення дотримання законодавства в сфері захисту персональних даних. Якщо обробка персональних даних може призвести до згаданого ризику для прав суб'єктів, на контролера покладається обов'язок дотримуватись ще й кодексів поведінки, розроблених відповідно до статті 40 GDPR.

Отже, можна зробити висновок, що обробка персональних даних з маркетинговою метою повинна відповідати принципам GDPR, які є основою законодавства ЄС щодо захисту персональних даних. Використання цифрових технологій для підбору більш точної реклами, таких як профілювання та таргетинг покладає на контролера та розпорядника персональних даних обов'язки щодо

отримання згоди на обробку, із доступним та зрозумілим викладом інформації щодо мети та способів обробки персональних даних, інформування суб'єкта даних щодо його прав, а також вчинення необхідних дій для забезпечення цілісності та конфіденційності зібраних даних. Окрім того, таргетування часто спирається на чутливі дані, що вимагає від контролера проведення додаткової оцінки відповідності, звернення до компетентних органів та приведення своєї діяльності у відповідність із кодексами поведінки.

1.2.2. Правова підстава обробки персональних даних для цілей цифрового маркетингу відповідно до GDPR

Як зазначалось, будь-яке збирання та обробка персональних даних повинні мати законну підставу, вичерпний перелік яких наведено в статті 6 GDPR.

До правових підстав, які найчастіше використовуються у сфері цифрового маркетингу належать (i) необхідність виконання договору (стаття 6.1 (b) GDPR) та (ii) згода суб'єкта персональних даних (6.1(a) GDPR).

(i) Необхідність виконання договору як правова підстава обробки персональних даних для цілей цифрового маркетингу

Як відомо, договір — це волевиявлення сторін, а метою його укладення є надання прав та створення обов'язків. Дійсність договору залежить від багатьох факторів, таких як дієздатність сторін, наміри та справжня воля сторін, наявність законодавчих обмежень щодо предмету договору та інші, перелік яких залежить від особливостей права, застосовного до договору [7. с. 13] .

Предметом договору може бути передача персональних даних особи [7. с. 94]. Наприклад, передача фото чи відео із зображенням особи за грошову винагороду [39]. Також передача персональних даних може бути необхідною для забезпечення виконання умов договору, предметом якого є надання онлайн-послуг. В останньому випадку, положення щодо надання згоди про передачу персональних даних (надалі

«згода) повинно чітко виділятись та відокремлюватись (*separability*) від інших положень договору [7. с. 66]. Якщо згода вказана як частина договору, яка не підлягає обговоренню, вважається, що вона не була надана вільно [31. с. 17]. Дійсність такої згоди залежить від дотримання законодавства про захист персональних даних, захист прав споживачів та загальних вимог щодо дійсності договору, в тому числі односторонніх заявлень [7, с. 95]. Тобто, до згоди, яка міститься в договорі застосовується цілий комплекс вимог, які містяться і в профільному законодавстві.

На практиці, виникає багато проблем із визначенням, на яку саме підставу для обробки персональних даних посилається контролер від час надання онлайн послуг.

Залежно від обставин, суб'єкт персональних даних може помилково вважати, що натискаючи кнопку «прийняти умови» він надає згоду на обробку персональних даних в розумінні статті 6(a), в той час як фактично він підписав договір із контролером. Така ж помилка може виникнути із сторони контролера, коли останній вважатиме підпис (тобто проставлення позначки навпроти «погодитись» чи натискання на кнопку «погодитись») суб'єкта персональних даних як надання згоди в розумінні статті 6.1 (a) [40. с. 7].

Описана ситуація виникає у зв'язку з тим, що в сучасних реаліях індустрія цифрової реклами настільки складна і технічно комплексна, що користувач не має об'єктивної можливості оцінити ризики пов'язані із наданням згоди, а згода втрачає своє значення [7. с. 97].

Більше того, відмова надати згоду в більшості випадків призводить до того, що користувач втрачає можливість використовувати онлайн сервіси.

Однак, в абзаці 2 преамбули 43 GDPR вказується, що *«[передбачається] презумпція ненадання згоди ..., якщо виконання договору, в тому числі, надання послуги, залежить від надання згоди, незважаючи на те, що така згода не є обов'язковою для такого виконання*» [11]. Таким чином, блокування онлайн сервісів через відсутність згоди користувача є прямим порушенням GDPR, хоча така практика є дуже поширеною.

EDPB розробив детальне Керівництво про обробку персональних даних згідно з статтею 6.1 (b) GDPR в контексті надання онлайн-послуг суб'єктам даних

(«Керівництво»). У Керівництві, посилаючись на рішення CJEU [41. п. 52] зазначається, що підхід до інтерпретації правової природи «необхідності» має незалежне значення в праві ЄС й «необхідність» слід розглядати відповідно до завдань встановлених в законодавстві про захист персональних даних [40. п. 22].

Надалі пропоную розглянути гучну справу ініційовану користувачем проти Meta (Facebook). Користувач L.B (надалі «Користувач») подав скаргу проти Facebook стверджуючи, серед іншого, що натискання ним кнопки «прийняти» під Умовами користування, коли він заходив до Facebook, не є актом надання згоди на обробку персональних даних, в тому числі для цілей поведінкової реклами [42].

За словами Користувача, у 2018 році (після дати набрання чинності GDPR), він завантажив додаток Facebook, який перед цим видаляв, аби продовжити його використання. Того ж року Facebook оновив Умови надання послуг, відповідно до яких всім наявним користувачам пропонувалось або погодитись із новими положеннями, або видалити аккаунт. Під час входу Користувач прийняв Умови надання послуг, шляхом проставлення позначки «Погодитись». Водночас, Користувач намагався обмежити використання своїх персональних даних у Facebook, не надаючи інформації про себе в профілі, а також намагався відмовитись від відстеження його активності в цілях поведінкової реклами. Незважаючи на це, Facebook обробляв його чутливі персональні дані, зокрема щодо гомосексуальної орієнтації та політичних поглядів й за допомогою таргетингу підбирав відповідний контент.

Facebook, в свою чергу, посилається на Умови надання послуг та Політику конфіденційності як правову підставу обробки персональних даних Користувача, тобто вказує, що законною підставною в даному випадку є *необхідність* виконання договорів у розумінні статті 6(1)(b) GDPR. Як фактичне підґрунтя Facebook вказує на характер діяльності платформи: користувачі використовують платформу безоплатно, а дохід, в основному, Facebook отримує від реклами [43].

Справа розглядалась в національному суді, апеляції, Уповноваженим з персональних даних Ірландії, та EDPB. Апеляція та Уповноважений прийняли

рішення на користь Meta [4. с. 67] Надалі справу було передано до CJEU для інтерпретації статті 6(1)(b) GDPR.

Суд в своєму аналізі посилається на Керівництво, де зазначається, що «*як правило, обробка персональних даних для цілей поведінкової реклами не є необхідною для виконання договору про онлайн-послуги*» [43. п. 52] надалі, однак, зазначаючи, що «*в певних випадках персоналізація контенту може бути необхідною умовою для виконання договору*» Але знову ж таки, необхідно встановити прямий причинно-наслідковий зв'язок між обробкою персональних даних та конкретною метою юридичного обов'язку, який, у даній справі, явно відсутній [43. п. 61-62].

На додаток, у своєму рішенні Суд звернув увагу на характер персональних даних, які Facebook обробляв для цілей таргетингу. Зокрема, дані щодо сексуальної орієнтації та політичних переконань, які є чутливими даними в розумінні GDPR. Користувач не вказував їх в своєму профілі. Однак, Facebook за допомогою технічних алгоритмів проаналізував список його друзів, більшість з яких були гомосексуальної орієнтації, а політичні переконання були визначені шляхом порівняння профілю Користувача зі схожими профілями кристувачів, які ставили вподобання до постів відповідного політичного діяча.

Суд зазначив, що обробка чутливих даних повинна здійснюватися у відповідності із статтею 9 GDPR [43. п. 60-62], що у даному випадку вимагає отримання від Користувача явної згоди на обробку таких даних.

Отже у своєму рішенні Суд прийшов до висновку, що, по-перше, обробка персональних даних не є «необхідною» в розумінні статті 6(1)(b) GDPR для надання онлайн-сервісів Facebook, та, по-друге, обробка чутливих персональних даних вимагає окремої явної згоди користувача.

Щодо тих випадків, коли обробка персональних даних та, відповідно, персоналізація контенту є необхідною для виконання договору, EDPB вказує наступне. Для того, аби встановити таку необхідність, потрібно враховувати характер наданої онлайн-послуги, очікування середньостатистичного користувача, спосіб просування послуги серед користувачів та можливість надавати послугу без такої обробки [40. п. 57].

Підсумовуючи, необхідність виконання договору як правова підстава обробки персональних даних для надання онлайн-сервісів повинна використовуватись лише в тих випадках, коли надання онлайн-сервісу нерозривно пов'язане із обробкою персональних даних, а відсутність згоди унеможливлює виконання положень договору. Як вказує практика, на цю підставу для обробки персональних даних посилаються і великі компанії, такі як Facebook.

Однак, рішення Суду та аналіз позиції EDPB вказують, що Умови надання послуг та інші схожого роду договори між користувачем та платформою не можуть трактуватись як такі, на виконання яких платформа може обробляти дані користувача без його згоди. Якщо ж для цілей створення профілю користувача із подальшим таргетуванням обробляються чутливі персональні дані, контролер персональних даних повинен отримати явну згоду на таку обробку.

(ii) Згода суб'єкта персональних даних як правова підстава обробки персональних даних для цілей цифрового маркетингу

Концепція згоди в GDPR детально досліджена на рівні ЄС. У 2020 році Робоча група із захисту персональних даних при Європейській Комісії видала оновлену версію Керівництва про згоду відповідно до GDPR [44]. Крім цього, аналіз згоди як підстави обробки персональних даних досліджувався CJEU, EDPB, національними судами держав-членів ЄС та Уповноваженими із захисту персональних даних. Велику теоретичну базу напрацьовано і серед науковців.

У цій частині своєї роботи я пропоную проаналізувати ключові елементи згоди, а далі дослідити як на практиці контролери персональних даних отримують згоду користувачів для цілей маркетингу та які особливості варто враховувати, зважаючи на специфіку індустрії.

Визначення згоди міститься у статті 4 (11) GDPR:

«*згода суб'єкта даних означає будь-яке вільно надане, конкретне, поінформоване та однозначне зазначення бажань суб'єкта даних, яким він або вона,*

шляхом оформлення заяви чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних» [11].

EDPB виділяє наступні елементи згоди:

- Вільно надана
- Конкретна
- Проінформована
- Недвозначна вказівка на бажання суб'єкта даних, виражена шляхом заяви або чіткої підтверджувальної дії, що означає згоду на обробку його або її персональних даних [43. п. 11].

У статті 7 та преамбулах 32, 33, 42, 43 розкривається зміст зазначених елементів та вказуються на те, які дії повинен вчинити суб'єкт персональних даних аби згода відповідала всім вказаним елементам [43. п. 9].

Вказане визначення згоди та положення, через які розкриваються її елементи застосовуються і до таргетингу та прямого маркетигну [45]. Однак, найбільше проблем виникає при встановленні *коли* та *за яких умов* суб'єкт персональних даних надав згоду на обробку його персональних даних комерційних цілях, яка б містила всі елементи [7. с. 59]

Розберемо елементи на прикладах.

Вільно надана згода та неоднозначна вказівка на бажання суб'єкта.

Згода не вважатиметься вільною, якщо на суб'єкта персональних даних здійснюється будь-який тиск або вплив, незалежно від їх інтенсивності [44. п. 14].

У 2020 році CJEU розглядав спір у справі *Orange Romania SA v. The Romanian National Supervisory Authority for the Processing of Personal Data (Romanian DPA),* де Orange Romania передбачила у договорі з користувачами положення про згоду на обробку персональних даних, при цьому напроти положення була проставлена «галочка», себто замість користувача. Якщо ж користувач хоче відмовитись від такої обробки — він змушений написати окремий запит.

Суд дійшов до висновку, що не може вважатись *вільною* згода, якщо на суб'єкта персональних даних покладається обов'язок вчинити додаткові дії, щоб відмовитись

від згоди [46. п. 50]. Таку ж позицію висловлює ECJ у справі C40/17 [47. п. 100-102] На думку юристки-практикантки в сфері захисту персональних даних, у своєму рішенні CJEU демонструє дещо новий підхід до трактування ідеї «вільної» згоди, надаючи їй абсолютну цінність [48].

Отже, практика вказує, що воля користувача щодо надання чи ненадання згоди на обробку його персональних даних є ключовим елементом згоди. Якщо ж контролер встановлює додаткові вимоги, які вимагають вчинення дій, щоб ускладнити відмову від надання згоди, то згода не може вважатись «вільно наданою».

Проінформована згода. EDPB зазначає, що для того щоб згода вважалась проінформованою користувачу повинні бути надані як мінімум наступні дані:

- Особа контролера
- Мета обробки відповідно до кожної наданої згоди
- Які види персональних даних використовуватимуться
- Інформація щодо права особи відмовитись від обробки персональних даних
- Інформація про використання технології автоматичного прийняття рішення чи профайлінгу відповідно до статті 22 (2) (c) GDPR
- Інформація щодо ризиків пов’язаних із відсутність належних гарантій щодо передачі персональних даних відповідно до статті 46 GDPR [44. с. 15]

Кожен із зазначених пунктів є важливим, тому повинен розглядатись комулятивно.

У вже згаданому рішенні CJEU суд також вказав, що користувач не надав Orange Romania «проінформовану» згоду. Наперед проставлена за користувача «галочка» навпроти згоди не означає, що користувач був ознайомлений з умовами обробки персональних даних [46. п. 47-51][3]

Отже, згода на обробку персональних даних є передумовою будь-якої законної обробки персональних даних. В правовому полі кожен із елементів згоди

[3] Рішення суду пара 47-51

розглядається окремо, однак, на практиці відсутність одного з елементів виключає й інші.

1.2.3. Регулювання ePrivacy Directive щодо захисту персональних даних під час здійснення цифрового маркетингу

ePrivacy Directive містить спеціальні правила щодо захисту персональних даних в секторі електронних комунікацій Водночас, стаття 5(3) ePrivacy Directive, покладає на держави-члени ЄС обов'язок дотримуватись положень GDPR під час надання користувачу доступу до електронних комунікаційних мереж, в тому числі обов'язку щодо повідомлення мети обробки персональних даних, отримання згоди користувача та реалізації права користувача відмовитись від такої обробки [49].

У розрізі діяльності щодо цифрового маркетингу розмежування між застосуванням цих двох інструментів наступне. Використання файлів cookies або подібних технологій на кінцевому обладнанні користувачів та отримання інформації через ці технології підпадає під дію статті 5(3) ePrivacy Directive, а, власне, подальша обробка будь-яких персональних даних, які отримуються в результаті такої реклами, регулюється GDPR. Отже, контролерам потрібно дотримуватися не лише вимог, які передбачені 5 (3) ePrivacy Directive, але й інших вимог, що випливають з GDPR [50. с. 19]

У статті 5(3) мова йде про зберігання та отримання доступу до «інформації». Тобто, автори навмисне використовують термін відмінний від терміну «персональні дані». Робоча група із захисту персональних даних при Європейській Комісії вказує, що інформація, зібрана за допомогою електронних комунікаційних чи інших сервісів не обов'язково є персональними даними в розумінні GDPR [51. с. 9].

Логіка цього підходу розкривається у преамбулі 24 ePrivacy Directive, де зазначається що «*кінцеве обладнання користувача та будь-яка інформація, що зберігається на таку обладнанні є частиною приватної сфери життя користувачів і вимагає захисту відповідно до ECHR*» [51. с. 9].

Тобто, будь-яке використання інформації отриманої через електронні комунікаційні сервіси з обладнання користувача підпадає під регулювання ePrivacy Directive, а тієї інформації, яка вважається персональними даними у розумінні GDPR — додатково регулюється GDPR.

Тепер варто коротко розмежувати, яка інформація, зібрана за допомогою cookies буде вважатись персональними даними, а яка ні.

Загалом, файли cookies — це дані, що зберігаються на веб-сторінці, процесорі чи іншому пристрої невеликими файлами з метою навігації по веб-сторінці, збереження логіну та паролю, запам’ятовування вподобань користувача і т.д. Часто файли cookies також використовуються для таргетованої реклами, вимірювання аудиторії та інших маркетингових цілей.

Юридичне ж значення має поділ cookies на основні (технічні) та неосновні (essential / non-essential cookies). До основних відносять ті, без яких функціонування веб-сторінки не можливе (наприклад, версія операційної системи, , а всі інші — неосновні. До неосновних файлів cookies відносять ті, що використовуються для вимірювання аудиторії та збирання даних в рекламних цілях.

Звертаючись до положень GDPR, у преамбулі 30 GDPR вказується, що файли cookies вважаються персональними даними. Однак, як вже зазначалось, сам текст ePrivacy Directive не розділяє такий підхід.

Тепер щодо розмежування, як зазначають юристи-практики, згідно зі статтею 6 GDPR, збір cookies можливий на основі згоди користувача (для преференційних, аналітичних чи маркетингових cookies) або законного інтересу контролера (для необхідних cookies), в такому випадку згода не потрібна [52]. Тобто, можна зробити висновок, що cookies, які необхідні для законного інтересу контролера, тобто ті, які є неосновними (технічними) і будуть вважатись «інформацією» в розумінні ePrivacy Directive, та, водночас, не є персональними даними в розумінні GDPR.

Отже, для визначення того, за яких умов відповідно до ePrivacy Directive дозволяється використовувати cookies для маркетингових цілей варто провести аналіз згоди в розумінні зазначеної директиви, як правової підстави для збору персональних

даних.

1.2.4. Правова підстава використання cookies для цілей цифрового маркетингу

У преамбулі 17 до ePrivacy Directive зазначається, що згода користувача або підписника повинна бути отримана відповідно до вимог GDPR, при цьому наголошується, що статус суб'єкта (фізична чи юридична особа) теж не має значення [53]. Таку відсилку до GDPR варто розглядати як передумову для законної обробки персональних даних та враховувати всі вимоги до змісту та елементів, які передбачені в GDPR [44. п. 7].

Як зазначає Робоча група із захисту персональних даних використання cookies інших, аніж основних, забороняється до надання згоди користувача. Під час завантаження веб-сторінки на девайс користувача забороняється встановлення cookies, допоки користувач не ознайомився та не виявив бажання погодитись на їх використання [54. с. 4]

Зазвичай під час завантаження веб-сторінки з'являється cookies банер, тобто вікно, у якому надається інформація щодо cookies, які опрацьовуються сайтом та відповідні кнопки «погодитись» чи «відмовитись» від опрацювання даних. До змісту банера застосовуються усі ті ж вимоги, що були наведені та проаналізовані у попередньому підрозділі. На додаток, CJEU у рішенні *C-673/17 - Planet49* зазначає, що надання згоди на збирання cookies є радше активною дією (наприклад, проставлення галочки чи натискання на кнопку «погодитись») [55. п. 52].

Відмова користувача надати cookies не повинна перешкоджати йому використовувати веб-сторінку [4. с. 232] Практично, власники веб-сторінок вдаються до хитрощів, аби отримати згоду користувача на використання його cookies, адже дані користувача мають неабияку цінність для рекламної індустрії. Серед таких хитрощів — створення дизайну банеру cookies таким чином, щоб користувач був змушений погодитись.

У 2020 році Google було оштрафовано на 150 мільйонів євро за те, що згоду на використання cookies [4. с. 232], в тому числі для цілей цифрового маркетингу, було важче надати, аніж відмовитись. Зокрема, щоб продовжити перегляд сайту «google.fr» або «youtube.com», користувач просто повинен натиснути кнопку «Я приймаю» в спливаючому вікні, яке зникне після підтвердження і йому буде дозволено переглядати сайт. У той же час, якщо користувач бажає відмовитися від використання файлів cookies, йому потрібно натиснути кнопку «Персоналізація» у цьому ж вікні, щоб отримати доступ до інтерфейсу, який дозволяє активувати або деактивувати файли cookies. Відповідно до рішення Органу із захисту персональних даних, застосування такого інтерфейсу суперечить положенням щодо добровільності згоди [57].

У 2022 році Орган із захисту персональних даних оштрафував Amazon на понад 35 мільйонів євро [4 с. 232] за те, що (1) на девайси користувачів автоматично, без надання згоди, встановлювались рекламні cookies та (2) банери cookies не містили достатньої інформації щодо мети збору даних та способів, як можна відмовитись від них [57].

Підсумовуючи, вимоги до згоди на використання cookies в ePrivacy Directive повторюють вимоги передбачені в GDPR із врахуванням практичних особливостей використання cookies.

У 2021 році Єврокомісія опублікувала результати Євробарометра та публічних консультацій щодо ефективності ePrivacy Directive. Як користувачі, так і зацікавлені сторони погоджуються, що захист персональних даних та конфіденційність повинні залишатись основними питаннями для регулювання. Однак, стейкхолдери зацікавлені в більш бізнес-орієнтовному підході, який би враховував як технологічні особливості так і сучасні тенденції цифрового маркетингу та радше сприяв його розвитку, а не обмежував. При цьому, сторони погоджуються й на тому, що ePrivacy Directive вже не відповідає вимогам часу. Тому у 2021 році Єврокомісія презентувала ePrivacy Regulation.

Хоча ePrivacy Regulation ще не прийнята, короткий огляд і узагальнення змін, які вона пропонує є необхідними для розуміння законодавства яке, найочевидніше, набуде чинності приблизно в один час із прийняттям України до ЄС.

В першу чергу, передбачається сама зміна природи із директиви на регламент призведе до його обов'язковості для всіх держав-членів.

Щодо ключових змін у сфері цифрового маркетингу передбачається:

- ePrivacy Regulation отримає більш широке застосування, поширюючи свою дію на соціальні мережі, месенджери та електронні скриньки.
- деталізується використання так званих cookies wall, тобто блокування доступу до сайту у випадку не надання згоди на використання cookies. Встановлюється, що функціонал веб-сторінки може бути обмежений, якщо особа не надала згоду на збирання cookies, але таке обмеження не повинно повністю блокувати доступ, а користувачу надається певна альтернатива. Також вводиться можливість купівлі підписки, яка дозволятиме використовувати сайт без збирання cookies.
- збирання аналітичних cookies тепер не вимагатиме згоди користувача.
- Передбачається можливість керувати саме чутливими персональними даними у браузері, тобто користувач може вибрати у функціоналі браузеру, що не надає згоди на обробку цієї категорії персональних даних та, відповідно, не буде необхідності кожного разу при відвідуванні сайті знову проставляти галочку навпроти відмови [58]

Зазначений перелік є дуже стислим та наведений для окреслення ключових змін які лише передбачаються.

Резюмуючи проведений вище аналіз, GDPR та ePrivacy Directive слугують надійними законодавчими інструментами, які послідовно отримав одностайну та зрозумілу практику застосування. GDPR — встановлює фундаментальні принципи обробки персональних даних, права користучачів та обов'язки контролерів та операторів, регулює відповідальність за порушення. ePrivacy Directive зосереджується на сфері електронних комунікацій. В обох документах фундаментальною підставою для здійснення обробки персональних даних в

маркетингових цілях є згода суб’єкта. Вимоги до згоди варіюються від вибраного контролером чи оператором способу, однак важливим є дотримання кумулятивних елементів законності згоди: вільно надана, конкретна, проінформована та недвозначна. Окрім цього, згода на обробку чутливих персональних даних повинна бути явною. Планується, що ePrivacy Regulation ще більше зміцнить регулювання цифрового маркетингу.

РОЗДІЛ 2. НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО У СФЕРІ ЦИФРОВОГО МАРКЕТИНГУ

Цей розділ присвячений дослідженню стану врегульованості та положень законодавства, яке застосовується під час здійснення цифрового маркетингу в Україні.

Варто відзначити, що на теоретичному рівні питання досліджене дуже вузько, а самих публікацій обмаль.

На мою думку, такий стан речей пов'язаний із наступними причинами. По-перше, українці в більшій мірі користуються платформами, соціальними мережами та застосунками «іноземного» походження, себто глобальних компаній, про які вже неодноразово згадувалось (Google, Meta). Такі компанії орієнтуються на законодавство ЄС та, за потреби, звертаються до українських правників за консультацією щодо врахування більш жорстких вимог українського законодавства, якщо такі існують. Однак, як буде далі доведено, на даний час національне законодавство майже не адресує ті вимоги, що передбачаються в ЄС щодо здійснення цифрового маркетингу. Таким чином, дотримання законодавства ЄС гарантує великим компаніям відсутність позовів та скарг на території України.

По-друге, українські компанії, які стрімко розвиваються та бажають виходити на європейський ринок створюють політики конфіденційності та умови надання послуг відповідно до нормативних вимог ЄС, оскільки GDPR застосовується й коли особа, чиї дані обробляються, є громадянином ЄС, навіть якщо сама обробка відбується на території України.

Незважаючи на вищевказане, за останніх декілька років внутрішній ринок електронної комерції в Україні зростав, а в 2023 році, почав поступово відновлюватись після колапсу під час початку повномасштабного вторгнення [59]. Відновлення та розвиток, безумовно, є позитивним явищем та попри це, малі та середні бізнеси, які орієнтуються на внутрішній ринок, підпадають під національне регулювання, а за його відсутності — користувачі не мають гарантій та захисту у

відповідній сфері.

2.1. Закон України «Про рекламу»

Як зазначає Самагальська Ю., відсутність спеціального закону щодо регулювання реклами в мережі Інтернет у національному законодавстві є поширеною практикою в більшості країн, оскільки загального регулювання щодо реклами достатньо [60].

Звертаючись безпосередньо до українського законодавства, яке може бути застосоване до цифрового маркетингу, одразу спадає на думку Закон України «Про рекламу» № 270/96-ВР від 03.07.1996 р.

В частині 1 статті 2 згаданого закону визначається, що його сфера регулювання поширюється на відносини, пов'язані з виробництвом, розповсюдженням та споживанням реклами на території України. Тобто, можна припустити, що закон міг би застосовуватись до реклами в інтернеті, спираючись на термін «споживання реклами».

Далі у законі міститься визначення реклами: «*реклама — інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару*» [61].

Знову ж таки, відповідно до визначення, згадка на «будь-яку форму» та «будь-який спосіб» спонукає зробити висновок, що закон може застосовуватись до реклами в інтернеті.

У статті 7 перелічено загальні принципи здійснення реклами, до яких, зокрема, належать: законність, точність, достовірність, використання форм та засобів, які не завдають споживачеві реклами шкоди. При подальшому аналізі статей стає зрозуміло, що закон не містить норм, які б адресували специфіку просування товарів та послуг в інтернеті. Хоча, на мою думку, застосування загальних принципів, згаданих вище, цілком можливе й до здійснення реклами в інтернеті.

Нажаль, судова практика судів вищих інстанцій з цього питання відсутня, а практика судів нижчих інстанцій непохитно заперечує застосування Закону України «Про рекламу» до відносин в Інтернеті.

У рішенні від 13.06.2022 № 640/22469/21 Окружний адміністративний суд м. Києва вказує, що «*у розділі 2 Закону № 270/96-ВР послідовно наводиться визначення та порядок регулювання ведення реклами: на телебаченні і радіо (стаття 13), у друкованих засобах масової інформації (стаття 14), реклами послуг, що надаються з використанням електрозв'язку (стаття 15), зовнішньої реклами (стаття 16), внутрішньої реклами (стаття 17), реклами на транспорті (стаття 18), реклами під час демонстрування кіно- та відеофільмів (стаття 19).*

Правове регулювання здійснення реклами через мережу Інтернет у Законі № 270/96-ВР відсутнє» [62].

Повторюючи позицію наведену вище, дещо більше дослідив розміщення реклами в інтернеті, а саме на сторінці Facebook, Полтавський окружний адміністративний суд. У своєму Рішенні від 23.09.2020 № 440/4116/20 суд встановив, що розміщена на приватній сторінці Facebook користувачем інформація про проведення ТОВ "Винотерія" дегустації вин не може вважатись рекламою. Судом зазначено, що у Facebook компанію можна представляти як «сторінка», «профіль» та «група», однак технічна можливість розповсюджувати рекламу можлива із «сторінки» та не можлива із «профілю». Тому, на думку суду, повідомлення про дегустацію вин розміщене на «профілі» не може вважатись рекламою [63].

Тобто, суди буквально розтлумачили положення Закону України «Про рекламу», виключивши регулювання в мережі Інтернет, як таке, що прямо не передбачене.

У 2008 році до ВРУ внесли проект Закону України «Про інтернет рекламу» (реєст. № 3126) [64]. Структура проекту повторювала структуру чинного закону, а відмінність полягала лише в додаванні декількох нових визначень, таких як банерна та контекстна реклама, статті «Законодавство про інтернет рекламу», яка відсилала до «інших нормативно-правових актів, які регулюють відносини у сфері реклами» та ще декількох нечітких положень. Очікувано, проект закону не був розглянутий.

У Законі України «Про рекламу» передбачається право громадян та підприємств об’єднуватись в органи саморегулювання. Так, в Україні діють Всеукраїнська Рекламна Асоціація, Українська Асоціації Маркетингу, Інтернет Асоціація України (Комітет з питань інтернет-реклами). На відміну від ЄС, органи саморегулювання рекламної та маркетингової діяльності в Україні не адресують проблематики здійснення реклами в мережі Інтернет. Серед документів Всеукраїнської Рекламної Асоціації відсутні аналоги ICC Code, як і будь-які інші кодекси чи рекомендації щодо дотримання вимог законодавства чи пропозиції вдосконалення [65]. На сайті Української Асоціації Маркетингу в розділі «Стандарти» міститься посилання на деякі європейські акти, однак, застарілі. Відповідно, органи саморегулювання в Україні також не сприяють розвитку регулювання цифрового маркетингу. Комітет з питань інтернет-реклами також не адресує зазначених питань.

Підсумовуючи, Закон України «Про рекламу» не застосовується до регулювання реклами в мережі Інтернет й, відповідно, не адресує питання здійснення цифрового маркетингу. Серед причин відсутності норм щодо реклами в інтернеті варто виділити застарілий підхід до регулювання індустрії реклами. Спроби врегулювати інтернет рекламу окремим законом теж не були ефективні через слабку законодавчу техніку та, найімовірніше, відсутність політичної волі на той час. На рівні органів саморегулювання ініціативи щодо напрацювання внутрішніх правил теж відсутні.

2.2. Закон України «Про електронну комерцію»

Закон України «Про електронну комерцію» регулює порядок вчинення електронних правочинів із застосуванням інформаційно-комунікаційних систем.

Відповідно до ч. 4 статті 11 вищезазначеного закону: «*Пропозиція укласти електронний договір (оферта) може бути зроблена шляхом надсилання комерційного електронного повідомлення, розміщення пропозиції (оферти) у мережі Інтернет або інших інформаційно-комунікаційних системах*» [66]. Отже, даним законом

регулюється порядок надсилання комерційних повідомлень, які є невід'ємною частиною цифрового маркетингу.

На додаток, відповідно до статті 10 згаданого закону: «*Інформування потенційних покупців (замовників, споживачів) щодо товарів, робіт, послуг здійснюється відповідно до вимог Закону України «Про рекламу» та може здійснюватися шляхом надсилання комерційних електронних повідомлень*». Тобто, фактично дана стаття встановлює, що Закон України «Про рекламу» все-таки поширюється на рекламу з застосуванням мережі інтернет, а саме в частині надсилання електронних комерційних повідомлень, однак з особливостями вказаними у даному законі.

Відповідно до п. 10 статті 3: «*комерційне електронне повідомлення - електронне повідомлення у будь-якій формі, метою якого є пряме чи опосередковане просування товарів, робіт чи послуг або ділової репутації особи, яка провадить господарську або незалежну професійну діяльність*».

Зміст дефініції електронного комерційного повідомлення відповідає визначенню «прямого маркетингу»[67. с. 293]. Такої ж думки дотримуються юристи-практики [68]. Тому можна стверджувати, що нормативне регулювання здійснення прямого маркетингу передбачене в Законі України «Про електронну комерцію».

Одразу варто нагадати, що як зазначалась в Розділі 1.2.1.2 (ii) питання здійснення прямого маркетингу в ЄС регулюється GDPR, а саме в преамбулі 47 є чітка вказівка, що всі положення щодо згоди на обробку персональних даних (стаття 6 GDPR) застосовуються і до прямого маркетингу. Такий же обов'язок передбачається у статті 13 ePrivacy Directive.

Отже, нижче пропоную порівняти регулювання прямого маркетингу в Україні із регулюванням, передбаченим в ЄС.

Вимоги до змісту електронного комерційного повідомлення містяться у ч. 2-4 статті 10 згаданого закону:

- наявність згоди особи на отримання таких повідомлень, або ж можливості відмовитись від таких повідомлень в будь-який час;

- комерційне повідомлення повинно бути ідентифіковано як комерційне та надіслане з рекламною метою;
- комерційне повідомлення повинно містити повну інформацію про продавця;
- вимоги щодо інформації про товар та його ціну.

Серед запропонованих вимог увагу варто зосередити на вимогах до згоди.

Формулювання щодо згоди передбачає, що суб’єкт електронної комерції зобов'язаний отримати згоду користувача на отримання комерційних повідомлень або надіслати комерційне повідомлення з вказівкою на право користувача відмовитись від його отримання. Якщо користувач ігнорує таке повідомлення, це буде вважатись мовчазною згодою.

Однак, надалі по тексту закону не розкривається поняття «згоди» та не наводяться її ознаки чи хоча б загальні вимоги щодо правил її надання. Відповідно, не зрозуміло у якій формі може бути надана згода: письмово, усно, вчинення конклюдентних дій.

Вбачається, що будь-який суб’єкт господарювання може використати електронну скриньку чи номер телефону особи для надсилання їй комерційних повідомлень, вказавши в його змісті опцію «відмовитись». При чому, вимог до форми здійснення права на відмову теж не становлено.

Тобто, з точки зору українського законодавства цілком правомірним є надіслати особі комерційне електронне повідомлення де великим шрифтом та з яскравими малюнками надається інформація щодо товарів чи послуг, а внизу, маленьким непримітним шрифтом знаходиться повідомлення про можливість відмовитись, наприклад, шляхом подання окремої заявки на якусь електронну пошту суб’єкта господарювання. Практично, більшість комерційних повідомлень містять посилання, при натисканні на яке, система автоматично виключає користувача із списку отримувачів повідомлень.

Ще одна неврегульованість — вказівка на можливість відмовитись від комерційного повідомлення «в будь-який час». Тобто, передбачене право

користувача, водночас відсутнє нормування, як суб'єкт господарювання повинен виконати його кореспондуючий обов'язок.

Порівнюючи із вимогами, які ставляться до надання згоди та її елементів в ЄС, вбачається, що в українському законодавстві підхід до згоди кардинально інший. По перше, на відміну від GDPR, де вимагається явна, конкретна згода (unambiguous), в національному законодавстві згода може бути неявна. Таким чином, вимоги до інших елементів правомірності згоди відповідно до GDPR теж не застосовні.

Електронна комерція, як і маркетинг не обмежуються кордонами. Включення України до списку кандидатів в члени ЄС слугує додатковим поштовхом для українського бізнесу розглядати розширення на ринок ЄС, як наступний амбітний крок.

Однак, якщо суб'єкти господарювання, що зареєстровані та здійснюють свою діяльність відповідно до законодавства України надішлють електронне комерційне повідомлення громадянину Бельгії, вони явно порушать положення GDPR (відповідно до принципу екстериторіальності). Таке повідомлення буде суперечити статті 6 GDPR щодо отримання згоди суб'єкта на отримання прямих маркетингових повідомлень.

Підсумовуючи, на даний час в Україні підхід до регулювання прямого цифрового маркетингу не відповідає положенням, що містяться в законодавстві ЄС.

2.3. Закон України «Про захист персональних даних»

Закон України «Про захист персональних даних» від 01.06.2010 р. є фундаментальним нормативно-правовим актом у сфері захисту персональних даних в Україні. Закон був розроблений у 2010 році та ґрунтувався на Директиві 95/46/ЄС від 24 жовтня 1995 року, яка замінена GDPR. Зважаючи на те, що Закон був прийнятий майже 13 років тому та базується на застарілій директиві, його положення не узгоджені з положеннями чинних GDPR та ePrivacy Directive.

Нижче пропоную розібрати основні відмінності у регулюванні, які є важливими для захисту прав суб'єктів під час здійснення щодо них заходів цифрового маркетингу.

Ігор Усенко, заслужений юрист України, у своєму Коментарі до закону зазначає, що взагалі назва закону не повністю відображає його зміст. У сучасному вигляді закон спрямований на захист та обробку персональних даних, які знаходяться в базах даних, а не на всі аспекти захисту персональних даних загалом [69]. У статті «Чому закон про захист персональних даних неможливо виконати» автор цитує слова політикині та голови Державної регуляторної служби (2015-2019 року) Ксенії Ляпіної щодо суті закону: «*Ключова ідея закону зовсім не в тому, щоб захищати право людини на приватність, а в тому, щоб створити державну базу даних баз даних, які вимагають контролю щодо захисту*» [70].

Тобто з самого початку закон приймався, аби врегулювати суспільні відносини, що виникають у зв'язку з створення баз персональних даних, а не у зв'язку із фактом обробки персональних даних, що впливає на фундаментальні права людини.

Наступна відмінність полягає у змістовно різних визначеннях, що становить персональні дані. Відповідно до статті 2 закону: «*персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована*». У Рішенні від 20.01.2012 № 2-рп/2012 Конституційний Суд України («КСУ») розтлумачив детальніше, що входить до поняття «персональні дані». Зокрема, КСУ вживає поняття персональних даних як синонім до «інформація про особисте та сімейне життя особи» та наводить приклади таких даних [71].

У GDPR міститься інший підхід: «*персональні дані означає будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати*» [11].

Як тлумачить юрист-практик Дмитро Скумбрій: «*Персональні дані — це не лише набір даних, що дозволяє ідентифікувати конкретну фізичну особу. В [GDPR] відносять будь-які відомості, які описують або вказують на суб'єкта, з яким такий набір даних може асоціюватись.*» [72]. Таким чином, обсяг персональних даних відповідно до закону більш звужений, в той час як GDPR включає взагалі будь-яку

інформацію. Виходячи із визначення також можна прийти до висновку, що закон не застосовується до cookies [73].

Що стосується суб'єктів, яких виділяє закон, то як науковці [74. с. 116] [75. с. 472] так і практики [72] сходяться на тому, що «володілець» та «розпорядник» персональних даних в розумінні закону відповідає термінам «контролер» та «оператор», які містяться в GDPR.

Далі пропоную проаналізувати принципи обробки персональних даних передбачені у законі.

Принципи обробки персональних даних закріплені в статті 6 «Загальні вимоги до обробки персональних даних». Вони не виділяються окремо, а закріплені як конкретні вимоги, що ставляться законодавцем до суб'єкта, який обробляє персональні дані, а деякі із принципів випливають із змісту інших статей.

До таких вимог (принципів) належать:

- відкритість і прозорість
- точність та достовірність та оновлення в міру потреби персональних даних
- склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки
- визначення конкретних і законних цілей обробки за згодою суб'єкта
- [обробка] не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися [76].

До принципу, який випливає із змісту відносять також підзвітність [77. с. 75-77].

У Постанові від 19 вересня 2018 року у справі № 806/3265/17 Велика Палата Верховного Суду України перелічує такі принципи як відкритість прозорість, відповідальність, адекватність, не надмірність складу та змісту персональних даних стосовно визначеної мети їх обробки [78]. Отже, у законі, на відміну від GDPR, принципи подаються не структуровано та завуальовано, що породжує неточність у їх визначені. У цій же Постанові міститься важливий аналіз щодо відсутності права

відмовитись від обробки персональних даних та наслідків відмови, що порушує конституційні права особи [79].

Переходячи до підстав обробки персональних даних. У статі 6 закону надається вичерпний перелік підстав, який відображає підстави, зазначені в GDPR.

Як згадувалось у попередньому розділі, для цілей цифрового маркетингу найчастіше компанії посилаються на згоду особи, або ж на необхідність виконання договору. Тому саме ці підстави пропоную проаналізувати детальніше.

В статті 11 закону формулювання щодо договору наступне: «*укладення та виконання правочину, стороною якого є суб'єкт персональних даних, або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних*» [76].

Як вбачається, український законодавець вбачає саме факт укладення договору, як правову підставу обробки персональних даних. На думку Ірини Павлюк, юристки-практикантки у сфері захисту персональних даних, такий підхід зумовлений особливістю українського законодавства, а саме тим, що відповідно до Цивільного Кодексу України правочин відображає волю особи, тому відповідно, особа погоджуючись на укладення правочину автоматично надає згоду на обробку персональних даних [80].

Такий же підхід висловив Вінницький апеляційний суд у справі № 127/13877/19 від 24 червня 2020 вказавши: «*Різниця між правочином та згодою, як окремою підставою для обробки персональних даних лише в тому, що сам по собі договір (незалежно від змісту його положень) є підставою для обробки даних особи, незалежно від надання чи ненадання окремої згоди*» [81].

Я цілком не погоджуюсь із таким твердження, зважаючи на наступне. Як досліджено в Розділі 1, для виконання договору щодо надання онлайн послуг, як правило, обробка персональних даних не є критично необхідною. Специфіка індустрії цифрового маркетингу якраз зосереджується на тому, аби залучити користувачів до інтеракції з метою просування товарів чи послуг таким чином, або викликати у користувача бажання придбати їх. Таке бажання навіюється за допомогою використання таких інструментів як поведінкова реклама, таргетинг та

профілювання. Тобто, та «воля» про яку вказують юристка та суд під час свого аналізу в реаліях цифрового маркетингу не відображає вільне волевиявлення суб'єкта.

В GDPR акцент робиться саме на необхідності виконання договору і прямому причинно-наслідковому зв'язку, тобто самого факту його укладення не достатньо.

На додаток, такий підхід суперечить вимозі GDPR щодо чіткої відокремленості згоди від самого договору, де згода розглядається як, по-суті, окремий договір. До згоди, як окремого договору, застосовуються вимоги щодо дійсності, які містяться в спеціальному законодавстві.

Інша неузгодженість між законом та GDPR — підхід до визначення згоди.

Відповідно до визначення в законі «*згода суб'єкта персональних даних - 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*» [76].

Таким чином, можна визначити наступні елементи згоди:

- добровільність
- проінформованість
- визначення мети обробки
- обов'язкова письмова форма, або інший спосіб, який дозволяє ідентифікувати згоду

На жаль, в наукових колах елементи згоди відповідно до Закону України «Про захист персональних даних» не отримали достатньої уваги.

Щодо першого елементу, добровільність визначається як «відсутність примусу», при чому мається на увазі як прямий, так і опосередкований примус [82 с. 58].

Водночас, норма не дає відповідей на питання, чи вважатиметься примусом застосування практик темних патернів. Наприклад, проставлення згоди на обробку персональних даних за суб'єкта чи використання більшого, яскравішого шрифту навпроти поля «погодитись».

Щодо елементу проінформованості, на практиці, як стверджує вже згаданий юрист-практик Дмитро Скумбрій, компанії створюють повідомлення про обробку персональних даних заформалізованою мовою, що ускладнює розуміння мети та способів обробки персональних даних неекспертним користувачем. А вимогу щодо обов'язкової письмової форми юрист справедливо називає архаїзмом [72].

У Роз'ясненні Уповноваженого Верховної Ради України з прав людини, від 08.01.2014 вказується, що « […] *інформована згода ґрунтується на одержанні повної, об'єктивної і всебічної інформації стосовно майбутньої обробки персональних даних*» [83].

Проінформованість також розкривається крізь статтю 12 закону, де визначається, що «*суб'єкт обов'язково повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, мету збору персональних даних та осіб, яким передаються його персональні дані*» [76]. Перелік інформації, що розкривається відповідно до закону відповідає вимогам GDPR. Однак, неузгодженість міститься у абз.3 ч.2 статті 12 закону, відповідної до якої, у випадках, коли неможливо повідомити вищевказану інформацію в момент збору, таке повідомлення потрібно здійснити протягом тридцяти днів з моменту збору.

Відповідно до GDPR відсутність елементу «проінформованості» виключає законність згоди. На моє переконання, надання інформації вже після збору персональних даних, тобто *post factum* — це як намагання «узаконити» згоду, отримання якої відбулось із порушенням прав суб'єкта персональних даних.

Щодо визначення мети обробки, то в законі загалом повторюється підхід, зазначений в GDPR. Законом передбачено обов'язок володільця або розпорядника персональних даних отримувати окрему згоду щодо кожної іншої мети обробки.

Законом також враховано положення GDPR щодо «явної», а в контексті закону «однозначної» згоди на обробку чутливих персональних даних. Також розроблено окремий Порядок [84] відповідно до якого володілець персональних даних зобов'язаний повідомити Уповноваженого з прав людини (надалі «Уповноважений»)

щодо факту обробки чутливих персональних даних, аби Уповноважений міг в будь-який час ініціювати перевірку [85].

Однак варто врахувати, що, як зазначалось в Розділі 1.2.1 сучасні технології профілювання дозволяють аналізувати загальну інформацію щодо особи та на основі цієї інформації встановлювати, до прикладу, расову, етнічну приналежність особи, її сексуальну орієнтацію (як у прикладі з Facebook). Особа сама не надає цієї інформації, однак, під час автоматичної обробки відбувається аналіз даних, віднесених до чутливих. Тому доцільно конкретизувати вимогу щодо «однозначності» згоди, врахувавши проаналізовану практику CJEU.

Ще одне критичне зауваження до закону — відсутність дієвих механізмів захисту персональних даних та не ефективний інститут відповідальності за порушення.

Провівши наліз звіту Уповноваженого за 2021 рік, можна дійти висновку, що проблему порушення права на приватність в контексті здійснення обробки персональних даних для маркетингових цілей взагалі не вказується. Лише зазначається статистика, де вказується, що із загальної кількості звернень до Уповноваженого певну, не велику частку займають звернення щодо втручання в особисте і сімейне життя під час використання інформаційно-телекомунікаційних технологій і систем. Водночас, із загальної кількості звернень за рік (4 146) до суду для адміністративного провадження було передано лише 20. Більшість таких звернень стосуються порушення закону під час діяльності зі стягнення заборгованості за грошовими зобов’язаннями фізичних осіб, поширення персональних даних споживачів комунальних послуг, поширення та витік персональних даних із державних установ та організацій [86. с. 25-28].

Така сумна статистика вказує, що на даний час Закон України «Про захист персональних даних» не передбачає дієвого механізму відповідальності. Що стосується обробки персональних даних із рекламними та іншими маркетинговими цілями, Уповноважений взагалі не розглядав такі питання та не визначає їх як пріоритетні чи такі, що потребують уваги.

Порівняно із значними штрафами, які накладаються відповідно до GDRP, адміністративні штрафи в Україні, де найбільша можлива сума штрафу 2000 нмдг є мізерними і по-суті знецінюють весь інститут захисту персональних даних.

Підсумовуючи вищевикладене, Закон України «Про захист персональних даних» містить загальні положення щодо обробки персональних даних, які частково базувались на скасованій директиві. Закон не враховує особливостей здійснення збирання та обробки персональних даних під час отримання згоди на обробку персональних даних в маркетингових цілях, не враховує особливості збирання cookies, автоматизованої обробки та профілювання. Законом також не передбачено дієвого механізму захисту прав суб'єктів персональних даних у разі порушення закону.

РОЗДІЛ 3. НАПРЯМКИ ГАРМОНІЗАЦІЇ ЗАКОНОДАВСТВА УКРАЇНИ ПРО ЦИФРОВИЙ МАРКЕТИНГ НА ШЛЯХУ ДО ЧЛЕНСТВА В ЄС

Гармонізація законодавства України відповідо до положень права Європейського Союзу в частині виконання міжнародно-правових зобов'язань України у сфері європейської інтеграції є невід'ємним та найголовнішим кроком для отримання статусу держави-члена ЄС.

Приведення у відповідність українського законодавства із GDPR стане першим та найголовнішим кроком на шляху до створення захищеного клієнт-орієнтовного цифрового простору.

Відповідно до Розділу III «Юстиція, свобода та безпека» статті 15 «Захист персональних даних» Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони («Угода про асоціацію»), Україна взяла на себе зобов'язання співпрацювати «*з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів*» [87]. Відповідно до статті 11 Угоди про співробітництво між Україною та Європейською організацією з питань юстиції, Україна зобов'язується створити гарантії рівня захисту персональних даних, які б були «принаймні еквіваленті» тим, що містяться у Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року і наступних змін до неї та GDPR [88].

На даний час в Парламенті зареєстровано та активно опрацьовується два євроінтеграційних законопроекти щодо захисту персональних даних.

Перший і основний Проєкт Закону про захист персональних даних від 25.10.2022 року № 8153.

У пояснювальній записці до законопроєкту зазначається, що метою його прийняття є «*пришвидшення інтеграції України до Єдиного цифрового ринку Європейського Союзу, а також максимальне наближення положень національного законодавства до європейських вимог у сфері захисту персональних даних*» [89].

У пояснювальній записці також зазначається, що проєкт закону передбачає приведення термінології у відповідність до законодавства ЄС, розширення та деталізацію принципів обробки персональних даних, встановлення додаткових вимог щодо згоди на обробку персональних даних та врегулювання обробки даних в інтернеті та обробки даних для цілей прямого маркетингу, зобов'язання щодо впровадження контролерами заходів для забезпечення захисту даних за призначенням та за замовчуванням, деталізацію прав суб'єктів та посилення відповідальності за порушення [89].

Проєкт закону передбачає також внесення змін до Закону України «Про електронну комерцію», покладачи обов'язок на учасників відносин у сфері електронної комерції забезпечити захист персональних даних відповідно до (майбутнього) Закону України «Про захист персональних даних» [90].

Серед запровадженої термінології надається визначення профілювання, прямого маркетингу, послуг інформаційного суспільства, широкомасштабної обробки персональних даних.

Загалом текст законопроєкту повторює положення GDPR. Однак, все ще існують прогалини, які мають істотний вплив на захист прав суб'єктів персональних даних під час здійснення прямого маркетингу. Як зазначається у Висновку Комітету з питань інтеграції України до Європейського Союзу («Висновок»), у визначенні «персональні дані» не враховано конкретизовані способи ідентифікації особи [91]. Серед перелічених способів ідентифікації згадуються і дані про місцеперебування та онлайн-ідентифікатор особи (тобто геолокаційні дані, IP адреса, cookies).

Відсутність такої конкретизації малоймовірно суттєво вплине на практику застосування норм законопроєкту, оскільки, на мою думку, недоліки законодавчої техніки не повинні були б обмежувати захист прав осіб. З іншої сторони, свідоме ігнорування такої конкретизації може недобросовісно тлумачитись зацікавленими особами як небажання законодавця підвести під жорстке нормативне врегулювання використання даних, які дозволяють відстежувати поведінку особи в цифровому середовищі в режимі реального часу.

Ще одна важлива для цілей цієї роботи неузгодженість, що згадується в Висновку — включення до терміну «обробка персональних даних», серед іншого, профілювання, що не передбачено в GDPR, однак і не суперечить йому. Визначення профілювання як одного із способів обробки персональних даних означитиме, що до цієї діяльності застосовуватимуться загальні вимоги, що містяться в законі. На моє переконання, це сприятиме якраз ще більшому захисту прав суб'єктів під час обробки їх персональних даних за допомогою автоматизованих систем з метою передбачення їх поведінки.

В іншій частині, законопроєкт потребує доопрацювання, однак не суперечить положенням GDPR [91].

Ще один комплементуючий законопроект, який покликаний наблизити українське законодавство в сфері захисту персональних даних та, як результат, сприятиме створенню сучасного правового регламентування цифрового маркетингу — Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації від 18.10.2021 № 6177 [92].

Як зазначається у пояснювальній записці до законопроекту, відповідно до європейських та міжнародних стандартів на держави-члени покладається обов'язок створити незалежні контролюючі органи. Серед завдань такого органу виділяють моніторинг та сприяння захисту персональних даних, надання консультацій, розгляд скарг щодо порушення законодавства про захист персональних даних та нагляд за контролерами та операторами [93]. Відповідно до статті 2 зазначеного законопроєкту, передбачається створення нового органу виконавчої влади із спеціальним статусом — комісії з питань захисту персональних даних та доступу до публічної інформації. Багато положень законопроєкту зазнали критики, зокрема, щодо статусу запропонованого органу, недоопрацьована процедура оскарження порушень, порушенні принципу правової визначеності [94].

Як зазначає Іван Городиський, адвокат та сертифікований юрист у сфері захисту персональних даних, існує гостра потреба в незалежному органі, однак в теперішньому вигляді законопроект потребує доопрацювання, зокрема виділення його із виконавчої гілки влади [95]. Водночас, Комітет з питань інтеграції України до

Європейського Союзу вказує, що положення законопроєкту не суперечать європейському законодавству, однак потребують доопрацювання [96].

Враховуючи вищезгадані законопроєкти щодо наближення законодавства України у сфері захисту персональних даних до стандартів ЄС, можна ствердно сказати, що євроінтеграційні законопроєкт «Про захист персональних даних» цілком відображає положенням GDPR у контексті регулювання здійснення цифрового маркетингу. Однак, складнощі виникли на етапі створення спеціального органу, на якого б покладались функції із моніторингу, контролю та розгляду скарг щодо порушення законодавства про захист персональних даних.

Окрему увагу потрібно звернути на законопроєкт № 9206 «Про внесення змін до Закону України "Про рекламу" щодо імплементації норм європейського законодавства у національне законодавство України шляхом імплементації окремих положень acquis ЄС у сфері аудіовізуальної реклами (Європейської конвенції про транскордонне телебачення, Директиви Європейського парламенту та Ради 2010/13/ЄС про аудіовізуальні медіа послуги від 10 березня 2010 року зі змінами, внесеними Директивою (ЄС) 2018/1808 від 14 листопада 2018 року) та до деяких інших законів», який вже прийнятий за основу Верховною Радою України.

Сам проєкт закону в більшій мірі стосується європейського законодавства, яке не окреслювалось у даній роботі, оскільки виходить за межі дослідження поставленої проблематики. Проте, у ньому пропонуються важливі зміни до Закону України «Про рекламу». Зважаючи на принцип технологічної нейтральності, вводяться поняття реклами з використанням електронних комунікацій, продакт плейсменту, реклами на платформах спільного доступу та органів саморегулювання [97].

Важливим нововведення міститься в запропонованій редакції частини 10 статті 13, відповідно до якої «*суб'єктам у сфері аудіальних та аудіовізуальних медіа забороняється обробляти зібрані чи іншим чином отримані персональні дані дітей з такою комерційною метою як прямий маркетинг та профілювання, включаючи поведінково орієнтовану рекламу*» [97]. Наведене положення хоча і застосовується до різних видів медіа, воно закріплює фундаментальну заборону опрацьовувати дані дітей для маркетингових цілей.

Таким чином, виконання Україною зобов'язань щодо імплементації європейського законодавства у сфері медіа матиме додатковий позитивний вплив на цифровий маркетинг. Проєкт закону № 9206 викорінює застарілий підхід до виключення інтернет реклами із сфери регулювання українського законодавства.

Спираючись на проведений вище аналіз законодавчих ініціатив українського Парламенту щодо приведення у відповідність законодавства України із законодавством ЄС, можна стверджувати, що наразі Україна стрімко рухається європейських стандартів у захисті персональних даних під час здійснення цифрового маркетингу та у регулюванні сучасних видів реклами.

Важливо зауважити, що законодавець в більшій мірі повторює формулювання норм, закріплених в директивах ЄС. Водночас, законопроєкти містять й прогалини. У випадку врахування рекомендацій комітетів та усунення розбіжностей прийняття законопроєктів № 8153, № 6177 у сфері захисту персональних даних та № 9206 у сфері реклами слугуватиме кроком до гармонізації українського законодавства у сфері цифрового маркетингу та підвищенню захисту прав користувачів в цифровому просторі.

ВИСНОВКИ

Під час написання цієї роботи було проведено дослідження основних напрямків регулювання цифрового маркетингу в ЄС та в Україні. На виконання поставлених завдань було проаналізовано регулювання ЄС та законодавство України. За результатами дослідження необхідно навести наступні висновки.

Україна, обравши шлях європейської інтеграції, зобов'язалась дотримуватись ряду вимог, що стосуються наближення свого законодавства до стандартів Європейського Союзу. Однією з таких вимог є належний захист персональних даних.

Правову основу регулювання цифрового маркетингу є ЄС становить законодавство про захист персональних даних.

Серед основних вимог, які ставляться до контролерів та операторів персональних даних від час здійснення цифрового маркетингу із використанням персональних даних користувачів — отримання законної, явної, проінформованої та однозначної згоди на обробку персональних даних. Додаткові вимоги до згоди встановлюються у випадку здійснення автоматизованої обробки, профілювання, обробки чутливих персональних даних. Важливою умовою є надання достатньої та зрозумілої інформації щодо цілей та мети обробки персональних даних, тому окремо приділено увагу вимогам до cookies банерів.

На відміну від ЄС, в Україні питання захисту персональних даних користувачів під час здійснення цифрового маркетингу майже не врегульовано. Першою й найголовнішою проблемою є концептуально інше законодавство, яке приймалось з метою унормування відносин, що існували у зв’язку із опрацюванням баз даних, а не з метою захисту права на приватність.

Ще одна проблематика, обмежене застосування законодавства про рекламу. На даний час, регулювання рекламної діяльності ігнорує принцип технологічної нейтральності та не поширюється на цифровий простір.

Аби усунути розбіжності в регулюванні, необхідно змінити, в першу чергу, Закон України «Про захист персональних даних», а також внести зміни до Закону України «Про електронну комерцію».

На сьогодні в Парламенті вже наявні євроінтеграційні проєкти законів, що передбачають внесення зазначених змін. Загалом, вони повторюють регулювання, що міститься в законодавстві ЄС. Однак, деякі норми потребують доопрацювання.

На основі проведеного аналізу, пропонується врахувати практику застосування європейського законодавства у сфері захисту персональних даних та прийняти згадані законопроєкти, однак із врахуванням зауважень профільних комітетів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The Economist. ‘Little Brother’. The Economist. URL: https://www.economist.com/special-report/2014/09/11/little-brother?ah=906e69ad01d2ee51960100b7fa502595&zid=291 (date of access: 01.03.2023).
2. Всеукраїнська рекламна асоціація. Об’єми рекламно-комунікаційного ринку України 2021 і прогноз розвитку ринку в 2022 році від ВРК. VRK . Головна. URL: https://vrk.org.ua/news-events/2021/ad-volume-2021.html (дата звернення: 04.03.2023).
3. Digital in Ukraine: All the Statistics You Need in 2021 – DataReportal – Global Digital Insights. DataReportal – Global Digital Insights. URL: https://datareportal.com/reports/digital-2021-ukraine (date of access: 09.03.2023).
4. European Commission, Directorate-General for Communications Networks, Content and Technology, Armitage, C., Botton, N., Dejeu-Castang, L., et al., Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers : final report, Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2759/294673
5. Helberger, N and others, ‘Macro and exogenous factors in computational advertising: Key issues and new research directions.’ Journal of Advertising (2020), 49(4), c. 381.
6. Carrascosa, J. M., J. Mikians, R. Cuevas, V. Erramilli, and N. Laoutaris (2015). ‘I always feel like somebody’s watching me: measuring online behavioural advertising’. In Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies. URL: https://conferences2.sigcomm.org/co-next/2015/img/papers/conext15-final80.pdf (date of access: 09.03.2023)
7. European Parliament's Policy Department for Citizens’ Rights and Constitutional Affairs ‘Regulating targeted and behavioural advertising in digital services How to ensure users' informed consent’, 2021. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU(2021)694680_EN.pdf

8. Irish Council for Civil Liberties 'The Biggest Data Breach', May 2022 URL: https://www.iccl.ie/digitaldata/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe.
9. Norwegian Consumer Council 'Deceived by design. how tech companies use dark patterns to discourage us from exercising our rights to privacy', 2018. URL: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf; "Privacy's Blueprint: The Battle to Control the Design of New Technologies", p. 36 URL:https://books.google.no/books?id=YERMDwAAQBAJ&lpg=PA35&dq=nudging%20away%20from%20privacy&hl=no&pg=PA36#v=onepage&q=nudging%20away%20from %20privacy&f=false
10. European Union, Types of legislation. URL: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en (date of access: 10.03.2023).
11. 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 URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Переклад: https://gdpr-text.com/uk/
12. EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities Adopted on 12 March 2019. URL: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf
13. Агресивна реклама - що це таке, визначення та поняття - 2021 - Economy-Wiki.com. Economy-Pedia.com. URL: https://uk.economy-pedia.com/11038030-aggressive-advertising (дата звернення: 15.03.2023)
14. European Commission, "Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market", 2021/C 526/01

15. Key Statements on the Judgment by the Court of Appeal of 01/24/2014, Ref. No. 5 U 42/12 *Federation of German Consumer Organizations v. Facebook Ireland Limited.* URL:https://www.vzbv.de/sites/default/files/downloads/key-statements-vzbv-facebook-2014-01-24.pdf
16. Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation. Taylor & Francis. URL: https://www.tandfonline.com/doi/full/10.1080/17441056.2018.1538033 (date of access: 01.04.2023)
17. The German Facebook case: the law and economics of the relationship between competition and data protection law - European Journal of Law and Economics. SpringerLink. URL: https://link.springer.com/article/10.1007/s10657-022-09727-8#Fn15 (date of access: 03.04.2023).
18. European Commission - Press corner. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1978 (date of access: 03.04.2023)
19. Акт про цифрові послуги (DSA) та Акт про цифрові ринки (DMA): нові підходи ЄС до регулювання Інтернет-посередників – Лабораторія цифрової безпеки, 2022.
20. The International Council for Advertising Self-Regulation ICAS. URL: https://icas.global/wpcontent/uploads/2014_International_Guide_to_Developing_an_SRO.pdf (date of access: 03.04.2023).
21. EASA – European Advertising Standards Alliance. URL: https://www.easa-alliance.org/about-easa/charter/ (date of access: 03.04.2023).
22. Activity Report 2022 – European Interactive Digital Advertising Alliance. European Interactive Digital Advertising Alliance. URL: https://edaa.eu/portfolio/2022-activity-report/ (date of access: 04.04.2023)
23. European Interactive Digital Advertising Alliance. European Industry SelfRegulatory Framework on Data-Driven Advertising, 2011. URL:

https://edaa.eu/wp-content/uploads/OBA-Framework.pdf (date of access: 04.04.2023).

24. EDAA. Your Online Choices | EDAA. URL: https://youronlinechoices.eu/ (date of access: 05.04.2023).
25. ICC Code of Advertising and Marketing Communication Practice, Building consumer trust through responsible marketing, 2018 Edition. URL: https://cms.iccwbo.org/content/uploads/sites/3/2018/09/icc-advertising-and-marketing-communications-code-int.pdf (date of access: 05.04.2023).
26. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html (date of access: 06.04.2023)
27. Data Protection. European Data Protection Supervisor. URL: https://edps.europa.eu/data-protection/data-protection_en (date of access: 14.04.2023)
28. Council of Europe: European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, 31 August 2020, available at: https://www.refworld.org/docid/5a016ebe4.html (date of access: 06.04.2023)
29. The principles. Information Commissioner's Office (ICO). URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (date of access: 09.04.2023).
30. EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0' Adopted on 20 October 2020 URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
31. EDPB 'Guidelines 8/2020 on the targeting of social media users Version 2.0' Adopted on 13 April 2021. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en

32. EDPB 'Article 29 Working Party Guidelines on transparency under Regulation 2016/679' the targeting of social media users Version 2.0' Adopted on 13 April 2021. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
33. EDPB 'Article 29 Working Party: Guidelines on Transparency under Regulation 2016/679' (wp260rev.01) URL: https://ec.europa.eu/newsroom/article29/items/622227/en
34. EDPB 'Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679 WP259', 28 November 2017 URL: https://ec.europa.eu/newsroom/article29/items/623051/en
35. Bridewell. 'Function Creep': A Very Real Risk That Every DPO Should Be Aware Of | Bridewell. Bridewell. URL: https://www.bridewell.com/insights/blogs/detail/function-creep-a-very-real-risk-that-every-dpo-should-be-aware-of (date of access: 12.04.2023).
36. C-77/21 Digi Távközlési és Szolgáltató Kft. ("Digi") v. Nemzeti Adatvédelmi és Információszabadság Hatóság URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=267405&pageIndex=0&doclang=BG&mode=lst&dir=&occ=first&part=1&cid=365738
37. Whittaker Z. Oracle's BlueKai tracks you across the web. That data spilled online. TechCrunch. URL: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/?guccounter=1 (date of access: 14.04.2023).
38. 'Mobile Operating System Market Share Europe' (*StatCounter Global Stats*) URL: https://gs.statcounter.com/os-market-share/mobile/europe
39. Italian Court of Cassation, First Civil Section, Decision of 29 January 2016, n- 1748. URL:https://curia.europa.eu/juris/document/document.jsf?text=&docid=191305&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1
40. EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, 8 October 2019, URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

41. CJEU, Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, 18 December 2008 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62006CJ0524
42. Irish DPC greenlights Facebook's "GDPR bypass" . URL: https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass (date of access: 20.04.2023).
43. LB (through NOYB) v Facebook Ireland Limited, Draft Decision for the purposes of Article 60 GDPR of the Data Protection Commission made pursuant to Section 113(2)(a) of the Data Protection Act 2018 URL: https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf
44. EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
45. Intersoft Consulting, Email Marketing - General Data Protection Regulation URL: https://gdpr-info.eu/issues/email-marketing/ (date of access: 23.04.2023).
46. Judgment of the Court (Second Chamber) of 11 November 2020 *Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal* URL: https://curia.europa.eu/juris/document/document.jsf;jsessionid=396515B281FF6802B7A64E21FFA138AF?text=&docid=233544&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=17756310
47. *Fashion ID GmbH & Co. KGVerbraucherzentrale NRW eV, interveners v Facebook Ireland Ltd*, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, 29 July 2019 URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=EN
48. Cynthia O'Donoghue & Angelika Christoforou, CJEU delivers judgment on conditions for valid consent in an offline context. Technology Law Dispatch. URL: https://www.technologylawdispatch.com/2020/11/in-the-courts/cjeu-delivers-

judgment-on-conditions-for-valid-consent-in-an-offline-context/ (date of access: 01.05.2023).

49. N. van Eijk, N. Helberger, L. Kool, A. van der Plas and B. van der Sloot, 'Online tracking: questioning the power of informed consent' (2012 Vol. 14 No. 5) URL: https://www.ivir.nl/publicaties/download/Info_2012_5.pdf
50. Meijer, A. Online behavioural advertising and the Proposal for the ePrivacy Regulation. Tilburg, March 2020 URL: http://arno.uvt.nl/show.cgi?fid=151205
51. ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2010 on online behavioural advertising' Adopted on 22 June 2010, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf
52. Законодавство про cookie банери у різних країнах світу. Legal IT group. URL: https://legalitgroup.com/cookie-banne/ (дата звернення: 01.05.2023).
53. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219
54. ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Working Document 02/2013 providing guidance on obtaining consent for cookies', Adopted on 2 October 2013 URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf
55. Judgment of the Court (Grand Chamber) of 1 October 2019 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH Request for a preliminary ruling from the Bundesgerichtshof URL:https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=875890
56. Délibération SAN-2021-023 du 31 décembre 2021. National Commission for Computing and Liberties. Deliberation of the restricted formation n°SAN-2021-023

of December 31, 2021 concerning the companies GOOGLE LLC and GOOGLE IRELAND LIMITED URL: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840062 (date of access: 02.05.2023).

57. Cookies: the Council of State confirms the 2020 sanction imposed by the CNIL against Amazon | CNIL. CNIL |. URL: https://www.cnil.fr/en/cookies-council-state-confirms-2020-sanction-imposed-cnil-against-amazon (date of access: 02.05.2023).
58. ePrivacy Regulation: What Is It & How Does It Affect Cookies? - CookieYes. CookieYes. URL: https://www.cookieyes.com/blog/eprivacy-regulation/ (date of access: 01.05.2023).
59. Ukrinform. Попри війну 76% підприємців планують розширення бізнесу в 2023 році – ЕВА. Укрінформ - актуальні новини України та світу. URL: https://www.ukrinform.ua/rubric-economy/3671001-popri-vijnu-76-pidpriemciv-planuut-rozsirenna-biznesu-v-2023-roci-eva.html (дата звернення: 07.05.2023).
60. Samagalska Y. Legal regulation of internet advertising / Y. Samagalska // Вісник Львівського університету. Серія юридична. - 2018. - Вип. 66. - С. 209. - URL: http://nbuv.gov.ua/UJRN/Vlnu_yu_2018_66_25.
61. Верховна Рада України, Закон України «Про рекламу» № 270/96-ВР від 03.07.1996 р. URL: https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text
62. Окружний адміністративний суд м. Києва, Рішення від 13.06.2022 № 640/22469/21
63. Полтавський окружний адміністративний суд, Рішення від 23.09.2020 № 440/4116/20
64. Проект Закону України від 08.09.2008 № 3126 URL: https://ips.ligazakon.net/document/JF2EU00A?an=192
65. Всеукраїнська Рекламна Асоцівція, Правила ринку. Головна. URL: https://vrk.org.ua/market-rules.html (дата звернення: 02.05.2023).

66. Верховна Рада України, Закон України «Про електронну комерцію» Відомості Верховної Ради (ВВР), 2015, № 45 URL: https://zakon.rada.gov.ua/laws/show/675-19#Text
67. Сенишин О. С., Кривешко О. В. Маркетинг : навч. посібник. Львів : Львівський національний університет імені Івана Франка, 2020.
68. Андрій Корня, Захист персональних даних у процесі використання таргетованої реклами та прямого маркетингу: стаття в Юрист & Закон No. 21, 13 червня 2019 URL: https://uz.ligazakon.ua/ua/magazine_article/EA012761
69. Ігор Усенко, Право на приватність. Коментар до Закону України «Про захист персональних даних». URL: https://privacy.khpg.org/1604922604
70. Черніков А., Європейська Правда «Чому закон про захист персональних даних неможливо виконати?» - 2012. URL: https://www.epravda.com.ua/publications/2012/01/27/314140/
71. Рішення Конституційного Суду України від 20.01.2012 № 2-рп/2012 у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text
72. Дмитро Скумбрій 'Не дуже конфіденційна інформація. Захист даних: GDPR та практика ЄСПЛ'- Юридична Газета. Юридична газета – онлайн версія. URL: https://yur-gazeta.com/dumka-eksprta/ne-duzhe-konfidenciyna-informaciya-zahist-danih-gdpr-ta-praktika-espl.html (дата звернення: 04.05.2023).
73. Дейкун І., 'GDPR чи Закон України «Про захист персональних даних» - що ефективніше?' / the Journal of Eastern European Law / Журнал східноєвропейського права. – 2019. – No 63.
74. Актуальні проблеми цивілістики у цифрову добу: онлайнові соціальні мережі : монографія / за ред. Є. О. Харитонова, О. І. Харитонової; уклад. Б. В. Фасій ; НУ ОЮА. - Одеса : Юридична література, 2018. -с. 116.
75. Берназ-Лукавецька О. М. Захист персональних даних у соціальній мережі / О. М. Берназ-Лукавецька // Часопис цивілістики : наук.-практ. журн. / редкол.: С.

В. Ківалов (голов. ред.), Є. О. Харитонов (заст. голов. ред.), К. Г. Некіт (відп. секр.) [та ін.]. - Одеса, 2018. – Вип. 30. – С. 56-59.

76. Верховна Рада України, Закон України «Про захист персональних даних» Відомості Верховної Ради (ВВР), 2010, № 34, ст. 481 URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
77. Посібник з європейського права у сфері захисту персональних даних : посібник. 2018. 436 с., ст. 75–77. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf
78. Верховний Суд. Велика Палата. Постанова від 18.09.2018 № 806/3265/17 URL: https://verdictum.ligazakon.net/document/76822787
79. Фісун В. Проблеми захисту персональних даних: досвід України та інших країн - Юридична Газета Опубліковано в №10 (716). Юридична газета – онлайн версія. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html (дата звернення: 10.05.2023).
80. Ірина Павлюк. Згода на обробку персональних даних: у яких випадках вона не вимагається - Юридична Газета. Юридична газета – онлайн версія. URL: https://yur-gazeta.com/dumka-eksperta/zgoda-na-obrobku-personalnih-danih-u-yakih-vipadkah-vona-ne-vimagaetsya.html (дата звернення: 02.05.2023).
81. Вінницький апеляційний суд. Постанова № 127/13877/19 від 24 червня 2020 URL: https://reyestr.court.gov.ua/Review/90109587
82. Бем М., Городиський І., Саттон Г., Родіоненко О. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник / М. Бем, І. Городиський, Г. Саттон, О. Родіоненко ; Європейський Союз, Рада Європи - К.: К.І.С., 2015. – с. 58
83. Уповноважений з прав людини, Роз'яснення до Типового порядку обробки персональних даних від 08.01.2014. URL: https://zakon.rada.gov.ua/laws/show/n0001715-14#Text

84. Уповноважений з прав людини, Наказ 08.01.2014 № 1/02-14, Про затвердження документів у сфері захисту персональних даних, Порядок повідомлення Уповноваженого Верховної Ради з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, затверджений наказом Уповноваженого Верховної Ради України з прав людини №1/02-14 від 08 січня 2014р. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

85. Уповноважений Верховної Ради України з прав людини - Порядок та форми здійснення повідомлень, додаткова інформація. Уповноважений Верховної Ради України з прав людини - Головна. URL: https://ombudsman.gov.ua/uk/oprilyudnennya-informaciyi-na-vimogu-statti-9-ta-24-zakonu-ukrayini-pro-zahist-personalnih-danih/poryadok-ta-formi-zdijsnennya-povidomlen-dodatkova-informaciya (дата звернення: 10.05.2023).

86. Щорічна Доповідь Уповноваженого з прав людини Про стан додержання прав і свобод людини і громадянина в Україні, 2021 URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/schoricha-dopovid-2021.pdf

87. Відомості Верховної Ради, Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, ратифіковано із заявою Законом № 1678-VII від 16.09.2014URL: https://zakon.rada.gov.ua/laws/show/984_011

88. Відомості Верховної Ради, Угода про співробітництво між Україною та Європейською організацією з питань юстиції, ратифіковано Законом № 1839-VIII від 08.02.2017 URL: https://zakon.rada.gov.ua/laws/show/984_024-16#Text

89. Верховна Рада України, Законопроєкти, Пояснювальна Записка до Проєкту Закону України «Про захист персональних даних» URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1517430

90. Верховна Рада України, Законопроєкти, Проєкт Закону про захист персональних даних № 8153 від 25.10.2022 URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707
91. Верховна Рада України, Комітет з питань інтеграції України до Європейського Союзу, Висновок щодо проєкту Закону про захист персональних даних https://itd.rada.gov.ua/billInfo/Bills/pubFile/1562145
92. Верховна Рада України, Законопроєкти,Проєкт Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації від 18.10.2021 № 6177. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/27996
93. Верховна Рада України, Законопроєкти, Пояснювальна Записка до Проєкту Закону України про Національну комісію з питань захисту персональних даних та доступу до публічної інформації від 18.10.2021 № 6177 . URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/971272
94. Українська Гельсінська Спілка з прав людини Аналіз проєкту Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації», 2021. № 6177 URL: https://www.helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-natsionalnu-komisiiu-z-pytan-zakhystu-personalnykh-danykh-ta-dostupu-do-publichnoi-informatsii-6177/
95. Іван Городиський. Ініціативи створення нового органу із захисту персональних даних: чи достатньо гарантій його незалежності | Центр Дністрянського. Центр Дністрянського | Центр Дністрянського. URL: https://dc.org.ua/news/iniciativi-stvorenna-novogo-organu-iz-zahistu-personalnih-danih-ci-dostatno-garantij-jogo-nezaleznosti?fbclid=IwAR0KdjVswJ7tquHfwb3WWvMnN7ESLDoahUaRRe_R6tcrIkKHMByT4K0EOtM (дата звернення: 06.05.2023).
96. Верховна Рада України, Комітет з питань інтеграції України до Європейського Союзу, Висновок щодо проєкту Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації (реєстр. №

6177 від 18.10.2021, н.д. Тарасенко Т.П., Чернєв Є.В. та інші) URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1201306

97. Верховна Рада України, Проєкт Заокону України № 9206 «Про внесення змін до Закону України "Про рекламу" щодо імплементації норм європейського законодавства у національне законодавство України шляхом імплементації окремих положень acquis ЄС у сфері аудіовізуальної реклами (Європейської конвенції про транскордонне телебачення, Директиви Європейського парламенту та Ради 2010/13/ЄС про аудіовізуальні медіа послуги від 10 березня 2010 року зі змінами, внесеними Директивою (ЄС) 2018/1808 від 14 листопада 2018 року) та до деяких інших законів». URL: https://itd.rada.gov.ua/billInfo/Bills/Card/41772