Вищий навчальний заклад «Український католицький університет»

Факультет суспільних наук
назва факультету

Кафедра теорії права та прав людини
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (магістерської роботи)
магістр
(освітній ступінь)

на тему «Правова регламентація захисту персональних даних у цільовому маркетингу»

Виконала:
студентка ІІ курсу, групи СПЛ17/М
спеціальності
081 «Право»
(шифр і назва спеціальності)

Олійник Вікторія-Анна Олександрівна
(прізвище та ініціали)

Керівник Бем Маркіян
(прізвище та ініціали)

Рецензент Гродиський Іван
(прізвище та ініціали)

Львів – 2018 року

Вищий навчальний заклад «Український католицький університет»

Факультет суспільних наук

Кафедра теорії права та прав людини

Освітній ступінь **магістр**

Спеціальність **081 – «Право»**

Освітня програма **«Права людини»**

ЗАТВЕРДЖУЮ

Завідувач кафедри_____

_____

“____” _____20___року

З А В Д А Н Н Я

1. НА ДИПЛОМНИЙ ПРОЕКТ (МАГІСТЕРСЬКУ РОБОТУ) СТУДЕНТЦІ

Олійник Вікторії-Анни Олександрівни

(прізвище, ім’я, по батькові)

1. Тема проекту (роботи): «Правова регламентація захисту персональних даних у цільовому маркетингу».

керівник проекту (роботи) Бем Маркіян, кандидат юридичних наук,

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені “___”_____20__року №___ (дата і номер протоколу ВР факультету).

2. Строк подання студентом проекту (роботи) 17 грудня 2018 року.

3. Вихідні дані до проекту (роботи):

З часу розробки цифрових технологій важливість захисту персональних даних постійно зростає, оскільки їх обробка стає дедалі простішою та масштабнішою. Виник новий спосіб визначення потреб на ринку і просування продукції (робіт, послуг) – цільовий маркетинг. У зв’язку з цим з’явилася потреба врегулювати відносини, пов’язані із захистом персональних даних, адже технології, що використовуються у цільовому маркетингу становлять загрозу для права людини на приватність.

Тому на міжнародному рівні питання захисту даних від несанкціонованої обробки особливо стимулюється. У цьому контексті

було підписано багато угод, включаючи Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних, яку ратифікувала Україна та прийняла відповідні законодавчі акти, передусім Закон «Про захист персональних даних». У Європейському Союзі були прийняті директиви, а нещодавно – Загальний регламент про захист даних. Відтак, це питання надзвичайно актуальне.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

- Що є предметом законодавства про захист персональних даних?
- Як регламентується захист персональних даних на міжнародному рівні та в Україні?
- Що таке цільовий маркетинг?
- Яку загрозу для прав людини створюють технології, що використовуються для пошуку цільової аудиторії?
- Які права суб'єктів персональних даних при обробці їх інформації в ході цільового маркетингу?
- Які обов'язки покладені законодавством на володільців персональних даних, що застосовують технології цільового маркетингу?
- Які гарантії існують для захисту персональних даних у цільовому маркетингу?
- Хто і як здійснює контроль за захистом персональних даних?
- Яким чином можна притягнути до відповідальності порушників законодавства про захист персональних даних?

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Відсутній.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	Завдання прийняв
1	Маркіян Бем, старший викладач		
2	Маркіян Бем, старший викладач		
3	Маркіян Бем, старший викладач		

7. Дата видачі завдання 01.06.2018

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	2. Примітка
1	Аналіз наукової літератури (первинний)	09.05.2018	
2	Аналіз наукової літератури (вторинний)	01.09.2018	
3	Аналіз регулювання в різних юрисдикціях:		
4	А) Європейський Союз	06.07.2018	
5	Б) Україна	10.08.2018	
6	В) Інші юрисдикції (за результатами виконання завдань 1 та 2)	10.08.2018	
7	Г) Аналіз судової практики (ЄСПЛ, Суд ЄС, українські суди)	01.09.2018	
8	Написання І розділу (порівняльний аналіз права у різних юрисдикціях)	12.08.2018	
9	Написання ІІ розділу (визначення місця права на забуття у системі прав людини)	07.09.2018	
10	Написання ІІІ розділу (право на забуття в Україні)	01.10.2018	
11	Написання вступу та висновків (за результатами виконання завдання 5,6 та 7)	01.11.2018	
12	Виправлення недоліків та доопрацювання дослідження	30.11.2018	
13	Належне оформлення роботи	01.12.2018	

Студент _____ **Олійник В.-А.**
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ **Бем М.**
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП

Глобалізація, що набирає все більших масштабів, розвиток інформаційного суспільства призводять до необхідності захисту приватної сфери життя людини, до якої повинна мати доступ лише одна особа чи обмежене коло осіб. Те, на скільки конкретна держава зможе забезпечити захист персональних даних, і визначає її можливість бути гарантом відповідних конституційних, а також наданих іншими законодавчими актами прав і свобод.

Однак, людський прогрес детермінує все більше проблем, які потребують врегулювання. Тому нормативно-правова база повинна постійно оновлюватися, пристосовуватись до новітніх технологій, особливо якщо вони можуть завдати шкоду охоронюваним інтересам суспільства.

Саме тому на міждержавному рівні постійно постає питання захисту персональних даних від несанкціонованої обробки, що призводить до підписання конвенцій, серед яких, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. До неї Україна приєдналася у 2006 році. З тих пір Верховною Радою було прийнято Закон «Про захист персональних даних», надано відповідні повноваження Уповноваженому Верховної Ради з прав людини, закріплено міри відповідальності за порушення законодавчих заборон.

Втім, досі закріплене Конституцією України право на приватність гарантується не повною мірою. Значний ризик для прав людини, а саме – деанонімізацію (небажану та незаконну ідентифікацію), несуть в собі технології цільового маркетингу. Передусім, тому, що недостатнє правове регулювання та технологічне забезпечення значно ускладнює процес проведення превентивних дій щодо недопущення незаконної обробки персональних даних чи застосування мір відповідальності до винних осіб. Сама фізична особа часто навіть не здогадується про те, що її даними володіють інші суб'єкти правовідносин.

Актуальність теми зумовлена відсутністю в українському законодавстві правових норм, що відповідають сучасному розвиткові технологій, які використовуються для ідентифікації особи у ході цільового маркетингу.

Новизна роботи полягає в тому, що вперше проаналізовано специфіку обробки персональних даних у цільовому маркетингу. Наукові напрацювання з цього питання характеризуються фрагментарністю, розглядають тільки певний аспект проблематики, що є предметом дослідження.

Теоретичне і практичне значення роботи полягає у закладенні фундаменту для подальших досліджень у наукових розробок щодо удосконалення захисту персональних даних в державі, а також – можливості практичного застосування висновків, зроблених на підставі дослідження у діяльності з надання маркетингових послуг, та безпосередньо – при здійсненні контролю за такою діяльністю.

Мета – проаналізувати законодавство про захист персональних даних з точки зору відповідності та достатності правового регулювання використання персональних даних у ході цільового маркетингу; встановити практичні проблеми, які потребують вирішення.

Поставлена мета досягається шляхом розв’язання наступних **завдань:**

1. Дослідити предмет законодавства про захист персональних даних у міжнародній та національній правових системах.
2. Розглянути специфіку цільового маркетингу та обробки персональних даних у ході його використання, встановити, які правові ризики при цьому виникають.
3. Проаналізувати права суб’єктів персональних даних та обов’язки володільців даних у ході цільового маркетингу.
4. Виокремити гарантії, що сприяють забезпеченню прав суб’єктів персональних даних під час використання технологій цільового маркетингу.
5. Встановити, яким чином здійснюється захист прав суб’єктів персональних даних.

6. Дослідити можливість притягнення до відповідальності володільців персональних даних, що використовують технології цільового маркетингу.

Об'єктом дослідження виступають правові відносини, що виникають при здійсненні цільового маркетингу та торкаються захисту права особи на повагу до приватного життя.

Предметом дослідження є правове регулювання захисту персональних даних у ході цільового маркетингу.

Теоретичні підходи і методологія дослідження. У ході роботи ми використовували історичний метод, при аналізі формування законодавства про захист персональних даних; системний метод – при комплексному дослідженні норм міжнародного та національного законодавства про захист персональних даних, а при їх співставленні – метод порівняння; метафізичні та загально-філософські методи (аналіз, синтез, індукція та дедукція) – при опрацюванні норм законодавства та екстраполювання їх на сферу цільового маркетингу.

Дослідження базувалося на фундаментальних працях українських та іноземних науковців: Г. Булля, С. Вард, Б. Джеррі та Д. Міллігана, Д. Кліффорда, А. Роснагеля, Ф. Шольца, М. Бема та І. Городиського, Б. Воєводіна, Ю. Зоріної, О. Карась, А. Пазюк.

Структура роботи. Робота складається зі вступу, теоретичного і двох практичних розділів. У кінці роботи подаються детальні висновки, які випливають зі змісту дослідження, а також список використаних джерел та додатки. Обсяг тексту роботи становить 88 сторінок. Перелік літератури налічує 115 позицій.

РОЗДІЛ І
ВПЛИВ ЦІЛЬОВОГО МАРКЕТИНГУ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

З поширенням комп'ютерних баз даних для зберігання особистої інформації в Європі та Америці в 1970-х, почало з'являтися законодавство про захист даних[1]. Швидке використання цієї нової інформаційної технології урядовими установами та бізнесом викликало побоювання щодо потенційно шкідливих наслідків, таких як злами даних або таємне спостереження з боку державних чи комерційних структур, що мали потенційно приголомшливий вплив на особисту приватність, свободи і права людини.

Саме тоді з'являється необхідність вберегти особу від можливої та, водночас, небажаної ідентифікації, захищаючи її основні права. З цього бере свій початок законодавство про захист персональних даних.

1.1. Предмет законодавства про захист персональних даних

Термін «захист даних» започаткований у Європі для позначення законодавства про захист приватності (англ. *privacy-protective legislation*), тоді як у США говорили про приватність самих даних (*data privacy*)[2].

Законодавство про захист персональних даних стосується не самих лише даних, а права особи на приватність (від англ. *privacy*). Ця назва не була закріплена в законах чи міжнародних актах, але правозастосовною практикою визнається предметом регулювання[3].

Через розмитість поняття «приватності» та динамічний розвиток суспільних відносин, практично немає необхідності давати дефініцію цьому терміну, оскільки визначення саме по собі не відграє особливо важливої ролі

[1] Cate F. The EU *Data Protection Directive, Information Privacy, and the Public Interest* [Електронний ресурс] / Fred H. Cate // Articles by Maurer Faculty. – 1995. – Режим доступу: https://www.repository.law.indiana.edu/facpub/646. Regan, P.M. *Personal information policies in the United States and Britain: The dilemma of implementation considerations*. Journal of Public Policy, 1984, 4(01). p. 19-38.
[2] Swire P., Ahmad K. *Foundations of Information Privacy and Data Protections*. International Association of Privacy Professionals, Portsmouth, 2012. p. 4.
[3] Schiedermair S. *Der Schutz des Private*. Suhrkamp Verlag AG, Berlin 2001. p. 22.

для захисту персональних даних[4]. Теоретично, право на приватність розглядається у всіх аспектах, необхідних для створення та забезпечення державою необмеженої свободи особистості[5]. Воно містить у собі різні складові[6]. До них відносяться: фізична недоторканність та здоров'я[7], варіації поведінки та особистих якостей, а також здатність індивідуума до прийняття рішення[8]. На підставі цієї інформації третя сторона може зробити певні висновки щодо особи. У зв'язку з цим, виникає поняття так званої «інформаційної приватності»[9], що дозволяє кожному (кожній) самостійно вирішити, хто, і до якої інформації про нього (неї) може отримати доступ[10].

Ентоні Лестер, узагальнюючи, виділяє три складові поняття «приватності»:

- повага до особистої ідентичності, включаючи релігійні переконання (чи їх відсутність), етнічного походження, гендерних та сексуальних вподобань;
- повага до психологічного і фізичного стану, включаючи право вибору лікування та право відмовитися від непотрібних медичних втручань;
- повага до конфіденційності приватної інформації: від таємниці листування – до захисту від непотрібного взяття зразків відбитків пальців та/чи ДНК[11].

Зрозуміло, що захист персональних даних не є самоціллю, натомість – виступає одним із елементів захисту самої особи[12]. Якщо би дані були предметом правового регулювання, ця галузь би не входила до сфери захисту прав людини, а, швидше, стосувалася б технологій обробки персональних даних. Отже, захисту потребують не дані *per se*, а інформація, яка сприяє

[4] Schwichtenberg S. *Datenschutz in drei Stufen*. Springer Vieweg, Bremen 2018, p.. 11.
[5] Sandfuchs B. *Privatheit wider Willen*. Mohr Siebeck, Tübingen 2015, p. 9.
[6] Mills J. *Privacy. Oxford University Press*, 2008, 408 p. 14.
[7] *Ibid.*
[8] Sandfuchs B. *Privatheit wider Willen*, p. 10.
[9] Rössler B. *Der Wert des Privaten*. Suhrkamp Verlag, 2001, p. 201.
[10] Schwichtenberg S. *Datenschutz in drei Stufen*, p. 21.
[11] Lester A. *Five Ideas to Fight For: How Our Freedom is Under Threat and Why It Matters*. Oneworld Publications, London 2016, 256 p.
[12] Bull H. P. *Informationelle Selbstbestimmung – Vision oder Illusion*. Mohr Siebeck, Tübingen 2011, p.1.

ідентифікації особи. Тому, термін «захист персональних даних» не зовсім вірно відображає суть цього поняття[13].

Предметом захисту персональних даних є правові відносини, пов'язані із захистом і обробкою персональних даних[14]. Таке визначення закріпив законодавець у Законі України «Про захист персональних даних». Однак, у такій дефініції допущено логічну помилку – визначення невідомого через невідоме. Адже термін «захист» тлумачиться через «захист». А поняття обробки розкривається у наступних статтях Закону. До цього ми повернемося пізніше у підрозділі 1.1.2., а поки що зосередимося на тому, якими актами такі відносини регламентуються на міжнародному рівні.

2.1.1. Міжнародне регулювання захисту персональних даних

Цей підрозділ знову починаємо із загального. Оскільки персональні дані є аспектом права особи на повагу до приватного життя (приватність), про що йшла мова на початку підрозділу 1.1., то історія правового регулювання сягає сивої давнини, коли відокремленого від інших прав людини, права на захист персональних даних не існувало.

Саме Велику Британію науковці вважають матір'ю законодавства про приватність. Ще у Великій Хартії Вольностей 1215 р. було закладено його правову основу. У 1628 р. Головний суддя Англії та Вельсу Едвард Кок запропонував Королю підписати «Петицію про право» (англ. *Petition of Right*), в якій було сформульовано принцип особистої недоторканості. Згодом він кристалізується в «Габеас Корпус Акт» 1679 р. (англ. *Habeas Corpus Act*) та в Біллі про права 1689 р. (англ. *Bill of Rights*)[15].

Право на повагу до приватного життя закріплено у різноманітних універсальних міжнародно-правових актах. У ст. 12 Загальної декларації прав

---

[13] Bull H. P. *Informationelle Selbstbestimmung – Vision oder Illusion*. Mohr Siebeck, Tübingen 2011, p.1.

[14] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

[15] Олійник В. С. Конституційне право людини на особисту недоторканність і його забезпечення органами внутрішніх справ України: дис. … кандидата юрид. наук : 12.00.02 «Конституційне право» / В. С. Олійник ; Київськ. нац. ун-т внутр. справ. – Київ, 2006. – 225 с.

людини від 10 грудня 1948 р. міститься норма про заборону безпідставного втручання у особисте і сімейне життя[16]. У зв'язку з цим, слід згадати ст. 17 Міжнародного Пакту про громадянські та політичні права 1966 р.:

> "1. Ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію. 2. Кожна людина має право на захист закону від такого втручання чи таких посягань"[17].

Аналогічне за змістом положення включене і до ст. 16 Конвенції про права дитини 1989 р.[18].

Основні принципи права на повагу до приватного життя отримали свій розвиток і в інших міжнародно-правових документах. У рамках Організації з економічного співробітництва та розвитку (далі – ОЕСР) було розроблено «Базові принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних» (англ. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), схвалені Рекомендацією Ради ОЕСР від 23 вересня 1980 р., нова редакція яких була ухвалена у 2013 р.[19]. Генеральна Асамблея ООН резолюцією №95 (XLV) прийняла «Керівні принципи регулювання комп'ютерних файлів, які містять персональні дані» (англ. Guidelines for the Regulation of Computerized Personal Data Files)[20].

На регіональному рівні положення щодо захисту права на приватність містяться в документах, прийнятих відповідними регіональними організаціями. Так, за океаном діє Американська конвенція з прав людини 1969 р., що у ст. 11

---

[16] Загальна декларація прав людини ООН від 10 грудня 1948 р. [Електронний ресурс] / Генеральна Асамблея ООН // Сайт Верховної Ради України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/995_015.

[17] Міжнародний пакт про громадянські і політичні права ООН від 6 грудня 1966 р. [Електронний ресурс] / Генеральна Асамблея ООН // Сайт Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_043.

[18] Конвенція про права дитини від 20.11.1989 р. // Зібрання чинних міжнародних договорів України. – 1990. – № 1. – С. 205.

[19] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Електронний ресурс]. – 2013. – Режим доступу: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[20] Стандарти захисту персональних даних в соціальній сфері / М. В. Бем,, І. М. Городиський. – Львів: б.в., 2018. – 110 с.

закріплює право на повагу до людської честі та гідності, а також заборону безпідставного чи образливого втручання в особисте і сімейне життя людини[21].

Американська Федеральна Комісія з Комунікацій (America's Federal Communications Commission) 27 жовтня 2016 року оголосила про нове правило захисту особистої конфіденційності у всесвітній павутині. Інтернет-провайдери повинні отримувати згоду користувачів, перед тим, як збирати та обмінюватися даними, які вважаються чутливими, включаючи фінансову інформацію та історію веб-перегляду користувачів. Однак, ці норми не торкаються діяльності таких великих провайдерів, як *Google, Facebook*, оскільки її регулювання здіснює інший орган – Федеральна торгова комісія (Federal Trade Commission)[22].

На європейському рівні, у ст. 8 Конвенції про захист прав людини і основоположних свобод 1950 р. зазначено: "Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції"[23]. У ст. 7 Хартії основних прав Європейського Союзу задекларовано право на повагу до особистого і сімейного життя, а ст. 8 закріплює право на захист відомостей про особу, що мають персональний характер[24].

> "2. Така інформація може використовуватися тільки згідно встановлених правил у відповідних цілях і на основі наданого заінтересованою особою дозволу чи на інших правомірних підставах, передбачених законом. Кожна людина має право на доступ до належать до нього зібраним відомостями і добиватися внесення в них виправлення. 3. Дотримання цих правил підлягає контролю з боку незалежного органу"[25].

Останні два положення закріплюють важливі принципи для обробки персональних даних, на яких повинні базуватися інші нормативно-правові акти

---

[21] Американская Конвенция о Правах Человека [Електронний ресурс]. – Режим доступу: http://hrlibrary.umn.edu/russian/instree/Rzoas3con.html.

[22] Digital advertisers battle over online privacy [Електронний ресурс] // The Economist. – 2016. – Режим доступу: https://www.economist.com/business/2016/11/05/digital-advertisers-battle-over-online-privacy.

[23] Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 04 листопада 1950 року // Офіційний вісник України. – 1998. – № 13. – Ст. 270.

[24] Хартія основних прав Європейського Союзу [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/card/994_524#Current.

[25] *Ibid.*

країн-членів ЄС, та й загалом – законодавство про захист персональних даних, бо ці норми носять або мають універсальний характер. Перш за все, повинні існувати правила щодо обробки персональних даних. Дозвіл на будь-які дії зі своїми даними повинен давати суб'єкт персональних даних, однак можуть існувати визначені законом винятки з цього загального правила. Суб'єкту персональних даних повинна надаватися можливість дізнаватися, хто, які відомості, і в якому обсязі, про нього збирає та вносити поправки до них. До того ж, важливим є створення в державі контролюючого органу, який здійснюватиме моніторингову та наглядову діяльність, притягатиме порушників законодавства (про захист персональних даних) до відповідальності.

Засади обробки персональних даних, права особи у зв'язку з обробкою відомостей про неї, правові основи транскордонної передачі даних закріплено у Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р.[26]. Згодом було прийнято Додатковий протокол до неї від 08 листопада 2001 р.[27]. Ці документи ратифіковані Україною 6 липня 2010 р. Протокол конкретизував положення, викладені в Конвенції. Він містить норми щодо транскордонного потоку інформації, а також – закріплює необхідність створення спеціального органу для здійснення функцій нагляду та контролю за додержанням законодавства про захист персональних даних. Зважаючи на сучасні тенденції розвитку технологій, що пов'язані з автоматизованою обробкою інформації, Комітет Міністрів Ради Європи має на меті актуалізувати положення Конвенції № 108[28].

Європейський Союз на даний момент надзвичайно прискіпливо займається питаннями захисту персональних даних. Схвалені ним норми є передовими стандартами у цій сфері. Серед них:

---

[26] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Міжнародний договір / Офіційний вісник України. – 2011 – № 1, № 58. – 2010. – Ст. 1994. – Ст. 85.

[27] Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних: Міжнародний договір / Офіційний вісник України. – 2011 – № 1, № 58. – 2010. – Ст. 1994. – Ст. 86.

[28] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 7.

- Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (далі – Загальний регламент про захист даних)[29], який з 25 травня 2018 року замінив Директиву 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 р.[30];
- Директива 2002/58/ЄС Європейського Парламенту та Ради «Про обробку персональних даних та захист таємниці сектора електронних комунікацій» (Директива про секретність та електронні комунікації) від 12.07.2002 № 2002/58/ЄС, яку незабаром, але не раніше 2020 року замінить новий Регламент «Про повагу до приватного життя та захисту персональних даних в електронній комунікації та скасування Директиви 2002/58/ЄС» (далі – Регламент про конфіденційність та електронні повідомлення, англ. – Regulation on Privacy and Electronic Communications)[31].

Відповідно до норм Загального регламенту, ***персональними даними*** визнається

> "інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати (прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи). І будь-які дії з цими відомостями інших осіб, яким до них надано доступ, становлять обробку персональних даних"[32].

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

[30] Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року / Європейський Союз. – [Електронний ресурс]. Цит. 02.02.2018 р. Режим доступу – http://zakon4.rada.gov.ua/laws/show/994_242.

[31] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[32] Загальний регламент про захист даних (ЄС) 2016/679 від 27 квітня 2016 року [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16.

Незважаючи на те, що зазначені вище акти не є частиною національного законодавства, положення Директиви 95/46/ЄС були імплементовані в Закон України «Про захист персональних даних», прийнятий на виконання Конвенції № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». А Загальним регламентом обумовлено дотримання встановлених ним норм при обробці даних резидентів ЄС. Отже, настав час проаналізувати нормативно-правові акти нашої держави, зокрема, і на предмет відповідності нововведенням.

2.1.2. Національна регламентація захисту персональних даних

Для українського законодавця характерне введення міжнародних стандартів у систему принципів захисту відомостей, що становлять персональну інформацію. Так, Конституція України передбачає право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31), інформаційну приватність (ст. 32)[33]. Закріплена заборона втручання в особисте і сімейне життя людини, введено обмеження на обробку конфіденційної інформації, гарантовано можливість доступу до особистих відомостей та захисту своїх прав. Ці приписи знаходять відображення в інших законодавчих актах і тлумачаться в рішеннях Конституційного суду України.

У справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 лютого 2012 року № 2-рп/2012 КСУ інтерпретує поняття інформація про особисте та сімейне життя особи[34]. Стосовно питання згоди на обробку інформації (в тому числі, конфіденційної) про особу, КСУ висловився у рішенні у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа

[33] Конституція України прийнята Верховною Радою України 28.06.1996 р. № 254к/96–ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
[34] Рішення Конституційного Суду України від 20.01.2012 р. № 2-рп/2012 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/v002p710-12.

К.Г.Устименка)[35]. Тому ці два рішення також є формальними джерелами правових норм про захист персональних даних.

Окрім цього, Цивільний кодекс України у статтях 301, 303, 304, 306, 307, 308, а також закріплений у п. 1 ч. 1 ст. 3 ЦК принцип неприпустимості свавільного втручання у сферу особистого життя людини, дає можливість громадянам охороняти своє право усіма доступними способами цивільного захисту, в тому числі, самозахисту та у судовому порядку[36]. Окрім цього, закріплюється позитивний обов'язок держави забезпечувати і гарантувати особам здійснення їх прав.

Від *lex generalis* перейдемо до *lex specialis* – до Закону України «Про захист персональних даних» та Закону «Про захист інформації в інформаційно-телекомунікаційних системах». До першого з них ми неодноразово зверталися під час нашого дослідження, а останнім – регулюються механізми роботи банерообмінних мереж, аналітичних сервісів та інформаційно-телекомунікаційних систем[37].

Окрім цього, існують також підзаконні нормативно-правові акти, затверджені Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14:

- Типовий порядок обробки персональних даних, який регламентує основні вимоги щодо організації обробки персональних даних володільцями[38], а також Роз'яснення, затверджене Уповноваженим Верховної Ради України з прав людини[39];
- Порядок здійснення Уповноваженим ВРУ контролю за додержанням законодавства про захист персональних даних, що містить, в тому

[35] Рішення Конституційного Суду України від 30.10.1997 р. № 5-зп (справа К. Г. Устименка) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v005p710-97.

[36] Цивільний кодекс України: Закон України № 435-IV від 16 січня 2003 р. // Офіційний вісник України. – 2003. – № 11. – Ст. 461.

[37] Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України, 1994, № 31, ст. 286

[38] Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v1_02715-14.

[39] Роз'яснення до Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/n0001715-14.

числі, положення стосовно процедури перевірки контролюючим органом осіб, що здійснюють обробку персональних даних[40];

- Порядок повідомлення Уповноваженого ВРУ 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, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації[41];
- Про затвердження Порядку обробки персональних даних в інформаційній автоматизованій системі «Облік передачі та отримання даних з Євроюсту», що прийняті на виконання Первинного акта «Про ратифікацію Угоди про співробітництво між Україною та Європейською організацією з питань юстиції» від 08 лютого 2017 № 1839-VIII 1839-VIII, та Міжнародного акта «Угода про співробітництво між Україною та Європейською організацією з питань юстиції» від 27 червня 2016[42].

Зрозуміло, що основним серед усієї сукупності актів є Закон України «Про захист персональних даних». Попередні 4 підзаконні акти прийняті саме на його виконання. У цілях нашого дослідження, ми здійснимо порівняння Загального регламенту про захист даних із сучасним українським законодавством у 2 і 3 розділах, проаналізуємо положення Регламенту про конфіденційність та електронні повідомлення, що перебуває на стадії розробки, а також розглянемо вплив цих нормативно-правових актів на маркетингову діяльність суб'єктів господарювання.

Саме Закон України «Про захист персональних даних» містить поняття персональних даних, їх обробки, визначає суб'єктів цих правовідносин. Ним встановлюються правила будь-яких операцій з персональними даними (автоматизованих чи неавтоматизованих), передбачено повноваження

[40] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 9.
[41] *Ibid.*
[42] Наказ Ганеральної Прокуратури України від 13.07.2018 № 134 «Про затвердження Порядку обробки персональних даних в інформаційній автоматизованій системі "Облік передачі та отримання даних з Євроюсту"» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0908-18.

контролюючих органів, можливість притягнення правопорушників до відповідальності тощо.

Але не все, що стосується особистих відомостей регулюється Законом. Обробка персональних даних з архівів репресивних органів регламентована Законом України «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 років»[43].

Дія Закону не поширюється на створення баз персональних даних в особистих і побутових, творчих і журналістських цілях[44]. Стосовно журналістської діяльності варто згадати про виняток, коли здійснюється явне і грубе порушення прав на повагу до приватного життя інших осіб, бо в такому випадку можуть бути застосовані санкції, передбачені Законом. Тут прослідковується тонка грань між публічним і приватним життям особи, між захистом персональних даних та свободою вираження поглядів. Широко відомим є рішення ЄСПЛ у справі «Фон Ганновер проти Німеччини»[45]. Тут суд розмежував факти, що здатні внести вклад у розвиток демократичного суспільства та такі, що становлять сферу приватності. Отже, навіть фото покійного принца Реньє III могло бути опубліковане у ЗМІ, тому що воно впливає на думку громадськості. Так само у справі «Флінккіля та інші проти Фінляндії» ЄСПЛ не відмітив вторгнення в особисте життя. Так, журналістам, які розмістили відомості про коханку державного посередника було виплачено грошову компенсацію за те, що їх раніше притягнули до відповідальності. Суд вважав, що оскільки ця жінка фігурувала у подіях, що сталися біля будинку відомого публічного діяча, то відповідно інформація стосовно цього випадку може бути розголошеною[46].

[43] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 9.
[44] Про захист персональних даних (Текст резюме від 01.06.2010) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/anot/2297-17.
[45] Von Hannover v. Germany (заява № 40660/08, рішення від 24.06.2005).
[46] Flinkkila and Others v. Finland (заява № 25576/04, рішення від 06.04.2010).

Тобто межею захисту персональних даних є також право на свободу вираження поглядів. І, якщо в Європі перевага надається першому[47], то в ліберальних США – навпаки. Тому в них досі немає єдиного нормативно-правового акта на кшталт Загального регламенту про захист даних.

Стосовно сутності ***захисту інформації*** мусимо заглянути в інший акт – Закон України «Про інформацію», згідно ст. 1 якого захист становить сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї[48].

Особливе значення має поняття «***обробки***». Адже, воно включає збирання, реєстрацію, накопичення, зберігання, адаптування, зміну, поновлення, використання і поширення (розповсюдження, реалізацію, передачу), знеособлення, знищення персональних даних[49]. Тобто, будь-які операції з персональними даними, як в Україні, так і закордоном, автоматично визнаються обробкою персональних даних.

Стосовно дефініції терміну «персональні дані», серед науковців точиться дискусія. Так, В. Брижко зазначає, що це сукупність чи окремі відомості про фізичну особу, яка ідентифікована, або може бути ідентифікованою[50]. Інша науковець, Г. Виноградова, вважає, що персональні дані – це сукупність документованих або публічно оголошених відомостей про фізичну особу[51]. На нашу думку, не варто зводити персональні дані тільки до таких відомостей, що доступні третім особам, внаслідок їх розголошення чи документального оформлення. Адже, особиста інформація властива людині, буквально, від народження (наприклад, дата народження). І не обов'язково чекати запису в журналі обліку новонароджених чи реєстрації в органах РАЦС.

---

[47] Нагнічук О. І. *Співвідношення права на свободу вираження щодо публічних осіб та права на повагу до приватного та сімейного життя публічних осіб у практиці Європейського суду з прав людини* / О. І. Нагнічук // Наукові записки НаУКМА. Юридичні науки. – 2015. – Т. 168. – С. 72-77.

[48] Закон України «Про інформацію» Відомості Верховної Ради України (ВВР), 1992 р., № 48, ст. 650.

[49] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

[50] Брижко В.М. *Організаційно-правові питання захисту персональних даних*. Дис. … канд. юрид. наук: 12.00.07 Національна академія державної податкової служби України. – К., 2004.

[51] Виноградова Г. В. *Правове регулювання інформаційних відносин в Україні*. – К., 2006. – 176 с.

Водночас, А. Марущак, при визначенні поняття «персональні дані», оперує терміном «***конфіденційна інформація про особу***»[52]. Проте конфіденційними персональні дані можуть вважатися на підставі закону чи за бажанням особи (ч. 1 ст. 5 Закону України «Про захист персональних даних» у порівнянні з ч. 2 ст. 21 Закону України «Про інформацію»)[53]. Так, не є конфіденційною інформація, що стосуються здійснення особою, яка займає публічну посаду, посадових або службових повноважень[54]. Отже, не слід ототожнювати персональні дані з конфіденційними.

Згідно ст. 2 Закону України «Про захист персональних даних» під ***персональними даними*** розуміються "відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована"[4].

Фактично це визначення перегукується із даним у Конвенції № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», де зазначається, що це – інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною[55]. У Загальному Регламенті поняття «персональних даних» розширене (див. п. 1.1.1.), що детерміновано актуальною практикою, в тому числі рішеннями Суду ЄС. Про це буде йти мова у наступному підрозділі.

В цілому українське законодавство містить більше 3000 нормативно-правових актів, сфера регулювання яких охоплює, серед іншого, обробку інформації про фізичну особу[56]. Однак, зазвичай, вони конкретизують зміст персональних даних відповідно до виду правовідносин, що входять до сфери їхньої регламентації (цивільної, трудової, адміністративної, кримінально-процесуальної тощо). Відтак, перелік таких даних відрізняється в залежності від сфери дії акта. Законом України «Про захист персональних даних» також не

[52] Марущак А. *Інформаційне право: доступ до інформації*. – К., 2007. – 535 с.
[53] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.
[54] *Ibid.*
[55] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Міжнародний договір / Офіційний вісник України. – 2011 – № 1, № 58. – 2010. – Ст. 1994. – Ст. 85.
[56] Каретник О. С. *Поняття інформації про фізичну особу (персональні дані) в цивільному праві України* / О. С. Каретник // Часопис Київського університету права. – 2013. – № 2. – С. 229.

встановлено точної сукупності відомостей, які потребують захисту, тому такою може бути сприйнята будь-яка інформація про людину.

При порівнянні переліків персональних даних в різних законодавчих актах (нами розглядалися Закон України «Про інформацію»[57], Закон «Про Всеукраїнський перепис населення»[58], Постанова Верховної Ради України «Про затвердження положень про паспорт громадянина України та про паспорт громадянина України для виїзду за кордон»[59], Закон України «Про Державний реєстр виборців»[60]) можна помітити, що в основу їх формування покладено різні принципи, в залежності від наміру законодавця. Спільним для всіх цих актів є такий перелік персональних даних: прізвище, ім'я та по батькові; стать; національність; дата і місце народження; сімейний стан. Будемо вважати цю інформацію такою, що найчіткіше ідентифікує особу.

Втім, у зв'язку з розвитком комп'ютерних технологій, слід мати на увазі, що існує значно більше відомостей, які можна вважати персональними даними, хоч, на перший погляд, вони такими не є. Зокрема, IP-адреса, GPS-локація, поштова адреса, навіть дані про пристрій, з якого людина підключається до мережі (розміри, операційна система) тощо – по суті, чи не будь-яка інформація, що її може отримати комп'ютерна система, дасть їй змогу доволі точно ідентифікувати особу.

Надалі такі відомості можуть використовувати суб'єкти з будь-якими інтенціями. Наприклад, для здійснення різноманітних досліджень, аналізу ринку потенційних споживачів. У наступних розділах буде йти мова саме про використання даних з метою залучення нових покупців, просування бренду (товару) та його адаптування під потреби ринку. Це і є завданнями цільового маркетингу, кінцева мета якого – споживач і задоволення його потреб.

---

[57] Закон України «Про інформацію» Відомості Верховної Ради України (ВВР), 1992 р., № 48, ст. 650.
[58] Закон України «Про Всеукраїнський перепис населення» Відомості Верховної Ради України (ВВР), 2000 р., № 51-52, ст. 446.
[59] Постанова Верховної Ради України «Про затвердження положень про паспорт громадянина України та про паспорт громадянина України для виїзду за кордон» Відомості Верховної Ради України (ВВР), 1992 р., № 37, ст. 545.
[60] Закон України «Про Державний реєстр виборців» Відомості Верховної Ради України (ВВР), 2007 р., № 20, ст. 282.

2.2. Поняття цільового маркетингу

Класиком маркетингу, Філіпом Котлером, було сформульовано така дефініція: “Маркетинг – це вид людської діяльності, що спрямована на задоволення потреб шляхом обміну”[61]. Під «обміном» Ф. Котлер вбачав взаємовигідні зв’язки контрагентів: клієнт оплачує вартість, а продавець/постачальник забезпечує його товаром та сервісом у відповідній кількості та якості. Науковець пов’язує прибуток компанії із задоволенням споживача, – перше без другого неможливо. “Мета маркетингу – залучати нових клієнтів, обіцяючи вищу споживчу цінність, і зберігати старих клієнтів, постійно задовольняючи їх мінливі запити”[62].

Поняття «маркетингу» набуло закріплення і в українському законодавстві та моє ознаки комерційної діяльності, що реалізовується з метою отримання прибутку. Зокрема, пп. 14.1.108. п. 14.1 ст. 14 Податкового кодексу:

> “послуги, що забезпечують функціонування діяльності платника податків у сфері вивчання ринку, стимулювання збуту продукції (робіт, послуг), політики цін, організації та управлінні руху продукції (робіт, послуг) до споживача та після продажного обслуговування споживача в межах господарської діяльності такого платника податків. Маркетингом у розумінні ПК України називаються послуги з розміщення продукції платника податку в місцях продажу, з вивчення, дослідження та аналізу споживчого попиту, внесення продукції (робіт, послуг) до інформаційних баз продажу, послуги зі збору та розповсюдження інформації про продукцію (роботи, послуги)”[63].

Економічний енциклопедичний словник визначає ***цільовий маркетинг*** як вид маркетингу, що передбачає орієнтацію на окремий, відібраний із декількох, сегмент ринку[64].

Обираючи свій цільовий сегмент, постачальник товарів і послуг спрямовує наявні в нього ресурси на просування свого продукту серед конкретної групи осіб – цільової аудиторії (далі – ЦА). Завдяки цьому можна

---

[61] Котлер Ф. *Основы маркетинга* / Филип Котлер, Гари Армстронг, Джон Сондерс, Вероника Вонг. – 2-е европ. изд. – М., СПб., К. : Изд. дом «Вильямс», 2006. – С. 32.
[62] *Ibid.*
[63] Податковий кодекс України (Відомості Верховної Ради України (ВВР), 2011, № 13-14, № 15-16, № 17, ст.112.
[64] Економічний енциклопедичний словник : В 2 т. / За ред. С. В. Мочерного. – Львів : Світ. – Т. 1. – 2005. – 616 с.

зосередити рекламну кампанію суто на тих, хто з великою ймовірністю зацікавиться пропозицією. Отже, такий маркетинг буде значно ефективнішим.

Масові рекламні компанії спрямовані на широке коло споживачів, для чого можуть використовувати друковані видання, телемаркетинг, рекламу в Інтернеті, масові поштові розсилки. На відміну від них, цільовий маркетинг є персоналізованим. Інформування проводиться засобами адресних розсилок (пошта, E-mail, телефонний дзвінок, SMS), тому обов'язковою умовою є наявність персональної інформації про клієнта.

У нашому дослідженні ми більше звертатимемо увагу саме на маркетингову діяльність в мережі інтернет. По-перше, там існує більше можливостей для обробки даних, а, відповідно, і загроз. По-друге, з розвитком інформаційних технологій, онлайн-маркетинг набирає все більших масштабів. Саме тому оцінка такої діяльності з точки зору захисту персональних даних є дійсно необхідною.

Отже, у ході цільового маркетингу використовуються відомості, що можуть ідентифікувати особу.

Питання регламентації цільового маркетингу обговорювалося при створенні Загального Регламенту про захист даних, в часи, коли ще була чинною Директива 95/46/ЄС. Робоча група за ст. 29 (Article 29 Data Protection Working Party, скорочено – *A29WP*)[65] наголошувала на тому, що цільовий маркетинг підпадає під регулювання Директиви 95/46/ЄС, з двох причин:

- використання файлів *cookie*, зазвичай, передбачає обробку унікальних ідентифікаторів і збирання IP-адрес, що дозволяє відстежувати певні пристрої (навіть якщо використовуються динамічні IP-адреси);
- зібрана інформація стосується особистісних характеристик користувачів, і використовується для впливу на їхню поведінку[66].

[65] Робоча група по статті 29 була консультативним органом, що складається з представника органу із захисту даних кожної держави-члена ЄС, європейського спостерігача з питань захисту даних і Європейської комісії. 25 травня 2018 року його замінила Європейська рада із захисту даних (ст. 68 Загального регламенту про захист даних).

[66] Opinion 2/2010 on "online behavioural advertising" [Електронний ресурс]. – 2010. – Режим доступу: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

Тепер ці висновки набули закріплення в Загальному регламенті про захист даних у п. 30, згідно якого будь-які онлайн-ідентифікатори, отримані з пристроїв, додатків, інструментів чи протоколів користувачів, визнаються персональними даними, адже безпосередньо пов'язані з конкретною особою[67].

Основним інструментом цільового маркетингу є персоналізована реклама. Її витоки, на думку науковця А. В. Пазюка, сягають 90-их рр. XX ст. Так, у 1996 році компанія Yahoo опрацьовувала профілі 175 млн. людей, вибравши їх зі списків прямої розсилки. Після отримання претензій від користувачів, Yahoo вирішила знищити дані з адресами 85-ти млн. осіб, що відмовилися надати згоду на включення їх до списків розсилки[68]. А вже наступного року компанія American Online (AOL) запропонувала бізнес-партнерам передати їм телефонні номери своїх абонентів у маркетингових цілях. Позаяк останні вважали це суттєвим порушенням умов угоди про надання послуг, компанія була змушена відмовитися від своїх планів[69].

То що це таке, персоналізована реклама, і яким чином вона використовується у цільовому маркетингу?

Персоналізована реклама – це реклама, зорієнтована на певну групу осіб, об'єднаних спільними ознаками, що мають єдину мету та завдання. Така спільнота людей складає ЦА рекламодавця. Вона визначається за допомогою ***таргетингу*** (англ. *target* – ціль), тобто сукупності механізмів, що дають можливість виокремити за відповідними критеріями з наявної аудиторії лише певну частину, і показати рекламне повідомлення саме їй[70].

Така технологія допомагає знизити витрати рекламодавця на залучення споживачів до виробленого ним продукту. У разі використання таргетингу,

---

[67] Загальний регламент про захист даних (ЄС) 2016/679 від 27 квітня 2016 року [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16.

[68] Пазюк А.В. *Захист права на приватність користувачів Інтернет* [Електронний ресурс]. – Режим доступу: https://docs.google.com/document/d/1uGCRGY3zI_HuxbrOGcylR9pFNU7UA_ZV9YtWNTbW6EI/edit?hl=ru.

[69] Berman J., Mulligan D. *Privacy in the Digital Age: Work in Progress*// Nova Law Review. – 1999. – Vol. 23. – No 2.

[70] Ward S. *Small Business: Canada Expert Target Marketing* [Електронний ресурс]. – Режим доступу : http://sbinfocanada.about.com/od/ marketing/g/targetmarketing.htm.

рекламні матеріали показуються лише тому, хто відповідає заздалегідь встановленим характеристикам[71].

Мабуть, першим проявом таргетингу було розміщення на дверях церкви реклами про продаж молитовників. ЦА – прихожани[72]. Більш сучасний приклад – реклама засобів проти акне, яку показують, переважно, дівчатам від 16-ти до 25-ти років, що зазвичай мають проблемну шкіру під час пубертатного періоду.

Розміщують таргетовану рекламу навіть на інтернет-сторінках без комерційного контенту (англ. *content* – зміст), щоб постійно підтримувати інтереси споживача, формувати попит, реалізовувати маркетингові кампанії, орієнтовані на довготривалий ефект, маючи при цьому відому і вивчену ЦА, відповідаючи її соціальним очікуванням, стилю життя та рівню доходу[73].

Залежно від критеріїв формування цільової аудиторії таргетинг поділяється на різні види.

1) Географічний (геотаргетинг), що спрямований на відвідувачів сайту залежно від території (країна, місто, район у місті, село), на яку націлена рекламна кампанія[74]. Місцезнаходження користувача може визначатися за IP-адресою та/або за даними геолокації (GPS). Підвидом є локальний таргетинг, зосереджений на пошуку закладів поблизу місцязнаходження користувача[75].

2) Часовий (темпоральний) таргетинг – налаштування демонстрації реклами в момент, коли типовий представник ЦА перебуває онлайн. Можна також обмежити частоту показів реклами[76].

3) Мовний таргетинг обмежує показ реклами на сайтах з користувачами, які володіють певною мовою. Наприклад, на англомовних[77].

---

[71] Карась О. *Таргетинг – один із видів стратегічної реклами* / Олена Карась // Журнал європейської економіки. – 2014. – Т. 13, № 3. – С. 326.

[72] Ищенко О. А. *Вопросы правового регулирования рекламы в Российской Федерации* / Ищенко О. А., Пермяков О. В. // Реклама и право. – 2004. – № 1. – С. 16.

[73] Богданов Б. *Воздушные шарики в рекламе* [Електронний ресурс]. – Режим доступу: http://telnews.ru/column/13061/http://medialaw.org.ua/analytics/povnyj-dostup-shho-zminyuye-zakonoproekt-0947.

[74] Карась О. *Таргетинг – один із видів стратегічної реклами*, С. 330.

[75] Воєводін Б. В. *Цивільно-правові аспекти таргетованої (цільової) реклами, персоналізації та приватності у рекламі* / Б. В. Воєводін // Європейські перспективи. – 2013. – № 11. – С. 118.

[76] Карась О. *Таргетинг – один із видів стратегічної реклами*, С. 331.

[77] Карась О. *Таргетинг – один із видів стратегічної реклами*, С. 331.

4) Соціально-демографічний – спрямований на показ реклами для певної категорії споживачів залежно від віку, статі, сімейного положення, купівельної спроможності (матеріального стану), посади, освіти, соціального статусу[38]. Наприклад, для рекламодавця ЦА можуть бути студенти ВНЗ, що цікавляться юридичною літературою, або домогосподарки від 25 до 35 років, заміжні, з дітьми, що користуються недорогою косметикою.

5) Психологічний таргетинг – враховує психологічні особливості споживачів реклами (психотип, соціотип)[78].

6) Тематичний таргетингом – показ реклами на сайтах з певним контентом. Результатом застосування цієї технології є контекстна реклама. Система *Google AdSense* автоматично розміщує рекламні оголошення на сайтах з відповідною тематикою[38]. Прикладом може слугувати блог про рибальство, на якому розміщується реклама інтернет-магазину вудочок та рибальських човнів.

7) Таргетинг за сайтами дозволяє чи забороняє показувати рекламу на сайтах певної тематики[39]. До прикладу, рекламу ресторану, що спеціалізується на м'ясних стравах, недоцільно показувати на сайтах про вегетаріанську їжу.

8) Таргетинг за провайдерами дозволяє обирати провайдерів Інтернет-послуг, на користувачів яких націлена реклама. Для цього виду таргетингу використовуються IP-адреси єдиного провайдера[79].

9) За типами браузерів і операційних систем – вид таргетингу, завдяки якому рекламу побачать лише відвідувачі з певним типом браузера і операційної системи[80].

10) Таргетинг за видами організацій, дозволяє показувати рекламу тільки конкретним із них (банкам, підприємствам, університетам тощо)[81].

11) Поведінковий таргетинг виділяє ЦА на основі інтересів, уподобань і смаків користувачів. Ці дані відстежуються за допомогою *cookie*-файлів, а в

---

[78] Чистов К. *«Оценка по поведению» Технологии таргетинга сегодня и завтра* // Інтернет-Форум. – 2007. – 21 бер. – С. 43–55.
[79] Карась О. *Таргетинг – один із видів стратегічної реклами*, С. 331.
[80] *Ibid.*
[81] Ализар А. *Поведенческий таргетинг: назад в будуще. Вебпланета* [Електронний ресурс]. – Режим доступу: webplanet.ru/news/advert/2007/ 8/30/behaviorism.html.

режимі реального часу можна прослідкувати за покупками, які здійснює власник дисконтної картки. Створюється профіль клієнта з його вподобаннями, інтересами, даними про фінансове становище тощо. Цей напрямок таргетингу вважається найперспективнішим[82].

12) Одним із підвидів поведінкового таргетингу можна назвати таргетинг за інтересами. Таким чином відстежуються найбільш відвідувані даним користувачем веб-сайти і наступного разу йому пропонується реклама, що містить у собі інформацію з попереднього пошуку[83]. Прикладом може слугувати випадок, коли користувач шукав інформацію про якусь музичну рок-групу. Потім він хотів знайти фестиваль, який проходитиме найближчим часу. Цього разу на екрані висвітлюватиметься реклама про концерт за участі тієї ж групи чи, наприклад, рок-концерт.

13) Наступний підвид – ремаркетинг. У такому випадку, реклама направляється користувачам, які при відвідуванні сайту рекламодавця не здійснили покупки запропонованого продукту, і наступного разу завітали на сайт із схожими товарами[84]. Наприклад, клієнт (-ка) переглянув одноденні чутливі контактні лінзи, але так і не купив їх. Тому при відвідуванні сайтів, що входять до однієї рекламо-обмінної групи йому/їй показуватимуть рекламу із цими лінзами.

14) Ще одним підвидом є геоповедінковий таргетинг, що, при показі реклами, орієнтується на інтереси та звички користувача відповідно до даних про його місце знаходження та траєкторію переміщення, улюбленіі місця та заклади, які він найчастіше відвідує. Це враховується при націлюванні рекламних матеріалів[85]. Наприклад, якщо особа часто заходить на сайти інтернет-магазинів, то їй буде цікаво дізнатися про акційні пропозиції, які пропонують ці маркети.

---

[82] Карась О. *Таргетинг – один із видів стратегічної реклами*, С. 330.
[83] Бородкин А. *Поведенческий таргетинг: изображая жертву* [Електронний ресурс]. – Режим доступу: http://itua.info/analytics/10100.html.
[84] *Ibid.*
[85] *Ibid.*

Дослідження Гарвардського бізнес-огляду (*Harvard Business Review*) 2016 року висвітлило 3 переваги таргетингу для маркетологів:

- він може вплинути на зміну світобачення споживача; він починає відкривати себе з іншого ракурсу, і в нього виникає відчуття, що продукт в оголошенні – саме те, чого йому бракувало;
- завдяки таргетингу можна проаналізувати недоліки маркетингової кампанії конкурентів і припасувати свою пропозицію до виявлених потреб споживача з особливостями, які відрізняють цю компанію від інших;
- позитивний ефект від таргетингу має місце лише тоді, коли споживачі знають, що отримують персоналізовану рекламу, тому ключове значення має прозорість (транспарентність)[86].

Із зазначеного стає зрозуміло, в чому проблема цільового маркетингу. Сама стратегія будується, а реклама, відповідно, показується, залежно від поведінкових характеристик користувача. Це і є його персональні дані, що збираються при використанні таргетингу. Для його здійснення та формування профілю користувача застосовуються *cookie*-файли.

Cookie[87] – це невеликі текстові файли, які зберігаються в браузері під час відвідування певних веб-сторінок[88]. Браузер зберігає цю інформацію і передає на сайт, коли користувач робить наступний запит. Деякі файли *cookies* можуть зберігатися тільки протягом однієї сесії (одноразового сеансу зв'язку із сайтом), вони видаляються після закриття браузера. Інші, встановлені на деякий період часу, записуються в спеціальний файл і зберігаються на комп'ютері. Зазвичай, такий файл називається «*cookies.txt*» і знаходиться в робочій директорії браузера[89]. Так звані «реп'яшки», можуть зберігатися на комп'ютерах та в браузерах користувачів тимчасово (впродовж одного сеансу) чи постійно,

[86] Walker Reczek R., Summers C., Smith R. Targeted Ads Don't Just Make You More Likely to Buy — They Can Change How You Think About Yourself [Електронний ресурс]. – Режим доступу: https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself.

[87] В українському перекладі Загального регламенту про захист персональних даних вживається термін «реп'яшки» (п. 30). «*Cookies*» усе ж таки є універсальним поняттям, тому тут послуговуватимемося ним. Водночас, хотілося б відзначити вдале намагання перекладачів адаптувати англійський термін українською.

[88] Інформація про файли cookie [Електронний ресурс]. – Режим доступу: http://www.canon.ua/cookie-information.

[89] Безпека і анонімність в Інтернеті [Електронний ресурс]. – Режим доступу: http://estdomain.com.ua/bezpeka-i-anonimnist-v-interneti/

надходити із сайту, який переглядає користувач, або з реклами на інших сайтах[90].

Файли *cookie* можуть підвищити продуктивність роботи із сайтом, зокрема, коли не потрібно кожного разу проходити наново процедуру логінування. Так, при необхідності авторизованого доступу під час входу на певний веб-сайт в *cookies* протягом сесії зберігається «код сеансу» користувача, в якому зашифрований його обліковий запис (ім'я та пароль). Це дозволяє не вводити одні й ті ж дані при запитах кожного документа, що вимагає авторизації. Якщо ж поставити галочку в полі «Запам'ятати мене», то *cookie* сайту буде зберігатися на комп'ютері, поки особа не скасує підключення до цього сервера під своїми реєстраційними параметрами[91].

Наприклад, на сайті Укрзалізниці при бронюванні чи купівлі квитків у покупця є можливість зберегти свої дані, щоб надалі вони одразу ж автоматично з'являлися у полях, які потрібно заповнити. Як і у випадку сеансових *cookies*, на комп'ютері буде зберігатися не обліковий запис (ім'я та пароль), а тільки «код постійного підключення». Проте інколи *cookie*, особливо, ті, що зберігаються завдяки банерній рекламі, можуть становити загрозу для конфіденційності, відслідковуючи відвідані сайти[92]. Більше про це – в наступному підрозділі.

Таким чином, основним призначенням файлів *cookie* є автентифікація користувача, визначення його інтересів та збереження персональних даних, що загрожує таємниці особистого життя передбаченої перш за все ст. 32 Конституції України та іншими законодавчими актами. Використання *cookies* в рекламних кампаніях дозволяє відслідковувати, які сайти окремої банерообмінної мережі відвідує користувач, що дозволяє коригувати модель

---

[90] Видалення файлів cookie та керування ними. [Електронний ресурс]. – Режим доступу: https://support.microsoft.com/uk-ua/help/17442/windows-internet-explorer-delete-manage-cookies

[91] Степаненко О. О. *Програмування Інтернет-застосувань* [Електронний ресурс]. – Режим доступу: http://eir.zntu.edu.ua/bitstream/123456789/2873/1/Stepanenko_Methodical_instructions.pdf.

[92] Алікберов А. *Що таке cookies і як з ними працювати* [Електронний ресурс]. – Режим доступу: http://citforum.ru/internet/html/cookie.shtml.

подачі реклами для конкретного споживача. Збір, обробка та збереження вказаної інформації має своїм наслідком створення профілю користувача[93].

Одним із видів *cookies* є трекінгові. Вони записують на комп'ютері здійснені операції та можуть передавати цю інформацію третім особам[94], що ставить під загрозу безпеку персональних даних користувача.

З метою персоналізації та створення профілю користувача, рекламодавець може зберігати дані логінування (***log file***). Це дані користувача Інтернету, які автоматично надсилаються на сервер, на який здійснюється вхід: IP-адреса, час вашого запиту та його результат, URL-адреса, інколи – навіть ім'я власника домену або його E-mail-адресу[95]. Тоді вже можна адаптувати рекламу до локації, в якій зафіксована IP-адреса. Наприклад: подорожуючи до Берліна, Ви будете отримувати рекламу про події або ресторани, що розміщені поблизу.

Суд ЄС у рішенні ***Scarlet v Sabam*** констатував, що IP-адреси класифікуються як особисті дані, оскільки вони дозволяють користувачам бути безпосередньо ідентифікованими[96]. Робоча група за ст. 29 кілька разів чітко зазначила, що IP-адреси являють собою особисті дані відповідно до положень цієї Директиви, оскільки їх можна простежити за допомогою фізичної особи, яка співпрацює з провайдером Інтернету[97].

З іншого боку, існують динамічні IP-адреси, які, здавалося б, не пов'язані з користувачем. Наприклад, коли за одним ПК сидять кілька людей. Усі сумніві стосовно цього розвіяв знову Суд ЄС. Вердиктом у справі ***Patrick Breyer v Bundesrepublik Deutschland*** він постановив, що навіть такі дані достатньо ідентифікують особу, тому їх слід вважати персональними[98]. Федеральний верховний суд Німеччини прослідував цьому висновку в своєму рішенні від 16.05.2017 р. № VI ZR 135/13. Позивач скаржився на те, що після

[93] Воєводін Б. В. *Цивільно-правові аспекти таргетованої (цільової) реклами, персоналізації та приватності у рекламі*, С. 117.
[94] Sandfuchs B. *Privatheit wider Willen*, p. 15.
[95] Scholz, P. *Datenschutz beim Interneteinkauf.* Nomos Verlagsgesellschaft, Baden Baden 2003, 464 p.
[96] Scarlet v Sabam Case (заява № C-70/10 від 24.11.2011).
[97] WP 01245/07/EN, WP 136 Opinion 4/2007 on the concept of personal data https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
[98] Patrick Breyer v Bundesrepublik Deutschland (справа № C-582/14, рішення від 19.10.2016).

завершення сеансу на великій кількості німецьких інтернет-порталів, з метою запобігання атакам та полегшення переслідування злочинців, зберігається назва завантаженої сторінки, час пошуку та IP-адреса комп'ютера[99].

На думку Суду, динамічна IP-адреса, яка зберігається постачальником медіа-послуг онлайн, коли особа отримує доступ до публічного веб-сайту цього постачальника, є для постачальника (захищеними) персональними даними[100].

Далі Суд зауважує, що законом можуть бути передбачені винятки, коли ці дані можна використовувати. Зокрема, якщо це необхідно для підключення та оплати за використання засобів телекомунікації (ч. 1 ст. 15 Закону про засоби телекомунікації Німеччини)[101]. Тобто, як і в рішенні Суду ЄС, так і в німецькому правопорядку, винятком для збереження і використання персональних даних без згоди особи є необхідність забезпечення функціонування системи телекомунікацій. Втім, все одно потрібно забезпечити пропорційність з інтересами, правами і свободами користувача[102]. Федеральний Верховний суд так і не вирішив питання щодо необхідності зберігання цих даних після виходу з порталу, тому що це поза межами його компетенції. Тепер справа знаходиться на повторному розгляді в суді І інстанції, який і має прийняти рішення з цього питання[103].

2.3. Правові ризики використання цільового маркетингу

З метою планування і реалізації маркетингової стратегії, необхідно розробити SWOT-аналіз. Він допомагає зрозуміти сильні та слабкі сторони компанії на ринку, визначити можливості та спрогнозувати ризики.

---

[99] Bundesgerichtshof zur Zulässigkeit der Speicherung von dynamischen IP-Adressen http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2017&Sort=3&nr=78289&pos=4&anz=78.

[100] *Ibid.*, Переклад – наш.

[101] Telemediengesetz [Електронний ресурс]. – Режим доступу: https://dejure.org/gesetze/TMG/15.html..

[102] Bundesgerichtshof zur Zulässigkeit der Speicherung von dynamischen IP-Adressen.

[103] Bleich H. *BGH bestätigt: Dynamische IP-Adressen sind personenbezogene Daten* [Електронний ресурс]. – Режим доступу: https://www.heise.de/newsticker/meldung/BGH-bestaetigt-Dynamische-IP-Adressen-sind-personenbezogene-Daten-3714967.html.

Небезпеки для бізнесу можуть бути різноплановими. У цілях нашого дослідження, ми розглянемо правові ризики використання цільового маркетингу, а саме – ризики, які стосуються захисту персональних даних.

Німецькі науковці розрізняють 3 види загроз: небезпеку, ризик та незначний залишковий ризик[104]. Віднесення до того чи іншого виду залежить від 2 факторів. По-перше, чи дані, що обробляються, стосуються конкретної особи. Якщо так, то констатуємо найнижчий рівень – незначний залишковий ризик. По-друге, вирішуємо питання цілі обробки даних. Якщо метою є зробити певні висновки щодо поведінки суб'єкта чи його/її особистих характеристик, тоді існує небезпека втручання в приватне життя; в іншому випадку, – наявний звичайний ризик[105].

Сам по собі цільовий маркетинг не є небезпечним з точки зору захисту персональних даних. Загроза криється в технологіях, що використовуються для його здійснення. Адже не завжди споживачі знають про те, що компанії обробляють їхні дані. Саме тому нагальним питанням є вирішення цієї проблеми на законодавчому рівні.

Проте нові правила Загального регламенту про захист даних також не охоплюють всіх питань. При відмові користувача від збереження файлів *cookie*, нерідко стає неможливим наступне використання сайту. Фактично, такий стан речей повинен змінитися з набранням чинності Регламентом про конфіденційність та електронні повідомлення. Тільки тоді адміністратори веб-сайту зможуть збирати файли *cookie* лише за попередньої згоди користувача. Тим не менше, він зможе користуватись всіма функціями сайту без цієї згоди. Тобто, *opt-out* має бути змінений на *opt-in*[106], коли передача персональних даних рекламодавцю може здійснюватися лише за погодженням відвідувача сайту[107]. Таким чином в ЄС намагаються боротися з так званими «стінами

[104] Тобто такий, що продовжує існувати, не дивлячись на всі вжиті заходи (прим. – наше).
[105] Schwichtenberg S. *Datenschutz in drei Stufen*, p. 56.
[106] При використанні механізму *opt-out* дані користувачів збираються, поки вони явно проти цього не заперечать. У методі *opt-in* – навпаки, для обробки даних треба спочатку отримати згоду суб'єкта.
[107] *Die ePrivacy-Verordnung ist auf dem Weg! Womit müssen Sie rechnen? Digital Guide* [Електронний ресурс]. – Режим доступу: https://hosting.1und1.de/digitalguide/websites/online-recht/eprivacy-verordnung/.

відстеження» (*tracking wall*), коли для нормальної роботи сайту користувач повинен погодити обробку *cookie* та відключити блокування реклами.

Принципи цільового маркетингу притаманні й технології *Social media marketing* (SMM) – рекламування та просування бренду чи окремого товару за допомогою соціальних мереж. При цьому самі соціальні мережі (такі як *Facebook, Instagram, Twitter* тощо) виступають розповсюджувачами реклами. Технологія SMM базується на основі:

- відомостей, внесених користувачами до свого профілю;
- статистики відвідуваності сторінок інших користувачів;
- даних, що збирається на основі аналізу дій користувача в соціальній мережі, його уподобаннях та інтересах;
- інформації, що збираються поза соціальною мережею (досліджується інформація з сайтів, які об'єднані однією банерообмінною мережею на основі використання *cookies*).

Небезпека використання SMM полягає у надмірній кількості інформації про споживача, якою рекламодавець володіє. Це тягне за собою не лише можливі зловживання стосовно змісту реклами, а й неприпустимі порушення таємниці особистого життя особи[108].

Cookies таять у собі ще більшу небезпеку. За допомогою персональних даних можна не тільки успішно продати вироблену продукцію, а й впливати на свободу вираження поглядів. Величезний скандал був, коли *Cambridge Analtica* використовувала дані користувачів *Facebook*, щоб переконати виборців голосувати за Дональда Трампа під час виборчої кампанії в США[109].

Але це не єдиний випадок, коли *Facebook* звинуватили в зловживанні захистом даних. Австрійський юрист Макс Шремс звернувся до суду, оскільки Комісар із захисту даних Ірландії відмовився роглядати його скарги про незаконність передачі даних *Facebook Ireland Limited* до американської

[108] Воєводін Б. В. *Цивільно-правові аспекти таргетованої (цільової) реклами, персоналізації та приватності у рекламі*, С. 118.
[109] Grassegger H., Krogerus M., The Data That Turned the World Upside Down [Електронний ресурс]. – Режим доступу: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win (28.01.2017).

материнської компанії *Facebook Inc*., адже обробка даних в Сполучених Штатах не відповідає європейським стандартам. Зокрема, виявлено можливість *NSA*[110] отримати доступ до баз даних *Facebook Inc.* Ця справа, відома під назвою «Європа проти Facebook» (***Europa vs. Facebook***), наразі перебуває на розгляді у Верховному суді Австрії[111]. Але прагнення справедливості Макса не дрімає – одразу після набрання чинності Загальним регламентом про захист даних, він подав позов до суду проти *Facebook* та *Google* через примушування ними користувачів акцептувати нову політики конфіденційності[112].

Проте не тільки в інтернет-мережі знаходимо випадки використання цільового маркетингу. Так, у рамках експерименту компанією *Amscreen* у білборди було вмонтовано відеокамери з функцією розпізнавання облич, щоб компанії могли спостерігати за тим, які саме люди, в який час і в якому місці звертають увагу на їхнє повідомлення. Завдяки цій технології невдовзі рекламодавці зможуть у режимі реального часу змінювати ту чи іншу рекламу відповідно до віку чи статі реципієнта[113].

Наведемо ще один, вражаючий приклад. Воєнні бази є об'єктом, що повинен бути під особливою охороною. Тим більше, якщо це військові частини армії США. Тим більше, якщо вони знаходяться в Африці та на Близькому Сході. Не знаючи те, що ховається за оприлюдненням результатів дослідження, *Strava* опублікувала теплову карту, на якій було 13 трлн. точок GPS. Таким чином компанія хотіла проаналізувати попит на свої трекінгові годинники та показати світові, на скільки вони популярні[114]. Натомість, їм вдалося зробити те, що було не під силу східним контррозвідкам. В районах, де, як відомо, годинники не купували, виднілися точки правильної форми. Отже, там був рух. "Виглядає дуже привабливо, але не вражаюче – для Служби безпеки. Бази

[110] NSA (National Security Agency), укр. - Агентство національної безпеки – агентство криптологічної розвідки США.

[111] Schrems, Complaint against Facebook Ireland Ltd – 23 "PRISM" [Електронний ресурс]. – Режим доступу: http://www.europe-v-facebook.org/prism/facebook.pdf.

[112] Hern A. *Facebook and Google targeted as first GDPR complaints filed* [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/technology/2018/may/25/facebook-google-gdpr-complaints-eu-consumer-rights.

[113] Хадсон А. *Адресные рекламы знают о вас больше, чем вы думаете* [Електронний ресурс]. – Режим доступу : http://www.bbc.com/ukrainian/mobile/ukraine_in_russian/2013/08/130801_ru_s_targeted_adverts.shtml

[114] Drew Robb, *Building the Global Heatmap* [Електронний ресурс]. – Режим доступу: https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de.

США чітко ідентифіковані і відображені на карті"[115], – написав у своєму *Twitter* австралійский військовий аналітик Натан Русер з організації *IUC Analysts*[116].

Набув розголосу й інший випадок неналежної обробки даних провайдером мережі Wi-Fi. Звичайні люди проходили повз кафе, а потім у стрічці новин *Facebook* вони отримували рекламу закладу, до мережі Wi-Fi якого автоматично підключався їх мобільний пристрій. Надалі цей провайдер міг відслідковувати шлях пересування власників зафіксованих у мережі мобільних пристроїв[117].

Така реклама, з одного боку, допомагає відфільтрувати інформацію, яка становить інтерес для певної людини, є корисною для неї, а з іншого боку, стає втручанням в її особисте життя.

Наприклад, Ви купили подорож в певного туроператора. Тепер у нього є Ваші контактні дані, і він надсилає Вам повідомлення про наявні акції. Оскільки Ви любите подорожувати, то ця інформація для Вас корисна. Якби ж, наприклад, такої змоги відправитися в поїздку у Вас не було, повідомлення, що приходить, стали причиною Вашого задуманого і спохмурнілого обличчя. Ще гірша історія у тих, хто ніяк не може скинути зайву вагу (наприклад, внаслідок хвороби), але отримує рекламу із зображеннями стрункіх дівчат/мускулистих хлопців, бо раніше постійно цікавився (-лася) здоровим способом життя. Чи в ситуації, коли батьки проти вакцинації свого чада; вони не побачать в інтернеті статті про користь вакцини, якщо перед цим постійно шукали в *Google* її недоліки. Система просто видаватиме те, що на підставі попередніх запитів вважатиме найбільш релевантним, не враховуючи етичні питання.

---

[115] Nathan Ruser [Електронний ресурс]. – Режим доступу: https://twitter.com/Nrg8000/status/957318498102865920?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E957318498102865920&ref_url=https%3A%2F%2Frussian.rt.com%2Fworld%2Farticle%2F475068-fitnes-treker-voennye-bazy-ssha.
Текст першоджерела: "It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable".

[116] Крутов М. *Бігун – знахідка для шпигуна: популярний фітнес-застосунок «здав» приховані позиції військових* [Електронний ресурс]. – Режим доступу: https://www.radiosvoboda.org/a/29007716.html.

[117] *Прошли мимо кафе, а вам тут же показали его рекламу? Это не паранойя В Москве работает бесплатный вайфай. Его оператор собирает очень много данных пользователей* [Електронний ресурс]. – Режим доступу: https://meduza.io/feature/2018/10/24/proshli-mimo-kafe-a-vam-tut-zhe-pokazali-ego-reklamu-eto-ne-paranoyya?fbclid=IwAR2nvenZg2E8eF-Xg36YvSwB88Wp1h5IXt22S27v6wep-RbnQOCljk_FMUc.

Науковці називають це «бульбашкою фільтрів» (англ. *filter bubble*)[118], або «ехо-камерами» (нім. *Echokammer*)[119]. Користувач постійно стикається з рекламними повідомленнями на одну тематику, з урахуванням його особистих інтересів. Однак, це ускладнює створення нових захоплень, оскільки оферти, які раніше не відповідали очікуванням одержувача реклами, рідше або зовсім не з'являються в пошуковій видачі. Як результат, одержувач реклами обмежений у своїй свободі розвитку, не усвідомлюючи цього[120].

Звуження кола інтересів та наслідки цього не є специфічною особливістю цільового маркетингу. Цей ефект також виникає, наприклад, якщо користувач соціальних мереж неодноразово демонструє повідомлення, які, насправді чи не зовсім, відповідають його думці[121]. Збільшення ролі таких фільтрів ставить перед суспільством нові виклики, які в майбутньому також повинні будуть опинитися в правовому полі. Проте це буде менш проблемно з точки зору захисту персональних даних, ніж нова сфера приватності, яка може збігатися із захистом персональних даних, як таким[122].

Прослідковується використання персональних даних при застосуванні технології таргетингу, що провокує ризик надмірного втручання в приватне життя особи. Так, на інтернет-сторінці компанії *Google* можна знайти інформацію про оголошення, які з'являються під час користування браузером. Вони відображаються в залежності від наступних факторів:

- місцезнаходження;
- часу доби;
- нещодавніх та попередніх пошукових запитів, пов'язані з поточним;
- історії веб-пошуку і налаштування параметрів оголошень;

[118] Pariser E. *Filter Bubble: : How the New Personalized Web is Changing what We Read and how We Think*. Penguin Books 2012, 294 p.
[119] Sandfuchs B. *Privatheit wider Willen*, p. 28.
[120] *Ibid.*
[121] Hermstrüwer Y. *Informationelle Selbstgefährdung*, Tübingen 2016, 4p. 119.
[122] Bull H. I*nformationelle Selbstbestimmung*, p. 37.

- відвідування веб-сторінок, що належать компаніям, які здійснюють рекламну діяльність через служби *Google*;
- інформації в обліковому записі користувача, яка не містить персональної інформації про особу, наприклад вік чи стать;
- попередньої взаємодії з оголошеннями, рекламними службами або результатами пошуку[123].

Що ж до оголошень у службі *Gmail*, то вони формуються і завдяки вмісту поштової скриньки. Наприклад, якщо користувач за останній час отримав чимало повідомлень про фотографування та фотокамери, то у службі *Gmail* він може побачити оголошення з пропозицією від місцевого магазину фототехніки[124]. Тут же зазначається, що добір оголошень у службі *Gmail* повністю автоматизований та ніхто не читає листи користувачів. Та в будь-якому разі це все одно є порушенням загальних принципів приватності та особистих немайнових прав людини. І хоча поштовий ресурс заперечує можливість прочитання кореспонденції, то у *Messenger* це – цілком реально. Непоодинокими є випадки, коли користувачі отримують рекламу саме про те, про що не давно відбувалася переписка: чи то автобусний тур Європою, чи купівля укулеле[125].

Отже, можна виділити ***дві основні проблеми***, пов'язані з безпекою персональних даних фізичної особи. По-перше, ***компанії без відома і згоди (чи без належно наданої згоди) користувачів зберігають їх персональні дані на своїх серверах***. Утім, збирання та передачу *cookies* можна контролювати і блокувати у сучасних версіях веб-переглядачів. З'явилися застосунки, що уможливлюють контроль над використанням *cookies (Cookie Managers)*[126]. Зокрема, ліцензійна антивірусна програма *Avast* надає можливість розпізнавати шкідливі *cookie*-файли та видаляти їх.

---

[123] Про оголошення Google [Електронний ресурс]. – Режим доступу: https://support.google.com/ads/answer/1634057?hl=uk

[124] *Ibid*.

[125] Чотириструнний щипковий музичний інструмент; на вигляд нагадує гітару, але значно менший за розмірами.

[126] Алікберов А. *Що таке cookies і як з ними працювати* [Електронний ресурс]. – Режим доступу: http://citforum.ru/internet/html/cookie.shtml.

Наступна проблема полягає в тому, що ***на хостах комп'ютерних мереж[127] акумулюються величезні масиви персональних даних, що можуть бути використані з комерційною метою***, тому підвищуються вимоги щодо захисту від несанкціонованого доступу до такої інформації. Користувачі повинні бути впевнені, що їх імена, адреси електронної пошти, телефонні номери тощо, не будуть доступними для третіх осіб. І тут уже важливе значення має законодавче нормування діяльності комерційних серверів у сфері використання механізму *cookie*, детальніше про це можна прочитати в наступних розділах. Як і про те, як нам самим захистити себе від несанкціонованого використання персональних даних.

[127] Пристрій, що зв'язаний з іншими пристроями однієї мережі.

ВИСНОВКИ ДО РОЗДІЛУ І

Отже, законодавство про захист персональних даних регламентує правовідносини, що пов’язані з обробкою інформації про фізичну особу, яка ідентифікована чи може бути конкретно ідентифікована. Цією інформацією може бути будь-яка, навіть дані про IP-адресу, GPS-локацію і т.д. Так само, і обробкою визнаються будь-які операції з персональними даними (збирання, зберігання, зміна, видалення, знеособлення і т.п.).

Утім, предметом захисту є не дані як такі, а сфера приватного життя фізичної особи. У зв’язку з цим, нормативно-правовими актами у сфері захисту персональних даних є загальні – такі, що гарантують право особи на повагу до приватного життя (приватність):

- універсальні: Загальна декларація прав людини, Міжнародний Пакт про громадянські та політичні права, Конвенція про права дитини;
- локальні: Американська конвенція з прав людини, Конвенція про захист прав людини і основоположних свобод, Хартія основних прав Європейського Союзу;
- та спеціальні, що безпосередньо регламентують діяльність з обробки персональних даних, зокрема: «Базові принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних» (ОЕСР), «Керівні принципи регулювання комп’ютерних файлів, які містять персональні дані» (Генасамблея ООН), Конвенції Ради Європи № 108 «Про захист осіб у зв’язку з автоматизованою обробкою персональних даних», з Протоколом, Загальний регламент про захист даних, Директива про секретність та електронні комунікації 2002/58/ЄС.

Захист персональних даних згідно українського законодавства регламентується Конституцією України (див., роз’яснення КСУ у справах за зверненням Жашківської районної ради та Г. Устименка), Цивільним кодексом, законами «Про захист персональних даних» (був прийнятий на виконання Конвенції № 108), «Про захист інформації в інформаційно-телекомунікаційних

системах» та іншими документами у сфері захисту персональних даних, а також – міжнародними договорами, ратифікованими Україною.

Цільовий маркетинг – це вид людської діяльності, що передбачає орієнтацію виробництва продукції, надання послуг на окремий, відібраний із декількох, сегмент ринку.

Для того, щоб визначити цей сегмент, який є цільовою аудиторією, маркетингова компанія застосовує різноманітні механізми, зокрема, таргетинг. Таким чином, опрацьовуються текстові файли *cookies* та дані логінування, що містять персональні дані користувачів, такі, як логін, пароль, IP-адреса, URL-адреса, дані поведінкового профілю (уподобання, покупки тощо).

Обробка цих текстових файлів створює різного роду небезпеки для захисту персональних даних, приклади яких ми наводили у підрозділі 1.3.

Ми виділили два основних види ризиків: по-перше, віддалені сервери без належної згоди користувачів можуть зберігати інформацію про них; по-друге, персональні дані акумулюються у великих обсягах, тому існує небезпека злому і втрати величезної кількості даних, передачі їх третім особам без належних на те підстав тощо.

РОЗДІЛ ІІ
РЕГЛАМЕНТАЦІЯ ПРАВ СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЇ ЦІЛЬОВОГО МАРКЕТИНГУ

Перед тим, як конкретно перейти до прав суб'єктів персональних даних, розглянемо принципи, на основі яких може здійснюватися обробка персональних даних:

- ***законність*** – обробка здійснюється на основі законодавства, що відповідає критеріям передбачуваності. У справі «С. і Марпер проти Сполученого Королівства» ЄСПЛ сформулював 2 критерії законності. По-перше, обробка має здійснюватися за однією з підстав, закріплених у законодавстві. По-друге, сам закон повинен відповідати критеріям передбачуваності – положення закону повинні бути достатньо чіткими, щоб громадянин міг – в разі необхідності, з належною допомогою – погоджувати з ним свою поведінку[128];

- ***визначеність мети*** – обов'язковою є наявність чітких та легітимних цілей: дані не можуть використовуватися у спосіб, що суперечить цим цілям[129]. Мета обробки має визначатися законом, або установчими, локальними актами суб'єкта господарювання, прийнятими відповідно до законодавства про захист персональних даних[130]. Якщо персональні дані збираються з однією метою, вони не можуть використовуватися з іншою. Наприклад, замовляючи таксі, ми не сподіваємося, що потім будемо отримувати рекламні повідомлення про акції від їхньої мережі. Тому володілець даних повинен повідомити особу про зміну мети обробки даних і отримати нову згоду від суб'єкта;

---

[128] «S. and Marper v. The United Kingdom» (заяви № 30562/04 і 30566/04, рішення від 04/12/2008), див. для порівняння «Avilkina and Others v. Russia» (заява № 1585/09, рішення від 06/06/2013);
Стосовно передбачуваності закону, див. «Rotaru v. Romania» (заява № 28341/95, рішення від 04/05/2000)

[129] Про захист персональних даних (Текст резюме від 01.06.2010). Електронний ресурс http://zakon.rada.gov.ua/laws/anot/2297-17

[130] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

- ***точність та достовірність*** – повинна бути можливість актуалізації даних. Так, суб'єкт вправі звертатися до володільця даних з вимогою виправити неточності, а володілець, у свою чергу, зобов'язаний вживати розумні заходи, щоб підтримувати персональні дані суб'єкта в актуальному стані[131];

- ***адекватність, відповідність, ненадмірність*** – означає мінімізацію даних, що підлягають обробці. Обсяг зібраних і збережених відомостей повинен бути пропорційним меті обробки[132]. Наприклад, заповнюючи реєстраційну форму на захід, на який запрошено велику кількість людей, Ви не зобов'язані вказувати свій номер телефону. Зрозуміло, що на електронну пошту Вам надсилатимуть сповіщення про час і місце проведення заходу, можуть попросити підтвердити присутність. Однак, з дуже малою ймовірністю, якщо зареєструються 100 і більше осіб, кожній/кожному з них будуть телефонувати. Так само, організаторам не потрібно знати Ваш вік, якщо тільки захід не передбачено для повнолітніх (тоді достатньо зазначити, що Вам більше 18), або він орієнтований на аудиторію певного віку (можна створити вікові групи 18-25, 25-35, 35-50, 50-65 і тощо);

- ***цілісність та конфіденційність*** – створює обов'язок гарантувати належну безпеку персональних даних при їх обробці, у тому числі, захист проти несанкціонованого чи незаконного опрацювання та проти ненавмисної втрати, знищення чи завдання шкоди, із застосуванням відповідних технічних і організаційних інструментів;

- ***підзвітність*** – ця засада, як медаль, має дві сторони: з одного боку володілець даних має повідомляти орган про здійснення обробки та про будь-яке порушення захисту персональних даних, яке настало під час здійснення ним обробки; з іншого боку, суб'єкт персональних даних має право знати про дані, що обробляються та про іншу релевантну інформацію;

---

[131] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 51.
[132] Закон України «Про захист персональних даних» у порівнянні з Директивою 95/46/ЄС.

- ***справедливість, прозорість (транспарентність)*** – інформація про обробку персональних даних повинна бути відкритою, політика обробки має містити доступні та зрозумілі правила. Водночас, постає необхідність повідомити суб'єкта про обробку його персональних даних, про їх обсяг і види, як і дати йому можливість контролювати цю обробку[133].

Цих принципів повинні дотримуватися особи, що здійснюють обробку персональних даних. Зокрема, щоб обробка даних у цільовому маркетингу була законною, вона повинна базуватися на одній із підстав, закріплених у ст. 11 Закону. З цією метою, ***обробка може ґрунтуватися на необхідності захисту законних інтересів володільців даних*** (п. 6 ст. 11 Закону). Водночас, застосовується критерій відповідності, адже передбачено, що інтерес володільця не повинен переважати основоположних прав і свобод суб'єкта персональних даних[134]. Тому розглянемо конкретніше права фізичних осіб у зв'язку з обробку відомостей про них.

2.1. Права суб'єктів персональних даних в ході здійснення цільового маркетингу

У цьому підрозділі підсумуємо права фізичних осіб при обробці персональних даних, закріплені в українському законодавстві. До поля зору потрапить також Загальний регламент про захист даних. Це обумовлено тим, що інформацію про українських споживачів можуть обробляти суб'єкти господарювання з місцезнаходженням у ЄС. Наприклад, при купівлі товарів онлайн, під час отримання дисконтної картки на знижки в європейських супермаркетах, дані клієнтів вносяться до бази. Потім такі покупці вважаються цільовою аудиторією виробника/продавця/постачальника.

Хто ж є суб'єктом персональних даних?

---

[133] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 51.

[134] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

Ним визнається фізична особа, персональні дані якої обробляються. Тобто, персональні дані можуть належати тільки людині. Згідно ст. 8 Закону вона має право:

1) ***на інформацію*** стосовно:

- джерел збирання (корелюється з принципом законності), місцезнаходження своїх персональних даних, мети їх обробки, місцезнаходження або місця проживання (перебування) володільця чи розпорядника персональних даних;
- умов надання доступу до персональних даних, передусім третім особам (тобто знати про всі операції, які здійснюються з цими даними)[135];

2) ***на доступ до своїх персональних даних*** – для цього, як і для отримання інформації, надсилається запит до володільця даних в порядку ст. 16 Закону. У запиті зазначаються прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит[136];

3) ***на отримання відповіді на запит*** до володільця даних з питанням, чи здійснюється обробка його/її персональних даних, а також – на отримання переліку таких даних, впродовж тридцяти календарних днів з дня надходження запиту, крім передбачених законом випадків;

4) ***на пред'явлення вмотивованої вимоги із запереченням проти обробки*** своїх персональних даних володільцю;

5) ***на зміну або знищення своїх персональних даних*** володільцем/розпорядником персональних даних, якщо здійснюється незаконна обробка чи дані не відповідають дійсності;

6) ***на захист від незаконної обробки та випадкової втрати своїх персональних даних***, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист

[135] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 57.
[136] Див. Додаток 1.

від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи[137];

7) ***на звернення зі скаргами*** до контролюючих органів (Уповноваженого Верховної Ради України з прав людини або суду);

8) ***на правовий захист*** в разі порушення законодавства про захист персональних даних;

9) ***на обмеження права на обробку*** своїх персональних даних, надаючи застереженн разом зі згодою;

10) ***на відкликання згоди*** на обробку персональних даних[138]. Але якщо така згода не була єдиною підставою для обробки даних (наприклад, існують інші причини, передбачені законом), то це не буде за собою тягнути автоматичного припинення опрацювання даних суб'єкта. Наприклад, у цільовому маркетингу дані можуть оброблятися на підставі законного інтересу володільця;

11) ***на ознайомлення з механізмами автоматичної обробки*** персональних даних (відповідно до Загального регламенту – профайлинг);

12) ***на захист від автоматизованого рішення***[139].

Таким чином, першим і основоположним правом суб'єкта персональних даних є отримання інформації про початок їх обробки. Він/вона вправі дізнатися про: 1) володільця персональних даних, 2) склад та 3) зміст зібраних персональних даних, 4) свої права, визначені Законом, 5) мету збирання персональних даних та 6) осіб, яким передаються його/її персональні дані (ч. 2 ст. 12 Закону)[140]. У цілях нашого дослідження ми не будемо розглядати винятки, коли дозволено опрацювання даних без дозволу суб'єкта, адже маркетингова діяльність під них не підпадає.

Не менш важливим є право на доступ до інформації про себе, зокрема, на отримання відомостей про всі операції зі своїми персональними даними

---

[137] Див. Додаток 1.
[138] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.
[139] *Ibid.*
[140] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 51.

(крім випадків, коли це обмежено законом). У Директиві 95/46/ЄС містилося аналогічне положення.

Тлумачення цього положення надав Суд ЄС у справі «***Мер і члени міської ради Роттердаму проти М.Е.Е. Ріджкебура***». Суд постановив, що право на отримання зазначених вище відомостей повинне бути ретроспективним, стосуватися минулого, "інакше суб'єкт не матиме змоги повністю реалізувати свої права на те, щоб його дані вважалися незаконно або неправильно виправленими, стертими чи заблокованими, або на подання позову до суду та отримання компенсації за завдані збитки"[141]. Тому володілець повинен зберігати усю інформацію про те, кому він передає дані суб'єкта.

Знання про механізми автоматичної обробки – ще одне право суб'єкта персональних даних, про яке слід додати кілька ремарок. Профайлинг – це запорука успіху цільового маркетингу, як і бізнесу в цілому. Створення профілів клієнтів означає аналіз їх поведінки, звичок і вподобань, покупок, читай – купівельної спроможності. Цю інформацію продавець може використовувати у повідомленнях про акції (цікаво покупцям з низьким та середнім рівнем заробітку), для реклами нових імпортованих товарів (коньяком із багаторічною витримкою зацікавляться заможні покупці).

Але все це є втручанням у права суб'єктів персональних даних. Тому, у володільця даних є певні зобов'язання щодо інформування та отримання згоди особи, а також – здійснення обробки на підставі закону (п. 6 ст. 11 Закону), дотримання принципів обробки тощо[142].

Окрім цього, Законом у ст. 2 передбачено ***знеособлення персональних даних***, що зумовлює вилучення відомостей, які прямо чи опосередковано ідентифікують особу[143]. Втім, не передбачено порядку проведення цього знеособлення. Не роз'яснена ця процедура і в підзаконних актах. Практика іде таким шляхом, що при обробці даних автоматизованою системою, вони

[141] CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 7 May 2009.
[142] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 69.
[143] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

підлягають додатковому шифруванню. Якщо ж персональна інформація знаходиться у картотеках, то її стирають, а замість неї – проставляється ідентифікатор[144].

Особливого значення знеособлення набуває при обробці «чутливих» даних. Наприклад, під час пошуку цільової аудиторії для просування ліків, фармацевтична компанія обробляє інформацію про здоров'я пацієнтів лікарень. У цьому разі, необхідне шифрування, присвоєння спеціального індикатора.

Вартує зупинитися і на праві особи вимагати знищення її персональних даних. Воно конкретизоване у ст. 15 Закону, яка передбачає 4 випадки: закінчення строку зберігання даних, припинення правовідносин між сторонами, за приписом Уповноваженого (-ї) або посадових осіб секретаріату, за рішенням суду, що набрало законної сили[145]. Законом також передбачено, що суб'єкт персональних даних може вимагати їх зміни чи видалення, якщо вони не відповідають дійсності (п. 6 ч. 2 ст. 8 та ст. 20 Закону) та тільки видалення – при незаконній обробці (п.п. 6 та 11 ч. 2 ст. 8 та ст. 15 Закону)[146]. Коли особа отримує рекламу, в якій відомості про неї зазначені з помилками (наприклад, дівоче прізвище після зміни на прізвище чоловіка, або реклама про знижки до дня народження півроку після дня народження), то більш доцільним буде просто змінити дані. Якщо взагалі незрозуміло, яким чином рекламодавець отримав персональні дані клієнта, можна вимагати їх видалення з одночасним зверненням за захистом свого права (про це детальніше в розділі ІІІ). У цьому випадку йдеться про настання для суб'єкта негативних юридичних наслідків.

Водночас, Загальний Регламент передбачає значно більше прав суб'єктів персональних даних. У Європі також центральну позицію займає згода суб'єкта персональних даних, без такої – забороняється їх опрацювання. Більше того, встановлюються окремі правила для обробки відомостей про дитину, яка ідентифікована чи може бути ідентифікованою. Визначається, що до

---

[144] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 16.
[145] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.
[146] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 63.

досягнення 16-ти років згоду на збирання інформації про дітей повинні надавати батьки. Втім, граничний вік, коли особа може самостійно обирати, чи надавати згоду, Загальний регламент залишає на розсуд держави (мінімум – 12 років)[147].

Загальний регламент про захист даних містить положення про відкритість, прозорість інформації, яка стосується опрацювання персональних даних, створює підстави для доступу до них. Водночас, встановлюється можливість на прохання суб'єкта даних здійснювати передачу даних від одного контролера до іншого, закріплюється «право на забуття» [148]. Вважаємо, що це є проривом у сфері захисту даних. Однак, не всі ці норми забезпечуються великими гравцями на ринку цільового маркетингу (наприклад, *Facebook*), як і положення про створення профілів користувачів[149].

Як Законом, так і Загальним регламентом визначено чутливі категорії персональних даних, що потребують особливого захисту. Серед них,

> "відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках тощо, біометричні дані, генетичні дані, про стан здоров'я та статеве життя, притягнення до адміністративної чи кримінальної відповідальності, застосування щодо особи заходів в рамках досудового розслідування, вжиття щохдо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність», а також інформація про вчинення щодо особи тих чи інших видів насильства, місцеперебування та/або шляхи пересування особи" (ст. 7 Закону, в порівнянні з п.п. 10, 51 Загального регламенту)[150].

У ст. 7 Закону, передбачено цілий перелік винятків, коли обробку таких відомостей можна здійснювати:

1) при однозначній згоді суб'єкта персональних даних на їх обробку;

---

[147] Загальний регламент про захист даних (ЄС) 2016/679 від 27 квітня 2016 року [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16.

[148] *Ibid*.

[149] *Digital advertisers battle over online privacy* [Електронний ресурс] // The Economist. – 2016. – Режим доступу: https://www.economist.com/business/2016/11/05/digital-advertisers-battle-over-online-privacy.

[150] Закон України «Про захист персональних даних» Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481, в сукупності з «Порядком повідомлення Уповноваженого Верховної Ради України 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, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації», затвердженим Наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14.

2) у разі необхідності здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин із забезпеченням відповідного захисту;

3) якщо суб'єкт даних недієздатний або обмежено дієздатний;

4) із забезпеченням відповідного захисту релігійною чи громадською організацією, політичною партією або професійною спілкою та стосується виключно персональних даних членів цих об'єднань чи осіб, дотичних до них, а дані не передаються третім особам без згоди цих суб'єктів;

5) для обґрунтування, задоволення або захисту правової вимоги;

6) необхідна в цілях охорони здоров'я, для лікування, піклування та надання медичних послуг тощо;

7) стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

8) інформація, що явно оприлюднені суб'єктом персональних даних[151].

Дія цих положень, на нашу думку, поширюється також на випадки обробки інших даних, тим більше, що їх захист менш жорсткий[152].

До зазначених винятків слід віднести і обмеження, що можуть застосовуватися в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб[153]. Існують і застереження, засновані на нормах трудового, податкового, пенсійного, виборчого та інших законодавств. Так, наприклад, не потрібно давати згоду на обробку персональних даних, що становлять базу персональних даних співробітників підприємства, установи, організації тощо[154].

Натомість, як зазначають деякі дослідники, зокрема В. Ліпкан та Ю. Максименко, існує занадто багато випадків, коли допускається збирання,

---

[151] Закон України «Про захист персональних даних» Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481.

[152] Див. для порівняння *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 55.

[153] Закон України «Про захист персональних даних» Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481.

[154] Співак Н. *Типові помилки у сфері захисту персональних даних* / Співак Н. [Електронний ресурс]. – Режим доступу: http://www.apteka.ua/article/116863.

зберігання, використання і поширення персональних даних особи без її згоди[155]. Щоправда, ***цільовий маркетинг не підпадатиме під більшість із них, тому обов'язково слід повідомляти суб'єкта про обробку його даних***. Більше про це – в наступному підрозділі.

При диференціації персональних даних на звичайні та конфіденційні (чутливі), деякі науковці наполягають визначити, до якої з цих груп належать файли *cookies*[156]. Але, в епоху *big data*, аналітичні методи обробки даних спричинили розмивання кордонів між цими двома категоріями. Для маркетологів, ця категоризація взагалі є обмеженням, оскільки не дозволяє забезпечити гнучкість, необхідну в умовах технологічного прогресу[157]. Маркетологи наполягають на тому, що таргетинг є достатньо безпечним і не потребує детального регулювання, адже власника даних неможливо ідентифікувати. Припускають, що користувачі залишаються анонімними, оскільки вони можуть бути ідентифіковані лише через виданий трекінговий *cookie*-файл. Проте, з юридичної точки зору, ця позиція не відповідає дійсності[158]. Саме тому в наступному розділі ми розповімо, на що потрібно звернути увагу особам, які здійснюють обробку персональних даних у ході цільового маркетингу: і не важливо, чи це IP-адреса, чи *cookies.*

2.2. Обов'язки володільців персональних даних при використанні технології цільового маркетингу

Цілком зрозуміло, що правам, про які йшла мова у підрозділі 2.1. кореспондують обов'язки. Про них поговоримо у цьому підрозділі. За традицією почнемо з українського законодавства, продовжимо тим, яких вимог повинні дотримуватися маркетологи при обробці даних ***резидентів ЄС***, а також – коли саме це їх стосується. В кінці ж визначимо, наскільки таке регулювання

---

[155] Ліпкан В. *Інформаційні права і свободи людини і громадянина* / В. Лапкан, Ю. Максименко // Підприємництво, господарство і право. – 2011. – №9 (189). – С. 64.

[156] Koëter J. *Behavioural targeting and data protection* [Електронний ресурс]. – Режим доступу: http://www.cambridgeforums.com/ww.admin/materials/privacy/5Behavioral%20targeting_paper_draft%20publication_030510.pdf.

[157] De Hert P., Papakonstantinou V. *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*. Computer law & Security review 2012, p. 130-142.

[158] Koëter J. *Behavioural targeting and data protection*.

відповідає самій технології цільового маркетингу, а також те, чи ускладнилося і як – життя маркетологів після прийняття Загального Регламенту.

Але, стандартно, почнемо з визначення. ***Володільцем персональних даних***, згідно Закону, є фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом[159]. У підрозділі 1.2. ми зазначали, що маркетинг є комерційною діяльністю, метою якої є отримання прибутку. Тому слід розуміти, що особами, які здійснюють цільовий маркетинг можуть бути лише суб'єкти господарювання у розумінні Господарського кодексу України – підприємства та їх об'єднання, та фізичні особи - підприємці[160].

У ході використання цільового маркетингу беруть участь володільці та розпорядники, які вправі від імені володільця здійснювати обробку даних, зібраних в маркетингових цілях.

Такий поділ присутній і в Загальному регламенті про захист даних – на контролерів та операторів. Помітно, що до останніх ставляться додаткові вимоги:

- вони опрацьовують персональні дані лише на підставі задокументованих (з метою доказування) вказівок контролера, забезпечуючи збереження конфіденційності;
- вживають усіх заходів, необхідних для безпеки опрацювання персональних даних;
- допомагають контролеру здійснювати його обов'язки, також – належними технічними та організаційними заходами;
- на розсуд контролера, видаляють або повертають усі персональні дані контролеру після постачання послуг;
- звітують перед контролером[161].

---

[159] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

[160] Господарський кодекс України від 16.01.2003 р № 436-IV // Відомості Верховної Ради України. – 2003. – № 18. – № 19-20. – № 21-22. – Ст.144.

[161] Загальний регламент про захист даних (ЄС) 2016/679 від 27 квітня 2016 року [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16.

Однак, на думку науковців, такий поділ навряд чи можна назвати досконалим, тим більше при використанні технологій цільового маркетингу. Здається очевидним, що рекламні мережі, які збирають та обробляють інформацію, розміщують файли cookie, класифікуються як контролери даних. Хоча, насправді, веб-переглядач суб'єкта даних автоматично передає інформацію напряму маркетинговій компанії, щоб полегшити відправлення та читання cookie з метою розробки персоналізованої реклами. Важливо зазначити: незважаючи на те, що передача даних обумовлена браузером, її здійснює веб-майстер (власник, адміністратор сайту)[162].

Так, у рішенні *Google Spain v AEPD and Mario Costeja González* Суд ЄС встановив, що дочірня компанія *Google Inc.*, розташована на території Іспанії, повинна була діяти відповідно до європейського законодавства (на той час чинною була Директива 95/46/ЄС). Оскільки *Google Spain* та *Google Inc.* згідно європейських норм є однією юридичною особою, то відповідальність повинна бути покладена на материнську компанію (*Google Inc.*). Водночас, Суд ЄС дійшов висновку, що пошукова система відповідає за інформацію, яка показується у видачі[163].

Факти справи стосувалися публікації в газеті відомостей про заявника та його майно, зокрема про те, що воно підлягає конфіскації за борги із соціального страхування. Ця інформація набула поширення в мережі інтернет. Але після скарги Маріо Гонсалеса, ***Google Inc. зобов'язали забезпечити резидентів ЄС можливістю вимагати видалення своїх даних з пошукової видачі*** (на зразок «права на забуття»)[164].

Для цілей нашого дослідження це рішення релевантне тим, що воно підтверджує сформульовану раніше тезу, що веб-переглядачі, адміністратори сторінок і пошукових систем зобов'язані дотримуватися вимог законодавства,

---

[162] *EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour* [Електронний ресурс]. – Режим доступу: https://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N101BF.

[163] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (заява № C-131/12, рішення від 13.05.2014).

[164] *Ibid.*

якщо в ході реалізації технологій цільового маркетингу, вони здійснюють обробку персональних даних користувачів.

У зв'язку з цим, складно вирішити питання, хто є відповідальною особою за дотримання законодавства про захист персональних даних. Адже власник веб-сайту може здійснювати передачу даних і визначати ціль – для надання маркетингових послуг. При цьому, не слід недооцінювати роль самого рекламодавця. Коли особа натискає на рекламне оголошення, її дані збирають з метою створення статистики та ре-таргетингу. Далі, ця інформація може передаватися іншим рекламним мережам для здійснення ними маркетингу. Таким чином, з'являється питання «співконтролерів» або співволодільців[165].

Таких учасників правовідносин із обробки персональних даних не знає наше законодавство. Проте з точки зору цільового маркетингу, варто було б ввести такі поняття. Якщо мова йде про онлайн-маркетинг (на веб-сайтах і в соціальних мережах), то використовуються механізми *Google Analytics* та *Facebook Analytics*. Ці дві компанії і рекламодавець (найчастіше сам виробник/постачальник/виконавець), або маркетингова компанія будуть мати однаковий доступ до даних, зібраних у маркетингових цілях. Отже, їх можна визначити співволодільцями персональних даних.

А в прикладі з *Facebook* та *Instagram,* кожен з них має свою базу даних, щодо яких може приймати відповідні рішення, а водночас – доступ до даних контрагента[166]. Тобто наявні різні рівні доступу до даних, тому ці дві компанії є володільцями власних баз даних і співволодільцями даних контрагента.

Зважаючи на це, науковець Де Герт вважає розподіл на контролерів і операторів застарілим в епоху Web 2.0. Він радить взагалі скасувати поняття «операторів»[167]. Ми підтримуємо такий погляд, адже, дійсно, використання технологій цільового маркетингу, створює можливість усім суб'єктам цієї

---

[165] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (заява № C-131/12, рішення від 13.05.2014).*Ibid*.

[166] Політика захисту персональних даних [Електронний ресурс]. – Режим доступу: https://www.facebook.com/privacy/explanation.

[167] De Hert *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, p. 130-142.

діяльності мати необмежений доступ до персональних даних, що обробляються. А відтак, – і вчиняти порушення законодавства про захист персональних даних. Тому в цьому підрозділі ми зосередимо увагу саме на зобов'язаннях володільців персональних даних.

До моменту початку обробки персональних даних, майбутній володілець, повинен визначити:

1) мету та підстави обробки персональних даних;

Мета обробки повинна бути чіткою та законною. Процедури обробки, строк обробки та склад персональних даних повинні бути пропорційними меті. Якщо ж володілець змінив мету обробки, він повинен попередити суб'єкта даних і отримати нову згоду від нього.

2) категорії суб'єктів персональних даних;

3) склад персональних даних;

4) порядок обробки персональних даних, а саме:

- спосіб збору, накопичення персональних даних;
- строк та умови зберігання персональних даних;
- умови та процедуру їх зміни, видалення або знищення;
- умови та процедуру передачі персональних даних та перелік третіх осіб, яким можуть передаватися персональні дані;
- порядок доступу до персональних даних осіб, які здійснюють обробку, а також суб'єктів персональних даних;
- заходи забезпечення захисту персональних даних;
- процедуру збереження інформації про операції, пов'язані з обробкою персональних даних та доступом до них[168].

У випадках, передбачених Законом, володілець також визначає обов'язки та права осіб, відповідальних за організацію роботи, пов'язаної із захистом персональних даних під час їх обробки[169].

[168] Наказ Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v1_02715-14.
[169] *Ibid*.

Як зазначалося в попередньому підрозділі, необхідним є ***повідомлення суб'єкта персональних даних про їх обробку та отримання його/її згоди***. Наголосимо, що саме на володільцеві лежатиме тягар доведення вжиття усіх можливих заходів з метою повідомлення суб'єктів про збір інформації щодо них. Наприклад, у ході перевірки контролюючим органом. Відсутність доказів надання інформації суб'єктові персональних даних свідчитиме про порушення зобов'язань за ст. 12 Закону[170].

З іншого боку, законотворець чітко не визначив форму повідомлення про обробку персональних даних, зобов'язуючи, при цьому, сповіщати кожного суб'єкта окремо. Однак, такі вимоги видаються надмірними з точки зору маркетологів. Тому допускається вжиття різних способів повідомлення, зокрема, отримання підтвердження повідомлення від самого суб'єкта чи шляхом направлення односторонніх повідомлень, чи розміщення інформації на веб-сайтах[171].

Для згоди важливими є ще два параметри: ***добровільність та інформованість***. Як міжнародні акти, так і національне законодавство (п. 11 ч. 2 ст. 8 Закону) забороняє прямий чи опосередкований примус для отримання згоди від суб'єкта даних. Водночас, особа повинна бути повідомлена про те, ким, з якою метою, в якій мірі (перелік даних), оброблятимуться її дані, кому їх будуть передавати, а також – які права вона має у зв'язку з обробкою інформації про неї[172]. Наприклад, при використанні банерної реклами чи «спливаючих вікон», ці об'єкти мають містити назву відповідальної особи. Залежно від виду *cookies* також потрібно зазначати, що завдяки цим даним формується поведінковий профіль користувача, що самі дані можуть бути передані в треті країни[173].

---

[170] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 56.
[171] *Ibid.*
[172] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 35.
[173] Rürup M., Gradow L. *Mythen rund um DSGVO, Cookies, Einwilligung, E-Privacy – aufgelöst* [Електронний ресурс]. – Режим доступу: https://t3n.de/news/mythen-rund-um-dsgvo-cookies-1123331/?utm_source=google&utm_medium=amp-button.

Відповідальна особа повинна створити такий механізм, за якого дані про особу ним збиратимуться тільки після її згоди. Також бажано, щоб така згода була задокументована (наприклад, у вигляді коду). Тоді це може слугувати доказом в разі відкриття провадження щодо можливих порушень або перевірки Уповноваженим. Разом зі згодою слід записувати й інші дані – такі, як час і дату сеансу, агента користувача, віддалені URL-адреси, щоб підтвердити, що до отримання згоди не було завантажено файли *cookie*[174].

Цікавими є встановлені у Загальному регламенті вимоги щодо надання згоди та, в цілому, – політики приватності компаній. Формулювання повинно бути доступним, простим і зрозумілим користувачам. Звичайного посилання перед згодою на політику конфіденційності – недостатньо[175].

У Регламенті про конфіденційність та електронні повідомлення передбачені деякі особливості надання згоди. Коли документ набере чинності, не потрібно буде отримувати згоду користувача для обробки cookie-файлів, які використовуються лише для технічних цілей (наприклад, щоб зберегти товари у кошику для покупок на сайті інтернет-магазину). З іншого боку, при використанні *cookies* для відстеження або реклами буде потрібно отримати експліцитну, інформовану, добровільну згоду[176].

Ще один обов'язок, покладений законодавством на володільців персональних даних, також є доволі обтяжливим, бюрократичним. Йдеться про те, що згідно ч. 1 ст. 21 Закону володілець персональних даних протягом десяти робочих днів зобов'язаний повідомляти суб'єкта персональних даних про передачу персональних даних третій особі, якщо цього вимагають умови його згоди або інше не передбачено законом[177]. Тобто, спочатку первісний, а потім і

---

[174] Rürup M., Gradow L. *Mythen rund um DSGVO, Cookies, Einwilligung, E-Privacy – aufgelöst* [Електронний ресурс]. – Режим доступу: https://t3n.de/news/mythen-rund-um-dsgvo-cookies-1123331/?utm_source=google&utm_medium=amp-button.

[175] Загальний регламент про захист даних (ЄС) 2016/679 від 27 квітня 2016 року [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16.

[176] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

[177] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

новий, володільці персональних даних особи повинні повідомити її про обробку цих даних. Утім, авторитетні науковці стверджують, що такі вимоги не передбачені жодним міжнародним актом, і взагалі є зайвими. Те саме стосується необхідності повідомляти про зміну, видалення чи знищення персональних даних[178]. Ці норми ускладнюють процес ведення бізнесу, і на практиці про них часто забувають.

Нами було проведено дослідження функціонування кількох юридичних осіб, які здійснюють цільовий маркетинг. Кожен із них надсилає рекламні повідомлення постійним клієнтам. Було виявлено, що ці юридичні особи самостійно здійснюють маркетингову діяльність. Наприклад, у відповідь на наші запити ТОВ «РУШ» (відомий як магазин «EVA») та ТОВ «Книгарня "Є"» повідомили, що нікому не передають персональні дані своїх клієнтів. З цього можна зробити висновок, що вони мають спеціальні маркетингові відділи.

Звичайно, не кожна компанія може мати такі підрозділи, особливо, якщо вона доволі мала. Такі юридичні особи та фізичні особи – підприємці (разом – замовники) користуються послугами спеціальних маркетингових компаній. Якщо замовники самі збирають дані, то вони вже здійснюють їх обробку, а отже, є володільцями інформації, тоді маркетингова компанія стає розпорядником. Якщо дані збирає розробник реклами і сам їх використовує, то він і буде володільцем персональних даних.

Друга ситуація надзвичайно поширена в інтернеті. За допомогою таргетингу маркетолог визначає цільову аудиторію, збирає дані про користувачів відповідних сайтів, і вже тоді надсилає їм рекламу від замовника.

Перш за все, щоб встановити, наскільки обробка даних зазначеними вище компаніями відповідає вимогам законодавства, ми заглянули в політику конфіденційності цих фірм. З метою економії місця і простору, опишемо політику приватності магазину, в якому пересічні студентки інколи купують колготки і лак для волосся, і який інколи надсилає їм СМС-повідомлення про доступні акції, – «EVA».

---

[178] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 57.

На сайті цієї компанії можна знайти сторінку «Куточок споживача», де розміщена «Публічна угода». У пункті 10 містяться положення про «Конфіденційність і захист інформації». Вони цілком відповідають вимогам статті 13 Загального регламенту.

Зокрема, там вказано, що персональні дані Користувача/Покупця обробляються відповідно до Закону України від 01 червня 2010 року № 2297-VI «Про захист персональних даних», тобто є вказівка на застосовне законодавство.

Цілі опрацювання персональних даних зазначено у п. 10.4 «Публічної угоди»:

- для реєстрації Користувача на Сайті;
- для виконання своїх зобов'язань перед Користувачем/Покупцем;
- для оцінки та аналізу роботи Сайту;
- для визначення переможця в акціях, що проводяться Продавцем[179].

Інформація стосовно персональних даних зберігається в базі даних Продавця за адресою: 49055, Україна, м. Дніпро, пр. О. Поля, 104А та використовується виключно з метою дотримання вимог, що діють у сфері регулювання податкових відносин, відносин у сфері бухгалтерського обліку та відносин у сфері реклами[180]. Тобто, у «Публічній угоді» міститься інформація про особу, контактні дані та законні інтереси контролера.

Продавцем, відповідно до «Публічної угоди», є Товариство з обмеженою відповідальністю «РУШ», Код ЄДРПОУ 32007740, місцезнаходження: 49055, Україна, м Дніпро, пр. О. Поля, 104А, та/або інша юридична особа чи фізична особа-підприємець, товар яких розміщений в Інтернет-магазині EVA[181]. Та, згідно даних Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, ТОВ «РУШ» має іншу юридичну адресу.

[179] Публічна угода ТОВ «РУШ» [Електронний ресурс]. – Режим доступу: https://eva.ua/ua/publichnyj-dogovor.
[180] *Ibid.*
[181] *Ibid.*

Разом з тим, у «Публічній угоді» зазначена інформація стосовно створення користувацьких профілів та маркетингової діяльності товариства. Продавець отримує відомості про IP-адресу відвідувача Сайту магазину «EVA». Ця інформація не використовується для встановлення особистості відвідувача[182].

Також продавець має право відправляти інформаційні, в тому числі рекламні повідомлення, на електронну пошту і мобільний телефон Користувача/Покупця з його згоди. Користувач/Покупець має право відмовитися від отримання рекламної та іншої інформації без пояснення причин відмови. Сервісні повідомлення, що інформують Користувача/Покупця про замовлення та етапи його обробки, відправляються автоматично і не можуть бути відхилені Користувачем/Покупцем[183].

Щодо можливості доступу суб'єкта персональних даних до відомостей про його особу – в «Публічній угоді» відповідних положень немає. Втім, можна зробити висновок, що такий доступ надається згідно ст. 16 Закону «Про захист персональних даних» – у порядку запиту протягом 30 календарних днів з дня його надходження[184].

Також можна змінити свої анкетні дані, що були надані користувачами спочатку, що відповідає п. 6 ч. 2 ст. 6 Закону[185].

Зрештою, політика приватності на сайті «EVA» доступна і легка для прочитання та розуміння пересічних громадян і відповідає українському законодавству та вимогам Загального регламенту про захист даних.

В принципі, те ж саме стосується «Книгарні "Є"». У відповідях на запити, в компаніях нам відповіли в межах передбаченого строку (30 днів). В обох випадках, інформація із баз персональних даних нікому не передається. Доступ до них мають виключно працівники, які в силу своїх посадових обов'язків здійснюють адміністрування цих баз. З ними укладаються письмові

[182] Публічна угода ТОВ «РУШ» [Електронний ресурс]. – Режим доступу: https://eva.ua/ua/publichnyj-dogovor.
[183] *Ibid.*
[184] Закон України «Про захист персональних даних» Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481.
[185] *Ibid.*

зобов'язання про нерозголошення персональних даних. До того ж. компанії запевнили, що своєчасно вживають необхідних заходів з метою забезпечення захисту персональних даних від випадкових втрати чи знищення, незаконної обробки, у тому числі, незаконного знищення чи доступу до даних.

Отже, можна констатувати, що господарські товариства, запити до яких ми надсилали, справді дотримуються законодавства про захист персональних даних і самостійно викладають свої політики приватності у відповідності до міжнародних стандартів.

Водночас, студенти Магістерської програми з прав людини Українського католицького університету надсилали схожі запити до інших володільців персональних даних, які займаються маркетинговою діяльністю. Щоб перевірити законність дій однієї з таких компаній, на їхню електронну адресу було надіслано листа з проханням надати персональні дані клієнта. Втім, у повідомленні не було зазначено жодних ідентифікуючих ознак, крім прізвища, імені та по-батькові та номера картки постійного клієнта (не було навіть зазначено реквізити паспорта, що передбачено п. 1 ч. 4 ст. 16 Закону[186]). У відповідь було отримано всю інформацію, яка містилася у базі даних компанії, включно з номером телефону та домашньою адресою, та навіть була надана копія анкети з особистим підписом. В кінці, наче з іронією, працівники володільця персональних даних зазначили, що компанія "дотримується усіх передбачених чинним законодавством України заходів щодо забезпечення захисту персональних даних від випадкових втрати, знищення, незаконної обробки, у тому числі, незаконного знищення чи доступу до персональних даних".

Це було кричущим порушенням законодавства, яке ілюструє неналежність захисту персональних даних, та означає, що десь (у законодавстві чи практиці) існують суттєві прогалини, які необхідно найближчим часом виправити. Наприклад, вартувало б оновити ст. 16 Закону, оскільки у такому

[186] Закон України «Про захист персональних даних» Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481.

вигляді, як зараз, вона не встановлює чітких критеріїв для верифікації суб'єкта звернення, тому є можливими такі колапси на практиці.

2.3. Гарантії дотримання законодавства про захист персональних даних у цільовому маркетингу

При регламентації обробки персональних даних у ході цільового маркетингу, передусім, потрібно знайти баланс між інтересами компаній і правами споживачів. Цей процес ускладнюється тим, що, з одного боку, існує право особи на захист відомостей, які її ідентифікують, а з другої – право на інформацію про продукти та послуги, які пропонує придбати суб'єкт господарювання.

Для розв'язання розкритих проблем вчені пропонують цілу низку заходів. Наприклад, у пошуковій видачі можна окремо відображати передплачену рекламу, спонсорські посилання та всі інші результати пошуку[187]. В принципі, так і функціонує реклама в *Google*. Повідомлення відображаються зверху з позначкою, що це реклама.

Тільки навряд чи цього достатньо. Адже перш за все, маркетингові компанії повинні забезпечити анонімність даних, що ними використовуються, наприклад, при створенні «інформаційного профілю» користувача. Таким чином, ***слід знеособлювати дані та використовувати систему подвійної асоціації***[188]. Зібрані на основі таргетингу відомості повинні оброблятися виключно у маркетингових цілях, щоб було неможливо передати їх третім особам.

Споживач ***повинен знати, що маркетингова компанія використовує тергетингові механізми. Це також можна назвати своєрідною гарантією забезпечення захисту персональних даних.*** Основним завданням виробника, чи надавача послуг, а, відповідно, і маркетолога, у сфері захисту персональних

---

[187] Зоріна Ю.І. *Цивільно-правові відносини при здійсненні рекламної діяльності* : дис... канд. юрид. наук: 12.00.03 / Київський національний ун-т ім. Т.Г.Шевченка. – К., 2007. – С. 8.

[188] Воєводін Б. В. *Цивільно-правові аспекти таргетованої (цільової) реклами, персоналізації та приватності у рекламі*, С. 122.

даних є інформування потенційного клієнта про відомості, які він збирає, технології, що використовує, а також – надання можливості дозволити чи відмовитися від збору таких даних, змінити їх параметри, обмежити їх обробку, доступ до них третіх осіб тощо. Також видається перспективною ідея ліцензування роботи маркетингових фірм, що стосується обробки персональних даних. Та, як і всі інші володільці баз персональних даних, вони також повинні надсилати свої заяви до омбудсмана, а інформацію про таких суб'єктів господарювання слід розміщувати на офіційному сайті Уповноваженого.

Вагомим кроком є ***заборона збереження у cookie-файлах даних щодо раси, релігійних переконань, сексуальної орієнтації, стану здоров'я, тобто даних, що визначені законом як конфіденційна інформація***. Це поставить крапку в питанні про віднесення таких даних до «чутливої» категорії, і забезпечить збереженість цієї інформації.

Дані логінування можна кожного разу вводити заново, не зберігаючи їх у браузері. Альтернативний варіант – шифрування таких даних (логінів і паролів) за допомогою спеціальних програм (наприклад, антивірусу *Avast*).

У п. 78 Загального регламенту про захист даних передбачено:

> Захист прав і свобод фізичних осіб у зв'язку з опрацюванням персональних даних вимагає застосування відповідних технічних та організаційних інструментів для забезпечення виконання вимог цього Регламенту. Для того, щоб мати можливість підтвердити відповідність цьому Регламенту, контролер повинен ухвалити норми внутрішньої політики та забезпечити застосування інструментів, що відповідають, зокрема, принципам захисту даних за призначенням та захисту даних за замовчуванням. Такі заходи можуть передбачати, між іншим, скорочення опрацювання персональних даних, якомога швидше використання псевдонімів до персональних даних, прозорість щодо функцій та опрацювання персональних даних, уможливлення суб'єкта даних відстежувати опрацювання даних, уможливлення контролера створювати та вдосконалювати характеристики безпеки. Під час створення, розроблення, відбору та використання застосунків, сервісів та продуктів, що засновано на опрацюванні персональних даних, або опрацюванні персональних даних для виконання своїх завдань, необхідно заохочувати виробників продуктів, сервісів і застосунків враховувати право на захист даних під час створення та розроблення таких продуктів, сервісів і застосунків і, з належним дотриманням сучасного рівня розвитку, переконуватися, що контролери і оператори здатні виконувати свої зобов'язання щодо

захисту даних. Принципи захисту даних за призначенням та захисту даних за замовчуванням необхідно також брати до уваги в контексті публічних тендерів.[189]

Від маркетологів така норма вимагає застосування новітніх технологій, які забезпечують збереженість даних (*Data Protection by Design*) та налаштувань конфіденційності (*Data Protection by Default*). Одним із засобів, що відповідають цій нормі є ***анонімізація та псевдонімізація***[190].

Про технологію *Opt-in* ми вже побіжно згадували. Поки що її застосування не є обов'язковим, вона передбачена Регламентом про конфіденційність та електронні повідомлення[191]. Поки що він не прийнятий, однак є позитивна практика деяких веб-сайтів, які дають доступ до контенту, навіть якщо користувач відмовляється від залишення на сторінці файлів *cookie.* На жаль, це ще не стало загальною практикою і часто особа не має вибору – мусить давати згоду на опрацювання її даних, що зберігаються у *cookie*-файлах.

Є також кілька стратегій, які можна використовувати для боротьби з небажаною рекламою:

- встановлення блокування реклами (Ad-Blocker) та спливаючих вікон (Pop-up-Blocker), щоб приховати рекламу та блокувати передачу даних;
- налаштування параметрів веб-браузера (наприклад, блокування файлів cookie, Flash і JavaScript);
- використання приватного чи анонімного режиму браузера;
- використання дискретних пошукових систем;
- маскування IP-адреси (через VPN, браузер Tor і т.п.)[192].

Гарантіями захисту прав людини у сфері персональних даних можна вважати і можливість звернення до володільця даних із заявою про отримання

[189] Загальний регламент про захист даних (ЄС) 2016/679 від 27 квітня 2016 року [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16.
[190] Roßnagel A. *Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung*. Springer Fachmedien Wiesbaden GmbH 2017, p. 131.
[191] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.
[192] Internetwerbung: Werbemöglichkeiten im Internet vs. Datenschutz? Datenschutz.org, [Електронний ресурс]. – Режим доступу: https://www.datenschutz.org/internetwerbung.

інформації щодо обробки. А якщо вже сталося, то особа має право подати скаргу до наглядового органу (в Україні – Уповноважений з прав людини згідно ст. 23 Закону), але це не завжди дає результати, як це було у справі Макса Шремса[193].

У ході нашого дослідження, ми, на жаль, також зіткнулися з проблемо, що Секретаріат Уповноваженої неналежним чином відповідає на запити. Зокрема, після розгляду нашого звернення про надання публічної інформації стосовно одного з мобільних операторів України, щодо якого була проведена перевірка, нам відповіли листом, де було приховано 25 сторінок. Решта була вказана, як конфіденційна інформація. Надалі ми плануємо оскаржувати таку відповідь державного органу.

Великою перевагою Загального регламенту є нотифікаційні гарантії. Вони вступають у дію, знову ж таки, уже після порушення прав суб'єкта персональних даних, але створюють для нього можливість вжити якнайшвидших заходів реагування. Так, контролер повинен протягом 72 годин повідомити наглядовий орган про порушення законодавства про захист персональних даних, або надати супровідну інформацію про причини затримки. Водночас, контролер здійснює повідомлення суб'єкта даних у випадку ймовірного виникнення високого ризику для прав і свобод фізичних осіб. Окрім цього, він надає інформацію щодо порушень, їх наслідків і вжитих заходів. Але не завжди, а тільки тоді, коли справді виникає ризик для прав людини.

Незважаючи на ці всі ризики, 39 % споживачів надають перевагу цільовому маркетингу, що створює релевантний контент, за даними дослідження *Sodexo Rewards and Benefits Services.* 21 % респондентів не проти отримувати товари та послуги, які не є припасованими до їх потреб. Це дослідження показало, що насправді 58 % опитаних віком від 55 років та 67 %

[193] Maximilian Schrems and Data Protection Commissioner (справа № 2013/765/JR від 10.12.2013).

молодих людей 18-44 років, не вважають цільовий маркетинг набридливим чи таким, що посягає на їх права[194].

Вірити, чи ні даним опитування – кожен (-а) обирає самостійно. При цьому, не треба забувати про всі позитивні сторони таргетингу, що економить час, кошти, зусилля. Головним питанням залишається забезпечення схоронності персональних даних, добросовісного дотримання правил обробки. Тільки так компанія створить велику аудиторію постійних покупців, кожного разу розширюючи її потенційними клієнтами.

У протилежному випадку, несумісна із законами та Загальним регламентом практика маркетингових компаній матиме наслідком відповідну реакцію контролюючих органів. Про це, та про відповідальність у разі порушення встановлених норм про захист персональних даних, розповімо в наступному розділі.

[194] Davies J. *Consumers Like Targeted Marketing Despite Privacy Concerns* [Електронний ресурс]. – Режим доступу: http://digitalmarketingmagazine.co.uk/digital-marketing-data/consumers-like-targeted-marketing-despite-privacy-concerns/4531 (04.08.2017).

ВИСНОВКИ ДО РОЗДІЛУ ІІ

Здійснюючи обробку персональних даних, відповідальна особа повинна дотримуватися основних принципів: законності; наявності мети; точності та достовірності; адекватності, пропорційності, ненадмірності; цілісності та конфіденційності; підзвітності; справедливості, прозорості.

Підставою для обробки персональних у цільовому маркетингу є законний інтерес володільця даних, тобто особи, що здійснює маркетингову діяльність. Тоді цей інтерес не повинен переважувати основоположних прав і свобод суб'єкта персональних даних. Іншою підставою є згода самого суб'єкта на обробку інформації про нього/неї.

За суб'єктами персональних даних, якими можуть бути тільки фізичні особи, закріплено цілий список прав, серед яких: право на отримання інформації щодо обробки персональних даних, на доступ до своїх персональних даних, направляти заперечення щодо обробки персональних даних, право суб'єкта на видалення та зміну персональних даних, право заперечувати проти обробки, на знеособлення персональних даних та інші.

Водночас, Загальним регламентом встановлено ширший список прав, що охоплює більше випадків їх можливого порушення. Європейським законодавством також взято до уваги тенденції сучасного розвитку цільового маркетингу, та технологій, що використовуються під час такої діяльності. На жаль, українське законодавство з цього питання пасе задніх.

Те ж саме помічаємо стосовно обов'язків володільців персональних даних, якими можуть бути суб'єкти господарської діяльності (фізичні особи - підприємці або юридичні особи), які визначають мету обробки персональних даних, встановлюють склад цих даних та процедури їх обробки, якщо інше не визначено законом. Також слід зазначити, що саме ці особи несуть відповідальність за порушення законодавства про захист персональних даних.

У підрозділі 2.2. ми відстоювали позицію про відсутність потреби розподілу на володільців і розпорядників суб'єктів господарювання, що

надають маркетингові послуги. Адже, зазвичай, залучені в цей процес особи мають необмежений доступ до бази даних і профілів користувачів. Звісно, це питання буде вирішуватися у конкретному випадку окремо, але, за загальним правилом, тим більше при використанні інтернет-технологій, усі ці особи мають однаковий доступ до даних.

До обов'язків володільців персональних даних у сфері цільового маркетингу належить: визначення мети обробки, повідомлення суб'єкта персональних даних про обробку та отримання від нього добровільної, інформованої згоди, повідомлення про зміну мети обробки та отримання нової згоди та інші, передбачені законодавством.

Водночас учасники маркетингової діяльності повинні забезпечити гарантії прав суб'єктів персональних даних, що полягають у знеособленні даних та використанні системи подвійної асоціації, попередженні про застосування тергетингових механізмів, забороні збереження у cookie-файлах «чутливих» даних, анонімізації та псевдонімізації клієнтів.

РОЗДІЛ ІІІ
ЗАХИСТ ПРАВ СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ПОРУШЕННІ ЇХНІХ ПРАВ У ХОДІ ЦІЛЬОВОГО МАРКЕТИНГУ

Захист персональних даних, насамперед, здійснюють володільці, розпорядники персональних даних та треті особи, яким надано доступ до таких відомостей (ст. 24 Закону)[195]. У попередньому розділі ми пояснювали, що до діяльності з цільового маркетингу залучені багато суб'єктів: виробник продукції та постачальник послуг, маркетингова компанія, веб-переглядач, адміністратор веб-сторінок, пошукових систем. Кожен із них може здійснювати обробку даних, отриманих внаслідок застосування технології таргетингу. У зв'язку з цим, складно вирішити, хто повинен нести відповідальність за порушення законодавства про захист персональних даних. Оскільки зобов'язання дотримуватися законодавства про захист персональних даних покладені на володільців, розпорядників і третіх осіб, то в окремому кожному випадку буде вирішуватися, хто, в якій мірі та яким чином отримав доступ до даних. Окремим питанням буде розглядатися, на якому етапі було вчинено порушення і хто саме в цей момент здійснював обробку (в якій із баз даних конкретні відомості зберігалися).

Ці суб'єкти правовідносин повинні створити (визначити) спеціальний структурний підрозділ чи відповідальну особу, що буде організовувати роботу, пов'язану із захистом персональних даних при їх обробці. Працівники підприємств мають діяти у межах повноважень, передбачених посадовими інструкціями, вміти працювати з базами даних. Ці особи перед початком роботи з базами даних (чи безпосередньо при прийнятті на роботу) підписують зобов'язання не розголошувати інформацію, що стала їм відомою в ході

[195] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

виконання професійних обов'язків, та нести відповідальність за порушення законодавства про захист персональних даних[196].

Зазвичай відповідальні особи є одержувачами даних володільця і здійснюють такі функції щодо захисту персональних даних:

1) проводять оцінку ризиків та консультують володільця / розпорядника щодо належної організації процесу обробки персональних даних;

Оцінці підлягає шкода, що буде завдана суб'єкту персональних даних у разі їх втрати, видалення, умисного чи випадкового протиправного розповсюдження. Корисно буде також визначити, наскільки сильна мотивація в інших працівників підприємства незаконно заволодіти відомостями, чи іншим чином порушити права суб'єкта персональних даних. На підставі цього, підрозділ / посадова особа розробляє пропозиції щодо порядку захисту персональних даних, роботи із запитами суб'єктів та третіх осіб, визначення оптимального складу даних, що підлягатиме обробці, порядок збору персональних даних та повідомлення про це суб'єкта, порядку та рівнів доступу працівників до персональних даних, порядок документування процесів, пов'язаних з обробкою персональних даних та ін.[197].

2) проводити консультації для інших працівників / підрозділів володільця щодо розгляду запитів суб'єктів та третіх осіб про отримання доступу до персональних даних;

3) проводити моніторинг процесів обробки персональних даних на предмет їх відповідності законодавству. Моніторинг може проводитися у формі аудиту, висновки якого з пропозиціями покращення потім можна довести до відома володільця даних.

4) доводити до відома керівництва та Уповноваженого (-ї) випадки порушення прав суб'єктів персональних даних, надавати рекомендації менеджерам щодо вжиття першочергових заходів, спрямованих на мінімізацію

[196] Закон України «Про захист персональних даних», порівн. з Типовим порядком обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14.
[197] *Ibid.*

потенційних негативних наслідків, ініціювання розслідування інциденту, повідомлення суб'єкта (-ів) персональних даних, чиї права порушено;

5) ознайомлювати керівництво та працівників володільця із вимогами чинного законодавства про захист персональних даних, внесеними до нього змінами та доповненнями, актуальними проблемами у сфері захисту персональних даних, організовувати навчання працівників;

6) взаємодіяти з Уповноваженим (-ою). Це може проявлятися в отриманні консультацій, направленні до Секретаріату пропозицій про внесення змін до нормативно-правових актів (прийняття нових), співпраці під час проведення заходів контролю, і, звісно, – у вчасному виконанні приписів Уповноваженого[198].

Інформацію про відповідальний підрозділ / особу, суб'єкти господарювання повідомляють Уповноваженому (-ій) Верховної Ради України з прав людини. Особи, до яких немає вимоги щодо створення підрозділу чи призначення відповідальної особи, самостійно здійснюють таку діяльність та комунікують з Уповноваженим (-ою) (фізичні особи - підприємці, самозайняті особи)[199].

Разом із організаційними заходами слід забезпечити реалізацію прав суб'єктів персональних даних, їх гарантій, виконання обов'язків володільцями / розпорядниками. Як мінімум, особу слід інформувати про обробку її даних. Якщо це не здійснено, то ставиться під питання сама можливість захисту прав суб'єкта персональних даних.

Яскравий приклад цьому перебував на розгляді в ЄСПЛ у справі «***I. v. Finland***». Заявниця скаржилася на неспроможність лікарні гарантувати захист її персональних даних. Відтак, широкому загалу стало відомо про її хворобу – СНІД. Але в межах національного судочинства, їй так і не вдалося відстояти справедливість. ЄСПЛ констатував: «заявниця програла цивільну справу через

[198] Закон України «Про захист персональних даних», порівн. з Типовим порядком обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14.
[199] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

те, що ***не змогла довести причинно-наслідковий зв'язок між недоліками в правилах доступу та поширенням інформації про стан її здоров'я***» [200]. Суд встановив необхідність посилення контролю над збереженням медичних карток (анамнезів) пацієнтів лікарні, забезпечити доступом до них тільки персонал, що безпосередньо залучений до лікування та вести облік таких осіб[201].

Інформований – значить захищений. Так, згідно ч. 5 ст. 55 Конституції України особа має право будь-якими не забороненими законом засобами захищати свої права і свободи від порушень і протиправних посягань[202]. Існують різні механізми захисту персональної інформації. Звісно, межею для дій особи щодо захисту своїх даних є й права третіх осіб.

Серед цивільно-правових способів захисту завжди вагому роль відіграє ***самозахист***. Так, фізична особа у випадку обробки відомостей про неї може звернутися до володільця чи розпорядника персональних даних з вмотивованою вимогою задовольнити її права за ст. 8 Закону, яка цитувалася у першому підрозділі другого розділу. Окрім цього, можна в будь-який момент відкликати згоду на обробку персональних даних, вимагати їх зміни або знищення (ст. 8 Закону)[203].

До механізмів захисту персональних даних також слід віднести ***можливість відмови у доступі до такої інформації третім особам***. Так, цікавим є випадок, який розглядався в ЄСПЛ у 1989 р., справа «Гаскін проти Сполученого Королівства» («Gaskin v. the United Kingdom»). Заявник, Грем Гаскін звернувся до міської ради Ліверпуля з метою отримати інформацію щодо своїх опікунів, у сім'ях яких він виховувався. Йому відмовили, тому що не всі опікуни дали згоду на передачу йому своїх даних з архіву. ЄСПЛ постановив, що потрібно забезпечити інтереси особи, яка намагається отримати

---

[200] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 81.
[201] I. v. Finland, no. 20511/03, 17 July 2008
[202] Конституція України прийнята Верховною Радою України 28.06.1996 р. № 254к/96–ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
[203] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

доступ до матеріалів про її особисте і сімейне життя, коли до автора записів або немає доступу, або він неправомірно відмовляється дати згоду[204].

Якщо одна із зазначених вимог суб'єкта персональних даних не буде виконана, така особа може ***оскаржити дії чи бездіяльність володільця або ж розпорядника персональних даних до суду чи Уповноваженого (-ї) Верховної Ради України з прав людини*** (ст. 22 Закону України «Про захист персональних даних»)[205]. Останній вид захисту є особливим інститутом для українського законодавця, оскільки був введений не так давно – 1 січня 2014 року – Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних». Повноваження щодо контролю за додержанням законодавства про захист персональних даних було покладено на Уповноваженого Верховної Ради України з прав людини відповідно до Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних»[206]. Водночас, цей орган не підміняє інші, до компетенції яких входить захист і поновлення порушених прав і свобод людини. Так, згідно ст. 17 Закону «Про Уповноваженого (-ї) Верховної Ради України з прав людини» Уповноважений (-а) не розглядає тих звернень, які розглядаються судами, не зупиняє вже розпочатий розгляд, якщо заінтересована особа подала позов, заяву або скаргу до суду[207].

Таким чином, саме на Уповноваженого (-у) покладено особливі обов'язки по захисту прав суб'єктів персональних даних і нагляду за дотриманням законодавства в цілому. Інститут Уповноваженого (-ї) є незалежним органом (ст. 4 Закону України «Про Уповноваженого Верховної Ради України з прав людини»), підзвітним лише Верховній Раді України (щорічні та спеціальні доповіді згідно ст. 18 Закону «Про Уповноваженого

[204] Gaskin v. the United Kingdom (заява № 10454/83 від 07.07.1989 року).
[205] Закон України «Про захист персональних даних» Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481.
[206] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Міжнародний договір / Офіційний вісник України. – 2011 – № 1, № 58. – 2010. – Ст. 1994. – Ст. 85.
[207] Закон України «Про Уповноваженого Верховної Ради України з прав людини» // Відомості Верховної Ради України. - 1998. - № 20.

Верховної Ради України з прав людини»)[208]. Компетенція цієї посадової особи, як і службовців Секретаріату – дуже широка, що дозволяє ефективно здійснювати покладені на них обов'язки. Уповноважений (-а) на час здійснення повноважень користується імунітетом, іншими гарантіями за ст. 20 Закону «Про Уповноваженого Верховної Ради України з прав людини» та правами, передбаченими положеннями цього Закону (наприклад, правом невідкладного прийому усіма органами публічної влади, посадовими та службовими особами, особами приватного права згідно ст. 13 Закону «Про Уповноваженого Верховної Ради України з прав людини»)[209].

Державний контроль за дотриманням законодавства про захист персональних даних, який ми розглядатимемо в підрозділі 3.1., хоч і не є безпосереднім способом захисту, – він передує йому. Наглядова діяльність органів державної влади покликана попередити правопорушення, уособлюючи охоронну та регулятивну функції державної влади.

3.1. Державний контроль за дотриманням законодавства про захист персональних даних

Згідно ст. 22 Закону контрольну функцію за додержанням законодавства про захист персональних даних здійснюють Уповноважений (-а) Верховної Ради України з прав людини та суди.

Захист персональних даних забезпечується Уповноваженим (-ою). Він/вона має право на проведення планових, позапланових, виїзних та безвиїзних перевірок (ст. 23 Закону України «Про захист персональних даних»)[210].

Відповідно до ст. 23 Закону України «Про захист персональних даних» здійснюючи повноваження у сфері захисту персональних даних, омбудсман:

- затверджує нормативно-правові акти;

[208] Закон України «Про Уповноваженого Верховної Ради України з прав людини» // Відомості Верховної Ради України. - 1998. - № 20.
[209] *Ibid.*
[210] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

- відповідає на звернення фізичних і юридичних осіб;
- здійснює нагляд (контроль) за діяльністю володільців або розпорядників персональних даних, зокрема, проводячи їх перевірки;
- вправі отримувати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних у рамках здійснення контролю;
- видає обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства, складає протоколи про притягнення до адміністративної відповідальності;
- надає рекомендації та роз'яснення щодо практичного застосування законодавства про захист персональних даних, направляє їх до суду;
- взаємодіє із структурними підрозділами або відповідальними особами, які організовують роботу, пов'язану із захистом персональних даних при їх обробці, оприлюднює інформацію про них[211];
- може звертатися з пропозиціями до інших органів публічної влади, їх посадових осіб;
- надає висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них;
- здійснює інформативну та моніторингову діяльність щодо застосування законодавства з питань захисту персональних даних, а також – нових практик, тенденцій та технологій у цій сфері;
- організовує та забезпечує взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними;
- бере участь у роботі міжнародних організацій з питань захисту персональних даних[212].

Врешті-решт, Уповноважений (-а) щорічно звітує перед Верховною Радою про стан дотримання законодавства про захист персональних даних[213].

---

[211] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.
[212] *Ibid.*
[213] *Ibid.*

Крім того, ч. 1 ст. 13 Закону України «Про Уповноваженого Верховної Ради України з прав людини» передбачає значну кількість повноважень цього контролюючого органу при проведенні ним перевірок[214].

Водночас, статтею 14 Закону України «Про Уповноваженого Верховної Ради України з прав людини» передбачено обов'язок Уповноваженого (-ї) забезпечувати виконання покладених на нього/неї функцій та повною мірою використовувати надані йому/їй права, як і зберігати конфіденційну інформацію[215].

Процедура проведення перевірок встановлена Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженим наказом Уповноваженої №1/02-14 від 08 січня 2014 р.[216]. Такі перевірки бувають виїзні (за місцезнаходженням юридичної особи / фізичної особи - підприємця), безвиїзні (в приміщенні Секретаріату Уповноваженого (-ї) на підставі наданих суб'єктом господарювання документів), планові (проводяться на підставі плану проведення перевірок на відповідний квартал та рік, інформація про них розміщується на сайті омбудсмана) та позапланові (проводяться за власною ініціативою Уповноваженого (-ї), чи у разі повідомлення про порушення володільцем / розпорядником вимог законодавства)[217]. Особливістю цих перевірок, на відміну від тих, які проводять інші контролюючі органи (ДФС, Держпраці, ПФУ), є те, що володілець персональних даних не отримує жодних попереджень перед проведенням моніторингових заходів.

Перевірки можуть проводитися самим Уповноваженим (-ою), керівником Секретаріату та його заступником, Представниками

---

[214] Закон України «Про Уповноваженого Верховної Ради України з прав людини» // Відомості Верховної Ради України. - 1998. - № 20.
[215] *Ibid.*
[216] Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v1_02715-14.
[217] Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v1_02715-14.

Уповноваженого (-ї), керівниками структурних підрозділів Секретаріату та їх заступниками, працівниками Секретаріату Уповноваженого (-ї)[218]. Після прибуття вказаних посадовців за місцезнаходженням суб'єкта перевірки, вони зобов'язані пред'явити посвідчення, додаток до нього, а також видане Уповноваженим на конкретний строк доручення. Хорошою практикою є ведення журналу перевірок суб'єктом господарювання. Після запису в такому журналі, підприємство зобов'язане надати доступ до приміщень, архівів, навіть інформації з обмеженим доступом, чи такої, що містить комерційну таємницю, якщо це необхідно для проведення перевірки. Вона не підлягає подальшому розголошенню[219].

За результатами перевірок складаються акт у двох примірниках з відповідними реквізитами. Акт підписується Уповноваженим чи посадовою особою та суб'єктом перевірки. Якщо останній не згідний з висновками, він має право зробити відмітку про застереження. Якщо він взагалі відмовляється підписати акт, про це робиться відповідний запис. Один примірник залишається в Секретаріаті Уповноваженого, інші віддається суб'єкту перевірки. Якщо він відмовляється від цього, акт повинен бути йому надісланий поштовим відправлення протягом 5 робочих днів[220].

На підставі такого акта, при виявленні порушень законодавства про захист персональних аних, складається припис про їх усунення, що надсилається суб'єктові впродовж 5 робочих днів, а другий примірник залишається в Секретаріаті Уповноваженого. На виконання вимог припису підприємству надається строк не менше 30 календарних днів. Після спливу цього строку суб'єкт повинен проінформувати Уповноваженого про виправлення порушень з додаванням копій відповідних документів. За необхідності може бути проведена позапланова перевірка[221].

---

[218] Фотографії цих осіб розміщені на сайті омбудсмана, тому під час візиту з перевіркою можна перевірити, чи дійсно особи, що завітали, мають такі повноваження.
[219] Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v1_02715-14.
[220] *Ibid.*
[221] *Ibid.*

У разі невиконання припису протягом вказаного у ньому строку складається протокол про адміністративне правопорушення за ст. 188-40 КУпАП за формою та у порядку, передбаченому законодавством та Порядком оформлення матеріалів про адміністративні правопорушення[222]. У випадку порушення ст. 188-39 чи ст. 188-40 КУпАП органи контролю складають протокол про адміністративне правопорушення відповідно до п. 1 ч. 1 ст. 255 КУпАП. При наявності у вчиненому суб'єктом перевірки діянні ознак кримінального правопорушення, матеріали перевірки підлягають направленню до правоохоронних органів[223]. Більш конкретно зупинимося на кримінальній відповідальності в наступному підрозділі.

Показником успішності та фахового рівня роботи Секретаріату Уповноваженого з прав людини є його широка міжнародна співпраця з Євроюстом, Європолом, Управлінням з питань запобігання зловживанням та шахрайству[224], Групою керівників уповноважених органів з питань захисту персональних даних країн Центральної та Східної Європи, членство в Глобальній мережі усунення порушень у сфері приватності (*Global Privacy Enforcement Network*, GPEN), регулярний експертний обмін з Радою Європи, участь у Міжнародній робочій групі з питань захисту персональних даних у сфері телекомунікацій (*International Working Group on Data Protection in Telecommunications,* IWGDPT)[225] та у конференціях Центрально- та Східноєвропейських органів влади із захисту персональних даних (*Central and Eastern European Data Protection Authorities*, CEEDPA).

З іншого боку, сайт Уповноваженого давно не оновлювався, тож на ньому неможливо знайти результати перевірок за останні роки. Актуальна інформація на сайті за 2015 рік. Так, у 2015 році посадові особи Управління з

[222] Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v1_02715-14.
[223] *Ibid.*
[224] ОЛАФ (OLAF, European Anti-Fraud Office), скорочення оригінальної назви французькою мовою.
[225] Козак В. *Захист персональних даних: право, практика, нагляд* / В. Козак [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/doccatalog/ document?id=51760.

питань захисту персональних даних здійснили 62 планові та позапланові перевірки:

- 17 володільців персональних даних, надають соціальні послуги, підвідомчі заклади та установи Міністерства соціальної політики України;
- 11 володільців персональних даних у сфері надання телекомунікаційних та інших споживчих послуг;
- 10 закладів та установ, бази даних яких містять інформацію, взяту із судових рішень або рішень адміністративних органів (будинки дитини, дитячі будинки-інтернати, психоневрологічні інтернати, геріатричні пансіонати, будинки-інтернати для громадян похилого віку та інвалідів тощо);
- 10 структурних підрозділів, підвідомчих закладів та установ Міністерства внутрішніх справ України та Державної міграційної служби України;
- 6 господарюючих суб'єктів, що здійснюють обробку персональних даних з метою надання медичної допомоги та медичних послуг;
- 3 володільця персональних даних призовників, військовозобов'язаних, мобілізованих і т.д.;
- 2 загальноосвітніх навчальних закладів, 2 ОСББ та 1 ЖЕК[226].

У 2015 році Управління з питань захисту персональних даних провело перевірку мобільного оператора «МТС» (ПрАТ «ВФ Україна»). Ми надіслали до Уповноваженої запит про надання інформації про результати перевірки. На жаль, відомості, які прийшли нам у відповідь мізерні, адже Секретаріат визначив майже всю інформацію такою, що містить комерційну таємницю (див. підрозділ 2.3.). Але нам надіслали припис № 9-15 від 29.12.2015 р. про усунення порушення вимог законодавства у сфері захисту персональних даних, виявленого під час перевірки ПрАТ «МТС Україна» (ПрАТ «ВФ Україна»)[227].

З цього припису можна зробити висновки, які саме порушення були допущені великим мобільним оператором. Зокрема, ПрАТ «МТС Україна»

[226] Результати перевірок на сайті Уповноваженого [Електронний ресурс]. – Режим доступу: http://www.ombudsman.gov.ua/ua/page/zpd/kontrol/rezultati-perevirok.
[227] Тут і далі – див. Додаток 4.

занадто довго зберігав дані своїх абонентів – понад строки позовної давності (3 роки) з моменту розірвання договірних відносин між суб'єктом персональних даних та володільцем. Уповноважений зобов'язав приватне акціонерне товариство припинити таке зберігання та видалити дані колишніх абонентів.

До того ж, ПрАТ «МТС Україна» не забезпечила надання своїм абонентам, які уклали договір про надання телекомунікаційних послуг, чи зареєструвалися в оператора в порядку, передбаченим ст. 32 Закону «Про телекомунікації», безоплатний доступ до своїх персональних даних, в тому числі, до розшифровок нарахованої до сплати суми за ненадані телекомунікаційні послуги без обмежень будь-яким розрахунковим періодом.

Фірма одержувала у працівників згоду на обробку персональних даних при оформленні трудових відносин та у випадках, коли така обробка здійснювалася відповідно до закону. У розділі другому, ми саме акцентували увагу на тому, що в таких випадках згода суб'єкта непотрібна.

Втім, у компанії не фіксували дати позбавлення права доступу до персональних даних працівників. Це могло би мати жахливі наслідки, якби стався витік даних, адже було би важко встановити, хто саме до цього причетний.

Кричущим порушенням була невідповідність Закону «Про захист персональних даних» додатку 3 «Зобов'язання про нерозголошення конфіденційної інформації» до Політики ІТТ-БЕУ-064-6 «Забезпечення режиму безпеки (конфіденційності) інформації в ПрАТ «МТС Україна», затвердженої наказом генерального директора ПрАТ «МТС Україна» від 25.02.2015 № ОД/Н 052.0. Ми неодноразово наголошували, що конфіденційна інформація містить «чутливі дані», обробка яких здійснюється за більш жорсткими правилами. Тому таке порушення недопустиме.

3.2. Відповідальність за порушення норм законодавства про захист персональних даних

Порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом. В іншому випадку не буде забезпечено виконання норм-заборон, які мають особливо вагоме значення у сфері захисту суспільних правовідносин. В самому ж Законі України «Про захист персональних даних» не прописано санкцій, на основі яких порушників можна було б притягнути до відповідальності, міститься лише бланкетна норма, що відсилає до інших законодавчих актів.

Притягати до адміністративної відповідальності мають право уповноважені особи секретаріату Уповноваженого Верховної Ради України з прав людини або його представники в силу положення ст. 255 КУпАП щодо порушень ст.ст. 188-39, 188-40 КУпАП[228].

Відповідно до ст. 188-39 КУпАП громадяни, посадові особи, фізичні особи - підприємці притягуються до адміністративної відповідальності за:

- неповідомлення або несвоєчасне повідомлення Уповноваженого (-ї) про зміну відомостей, які підлягають повідомленню, або подання неповних чи недостовірних відомостей;
- невиконання законних вимог (приписів) Уповноваженого (-ї) чи посадових осіб Секретаріату стосовно запобігання або усунення порушень законодавства;
- недодержання порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних[229].

Зокрема, згідно ч. 1 ст. 188-39 КУпАП накладається штраф на громадян – від ста до двохсот неоподатковуваних мінімумів доходів громадян, а на посадових осіб, громадян - суб'єктів підприємницької діяльності – у два рази

[228] Кодекс України про адміністративні правопорушення від 07.12.1984 // Відомості Верховної Ради УРСР. – 1984. – додаток до № 51. – Ст. 1123.
[229] *Ibid.*

більший[230]. Частина 2 цієї ж статті передбачає штрафну санкцію за невиконання законних вимог (приписів) омбудсмана або посадових осіб секретаріату щодо запобігання або усунення порушень законодавства про захист персональних – до трьохсот неоподатковуваних мінімумів доходів громадян, а для посадових осіб і громадян - суб'єктів господарювання – до однієї тисячі неоподатковуваних мінімумів доходів громадян[231]. За недодержання встановленого захисту персональних даних, що призвело до несанкціонованого доступу до них або порушення прав суб'єкта встановлено штраф для громадян – у розмірі до п'ятисот неоподатковуваних мінімумів доходів громадян, а для посадових осіб і громадян - господарюючих суб'єктів – до однієї тисячі неоподатковуваних мінімумів доходів громадян[232]. Передбачаються також більші штрафи за вчинення цих правопорушень повторно.

Раніше можна було притягнути до адміністративної відповідальності за неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням відомостей про нього до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються. На жаль, із внесенням змін до Закону України «Про захист персональних даних» такої санкції більше не існує, хоча вартувало би встановити[233].

Найбільш неоднозначною, на наш погляд, є ч.4 ст. 188-39 КУпАП. Вона складається з двох фактів, поєднаних причинно-наслідковим зв'язком: недодержання порядку захисту персональних даних і незаконний доступ до них[234].

Щодо, власне, «порядку захисту», то законотворець нормативно не закріпив таке визначення. Тут знову ж таки можна говорити про зобов'язання володільця вживати необхідні організаційні та технічні заходи для збереження даних (*privacy by default and by design*). Водночас, працівники мають

---

[230] Кодекс України про адміністративні правопорушення від 07.12.1984 // Відомості Верховної Ради УРСР. – 1984. – додаток до № 51. – Ст. 1123.
[231] *Ibid.*
[232] *Ibid.*
[233] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 98.
[234] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 95.

дотримуватися вимог конфіденційності (зазвичай, передбачені у спеціальних договорах чи в посадовій інструкції).

Тому до типових порушень законодавства про захист персональних даних належать: розголошення працівниками персональних даних, що стали їм відомі в ході виконання обов'язків; залишення робочого місця з незавершеною сесією роботи; передачу особистого паролю доступу іншим особам; відсутність особи чи структурного підрозділу з питань захисту персональних даних; відсутність системи ідентифікації користувача перед отриманням доступу до персональних даних; відсутність обліку операцій пов'язаних з обробкою персональних даних; неорганізоване ведення документації, недостатній рівень антивірусного захисту та інше[235].

Як уже зазначалося, важливим є саме причинно-наслідковий зв'язок між однією (чи кількома) з цих дій і порушенням прав суб'єкта персональних даних, несанкціонованим доступом до них.

Специфічною є регламентація порядку доступу до персональних даних третіх осіб. Власне кажучи, Закон у ст. 14 диференціює поняття доступу та поширення (передачу) даних третім особам. Згідно ст. 16 Закону доступ до даних базується на принципі «запит-відповідь». Якщо ж оприлюднення чи поширення відбулося без запиту, то такі дії не є «доступом»[236].

Що ж, це один з тих випадків, коли Закон термінологічно не співпадає з міжнародними документами, де доступу асоціюється виключно з правом самого суб'єкта персональних даних. Коли ж мова йде про отримання персональних даних третіми особами, таке може характеризуватися як розкриття (disclosure – у межах однієї країни), передача (transfer – транскордонна передача даних), поширення (dissemination). Фактично будь-яке протизаконне поширення, оприлюднення, чи передача даних третім особам

[235] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 95.
[236] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, ст. 481.

становить правопорушення, за яке винні мають нести відповідальність, зокрема адміністративну[237].

Проте, говорячи про наслідки у вигляді «порушення прав суб'єкта персональних даних», ми повинні розуміти, що мова йде про ст. 8 Закону. Тобто, такими порушеннями можуть бути, скажімо, відсутність доступу до своїх персональних даних у суб'єкта, чи інформації про порядок їх обробки, недотримання володільцем тридцятиденного строку для надсилання відповіді на запит суб'єкта даних, неможливість застосовувати засоби правового захисту тощо[238].

Насправді, на практиці доволі важко знайти кон'юнкцію між цими порушеннями та порядком захисту персональних даних. Вони, скоріше, є результатом умисних чи недбалих дій з боку володільця даних, тому їх слід кваліфікувати як окремі правопорушення.

Так само складно довести причинно-наслідковий зв'язок між несанкціонованим поширенням, передачею, оприлюдненням персональних даних та порушенням прав фізичної особи на захист своїх персональних даних від незаконної обробки тощо, передбаченої п. 7 ч. 2 ст. 8 Закону, та довести, що саме їх порушення призвело до небажаного результату. Для цього потрібно передбачити в законодавстві більш чіткі вимоги стосовно захисту персональних даних. До того ж, дуже сильно звужується обсяг відповідальності володільця даних, по суті, він напряму залежатиме від настання тяжких наслідків. Науковці стверджують, що в рідкісних випадках недотримання окремих чи кількох одразу норм призводить до порушення «порядку захисту»[239].

У Єдиному державному реєстрі судових рішень нам вдалося відшукати кілька проваджень, за результатами яких винних осіб було притягнуто до відповідальності за ч. 4 ст. 188-39 КУпАП.

Так, у справі №712/7475/17 у рішенні від 26 червня 2017 року Соснівський районний суд м. Черкаси встановив факт оприлюднення

---

[237] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 95.
[238] *Ibid.*
[239] *Ibid.*

заступником голови адміністративної комісії Черкаської міської ради персональних даних 26-и осіб, яких було притягнуто до адміністративної відповідальності на сайті «Facebook» (www.facebook.com) у мережі Інтернет у вільному доступі. Було вказано прізвище, ініціали, місце роботи, робоча адреса, обставини правопорушення, вид і розмір адміністративного стягнення. Суд констатував порушення вимоги ч. 3 ст. 10 (розголошення даних, що стали відомі у зв'язку з виконанням професійних обов'язків) та ч. 1 ст. 24 (незаконний доступ) Закону України «Про захист персональних даних»[240].

Підсудного було визнано винним у вчиненні адміністративного правопорушення, передбаченого ч. 4 ст. 188-39 КУпАП України і застосовано адміністративне стягнення у вигляді штрафу в розмірі 300 неоподаткованих мінімумів доходів громадян, що склало 5100 гривень на момент набрання чинності постанови[241].

Наступна стаття КУпАП, за якою можна притягнути до відповідальності за недотримання законодавства про захист персональних даних – ст. 188-40 КУпАП:

> "невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини тягне за собою накладення штрафу на посадових осіб, громадян – суб'єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян"[242].

В якості невиконання законних вимог розцінюються наступні дії працівників володільця:

- ненадання документів/інформації;
- невчасне надання документів/інформації;
- відмова в наданні документів/інформації;
- недопущення до проведення перевірки;

[240] Постанова Соснівського районного суду м. Черкаси від 27.06.2017. [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/67389027.
[241] *Ibid.*
[242] Кодекс України про адміністративні правопорушення від 07.12.1984 // Відомості Верховної Ради УРСР. – 1984. – додаток до № 51. – Ст. 1123.

- ненадання доступу до приміщень;
- ненадання доступу до інформації/ документів, що є в електронному вигляді[243].

У разі притягнення до адміністративної відповідальності, суб'єкт господарювання має можливість оскаржити постанову до місцевих загальних судів як адміністративним судів (ст. 20 КАС України)[244]. Скаргу на постанову по справі про адміністративне правопорушення може бути подано протягом десяти днів з дня винесення постанови (ст. 289 КУпАП), позаяк після закінчення цього строку вона набирає законної сили (ст. 291 КУпАП)[245].

Кримінальним кодексом України у ст. 182 також передбачено відповідальність за злочини у сфері обігу персональних даних. За порушення недоторканості приватного життя, а саме за протизаконну обробку конфіденційної інформації про особу або незаконну зміну такої інформації на винну особу накладається штраф від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або покарання у вигляді виправних робіт на строк до двох років, або арешт на строк до шести місяців, або обмеження волі на строк до трьох років[246]. Якщо діяння вчинено повторно чи було завдано істотну шкоду, тобто матеріальні збитки, які в сто і більше разів перевищують неоподатковуваний мінімум доходів громадян, то збільшується розмір санкцій. Максимальна межа – 5 років позбавлення волі[247].

З іншого боку, детально аналізуючи заборонені законодавством дії щодо персональних даних, можна констатувати, що часто вони спрямовані на завдання не збитків, а моральної шкоди. Тому слід, серед інших, застосовувати норми цивільно-правової відповідальності[248]. Це буде доречно, якщо доступ до

---

[243] Стандарти захисту персональних даних в соціальній сфері / М. В. Бем,, І. М. Городиський. – Львів: б.в., 2018. – С. 92.

[244] Кодекс адміністративного судочинства України // Закон України від 06.07.2005р. - № 35,-36, 37 // Відомості Верховної Ради. – 2005. – № 35-36, 37. – ст. 44.

[245] Кодекс України про адміністративні правопорушення від 07.12.1984 // Відомості Верховної Ради УРСР. – 1984. – додаток до № 51. – Ст. 1123.

[246] Кримінальний кодекс України: Кодекс України, Кодекс, Закон від 05.04.2001 № 2341-III // Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст. 131.

[247] *Ibid.*

[248] Сопілко І. М. *Щодо вдосконалення системи захисту персональних даних в процесі їх обробки* / І. М. Сопілко // Форум права. - 2013. - № 1. - С. 944.

персональних даних, що мали би використовуватися у маркетингових цілях отримають інші особи без легітимних підстав. Класичний випадок – злам даних. Тоді постраждала особа, суб'єкт персональних даних, зможе вимагати відшкодування завданої шкоди.

Наприклад, ст. 277 Цивільного кодексу наділяє фізичних осіб правом спростувати недостовірну інформацію або дати відповідь, незалежно від способу поширення такої інформації чи вини поширювача. Згідно ст. 278 ЦК рішенням суду можна заборонити розповсюдження інформації, якою порушуються особисті немайнові права, в номері (випуску) газети, у книзі, кінофільмі, теле-, радіопередачі тощо, а якщо усунення порушення неможливе, – вилучається тираж газети, книги тощо та підлягають знищенню[249].

Відповідно до ст. 296 ЦК використання імені допускається лише за згодою фізичної особи, а після її смерті – за згодою її дітей, вдови (вдівця), а за їх відсутності – батьків, братів та сестер. Не потрібно згоди суб'єкта у випадку використання його імені для висвітлення його власної діяльності або діяльності організації, членом якої він/вона є, а також – коли вказується тільки початкова літера прізвища у ЗМІ чи в літературних творах. Стосовно затриманого (-ї), підозрюваного (-ї), обвинуваченого (-ї), особи, яка вчинила адміністративне правопорушення, то має бути відповідне рішення суду, що набрало законної сили[250].

Тобто, не зважаючи на те, що Законом України «Про захист персональних даних» не передбачено міри покарання за незаконну обробку даних, – в інших правових актах. Тобто, підстави для притягнення винних осіб до відповідальності за порушення законодавства про захист персональних даних містяться у Законі, а порядок притягнення до відповідальності – в інших законодавчих актах (ЦК, КУпАП, КК та процесуальних кодексах). Отже, можливість здійснення захисту на належному рівні забезпечена.

---

[249] Цивільний кодекс України: Закон України № 435-IV від 16 січня 2003 р. // Офіційний вісник України. – 2003. – № 11. – Ст. 461.
[250] *Ibid.*

Однак, науковці іншої думки. Проблема в тому, що ми боремося з порушеннями законодавства про захист персональних даних уже *post factum.* Це не свідчить про системний підхід у сфері захисту прав людини і не сприятиме в цілому покращенню ситуації, що склалася. Так, суб'єктам, зокрема і маркетингової діяльності, простіше змінювати свої політики конфіденційності вже після винесення відповідного припису Уповноваженим, як в історії з ПрАТ «МТС Україна». У такому разі, їм просто нікуди дітися. А для Секретаріату Уповноваженого це – надмірне навантаження. Ці зусилля можна було би спрямувати на гармонізацію українського законодавства з європейськими стандартами[251].

Взагалі, така боротьба з порушниками є неефективною; вартувало б проводити ще й превентивні заходи. Тоді б не тільки наставали негативні наслідки для порушника, а й був певний попереджувально-стримуючий вплив на інших володільців персональних даних.

Фахівці пропонують ввести нові види відповідальності з мінімальними санкціями. Так, щоб за саме порушення імперативних вимог Закону, відповідальна особа несла негативні наслідки: як, наприклад, даних, незаконну обробку персональних даних (у даному випадку з порушенням статті 6, 7 та 11 Закону), обробку персональних даних на підставі згоди з порушенням основних вимог, що ставляться до неї (поінформованість, добровільність, наявність документів, що підтверджують її надання), відмову в наданні доступу суб'єкту до його персональних даних, надання неповних відомостей чи надання відповіді з порушенням визначених Законом строків, ненадання відомостей щодо порядку обробки персональних даних, ненадання відомостей про порядок доступу до персональних даних, незаконне поширення чи передача персональних даних, відсутність обліку операцій, пов'язаних з обробкою персональних даних, відмову змінити/видалити персональні дані, що не відповідають дійсності, непризначення відповідальної особи, нечітке

[251] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 92.

визначення її обов'язків, порушення умов щодо призначення розпорядника тощо[252].

З іншого боку, якщо порівнювати наше законодавство з вимогами більш актуального Загального регламенту про захист персональних даних, то помічаємо, що сучасне європейське право застосовує більш суворі санкції до правопорушників.

Наприклад, згідно ст. 82 Загального регламенту, контролер повинен відшкодувати усю заподіяну матеріальну та моральну шкоду. Тягар доказування непричетності до заподіяння шкоди лежить на обох – контролерові та операторові. При залученні декількох контролерів / операторів – шкода відшкодовується кожним із них у повному обсязі[253]. Тобто, мова йде про солідарне відшкодування.

Взагалі, Загальним регламентом передбачено, що санкції повинні бути дієвими, пропорційними та стримувальними, але відносить їх до дискреції держав-членів. У кожному разі, при вирішенні питання про накладення штрафу, береться до уваги:

- специфіка, ступінь тяжкості і тривалість порушення, обсяг і ціль опрацювання, кількість суб'єктів даних, та рівень шкоди, заподіяної їм;
- характер умислу (навмисно чи недбало);
- дії, вжиті контролером або оператором для зниження рівня заподіяної шкоди;
- ступінь відповідальності контролера або оператора, зважаючи на створені *privacy by default* та *by design*;
- наявність попередніх порушення з боку контролера або оператора;
- рівень співпраці з наглядовим органом для відшкодування порушення і скорочення можливих негативних наслідків порушення;
- категорії персональних даних;

[252] *Стандарти захисту персональних даних в соціальній сфері* / М. В. Бем,, І. М. Городиський, С. 98.
[253] Загальний регламент про захист даних (ЄС) 2016/679 від 27 квітня 2016 року [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16.

- спосіб, у який наглядовому органу стало відомо про порушення, тобто, чи контролер повідомив про це;
- чи були раніше застосовані до контролера або оператора попередження, стягнення, інші засоби реагування на порушення;
- дотримання затверджених кодексів поведінки;
- інші обставини, що обтяжують або пом'якшують відповідальність, наприклад, фінансова вигода або витрати, яких вдалося уникнути, прямо чи опосередковано, від порушення[254].

Штрафи за порушення норм Загального регламенту, сягають, на перший погляд, космічних сум – 10 млн. і 20 млн. євро і т.д.. Однак, збитки, завдані витоком чи зламом персональних даних, зазвичай, набагато більші[255].

Відтак, вважаємо за можливе і, навіть, необхідне, запозичити критерії з Регламенту, які враховуються при вирішенні питання про санкції. А також встановити відповідальність за вищезазначені порушення національного законодавства.

[254] Загальний регламент про захист даних (ЄС) 2016/679 від 27 квітня 2016 року [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16.
[255] *Ibid.*

ВИСНОВКИ ДО РОЗДІЛУ ІІІ

Отже, відповідальними особами за захист прав суб'єктів у ході використання цільового маркетингу можуть бути виробник продукції та постачальник послуг, маркетингова компанія, веб-переглядач, адміністратор веб-сторінок, пошукових систем. Усе залежить від того, хто, в якій мірі та яким чином отримав доступ до даних і як здійснюється обробка. Окремим питанням буде розглядатися, на якому етапі було вчинено порушення і хто саме в цей момент здійснював обробку (в якій із баз даних конкретні відомості зберігалися). Тобто, відповідальна особа встановлюватиметься відносно кожного конкретного випадку.

Особа, що здійснює обробку персональних даних повинна проводити превентивні заходи, спрямовані на виконання своїх обов'язків під час маркетингової діяльності.

До способів захисту прав суб'єктів персональних даних можна віднести самозахист, коли фізична особа може вимагати від володільця чи розпорядника даних задовольнити її права за ст. 8 Закону, наприклад, відкликати згоду на обробку персональних даних, вимагати їх зміни або знищення, відмовити у доступі до такої інформації третім особам.

Суб'єкт також користується правом оскаржити дії чи бездіяльність володільця або ж розпорядника персональних даних до суду чи Уповноваженого (-ї) Верховної Ради України з прав людини. Саме ці суб'єкти здійснюють контроль за дотриманням законодавства про захист персональних даних.

Так, Уповноважений (-а) має право на проведення перевірок, винесення припису про порушення законодавства, а також – на притягнення винних осіб до адміністративної відповідальності.

Справи про порушення законодавства про захист персональних даних у ході використання цільового маркетингу розглядаються в порядку цивільного, адміністративного (справи про адміністративні правопорушення) та

кримінального судочинства. Однак, у ході проведення дослідження, нами було встановлено, що таких проваджень майже немає. На жаль, мусимо визнати, що це не пов’язано з дотриманням прав суб’єктів персональних даних, а скоріше є системною проблемою – незнанням фізичними особами своїх прав, невиконанням володільцями та розпорядниками персональних даних своїх обов’язків до винесення відповідного припису Уповноваженим (-ою) та відсутністю превентивних механізмів, які би сприяли виправленню ситуації.

Відтак, пропонується передбачити Законом «Про захист персональних даних» можливості накладення бодай мінімальних санкцій на підприємства та організації, що здійснюють обробку персональних даних, порушуючи законодавство. Це сприятиме протидії правопорушенням і у сфері цільового маркетингу.

ВИСНОВКИ

Підсумовуючи, нагадаємо, що предметом законодавства про захист персональних даних у міжнародній та національній правових системах є правовідносини, що пов'язані з обробкою інформації про фізичну особу, яка ідентифікована чи може бути конкретно ідентифікована.

Водночас, було встановлено, що не дані, як такі, – право особи на приватність, потребує законодавчої регламентації. Воно набуло закріплення у різноманітних правових актах: міжнародних (локальних, універсальних) та національних (починаючи від Конституції, закінчуючи підзаконними актами). Основним для України є Закон «Про захист персональних даних».

Персональні дані становить будь-яка інформація про фізичну особу, завдяки якій можна ідентифікувати людину. Обробкою є будь-яка операція, що здійснюється з такими відомостями.

Персональні дані (в т.ч., файли *cookies* та дані логінування) використовуються у ході здійснення цільового маркетингу, адже це дозволяє орієнтувати виробництво продукції, надання послуг, на окремий, відібраний із декількох, сегмент ринку, тобто легітимною метою є забезпечення інтересів володільця даних. Однак, виникають ризики для захисту даних: віддалені сервери без належної згоди користувачів можуть зберігати їх інформацію; дані акумулюються у великих масивах, тому підвищуються ризики їх втрати, знищення, порушення вимог щодо захисту.

Тому нагальним постає питання забезпечення прав суб'єктів персональних даних на отримання інформації щодо обробки його персональних даних, на доступ до них, на заперечення проти обробки, видалення та зміну персональних даних і т.і. Ці права не можуть існувати без кореспондуючих обов'язків володільців даних стосовно визначення мети обробки, повідомлення суб'єкта персональних даних про обробку та отримання від нього добровільної, інформованої згоди, повідомлення про зміну мети обробки та отримання нової згоди та інші, передбачені законодавством.

Значну роль у захисті прав суб'єкта даних відіграють гарантії, що їх повинні надавати суб'єкти господарювання у ході застосування цільового маркетингу: знеособлення даних, використання системи подвійної асоціації, попередження про застосування тергетингових механізмів, заборона збереження у cookie-файлах «чутливих» даних, анонімізація та псевдонімізація клієнтів.

Дослідивши положення українського законодавства, ми здійснили їх порівняльний з нормами Загального регламенту, який вважається нормативно-правовим актом, що найкраще відповідає сучасному стану розвитку технологій цільового маркетингу. Внаслідок цього, ми дійшли висновку про відсталість національного регулювання. Це підтвердилося практикою. Суб'єкти господарювання, політику конфіденційності яких ми досліджували або прямо імплементували у свої правила положення Загального регламенту, або ж здійснювали порушення норм законодавства про захист персональних даних.

У зв'язку з цим, у третьому розділі, ми описали можливості захисту суб'єктом даних своїх прав. Передусім, Законом передбачено 2 види контролю: Уповноваженим (-ою) Верховної Ради України з прав людини та судами – в порядку цивільного, адміністративного та кримінального судочинства. Наявні також інші можливості захисту (самозахисту) фізичною особою своїх прав.

Якщо з введенням у дію Загального регламенту чисельність звернень до контролюючих органів стосовно використанням цільового маркетингу зросла у кілька разів, то в Україні таких рішень дуже мало. Суспільний резонанс навколо Загального регламенту вважаємо наслідком послідовної та системної політики у сфері захисту персональних даних. Втім, у нашій подальшій науковій та практичній діяльності, ми будемо продовжувати перевірку суб'єктів господарювання, які здійснюють маркетингову діяльність на предмет її відповідності нормам законодавства про захист персональних даних. Таким чином, ми реалізуємо право громадського контролю та, маємо надію, піднімемо питання захисту права людини на приватність, як одного з основоположних – у сучасному технологізованому світі на новий, якісно кращий, рівень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Міжнародні нормативно-правові акти

1. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Електронний ресурс]. – 2013. – Режим доступу: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

2. WP 136 Opinion 4/2007 on the concept of personal data [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

3. Американская Конвенция о Правах Человека [Електронний ресурс]. – Режим доступу: http://hrlibrary.umn.edu/russian/instree/Rzoas3con.html.

4. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року / Європейський Союз. – [Електронний ресурс]. Цит. 02.02.2018 р. Режим доступу – http://zakon4.rada.gov.ua/laws/show/994_242.

5. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних: Міжнародний договір / Офіційний вісник України. – 2011 – № 1, № 58. – 2010. – Ст. 1994. – Ст. 86.

6. Загальна декларація прав людини ООН від 10 грудня 1948 р. [Електронний ресурс] / Генеральна Асамблея ООН // Сайт Верховної Ради України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/995_015.

7. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних: Міжнародний договір / Офіційний вісник України. – 2011 – № 1, № 58. – 2010. – Ст. 1994. – Ст. 85.

8. Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 04 листопада 1950 року // Офіційний вісник України. – 1998. – № 13. – Ст. 270.

9. Конвенція про права дитини від 20.11.1989 р. // Зібрання чинних міжнародних договорів України. – 1990. – № 1. – С. 205.

10. Міжнародний пакт про громадянські і політичні права ООН від 6 грудня 1966 р. [Електронний ресурс] / Генеральна Асамблея ООН // Сайт Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_043.

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

12. Хартія основних прав Європейського Союзу [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/card/994_524#Current.

Національне законодавство

13. Конституція України прийнята Верховною Радою України 28.06.1996 р. № 254к/96–ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

14. Рішення Конституційного Суду України від 20.01.2012 р. № 2-рп/2012 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/v002p710-12.

15. Рішення Конституційного Суду України від 30.10.1997 р. № 5-зп (справа К. Г. Устименка) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v005p710-97.

16. Господарський кодекс України від 16.01.2003 р № 436-IV // Відомості Верховної Ради України. – 2003. – № 18. – № 19-20. – № 21-22. – Ст.144.

17. Кодекс адміністративного судочинства України // Закон України від 06.07.2005р. - № 35,-36, 37 // Відомості Верховної Ради. – 2005. – № 35-36, 37. – ст. 44.

18. Кодекс України про адміністративні правопорушення від 07.12.1984 // Відомості Верховної Ради УРСР. – 1984. – додаток до № 51. – Ст. 1123.

19. Кримінальний кодекс України: Кодекс України, Кодекс, Закон від 05.04.2001 № 2341-III // Відомості Верховної Ради України (ВВР). – 2001. – № 25-26. – Ст. 131.

20. Податковий кодекс України (Відомості Верховної Ради України (ВВР). – 2011. – № 13-14, № 15-16, № 17. – Ст.112.

21. Цивільний кодекс України: Закон України № 435-IV від 16 січня 2003 р. // Офіційний вісник України. – 2003. – № 11. – Ст. 461.

22. Закон України «Про Всеукраїнський перепис населення» Відомості Верховної Ради України (ВВР). – 2000. – № 51-52. – Ст. 446.

23. Закон України «Про Державний реєстр виборців» Відомості Верховної Ради України (ВВР). – 2007. – № 20. – Ст. 282.

24. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

25. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.

26. Закон України «Про інформацію» Відомості Верховної Ради України (ВВР) . – 1992. – № 48. – Ст. 650.

27. Закон України «Про Уповноваженого Верховної Ради України з прав людини» // Відомості Верховної Ради України. – 1998. – № 20.

28. Постанова Верховної Ради України «Про затвердження положень про паспорт громадянина України та про паспорт громадянина України для виїзду за кордон» Відомості Верховної Ради України (ВВР). – 1992. – № 37. – Ст. 545.

29. Наказ Ганеральної Прокуратури України від 13.07.2018 № 134 «Про затвердження Порядку обробки персональних даних в інформаційній автоматизованій системі "Облік передачі та отримання даних з Євроюсту"»

[Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0908-18.

30. Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v1_02715-14.

31. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v1_02715-14.

32. Про захист персональних даних (Текст резюме від 01.06.2010) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/anot/2297-17.

33. Роз'яснення до Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/n0001715-14.

Судова практика

34. «S. and Marper v. The United Kingdom» (заяви № 30562/04 і 30566/04, рішення від 04/12/2008)

35. Flinkkila and Others v. Finland (заява № 25576/04, рішення від 06.04.2010).

36. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (заява № C-131/12, рішення від 13.05.2014).

37. Patrick Breyer v Bundesrepublik Deutschland (справа № C-582/14, рішення від 19.10.2016).

38. Maximilian Schrems and Data Protection Commissioner (справа № 2013/765/JR від 10.12.2013).

39. College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer (заява № C-553/07, рішення від 07.05.2009).

40. «Avilkina and Others v. Russia» (заява № 1585/09, рішення від 06.06.2013)

41. Gaskin v. the United Kingdom (заява № 10454/83 від 07.07.1989 року).

42. «Rotaru v. Romania» (заява № 28341/95, рішення від 04.05.2000)

43. Von Hannover v. Germany (заява № 40660/08, рішення від 24.06.2005).

44. I. v. Finland (заява № 20511/03 від 17.06.2008).

45. Scarlet v Sabam Case (заява № C-70/10 від 24.11.2011).

46. Постанова Соснівського районного суду м. Черкаси від 27.06.2017. [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/67389027.

Наукова література

47. Bull H. P. Informationelle Selbstbestimmung – Vision oder Illusion. Mohr Siebeck, Tübingen 2011, 142 p.

48. De Hert P., Papakonstantinou V. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer law & Security review 2012, p. 130-142.

49. Hermstrüwer Y. Informationelle Selbstgefährdung, Tübingen 2016, 436p.

50. Lester A. Five Ideas to Fight For: How Our Freedom is Under Threat and Why It Matters. Oneworld Publications, London 2016, 256 p.

51. Mills J. Privacy. Oxford University Press, 2008, 408 p.

52. Pariser E. Filter Bubble: How the New Personalized Web is Changing what We Read and how We Think. Penguin Books 2012, 294 p.

53. Rössler B. Der Wert des Privaten. Suhrkamp Verlag, Frankfurt am Main 2001, 350 p.

54. Roßnagel A., Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, Springer Fachmedien Wiesbaden GmbH 2017, p. 131.

55. Sandfuchs B. Privatheit wider Willen. Mohr, Tübingen 2015, 287 p.

56. Schiedermair S. Der Schutz des Private. Suhrkamp Verlag AG, Berlin 2001, p. 22.

57. Scholz, P. Datenschutz beim Interneteinkauf. Nomos Verlagsgesellschaft, Baden Baden 2003, 464 p.

58. Schwichtenberg S. Datenschutz in drei Stufen. Springer Vieweg, Bremen 2018, 167 p.

59. Swire P., Ahmad K. Foundations of Information Privacy and Data Protections. International Association of Privacy Professionals, Portsmouth, 2012. p.4.

60. Брижко В.М. Організаційно-правові питання захисту персональних даних. Дис. … канд. юрид. наук: 12.00.07 Національна академія державної податкової служби України. – К., 2004.

61. Виноградова Г. В. Правове регулювання інформаційних відносин в Україні. – К., 2006. – 176 с.

62. Котлер Ф. Основы маркетинга / Филип Котлер, Гари Армстронг, Джон Сондерс, Вероника Вонг. – 2-е европ. изд. – М., СПб., К. : Изд. дом «Вильямс», 2006. – С. 32.

63. Марущак А. Інформаційне право: доступ до інформації. – К., 2007. – 535 с.

64. Нагнічук О. І. Співвідношення права на свободу вираження щодо публічних осіб та права на повагу до приватного та сімейного життя публічних осіб у практиці Європейського суду з прав людини / О. І. Нагнічук // Наукові записки НаУКМА. Юридичні науки. – 2015. – Т. 168. – С. 72-77.

65. Олійник В. С. Конституційне право людини на особисту недоторканність і його забезпечення органами внутрішніх справ України: дис. … кандидата юрид. наук : 12.00.02 «Конституційне право» / В. С. Олійник ; Київськ. нац. ун-т внутр. справ. – Київ, 2006. – 225 с.

66. Стандарти захисту персональних даних в соціальній сфері / М. В. Бем,, І. М. Городиський. – Львів: б.в., 2018. – 110 с.

Статті

67. Berman J., Mulligan D. Privacy in the Digital Age: Work in Progress// Nova Law Review. – 1999. – Vol. 23. – No 2.

68. Regan, P.M. Personal information policies in the United States and Britain: The dilemma of implementation considerations. Journal of Public Policy, 1984, 4(01). p. 19-38.

69. Воєводін Б. В. Цивільно-правові аспекти тарґетованої (цільової) реклами, персоналізації та приватності у рекламі / Б. В. Воєводін // Європейські перспективи. – 2013. – № 11. – С. 118.

70. Зоріна Ю.І. Цивільно-правові відносини при здійсненні рекламної діяльності : дис... канд. юрид. наук: 12.00.03 / Київський національний ун-т ім. Т.Г.Шевченка. – К., 2007. – С. 8.

71. Ищенко О. А. Вопросы правового регулирования рекламы в Российской Федерации / Ищенко О. А., Пермяков О. В. // Реклама и право. – 2004. – № 1. – С. 16.

72. Карась О. Таргетинг – один із видів стратегічної реклами / Олена Карась // Журнал європейської економіки. – 2014. – Т. 13, № 3. – С. 326.

73. Каретник О. С. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України / О. С. Каретник // Часопис Київського університету права. – 2013. – № 2. – С. 229.

74. Ліпкан В. Інформаційні права і свободи людини і громадянина / В. Лапкан, Ю. Максименко // Підприємництво, господарство і право. – 2011. – №9 (189). – С. 64.

75. Сопілко І. М. Щодо вдосконалення системи захисту персональних даних в процесі їх обробки / І. М. Сопілко // Форум права. – 2013. – № 1. – С. 944.

76. Чистов К. «Оценка по поведению» Технологии таргетинга сегодня и завтра // Інтернет-Форум. – 2007. – 21 бер. – С. 43–55.

Словники

77. Економічний енциклопедичний словник : В 2 т. / За ред. С. В. Мочерного. – Львів : Світ. – Т. 1. – 2005. – 616 с.

Електронні джерела

78. Bleich H. BGH bestätigt: Dynamische IP-Adressen sind personenbezogene Daten [Електронний ресурс]. – Режим доступу: https://www.heise.de/newsticker/meldung/BGH-bestaetigt-Dynamische-IP-Adressen-sind-personenbezogene-Daten-3714967.html.

79. Bundesgerichtshof zur Zulässigkeit der Speicherung von dynamischen IP-Adressen [Електронний ресурс]. – Режим доступу: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2017&Sort=3&nr=78289&pos=4&anz=78.

80. Cate F. The EU Data Protection Directive, Information Privacy, and the Public Interest [Електронний ресурс] / Fred H. Cate // Articles by Maurer Faculty. – 1995. – Режим доступу: https://www.repository.law.indiana.edu/facpub/646.

81. Davies J. Consumers Like Targeted Marketing Despite Privacy Concerns [Електронний ресурс]. – Режим доступу: http://digitalmarketingmagazine.co.uk/digital-marketing-data/consumers-like-targeted-marketing-despite-privacy-concerns/4531 (04.08.2017).

82. Die ePrivacy-Verordnung ist auf dem Weg! Womit müssen Sie rechnen? Digital Guide [Електронний ресурс]. – Режим доступу: https://hosting.1und1.de/digitalguide/websites/online-recht/eprivacy-verordnung/.

83. Digital advertisers battle over online privacy [Електронний ресурс] // The Economist. – 2016. – Режим доступу:

https://www.economist.com/business/2016/11/05/digital-advertisers-battle-over-online-privacy.

84. Drew R. Building the Global Heatmap [Електронний ресурс]. – Режим доступу: https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de.

85. EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour [Електронний ресурс]. – Режим доступу: https://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N101BF.

86. Grassegger H., Krogerus M., The Data That Turned the World Upside Down [Електронний ресурс]. – Режим доступу: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win (28.01.2017).

87. Hern A. Facebook and Google targeted as first GDPR complaints filed [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/technology/2018/may/25/facebook-google-gdpr-complaints-eu-consumer-rights.

88. Internetwerbung: Werbemöglichkeiten im Internet vs. Datenschutz? Datenschutz.org, [Електронний ресурс]. – Режим доступу: https://www.datenschutz.org/internetwerbung/

89. Koëter J. Behavioural targeting and data protection [Електронний ресурс]. – Режим доступу: http://www.cambridgeforums.com/ww.admin/materials/privacy/5Behavioral%20targeting_paper_draft%20publication_030510.pdf accessed on.

90. Nathan Ruser [Електронний ресурс]. – Режим доступу: https://twitter.com/Nrg8000/status/957318498102865920?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E957318498102865920&ref_url=https%3A%2F%2Frussian.rt.com%2Fworld%2Farticle%2F475068-fitnes-treker-voennye-bazy-ssha.

91. Opinion 2/2010 on “online behavioural advertising” [Електронний ресурс]. – 2010. – Режим доступу: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

92. Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

93. Rürup M., Gradow L. Mythen rund um DSGVO, Cookies, Einwilligung, E-Privacy – aufgelöst [Електронний ресурс]. – Режим доступу: https://t3n.de/news/mythen-rund-um-dsgvo-cookies-1123331/?utm_source=google&utm_medium=amp-button.

94. Schrems, Complaint against Facebook Ireland Ltd – 23 “PRISM” [Електронний ресурс]. – Режим доступу: http://www.europe-v-facebook.org/prism/facebook.pdf.

95. Telemediengesetz [Електронний ресурс]. – Режим доступу: https://dejure.org/gesetze/TMG/15.html.

96. Walker Reczek R., Summers C., Smith R. Targeted Ads Don’t Just Make You More Likely to Buy — They Can Change How You Think About Yourself [Електронний ресурс]. – Режим доступу: https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself.

97. Ward S. Small Business: Canada Expert Target Marketing [Електронний ресурс]. – Режим доступу: http://sbinfocanada.about.com/od/marketing/g/targetmarketing.htm.

98. Ализар А. Поведенческий таргетинг: назад в будуще. Вебпланета [Електронний ресурс]. – Режим доступу: webplanet.ru/news/advert/2007/8/30/behaviorism.html.

99. Алікберов А. Що таке cookies і як з ними працювати [Електронний ресурс]. – Режим доступу: http://citforum.ru/internet/html/cookie.shtml.

100. Безпека і анонімність в Інтернеті [Електронний ресурс]. – Режим доступу: http://estdomain.com.ua/bezpeka-i-anonimnist-v-interneti.

101. Богданов Б. Воздушные шарики в рекламе [Електронний ресурс]. – Режим доступу: http://telnews.ru/column/13061/http://medialaw.org.ua/analytics/povnyj-dostup-shho-zminyuye-zakonoproekt-0947.

102. Бородкин А. Поведенческий таргетинг: изображая жертву [Електронний ресурс]. – Режим доступу: http://itua.info/analytics/10100.html.

103. Видалення файлів cookie та керування ними. [Електронний ресурс]. – Режим доступу: https://support.microsoft.com/uk-ua/help/17442/windows-internet-explorer-delete-manage-cookies.

104. Інформація про файли cookie [Електронний ресурс]. – Режим доступу: http://www.canon.ua/cookie-information.

105. Козак В. Захист персональних даних: право, практика, нагляд / В. Козак [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/doccatalog/ document?id=51760.

106. Крутов М. Бігун – знахідка для шпигуна: популярний фітнес-застосунок «здав» приховані позиції військових [Електронний ресурс]. – Режим доступу: https://www.radiosvoboda.org/a/29007716.html.

107. Пазюк А.В. Захист права на приватність користувачів Інтернет. [Електронний ресурс]. – Режим доступу: https://docs.google.com/document/d/1uGCRGY3zI_HuxbrOGcylR9pFNU7UA_ZV9YtWNTbW6EI/edit?hl=ru.

108. Політика захисту персональних даних [Електронний ресурс]. – Режим доступу: https://www.facebook.com/privacy/explanation.

109. Про оголошення Google [Електронний ресурс]. – Режим доступу: https://support.google.com/ads/answer/1634057?hl=uk.

110. Прошли мимо кафе, а вам тут же показали его рекламу? Это не паранойя В Москве работает бесплатный вайфай. Его оператор собирает очень много данных пользователей [Електронний ресурс]. – Режим доступу:

https://meduza.io/feature/2018/10/24/proshli-mimo-kafe-a-vam-tut-zhe-pokazali-ego-reklamu-eto-ne-paranoyya?fbclid=IwAR2nvenZg2E8eF-Xg36YvSwB88Wp1h5IXt22S27v6wep-RbnQOCljk_FMUc

111. Публічна угода ТОВ «РУШ» [Електронний ресурс]. – Режим доступу: https://eva.ua/ua/publichnyj-dogovor/

112. Результати перевірок на сайті Уповноваженого [Електронний ресурс]. – Режим доступу: http://www.ombudsman.gov.ua/ua/page/zpd/kontrol/rezultati-perevirok.

113. Співак Н. Типові помилки у сфері захисту персональних даних / Співак Н. [Електронний ресурс]. – Режим доступу: http://www.apteka.ua/article/116863.

114. Степаненко О. О. Програмування Інтернет-застосувань [Електронний ресурс]. – Режим доступу: http://eir.zntu.edu.ua/bitstream/123456789/2873/1/Stepanenko_Methodical_instructions.pdf.

115. Хадсон А. Адресные рекламы знают о вас больше, чем вы думаете [Електронний ресурс]. – Режим доступу: http://www.bbc.com/ukrainian/mobile/ukraine_in_russian/2013/08/130801_ru_s_targeted_adverts.shtml.

ДОДАТОК 1

ТОВ «РУШ»
Код ЄДРПОУ 32007740
49055, Україна, м. Дніпро,
пр. О. Поля, 104 А

Олійник Вітани Олександрівни
79034, м. Львів,
[redacted]
паспорт [redacted]
тел.: [redacted]

Запит
про надання відомостей щодо обробки персональних даних

Шановні пані та панове!

Я, Олійник Вітана Олександрівна, [redacted] р.н., паспорт СЕ [redacted], є учасницею програми лояльності **«EVA МОЗАЇКА»** та власницею дисконтної картки мережі «**EVA**» №: «[redacted]».

Відповідно до пункту 10.1 Публічної угоди, розміщеної на Вашому сайті, персональні дані Користувача/Покупця обробляються відповідно до Закону України від 01 червня 2010 року № 2297-VI «Про захист персональних даних». Також згідно пункту 8.3. Правил участі у програмі лояльності «EVA МОЗАЇКА» мережі магазинів EVA, ТОВ «РУШ» Оператор і його уповноважені особи зобов'язуються забезпечувати зберігання персональних даних Учасника відповідно до Закону України «Про захист персональних даних».

Згідно частини 2 статті 8 Закону України «Про захист персональних даних», як власник своїх персональних даних, я маю право на отримання інформації, що стосується їх обробки.

У зв’язку з цим, прошу надати мені такі відомості:

1) чи здійснюється обробка моїх персональних даних, і якщо так – то яких саме;

2) джерела збирання, місцезнаходження моїх персональних даних, мету їх обробки;

3) хто є володільцем і чи є розпорядник моїх персональних даних, їх місцезнаходження або місце проживання (перебування);

4) умови надання доступу до персональних даних;

5) особи, яким передаються мої персональні дані. Зокрема, у п. 8.4. Правил участі у програмі лояльності «EVA МОЗАЇКА» мережі магазинів EVA, ТОВ «РУШ» вказано, що зазначені учасником в Анкеті персональні дані можуть бути використані Оператором та уповноваженими ним організаціями, в тому числі за межами України. Хто є цими уповноваженими організаціями;

6) механізм обробки персональних даних;

7) чи приймаються якісь автоматизовані рішення стосовно моїх персональних даних.

У разі ненадання ТОВ «Руш» запитуваної інформації, залишаю за собою право звернутися на підставі пункту 8 частини другої статті 8 Закону України «Про захист персональних даних» зі скаргою до Уповноваженого Верховної Ради України з прав людини, який, відповідно до статті 23 Закону, має повноваження з проведення перевірки володільців або розпорядників персональних, видання обов’язкових приписів щодо надання інформації, та притягнення до відповідальності за вчинення адміністративних правопорушень у сфері захисту персональних даних та доступу до публічної інформації, передбачених статтями 212-3 та 188-39 КУпАП.

Сподіваюся на Ваше розуміння та сприяння у наданні запитуваної мною інформації.

03.11.2018 р. Олійник В.О.

ДОДАТОК 2

Уповноваженій Верховної Ради України з прав людини
Секретаріат Уповноваженої
Верховної Ради України з прав людини
01008, м. Київ, вул. Інститутська, 21/8
Олійник Вікторії-Анни Олександрівни,
79034, м. Львів, [redacted]
тел.: [redacted]
e-mail: witanagr20@gmail.com

Скарга
про порушення права на отримання відомостей
щодо обробки персональних даних

Шановна Денісова Людмила Леонтіївна!

Звертаюсь до Вас у зв'язку з порушенням мого права на отримання відомостей щодо обробки персональних даних, що надане мені згідно ст. 8 Закону України «Про захист персональних даних». До суду з цього питання я ще не зверталася.

03.11.2018 року, я, Олійник Вікторія-Анна Олександрівна, звернулась до ТОВ «РУШ», код ЄДРПОУ 32007740, що зареєстроване за адресою: 49055, Україна, м. Дніпро, пр. О. Поля 104, із запитом, в якому просила надати мені таку інформацію:

1) чи здійснюється обробка моїх персональних даних, і якщо так – то яких саме;

2) джерела збирання, місцезнаходження моїх персональних даних, мету їх обробки;

3) хто є володільцем і чи є розпорядник моїх персональних даних, їх місцезнаходження або місце проживання (перебування);

4) умови надання доступу до персональних даних;

5) особи, яким передаються мої персональні дані. Зокрема, у п. 8.4. Правил участі у програмі лояльності «EVA МОЗАЇКА» мережі магазинів EVA, ТОВ «РУШ» вказано, що зазначені учасником в Анкеті персональні дані можуть бути використані Оператором та уповноваженими ним організаціями, в тому числі за межами України. Хто є цими уповноваженими організаціями;

6) механізм обробки персональних даних;

7) чи приймаються якісь автоматизовані рішення стосовно моїх персональних даних.

У своєму запиті я вказала, що у разі ненадання ТОВ «Руш» запитуваної інформації, залишаю за собою право звернутися на підставі пункту 8 частини другої статті 8 Закону України «Про захист персональних даних» зі скаргою до Уповноваженої Верховної Ради України з прав людини.

Так, Законом України «Про захист персональних даних» в абз. 3 ч. 5 ст. 16 передбачено необхідність задовольнити такий запит на отримання відомостей про обробку персональних даних протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

Відтак, пройшло вже тридцять чотири дні, а мій запит все ще не задоволено. Втім, мене не повідомлено ні про відстрочення, ні про відмову в доступі до персональних даних згідно ст. 17 зазначеного вище Закону.

Таким чином, відповідальні посадові особи ТОВ «Руш», які не відповіли на мій запит від 03.11.2018 року, **порушили моє право як суб'єкта персональних даних на отримання відомостей щодо їх обробки, що прямим порушенням норми закону.**

Відповідно, на мою думку, в їх діях є ознаки адміністративних правопорушень у сфері захисту персональних даних та доступу до публічної інформації, передбачених статтями 212-3 та 188-39 КУпАП.

Згідно з п. 8-1 частини 1 статті 255 КУпАП у справах про правопорушення, передбачені статтями 212-3 та 188-39 КУпАП (крім порушень права на інформацію відповідно до Закону України «Про адвокатуру та адвокатську діяльність»), протоколи про правопорушення мають право складати уповноважені особи секретаріату Уповноваженого Верховної Ради України з прав людини.

Відповідно до ст. 23 Закону України «Про захист персональних даних» серед повноважень Уповноваженої у сфері захисту персональних даних є право:

- проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженою, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;
- за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;
- складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом, тощо.

Крім того, пункти 1, 4, 5, 6, 7, 11, 14 частини 1 статті 13 Закону України «Про Уповноваженого Верховної Ради України з прав людини» передбачають, що Уповноважена Верховної Ради України за прав людини має право, зокрема:

- невідкладного прийому керівниками підприємств;
- безперешкодно відвідувати підприємства та ознайомлюватися з документами, у тому числі тими, що містять інформацію з обмеженим доступом, та отримання їх копій;

- вимагати від посадових осіб підприємств сприяння проведенню перевірок діяльності підконтрольних і підпорядкованих їм підприємств, установ, організацій, виділення спеціалістів для участі у проведенні перевірок, експертиз і надання відповідних висновків;
- запрошувати громадян України, іноземців та осіб без громадянства для отримання від них усних або письмових пояснень щодо обставин, які перевіряються по справі;
- направляти на відповідні підприємства акти реагування Уповноваженої у разі виявлення порушень прав і свобод людини і громадянина для вжиття цими підприємствами заходів;
- здійснювати інші повноваження, визначені законом, зокрема проводити перевірки за зверненнями громадян і громадянок відповідно до п. 1 ст. 16 Закону України «Про Уповноваженого Верховної Ради України з прав людини».

Водночас, ст. 14 Закону України «Про Уповноваженого Верховної Ради України з прав людини» передбачено обов'язок Уповноваженої забезпечувати виконання покладених на неї функцій та повною мірою використовувати надані їй права, як і зберігати конфіденційну інформацію.

На підставі вищевикладеного та керуючись статтями 8, 23 Закону України «Про захист персональних даних», статями 188-39, 212-3, 255 Кодексу України про адміністративні правопорушення, пунктами 1, 4, 5, 6, 7, 11, 14 частини 1 статті 13, статтею 14 Закону України «Про Уповноваженого Верховної Ради України з прав людини», статтею 20 Закону України «Про звернення громадян»,

ПРОШУ:

1. Розглянути мою скаргу в порядку, передбаченому законодавством, і вирішити у термін не більше одного місяця від дня її надходження, а про продовження терміну – повідомити мене, будь ласка.
2. Провести перевірку на предмет дотримання ТОВ «РУШ» законодавства про захист персональних даних.
3. Визначити, чи було вчинено посадовими особами ТОВ «РУШ» адміністративні правопорушення, передбачені статями 188-39, 212-3 КУпАП, у зв’язку з відмовою у наданні мені відомостей про обробку моїх персональних даних.
4. У разі виявлення адміністративних правопорушень, притягти до адміністративної відповідальності осіб, які протиправно обмежили доступ до відомостей про обробку моїх персональних даних.
5. Направити до ТОВ «РУШ» акти реагування на вищезазначені порушення мого права на отримання відомостей щодо обробки моїх персональних даних.

Додаток:

1. Копія квитанції про надсилання запиту до ТОВ «РУШ» про надання відомостей щодо обробки персональних даних.

7 грудня 2019 року _____ /Олійник В.-А. О./

ДОДАТОК 3

Уповноваженій Верховної Ради
України з прав людини
01008, Україна, м. Київ,
вул. Інститутська, 21/8

Олійник Вітани Олександрівни
79034, м. Львів,
[redacted]
[redacted]
E-mail: [redacted]

Запит
на отримання публічної інформації

Шановна Денісова Людмила Леонтіївна!

Відповідно до статті 34 Конституції України кожному гарантовано право на отримання, зберігання та поширення інформації. Гарантія права на інформацію забезпечується обов'язком органів державної влади та органів місцевого самоврядування, як розпорядників інформації, оприлюднювати інформацію, яка була отримана або створена в процесі їхньої діяльності згідно статтей 3, 4, 14 Закону України «Про доступ до публічної інформації».

Згідно статті 5 Закону України «Про доступ до публічної інформації» доступ до інформації забезпечується шляхом надання інформації за запитами на інформацію, при цьому згідно статті 19 цього закону запитувач має право звернутися до розпорядника інформації із запитом на інформацію незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини

подання запиту. Водночас, згідно статті 14 Закону України «Про Уповноваженого Верховної Ради України з прав людини», Секретаріат Уповноваженого з прав людини зобов'язаний за дорученням Уповноваженого забезпечити оприлюднення та надання інформації за запитами, адресованими Уповноваженому з прав людини, відповідно до Закону України «Про доступ до публічної інформації».

Зважаючи на вищенаведене, відповідно до статей 5, 6, 13 Закону України «Про доступ до публічної інформації», статей 5, 6 Закону України «Про інформацію», статті 14 Закону України «Про Уповноваженого Верховної Ради України з прав людини» прошу надати інформацію:

1) акт за результатами перевірки оператора мобільного зв'язку «МТС» (ПрАТ «ВФ Україна»);

2) протокол за результатами перевірки оператора мобільного зв'язку «МТС» (ПрАТ «ВФ Україна»), за наявності такого;

3) припис, винесений за результатами цієї перевірки.

Відповідно до статті 20 Закону України «Про доступ до публічної інформації», прошу надати відповідь протягом 5 робочих днів з дня отримання запиту. Відповідь прошу надіслати на адресу: 79034, м. Львів, вул. Червоної калини 7а або на адресу електронної пошти: witanagr20@gmail.com.

У випадку, якщо запитувана інформація буде перевищувати 10 сторінок, гарантую відшкодування фактичних витрат на копіювання та друк згідно зі статтею 21 Закону України «Про доступ до публічної інформації».

Звертаю Вашу увагу, що у разі ненадання відповіді на запит або надання неповної інформації, залишаю за собою право звернутися до суду або вимагатиму притягнення Вас до адміністративної відповідальності за статтею 212-3 Кодексу України про адміністративні правопорушення.

Сподіваюся на Ваше розуміння та сприяння у наданні запитуваної мною інформації.

03.11.2018 р. Олійник В.О.

ДОДАТОК 4

ПРЕДСТАВНИК
Уповноваженого Верховної Ради України з прав людини
вул. Інститутська, 21/8, м. Київ, 01008 E-mail: hotline@ombudsman.gov.ua тел. (044) 253 48 59, факс 226 34 27

06.12.2018 № 5/9-003736.18/35-177

На №_____ від __.__.20__

Олійник В.О.

[redacted]

Шановна Вітано Олександрівно!

У відповідь на Ваш інформаційний запит від 19.11.2018 (отриманий 30.11.2018), щодо отримання інформації про результати перевірки «МТС» (ПрАТ «ВФ Україна»), повідомляю таке.

Відповідно до пункту 2 частини першої статті 23 Закону України «Про захист персональних даних» Уповноважений Верховної Ради України з прав людини (далі – Уповноважений) має право проводити планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим. На виконання зазначених повноважень Уповноваженим був розроблений та затверджений Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних (наказ Уповноваженого від 08.01.14 № 1/2-14) (далі - Порядок).

Для здійснення вищезазначеної функції контролю за додержанням законодавства про захист персональних даних Уповноважений наділений відповідними повноваженнями. Зокрема, згідно з частиною 3 частини першої статті 23 Закону України «Про захист персональних даних» отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом. При цьому відповідно до пункту 5.9. Порядку, будь-яка інформація, яка стала відомою Уповноваженому та/або

уповноваженій посадовій особі (особам) під час проведення перевірки, не підлягає розголошенню.

Зважаючи на наведене вище, у розумінні пункту 1 частини другої статті 6 Закону України «Про доступ до публічної інформації», інформація, надана суб'єктом перевірки на вимогу перевіряючих вважається такою, що отримана конфіденційно.

При цьому Акт перевірки додержання вимог законодавства про захист персональних даних містить відомості отримані конфіденційно (пункт 1 частини другої статті 6 Закону України «Про доступ до публічної інформації»), які у розумінні статті 505 Цивільного кодексу України є комерційною таємницею, розголошення якої може призвести до завдання істотної шкоди легітимним інтересам суб'єкта перевірки, яка на момент надання відповіді на Ваш запит буде значно переважати суспільний інтерес в її отриманні (пункти 2 та 3 частини другої статті 6 Закону України «Про доступ до публічної інформації»).

Відповідно до частини другої статті 7 Закону України «Про доступ до публічної інформації» розпорядники інформації, визначені частиною першою статті 13 цього Закону, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди - лише в інтересах національної безпеки, економічного добробуту та прав людини.

Відтак, запитувана Вами інформація може бути надана лише за згодою осіб, яких вона стосується, або в інтересах національної безпеки, економічного добробуту та прав людини.

Так, викладені у Вашому запиті від 19.11.2018 аргументи з метою отримання доступу до конфіденційної інформації жодним чином не відображають суспільного інтересу, а також інтересів національної безпеки, економічного добробуту та прав людини.

Відповідно, запитувана Вами інформація стосується комерційної діяльності особи, а поширення її за відсутності згоди ПрАТ «ВФ Україна» не є необхідним та допустимим.

Враховуючи зазначене вище, відповідно до частини сьомої статті 6 Закону України «Про доступ до публічної інформації» надсилаємо Вам копію Акту перевірки додержання вимог законодавства про захист персональних даних, за виключенням інформації, що не підлягає наданню.

Водночас, надаємо копію Припису про усунення порушень вимог законодавства у сфері захисту персональних даних, виявлених під час перевірки від 29.12.2015 № 9-15.

Інших документів за результатами перевірки не видавалось.

Особою, відповідальною за розгляд Вашого запиту є головний спеціаліст відділу перевірок дотримання інформаційних прав Департаменту моніторингу інформаційних прав Секретаріату Уповноваженого Верховної Ради України з прав людини Онопченко Марина Сергіївна.

Також інформую, що відповідно до статті 23 Закону України «Про доступ до публічної інформації» прийняте рішення за результатом розгляду

запиту на інформацію може бути оскаржено до керівника розпорядника інформації, вищого органу або суду. Оскарження рішень, дій чи бездіяльності розпорядників інформації до суду здійснюється відповідно до Кодексу адміністративного судочинства України.

Додаток: на 5 арк.

З повагою
представник Уповноваженого
з дотримання інформаційних
прав та представництва
в Конституційному Суді України **В. Барвіцький**

Примірник 2

АКТ
перевірки додержання законодавства про захист персональних даних

«29» травня 2015 року м. Київ

Нами, завідувачем відділу контролю Управління з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини Кривлею С.Г., головним спеціалістом відділу контролюУправління з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини Мамчуром Ю.І., провідним спеціалістом відділу контролю Управління з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини Курупом В.М., спеціалістом І категорії відділу контролю Управління з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини Мельничук А.О., у присутності:

- начальника Департаменту безпеки ПрАТ «МТС Україна» Вінцевича Д.С.;
- старшого експерта з питань інформаційної безпеки Погуляки А.Г.;
- спеціаліста криптозахисту інформації відділу інформаційної безпеки Кравченка Д.М.;
- начальника Юридичного департаменту Полякова С.

(посада, ПІБ керівника (уповноваженої ним особи) юридичної особи або ПІБ фізичної особи, якою проводилась перевірка)

проведено *позапланову виїзну*
(планової, позапланової, документарної, виїзної)

перевірку додержання законодавства у сфері захисту персональних даних

ПрАТ «МТС Україна»,
що знаходиться за адресою: вул. Лейпцизька, 15, м. Київ
(найменування, місце знаходження юридичної особи або ПІБ, місце проживання фізичної особи, якою проводилась перевірка)

Перевірку розпочато: «*23*» *червня* 2015 року о *09* год. *35* хв.
Перевірку закінчено: «*21*» *липня* 2015 року о *13* год. *00* хв.

У ході перевірки було досліджено такі документи:

1. Статут ПрАТ «МТС Україна», затверджений позачерговими зборами акціонерів ПрАТ «МТС Україна» від 19.05.2015 (протокол № 34);

2. Наказ генерального директора ПрАТ «МТС Україна» від 25.02.2015 № ОДИ-052.0 «Про введення в дію Політики ІТ-БЕУ 064-6 «Забезпечення режиму безпеки (конфіденційності) інформації в ПрАТ «МТС Україна»;

3. Наказ генерального директора ПрАТ «МТС Україна» від 17.06.2014 № ОДИ-177.0 «Про введення в дію Політики ІТ-БЕУ 012-3 «Обробка персональних даних в ПрАТ «МТС Україна»;

4. Наказ генерального директора ПрАТ «МТС Україна» від 03.12.2012 № ОДИ-540 «Про введення в дію Регламента процесу РП-БЕУ 140-3 «Організація діловодства з матеріальними носіями інформації, що містять комерційну та іншу конфіденційну інформацію ПрАТ «МТС Україна»;

5. Наказ генерального директора ПрАТ «МТС Україна» від 13.09.2013 № ОДИ-311.0 «Про введення в дію нової версії «Договору про надання послуг

[далі на сторінках з 2 по 28 міститься інформація, що стосується комерційної діяльності ПрАТ «ВФ Україна»]

Перевірку провели:

Завідувач відділу контролю Управління з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини — (підпис) — Кривда С.Г. (прізвище, ініціали)

Головний спеціаліст відділу контролю Управління з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини — (підпис) — Мамчур Ю.І. (прізвище, ініціали)

Провідний спеціаліст відділу контролю Управління з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини — (підпис) — Куруц В.М. (прізвище, ініціали)

Спеціаліст І категорії відділу контролю Управління з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини — (підпис) — Мельничук А.О. (прізвище, ініціали)

Акт перевірки складено у двох примірниках:

Перший примірник знаходиться в *ПрАТ «МТС Україна»*

Другий примірник знаходиться у *Секретаріаті Уповноваженого Верховної Ради України з прав людини*

З Актом перевірки ознайомлений:

Акт підписано із зауваженнями

Нач. ДБ Вишневе де — (посада) — 22.01.2016 (прізвище, ініціали, дата)

Один примірник Акта перевірки отримав:

Нач. ДБ Вишневе де — (посада, ПІБ керівника (уповноваженої ним особи) юридичної особи або ПІБ фізичної особи, щодо якої проводилась перевірка) — (підпис) — 22.01.2016 (дата)

Примірник 2

ПРИПИС № 9-15

про усунення порушення вимог законодавства у сфері захисту персональних даних, виявленого під час перевірки

29 грудня 2015 року
(дата складання припису)

вул. Інститутська, 21/8, м. Київ
(місце складання припису)

Видано

ПрАТ «МТС Україна»,
що знаходиться за адресою: Лейпцизька, 15, м. Київ, 01601
Генеральний директор – Іван Золочевський

(найменування юридичної особи, її місцезнаходження, прізвище, ім'я та по батькові керівника юридичної особи прізвище, ім'я та по батькові, місце проживання фізичної особи, щодо якої проводилась перевірка)

Згідно з Актом перевірки додержання законодавства у сфері захисту персональних даних, яка відбулась

у період з 23 червня 2015 року по 21 липня 2015 року
в ПрАТ «МТС Україна»,
що знаходиться за адресою: Лейпцизька, 15, м. Київ, 01601

(дата, місце проведення перевірки)

встановлено порушення:

– ч. 3 ст. 6, п. 2 ч. 2 ст. 15 Закону України «Про захист персональних даних» та п.п. 2.3, 2.10 Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14, щодо обов'язку володільця персональних даних здійснювати обробку персональних даних суб'єктів у пропорційно визначений меті обробки строк (строк має бути не більший, ніж це необхідно для мети їх обробки);

– п. 3 ч. 2 ст. 8, ч. 6 ст. 16, ч. 1 ст. 19 Закону України «Про захист персональних даних» щодо гарантування володільцем персональних даних суб'єкту персональних даних права безоплатного доступу до будь-яких відомостей про себе.

Зобов'язую:

1. Припинити зберігати персональні дані абонентів ПрАТ «МТС Україна» понад строки позовної давності (3 роки) з моменту припинення договірних відносин між суб'єктом персональних даних та володільцем (розпорядником) (*строк виконання 31 січня 2016 року*).

2. Видалити (знищити) персональні дані абонентів ПрАТ «МТС Україна», що зберігаються понад строки позовної давності (3 роки) з моменту припинення договірних відносин між суб'єктом персональних даних та володільцем (розпорядником) (*строк виконання 31 січня 2016 року*).

3. Забезпечити надання абонентам ПрАТ «МТС Україна», які уклали договір про надання телекомунікаційних послуг, чи зареєструвалися в оператора в порядку, передбаченому ст. 32 Закону України «Про телекомунікації», безоплатний доступ до своїх персональних даних, в тому числі до розшифровок нарахованої до сплати суми за надані

телекомунікаційні послуги без обмежень будь-яким розрахунковим періодом (*строк виконання 31 січня 2016 року*).

4. Припинити одержувати у працівників ПрАТ «МТС Україна» згоду на обробку персональних даних при оформленні трудових правовідносин та у випадках, коли така обробка здійснюється відповідно до закону (*строк виконання 31 січня 2016 року*).

5. Забезпечити фіксацію дати позбавлення права доступу працівників ПрАТ «МТС Україна» до персональних даних суб'єктів (*строк виконання 31 січня 2016 року*).

6. Привести додаток 3 «Зобов'язання про нерозголошення конфіденційної інформації» до Політики ПТ-БЕУ-064-6 «Забезпечення режиму безпеки (конфіденційності) інформації в ПрАТ «МТС Україна», затвердженої наказом генерального директора ПрАТ «МТС Україна» від 25.02.2015 № ОДИ 052.0, у відповідність із Законом України «Про захист персональних даних» (*строк виконання 31 січня 2016 року*).

Юридичній особі або фізичній особі, яка отримала припис, необхідно направити письмову інформацію про виконання припису до Уповноваженого Верховної Ради України з прав людини.

Цей припис підлягає обов'язковому виконанню у строк – до 31 січня 2016 року.

Строк інформування про усунення виявленого порушення – до 05 лютого 2016 року.

Припис складено у двох примірниках:

Перший примірник знаходиться *в ПрАТ «МТС Україна»*

Другий примірник знаходиться *у Секретаріаті Уповноваженого Верховної Ради України з прав людини*

Уповноважена посадова особа: _____ **Кривда С.Г.**
(підпис)